Galoisの基本定理の多角的な証明とその完全な解説

本稿では、体論における中心的な里程標である**Galoisの基本定理 (fundamental theorem of Galois theory)**について、現代代数学の標準的なアプローチから幾何学的・圏論的な視点、あるいは歴史的な原点に至るまでの5つの異なる証明法・アプローチを包括的、かつ完全に厳密なステップで解説する。いかなる論理の飛躍や要約をも排除し、各証明を自己完結的に記述した。

1. 基礎概念の定義

定義 1.1 (体拡大と拡大次数)

体 L がその部分集合として体 K を含むとき、対 L/K を**体拡大 (field extension)**と呼ぶ。このとき L は K 上のベクトル空間とみなすことができる。そのベクトル空間としての次元を L/K の**拡大次数 (extension degree)**と呼び、$[L:K]$ で表す。$[L:K]$ が有限であるとき、L/K を**有限次拡大 (finite extension)**という。

定義 1.2 (分離拡大と正規拡大)

L/K を代数拡大とする。

1. L の任意の元 α の K 上の最小多項式が重根を持たないとき、L/K を**分離拡大 (separable extension)**という。
2. $K[x]$ の任意の既約多項式が L に少なくとも1つの根を持つならば、その多項式が L においてすべての根に（一次式の積として）完全に分解するとき、L/K を**正規拡大 (normal extension)**という。

定義 1.3 (Galois拡大とGalois群)

体拡大 L/K が分離拡大かつ正規拡大であるとき、これを**Galois拡大 (Galois extension)**という。このとき、L から L への自己同型写像であって K の各元を動かさないもの（K 自己同型）全体の集合は写像の合成を演算として群をなす。これを L/K の**Galois群 (Galois group)**と呼び、$\mathrm{Gal}(L/K)$ で表す。

定義 1.4 (不変体)

L を体とし、G を L の自己同型群の部分群とする。このとき、G のすべての元によって固定される L の元全体の集合

$$L^G = \{x \in L \mid \forall \sigma \in G, \sigma(x) = x\}$$

は L の部分体となる。これを G の**不変体 (fixed field)**と呼ぶ。

2. 理解を助けるための具体例

例 2.1 ($\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ のGalois対応)

有理数体 $\mathbb{Q}$ に対し、$\sqrt{2}$ と $\sqrt{3}$ を添加した体 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ を考える。この拡大は $K = \mathbb{Q}$ 上の多項式 $f(x) = (x^2-2)(x^2-3)$ の最小分解体であり、有限次Galois拡大である。拡大次数は $[L:K] = 4$ である。

この拡大のGalois群 $G = \mathrm{Gal}(L/K)$ は、以下の4つの写像からなる位数4の群（クラインの四元群 $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$）となる。

- $\mathrm{id} : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto \sqrt{3}$ （恒等写像）
- $\sigma_1 : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3}$
- $\sigma_2 : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}$
- $\sigma_3 : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}$

群 G のすべての非自明な部分群と、対応する不変体（中間体）の関係は以下の通りである。

- 部分群 $H_1 = \{\mathrm{id}, \sigma_1\}$ の不変体は $L^{H_1} = \mathbb{Q}(\sqrt{3})$ であり、$[L : \mathbb{Q}(\sqrt{3})] = 2 = |H_1|$。
- 部分群 $H_2 = \{\mathrm{id}, \sigma_2\}$ の不変体は $L^{H_2} = \mathbb{Q}(\sqrt{2})$ であり、$[L : \mathbb{Q}(\sqrt{2})] = 2 = |H_2|$。
- 部分群 $H_3 = \{\mathrm{id}, \sigma_3\}$ の不変体は $L^{H_3} = \mathbb{Q}(\sqrt{6})$ であり、$[L : \mathbb{Q}(\sqrt{6})] = 2 = |H_3|$。

部分群の包含関係と中間体の包含関係が完全に反転して1対1に対応していることがわかる。

3. Galoisの基本定理の主張

定理 3.1 (Galoisの基本定理)

L/K を有限次Galois拡大とし、$G = \mathrm{Gal}(L/K)$ とする。このとき、以下の中間体全体の集合 $\mathcal{M}$ と部分群全体の集合 $\mathcal{H}$ の間に、包含関係を反転させる全単射が存在する。

$$\mathcal{M} = \{M \mid K \subset M \subset L\}$$
$$\mathcal{H} = \{H \mid H \text{ は } G \text{ の部分群}\}$$

対応は写像 $\Phi : M \mapsto \mathrm{Gal}(L/M)$ および $\Psi : H \mapsto L^H$ によって与えられ、互いに逆写像である。さらに、以下が成り立つ。

1. 拡大次数と群の位数の間には $[L : M] = |\mathrm{Gal}(L/M)|$ および $[M : K] = [G : \mathrm{Gal}(L/M)]$ が成り立つ。
2. 中間体 M が K 上の正規拡大であることと、対応する部分群 $H = \mathrm{Gal}(L/M)$ が G の正規部分群 ($H \triangleleft G$) であることは同値である。このとき、自然な群同型 $\mathrm{Gal}(M/K) \cong G/H$ が成立する。

4. 第1のアプローチ：Artinによる線形代数的証明

補題 4.1 (Dedekindの補題)

体 L から体 Ω への相異なる体準同型写像 $\sigma_1, \sigma_2, \ldots, \sigma_n$ は、Ω 上線形独立である。すなわち、$c_1\sigma_1 + c_2\sigma_2 + \cdots + c_n\sigma_n = 0$ ($c_i \in \Omega$) ならば、すべての $c_i = 0$ である。

証明1（古典的な帰納法による証明）

n に関する数学的帰納法で示す。
$n = 1$ のとき、σ_1 は体準同型であるから $\sigma_1(1) = 1 \neq 0$。よって $c_1\sigma_1(x) = 0\,(\forall x \in L)$ ならば $x = 1$ を代入して
$c_1 \cdot 1 = 0 \implies c_1 = 0$ となり成立する。
$n - 1$ まで成立すると仮定する。いま、自明でない線形従属の関係式が存在すると仮定し、その中で非零である係数の個数が最小であるものを

$$c_1\sigma_1 + c_2\sigma_2 + \cdots + c_n\sigma_n = 0 \quad (\forall x \in L, \text{すべての } c_i \neq 0) \quad \cdots (*)$$

とする。$\sigma_1 \neq \sigma_n$ であるから、ある $\alpha \in L$ が存在して $\sigma_1(\alpha) \neq \sigma_n(\alpha)$ となる。 任意の $x \in L$ に対して、$(*)$ に αx を代入する

と、$\sigma_i(\alpha x) = \sigma_i(\alpha)\sigma_i(x)$ より、

$$c_1\sigma_1(\alpha)\sigma_1(x) + c_2\sigma_2(\alpha)\sigma_2(x) + \cdots + c_n\sigma_n(\alpha)\sigma_n(x) = 0 \quad \cdots (**)$$

を得る。一方で、元の関係式 $(*)$ の全体に $\sigma_n(\alpha)$ を乗じると、

$$c_1\sigma_n(\alpha)\sigma_1(x) + c_2\sigma_n(\alpha)\sigma_2(x) + \cdots + c_n\sigma_n(\alpha)\sigma_n(x) = 0 \quad \cdots (***)$$

