8次多項式のガロア群が $\mathrm{PGL}_2(\mathbb{F}_7)$ に同型であることの証明手法

本稿では、有理数体 $\mathbb{Q}$ 上の8次多項式 $f(x) \in \mathbb{Q}[x]$ の最小分解体 L に関するガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ が射影一般線型群 $\mathrm{PGL}_2(\mathbb{F}_7)$ に同型であることを示すための具体的な方法論を、集合と写像の言葉を用いて論理的に厳密なステップで解説する。

1. 基本概念の定義

1.1. ガロア群と最小分解体

有理数体 $\mathbb{Q}$ 上の多項式 $f(x)$ の最小分解体 (splitting field) とは、$f(x)$ のすべての根を含む $\mathbb{Q}$ の最小の拡大体のことである。これを L と書く。

> **定義 1.1 (ガロア群)**
>
> 体拡大 $L/\mathbb{Q}$ のガロア群 (Galois group) $\mathrm{Gal}(L/\mathbb{Q})$ とは、L の自己同型写像 $\sigma : L \to L$ であって、任意の $a \in \mathbb{Q}$ に対して $\sigma(a) = a$ を満たすもの全体が写像の合成に関してなす群のことである。

$f(x)$ の次数が8で、$\mathbb{Q}$ 上分離的 (重複する根を持たない) であると仮定する。このとき L は $f(x)$ の8個の根 $\alpha_1, \alpha_2, \ldots, \alpha_8$ で生成される。任意の自己同型 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ は $f(x)$ の根の集合 $R = \{\alpha_1, \ldots, \alpha_8\}$ を R 自身へ全単射として写す。したがって、制限写像 $\sigma|_R$ を考えることにより、$\mathrm{Gal}(L/\mathbb{Q})$ は8次対称群 S_8 の部分群と自然に同一視できる。多項式 $f(x)$ が $\mathbb{Q}$ 上既約であることは、$\mathrm{Gal}(L/\mathbb{Q})$ が R 上に推移的 (transitive) に作用することと同値である。

1.2. 射影一般線型群 $\mathrm{PGL}_2(\mathbb{F}_7)$ の作用

次に、目的の群である $\mathrm{PGL}_2(\mathbb{F}_7)$ を定義し、それが8次置換群として実現される仕組みを記述する。$\mathbb{F}_7$ を位数7の有限体とする。

> **定義 1.2 (射影一般線型群)**
>
> 一般線型群 $\mathrm{GL}_2(\mathbb{F}_7)$ を、成分が $\mathbb{F}_7$ に属し、行列式が 0 でない 2×2 行列全体のなす群とする。その中心 Z はスカラー行列のなす正規部分群 $Z = \{cI \mid c \in \mathbb{F}_7^\times\}$ である。射影一般線型群 (projective general linear group) $\mathrm{PGL}_2(\mathbb{F}_7)$ は、商群 $\mathrm{GL}_2(\mathbb{F}_7)/Z$ として定義される。

この群は、$\mathbb{F}_7$ 上の射影直線 (projective line) $\mathbb{P}^1(\mathbb{F}_7) = \mathbb{F}_7 \cup \{\infty\}$ に自然に作用する。すなわち、行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_7)$ の属する剰余類は、$z \in \mathbb{P}^1(\mathbb{F}_7)$ に対して一次分数変換として以下のように作用する。

$$\phi_A(z) = \frac{az + b}{cz + d}$$

ここで、分母が 0 になる場合は ∞ に写され、∞ は a/c に写されるとする。$\mathbb{P}^1(\mathbb{F}_7)$ の元の個数は $7 + 1 = 8$ 個である。$\mathrm{PGL}_2(\mathbb{F}_7)$ の各元はこの8個の元の上の置換を引き起こし、この作用は忠実 (faithful) である。すなわち、単位元以外の元は非自明な置換を引き起こすため、単射な群準同型 $\mathrm{PGL}_2(\mathbb{F}_7) \hookrightarrow S_8$ が得られる。$\mathrm{GL}_2(\mathbb{F}_7)$ の位数は

