Galois 理論による代数学の基本定理の証明

MathTech 部員　田中大地

1　はじめに

こんにちは。今回は、Galois 理論の話を書きたいと思います。Galois 理論は方程式の可解性や作図問題の応用がありますが、代数学の基本定理の証明にも応用することができます。本記事でその証明を紹介したいと思います。前提知識として群論 (正規部分群、剰余群、準同型定理など) と体論 (分離拡大と正規拡大の基本性質など) を仮定するので、高校生には難しい内容かと思いますが、大学の代数学の感じが伝わればいいなと思います。まず、主張を正確に書きます。

Theorem 1.1. (代数学の基本定理) $a_0, a_1, \ldots, a_n \in \mathbb{C}, a_n \neq 0$ とする。
このとき多項式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ は $\mathbb{C}$ 内に根を持つ。

証明は、代数学の基本定理が成り立たないと仮定すると複素数体 $\mathbb{C}$ の二次拡大体が構成できるが、複素数体 $\mathbb{C}$ は二次拡大体を持たない事も示せるので、矛盾となるというものです。以下、証明に使う群論とガロア理論について説明します。

2　群論

群論で必要な定理は定理 2.6 と定理 2.7 である。この二つの定理をしめすために群の作用という概念を導入します。

Definition 2.1. (群作用) G:群、X:集合とする。

$$G \times X \ni (g, x) \longmapsto gx \in X$$

がつぎの (1)、(2) を満たすとき、この写像を作用といい、$G \curvearrowright X$ と書く。

(1) $e \in G$ を単位元とすると、$\forall x \in X, ex = x$
(2) $\forall g, h \in G, \forall x \in x, g(hx) = (gh)x$

また、$G \curvearrowright X$ の時、$x \in X$ に対して、
$\mathrm{Stab}(x) = \{g \in G \mid gx = g\}$ を x の安定化群、$\mathrm{Orb}(x) = \{gx \mid g \in G\}$ を x の軌道という。

次が成り立つ。

Proposition 2.2. (軌道分解)　$G \curvearrowright X$ のとき、$X = \bigsqcup_{\mathrm{Orb}(x)} \mathrm{Orb}(x)$

Proof. 任意の $x \in X$ に対して $x \in \mathrm{Orb}(x)$ であり、また $\forall x, y \in X$ に対して $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ または $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) = \emptyset$ なることが定義からわかるので、従う。 ■

Proposition 2.3. $G \curvearrowright X$ とする。
$x \in X$ に対して、$\mathrm{Stab}(x)$ は G の部分群であり、$|G/\mathrm{Stab}(x)| = |\mathrm{Orb}(x)|$ となる。

Proof.
$$\begin{array}{ccc} G/\mathrm{Stab}(x) & \longrightarrow & \mathrm{Orb}(x) \\ \cup\!\!\!\!\!\! \shortparallel & & \cup\!\!\!\!\!\! \shortparallel \\ \bar{g} & \longmapsto & gx \end{array}$$
によって一対一に対応する。 ■

Definition 2.4. G を群とする。
(1) $Z_G = \{h \in G \mid \forall g \in G, gh = hg\}$ を G の中心という。
(2) p を素数とするとき、位数が p べきである群を p 群という。

G:有限群、$X = G$ として、
$$G \times X \ni (g, h) \longmapsto ghg^{-1} \in X$$
を考えると作用になる。この作用について軌道分解の代表元 $\{h_i\}$ をとると、
$$\begin{aligned} G &= \bigsqcup_i |\mathrm{Orb}(h_i)| \\ &= \left(\bigsqcup_{i, h_i \in Z_G} \mathrm{Orb}(h_i) \right) \bigsqcup \left(\bigsqcup_{i, h_i \notin Z_G} \mathrm{Orb}(h_i) \right) \\ &= \left(\bigsqcup_{i, h_i \in Z_G} \{h_i\} \right) \bigsqcup \left(\bigsqcup_{i, h_i \notin Z_G} \mathrm{Orb}(h_i) \right) \end{aligned}$$
ここで、任意の $h \in Z_G$ は $\bigsqcup_{i, h_i \notin Z_G} \mathrm{Orb}(h)$ に含まれないから、$h \in \bigsqcup_{i, h_i \in Z_G} \{h_i\}$ 従って $Z_G = \bigsqcup_{i, h_i \in Z_G} \{h_i\}$ となるから、
$$|G| = |Z_G| + \sum_{i, h_i \notin Z_G} |\mathrm{Orb}(h_i)| \tag{1}$$
$|G| = p^n$ のとき、$h \notin Z_G$ なら $|\mathrm{Orb}(h)| = \frac{|G|}{|\mathrm{Stab}(h)|} = \frac{p^n}{|\mathrm{Stab}(h)|}$, $|\mathrm{Stab}(h)| < |G| = p^n$ となるから、$|\mathrm{Orb}(h)|$ は p の倍数、よって、(1) より $|Z_G|$ は p の倍数である。また、$Z_G \supseteq \{e\}$ だから、次が言えた。

