ガロア理論とガロアの逆問題

〈修士論文要旨〉

愛知教育大学大学院 教育学研究科
数学教育専攻 数学科内容学領域
214M045 清水 悠夏

1 Galois の定理

2 次方程式の起源は古く, 古代バビロニアの時代には既にその解法が知られていた. 一方で, 3 次方程式, 4 次方程式に解の公式が考え出されたのは 16 世紀頃である. 次に, 5 次方程式には解の公式が存在するかが考えられた.

この問いの答え, 5 次方程式に四則とベキ根のみによる解の公式が存在しないことは, Ruffini (1765-1822) と Abel (1802-29) の 2 人の結果を併せた次の主張によって示すことができる.

命題 6.10. K を標数 0 の体とし, $n \geq 5$ とすれば, K 上の n 次の多項式はベキ根によって解けない.

この主張の見通しを更によくしたのが, Galois (1811-32) である. Galois は群の概念をつくりだし, 次に述べる Galois の定理によってガロア拡大の中間体と多項式のガロア群の部分群との間に 1 対 1 対応が存在することを主張した. ここで, Galois の定理を述べるために必要なガロア群, 不変体, ガロア拡大の定義をする.

定義 16. 拡大体 E/F に対し, $\mathrm{Aut}(E)$ の部分群 $\mathrm{Gal}(E/F)$ を

$$\mathrm{Gal}(E/F) := \{\sigma \in \mathrm{Aut}(E) \,|\, {}^{\forall}\alpha \in F \text{ に対して} \sigma(\alpha) = \alpha\}$$

と定義し, E の F 上の**ガロア群** (Galois group) という. また, $f(x) \in F[x]$ に対し, $f(x)$ の F 上の最小分解体を E とするとき, $\mathrm{Gal}(E/F)$ を $f(x)$ の F 上の**ガロア群**という.

定義 17. E を体とする. このとき, $\mathrm{Aut}(E)$ の部分群 G に対し,

$$E^G := \{\alpha \in E \,|\, {}^{\forall}\sigma \in G \text{ に対して} \sigma(\alpha) = \alpha\}$$

と定義し, E^G を G の**不変体**と呼ぶ.

定義 22. E/F を有限拡大, $G := \mathrm{Gal}(E/F)$ に対し, $F = E^G$ を満たすとき E/F を**ガロア拡大**という.

Galois の定理. E/F をガロア拡大, $G := \mathrm{Gal}(E/F)$ とし,

$$\mathrm{Sub}(G) := \{H \,|\, G \text{ の部分群}\},\ \mathrm{Lat}(E/F) := \{B \,|\, E/F \text{ の中間体}\}$$

とおく. このとき, 写像 $\gamma : \mathrm{Sub}(G) \to \mathrm{Lat}(E/F)$ $(H \mapsto E^H)$ は全単射となり, 写像 $\delta : \mathrm{Lat}(E/F) \to \mathrm{Sub}(E/F)$ $(B \mapsto \mathrm{Gal}(E/B))$ は γ の逆写像となる.

この考え方によって, Galois は方程式が四則とベキ根で解けるための必要十分条件を明示的に与えた. 本論文第 6 節で Abel-Ruffini の定理 (命題 6.10) を, また第 4 節で Galois の定理 (定理 4.1) を証明している. そして, これらから 5 次方程式に解の公式がないことを導くことを前半の目標としている.

2 Galois の逆問題

本論文の後半では, Hilbert (1862-1943) が 1892 年に端緒を開いたガロアの逆問題: 「与えられた有限群 G に対して, $\mathbb{Q}$ 上のガロア拡大のガロア群が G に同型となる拡大体が存在するのか」という問いについて考察を行う. 本論文第 7 節では, 2 次多項式, 3 次多項式, 4 次多項式の $\mathbb{Q}$ 上のガロア群の判定法を与えている. 第 8 節では, $\mathbb{Q}$ 上のガロア群が C_4, D_5 と同型になるような多項式を与え, 構成した多項式の最小分解体の部分体や根, 既約性の考察を行っている.

2.1 4 次多項式のガロア群

既約な 4 次多項式の $\mathbb{Q}$ 上のガロア群を判定する方法を与える.

定義 29. $f(x) := c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ のとき,

$$\Delta := \prod_{i<j}(\alpha_i - \alpha_j)$$

と定義する. 多項式 $f(x) \in F[x]$ の**判別式** D を $D := \Delta^2$ とする.

定義 32. $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ の根を $\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4$ とする. このとき,

$$t_1 := \alpha_1\alpha_2 + \alpha_3\alpha_4,\ t_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4,\ t_3 := \alpha_1\alpha_4 + \alpha_2\alpha_3 \tag{2.1}$$

とおき, $f(x)$ の 3 **次分解多項式**を

$$r(x) := (x-t_1)(x-t_2)(x-t_3)$$

と定める.