$(7^2-1)(7^2-7)=2016$ であり、Z の位数は6であるから、$\mathrm{PGL}_2(\mathbb{F}_7)$ の位数は $2016/6=336$ となる。

> **例: 作用の具体例**
>
> 行列 $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ は変換 $z\mapsto z+1$ を引き起こす。この変換は $\infty\mapsto\infty$ と固定し、$0\mapsto 1\mapsto 2\mapsto\ldots\mapsto 6\mapsto 0$ という長さ7の巡回置換となる。したがって、この元のサイクル型は $(7,1)$ である。

2. 証明の具体的メソッド (下からの評価)

$f(x)$ のガロア群を $G=\mathrm{Gal}(L/\mathbb{Q})\subset S_8$ とする。$G\cong\mathrm{PGL}_2(\mathbb{F}_7)$ であることを完全に証明するためには、下からの評価 (元の存在による部分群の生成) と上からの評価 (不変量による包含関係の限定) を組み合わせるアプローチを取る。

2.1. 多項式 $f(x)$ の既約性 (推移性の保証)

まず、G が S_8 の推移的部分群であることを示さなければならない。これは $f(x)$ が $\mathbb{Q}[x]$ において既約であることを示すことに帰着される。特定の素数 p に対してモジュロ p で還元した多項式 $\bar{f}(x)\in\mathbb{F}_p[x]$ が8次の既約多項式になることを確認するか、あるいはEisensteinの既約判定法を用いる。既約性が証明されれば、ガロア群 G の根への作用の軌道 (orbit) はただ1つとなり、G は推移群であると結論づけられる。

2.2. Dedekindの定理とサイクル型の網羅的探索

ガロア群の元のサイクル型 (cycle type) を決定するための実用的な定理が Dedekindの定理 (Dedekind's theorem) である。

> **定理 2.1 (Dedekind)**
>
> $f(x)\in\mathbb{Z}[x]$ をモニック多項式とする。素数 p が $f(x)$ の判別式を割り切らないとき、$f(x)$ の各係数を法 p で還元して得られる多項式を $\bar{f}(x)\in\mathbb{F}_p[x]$ とする。もし $\bar{f}(x)$ 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 $\mathbb{Q}$ 上のガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ は、根の置換群として表現したときに、長さがそれぞれ $d_1,d_2,\ldots,d_k$ の互いに素な巡回置換の積となる元を含む。

$\mathrm{PGL}_2(\mathbb{F}_7)$ の元のサイクル型を $\mathbb{P}^1(\mathbb{F}_7)$ への作用を通じて分類すると、以下のような特徴的な型が存在する。

- **型 $(7,1)$**: 例として $z\mapsto z+1$ は ∞ を固定し、残り7元を巡回させる。位数7。
- **型 (8)**: 2-Sylow部分群の生成元に対応する位数8の元。
- **型 $(2,2,2,1,1)$**: 例として $z\mapsto -z$ は $0,\infty$ を固定する奇置換。位数2。

いくつかの素数 p_1,p_2 を選び、$f(x)$ をそれぞれ $\mathbb{F}_{p_i}$ 上で因数分解する。Dedekindの定理により、例えば p_1 で還元したときに8次既約になれば、型 (8) の元が G に存在することが言える。同様に、p_2 で7次既約多項式と1次式の積になれば、型 $(7,1)$ の元が G に存在することが保証される。これらの元によって生成される G の部分群を H とすると、$H\subset G$ であり、$H\cong\mathrm{PGL}_2(\mathbb{F}_7)$ であることが、計算的群論における推移群の分類から従う。これにより、群の位数について $|G|\geq 336$ が示される。

3. 分解式を用いたガロア群の上限の決定 (上からの評価)

ステップ2で得られた結論は G が $\mathrm{PGL}_2(\mathbb{F}_7)$ を部分群として含むということである。次に、G が $\mathrm{PGL}_2(\mathbb{F}_7)$ より大きくならないこと、すなわち $G\subset\mathrm{PGL}_2(\mathbb{F}_7)$ であることを示さなければならない。このために、群の作用とそれに付随する多

