代数学の基本定理

Masato Nakata

Faculty of Science, Kyoto University

Contents

Preface

代数学の基本定理の証明は，複素関数論によるものがよく知られているが，[3] では Galois 理論の応用として（複素関数論を用いずに）証明している．ただし，この本は行間が広いため，それらをすべて埋め，できる限り self-contained にしたものを本稿にて紹介する．線形代数の基礎と，群・環・体の定義が分かっていれば十分読めるであろう．

群論に関する部分は主に [2] を参考にした．可換環論の部分は [3] を，Galois 理論の基本定理の部分は [1] を，その他の体論は [4] を元に書いた．

§ 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の中で考えている[*1]．$\mathbb{C}(\alpha)$ 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[*2]．$K = \mathbb{C}$ 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 $\geqslant 3$ 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] 正確には，任意の $\mathbb{C}$ 上多項式 $g(X) \in \mathbb{C}[X]$ を取り，$\mathbb{C}$ の拡大体 $\mathbb{C}[X]/(g(X))$ において X の代表する元を α とする．

[*2] $f(X) \in \mathbb{R}[X]$ を α の（$\mathbb{R}$ 上）最小多項式として，$(X^2+1)f(X)$ の最小分解体を取る．**Corollary 1.3.11 and Proposition 1.3.16** 参照．

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 $L = \mathbb{R}$. □

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）単位群でない 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 $G = \mathrm{Gal}(K/\mathbb{R})$ 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[*3]．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[*4]．よって $\mathbb{C}$ の 2 次拡大体は存在しない. □

§ 1.2 有限群論

この節では，前節で認めた二つの事実を証明する．p を素数とする.

[*3] $H_0 = 1$ は $\mathbb{C} = K$ を意味する（Galois の基本定理）が，$[K : \mathbb{R}] = 2^n \neq 2 = [\mathbb{C} : \mathbb{R}]$ と仮定しているから $H_0 \neq 1$ でなければならない.

[*4] つまり「任意の複素係数 2 次方程式は少なくとも一つの解を持つ」ということだが，これは「絶対値が 1 であるような任意の複素数 $z_0 = a_0 + b_0\sqrt{-1}$ に対して，方程式 $z^2 = z_0$ は解を持つ」ことを確かめれば良い. そこで $a = \sqrt{(a_0+1)/2}$, $b = (a_0/|a_0|)\sqrt{(1-a_0)/2}$ と置けば，$z = a + b\sqrt{-1}$ は $z^2 = z_0$ の解であることが計算できる.

1.2.1 冪零群と可解群

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，$G_0 = G$，$G_i = [G_{i-1}, G]$（$i = 1, 2, \ldots$）によって定まる G の正規部分群の列

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant \cdots$$

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

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(n)} \trianglerighteq \cdots$$

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．
容易に分かるように，$G \neq 1$ が冪零ならば $G_1 < G_0$，可解ならば $G^{(1)} < G^{(0)}$ が成り立つ．

定義からすぐ分かることとして，

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 $i \geqslant 1$ 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

$G \neq 1$ 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

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

が存在する．

[*5] **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 $\alpha_1, \ldots, \alpha_n$ としたときに，有理数体 $\mathbb{Q}$ にこれらを添加した体拡大 $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}$ の Galois 群の可解性と，元の方程式の代数的な可解性とが密接に関係する．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 $1 \leqslant G$ 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

単純可換群の位数は 1 または素数である．

Proof. $G \neq 1$ 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 $\langle g \rangle \leqslant G$ 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**.* 任意の正規部分群 $G' \leqslant H \trianglelefteq G$ 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 の正規部分群 $G' < H \triangleleft G$ が存在する[*6]．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 の正規部分群 $H < H_1 \triangleleft G$ を取れる．以下同様の操作を繰り返せば，G の部分群の列

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

であって，各 G_{i-1}/G_i が（1 でない）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，次小節で p 群が冪零であることを証明する．そのための準備として，次の判定法を用意しておく（この命題の逆も簡単に示すことはできるが，本稿では必要ないため省略する）：

[*6] G の部分群 $G' \leqslant H \leqslant G$ の剰余群 H/G' が正規ならば H も正規である．より一般に，全射群準同型 $\varphi : G \to H$ について，H の正規部分群 $N \trianglelefteq H$ の逆像 $\varphi^{-1}(N)$ もまた G の正規部分群となる．

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．

$n \geqslant 2$ のとき $n-1$ までを仮定すると，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． □

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

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

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

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

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 $G_n \leqslant Z(G)$ を意味する．すると $[G_n, G] \leqslant [Z(G), G] = 1$ となるから，G は冪零. □

1.2.2 群作用と p 群

群 G が有限集合 Ω に右から作用している状況を考える：$\Omega \curvearrowleft G$. 元 $g \in G$ の Ω への作用を $x \mapsto x^g$ と表す．$x \in \Omega$ 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 $C_\Omega(S) = \{x \in \Omega \mid S \subset G_x\}$ と書く．

Lemma 1.2.4

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

Proof.

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

□

LEMMA 1.2.5

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

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

LEMMA 1.2.6

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

Proof. $\Theta \coloneqq \Omega \setminus C_\Omega(G)$ とおくと，G は自然に Θ へ作用する．任意の元 $y \in \Theta$ 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 $|\Theta|$ も p の倍数で，$|\Omega| = |\Theta| + |C_\Omega(G)| \equiv |C_\Omega(G)|$. □

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

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

THEOREM 1.2.4

p 群は冪零である．

Proof. G を p 群として，群 $G_0, G_1, \ldots$ 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． □

1.2.3 Sylow の定理

以上で事実 ii) を証明できた．次は i) について見ていこう．

Definition 1.2.3

群 G の部分群のうち，p 群でもあるものを G の p **部分群**（*p-subgroup*）と呼ぶ．G の p 部分群のうちで極大なものを p**-Sylow 部分群**（*Sylow p-subgroup*）と呼び，その全体を $\mathrm{Syl}_p(G)$ と書く．

Proposition 1.2.5

任意の群において，p-Sylow 部分群は存在する．

Proof. 群 G の p 部分群全体のなす族を $\mathcal{P}$ と置くと，これは単位群 $1 \leqslant G$ を含むから空でない．さらに $\mathcal{P}$ は有限集合であるから，極大元 $P \in \mathcal{P}$ を持つ．（$P_0 = 1 \in \mathcal{P}$ から出発して，$P_{i-1} < P_i \in \mathcal{P}$ なる P_i を繰り返し取っていけば良い．$\mathcal{P}$ が有限集合だからこの繰り返しは有限回で終わる．） □