Theorem 2.5. G を p 群とするするとき、$Z_G \supsetneq \{e\}$

Theorem 2.6. G が p 群で、$|G| = p^n$ なら $0 \leqq \forall t \leqq n$ に対して位数 p^t の部分群を持つ。

Proof. n の帰納法で示す。$n = 1$ は明らか。$n - 1$ まで成り立つとして n のときを示す。$Z_G \supsetneq \{e\}$ の位数 p の元 x をとり、$\mathrm{N} = \langle x \rangle$ とする。N は G の正規部分群であり、G/N は位数 p^{n-1} の群であるから帰納法の仮定から $0 \leqq \forall t \leqq n - 1$ に対して指数 p^t の部分群がある。言い換えれば、G には $0 \leqq \forall t \leqq n - 1$ に対して指

数 p^t の部分群がある。ここで、部分群の対応

$$\{G \text{ の } N \text{ を含む部分群 }\} \longleftrightarrow \{G/N \text{ の部分群 }\}$$

において、対応する部分群の指数は保たれる。実際、$N \subset H \subset G$ なる部分群 H をとると、対応する G/N の部分群は $\tilde{H} = H/N$ である。このとき、つぎの写像

$$(G/N)/\tilde{H} \ni \overline{g}\tilde{H} \longmapsto gH \in G/H$$
$$G/H \ni gH \longmapsto \overline{g}\tilde{H} \in (G/N)/\tilde{H}$$

は互いに逆写像となる。
よって、この部分群から G には指数が $p^t(0 \leqq t \leqq n-1)$ の部分群が存在することが分かった。$\{e\}$ は指数 p^n の部分群だから、$t = n$ の場合も存在する。これは位数 $p^t(0 \leqq \forall t \leqq n)$ の部分群が存在することを意味するので証明が完了した。 ■

Theorem 2.7. (Sylow) G を有限群で、$|G| = p^n m(p, m$ は互いに素) とする。このとき部分群 H で $|H| = p^n$ なるものがある。

Proof. $X = \{S \subset G \mid |S| = p^n(\text{但し } S \text{ は部分群とは限らない})\}$ とする。

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ \cup & & \cup \\ (g, s) & \longmapsto & gS = \{gs | s \in S\} \end{array}$$

は作用となる。

$$|X| = \begin{pmatrix} p^n m \\ p^n \end{pmatrix} = \left((x+1)^{p^n m} \text{ の } x^{p^n} \text{ の係数}\right)$$
$$(x+1)^{p^n m} \equiv (x^{p^n} + 1)^m \qquad \bmod p$$
$$\therefore |X| = \begin{pmatrix} p^n m \\ p^n \end{pmatrix} \equiv m \qquad \bmod p$$

軌道分解を考えると、

$$|X| = \sum_{\mathrm{Orb}(S)} |\mathrm{Orb}(S)| \equiv m \not\equiv 0 \qquad \bmod p$$

だから、$|\mathrm{Orb}(S)| \not\equiv 0$ となる S がある。$H = \mathrm{Stab}(S)$ とおく。

$$S = \bigcup_{y \in H} Hy = \bigsqcup_{Hy} Hy$$

よって $|Hg| = |H|$ より $|S| = p^n$ は $|H|$ で割り切れるので、$|H| = p^k(0 \leqq k \leqq n)$ と書ける。また、

$$\frac{|G|}{|H|} = p^{n-k} m = |\mathrm{Orb}(S)| \not\equiv 0 \qquad \bmod p$$

から、$k = n$ である。よって $|H| = p^n$ となり、H が求める部分群。 ■

3 Galois 理論

本節の目標は Thm3.5 である。

Definition 3.1. K/F を代数拡大とする。
(1) $\forall\alpha \in K$ の F 上最小多項式が K 上で一次多項式の積に分解されるとき K/F を正規拡大という。
(2) $\forall\alpha \in K$ の F 上最小多項式が K の代数閉包で重根を持たないとき K/F を分離拡大という。
(3) K/F が正規拡大かつ分離拡大のとき、K/F を Galois 拡大という。
(4) K/F 有限次 Galois 拡大とするとき $\mathrm{Gal}(K/F) = \{f \in \mathrm{Aut}(K) \mid f(x) = x(\forall x \in F)\}$ を Galois 群という。