となる。$(**)$ から $(***)$ を引くと、第 n 項が完全に相殺され、次の式を得る。

$$\sum_{i=1}^{n-1} c_i(\sigma_i(\alpha) - \sigma_n(\alpha))\sigma_i(x) = 0$$

帰納法の仮定より $\sigma_1, \ldots, \sigma_{n-1}$ は線形独立であるから、すべての係数は 0 でなければならない。特に第1項に注目すると、

$$c_1(\sigma_1(\alpha) - \sigma_n(\alpha)) = 0$$

でなければならない。しかし、仮定より $c_1 \neq 0$ かつ $\sigma_1(\alpha) - \sigma_n(\alpha) \neq 0$ であるため、これは矛盾である。したがって、相異なる体準同型は線形独立である。

【視点の転換：固有空間とLagrange補間型の射影作用素としての解釈】
帰納法による古典的な証明はやや技巧的であるが、本質的には線形代数における**「相異なる固有値に対応する固有ベクトルは線形独立である」**という事実と、**Lagrange補間**のアイデアに帰着する。体準同型を「積作用に対する固有ベクトル」と見なし、特定の準同型のみを抽出する線形変換（射影作用素）を構成することで、極めて見通しの良いエレガントな証明が可能となる。

補題 L (固有ベクトルとLagrange補間型の作用素)

Ω を体、V を Ω 上のベクトル空間とし、$v_1, \ldots, v_n \in V \setminus \{0\}$ とする。これらが張る部分空間を $W = \sum_{i=1}^{n} \Omega v_i$ とおく。
任意の相異なる添字 $k \neq l$ に対し、W 上の一次変換 T_{kl} が存在し、各 v_i が固有値 $\lambda_i^{k,l} \in \Omega$ を持つ固有ベクトル（すなわち $T_{kl}v_i = \lambda_i^{k,l}v_i$）であり、かつ $\lambda_k^{k,l} \neq \lambda_l^{k,l}$ を満たすとする。
このとき、$v_1, \ldots, v_n$ は Ω 上一次独立である。

補題 L の証明

各 $k \in \{1, \ldots, n\}$ に対し、W 上の一次変換 L_k を、Lagrange補間に用いる多項式に倣って次のように定める。

$$L_k = \prod_{l \neq k} \frac{T_{kl} - \lambda_l^{k,l}\mathrm{id}_W}{\lambda_k^{k,l} - \lambda_l^{k,l}}$$

この一次変換 L_k を各 v_m に作用させた結果を考える。
$m \neq k$ の場合、上の積の因子の中には必ず $l = m$ に対応する項 $\frac{T_{km} - \lambda_m^{k,m}\mathrm{id}_W}{\lambda_k^{k,m} - \lambda_m^{k,m}}$ が含まれる。v_m は T_{km} の固有値 $\lambda_m^{k,m}$ の固有ベクトルであるため、この因子が v_m を 0 に写す。したがって $L_k v_m = 0$ となる。
一方、$m = k$ の場合、すべての $l \neq k$ について $T_{kl}v_k = \lambda_k^{k,l}v_k$ であるため、各因子は $\frac{\lambda_k^{k,l} - \lambda_l^{k,l}}{\lambda_k^{k,l} - \lambda_l^{k,l}}v_k = v_k$ となり、結果として $L_k v_k = v_k$ となる。
すなわち、クロネッカーのデルタを用いて $L_k v_m = \delta_{km} v_k$ が成り立つ。

いま、一次関係式 $\sum_{i=1}^{n} c_i v_i = 0$ $(c_i \in \Omega)$ があるとする。両辺に L_k を作用させると、

$$L_k\left(\sum_{i=1}^{n} c_i v_i\right) = \sum_{i=1}^{n} c_i L_k v_i = c_k v_k = 0$$

$v_k \neq 0$ であるから $c_k = 0$ が得られる。これがすべての k について成り立つため、$v_1, \ldots, v_n$ は一次独立である。

証明2（補題 L を用いたDedekindの補題の証明）

相異なる体準同型 $\sigma_1, \ldots, \sigma_n \in \mathrm{Map}(L, \Omega)$ に対し、$v_i = \sigma_i$ とし、それらが張る Ω 上のベクトル空間を $W = \sum_{i=1}^{n} \Omega\sigma_i$ とする。
$k \neq l$ となる任意の組に対して、$\sigma_k \neq \sigma_l$ であるから、ある $\alpha_{kl} \in L$ が存在して $\sigma_k(\alpha_{kl}) \neq \sigma_l(\alpha_{kl})$ となる。
ここで、W 上の一次変換 T_{kl} を次のように定める。

$$T_{kl} : \sigma_i \mapsto (x \mapsto \sigma_i(\alpha_{kl}x) = \sigma_i(\alpha_{kl})\sigma_i(x)) = \sigma_i(\alpha_{kl})\sigma_i$$

この定義より、$T_{kl}\sigma_i = \sigma_i(\alpha_{kl})\sigma_i$ が成り立つ。すなわち、各 $v_i = \sigma_i$ は T_{kl} の固有ベクトルであり、その固有値は $\lambda_i^{k,l} = \sigma_i(\alpha_{kl})$ である。
α_{kl} の選び方から、

$$\lambda_k^{k,l} = \sigma_k(\alpha_{kl}) \neq \sigma_l(\alpha_{kl}) = \lambda_l^{k,l}$$

を満たす。これはまさに上述の補題 L の条件を完全に満たしている。
したがって、補題 L を適用することにより、$\sigma_1, \ldots, \sigma_n$ は一次独立であることが直ちに結論づけられる。

補題 4.2 (Artinの定理)

$G = \{\sigma_1, \ldots, \sigma_n\}$ を体 L の有限自己同型群とし、$K = L^G$ をその不変体とする。このとき、L/K は有限次拡大であり、拡大次数は $[L : K] = n$ である。

証明

$[L : K] \geq n$ および $[L : K] \leq n$ の双方を厳密に示す。

1. $[L : K] \geq n$ の証明：
$[L : K] = m < n$ と仮定して矛盾を導く。L/K の K 上のベクトル空間としての基底を $\omega_1, \ldots, \omega_m$ とする。ここで、未知数 $x_1, \ldots, x_n \in L$ に関する m 本の連立一次方程式系

$$\sum_{i=1}^{n} x_i\sigma_i(\omega_j) = 0 \quad (j = 1, \ldots, m)$$

を考える。方程式の数 m よりも未知数の数 n の方が大きいため、線形代数学の基本定理により、この方程式系はすべてが 0 ではない非自明な解 $x_1, \ldots, x_n \in L$ を必ず持つ。 任意の元 $\alpha \in L$ は基底の線形結合として $\alpha = \sum_{j=1}^{m} d_j\omega_j$ $(d_j \in K)$ と表される。各 σ_i は $K = L^G$ の元を固定するため $\sigma_i(d_j) = d_j$ である。これを用いると、

$$\sum_{i=1}^{n} x_i\sigma_i(\alpha) = \sum_{i=1}^{n} x_i\sigma_i\left(\sum_{j=1}^{m} d_j\omega_j\right) = \sum_{j=1}^{m} d_j\left(\sum_{i=1}^{n} x_i\sigma_i(\omega_j)\right) = \sum_{j=1}^{m} d_j \cdot 0 = 0$$