Sylow 部分群を考えるにあたって，重要な役割を果たすのが p **核**と呼ばれるものである．

Definition 1.2.4

群 G の p-Sylow 部分群すべての共通部分 $\mathcal{O}_p(G) \coloneqq \bigcap_{P \in \mathrm{Syl}_p(G)} P$ を G の p **核**（*p-core*）と呼ぶ．

Proposition 1.2.6

群の p 核は最大の正規 p 部分群である．

Proof. 群 G の p 核を $O \coloneqq \mathcal{O}_p(G)$ と置く．

これが G の p 部分群であることは明らか．また，G 上の自己同型によって p-Sylow 部分群は p-Sylow 群へ移るから，特に内部自己同型を考えれば，O の正規性が従う[*7]．

次に G の正規 p 部分群 $N \trianglelefteq G$ と p-Sylow 部分群 $P \in \mathrm{Syl}_p(G)$ を任意に取る．$P = NP$ を言えば良い．実際，このとき $N \leqslant P$ となり，P は任意であったから $N \leqslant O$ が従う．

$P \leqslant NP$ は明らか．逆の包含関係を示す．次の **Lemma 1.2.8** より $|NP|$ は $|N \times P| = |N| \times |P|$ の約数であり，N と P はともに p 部分群だから NP もまた p 部分群となる．すると，p-Sylow 部分群の極大性により，$P = NP$ となる． □

[*7] G の自己同型群 $\mathrm{Aut}(G)$ は集合 $\mathrm{Syl}_p(G)$ へ作用している．このことから，O は $\mathrm{Aut}(G)$ の各元の下で不変に保たれることが分かる．すなわち，任意の元 $g \in G$ と自己同型 $\sigma \in \mathrm{Aut}(G)$ に対して，$g \in O$ ならば $g^\sigma \in O$ が成り立つ．

LEMMA 1.2.8

$H_1, H_2 \leqslant G$ を群 G の部分群とすれば，

$$|H_1 H_2| = \frac{|H_1 \times H_2|}{|H_1 \cap H_2|}.$$

特に，$|H_1 H_2|$ は $|H_1 \times H_2|$ の約数となる．

Proof. 直積集合 $H_1 \times H_2$ 上の同値関係 $\sim$ を

$$(a,b) \sim (c,d) \overset{\text{def.}}{\iff} ab = cd$$

で定義すれば，$|H_1 H_2|$ は同値類の個数に等しい．また，各 $(a,b) \in H_1 \times H_2$ の同値類はちょうど $|H_1 \cap H_2|$ 個の元を含むから，主張が従う． □

COROLLARY 1.2.7

群 G が正規 p-Sylow 部分群 $P \in \mathsf{Syl}_p(G)$ を持てば，$\mathsf{Syl}_p(G) = \{P\}$ となる．逆に，$\mathsf{Syl}_p(G) = \{P\}$ であれば P は G の正規部分群となる．

Proof. もしある p-Sylow 部分群 $P \in \mathsf{Syl}_p(G)$ が正規であれば，**PROPOSITION 1.2.6** より $P \leqslant \mathcal{O}_p(G)$ が成り立つ．一方 p 核の定義から $P \geqslant \mathcal{O}_p(G)$ であるから，$P = \mathcal{O}_p(G)$，すなわち $\mathsf{Syl}_p(G) = \{P\}$ が従う．

逆は **PROPOSITION 1.2.6** から分かる． □

続いて，古典的に知られた次の定理を考える：

THEOREM 1.2.8（Cauchy の定理）

群 G の位数が p の倍数であれば，G は位数 p の元を持つ．

Proof. 集合 Ω を

$$\Omega = \{(x_1, \ldots, x_p) \mid x_1 \cdots x_p = 1,\ x_i \in G\ (1 \leqslant i \leqslant p)\}$$

で定義すると，p 次巡回群 $\mathbb{Z}_p$ は Ω へ作用する：

$$(x_1, \ldots, x_p) \mapsto (x_2, \ldots, x_p, x_1).$$

実際，

$$x_1 \cdots x_p = 1 \iff x_2 \cdots x_p = x_1^{-1} \iff x_2 \cdots x_p x_1 = 1.$$

この作用に **LEMMA 1.2.6** を適用すれば，$|\Omega| \equiv |C_\Omega(\mathbb{Z}_p)| \pmod{p}$ を得る．一方仮定により $|\Omega| = |G|^{p-1}$ は p の倍数であるから，$|C_\Omega(\mathbb{Z}_p)| \equiv 0$ となる．ここで $(1, \ldots, 1) \in C_\Omega(\mathbb{Z}_p)$ だから $|C_\Omega(\mathbb{Z}_p)| \neq 0$，特に $\geqslant 2$ とな

る．従ってある $(1,\dots,1) \neq (x_1,\dots,x_p) \in C_\Omega(\mathbb{Z}_p)$ が存在するが，これは $x_1 = \cdots = x_p \neq 1$ かつ $x_1^p = 1$ を意味する． □

COROLLARY 1.2.9

群 G について，$\mathrm{Syl}_p(G) = \{P\}$ ならば p は $[G:P]$ の約数でない．

Proof. $\mathrm{Syl}_p(G) = \{P\}$ とすれば，**COROLLARY 1.2.7** の後半によって，P は G の正規部分群となる．そこで p が $[G:P]$ の約数だと仮定すれば，**THEOREM 1.2.8** より位数 p の元 $gP \in G/P$ が存在する．一方このとき $\langle g\rangle P$ は G の p 部分群であるから，p-Sylow 部分群の極大性から $\langle g\rangle P = P$，すなわち $g \in P$ となり矛盾する．（$\langle g\rangle$ は g によって生成される部分群を表す．）よって p は $[G:P]$ の約数ではない． □

最後に，有限群論において最も重要な定理の一つである Sylow の定理を証明する．ただし，本来の Sylow の定理はもっと強い主張を含むが，ここでは事実 i) に相当する部分だけを述べる．定理の他の部分に関しても，証明中の $\mathrm{Syl}_p(N) = \{P\}$，$[N:P] \not\equiv 0$ および $[G:N] \equiv 1$ という関係からすぐに従う．

THEOREM 1.2.10（Sylow の定理）

群 G の位数が $|G| = p^e r$（$\gcd(p,r) = 1$）という形に書けたとする．このとき，G の p-Sylow 部分群の位数は p^e である．

Proof. G の p-Sylow 部分群 $P \in \mathrm{Syl}_p(G)$ を任意に取り，その正規化部分群 $N = N_G(P) = \{g \in G \mid g^{-1}Pg = P\}$ を考える．$P \trianglelefteq N$ であるから，**COROLLARY 1.2.7** と **COROLLARY 1.2.9** より，$\mathrm{Syl}_p(N) = \{P\}$ かつ $[N:P] \not\equiv 0 \pmod p$ が分かる．（P は N の p-Sylow 部分群であることに注意する．）