Theorem 3.2. K/F を有限次 Galois 拡大とする。このとき、$[K : F] = |\mathrm{Gal}(K/F)|$ ただし $[K : F]$ は K/F の拡大次数。

Proof. K/F は分離拡大だから、$\overline{K}$ を K の代数閉包とするとき、$\left|\mathrm{Hom}_F(K, \overline{K})\right| = [K : F]$ である。K/F は正規拡大でもあるから、$\forall\sigma \in \mathrm{Hom}_F(K, \overline{K})$ について $\sigma(K) \subset K$ である。$\mathrm{Ker}\,\sigma = 0, [K : F] < \infty$ なので次元定理から $\sigma(K) = K$ となる。よって $\mathrm{Hom}_F(K, \overline{K}) = \mathrm{Gal}(K/F)$ なので、従う。 ■

Theorem 3.3. (Artin) K を体とし、G を $\mathrm{Aut}(K)$ の有限部分群とする。このとき
$F = K^G = \{x \in K | \sigma(x) = x(\forall\sigma \in G)\}$ とすれば、K/F は有限次 Galois 拡大で $\mathrm{Gal}(K/F) = G$ となる。

Proof. $\alpha \in K$ に対し $\alpha = \{\sigma \in G | \sigma(\alpha) = \alpha\}, G = \bigsqcup_{i=1}^{n} \sigma_i H_\alpha$,

$$f_\alpha(X) = (X - \sigma_1(\alpha))(X - \sigma_2(\alpha)) \cdots (X - \sigma_n(\alpha)) \in K[X]$$

とする。$\forall\sigma \in G$ に対して

$$\begin{array}{ccc} G/H_\alpha & \longrightarrow & G/H_\alpha \\ \cup & & \cup \\ \sigma_i H_\alpha & \longmapsto & \sigma\sigma_i H_\alpha \end{array}$$

は全単射であるので、

$$\begin{aligned} \sigma(f_\alpha(X)) =& (X - \sigma\sigma_1(\alpha))(X - \sigma\sigma_2(\alpha)) \cdots (X - \sigma\sigma_n(\alpha)) \\ =& f_\alpha(X) \end{aligned}$$

となり、$f(X) \in F[X]$。また、$\sigma_i(\alpha) = \alpha$ なる i があるから、$f_\alpha(\alpha) = 0$ であり、$\sigma_i(\alpha) = \sigma_j(\alpha) \Longleftrightarrow \sigma_i H_\alpha = \sigma_i H_\alpha$ だから、$f_\alpha(X)$ は分離多項式。よって K/F は Galois 拡大。K/F が無限次拡大なら、$\beta_1, \beta_2, \ldots$ を

$$F \subsetneq F(\beta_1) \subsetneq F(\beta_1, \beta_2) \subsetneq \cdots$$

となるように取れるので、中間体 $M(F \subset M \subset K)$ で、$|G| < [F : M] < \infty$ である M がある。M/F は有限次分離拡大だから、$M = F(\beta)$ となる $\beta \in M$ をとると

$$[M : F] = \deg f_\beta(X) < |G|$$

なるから、矛盾。K/F は有限次 Galois 拡大である。
最後に、$\mathrm{Gal}(K/F) = G$ を示す。定義より $\mathrm{Gal}(K/F) \supset G$ である。$\forall \sigma \in \mathrm{Gal}(K/F)$ に対して、

$$f_\alpha(\sigma(\alpha)) = \sigma(f_\alpha(\alpha)) = 0$$

なので、$\sigma(\alpha) = \sigma_i(\alpha)(\exists i) \therefore \sigma = \sigma_i(\exists i)$ よって、$\mathrm{Gal}(K/F) \subset G$ となるから、$\mathrm{Gal}(K/F) = G$ を得る。 ■