が任意の $\alpha \in L$ で成立する。これは相異なる自己同型群の元 $\sigma_1, \ldots, \sigma_n$ が L 上で線形従属であることを意味し、Dedekindの補題に真っ向から矛盾する。したがって $[L : K] \geq n$ である。

2. $[L : K] \leq n$ の証明：
$[L : K] > n$ と仮定し、矛盾を導く。L 内に K 上線形独立な $n+1$ 個の元 $\alpha_1, \ldots, \alpha_{n+1}$ を取る。未知数 $y_1, \ldots, y_{n+1} \in L$ に関する n 本の連立一次方程式系

$$\sum_{j=1}^{n+1} y_j\sigma_i(\alpha_j) = 0 \quad (i = 1, \ldots, n)$$

を考える。方程式の数 n よりも未知数の数 $n+1$ の方が大きいため、非自明な解 $y_1, \ldots, y_{n+1} \in L$ が存在する。このような非自明な解の中で、**非零成分の個数が最小**であるものを選択する。その最小非零解を $y_1, \ldots, y_r, 0, \ldots, 0$ （ただし $y_1 \ldots y_r \neq 0$）とする。
全体を y_1 で割ることにより、 $y_1 = 1$ と正規化してよい。このときの方程式系は以下である。

$$\sigma_i(\alpha_1) + \sum_{j=2}^{r} y_j \sigma_i(\alpha_j) = 0 \quad (i = 1, \dots, n) \quad \cdots (\dagger)$$

群 G は恒等写像 $\mathrm{id} = \sigma_1$ を含む。$i = 1$ に対応する式は $\alpha_1 + \sum_{j=2}^{r} y_j \alpha_j = 0$ となる。もしすべての y_j が $K = L^G$ に属するのであれば、これは $\alpha_1, \dots, \alpha_r$ が K 上線形従属であることを意味し、選び方に矛盾する。したがって、少なくとも1つの成分（例えば y_2）は K に属さない。
$y_2 \notin L^G$ より、ある $\tau \in G$ が存在して $\tau(y_2) \neq y_2$ となる。方程式系 $(\dagger)$ の全体に τ を作用させると、

$$\tau(\sigma_i(\alpha_1)) + \sum_{j=2}^{r} \tau(y_j) \tau(\sigma_i(\alpha_j)) = 0 \quad (i = 1, \dots, n)$$

となる。写像の合成 $\tau\sigma_i$ は、 i が 1 から n まで動くとき、群の閉包性と全単射性から、元の群 $G = \{\sigma_1, \dots, \sigma_n\}$ の元を単に並び替えたものになる。したがって、上の方程式系は次のように書き直せる。

$$\sigma_i(\alpha_1) + \sum_{j=2}^{r} \tau(y_j) \sigma_i(\alpha_j) = 0 \quad (i = 1, \dots, n) \quad \cdots (\dagger\dagger)$$

$(\dagger)$ から $(\dagger\dagger)$ を引き算すると、第1項の $\sigma_i(\alpha_1)$ が消去され、

$$\sum_{j=2}^{r} (y_j - \tau(y_j)) \sigma_i(\alpha_j) = 0 \quad (i = 1, \dots, n)$$

を得る。この新しい方程式系の解の各成分を $z_j = y_j - \tau(y_j)$ と置く。$j = 2$ の成分は $z_2 = y_2 - \tau(y_2) \neq 0$ より、この解は非自明（すべてが 0 ではない）である。しかし、この解において非零になり得る成分は高々 $j = 2$ から r までの $r - 1$ 個であり、元の最小解の非零個数 r よりも確実に少ない。これは元の解の非零成分最小性に矛盾する。したがって $[L : K] \leq n$ である。両側不等式より $[L : K] = n$ が確定する。

【証明の背後にある本質1：$[L : K] \geq n$ と線形写像空間の次元】
前半の $[L : K] \geq n$ の証明において、「未知数と方程式の数を比較して背理法で矛盾を導く」という標準的な論法は、実は**「線形写像の空間の次元」**という代数的な構造を成分計算で表現したものである。連立方程式の技巧を排し、よりスッキリと本質を突いた視点は以下の通りである。

ステップ1：自己同型を「K-線形写像」として捉え直す
群 $G = \{\sigma_1, \dots, \sigma_n\}$ の各元は不変体 K の元を動かさないため、任意の $c \in K$ と $x \in L$ に対して $\sigma_i(cx) = c\sigma_i(x)$ が成り立つ。これは、σ_i たちが「L から L への K-線形写像」であることを意味する。

ステップ2：「K-線形写像全体の空間」の大きさを測る
L から L への K-線形写像全体の集合 $\mathrm{End}_K(L)$ は、写像の和と L の元によるスカラー倍により、L **上のベクトル空間**となる。
$[L : K] = m$（有限次元）と仮定すると、L の m 個の K-基底の行き先を L 内から自由に選ぶことで任意の写像が決定されるため、この空間の次元は $\dim_L(\mathrm{End}_K(L)) = m = [L : K]$ となる。

ステップ3：Dedekindの補題による次元の比較
n 個の自己同型 $\sigma_1, \dots, \sigma_n$ は $\mathrm{End}_K(L)$ の元であり、Dedekindの補題によりこれらは L 上一次独立である。線形代数の基本定理「一次独立なベクトルの最大数は、その空間の次元を超えない」より、ただちに

$$n \leq \dim_L(\mathrm{End}_K(L)) = [L : K]$$

が導かれる。このように、「独立なものが n 個あるなら、それが入っている空間の次元は n 以上でなければならない」という極めて透明な論理に帰着する。

【証明の背後にある本質2：$[L : K] \leq n$ とトレースによるガロア降下 (Galois Descent)】
上記の $[L : K] \leq n$ を示す後半の証明において、「非零成分が最小の解を取り、自己同型を作用させて引き算し、より小さい解を作って矛盾を導く」という論法は、線形代数における標準的かつ強力な技巧である。しかし、なぜそのような操作が成立するのか、その代数的な動機が見えづらい側面もある。

実は、Artinの定理の真の本質は、**「大きな体 L の世界で見つけた連立方程式の解を、群の作用に対する平均化（トレース）を用いて、基礎体**

K の世界に引きずり下ろすことができる」という**「ガロア降下」**の構造にある。技巧的な引き算を排除し、Dedekindの補題の威力を正面から使った、より本質的で直感的な証明のストーリーは以下の通りである。

ステップ1：L の世界における解空間の構築
$[L:K] > n$ と仮定し、K 上一次独立な $n+1$ 個の元 $\omega_1, \ldots, \omega_{n+1} \in L$ を取る。未知数 $x_1, \ldots, x_{n+1} \in L$ についての n 本の連立方程式系

$$\sum_{j=1}^{n+1} x_j \sigma_i(\omega_j) = 0 \quad (i = 1, \ldots, n)$$

を考える。方程式の数 n より未知数の数 $n+1$ の方が多いため、すべてが 0 ではない非自明な解 $x = (x_1, \ldots, x_{n+1}) \in L^{n+1}$ が存在する。このような解全体の集合（解空間）を V とする。V は L 上のベクトル空間である。