定理 7.1 ([4, Theorem 1])**.** $f(x)$ を $\mathbb{Q}$ 上既約な 4 次多項式とし, $f(x)$ の $\mathbb{Q}$ 上の最小分解体を F とする. また, $f(x)$ の 3 次分解多項式 $r(x)$ の $\mathbb{Q}$ 上の最小分解体を E, $r(x)$ の判別式を D とする.
(1) $r(x)$ が $\mathbb{Q}$ 上既約かつ $\sqrt{D} \notin \mathbb{Q}$ ならば, $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_4$.
(2) $r(x)$ が $\mathbb{Q}$ 上既約かつ $\sqrt{D} \in \mathbb{Q}$ ならば, $\mathrm{Gal}(F/\mathbb{Q}) \simeq A_4$.
(3) $r(x)$ が $\mathbb{Q}$ 上で分解するならば, $\mathrm{Gal}(F/\mathbb{Q}) \simeq V$.
$r(x)$ が $\mathbb{Q}$ 上で根を 1 つだけもつとき, それを $t \in \mathbb{Q}$ とする.
(4) $f^*(x) := (x^2 - tx + d)(x^2 + ax + (b-t))$ が E 上分解するならば, $\mathrm{Gal}(F/\mathbb{Q}) \simeq C_4$.
(5) $f^*(x)$ が E 上分解しないならば, $\mathrm{Gal}(F/\mathbb{Q}) \simeq D_4$.

この定理より, 以下の命題が証明される.

命題 7.8. $f(x) := x^4 + ax^2 + b \in \mathbb{Q}[x]$ を $\mathbb{Q}$ 上既約な多項式とし, $f(x)$ のガロア群を G とする.
(1) $\sqrt{b} \in \mathbb{Q} \Rightarrow G \simeq V$.
(2) $\sqrt{b} \notin \mathbb{Q}$ かつ $\sqrt{b(a^2-4b)} \in \mathbb{Q} \Rightarrow G \simeq C_4$.
(3) $\sqrt{b},\ \sqrt{b(a^2-4b)} \notin \mathbb{Q} \Rightarrow G \simeq D_4$.

命題 7.9. $f(x) := x^4 + bx^3 + cx^2 + bx + 1 \in \mathbb{Q}[x]$ を $\mathbb{Q}$ 上既約な多項式, $f(x)$ のガロア群を G とし, $h := c^2 + 4c + 4 - 4b^2$ とする. (1) $\sqrt{h} \in \mathbb{Q} \Rightarrow G \simeq V$.
(2) $\sqrt{h} \notin \mathbb{Q}$ かつ $\sqrt{h(b^2 - 4c + 8)} \in \mathbb{Q} \Rightarrow G \simeq C_4$.
(3) $\sqrt{h},\ \sqrt{h(b^2 - 4c + 8)} \notin \mathbb{Q} \Rightarrow G \simeq D_4$.

2.2 ガロア群が 4 次巡回群と同型になる多項式

幾つかの計算機実験と理論的な考察の結果として, ガロア群が C_4 と同型になる 3 つの $\mathbb{Q}$ 上の 4 次多項式を発見することができた:

$$
\begin{aligned}
f_1(x) &:= x^4 + 2u(s^2 + t^2)x^2 + u^2t^2(s^2 + t^2), \\
f_2(x) &:= x^4 + 4x^3 - (t^2 + 10)x^2 + 4x + 1, \\
f_3(x) &:= x^4 + t^2x^3 + (t^3 - 2t^2 + 4t - 2)x^2 + t^2x + 1.
\end{aligned}
$$

本論文の主結果は, 以下の 3 つの定理である.

定理 8.1. $f_1(x)$ の $\mathbb{Q}$ 上の最小分解体を K_1 とする.
(1) $\sqrt{s^2 + t^2} \notin \mathbb{Q}$ ならば $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq C_4$ である.
(2) K_1 の含む 2 次体は $\mathbb{Q}(\sqrt{s^2 + t^2})$ である.
(3) $f_1(x) \in \mathbb{Z}[x]$ のとき, $s,\ t$ が奇数かつ $u = 4a$ (a : 奇数) ならば $f_1(x)$ は $\mathbb{Q}$ 上既約である.
(4) $\Delta_1 := s^2 + t^2$ とすると, $f_1(x)$ の根は

$$
\pm\sqrt{-u\Delta_1 \pm u\sqrt{\Delta_1}}
$$

と表せる.