K/F を有限次 Galois 拡大、$G = \mathrm{Gal}(K/F)$ とする。

- 中間体 M に対し、$H(M) = \{\sigma \in G \mid \forall x \in M, \sigma(x) = x\}$ とおく。
- 部分群 $H \subset G$ に対して、$M_H = \{x \in K \mid \forall \sigma \in H, \sigma(x) = x\}$ とおく。

Proposition 3.4. K/F を有限次 Galois 拡大とする。中間体 M に対し、K/M 有限次 Galois 拡大であり、$\mathrm{Gal}(K/F) = H(M)$ となる。

Proof. 定義から有限次 Galois 拡大であること、$\mathrm{Gal}(K/F) = H(M)$ であることが確かめられる。 ■

Theorem 3.5. (Galois の基本定理)
K/F を有限次 Galois 拡大とする。

(1) $\mathbb{M} = \{K/F \text{ の中間体 } M\}, \mathbb{H} = \{\mathrm{Gal}(K/F) \text{ の部分群 }\}$ とおくとき、

$$\mathbb{M} \ni M \longmapsto H(M) \in \mathbb{H}$$

$$\mathbb{H} \ni H \longmapsto M_H \in \mathbb{M}$$

によって、一対一に対応する。

(2) $M_1, M_2 \in \mathbb{M}$ がそれぞれ $H_1, H_2 \in \mathbb{H}$ に対応するとき

$$M_1 \subset M_2 \Longleftrightarrow H_1 \supset H_2$$
$$M_1 \cdot M_2 \longleftrightarrow H_1 \cap H_2$$
$$M_1 \cap M_2 \longleftrightarrow \langle H_1, H_2 \rangle$$

(3) $M \longleftrightarrow H$ のとき

$$M/F \text{ が Galois 拡大} \Longleftrightarrow H \lhd G$$

であり、このとき

$$\mathrm{Gal}(M/F) \cong \mathrm{Gal}(K/F)/H$$

Proof. (1) $M \in \mathbb{M}$ とする。$M_{H(M)} = \{x \in K \mid \forall \sigma \in H(M), \sigma(x) = x\}$ であるから、$M \subset M_{H(M)}$ である。Thm3.3 より $K/M_{H(M)}$ は有限次 Galois 拡大であり、$\mathrm{Gal}(K/M_{H(M)}) = H(M)$ となる。一方 Prop3.4 から K/M も有限次 Galois 拡大で $\mathrm{Gal}(K/M) = H(M)$ なので、

$$[M_{H(M)} : M] = \frac{[K : M]}{[K : M_{H(M)}]} = \frac{|H(M)|}{|H(M)|} = 1$$

よって $M = M_{H(M)}$。
$H \in \mathbb{H}$ とする。$H(M_H) = \{\sigma \in \mathrm{Gal}(K/F) | \forall x \in M_H, \sigma(x) = x\}$ であるので、$H \subset H(M_H)$ となる。Thm3.3 から K/M_H は有限次 Galois 拡大であり、$\mathrm{Gal}(K/M_H) = H$ となる。一方 Prop3.4 より $\mathrm{Gal}(K/M_H) = H(M_H)$ なので、$H = H(M_H)$ となる。

(2) $M_1 \subset M_2 \Longleftrightarrow H_1 \supset H_2$ は明らか。
$M_1 \cdot M_2 \supset M_i (i = 1, 2)$ より、$H(M_1 \cdot M_2) \subset H(M_1) \cap H(M_2)$ である。$H(M_1) \cap H(M_2)$ の各元は M_1, M_2 を不変にするので、$M_1 \cdot M_2$ を不変にする。よって $H(M_1 \cdot M_2) \supset H(M_1) \cap H(M_2)$ だから、$H(M_1 \cdot M_2) = H(M_1) \cap H(M_2)$
$M_1 \cap M_2 \subset M_i (i = 1, 2)$ なので、$H(M_1 \cap M_2) \supset \langle H(M_1), H(M_2) \rangle = \langle H_1, H_2 \rangle$ である。$H = \langle H_1, H_2 \rangle$ とすると、$H \supset H_i (i = 1, 2)$ だから、$M_H \subset M_{H_i} = M_i (i = 1, 2)$ となり、$M_H \subset M_1 \cap M_2 \therefore H \supset H(M_1 \cap M_2)$
よって $H(M_1 \cap M_2) = \langle H_1, H_2 \rangle$
(3) M を中間体とする。$M \longleftrightarrow H$ とする。

$$\begin{aligned} M/F \text{ が有限次 Galois 拡大} &\overset{(a)}{\Longleftrightarrow} M/F \text{ が正規拡大} \\ &\overset{(b)}{\Longleftrightarrow} \forall \sigma \in \mathrm{Gal}(K/F), \sigma(M) \subset M \\ &\overset{(c)}{\Longleftrightarrow} H \lhd \mathrm{Gal}(K/F) \end{aligned}$$

