

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	1
1.2	有限群論	2
1.3	Galois 理論の基本定理	6

§ 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を言うには、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 ≥ 3 ならば可約である。□

COROLLARY 1.1.3

\mathbb{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 $a \in L \setminus \mathbb{R}$ 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 $L = \mathbb{R}$. \square

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. 有限次 Galois 拡大 K/\mathbb{R} の Galois 群を $G = \text{Gal}(K/\mathbb{R})$ 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 $S \leq G$ 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.

$n \leq 1$ ならば良い. $n \geq 2$ 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 $H_0 \leq G$ 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 $H \leq H_0$ を持つ. これに対応する中間体を $K/C/\mathbb{R}$ とすると, $H \leq H_0$ 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 $n \leq 1$. \square

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. \square

§ 1.2 有限群論

この節では, 前節で認めた二つの事実に証明する.

1.2.1 Sylow の定理

1.2.2 p 群の性質

有限群論の基本的な概念に、**冪零**と**可解**がある。これらの定義には多くのバリエーションがあり、ここではそのうちの一つを採り上げる。

DEFINITION 1.2.1

群 G が**冪零** (*nilpotent*) であるとは、 $G_0 = G$, $G_i = [G_{i-1}, G]$ ($i = 1, 2, \dots$) によって定まる G の正規部分群の列

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_n \supseteq \dots$$

が有限回で終わる、すなわち十分大きな n について $G_n = 1$ となることを言う。

また、 G が**可解** (*solvable*)*²であるとは、 $G^{(0)} = G$, $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ ($i = 1, 2, \dots$) によって定まる G の部分群の列

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots \supseteq G^{(n)} \supseteq \dots$$

が有限回で終わることを言う。簡単のため、 $G' = G^{(1)}$, $G'' = G^{(2)}$ といった表記をよく用いる。

定義からすぐ分かるように、

LEMMA 1.2.1

冪零群は可解である。

Proof. G が冪零群であれば、上の定義のように正規部分群 $G_i \trianglelefteq G$ を定義したとき、十分大きな n に対して $G_n = 1$ となる。任意の $i \geq 1$ に対して、もし $G^{(i-1)} \subset G_{i-1}$ ならば $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subset [G_{i-1}, G] = G_i$ となるから、結局 $G^{(n)} \subset G_n = 1$ が分かる。よって G は可解。□

あとで示すように p 群は冪零であるから、可解でもある。よって、次の命題から事実 ii) が従う：

PROPOSITION 1.2.1

G が可解群であれば、各 G_{i-1}/G_i が素数位数であるような G の部分群の列

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_n = 1$$

が存在する。

*² **可解**という名前の由来は、方程式の可解性にある。そもそも Galois 理論は「5 次以上の方程式が代数的に解ける（方程式が可解である）ための必要十分条件」の研究に端を発することは聞いたことがあると思う。この方程式の解を $\alpha_1, \dots, \alpha_n$ としたときに、有理数体 \mathbb{Q} にこれらを添加した体拡大 $\mathbb{Q}(\alpha_1, \dots, \alpha_n)/\mathbb{Q}$ の Galois 群の可解性と、元の方程式の代数的な可解性が密接に関係する。詳しい議論は本稿の範囲を大きく逸脱するため、省略する。

COROLLARY 1.2.2

p 群は指数 p の（正規）部分群を持つ。

Proof. G を p 群とすると、上で述べたことにより、これは可解である。よって **PROPOSITION 1.2.1** を使えば、 G/G_1 が素数位数であるような正規部分群 $G_1 \trianglelefteq G$ を取れる。 G が p 群であるから、 G/G_1 もまた p 群でなければならない。よって G/G_1 の位数は p であり、すなわち G_1 の指数は p となる。□

まず **PROPOSITION 1.2.1** を示そう。

DEFINITION 1.2.2

群 G が $1 \leq G$ と G 自身以外に正規部分群を持たないとき、 G を **単純群** (simple group) と呼ぶ。

LEMMA 1.2.2

単純可換群は素数位数である。

Proof. G を単純可換群として、その元 $1 \neq g \in G$ を任意に取る。 G が可換だから、 g によって生成された部分群 $\langle g \rangle \leq G$ は G の正規部分群であり、 G が単純だから $\langle g \rangle = G$ となる。よって G は g を生成元とする巡回群である。

G の位数を n として、これが合成数 $n = pq$ であるとき、 G の非自明な正規部分群 $\langle g^p \rangle$ が存在するが、これは G が単純であることに矛盾する。よって n は素数。□

Proof of PROPOSITION 1.2.1. 任意の部分群 $G' \leq H \leq G$ に対して、 G/H は可換であることに注意する。

G/G' が単純であれば、**LEMMA 1.2.2** より素数位数となる。単純でなければ、 G/G' の非自明な（正規）部分群が存在する。すなわち、 G の部分群 $G' < H < G$ が存在する。このとき G/H は可換群となるが、もし単純でなければ、やはり G の部分群 $H < H_1 < G$ を取れる。以下同様の操作を繰り返せば、 G の部分群の列