残りは $[G:N] \equiv 1 \pmod p$ を示せば良い．実際，$|G| = [G:N]\cdot[N:P]\cdot|P|$ であるから，$[G:N], [N:P] \not\equiv 0$ ならば $|P| = p^e$ となる．

P を次の集合 Ω へ右から正則に作用させる[*8]：

$$\Omega = \{Ng \mid g \in G\} \curvearrowleft P.$$

このとき $|\Omega| = [G:N]$ であり，**LEMMA 1.2.6** を使うと $[G:N] = |\Omega| \equiv |C_\Omega(P)|$ を得る．$C_\Omega(P) = \{N\}$ を示そう．P は N の部分群だから $N \in C_\Omega(P)$ は明らかである．逆の包含関係を見るために，$Ng \in C_\Omega(P)$ とする．これは $NgP = Ng$，すなわち $gPg^{-1} \leqslant N$ を意味する．脚注 [*7] で述べたように gPg^{-1} もまた p-Sylow 部分群であるから，$\mathrm{Syl}_p(N) = \{P\}$ より $gPg^{-1} = P$ を得る．これは $g \in N$ に他ならない．よって $C_\Omega(P) = \{N\}$ となり，$[G:N] \equiv 1 \pmod p$ が言えた． □

[*8] 本来**右正則作用**（*right regular action*）とは群 G が自身に右からの積で作用すること，すなわち $h^g := h\cdot g$ で定義される右作用 $G \curvearrowleft G$ のことである．今，Ω には G の右正則作用から自然に誘導された作用 $(Nh)^g := Nhg$ があり，Ω への正則作用とはこれを表している．

§ 1.3 Galois 理論の基本定理

この節では，Galois 理論の初歩について解説する．最終的な目標は，

- 有限次 Galois 拡大 L/K において，その Galois 群 $\mathrm{Gal}(L/K)$ の部分群と中間体が一対一に対応していること，
- そして Galois 群の位数と拡大次数が等しいこと

を示すことである．
以下，環と体はすべて 0 でない単位的かつ結合的な可換環・可換体とする[*9]．

1.3.1 可換環論

最初に，可換環論のいくつかの事実を証明しておこう．任意のイデアルが単項イデアルであるような環を **PID** と呼び，0 でも可逆元でもない任意の元が有限個の素元の積で書けるような環を **UFD** と呼んだ．

Definition 1.3.1

整域[*10] R の元 a は，それによって生成される単項イデアル (a) が素イデアルのとき**素元**（*prime element*）と呼ばれる．また $a \neq 0$ は，$a = bc$ ならば b と c の少なくとも一方が可逆元となるとき，**既約元**（*irreducible element*）と呼ばれる．

定義からすぐ分かるように，0 でない素元は既約元である．実際，$0 \neq a \in R$ を素元として $a = bc$ とすると $bc \in (a)$ であり，(a) が素イデアルだから b と c の少なくとも一方は (a) の元である．たとえば $b \in (a)$ とすれば，$b = ad$ なる $d \in R$ が存在する．このとき $a = bc = adc$ が成り立ち，R は整域だから $1 = dc$，すなわち c が可逆元となる．

Theorem 1.3.1

PID は UFD である．また，PID の素イデアルは 0 または極大イデアルである．

Proof. R を PID として，その可逆元でない元 $0 \neq a_0 \in R$ を任意に取る．イデアル (a_0) はある極大イデアル $\mathfrak{m}_1 = (p_1) \subset R$ に含まれ，このときある元 $a_1 \in R$ によって $a_0 = p_1 a_1$ となる．もし a_1 が可逆元でなければ，イデアル $(a_1) \subset R$ に対して同様の議論を繰り返せば，ある極大イデアル $\mathfrak{m}_2 = (p_2) \subset R$ と元 $a_2 \in R$ が存在して $a_1 = p_2 a_2$ となる．以下繰り返して，極大イデアル $\mathfrak{m}_1, \mathfrak{m}_2, \ldots \subset R$ と元 $a_1, a_2, \ldots \in R$ であって $a_{i-1} = p_i a_i$ を満たすものが取れる．

上の操作が有限回で終わらないとしよう．すなわち，どの a_i も可逆元にならなかったと仮定しよう．$a_{i-1} = a_i p_i$ という関係から，イデアルの包含 $(a_1) \subset (a_2) \subset \cdots$ を得る．この極限を $\mathfrak{a} = \bigcup_i (a_i)$ と置けば，これ

[*9] 単位的とは積に関する単位元の存在を意味し，結合的とは積が結合的であることを意味する．
[*10] 整域である必要はないが，簡単のため整域に限定して考える．

は R のイデアルである．R は PID であるから，$\mathfrak{a} = (a)$ となる元 $a \in \mathfrak{a}$ が存在する．このとき，a はある $\mathfrak{a}_i$ に含まれるから，$(a) \subset \mathfrak{a}_i$ となる．すると $(a_i) \subset (a_{i+1}) \subset \mathfrak{a} \subset (a_i)$ となるが，これは a_{i+1} が可逆元でないことに矛盾する．よって，ある a_i は可逆元となる．

以上より，ある極大イデアル $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ の元 $p_i \in \mathfrak{m}_i$ $(1 \leqslant i \leqslant n)$ と可逆元 $a_n \in R$ が存在して $a_0 = p_1 \cdots p_n a_n$ となることが分かる．従って R は UFD.

また，もし (a_0) が素イデアルであれば，$p_1 \cdots p_n = a_0 a_n^{-1} \in (a_0)$ だから $p_i \in (a_0)$ なる p_i が存在する．このとき $(a_0) = (p_i)$ は極大イデアルとなる． □

THEOREM 1.3.2

UFD において，既約元は素元である．

Proof. UFD R の既約元 $a \in R$ を任意に取り，$a = p_1 \cdots p_n$ と素元分解する．今 a は既約だから $n = 1$ かつ $a = p_1$ でなければならない．すなわち a は素元である． □

COROLLARY 1.3.3

体上の既約多項式は極大イデアルを生成する．正確に言うと，体 K 上の既約多項式 $p(X) \in K[X]$ によって生成される単項イデアル $(p(X)) \subset K[X]$ は極大イデアルである．

Proof. 体 K は PID であり，PID 上の多項式環もまた PID であった．よって $K[X]$ は UFD であり（**THEOREM 1.3.1**），また既約多項式 $p(X) \in K[X]$ で生成されるイデアル $(p(X)) \subset K[X]$ は素イデアルである（**THEOREM 1.3.2**）．既約多項式は 0 でないから，$(p(X))$ は極大イデアルである（**THEOREM 1.3.1**）． □