(a) K/F が有限次分離拡大だから成り立つ。
(b) $(\Rightarrow)$ $\alpha \in M$ の F 上最小多項式を $f(X)$ とすると、M/F が正規拡大であることから $f(X) = \prod_i (X - \alpha_i)$ $(\alpha_i \in M)$ とかける。$f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$ なので、 $\sigma(\alpha) = \alpha_i \in M$ である。
$(\Leftarrow)$ $\alpha \in M$ とする。

$$f(X) = \prod_{\sigma \in \mathrm{Gal}(K/F)} (X - \sigma(\alpha))$$

とすると、$\sigma(f(X)) = f(X)\ (\forall \sigma)$ より $f(X) \in F[X]$ である。$f(X)$ は α を根に持ち M 上で一次因子の積に分解されるので、α の F 上最小多項式も M 上で一次因子の積に分解されるので M/F は正規拡大である。
(c) $(\Rightarrow)$ $\sigma \in \mathrm{Gal}(K/F), \tau \in H, x \in M$ に対して $\sigma(x) \in M$ ゆえ $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$ となるから $\sigma^{-1}\tau\sigma \in H$ よって $H \lhd \mathrm{Gal}(K/F)$ となる。
$(\Leftarrow)$ $\sigma \in \mathrm{Gal}(K/F), \tau \in H$ について $\sigma^{-1}\tau\sigma \in H$ なので $x \in M$ なら $\sigma^{-1}\tau\sigma(x) = x$ つまり $\tau\sigma(x) = \sigma(x)$ これが任意の $\tau \in H$ で成り立つので $\sigma(x) \in M$ よって、$\sigma(M) \subset M$
最後に $\mathrm{Gal}(M/F) \cong \mathrm{Gal}(K/F)/H$ について

$$\mathrm{Gal}(K/F) \ni \sigma \mapsto \sigma|_M \in \mathrm{Gal}(M/F)$$

に準同型定理を使うと、単射準同型

$$\mathrm{Gal}(K/F)/H \ni \sigma H \mapsto \sigma|_M \in \mathrm{Gal}(M/F)$$

を得る。ここで、Prop3.4 より、$H = \mathrm{Gal}(K/M)$ なので

$$\begin{aligned} |\mathrm{Gal}(K/F)/H| &= \frac{|\mathrm{Gal}(K/F)|}{|\mathrm{Gal}(K/M)|} \\ &= \frac{[K:F]}{[K:M]} \\ &= [M:F] \\ &= |\mathrm{Gal}(M/K)| \end{aligned}$$

となるから、全射でもあるから $\mathrm{Gal}(M/F) \cong \mathrm{Gal}(K/F)/H$ がいえた。 ■

本記事の目標には関係ないが、興味深いので Galois 群の計算例を紹介しよう。

Example 3.6. 体の拡大 $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ を考える。これは、$f(X) = X^4 - 2 \in \mathbb{Q}[X]$ の最小分解体だから、有限次 Galois 拡大である。Eisenstein の既約判定定理から $f(X)$ は既約多項式であるから $[\mathbb{Q}(\sqrt[4]{2}] : \mathbb{Q}] = 4$ である。i の $\mathbb{Q}$ 上最小多項式は $X^2 + 1$ であるので、$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \leqq 2$ である。また $i \notin \mathbb{Q}$ なので、$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ となる。ゆえに、$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$ である。Galois 群を G とおく。$\sigma \in G$ は、$(\sigma(\sqrt[4]{2}), \sigma(i)) \in \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\} \times \{i, -i\}$ により決まるが、$|G| = 8$ だから、どの 8 パターンの対応をとる $\sigma \in G$ も存在する。ここで

$$\alpha_1 = \sqrt[4]{2}, \alpha_2 = -\sqrt[4]{2}, \alpha_3 = i\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$$