ステップ2：解空間 V の G-対称性
解 $x \in V$ に対して、任意の自己同型 $\tau \in G$ を各成分に作用させたベクトル $\tau(x) = (\tau(x_1), \ldots, \tau(x_{n+1}))$ を考える。元の方程式全体に τ を作用させると、

$$\sum_{j=1}^{n+1} \tau(x_j)(\tau\sigma_i)(\omega_j) = 0$$

となる。ここで i が 1 から n まで動くとき、写像の合成 $\tau\sigma_i$ は群 G の閉包性と全単射性により、元の群の元を単に並び替えているだけである。つまり、この新しい n 本の方程式のセットは「元の方程式の順番を入れ替えただけ」のものに過ぎない。したがって、$\tau(x)$ もまた同じ方程式系を完全に満たし、$\tau(x) \in V$ となる。すなわち、解空間 V は群 G の作用に関して閉じている。

ステップ3：トレース写像による K への降下
ここで、L の元の組である解 $x \in V$ を使って、K の元だけからなる解を構成したいと考える。そのための最も自然な代数的操作が、すべての $\tau \in G$ による軌道を足し合わせる**トレース (Trace)** である。

$$T(x) = \sum_{\tau \in G} \tau(x)$$

この $T(x)$ にさらに任意の自己同型 $\rho \in G$ を作用させると、和の順序が入れ替わるだけで $\rho(T(x)) = T(x)$ となる。すなわち、$T(x)$ の各成分は G のすべての元の作用で不変であるから、定義より $T(x)$ **は不変体 K の元だけからなるベクトル（$T(x) \in K^{n+1}$）**である。しかも、ステップ2より V の元への τ の作用は再び V の元を生み、ベクトル空間 V は足し算で閉じているため、$T(x)$ は依然として解である（$T(x) \in V$）。

ステップ4：Dedekindの補題による「トレース非退化性」の保証
唯一の問題は、「どんな解 x を持ってきても、和をとる過程で打ち消し合いが起こり、トレース $T(x)$ がすべて 0 ベクトルに潰れてしまうのではないか」という懸念である。ここで Dedekindの補題 が決定的役割を果たす。
V から任意の非零ベクトル v を一つ取る。ある成分 v_k は 0 ではない。V は L **上のベクトル空間**であるから、任意の $c \in L$ に対してスカラー倍 cv もまた V の解になる。もし、すべての $c \in L$ に対して $T(cv) = 0$ になってしまうと仮定する。その k 番目の成分に注目すると、

$$\sum_{\tau \in G} \tau(cv_k) = 0 \implies \sum_{\tau \in G} \tau(v_k)\tau(c) = 0 \quad (\text{すべての } c \in L \text{ について})$$

が成り立つ。これはまさに、相異なる体準同型 τ 達が、L の元 $\tau(v_k)$ を係数として恒等的に線形従属であるという関係式に他ならない。しかし、**Dedekindの補題により相異なる体準同型は一次独立**であるため、すべての係数は 0 でなければならない。特に $\tau = \mathrm{id}$ に対応する係数 $\mathrm{id}(v_k) = v_k$ も 0 となるが、これは $v_k \neq 0$ であったことに完全に矛盾する。したがって、ある $c \in L$ が存在して、$y = T(cv)$ は**すべてが 0 ではない K の元からなる解（$y \in V \cap K^{n+1} \setminus \{0\}$）**となる。

ステップ5：矛盾の結実
この K の元からなる非自明な解 y を元の方程式に代入する。群 G の元には恒等写像 $\sigma_1 = \mathrm{id}$ が含まれているため、$i = 1$ の式に注目すると、

$$\sum_{j=1}^{n+1} y_j \omega_j = 0$$

となる。y_j はすべて K に属し、かつすべてが 0 ではないため、これは $\omega_1, \ldots, \omega_{n+1}$ が K 上一次従属であることを意味する。これは最初の「K 上一次独立に取った」という前提に真っ向から矛盾する。ゆえに $[L:K] \leq n$ が成立しなければならない。

【証明の背後にある本質3：接合環 $L[G]$ と代数同型を用いた完全な証明】
これまでの次元比較やトレースの議論は、非可換環論における「接合環（歪群環）」の同型定理として完全に統合される。群 G を基底とする L 上のベクトル空間に対し、積を $(a\sigma)(b\tau) = a\sigma(b)\sigma\tau \quad (a, b \in L, \sigma, \tau \in G)$ と定義した、L 上の 1 を持つ結合代数を**接合環** $L[G]$ とする。

このとき、自然な写像 $\Phi : L[G] \to \mathrm{End}_K(L)$ を

$$\Phi\left(\sum_{\sigma \in G} a_\sigma \sigma\right)(x) = \sum_{\sigma \in G} a_\sigma \sigma(x) \quad (x \in L)$$

と定める。この Φ が L **上の代数同型写像** になることを以下の3ステップで証明する。

ステップ1：Φ が代数準同型であることの直接証明
Φ が L-線形であること、および単位元を保存すること（$\Phi(1 \cdot \mathrm{id}_G) = \mathrm{id}_L$）は定義より明らかである。積の保存については、基底元 $a\sigma$ と $b\tau$ に対して、 $L[G]$ 内部で積をとってから Φ で写すと：

$$\Phi((a\sigma)(b\tau))(x) = \Phi(a\sigma(b)\sigma\tau)(x) = a\sigma(b)\sigma(\tau(x))$$

それぞれを Φ で写してから $\mathrm{End}_K(L)$ 内で合成（積）すると：

$$(\Phi(a\sigma) \circ \Phi(b\tau))(x) = \Phi(a\sigma)(b\tau(x)) = a\sigma(b\tau(x)) = a\sigma(b)\sigma(\tau(x))$$

両者が完全に一致するため、Φ は L 上の代数準同型である。

ステップ2：Dedekindの補題による単射性の証明
ある元 $\sum_{\sigma \in G} a_\sigma \sigma \in \mathrm{Ker}(\Phi)$ が存在すると仮定する。これは任意の $x \in L$ に対して $\sum_{\sigma \in G} a_\sigma \sigma(x) = 0$ であることを意味する。写像としての線形結合 $\sum_{\sigma \in G} a_\sigma \sigma = 0$ であり、Dedekindの補題より相異なる自己同型 σ たちは L 上一次独立であるため、すべての係数は $a_\sigma = 0$ でなければならない。したがって $\mathrm{Ker}(\Phi) = \{0\}$ となり、Φ は単射である。

