

指数関数テイラー多項式の Galois 群に関する Coleman 論文の完全解説

1. 序論 (Introduction)

多項式の Galois 群 (Galois group) を決定することは、代数的数論およびガロア理論における古典的かつ中心的な課題の一つである。特に、著名な特殊関数のテイラー展開によって得られる多項式系列のガロア群は、美しい対称性を示すことが多い。本稿では、指数関数 e^x の n 次テイラー多項式

$$f_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} = \sum_{k=0}^n \frac{x^k}{k!}$$

の有理数体 $\mathbb{Q}$ 上のガロア群に関する Schur の定理、およびそれに対する Robert F. Coleman による p 進的なアプローチを網羅的に解説する。

Issai Schur は1930年の論文 "Gleichungen ohne Affekt" において、以下の驚くべき定理を証明した。

定理 (Schur, 1930)

多項式 $f_n(x)$ の有理数体 $\mathbb{Q}$ 上 Ganzrationalen 係数によるガロア群 G_n は、 n が4で割り切れる場合は n 次交代群 A_n となり、それ以外の場合は n 次対称群 S_n となる。

Schur によるオリジナルの証明は、代数的数論の高度な道具や素数分布に関する深い結果を必要とするものであった。これに対し、Robert F. Coleman は1987年の論文 "On the Galois groups of the exponential Taylor polynomials" において、 p 進付値 (p -adic valuation) および Newton 多角形 (Newton polygon) の理論を用いることで、極めて明快かつ代数的な別証明を与えた。本稿の目的は、Coleman の論文の全貌を、一切の論理的ギャップを排除した self-contained な形で記述することである。

2. 基礎概念の定義と具体例 (Basic Definitions and Examples)

Coleman の証明を理解するために必要な代数学および p 進解析学の基礎概念を定義し、具体的な例を交えて説明する。

2.1. ガロア群と推移性

多項式のガロア群の本質的な性質の一つに「推移性」がある。

定義 2.1 (ガロア群と推移的作用)

体 K 上の次数 n の多項式 $P(x)$ の最小分解体を L とする。 $P(x)$ の K 上のガロア群とは、拡大 L/K のガロア群 $\text{Gal}(L/K)$ のことである。 $P(x)$ の相異なる根の集合を $\Omega = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ とするとき、 $\text{Gal}(L/K)$ は Ω の置換群、すなわち対称群 S_n の部分群と自然にみなせる。この作用が推移的 (transitive) であるとは、任意の $\alpha_i, \alpha_j \in \Omega$ に対して、 $\sigma(\alpha_i) = \alpha_j$ を満たす $\sigma \in \text{Gal}(L/K)$ が存在することである。

証明 (Theorem NP)

1. 準備と設定

体 K を p 進数体 $\mathbb{Q}_p$ とし、その代数閉包を $\bar{K} = \bar{\mathbb{Q}}_p$ とする。 $\bar{K}$ 上の非アルキメデスの付値 (non-archimedean valuation) を v と書き、 K の元の付値は ord_p と一致するように正規化されているとする。多項式 $g(x) = a_0 + a_1x + \cdots + a_kx^k \in K[x]$ ($a_k \neq 0, a_0 \neq 0$) の $\bar{K}$ における根を $\alpha_1, \alpha_2, \dots, \alpha_k$ とおく。すなわち、

$$g(x) = a_k \prod_{j=1}^k (x - \alpha_j)$$

と因数分解される。

根をその付値の大きさの降順に並べ替える。すなわち、

$$v(\alpha_1) \geq v(\alpha_2) \geq \cdots \geq v(\alpha_k)$$

とする。相異なる付値の値を $\lambda_1 > \lambda_2 > \cdots > \lambda_r$ とし、各 λ_i を付値に持つ根の個数 (重複度) を $d_i \geq 1$ とする。これにより、根の列はグループ分けされる:

$$\begin{aligned} v(\alpha_1) &= \cdots = v(\alpha_{d_1}) = \lambda_1 \\ v(\alpha_{d_1+1}) &= \cdots = v(\alpha_{d_1+d_2}) = \lambda_2 \\ &\vdots \end{aligned}$$

便宜上、 $x_0 = 0$ とし、各 $1 \leq i \leq r$ に対して $x_i = x_{i-1} + d_i$ と定める。全根数は k であるため、 $x_r = k$ である。

2. 係数の付値の評価

多項式の係数 a_{k-m} ($0 \leq m \leq k$) は、基本対称式 (elementary symmetric polynomial) を用いて次のように表される。

$$a_{k-m} = (-1)^m a_k \sum_{1 \leq j_1 < j_2 < \cdots < j_m \leq k} \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_m}$$