とおく。すると次の対応を定める単射準同型 ϕ が考えられる。

$$\begin{array}{ccc} G & \longrightarrow & S_4 \\ \cup & & \cup \\ \sigma & \longmapsto & \begin{pmatrix} 1 & 2 & 3 & 4 \\ t_1 & t_2 & t_3 & t_4 \end{pmatrix} \end{array}$$

ただし $\sigma(\alpha_i) = \alpha_{t_i} (i = 1, 2, 3, 4)$ である。
$\sigma_1, \sigma_2 \in G$ を $\sigma_1(\alpha_1) = \alpha_3, \sigma_1(i) = i, \sigma_2(\alpha_1) = \alpha_1, \sigma_2(i) = -i$ となるようにとるとき、G は σ_1, σ_2 で生成される。$\phi(\sigma_1) = \begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}, \phi(\sigma_2) = \begin{pmatrix} 3 & 4 \end{pmatrix}$ であるので、$G \cong \left\langle \begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 4 \end{pmatrix} \right\rangle$ となる。

Example 3.7. (Artin-Schreier 拡大)
$\mathrm{ch}F = p > 0$ なる体 F と F 上多項式 $f(X) = X^p - X - a$ を考える。ここで $a \notin \{x^p - x \mid x \in F\}$ とする。$f(X)$ の根の一つ α を添加した体を $E = F(\alpha)$ としたとき E/F が p 次 Galois 拡大となることを示そう。
まず、α の最小多項式を $g(X)$ とするとき、$g(X) = g(X+1)$ となることを背理法で示す。$g(X) \neq g(X+1)$ を仮定すると、$g(X), g(X+1), \ldots, g(X+p-1)$ は相異なる。実際、$g(X+i) = g(X+j) \quad (0 \leqq i < j \leqq p-1)$ となるなら、$g(X) = g(X+j-i)$ である。ここで、$(j-i)k + pl = 1$ となる k, l をとると、

$$g(X) = g(X + k(j-i)) = g(X + 1 - pl) = g(X+1)$$

となるので矛盾が起きる。また、$g(X), g(X+1), \ldots, g(X+p-1)$ は、それぞれ $f(X)$ の根である $\alpha, \alpha+1, \ldots, \alpha+p-1$ の最小多項式であるので、$f(X) = \prod_{i=0}^{p-1} g(X+i)$ となることから、$p = \deg f(X) = \sum_{i=0}^{p-1} \deg g(X+i) = p \deg g(X)$ である。これは、$\alpha \in F$ を意味するが、$a \notin \{x^p - x \mid x \in F\}$ に反するので $g(X) = g(X+1)$ が示された。
$g(X)$ は相異なる p 個の根 $\alpha, \alpha+1, \ldots, \alpha+p-1$ をもつので $g(X) = f(X) \prod_{i=0}^{p-1}(X-i)$ である。以上から、E/F は p 次 Galois 拡大である。したがって、$\mathrm{Gal}(E/F) \cong \mathbb{Z}/p\mathbb{Z}$ である。

4　代数学の基本定理の証明

証明に使う命題をいくつか準備する。

Proposition 4.1. $\mathbb{R}$ 上の任意の奇数次数多項式は、$\mathbb{R}$ 内に根を持つ。

Proof. 中間値の定理から従う。 ■

補題として次の二つを示す。

Lemma 4.2. 標数 0 の体 F の任意の代数拡大は分離拡大である。

Proof. K を F の代数拡大体とする。$\alpha \in K$ の F 上最小多項式を $f(X)$ とする。F の標数 0 だから $\deg\frac{df}{dX}(X) = \deg f(X) - 1$ となる。$f(X)$ が分離多項式でないなら、$f(X)$ と $\frac{df}{dX}(X)$ は共通根 β を持つ。これは、$f(X)$ が β の最小多項式であることに矛盾するから、$f(X)$ は分離多項式である。したがって、K/F は分離拡大。 ■

Remark 4.3. 実数体 $\mathbb{R}$ は標数 0 である。Thm1.1 の証明では、$\mathbb{R}$ の Galois 拡大体を構成するが、Lem4.2 によって分離性はただちに従うから正規性だけが問題になる。