ステップ3：トレース写像を使う全射性の証明
写像 $\mathrm{Tr}(x) = \sum_{\sigma \in G} \sigma(x)$ は像が不変体 K に属し、Dedekindの補題より零写像ではないため、ある $\theta \in L$ が存在して $\mathrm{Tr}(\theta) = 1$ とできる。 任意の K-線形写像 $f \in \mathrm{End}_K(L)$ に対し、f の K-線形性とトレースの性質を駆使して整理すると、任意の $x \in L$ に対して次の関係式（トレースを用いた全射性の核となる等式）が成り立つ。

$$f(x) = \sum_{\sigma \in G} f(\sigma(\theta))\sigma^{-1}(x)$$

ここで、$\alpha = \sum_{\sigma \in G} f(\sigma(\theta))\sigma^{-1} \in L[G]$ という元を構成すると、各係数 $f(\sigma(\theta))$ は L の元であるため α は正しく定義されており、上の等式はまさに $\Phi(\alpha)(x) = f(x)$ を意味する。すなわち $\Phi(\alpha) = f$ となり、Φ は全射である。

結論：
以上より Φ は L 上の代数同型である。これに伴い、両辺の L-ベクトル空間としての次元は完全に一致しなければならない。定義域 $L[G]$ の次元は $|G| = n$、値域 $\mathrm{End}_K(L)$ の次元は $[L : K]$ であるから、ただちに $[L : K] = n$ が証明される。これがArtinの定理の最も洗練された代数的帰結である。

定理 3.1（Galoisの基本定理）のArtinによる完全証明

1. 写像の反転全単射性 ($\Phi \circ \Psi = \mathrm{id}$, $\Psi \circ \Phi = \mathrm{id}$) の証明:
任意の群の部分群 $H \subset G$ を取る。その不変体 L^H に対し、不変体拡大 L/L^H を考える。補題4.2（Artinの定理）を有限群 H と体 L に適用すると、$[L : L^H] = |H|$ である。 一方、定義から明らかに $H \subset \mathrm{Gal}(L/L^H)$ である。 $\mathrm{Gal}(L/L^H)$ もまた L の有限自己同型群であり、その不変体は定義からまさに L^H である。したがって、再度補題4.2を適用すると $[L : L^H] = |\mathrm{Gal}(L/L^H)|$ を得る。よって $|H| = |\mathrm{Gal}(L/L^H)|$ となり、包含関係 $H \subset \mathrm{Gal}(L/L^H)$ と位数の有限性から $H = \mathrm{Gal}(L/L^H)$ が成立する。すなわち $\Phi(\Psi(H)) = H$ である。
次に、任意の中間体 $M \in \mathcal{M}$ を取る。L/K は有限次Galois拡大であるから、ある K 上の分離既約多項式の最小分解体である。ゆえに L/M もまた最小分解体であり、分離性と正規性を引き継ぐためGalois拡大である。したがって、補題4.2より $[L : M] = |\mathrm{Gal}(L/M)|$ が成り立つ。$\mathrm{Gal}(L/M)$ の定義による不変体 $L^{\mathrm{Gal}(L/M)}$ を考えると、明らかに $M \subset L^{\mathrm{Gal}(L/M)}$ である。ここで補題4.2を群 $\mathrm{Gal}(L/M)$ に適用すると、$[L : L^{\mathrm{Gal}(L/M)}] = |\mathrm{Gal}(L/M)|$ となる。これらから

$$[L:M] = [L:L^{\mathrm{Gal}(L/M)}]$$

が得られ、包含関係 $M \subset L^{\mathrm{Gal}(L/M)}$ と次数の有限性から $M = L^{\mathrm{Gal}(L/M)}$ が成立する。すなわち $\Psi(\Phi(M)) = M$ である。以上より、Φ と Ψ は互いに逆写像であり、包含関係を反転させる全単射であることが証明された。

2. 次数の等式と正規部分群の同値性の証明:
塔の定理 $[L:K] = [L:M][M:K]$ および不変体の次数関係から、$[L:M] = |\mathrm{Gal}(L/M)|$。また、
$[M:K] = [L:K]/[L:M] = |G|/|\mathrm{Gal}(L/M)| = [G:\mathrm{Gal}(L/M)]$ となり、次数の関係式が従う。
任意の $\sigma \in G$ に対して、$\mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ が成り立つ。なぜなら、
$\tau \in \mathrm{Gal}(L/\sigma(M)) \iff \forall x \in M, \tau(\sigma(x)) = \sigma(x) \iff \forall x \in M, (\sigma^{-1}\tau\sigma)(x) = x \iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M) \iff \tau \in \sigma\mathrm{Gal}(L/M$
であるからである。
中間体 M が K 上正規拡大であることの定義は、任意の埋め込み（すなわち G の元 σ）に対して $\sigma(M) = M$ が成り立つことである。上記の等式から、これは $\mathrm{Gal}(L/M) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ がすべての $\sigma \in G$ で成り立つこと、すなわち $\mathrm{Gal}(L/M) \triangleleft G$ と完全に同値である。このとき、制限準同型写像 $\psi : G \to \mathrm{Gal}(M/K)\ (\sigma \mapsto \sigma|_M)$ を考える。その核は
$\ker(\psi) = \{\sigma \in G \mid \forall x \in M, \sigma(x) = x\} = \mathrm{Gal}(L/M)$ である。また、体の埋め込みの延長定理から ψ は全射である。したがって、群の準同型定理より $G/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$ が得られる。

5. 第2のアプローチ：原始元定理を用いる古典的証明

> **命題 5.1 (原始元定理)**
>
> L/K を有限次分離拡大とする。このとき、ある元 $\theta \in L$ が存在して、$L = K(\theta)$ と表すことができる。

証明

K が有限体である場合、L も有限体となる。有限体の乗法群 $L^\times$ は巡回群であることが代数学の基本定理（有限体の乗法群の有限部分群は巡回群）から知られている。その巡回群の生成元を θ とすれば、当然 $L^\times = \langle\theta\rangle$ となり、$L = K(\theta)$ が成立する。
以下、K は無限体とする。有限次拡大は有限個の元の添加で表せるため、数学的帰納法により、2つの元の添加 $L = K(\alpha, \beta)$ の場合に定理を示せば十分である。 α, β の K 上の最小多項式をそれぞれ $f(x), g(x) \in K[x]$ とする。L を含む拡大体において、$f(x)$ の相異なるすべての根を $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ とし、$g(x)$ の相異なるすべての根を $\beta = \beta_1, \beta_2, \ldots, \beta_m$ とする（分離性より重根は存在しない）。
K は無限体であるため、次の有限個の一次方程式の解とはならない元 $c \in K$ を選択することが可能である。

$$\alpha_i + c\beta_j = \alpha_1 + c\beta_1 \quad (j \neq 1) \implies c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$$