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = G'$$

であって、各 G_{i-1}/G_i が単純可換群であるものを取れる。**LEMMA 1.2.2** より、各 G_{i-1}/G_i はすべて素数位数である。□

さて、 p 群が冪零であることを証明しよう。冪零群の定義として、次のものが使いやすい：

PROPOSITION 1.2.3

群 $G = G_0$ から出発して、 $G_i = G_{i-1}/Z(G_{i-1})$ という群の列 G_0, G_1, \dots を作るとき、もし十分大きな n に対して $G_n = 1$ となるならば G は冪零である。

Proof. n に関する帰納法で証明する. $n = 1$ のときは $G = Z(G)$, つまり G が可換群であることを意味するから, 冪零である.

$n \geq 2$ のとき $n-1$ までは仮定すると, G_1 が冪零群となる. すると, 次の **LEMMA 1.2.3** によって G も冪零となる. \square

LEMMA 1.2.3

群 G について, $G/Z(G)$ が冪零群のとき G もまた冪零群となる.

Proof. $G/Z(G)$ を冪零群として, G の正規部分群の列

$$G = G_0 \geq G_1 \geq \cdots \geq G_n \geq \cdots, \quad G_i = [G_{i-1}, G]$$

を考える. これを自然な全射 $G \twoheadrightarrow G/Z(G)$ で送ることで, $G/Z(G)$ の正規部分群の列

$$G/Z(G) = Z_0 \geq Z_1 \geq \cdots \geq Z_n \geq \cdots, \quad Z_i = G_i Z(G)/Z(G)$$

を得る. 準同型は交換子を保つから, $Z_i = [Z_{i-1}, Z_0]$ が成り立ち, 十分大きな n に対して $Z_n = 1$ となる. これは G_n が準同型 $G \twoheadrightarrow G/Z(G)$ の核に含まれること, すなわち $G_n \leq Z(G)$ を意味する. すると $[G_n, G] \leq [Z(G), G] = 1$ となるから, G は冪零. \square

1.2.3 群作用と p 群

群 G が有限集合 X に右から作用している状況を考える: $X \curvearrowright G$. 元 $g \in G$ の X への作用を $x \mapsto x^g$ と表す. $x \in X$ の G 軌道を x^G , 固定化群を $G_x = \{g \in G \mid x^g = x\}$, $S \subset G$ の固定点の集合を $C_X(S) = \{x \in X \mid S \subset G_x\}$ と書く.

LEMMA 1.2.4

任意の元 $x \in X$ に対して, $|x^G| = [G : G_x]$.

Proof.

$$x^g = x^h \iff gh^{-1} \in G_x \iff G_x g = G_x h \quad (x \in X, g, h \in G).$$

\square

LEMMA 1.2.5

$|G : G_x|$ ($x \in X$) の公約数は $|X|$ の約数でもある.

Proof. X は軌道の非交叉和となっているから, **LEMMA 1.2.4** から従う. \square

LEMMA 1.2.6

G が p 群ならば, $|X| \equiv |C_X(G)| \pmod{p}$.

Proof. $Y := X \setminus C_X(G)$ とおくと, G は自然に Y へ作用する. 任意の元 $y \in Y$ に対して $G_y < G$ だから, $[G : G_y] \neq 1$ となる. さらに G が p 群だから $[G : G_y]$ は p の倍数. よって **LEMMA 1.2.5** より $|Y|$ も p の倍数で, $|X| = |Y| + |C_X(G)| \equiv |C_X(G)|$. \square

LEMMA 1.2.7

$G \neq 1$ を p 群, $1 \neq N \trianglelefteq G$ をその正規部分群とする. このとき $Z(G) \cap N \neq 1$ となる. 特に $N = G$ と取れば $Z(G) \neq 1$.

Proof. $X := N \curvearrowright G$ を共役作用とする. **LEMMA 1.2.6** より $|C_X(G)| \equiv |X| \pmod{p}$ となるが, N も p 群であるから $|X| \equiv 0$ である. よって $|C_X(G)|$ は p の倍数となる.

一方で $1 \in C_X(G)$ だから $|C_X(G)| \neq 0$ となり, p の倍数でもあるから $|C_X(G)| \geq 2$. さらに定義より $C_X(G) = Z(G) \cap N$ だから $Z(G) \cap N \neq 1$. \square

THEOREM 1.2.4

p 群は冪零である.

Proof. G を p 群として, 群 G_0, G_1, \dots を $G_0 = G$, $G_i = G_{i-1}/Z(G_{i-1})$ によって帰納的に定義する. G が p 群だから, 各 G_i もまた p 群である. よって **LEMMA 1.2.7** より, 十分大きな n に対して $G_n = 1$ となる. すると **PROPOSITION 1.2.3** から G の冪零性が従う. \square

§ 1.3 Galois 理論の基本定理