項式不変量 (分解式) を用いた代数的なメカニズムを厳密に構築する。

3.1. 判別式による交代群の排除

まず、多項式 $f(x)$ の判別式 $\Delta(f)$ を計算し、それが有理数の平方数ではないことを確認する。判別式は根の差の積の2乗であり、ガロア群が偶置換のみからなる交代群 A_8 に含まれるための必要十分条件は $\Delta(f)$ が平方数となることである。$\Delta(f)$ が平方数でない場合、G には奇置換が存在することが証明される。実際、$\mathrm{PGL}_2(\mathbb{F}_7)$ は型 (8) や型 $(2,2,2,1,1)$ のような奇置換を含んでおり、この事実と整合する。

3.2. $\mathrm{PGL}_2(\mathbb{F}_7)$ と 3-$(8,4,1)$ デザイン

$\mathrm{PGL}_2(\mathbb{F}_7)$ は S_8 の中で、ある特定の組合せ論的構造 (Steiner系) の自己同型群として一意に特徴づけられる。この構造を利用して、G がその構造を保存する部分群であることを示す。

> **定義 3.1 (3-$(8,4,1)$ デザイン)**
>
> 8個の元からなる有限集合 X と、その4点部分集合の族 (これをブロックと呼ぶ) $\mathcal{B}$ の組 $(X, \mathcal{B})$ であって、以下の条件を満たすものを 3-$(8,4,1)$ デザインと呼ぶ。
> ・ X の任意の3点部分集合は、$\mathcal{B}$ のただ1つのブロックに包含される。

組合せ論的な計算により、ブロックの総数は $\binom{8}{3} / \binom{4}{3} = 56/4 = 14$ 個となる。$X = \mathbb{P}^1(\mathbb{F}_7)$ としたとき、$\mathrm{PGL}_2(\mathbb{F}_7)$ の作用によってブロックがブロックへ写されるような特定のブロック族 $\mathcal{B}_0$ が存在する。重要な事実は、S_8 においてこの構造 $(X, \mathcal{B}_0)$ を保つ自己同型群、すなわち $\mathcal{B}_0$ を全体として $\mathcal{B}_0$ に写す置換の全体が、正確に $\mathrm{PGL}_2(\mathbb{F}_7)$ と一致することである。なお、このような構造はFano平面の拡張に関連している。

3.3. 不変多項式の構成

$G \subset \mathrm{PGL}_2(\mathbb{F}_7)$ を示すことは、$f(x)$ の根の集合 $R = \{\alpha_1, \ldots, \alpha_8\}$ の上に、ガロア群 G の作用で不変となる 3-$(8,4,1)$ デザインの構造が存在することを代数的に示すことと同値である。このために「不変多項式」を構成する。

> **定義 3.2 (不変多項式)**
>
> 変数 $x_1, \ldots, x_8$ の多項式 $P(x_1, \ldots, x_8)$ であって、その S_8 における固定部分群 (stabilizer) がちょうど $\mathrm{PGL}_2(\mathbb{F}_7)$ となるものを不変多項式と呼ぶ。

このような多項式 P は、具体的には次のように構成できる。先述のブロック族 $\mathcal{B}_0$ に属する14個の各ブロック $\{i,j,k,l\}$ に対して、単項式 $x_i x_j x_k x_l$ を作り、それらの和をとる。

$$P(x_1, \ldots, x_8) = \sum_{\{i,j,k,l\} \in \mathcal{B}_0} x_i x_j x_k x_l$$

置換 $\sigma \in S_8$ は変数の添字に自然に作用する。構成から、$\sigma \cdot P = P$ が成り立つことと $\sigma \in \mathrm{PGL}_2(\mathbb{F}_7)$ であることは同値である。この多項式は直観的にもブロック構造を代数的に表現したものである。