このような $c \in K$ を1つ固定し、$\theta = \alpha + c\beta$ と置く。明らかに $K(\theta) \subset K(\alpha, \beta)$ である。 逆の包含関係を示すために、$\beta \in K(\theta)$ であることを証明する。
$K(\theta)[x]$ 内の多項式 $h(x) = f(\theta - cx)$ を考える。このとき、

$$h(\beta) = f(\theta - c\beta) = f(\alpha) = 0$$

であり、かつ $g(\beta) = 0$ である。すなわち、β は $h(x)$ と $g(x)$ の共通根である。 もし β 以外の $g(x)$ の根 $\beta_j\ (j \neq 1)$ が $h(x)$ の根でもあると仮定すると、$h(\beta_j) = f(\theta - c\beta_j) = 0$ となり、ある添字 i に対して $\theta - c\beta_j = \alpha_i$ が成り立たねばならない。式を変形すると $\alpha + c\beta - c\beta_j = \alpha_i \implies \alpha_1 + c\beta_1 = \alpha_i + c\beta_j$ となるが、これは c の選び方に完全に矛盾する。
したがって、代数的閉包内において $h(x)$ と $g(x)$ が持つ共通根は $x = \beta$ ただ1つである。 ゆえに、$K(\theta)[x]$ における多項式としての最大公約元は $\gcd(h(x), g(x)) = x - \beta$ となる。多項式の最大公約元を求めるユークリッドの互除法は、係数体 $K(\theta)$ の内部の四則演算だけで完全に完結する。したがって、その結果得られる多項式 $x - \beta$ の係数は $K(\theta)$ に属していなければならない。 これより $\beta \in K(\theta)$ が従う。$\beta \in K(\theta)$ であれば、 $\alpha = \theta - c\beta \in K(\theta)$ も成り立ち、 $K(\alpha, \beta) = K(\theta)$ が完全に示された。

基本定理の古典的証明

L/K を有限次Galois拡大とし、M を任意の中間体とする。L/K が分離拡大であるから、その部分拡大 L/M も分離拡大である。原始元定理より、ある $\theta \in L$ が存在して $L = M(\theta)$ と表せる。θ の M 上の最小多項式を $f_M(x) \in M[x]$ とする。
L/K は正規拡大であるから、$\theta \in L$ の K 上の最小多項式、ひいては M 上の最小多項式 $f_M(x)$ は、L 内においてすべての根に完全に分解する。$f_M(x)$ の相異なる根を $\theta = \theta_1, \theta_2, \ldots, \theta_r$ とする（分離性より次数は $r = [L:M]$ である）。 任意の自己同型 $\sigma \in \mathrm{Gal}(L/M)$ は M の元を固定するため、 $0 = \sigma(f_M(\theta)) = f_M(\sigma(\theta))$ となり、$\sigma(\theta)$ は必ず集合 $\{\theta_1, \ldots, \theta_r\}$ のいずれかの元に写る。 $L = M(\theta)$ であるから、自己同型写像 σ は原始元 θ の行き先のみによって完全に決定され、かつその行き先は r 個の根のいずれかでなければならない。また、体の埋め込みの同型延長定理より、θ を任意の別の根 θ_i に写す M 自己同型は必ずちょうど1つ存在する。したがって、 $|\mathrm{Gal}(L/M)| = r = [L:M]$ が成り立つ。
次に、 $M = L^{\mathrm{Gal}(L/M)}$ を示す。多項式 $f_M(x) = \prod_{i=1}^{r}(x - \theta_i)$ を考える。この多項式の各係数は、根 $\theta_1, \ldots, \theta_r$ の基本対称式である。群 $\mathrm{Gal}(L/M)$ の元はこれらの根を置換するだけであるため、これらの基本対称式（すなわち $f_M(x)$ の係数）は $\mathrm{Gal}(L/M)$ の作用によって一切動かない。 したがって、$f_M(x)$ の係数が生成する体を M' とおくと、 $M' \subset L^{\mathrm{Gal}(L/M)}$ である。一方で、定義から明らかに $M' \subset M$ である。 多項式の構成から $f_M(x) \in M'[x]$ であり、θ はその根であるから、 θ の M' 上の最小多項式の次数は $f_M(x)$ の次数 r 以下である。すなわち $[L:M'] \leq r = [L:M]$ である。 包含関係 $M' \subset M$ と次数の比較 $[L:M'] \leq [L:M]$ から、 $M' = M$ でなければならない。ゆえに $M = L^{\mathrm{Gal}(L/M)}$ が成り立ち、すべての対応が厳密に証明された。

6. 第3のアプローチ：埋め込みの延長による証明

塔の定理 $[L:K]_s = [L:M]_s[M:K]_s$ の完全証明

K の代数的閉包を Ω とする。定義より、 $[M:K]_s = |\mathrm{Hom}_K(M, \Omega)|$ および $[L:M]_s = |\mathrm{Hom}_M(L, \Omega)|$ である。 いま、$\mathrm{Hom}_K(M, \Omega) = \{\tau_1, \tau_2, \ldots, \tau_a\}$ （ただし $a = [M:K]_s$）とする。また、恒等写像 $\mathrm{id}_M : M \to \Omega$ に対する L から Ω への M 固定埋め込みの全体を $\mathrm{Hom}_M(L, \Omega) = \{\lambda_1, \lambda_2, \ldots, \lambda_b\}$ （ただし $b = [L:M]_s$）とする。 代数的閉包の一般的性質（同型延長定理）により、各 τ_i に対し、それを L 全体へと延長した埋め込み $\tilde{\tau}_i : L \to \Omega$ が少なくとも1つ存在する。 ここで、 $a \times b$ 個の写像の集合 $S = \{\tilde{\tau}_i \circ \lambda_j \mid 1 \leq i \leq a, 1 \leq j \leq b\}$ を構成する。これが $\mathrm{Hom}_K(L, \Omega)$ と集合として完全に一致することを示す。
(1) 単射性（相異なる対からは相異なる写像が誘導されること）：
いま $\tilde{\tau}_i \circ \lambda_j = \tilde{\tau}_{i'} \circ \lambda_{j'}$ であると仮定する。この写像を M の元 $x \in M$ に制限する。 $\lambda_j, \lambda_{j'}$ は M 固定写像であるから $\lambda_j(x) = \lambda_{j'}(x) = x$。よって $\tilde{\tau}_i(x) = \tilde{\tau}_{i'}(x)$ となり、これは $\tau_i(x) = \tau_{i'}(x)$ を意味する。ゆえに $i = i'$ である。 $i = i'$ であれば、$\tilde{\tau}_i$ は全単射な像への同型であるから、 $\tilde{\tau}_i \circ \lambda_j = \tilde{\tau}_i \circ \lambda_{j'} \implies \lambda_j = \lambda_{j'}$ が従い、 $j = j'$ となる。よって $a \times b$ 個の写像はすべて相異なる。
(2) 全射性（任意の埋め込みがこの形で表せること）：
任意の $\sigma \in \mathrm{Hom}_K(L, \Omega)$ を取る。これを M に制限した写像 $\sigma|_M$ は K を固定する M から Ω への埋め込みであるから、ある i について $\sigma|_M = \tau_i$ となる。 ここで $\lambda = \tilde{\tau}_i^{-1} \circ \sigma$ という写像を考える。任意の $x \in M$ に対し、
$\lambda(x) = \tilde{\tau}_i^{-1}(\sigma(x)) = \tilde{\tau}_i^{-1}(\tau_i(x)) = x$ となるため、 λ は M を固定する L から Ω への埋め込みである。すなわち
$\lambda \in \mathrm{Hom}_M(L, \Omega)$。したがって、ある j が存在して $\lambda = \lambda_j$ となる。 式を変形すると $\sigma = \tilde{\tau}_i \circ \lambda_j$ となり、全射性が示された。 以上より、 $\mathrm{Hom}_K(L, \Omega)$ の要素数は正確に $a \times b$ である。すなわち $[L:K]_s = [L:M]_s \times [M:K]_s$ が完全に証明された。