1.3.2 代数拡大

体拡大のクラスのうちもっとも基本的なものは代数拡大である．

DEFINITION 1.3.2

体の包含関係 $K \subset L$ が与えられたとき[*11]，この関係を**体拡大**（*extension of fields*）と言い L/K という記号で表す．また，このとき L を K の**拡大体**（*extension field*）と呼ぶ．
二つの体拡大 L/M と M/K があるとき，M を体拡大 L/K の**中間体**（*intermediate field*）と呼ぶ．
拡大体の元 $x \in L$ は，K 上のある非零多項式の根であるとき，すなわちある多項式 $0 \neq f(X) \in K[X]$ が存在して $f(x) = 0$ となるとき，K 上**代数的**（*algebraic*）であると言う．L の任意の元が K 上代数的であるとき，体拡大 L/K を**代数的**（*algebraic*）であると言う．

[*11] 厳密には，単射体準同型 $K \hookrightarrow L$．もちろん体準同型はすべて単射だから，単に体準同型 $K \to L$ と言っても同じことである．

Definition 1.3.3

可換環[*12]の間の環準同型 $R \to A$ を R **代数**（R-*algebra*），または R **多元環**と呼ぶ．準同型を明示しない場合，単に A を R 代数などと言う．
R 代数を $\varphi : R \to A$ と書くとき，A には自然に R 加群としての構造が入る：

$$R \times A \xrightarrow{\varphi \times \mathrm{id}_A} A \times A \xrightarrow{\times} A, \quad (a, b) \mapsto \varphi(a)b.$$

R 代数の間の環準同型 $A \to B$ は，R 準同型でもあるとき R **代数準同型**（R-*algebra homomorphism*）などと呼ばれる．A から B への R 代数準同型全体のなす集合を $\mathrm{Hom}_R(A, B)$ と書く．特に $A = B$ のときは準同型を R **自己代数準同型**（R-*algebra endomorphism*），同型を R **自己代数同型**（R-*algebra automorphism*）と言い，それらのなす集合をそれぞれ $\mathrm{End}_R(A)$，$\mathrm{Aut}_R(A)$ と書く．特に誤解の恐れの無いときは，単に R 準同型，R 自己準同型，R 自己同型などと呼ぶ．

体拡大 L/K について，包含写像 $K \hookrightarrow L$ によって L は K 代数となる．特に K 上ベクトル空間となる．

Definition 1.3.4

体拡大 L/K について，拡大体 L の K 上ベクトル空間としての次元 $\dim_K L$ をこの体拡大の**次数**（*degree*）と呼び，$[L : K] = \dim_K L$ と書く．

次の二つの性質は基本的である：

Proposition 1.3.4

有限次体拡大 L/K とその中間体 $L/M/K$ の拡大次数について，$[L : K] = [L : M] \cdot [M : K]$ が成り立つ．

Proof. $n = [M : K]$, $m = [L : M]$ と置いて，M の K 上の基底を $x_1, \ldots, x_n \in M$，L の M 上の基底を $y_1, \ldots, y_m \in L$ とする．このときすぐに分かるように，$\{x_i y_j\}$ が L の K 上の基底となる．特に各 $x_i y_j$ は互いに相異なるから，$[L : K] = nm$ が成り立つ． □

Proposition 1.3.5

有限次体拡大は代数的である．

Proof. L/K を有限次体拡大として，$n = [L : K]$ と置く．任意の元 $a \in L$ を取り，これが K 上代数的であることを確かめる．

[*12] 可換環である必要はなく，一般の環では $R \to Z(A) \hookrightarrow A$ という環準同型として定義される（$Z(A)$ は環 A の中心）．しかし，本稿では体拡大の場合しか扱わないため，可換環に限定しておいた．

L の元の列 $1, x, x^2, x^3, \dots$ を考えると，L は n 次元ベクトル空間だから $1, x, \dots, x^n$ は線形独立である．よって，ある非自明[*13]な元 $a_0, \dots, a_n \in K$ が存在して $\sum_{i=0}^{n} a_i x^i = 0$ とできる．そこで $p(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ という多項式を考えれば，x は $p(X)$ の根となり，従って代数的である． □

Galois 理論への第一歩としては，最小多項式がもっとも重要である．

THEOREM 1.3.6

> L/K を体拡大として，$0 \neq x \in L$ を K 上代数的な元とする．このとき，x を根とするような（0 でない）多項式のうちで次数最小のものが（定数倍を除いて）ただ一つ存在し，それは整除関係についても最小である．特に最高次の係数が 1 となるように取ったものを，x の**最小多項式**（*minimal polynomial*）と呼ぶ．
> さらに，最小多項式は K 上既約多項式であり，K 代数としての同型 $K(x) \cong K[X]/(p(X))$ が存在する．ただし，$K(x)$ は K に x を添加した体である．また，体拡大 $K(x)/K$ の次数について $[K(x) : K] = \deg p(X)$ が成り立つ．

Proof. $\mathrm{eval}_x(f(X)) = f(x)$ で定義される環準同型 $\mathrm{eval}_x\, K[X] \to K$ を考え，その核を $\mathrm{Ker}\,\mathrm{eval}_x = (p(X))$ と置く．ここで $p(X)$ の最高次の係数が 1 となるように取れば，明らかに $p(X)$ は x の最小多項式である．

今，準同型定理から K 代数としての同型 $K[X]/(p(X)) \cong \mathrm{Im}\,\mathrm{eval}_x = K[x]$ が成り立っている．$K[x]$ は整域であるから $(p(X))$ は $K[X]$ の 0 でない素イデアルとなり（$x \in \mathrm{Ker}\,\mathrm{eval}_x$ だから 0 ではない），従って $p(X)$ は既約多項式である．すると **COROLLARY 1.3.3** より $(p(X))$ は極大イデアルとなり，$K[x] \cong K[X]/(p(X))$ が体となる．特に $K[x] = K(x)$ であるから，$K(x) \cong K[X]/(p(X))$.