3.4. 分解式 (Resolvent) の計算と有理根の判定

次に、この不変多項式を用いて、ガロア群が $\mathrm{PGL}_2(\mathbb{F}_7)$ に含まれるかどうかを判定するための方程式を構成する。S_8 における $\mathrm{PGL}_2(\mathbb{F}_7)$ の指数は $m = 40320/336 = 120$ である。左剰余類 $S_8/\mathrm{PGL}_2(\mathbb{F}_7)$ の完全代表系を $\{\tau_1, \ldots, \tau_{120}\}$ とする。

定義 3.3 (分解式)

多項式 $f(x)$ と不変多項式 P に付随する120次の分解式 $\Phi(y)$ を次のように定義する。

$$\Phi(y) = \prod_{k=1}^{120} (y - \tau_k \cdot P(\alpha_1, \dots, \alpha_8))$$

分解式 $\Phi(y)$ を展開したときの各係数は、根 $\alpha_1, \dots, \alpha_8$ に関する基本対称式の多項式として表される。したがって、ガロア理論の基本定理により、$\Phi(y)$ の係数はすべて有理数体 $\mathbb{Q}$ に属する。すなわち $\Phi(y) \in \mathbb{Q}[y]$ である。

定理 3.4 (ガロア群の包含判定)

$\Phi(y)$ が $\mathbb{Q}$ 上で重複する根を持たないと仮定する。このとき、$\Phi(y)$ が $\mathbb{Q}$ において有理根 $r \in \mathbb{Q}$ を持つことと、ガロア群 G が S_8 において $\mathrm{PGL}_2(\mathbb{F}_7)$ と共役 (conjugate) な部分群に含まれることは同値である。

証明

もし $G \subset \tau \mathrm{PGL}_2(\mathbb{F}_7) \tau^{-1}$ となるような $\tau \in S_8$ が存在したとする。このとき、値 $r = \tau \cdot P(\alpha_1, \dots, \alpha_8)$ は、任意の $\sigma \in G$ の作用に対して不変となる。なぜなら、$\tau^{-1} \sigma \tau \in \mathrm{PGL}_2(\mathbb{F}_7)$ であり、多項式 P は $\mathrm{PGL}_2(\mathbb{F}_7)$ の元の作用で不変になるように構成されているからである。ガロア群の作用で不変な数は基礎体 $\mathbb{Q}$ に属するため、$r \in \mathbb{Q}$ となり、分解式 $\Phi(y)$ は有理根を持つ。

逆に、$\Phi(y)$ が有理根 r を持つとする。その根は構成からある k について $r = \tau_k \cdot P(\alpha_1, \dots, \alpha_8)$ と表される。$r \in \mathbb{Q}$ であるから、任意の $\sigma \in G$ について $\sigma(r) = r$ が成り立つ。これは $\sigma \tau_k \cdot P(\alpha_1, \dots, \alpha_8) = \tau_k \cdot P(\alpha_1, \dots, \alpha_8)$ を意味し、重複根を持たないという仮定から、置換としての作用が $\tau_k^{-1} \sigma \tau_k \in \mathrm{PGL}_2(\mathbb{F}_7)$ を引き起こす。したがって G は $\tau_k \mathrm{PGL}_2(\mathbb{F}_7) \tau_k^{-1}$ の部分群となる。（証明終）

4. 結論

実際の計算手続きとしては、与えられた $f(x)$ の係数からNewtonの公式等を用いて $\Phi(y)$ の係数を有理数として計算し、$\Phi(y) = 0$ が有理根を持つことを示す。これにより、G が $\mathrm{PGL}_2(\mathbb{F}_7)$ と同型な部分群に包含されることが厳密に証明される。2節において素数還元を用いた Dedekindの定理から導かれた $|G| \geq 336$ という下限と、3節の分解式を用いた $G \subset \mathrm{PGL}_2(\mathbb{F}_7)$ という上限を統合することで、$G \cong \mathrm{PGL}_2(\mathbb{F}_7)$ であることが完全に証明される。

参考文献

- Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Springer-Verlag. https://link.springer.com/book/10.1007/978-3-662-02945-9
- Dixon, J. D. (1983). Computing resolvents and Galois groups. *Mathematics of Computation*, 41(164), 711-722. https://doi.org/10.1090/S0025-5718-1983-0717719-7