Lemma 4.4. 複素数体 $\mathbb{C}$ は二次拡大体を持たない。

Proof. L を $\mathbb{C}$ の二次拡大体とする。このとき、$\forall \alpha \in L \setminus \mathbb{C}$ はあるモニック二次多項式の根だから、解の公式から

$$\alpha = \frac{a \pm \sqrt{b}}{2} \qquad (a, b \in \mathbb{C})$$

と書ける。右辺は、$\mathbb{C}$ の元だから、$L = \mathbb{C}$ となる。これは、二次拡大であることに矛盾する。 ■

準備ができたので代数学の基本定理を証明する。

Proof. (Thm1.1 の証明) 代数学の基本定理が成り立たないとすると、$\mathbb{C}$ 上の既約多項式 $f(X)$ で、次数が 2 以上のものがある。$K = \mathbb{C}[X]/(f(X))$ とすれば、K は $\mathbb{C}$ の有限次拡大であり、拡大次数は 2 以上である。$\mathbb{C}$ は $\mathbb{R}$ の二次拡大体であるから、$K/\mathbb{R}$ は有限次拡大である。Lem4.2 より、$K/\mathbb{R}$ は有限次分離拡大である。K の $\mathbf{R}$ に関する Galois 閉包を $\tilde{K}$ とする。つまり、K の各元の $\mathbb{R}$ 上の共役元をすべて $\mathbb{R}$ に添加した体とする。$K \subset \tilde{K}$ であり、$\tilde{K}/\mathbb{R}$ は有限次 Galois 拡大となる。このとき、$\tilde{K}/\mathbb{R}$ の拡大次数が 2 のべきとなる。
$[\tilde{K} : \mathbb{R}] = 2^n m$($m$ は奇数) とおくとき、Thm2.7 より Galois 群 G の部分群 H で $|H| = 2^n$ となるものが取れる。H に対応する。中間体 $M(\mathbb{R} \subset M \subset \tilde{K})$ をとると、

$$[M : \mathbb{R}] = \frac{[\tilde{K} : \mathbb{R}]}{[\tilde{K} : M]} = \frac{|\mathrm{Gal}(\tilde{K}/\mathbb{R})|}{|\mathrm{Gal}(\tilde{K}/M)|} \overset{\mathrm{Thm3.4}}{=} \frac{|G|}{|H|} = m$$

$M = \mathbb{R}(\alpha)$ なる α をとると、α の最小多項式 $g(X) \in \mathbb{R}$ の次数は m であるので、$g(X)$ の既約性から Prop4.1 より、$m = 1$ でなくてはならない。よって $[\tilde{K} : \mathbb{R}] = 2^n$ となる。$[\tilde{K} : \mathbb{C}]$ は $[\tilde{K} : \mathbb{R}] = 2^n$ の約数だから $[\tilde{K} : \mathbb{C}] = 2^l, l > 0$ となる。Prop3.4 より、$\tilde{K}/\mathbb{C}$ は有限次 Galois 拡大である。Galois 群の位数は 2^l だから、Prop2.6 から、位数 2^{l-1} の部分群 $N \subset \mathrm{Gal}(\tilde{K}/\mathbb{C})$ をとると、N に対応する $\tilde{K}/\mathbb{C}$ 中間体は $\mathbb{C}$ の二次拡大体である。これは、$\mathbb{C}$ の二次拡大体が存在しないことに矛盾するから、代数学の基本定理は成り立つ。 ■

5　さいごに

Thm3.5 は、有限次 Galois 拡大 K/F の構造を Galois 群が支配しているという群と体をつなぐ興味深い定理です。今回は、かなり抽象的に使ったが、Example3.6 のように具体的に与えられた体の拡大の Galois 群を計算するのも面白いです。他にも、$\mathbb{Q}$ に $\zeta_n = \exp(2\pi i/n) \in \mathbb{C}$ を添加した体 $\mathbb{Q}(\zeta_n)$ を考えると $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ は、有限次 Galois 拡大になっていて Galois 群が $(\mathbb{Z}/n\mathbb{Z})^\times$ に同型になることがよく知られています。(このような拡大を円分拡大といいます。)

参考文献

[1] 雪江明彦, 代数学 1, 日本評論社,2010

[2] 雪江明彦, 代数学 2, 日本評論社,2010

[3] 藤崎源二郎, 体とガロア理論, 岩波書店,1991

[4] E.Artin 訳寺田文行, ガロア理論入門, ちくま学芸文庫,2010