基本定理の証明（不変体に対する評価の完結）

有限次分離拡大において $[L:K]_s = [L:K]$ が成り立ち、有限次正規拡大において $|\mathrm{Gal}(L/K)| = [L:K]_s$ が成り立つため、Galois拡大では $|\mathrm{Gal}(L/K)| = [L:K]$ である。
部分群 $H \subset G$ を取り、 $M = L^H$ とする。 L の任意の元 α に対し、群 H の作用による軌道を $H \cdot \alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ （ただし $\alpha_1 = \alpha$、 $k \leq |H|$）とする。次の軌道多項式を構成する。

$$g(x) = \prod_{i=1}^{k}(x - \alpha_i) = x^k - e_1(\alpha_1, \ldots, \alpha_k)x^{k-1} + \cdots + (-1)^k e_k(\alpha_1, \ldots, \alpha_k)$$

任意の $\sigma \in H$ は軌道の元を単に置換するだけであるため、各係数である基本対称式 e_m は σ の作用で不変である。すべての $\sigma \in H$ で不変であるから、 $g(x)$ のすべての係数は不変体 $M = L^H$ に属する。すなわち $g(x) \in M[x]$。 α は $g(\alpha) = 0$ を満たすため、 α の M 上の最小多項式 $m_\alpha(x)$ は $g(x)$ を割り切ねばならない。したがって、次数関係は
$[M(\alpha):M] = \deg(m_\alpha) \leq \deg(g) = k \leq |H|$ である。

原始元定理より $L = M(\theta)$ となる $\theta \in L$ が存在するため、上の不等式に θ を代入すれば、全体の拡大次数について $[L : L^H] \leq |H|$ を得る。 他方、 L/L^H はGalois拡大であるため、最初の議論より $[L : L^H] = |\mathrm{Gal}(L/L^H)|$ である。また、部分群の定義から明らかに $H \subset \mathrm{Gal}(L/L^H)$ であるため、 $|H| \leq |\mathrm{Gal}(L/L^H)| = [L : L^H]$ が成り立つ。 したがって、不等号が挟み込まれ、$[L : L^H] = |H|$ かつ $H = \mathrm{Gal}(L/L^H)$ が証明される。

7. 第4のアプローチ：Grothendieckによる圏論的証明

圏の同値性の完全な証明ステップ

有限次Galois拡大 $L/K, G = \mathrm{Gal}(L/K)$ を固定する。 関手 $F : \mathcal{C}_{L/K} \to G\text{-}\mathbf{finSet}$ $(A \mapsto \mathrm{Hom}_{K\text{-alg}}(A, L))$ が圏の同値（双対同値）を与えることを証明する。

1. 充満忠実性 (Fully Faithfulness) の厳密な証明:
任意の対象 $A, B \in \mathcal{C}_{L/K}$ に対し、写像 $\rho : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{G\text{-set}}(F(B), F(A))$ $(\psi \mapsto [f \mapsto f \circ \psi])$ が全単射であることを示す。 有限エタール代数の構造定理により、任意の対象は有限個の中間体の直積環 $\prod_i M_i$ に一意に同型となる。したがって、線形性から、対象が中間体そのものである場合 $A = L^H, B = L^{H'}$ の場合に全単射性を示せば十分である。
中間体 L^H から $L^{H'}$ への K 代数準同型写像 ψ を取る。 ψ は L^H の元を $L^{H'}$ 内へ写す。 $L/L^{H'}$ は有限次Galois拡大であるから、同型延長定理より ψ は L 全体の自己同型 $\sigma \in G$ に延長できる。この σ の条件は、 L^H 上で ψ と一致すること、すなわち $\sigma|_{L^H} = \psi$ である。これが $L^{H'}$ に収まるためには、 $\sigma(L^H) \subset L^{H'} \implies \sigma H' \sigma^{-1} \subset H$ という群論的包含関係が必要十分条件となる。
これを関手 F で写した世界で考える。 $F(L^H) = \mathrm{Hom}_K(L^H, L) \cong G/H$ （コセット空間）であり、$F(L^{H'}) = \mathrm{Hom}_K(L^{H'}, L) \cong G/H'$ である。 G-集合の間の射 $\gamma : G/H' \to G/H$ は、群の作用と可換（$\gamma(g \cdot x) = g \cdot \gamma(x)$）な写像である。 γ は代表元 $1 \cdot H'$ の行き先 $\gamma(1 \cdot H') = \sigma H$ によって完全に決定される。これがウェルディファインド (well-defined) であるための条件は、 H' の元 h' に対して $\gamma(h' \cdot H') = \gamma(1 \cdot H') \implies h'\sigma H = \sigma H \implies \sigma^{-1} h' \sigma \in H$ となり、まさに $\sigma^{-1} H' \sigma \subset H$ である。 したがって、代数側の射 ψ の自由度（共役自己同型の類）と、 G-集合側の射 γ の自由度（コセット写像の選び方）は、全く同一の群論的射条件 $\sigma^{-1} H' \sigma \subset H$ によって1対1に支配されている。よって、写像 ρ は全単射であり、関手は充満忠実である。

2. 本質的全射性 (Essential Surjectivity) の厳密な証明:
任意の有限 G-集合 X を取る。 G は有限群であるから、 X は有限個の軌道に一意に分解される。すなわち $X = \coprod_{i=1}^m X_i$。各推移的 G-集合 X_i は、ある安定化部分群 $H_i \subset G$ を用いて、コセット集合 G/H_i に G-同型である。 これに対し、代数側の圏 $\mathcal{C}_{L/K}$ の対象として、次の直積環を直接構成する。

$$A = \prod_{i=1}^m L^{H_i}$$

この構成した A に関手 F を適用する。不変体 L^{H_i} は体であるから、直積環からの体 L への準同型写像は、いずれか1つの成分への射影写像と、その成分からの体の埋め込みの合成に限られる。したがって、

$$F(A) = \mathrm{Hom}_{K\text{-alg}}\left(\prod_{i=1}^m L^{H_i}, L \right) \cong \coprod_{i=1}^m \mathrm{Hom}_{K\text{-alg}}(L^{H_i}, L)$$

となる。各成分について、 Artinの定理から $[L : L^{H_i}] = |H_i|$ であり、埋め込みの個数 $\mathrm{Hom}_K(L^{H_i}, L)$ は正確に $[G : H_i]$ 個の元からなる。さらに群 G の作用を考えると、この集合は G-集合として G/H_i と完全に同型である。 ゆえに、$F(A) \cong \coprod_{i=1}^m G/H_i \cong X$ となり、集合側の圏のいかなる対象も、代数側から関手を通じて本質的に復元される。