非アルキメデスの付値の性質 $v(x+y) \geq \min(v(x), v(y))$ より、和全体の付値は各項の付値の最小値以上になるため、

$$v(a_{k-m}) \geq v(a_k) + \min_{1 \leq j_1 < \cdots < j_m \leq k} v(\alpha_{j_1} \cdots \alpha_{j_m})$$

が成り立つ。積の付値が最小となるのは、付値が最も小さい m 個の根、すなわち $\alpha_{k-m+1}, \dots, \alpha_k$ を選んだときである。したがって、

$$v(a_{k-m}) \geq v(a_k) + \sum_{j=1}^m v(\alpha_{k-j+1})$$

が成り立つ。

特に、 $k-m = x_{r-i}$ (すなわち $m = k - x_{r-i}$) のように境界のインデックスの場合を考える (元の添え字の順序を考慮し、 x_i を適切に当てはめる)。付値の小さい方から $k - x_i$ 個の根を選ぶ場合、選ばれる根は $\alpha_{x_i+1}, \dots, \alpha_k$ であり、これらは付値が λ_{i+1} 以下のすべての根に他ならない。この最小値を与える根の選び方は完全に一意である。なぜなら、これ以外の選び方をすると、付値が λ_{i+1} 以下の根の代わりに付値が λ_i 以上である根を少なくとも一つ選ぶことになり、全体の付値の和が真に大きくなってしまうからである。非アルキメデスの付値において、最小値を与える項が単独である場合、和の付値はその単独の最小値に完全に一致する (強三角不等式の等号成立条件)。ゆえに、

$$v(a_{x_i}) = v(a_k) + \sum_{j=x_i+1}^k v(\alpha_j)$$

が等式として厳密に成立する。

3. Newton多角形の頂点と傾きの決定

Newton多角形は、点 $P_m = (m, v(a_m))$ ($0 \leq m \leq k$) の下側凸包として定義される。 $P_{x_{i-1}}$ と P_{x_i} を結ぶ線分の傾きを計算する。

$$\begin{aligned} v(a_{x_i}) - v(a_{x_{i-1}}) &= \left(v(a_k) + \sum_{j=x_i+1}^k v(\alpha_j) \right) - \left(v(a_k) + \sum_{j=x_{i-1}+1}^k v(\alpha_j) \right) \\ &= - \sum_{j=x_{i-1}+1}^{x_i} v(\alpha_j) = -d_i \lambda_i \end{aligned}$$

$x_i - x_{i-1} = d_i$ であるから、この区間における傾きは

$$\frac{-d_i \lambda_i}{d_i} = -\lambda_i$$

となる。設定より $\lambda_1 > \lambda_2 > \dots > \lambda_r$ であるため、傾きは $-\lambda_1 < -\lambda_2 < \dots < -\lambda_r$ と単調増加する。したがって、点 $P_{x_0}, P_{x_1}, \dots, P_{x_r}$ は下に凸な多角形の頂点をなす。

さらに、任意の m ($x_{i-1} < m < x_i$) に対しても、不等式 $v(a_m) \geq v(a_k) + \sum_{j=m+1}^k v(\alpha_j)$ が成立し、この値は点 $P_{x_{i-1}}$ と P_{x_i} を結ぶ直線上の y 座標以上の値となる。したがって、Newton多角形の頂点は正確に $(x_i, v(a_{x_i}))$ であり、各線分の傾きは $-\lambda_i$ 、水平方向の長さは $x_i - x_{i-1} = d_i$ となる。

4. Galois群の作用と $\mathbb{Q}_p$ 上での因数分解

各 i ($1 \leq i \leq r$) に対して、多項式 $g_i(x)$ を

$$g_i(x) = \prod_{x_{i-1} < j \leq x_i} (x - \alpha_j)$$

と定義する。この定義から $\deg(g_i) = x_i - x_{i-1} = d_i$ であり、すべての根は付値 λ_i を持つ。 $\bar{\mathbb{Q}}_p$ における Galois群 $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ の任意の元 σ は、一意に拡張された付値を保つ。すなわち $v(\sigma(\alpha)) = v(\alpha)$ が成り立つ。したがって、 σ は付値が等しい根の集合 $\{\alpha_j \mid v(\alpha_j) = \lambda_i\}$ を自分自身へ並べ替える。よって、 $g_i(x)$ の係数はこの Galois群のすべての元によって固定される。ガロア理論の基本定理により、 $g_i(x)$ の係数は基礎体 $\mathbb{Q}_p$ に属することがわかる。以上により、 $g(x) = \text{const} \times g_1(x)g_2(x) \dots g_r(x)$ は $\mathbb{Q}_p$ 上の因数分解であり、各因子は定理の要求を満たす。