定理 8.2. $f_2(x)$ の $\mathbb{Q}$ 上の最小分解体を K_2 とする.
(1) $\sqrt{t^2 + 16} \notin \mathbb{Q}$ ならば $\mathrm{Gal}(K_2/\mathbb{Q}) \simeq C_4$ である.
(2) K_2 の含む 2 次体は $\mathbb{Q}(\sqrt{t^2 + 16})$ である.
(3) $f_2(x) \in \mathbb{Z}[x]$ のとき, $t \in \mathbb{Z} \setminus \{0,\ \pm 3\}$ ならば $f_2(x)$ は $\mathbb{Q}$ 上既約である.
(4) $\Delta_2 := t^2 + 16$ とすると, $f_2(x)$ の根は

$$
\frac{-2 + \sqrt{\Delta_2} \pm \sqrt{\Delta_2 - 4\sqrt{\Delta_2}}}{2},\ \frac{-2 - \sqrt{\Delta_2} \pm \sqrt{\Delta_2 + 4\sqrt{\Delta_2}}}{2}
$$

と表せる.

定理 8.3. $f_3(x)$ の $\mathbb{Q}$ 上の最小分解体を K_3 とする.
(1) $\sqrt{t^2 + 16} \notin \mathbb{Q}$ ならば $\mathrm{Gal}(K_3/\mathbb{Q}) \simeq C_4$ である.
(2) K_3 の含む 2 次体は $\mathbb{Q}(\sqrt{t^2 + 4})$ である.
(3) $f_3(x) \in \mathbb{Z}[x]$ のとき, $t \in \mathbb{Z} \setminus \{0,\ 2\}$ ならば $f_3(x)$ は $\mathbb{Q}$ 上既約である.
(4) $\Delta_3 := t^2 + 4$ とすると, $f_3(x)$ の根は

$$
\begin{aligned}
&\frac{-t^2 + (t-2)\sqrt{\Delta_3} \pm \sqrt{t(t-2)(\Delta_3 - 2t\sqrt{\Delta_3})}}{4}, \\
&\frac{-t^2 - (t-2)\sqrt{\Delta_3} \pm \sqrt{t(t-2)(\Delta_3 + 2t\sqrt{\Delta_3})}}{4}
\end{aligned}
$$

と表せる.

2.3 ガロア群が 5 次 2 面体群と同型になる多項式

5 次多項式について, 次の命題 8.2 が成立する.

命題 8.2 ([5, Theorem 3])**.** $f(x) := x^5 + ax + b \in \mathbb{Q}[x]$ が $\mathbb{Q}$ 上既約, $f(x)$ の $\mathbb{Q}$ 上のガロア群を G, 判別式を D とする. $G \simeq D_5$ となる必要十分条件は, 以下の条件で (1), (2) を満たすことである.
(1) $\sqrt{D} \in \mathbb{Q}$,
(2) a, b に対し,

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)},\ b = a\mu$$

を満たす $\lambda,\ \mu \in \mathbb{Q},\ \lambda \neq 1,\ \mu \neq 0$ が存在する.

上の命題を用いて, ガロア群が D_5 と同型になる多項式を与えることができた. その結果を述べるために必要なフィボナッチ数列, リュカ数列を定義する.

定義 34. 数列 $\{F_n\}$ を $F_1 = 1,\ F_2 = 1,\ F_{n+2} = F_{n+1} + F_n\ (1 \leq n)$ で定義する. この数列を**フィボナッチ数列**という.

注意 1. $F_n = F_{n+2} - F_{n+1}$ なので, $F_0 = 0$ と定義しておく.

定義 35. 数列 $\{L_n\}$ を $L_1 = 1,\ L_2 = 3,\ L_{n+2} = L_{n+1} + L_n\ (1 \leq n)$ で定義する. この数列を**リュカ数列**という.

定理 8.4. 有理数 a を

$$a := \frac{5^4(2L_{2n-1}+3)}{2^6(L_{2n-1}+1)^4F_{2n-1}^2}$$

と定め, $f_4(x) := x^5 + ax + a$ とおく. また, $f_4(x)$ の $\mathbb{Q}$ 上の最小分解体を K_4 とする. このとき, $f_4(x)$ が $\mathbb{Q}$ 上既約ならば $\mathrm{Gal}(K_4/\mathbb{Q}) \simeq D_5$ である.

参考文献

[1] J. ロットマン, ガロア理論, (関口 次郎 訳), 丸善出版, 2012.

[2] 今野 一宏, 代数方程式のはなし, 内田老鶴圃, 2014.

[3] 松坂 和夫, 代数系入門, 岩波書店, 1976.

[4] L-C. Kappe and B. Warren, An elementary test for the Galois group of a quartic polynomial, Amer. Math. Monthly **96** (1989), no.2, 133–137.

[5] R. Kavanagh, On irreducible rational quintics, preprint, 2014.

[6] R. Louboutin, The simplest quartic fields with ideal class groups of exponents less than or equal to 2, J. Math. Soc. Japan **56** (2004), no.3, 717–727.