【基本定理の完全なる回収】
圏の同値性が確立されたため、圏の内部のオブジェクト（対象）およびサブオブジェクト（部分対象）の格子構造は、完全に一対一（反変であるため包含関係は反転）に対応しなければならない。 代数側の圏 $\mathcal{C}_{L/K}$ において、「直積環にこれ以上分解できない対象」とは、代数的に冪等元を持たない可換環、すなわち「中間体 M」そのものである。 関手 F による対応により、これは $G\text{-}\mathbf{finSet}$ 側における「これ以上直和に分解できない G-集合」、すなわち「推移的 G-集合 X」に一対一に対応する。 群論の一般定理により、基礎となる群 G 自身（これは $F(L)$ に対応する）からの全射を持つ推移的 G-集合は、部分群 H による商空間 G/H の形のものしか存在しない。 代数側の中間体の包含関係 $M_1 \subset M_2$ は、射の存在 $M_1 \hookrightarrow M_2$ に対応し、関手の反変性により集合側で

は全射 $G/H_2 \to G/H_1$ へと写される。これが成り立つための必要十分条件は、部分群の包含関係 $H_2 \subset H_1$ である。これによってGalois対応のすべての構造が完全に証明される。

8. 第5のアプローチ：Galoisのオリジナルな証明

証明（分解式の構成、ラグランジュ補間、有理関係式の推敲）

K 上の多項式 $f(x)$ の相異なるすべての根を $\alpha_1, \alpha_2, \ldots, \alpha_n$ とする。 ここで、 n 個の不確定元 $t_1, \ldots, t_n$ を導入し、次の線形結合の積を考える。

$$\prod_{\sigma \neq \tau \in S_n} \left(\sum_{i=1}^{n} t_i \alpha_{\sigma(i)} - \sum_{i=1}^{n} t_i \alpha_{\tau(i)} \right)$$

この積多項式は零多項式ではないため、 K が無限体であれば、この積が 0 とならないような具体的な元の組 $c_1, \ldots, c_n \in K$ が必ず選択できる。 この c_i を用いて、次の**ガロアの分解式 (Galois resolvent)**を定義する。

$$V = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

c_i の選び方から、根の任意の非自明な置換 $\sigma \in S_n \setminus \{\mathrm{id}\}$ に対して、 $V_\sigma = \sum c_i \alpha_{\sigma(i)}$ と置くと、 $n!$ 個の値 V_σ はすべて相異なる。次に、各根 α_k が V の有理式として表せることを、ラグランジュの補間公式を用いて明示的に示す。 多項式 $G(X) = \prod_{\sigma \in S_n} (X - V_\sigma)$ を構成する。この係数は根の対称式であるから $K[X]$ の多項式である。また、その微分多項式を $G'(X)$ とする。ここで、次の多項式を定義する。

$$P_k(X) = \sum_{\sigma \in S_n} \alpha_{\sigma(k)} \prod_{\tau \neq \sigma} (X - V_\tau)$$

この多項式 $P_k(X)$ の係数も、根の全置換に対して不変であるため、完全に K に属する（$P_k(X) \in K[X]$）。 ここで、変数 X に実際の値 $V = V_{\mathrm{id}}$ を代入する。 V は V_{id} であるから、 $\prod_{\tau \neq \sigma}(V - V_\tau)$ の項において、 $\sigma \neq \mathrm{id}$ のときは必ず因子 $(V - V_{\mathrm{id}}) = 0$ を含むため、和の中で $\sigma = \mathrm{id}$ の項だけが生き残る。したがって、

$$P_k(V) = \alpha_1 \cdot \prod_{\tau \neq \mathrm{id}} (V - V_\tau) = \alpha_k \cdot G'(V)$$

となる。 V_σ はすべて相異なるため $G'(V) \neq 0$ である。したがって、

$$\alpha_k = \frac{P_k(V)}{G'(V)} \equiv \phi_k(V) \quad (\phi_k(x) \in K(x))$$

となり、すべての根が分解式 V の K 係数有理式として完全に記述された。

Galoisは、根の間に成り立つ K 係数のあらゆる有理関係式（すなわち $P(\alpha_1, \ldots, \alpha_n) = 0$ となる多項式）を、置換した群でも依然として $P(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$ と真に保つような置換全体の集合として「方程式の群（Galois群）」を定義した。
いま、新しくいくつかの方程式の根（中間体 M に相当する既知の量）を基礎体に添加して、新しい基礎体 M を作ったとする。 これによって、元々は K 上では成り立たなかった、あるいは記述できなかった「新しい根の間の有理関係式」が大量に発生する。 群の定義の制約条件（関係式を不変に保つこと）から、満たすべき有理関係式の数が劇的に増加するため、それらをすべてクリアして不変に保つことのできる置換の候補集合は、元の群 G の中から条件に適合するものだけに強制的に絞り込まれる。 Galoisは、多項式 $G(X)$ が新しい体 M 上でどのように既約因子に因数分解されるか（どの V_σ が同じ既約成分の根として残るか）を追跡することにより、この「関係式の追加（体の拡大）」と「置換集合の制限（部分群への縮小）」の間に、一対一の完全な包含反転対応が存在することを証明した。

9. 各アプローチの比較まとめ

証明法	主たる道具立て	長所	短所
Artinアプローチ	Dedekindの補題、連立一次方程式	最短かつ最もエレガント。現代代数学の標準であり自己完結性が極めて高い。	抽象度が高く、多項式の具体的な根の挙動や方程式の解法という動機が見えにくい。
古典的アプローチ	原始元定理、最小多項式の係数	多項式の根の対称性と群の関係が非常に具体的であり、直観に合致する。	無限体と有限体での証明の分離や、最大公約多項式の互除法の議論など、泥臭い構成が必要。
埋め込みの延長	代数的閉包、分離次数、軌道多項式	積公式（塔の定理）が強力であり、一般の体拡大（非有限次など）への体系化に適する。	代数的閉包の存在性証明など、事前の重厚な準備論（Zornの補題など）が要求される。
圏論的アプローチ	有限エタール代数の圏、有限G集合	トポロジー（被覆空間の分類）との類似を包括する幾何学的かつ最高峰の視点。	有限次ガロア理論の証明という目的単体に対しては、道具立てがあまりにも大掛かり。
ガロアのオリジナル	ガロアの分解式、ラグランジュ補間	Galois自身の天才的な発想の原点。方程式の可解性（冪根による解法）に直接結びつく。	現代的な「体」の言語で記述されていないため、式の添字や置換の記述が極めて煩雑。

参考文献

[1] Artin, E. (1944). *Galois Theory*. Notre Dame Mathematical Lectures, No. 2. University of Notre Dame Press.

[2] Bourbaki, N. (2003). *Algebra II: Chapters 4–7*. Elements of Mathematics. Springer-Verlag.

[3] Galois, É. (1846). "Mémoire sur les conditions de résolubilité des équations par radicaux". *Journal de Mathématiques Pures et Appéles*, 11, 381–444.

[4] Grothendieck, A. (1971). *Revêtements étales et groupe fondamental (SGA 1)*. Lecture Notes in Mathematics, Vol. 224. Springer-Verlag.

[5] Lang, S. (2002). *Algebra*. Graduate Texts in Mathematics, Vol. 211. Springer-Verlag.