$p(X)$ の次数を $n = \deg p(X)$ と置き，$\{1, x, \dots, x^{n-1}\}$ が $K(x)$ の K 基底となることを確かめよう．まず，もしある非自明な元 $a_0, \dots, a_{n-1} \in K$ が存在して $\sum_{i=0}^{n-1} a_i x^i = 0$ となれば，$\sum_{i=0}^{n-1} a_i X^i \in \mathrm{Ker}\,\mathrm{eval}_x$ となるが，これは $p(X)$ の次数の最小性に矛盾する．よって $\{1, \dots, x^{n-1}\}$ は線形独立．また，$p(X) = \sum_{i=0}^{n} b_i X^i$ と書けば $x^n = -\sum_{i=0}^{n-1} b_i x^i$ であるから，$\{1, \dots, x^{n-1}\}$ は $K[x]$ を張る．以上より $\{1, \dots, x^{n-1}\}$ は $K(x) = K[x]$ の基底である． □

COROLLARY 1.3.7

> L/K を体拡大として，任意の元 $x \in L$ を取る．もし K 上の既約多項式 $p(X) \in K[X]$ が x を根として持つならば，$p(X)$ は x の最小多項式である．

Proof. もし x の最小多項式 $q(X)$ の次数が $\deg q < \deg p$ であれば，**THEOREM 1.3.6** より，q は p を割り切る．一方 p も q も既約であるから，$p = q$ を得る． □

1.3.3 分解体

[*13] 今の場合，**非自明**な元 $a_0, \dots, a_n$ とは，少なくとも一つの $0 \leqslant i \leqslant n$ に対して $a_i \neq 0$ であることを意味する．

この小節では最小分解体の存在と一意性を示す．次小節以降で見るように，標数 0 の体の Galois 拡大は本質的には最小分解体と同じであるので，Galois 拡大の存在を示すのに重要な役割を果たす．

Definition 1.3.5

体 K の拡大体 L/K が，多項式 $f(X) \in K[X]$ のすべての根を含むとき，L を $f(X)$ の**分解体**（*splitting field*）と呼ぶ．多項式 $f(X)$ の分解体のうちで極小なものを特に**最小分解体**（*minimal splitting filed*）と呼ぶ．
体 K が，自身の上のすべての多項式の分解体であるとき，これを**代数閉体**（*algebraically closed field*）と呼ぶ．

体の理論では，次の延長定理が本質的に重要である．

Theorem 1.3.8

体 K 上の多項式 $f(X) \in K[X]$ について，その K 上の最小分解体は K 同型を除いて一意である．

Proof. $f(X)$ の次数 $n = \deg f$ に関する帰納法で示す．L と L' をともに $f(X)$ の最小分解体とする．
$n = 1$ のとき，K が最小分解体だから良い．
$n > 1$ として，$n-1$ までの主張を仮定する．$p(X) \in K[X]$ を $f(X)$ の（K 上）既約因子として，その根 $x \in L$ および $x' \in L'$ を取る．このとき，**Theorem 1.3.6** によって K 同型 $K(x) \cong K[X]/(p(X)) \cong K(x')$ が存在する．
今，この K 同型によって L' を $K(x)$ の拡大体と思うことにして，$K(x)[X]$ 上で $f(X) = (X-x)f_1(X)$ と分解すれば，L と L' はともに $f_1(X)$ の最小分解体である．よって帰納法の仮定により，$K(x)$ 同型 $L \cong L'$ を得る．$K(x)$ 準同型は K 準同型でもあるから，主張が示された． □

続いて，最小分解体が存在することを示そう．上の **Theorem 1.3.8** はどのように最小分解体を構成しても良いと保証してくれる．

Theorem 1.3.9

体 K 上の多項式 $f(X) \in K[X]$ について，その K 上の最小分解体は存在する．また，その拡大次数は有限である．

Proof. $K[X]$ 内で $f(X) = p_1(X) \cdots p_r(X)$ と素元分解し（**Theorem 1.3.1**），その既約因子のうちで次数最大なものを $p(X)$ と置く．簡単のため，その最高次の係数を 1 とする．$p(X)$ の次数 $n = \deg p$ に関する帰納法で示す[*14]．
$n = 1$ のときは K がすでに分解体となっているから良い．
$n > 1$ として，$n-1$ までの主張を仮定する．**Theorem 1.3.6** より，$L := K[X]/(p(X))$ は K の n 次拡大体であって $p(X)$ の根を含む．よって帰納法の仮定により，$f(X)$ の L 上の最小分解体が存在する．これは K 上の

[*14] 厳密には，次数が n であるような既約因子の数を m としたときに，順序対 (n, m) の辞書式順序に関する帰納法になっている．

最小分解体でもある．実際，L'/K を $f(X)$ の任意の（K 上）分解体とすれば，$p(X)$ の根 $x \in L'$ を持つ．このとき 再び **Theorem 1.3.6** より，$L \cong K(x)$ が成り立つ．よって L' は L の拡大体であるから，$f(X)$ の L 上最小分解体を含む． □

1.3.4 分離拡大

この小節では，多項式 $f(X) = \sum a_i X^i$ の**導多項式**（*derivative*）を $f'(X) = \sum i a_i X^{i-1}$ で定義する．はじめに分離拡大と導多項式の関係を見てから，分離拡大の性質を調べていく．

Definition 1.3.6

代数拡大 L/K において，L の任意の元の最小多項式が重根を持たないとき，この拡大は**分離的**（*separable*）であると言う．K のすべての代数拡大が分離的であるとき，K を**完全体**（*perfect field*）と呼ぶ．

Proposition 1.3.10

$f(X) \in K[X]$ を体 K 上の多項式とする．このとき，元 $x \in K$ が $f(X)$ の重根であることと，$f(x) = f'(x) = 0$ であることは同値．

Proof. x が $f(X)$ の重根ならば，ある多項式 $g(X) \in K[X]$ を用いて $f(X) = (X-x)^2 g(X)$ と書ける．このとき

$$f'(X) = 2(X-x)g(X) + (X-x)^2 g'(X)$$

が成り立つから，$f(x) = f'(x) = 0$.

逆に，$f(x) = f'(x) = 0$ とすると，x は $f(X)$ の根であるからある多項式 $g(X) \in K[X]$ によって $f(X) = (X-x)g(X)$ とできる．この導多項式を計算すると

$$f'(X) = g(X) + (X-x)g'(X)$$

となるから，$f'(x) = 0$ は $g(x) = 0$ を導く．よって x は $f(X)$ の重根である． □

Definition 1.3.7

環 R の積に関する単位元 $1 \in R$ について，$n \cdot 1 = 0$ なる自然数 $n \geqslant 1$ のうちで最小のものを R の**標数**（*characteristic*）と呼び $\operatorname{char} R = n$ と表す．$n \cdot 1 = 0$ となるような $n \geqslant 1$ が存在しないときは便宜上 $\operatorname{char} R = 0$ と定義する．

定義からすぐ分かるように，標数 0 の体においては 1 次以上の多項式の導多項式は 0 でない．すなわち，$f(X) \in K[X]$ を体 K 上の多項式で $\deg f \geqslant 1$ とすると，$f'(X) \neq 0$．標数が 0 でなければ，このことは必ずしも成り立たない．たとえば体 K の標数を $p > 0$ とすれば[*15]，単項式 X^p の導多項式は $pX^p = 0$ となる．

