代数学の基本定理

Masato Nakata

Faculty of Science, Kyoto University

Contents

§ 1.1 代数学の基本定理

次の定理は代数学の基本定理と呼ばれ，とても重要なものである．この証明には，主に複素関数論によるものが知られているが，ここでは Galois 理論による代数的なものを紹介する．

Theorem 1.1.1

複素数体は代数閉体である．

以下，実数体を $\mathbb{R}$，複素数体を $\mathbb{C}$ で表す．$\mathbb{C}$ が代数閉体であることには，定義より，次を示せば良い：

- $\mathbb{C}$ 上代数的な任意の元 α に対して，$\alpha \in \mathbb{C}$ である．

ただし，α は $\mathbb{C}$ の十分大きな拡大体（たとえば $\mathbb{C}$ の代数閉包）の中で考えている．$\mathbb{C}(\alpha)$ で $\mathbb{C}$ に α を添加した体を表すとき，$\alpha \in \mathbb{C}$ は $\mathbb{C}(\alpha) = \mathbb{C}$ と同値である．さらに，$\mathbb{C}(\alpha)$ を含むような，$\mathbb{R}$ の有限次 Galois 拡大体 K を一つ取る[*1]．$K = \mathbb{C}$ を示せば，自動的に $\mathbb{C}(\alpha) = \mathbb{C}$ も従う．よって，次を示せば良い：

Theorem 1.1.2

$\mathbb{C}$ を中間体として持つような，$\mathbb{R}$ の任意の有限次 Galois 拡大 $K/\mathbb{C}/\mathbb{R}$ について，その拡大次数 $[K : \mathbb{R}]$ は 2 である．

実際，$\mathbb{C}$ の $\mathbb{R}$ 上拡大次数は $[\mathbb{C} : \mathbb{R}] = 2$ であり，さらに $[K : \mathbb{R}] = [K : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}]$ が成り立つから，もし上を示すことができれば $[K : \mathbb{C}] = 1$，すなわち $K = \mathbb{C}$ となる．

さて，**Theorem 1.1.2** の証明に一つだけ解析的な道具を使う．

Lemma 1.1.1

奇数次の $\mathbb{R}$ 上多項式は 1 次式または可約である．

Proof. $f(X) \in \mathbb{R}[X]$ を奇数次の多項式とすると，十分大きな実数 $x \in \mathbb{R}$ について $f(-x) < 0 < f(x)$ が成り立つ．よって，中間値の定理により f の零点 $x_0 \in \mathbb{R}$ が存在する．このとき $f(X)$ は $X - x_0$ を因子に持つから，$f(X)$ の次数が $\geqslant 1$ ならば可約である． □

Corollary 1.1.3

R の奇数次拡大体は $\mathbb{R}$ 自身のみである．

[*1] このような K は，$f(X) \in \mathbb{C}[X]$ を α の（$\mathbb{C}$ 上）最小多項式としたときに $f(X)$ の（$\mathbb{R}$ 上）最小分解体として取れば良い．

Proof. $L \neq \mathbb{R}$ を $\mathbb{R}$ の奇数次拡大体として, 元 $a \in L \backslash \mathbb{R}$ を任意に取る. a の $\mathbb{R}$ 上最小多項式を $f(X) \in \mathbb{R}[X]$ とすれば, その次数は $\mathbb{R}$ に a を添加した体 $\mathbb{R}(a)$ の拡大次数 $[\mathbb{R}(a):\mathbb{R}]$ と一致する. 一方 $[\mathbb{R}(a):\mathbb{R}] = [L:\mathbb{R}]/[L:\mathbb{R}(a)]$ が成り立ち，また $[L:\mathbb{R}]$ は奇数であると仮定したから，$[\mathbb{R}(a):\mathbb{R}]$ も奇数となる．よって **Lemma 1.1.1** より $f(X)$ は 1 次式または可約となるが，いずれの場合も仮定に矛盾する．従って $L = \mathbb{R}$. □

以下，特に断らない限り，群はすべて有限群を指すものとする．

Theorem 1.1.2 の証明のために，次の二つの事実は一旦認めることにする（これらは次節で証明する）:

i)（Sylow の定理）群 G の位数の素因子 p を任意に取り，$|G| = p^e r$（$\gcd(p,r) = 1$）とする．このとき，位数が p^e であるような G の部分群（**p-Sylow 部分群と呼ぶ**）が存在する．

ii) p 群（位数が素数 p の冪であるような群）は指数 p の部分群を持つ．

*Proof of **Theorem 1.1.2**.* Galois 拡大 $K/\mathbb{R}$ の Galois を $G = \mathrm{Gal}(K/\mathbb{R})$ と置く．G の位数は拡大次数 $[K:\mathbb{R}]$ と等しく，また $[K:\mathbb{R}] = [K:\mathbb{C}] \cdot [\mathbb{C}:\mathbb{R}]$ は $[\mathbb{C}:\mathbb{R}] = 2$ の倍数であるから，$|G|$ は 2 を素因子に持つ．よって i) より 2-Sylow 部分群 $S \leqslant G$ が存在して，$|G|/|S|$ は $|S|$ と互いに素，すなわち奇数となる．

S に対応する中間体 $K/L/\mathbb{R}$ を取る（Galois の基本定理）と，拡大次数について

$$[L:\mathbb{R}] = \frac{[K:\mathbb{R}]}{[K:L]} = \frac{|G|}{|S|}$$

が成り立つ．特に L は $\mathbb{R}$ の奇数次の拡大体であるが，**Corollary 1.1.3** より，これは $[L:\mathbb{R}] = 1$，すなわち $L = \mathbb{R}$ でしかあり得ない．従って $S = G$ となり，G は 2 群（位数が 2 の冪 $|G| = 2^n$）である．

$n \leqslant 1$ ならば良い．$n \geqslant 2$ として矛盾を導こう．中間体 $K/\mathbb{C}/\mathbb{R}$ に対応する G の部分群を $H_0 \leqslant G$ とする．G が 2 群だから H_0 もまた 2 群であり，ii) より指数 2 の部分群 $H \leqslant H_0$ を持つ．これに対応する中間体を $K/C/\mathbb{R}$ とすると，$H \leqslant H_0$ であるから C は $\mathbb{C}$ の拡大体であり，その拡大次数は $[C:\mathbb{C}] = [L:\mathbb{C}]/[L:C] = |H_0|/|H| = 2$ となる．しかし $\mathbb{C}$ の 2 次拡大体は存在しない（**Lemma 1.1.2**）から矛盾する．よって $n \leqslant 1$. □

Lemma 1.1.2

> $\mathbb{C}$ の 2 次拡大体は存在しない．

Proof. $K/\mathbb{C}$ を 2 次拡大体とすると，ある 2 次既約多項式 $f(X) \in \mathbb{C}[X]$ が存在して $K \cong \mathbb{C}[X]/(f(X))$ となる．一方，$\mathbb{C}$ 上の 2 次方程式については解の公式が知られていて，2 次式は常に可約である．よって $\mathbb{C}$ の 2 次拡大体は存在しない. □