[*15] 本稿では示さないが，一般に整域の標数は 0 か素数となることが分かる．証明は難しくない．

COROLLARY 1.3.11

標数 0 の体は完全体である．

Proof. 標数 0 の体 K が完全体でないとすると，重根を持つような最小多項式 $p(X) \in K[X]$ が存在する．このとき，**PROPOSITION 1.3.10** を使えば $p(X)$ と $p'(X)$ の共通根 $x \in X$ を得る．すると上で述べたように，もし $p'(X) = 0$ であれば $p(X) = 0$ でなければならないが，最小多項式は 0 でないから $p'(X) \neq 0$．しかし **COROLLARY 1.3.7** より $p(X)$ は x の最小多項式であり，最小多項式の次数の最小性（**THEOREM 1.3.6**）に矛盾する． □

PROPOSITION 1.3.12

分離拡大 L/K とその中間体 $L/M/K$ について，体拡大 L/M もまた分離的である．

Proof. L/K が代数拡大だから L/M もやはり代数拡大である．また，L の元 $x \in L$ を任意に取り，その K 上最小多項式を $p(X) \in K[X]$，M 上最小多項式を $q(X) \in M[X]$ とすると，$M[X]$ において $p(X)$ は $q(X)$ で割り切れる（**THEOREM 1.3.6**）．今 $p(X)$ は重根を持っていないから，$q(X)$ も重根を持たない．よって L/M は分離拡大である． □

1.3.5 正規拡大

次に正規拡大と自己同型の関係を調べよう．

DEFINITION 1.3.8

代数拡大 L/K が**正規**（*normal*）であるとは，L の任意の元の最小多項式が $L[X]$ において 1 次式の積に分解することを言う．

PROPOSITION 1.3.13

正規拡大 L/K とその中間体 $L/M/K$ について，体拡大 L/M もまた正規である．

Proof. L/M が代数拡大であることは良い．L の元 $x \in L$ を任意に取り，その K 上最小多項式を $p(X) \in K[X]$，M 上最小多項式を $q(X)$ とすると，**THEOREM 1.3.6** より，$L[X]$ において $p(X)$ は $q(X)$ で割り切れる．一方 L/K が正規拡大だから，$p(X)$ は $L[X]$ において 1 次式の積に分解する．従って $q(X)$ も 1 次式の積に分解する．よって L/M は正規拡大である． □

Lemma 1.3.1

代数拡大 L/K において，すべての L 上の K 自己準同型は同型である：$\mathrm{End}_K(L) = \mathrm{Aut}_K(L)$.

Proof. L 上の K 自己準同型 $\sigma \in \mathrm{End}_K(L)$ を任意に取る．σ は自動的に単射であるから，各元 $x \in L$ に対して $y^\sigma = x$ なる元 $y \in L$ が存在することを言えば良い．x の最小多項式を $p(X) \in K[X]$ として，x と共役な元全体を $\Omega := \{y \in L \mid p(y) = 0\}$ と置く．

$p(X)$ の任意の根 $y \in \Omega$ に対して，$p(y^\sigma) = (p(y))^\sigma = 0^\sigma = 0$ となる[*16]から，σ は Ω 上に作用する．σ は単射であり，Ω は有限集合であるから，σ は全射でなければならない．よって，$y^\sigma = x$ となるような根 $y \in \Omega$ が存在する． □

Lemma 1.3.2

正規拡大 L/K とその中間体 $L/M/K$ を取る．このとき，任意の K 準同型 $\sigma : M \to L$ と任意の元 $x \in L$ に対して，σ を K 準同型 $M(x) \to L$ へ拡張できる．

Proof. x の K 上最小多項式を $p(X) \in K[X]$，M 上最小多項式を $q(X) \in M[X]$ とすれば，**Theorem 1.3.6** から，$L[X]$ において $q(X)$ は $p(X)$ を割り切ることが分かる．

σ を K 準同型 $M[X] \to L[X]$ へ拡張したとき，K 上の多項式はすべて σ で不変である．特に，$p^\sigma(X) = p(X)$. 一方 σ が環準同型であるから，$q^\sigma(X)$ は $L[X]$ において $p^\sigma(X) = p(X)$ の因子となっている．今，体拡大 L/K は正規だから，$p(X)$ と，従って $q^\sigma(X)$ も，$L[X]$ において 1 次式の積に分解する．そこで，$q^\sigma(X)$ の根の一つを $y \in L$ とすれば，σ は K 準同型

$$M(x) \cong \frac{M[X]}{(q(X))} \xrightarrow{\sigma} \frac{L[X]}{(X-y)} \cong L(y) = L$$

を誘導する．これが求める準同型であった． □

Theorem 1.3.14

L/K を有限次正規拡大として，その中間体 $L/M/K$ を取る．このとき，任意の K 準同型 $M \to L$ は L 上の K 自己同型へ拡張できる．

Proof. 任意の K 準同型 $M \to L$ から出発して **Lemma 1.3.2** を繰り返し適用すれば，K 準同型 $L \to L$ まで拡張できる．（繰り返し適用できるのは **Proposition 1.3.13** から分かる．）**Lemma 1.3.1** より，これは K 自己同型である． □

[*16] $p(X) = \sum a_i X^i$ と書けば，$p(y^\sigma) = \sum a_i (y^\sigma)^i = \sum (a_i y^i)^\sigma = (p(y))^\sigma$.

Theorem 1.3.15

有限次正規拡大 L/K と任意の二元 $x,y \in L$ に対して，次は同値：

i）x と y は互いに共役；
ii）$x^\sigma = y$ となるような K 自己同型 $\sigma \in \mathrm{Aut}_K(L)$ が存在する．

Proof. i) を仮定して $p(X) \in K[X]$ を共通の最小多項式とすれば，**Theorem 1.3.6** より，K 同型 $K(x) \cong K[X]/(p(X)) \cong K(y)$ を得る．これは **Theorem 1.3.14** によって K 同型 $L \to L$ へ拡張され，x は y へ写される．

逆に ii) を仮定して $p(X) \in K[X]$ を x の最小多項式とすれば，$p(y) = (p(x))^\sigma = 0$，すなわち x と y は互いに共役となる（**Corollary 1.3.7**）． □

この小節の最後に，有限次拡大の場合に正規拡大と最小分解体が一致することを示そう．

Proposition 1.3.16

有限次拡大 L/K について，これが正規であることと，L が K 上のある多項式の最小分解体であることは同値．

Proof. L/K が有限次正規拡大とする．まず，有限次拡大だから $L = K(x_1,\dots,x_n)$ なる元 $x_1,\dots,x_n \in L$ が存在する．これらの最小多項式をそれぞれ $p_1(X),\dots,p_n(X) \in K[X]$ として，$f(X) \coloneqq \prod_{i=1}^n p_i(X)$ と置く．L/K が正規であるから，各 $p_i(X)$ は $L[X]$ 上で 1 次式の積に分解される．特に L は $f(X)$ の分解体である．また，もし中間体 $L/M/K$ が $f(X)$ の分解体であれば，M は x_i をすべて含むから $M = L$ となる．従って L は $f(X)$ の最小分解体．

逆に，L を多項式 $f(X) \in K[X]$ の最小分解体として，その根を $x_1,\dots,x_n \in L$ とする．このとき $L = K(x_1,\dots,x_n)$．任意の元 $y = y_1 \in L$ の最小多項式 $p(X) \in K[X]$ の根がすべて L に含まれることを示す．

$p(X)$ を L 上の多項式と見て，その L 上の最小分解体を L' として $p(X)$ の根を $y_1,\dots,y_m \in L'$ とすれば，$L' = L(y_1,\dots,y_m) = K(x_1,\dots,x_n,y_1,\dots,y_m)$ が成り立つ．体拡大 L'/K の中間体として，$L'' \coloneqq K(y_1,\dots,y_m)$ と置く．これは $p(X)$ の K 上の最小分解体である．

各 $1 \leqslant i \leqslant m$ について，**Theorem 1.3.6** によって K 同型 $K(y_1) \cong K[X]/(p(X)) \cong K(y_i)$ が成り立つ．今，包含写像による体拡大 $L''/K(y_1)$ とこの同型を介した体拡大 $L''/K(y_i) \cong K(y_1)$ があり，**Theorem 1.3.8** から K 自己同型 $\sigma_i \in \mathrm{Aut}_K(L'')$ であって $y_1^{\sigma_i} = y_i$ なるものが取れる．同様に，L' は $f(X)$ の L'' 上の最小分解体であるから，σ_i を K 同型 $\sigma_i \in \mathrm{Aut}_K(L')$ へ拡張できる．これらは $f(X)$ の根全体の集合 $\Omega \coloneqq \{x_1,\dots,x_n\}$ へ全単射として作用し[*17]，従って各 σ_i は L を L へ写す，すなわち $\sigma_i \in \mathrm{Aut}_K(L)$．特に $y_1 \in L$ の像が $y_i = y_1^{\sigma_i} \in L$ となるから，L/K は正規拡大である． □

1.3.6 Galois 拡大

[*17] **Lemma 1.3.1** の証明の後半と同じ．

この小節では Galois 理論の基本定理を証明する．そのために，Galois 理論の基本的な道具である Galois 群を導入しよう．基本定理が示すように，Galois 拡大と Galois 群は密接に関係している．

Definition 1.3.9

分離的な正規拡大を **Galois 拡大**（*Galois extension*）と呼ぶ．Galois 拡大 L/K について，$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ と置きこれを体拡大 L/K の **Galois 群**（*Galois group*）と呼ぶ．
Galois 群の部分群 $G \leqslant \mathrm{Gal}(L/K)$ が与えられたとき，$C_L(G)$ をその**不変体**（*invariant field*）あるいは**固定体**（*fixed field*）と言い[*18]，$\mathrm{Fix}(G) = L^G := C_L(G)$ などと書く．

Lemma 1.3.3

Galois 拡大 L/K の中間体 $L/M/K$ について，L/M は Galois 拡大となる．また，$G \leqslant \mathrm{Gal}(L/K)$ を Galois 群の部分群としたとき，その不変体 $\mathrm{Fix}(G) = L^G$ は体拡大 L/K の中間体となる．
これによって，次の集合の間の写像

$$\{L/M/K\} \underset{\mathrm{Fix}}{\overset{\mathrm{Gal}}{\rightleftarrows}} \{G \leqslant \mathrm{Gal}(L/K)\}$$

を得る．

Proof. 前半は **Propositions 1.3.12 and 1.3.13** から従う．
後半について，まず集合としての包含関係 $K \subset \mathrm{Fix}(G) \subset L$ が成り立つことは明らか． □

Lemma 1.3.4

二つの写像 Gal, Fix はともに順序を反転させる．つまり，Galois 拡大 L/K が与えられたとき，その中間体 $M \subset N$ に対して $\mathrm{Gal}(L/M) \geqslant \mathrm{Gal}(L/N)$ が成り立ち，Galois 群の部分群 $H \leqslant G \leqslant \mathrm{Gal}(L/K)$ に対して $\mathrm{Fix}(H) \geqslant \mathrm{Fix}(G)$ が成り立つ．

Proof. Gal と Fix の定義から明らか． □

この二つの写像は Galois 接続となっていて，幅広い分野に一般化されている．

Definition 1.3.10

X と Y を順序集合として，それらの間の順序を反転させる写像

$$X \underset{g}{\overset{f}{\rightleftarrows}} Y$$

[*18] $C_L(G)$ という記法については § 1.2.2 の冒頭を参照．

を考える．これらの写像が**随伴**（*adjunction*）[*19]という関係

$$x \leqslant gf(x), \quad y \leqslant fg(y) \quad (x \in X,\, y \in Y)$$

を満たすとき，この組 (f,g) を **Galois 接続**（*Galois connection*）と呼ぶ．上で $\leqslant$ を $=$ に置き換えた関係が成り立つとき（つまり f と g が全単射で互いに逆写像となっているとき）特に **Galois 対応**（*Galois correspondence*）と呼ぶ．

PROPOSITION 1.3.17

Galois 対応は sup と inf を保つ．

Proof. X と Y を順序集合として，その間の Galois 対応 (f,g) を考える．X の（空かもしれない）部分集合 $Z \subset X$ を任意に取り $s = \sup Z$ が存在すると仮定したとき，$f(s) = \inf f(Z)$ であることを示す．$f(\inf Z) = \sup f(Z)$ についても同様に証明できる．

まず，各元 $z \in Z$ に対して $z \leqslant s$ だから $f(s) \leqslant f(z)$ である．そこで，ある元 $y \in Y$ が存在して，任意の元 $z \in Z$ に対して $y \leqslant f(z)$ となるとする．$y \leqslant f(s)$ を言えば良い．今，任意の元 $z \in Z$ に対して $y \leqslant f(z)$ であるから，両辺を g で写して $z \leqslant g(y)$ を得る．よって，sup の定義より $s \leqslant g(y)$ となる．この両辺を f で写せば，$y \leqslant f(s)$.

以上より，$f(s) = \inf f(Z)$ が分かった． □

(Gal, Fix) が Galois 対応であることが基本定理の骨子であり，それを示すのがこの小節の目的である．

PROPOSITION 1.3.18

(Gal, Fix) は Galois 接続である．

Proof. L/K を Galois 拡大とすれば，**LEMMA 1.3.4** より Gal と Fix はともに順序を反転させる写像である．随伴関係も，定義からただちに従う． □

THEOREM 1.3.19（Galois）

有限次 Galois 拡大 L/K に対して，$[L:K] = |\mathrm{Gal}(L/K)|$ が成り立つ．特に，Galois 群は有限群である．

Proof. 拡大次数 $n = [L:K]$ に関する帰納法で示す．$n = 1$ のときは $\mathrm{Gal}(L/K) = \{\mathrm{id}_L\}$ だから明らか．

[*19] ここで言う随伴とは，圏論における随伴のことである．すなわち，X と Y を圏と見て f と g を反変函手と見たとき，f が g の左随伴となっている．Galois 対応は随伴同値のことである．続く **PROPOSITION 1.3.17** もやはり，一般の随伴同値で成り立つ性質である．

$n>1$ として，$n-1$ までの主張を仮定する．元 $x\in L\setminus K$ を任意に取り，$p(X)$ をその最小多項式，$r=\deg p$ をその次数とする．このとき **Theorem 1.3.6** より $[K(x):K]=r$ であるから，**Proposition 1.3.4** を使えば $[L:K(x)]=s$ となる．ただし $s:=n/r$ と置いた．今，$r\geqslant 2$ であるから $s<n$ となり，帰納法の仮定が成り立つ：$|\mathrm{Gal}(L/K(x))|=s$．$\{\sigma_1,\dots,\sigma_s\}=\mathrm{Gal}(L/K(x))$ と置こう．

一方，$L/K(x)$ が正規拡大であるから $p(X)$ の根 $x_1,\dots,x_r\in L$ を持ち，それらに対応して K 自己同型 $\tau_1,\dots,\tau_r\in\mathrm{Gal}(L/K)$ が存在する（**Theorem 1.3.15**）．このそれぞれは $x^{\tau_j}=x_j$ を満たす．そこで $\theta_{i,j}:=\sigma_i\tau_j\in\mathrm{Gal}(L/K)$ と置けば，$\{\theta_{i,j}\}=\mathrm{Gal}(L/K)$ となる．実際，任意の K 自己同型 $\sigma\in\mathrm{Gal}(L/K)$ に対して，$p(x^\sigma)=(p(x))^\sigma=0$ であるから，ある $1\leqslant j\leqslant r$ が存在して $x^\sigma=x_j$ とできる．このとき

$$x^{\sigma\tau_j^{-1}}=x_j^{\tau_j^{-1}}=x$$

であるから，$\sigma\tau_j^{-1}\in\mathrm{Gal}(L/K)$ は x も固定する．よって $\sigma\tau_j^{-1}\in\mathrm{Gal}(L/K(x))$ となり，ある $1\leqslant i\leqslant s$ を用いて $\sigma\tau_j^{-1}=\sigma_i$ と書ける．従って $\sigma=\theta_{i,j}$ となるから，$\{\theta_{i,j}\}=\mathrm{Gal}(L/K)$.

残りは $|\{\theta_{i,j}\}|=n$ を示せば良い．もし $\theta_{i,j}=\theta_{k,\ell}$ ならば

$$x_j=x^{\tau_j}=x^{\sigma_i\tau_j}=x^{\sigma_k\tau_\ell}=x_\ell$$

となるから，$j=\ell$．また，このとき $\sigma_i=\theta_{i,j}\tau_j=\sigma_k$ となり，$i=k$．以上より，$|\{\theta_{i,j}\}|=n$ が分かった．　□

Theorem 1.3.20（Galois）

(Gal, Fix) は Galois 対応である．

Proof. **Proposition 1.3.18** より，(Gal, Fix) が互いに逆の全単射であることを確かめれば良い．そのためには，有限次 Galois 拡大 L/K に対して $\mathrm{Fix}(\mathrm{Gal}(L/K))\subset K$ と $\mathrm{Gal}(L/K)\subset\mathrm{Gal}(L/\mathrm{Fix}(\mathrm{Gal}(L/K)))$ を示せば良い[*20].

まず前半の包含を確かめる．元 $x\in\mathrm{Fix}(\mathrm{Gal}(L/K))$ と，それに（K 上）共役な元 $y\in L$ を任意に取る．L/K は正規拡大であるから，**Theorem 1.3.15** により，$x^\sigma=y$ なる K 自己同型 $\sigma\in\mathrm{Gal}(L/K)$ を得るが，$x\in\mathrm{Fix}(\mathrm{Gal}(L/K))$ であったから $x^\sigma=x$．従って x の最小多項式は 1 次式であり，$x\in K$ となる．

後半の包含を言うには，$[L:\mathrm{Fix}(G)]\leqslant|G|$ を示せば十分である．実際このとき，**Proposition 1.3.18 and Theorem 1.3.19** を組み合わせれば

$$|G|\leqslant|\mathrm{Gal}(L/\mathrm{Fix}(G))|=[L:\mathrm{Fix}(G)]\leqslant|G|$$

となるから，$|G|=|\mathrm{Gal}(L/\mathrm{Fix}(G))|$．さらに，Galois 群は有限群であるから $G=\mathrm{Gal}(L/\mathrm{Fix}(G))$ が分かる．

$n:=|G|$ と置き，$\mathrm{Fix}(G)$ 上線形独立な $n+1$ 個の元 $x_1,\dots,x_{n+1}\in L$ が存在したとする．$G=\{\sigma_1,\dots,\sigma_n\}$ と書いて行列

$$A=\begin{pmatrix}x_1^{\sigma_1}&\cdots&x_{n+1}^{\sigma_1}\\ \vdots&&\vdots\\ x_1^{\sigma_n}&\cdots&x_{n+1}^{\sigma_n}\end{pmatrix}\in\mathrm{Mat}(n\times(n+1),\mathrm{Fix}(G))$$

[*20] このとき $\mathrm{Fix}(\mathrm{Gal}(L/K))=K$ と $\mathrm{Gal}(L/K)=\mathrm{Gal}(L/\mathrm{Fix}(\mathrm{Gal}(L/K)))$ となる．これが任意の有限次 Galois 拡大で成り立つのだから，K を中間体 $L/M/K$ に置き換えても成り立つ．よって (Gal, Fix) が互いに逆となる．

を考える．この行列を線形写像 $L^{\oplus n+1} \to L^{\oplus n}$ と見て，その核 $\mathrm{Ker}\, A$ に含まれる 0 でないベクトルのうち，0 でない成分の数が最小のものを選ぶ．適当に基底の順番を入れ替えることにより，このベクトルを $\alpha = (\alpha_1, \ldots, \alpha_r, 0, \ldots, 0)$ としても一般性を失わない．ただし各 $1 \leqslant i \leqslant r$ について $\alpha_i \neq 0$. □

References

[1] F. borceux and G. Janelidze. *Galois Theories*. Cambridge University Press, 2001.

[2] H. Kurzweil and B. Stellmacher. *The Theory of Finite Groups - An Introduction*. Springer, 2004.

[3] 永田雅宜. 可換体論（新板）. 褰華房, 1985.

[4] 桂利行. 代数学 III 体とガロア理論. 東京大学出版会, 2005.