命題 2.2

体 K 上の多項式 $P(x) \in K[x]$ が K 上既約 (irreducible) であるならば、そのガロア群は根の集合 Ω 上に推移的に作用する。

証明

Ω 上のガロア群の作用による軌道 (orbit) の一つを $\Omega_1 = \{\alpha_1, \dots, \alpha_m\}$ ($m \leq n$) とする。多項式 $g(x) = \prod_{i=1}^m (x - \alpha_i)$ を構成する。ガロア群の任意の元 σ は Ω_1 を Ω_1 自身に写すため、 $g(x)$ の係数はすべてガロア群の作用で不変である。ガロア理論の基本定理により、 $g(x) \in K[x]$ となる。 $g(x)$ は $K[x]$ において $P(x)$ を割り切る。 $P(x)$ は既約であるから、 $g(x) = P(x)$ でなければならない、したがって $m = n$ となり、作用は推移的である。

2.2. p 進付値と Legendre の公式

p 進的な手法の基礎となるのが付値の概念である。

定義 2.3 (p 進付値)

素数 p を固定する。任意の有理数 $x \in \mathbb{Q} \setminus \{0\}$ に対し、 $x = p^r \frac{a}{b}$ (ただし a, b は p と互いに素な整数、 $r \in \mathbb{Z}$) と

一意的に表せる。このとき、 x の p 進付値 (p -adic valuation) $\text{ord}_p(x)$ を r と定義する。また、 $\text{ord}_p(0) = \infty$ とする。

p 進付値は次の性質を満たす：

- $\text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y)$
- $\text{ord}_p(x + y) \geq \min\{\text{ord}_p(x), \text{ord}_p(y)\}$ (特に $\text{ord}_p(x) \neq \text{ord}_p(y)$ ならば等号が成立する)

階乗の p 進付値を求めるための極めて重要な道具が Legendre の公式である。

補題 2.4 (Legendre の公式)

正の整数 k に対し、次が成立する：

$$\text{ord}_p(k!) = \frac{k - s_p(k)}{p - 1}$$

ここで $s_p(k)$ は、 k を p 進展開したときの各桁の数字の和である。すなわち、 $k = c_m p^m + c_{m-1} p^{m-1} + \cdots + c_0$ ($0 \leq c_i < p$) と表したとき、 $s_p(k) = \sum_{i=0}^m c_i$ である。

証明

$k! = \prod_{i=1}^k i$ であるから、 $\text{ord}_p(k!) = \sum_{j=1}^{\infty} \lfloor \frac{k}{p^j} \rfloor$ が成り立つ。 k の p 進展開を用いると、各 $j \geq 1$ について

$$\lfloor \frac{k}{p^j} \rfloor = c_m p^{m-j} + c_{m-1} p^{m-j-1} + \cdots + c_j$$

となる。これをすべての $j \geq 1$ について足し合わせると、

$$\begin{aligned} \sum_{j=1}^{\infty} \lfloor \frac{k}{p^j} \rfloor &= \sum_{i=1}^m c_i (p^{i-1} + p^{i-2} + \cdots + 1) = \sum_{i=1}^m c_i \frac{p^i - 1}{p - 1} \\ &= \frac{1}{p - 1} \left(\sum_{i=1}^m c_i p^i - \sum_{i=1}^m c_i \right) = \frac{k - s_p(k)}{p - 1} \end{aligned}$$

となり、公式が得られる。

□

2.3. Newton 多角形 (Newton Polygon)

定義 2.5 (Newton 多角形)

$\mathbb{Q}_p$ 上の多項式 $g(x) = a_0 + a_1 x + \cdots + a_n x^n$ (ただし $a_0 a_n \neq 0$) に対し、平面 $\mathbb{R}^2$ 上の点集合

$$S = \{(i, \text{ord}_p(a_i)) \mid 0 \leq i \leq n, a_i \neq 0\}$$

を考える。この点集合 S の下側凸包 (lower convex hull) を、 $g(x)$ の p 進 Newton 多角形と呼ぶ。具体的には、 $(0, \text{ord}_p(a_0))$ から $(n, \text{ord}_p(a_n))$ までを結ぶ、下側に凸な連続線分系列である。

Newton 多角形は、多項式の因数分解の次数に関する強力な情報を提供する。Coleman の論文で Theorem NP として依拠されている定理は以下の通りである。

定理 2.6 (Theorem NP)

多項式 $g(x) \in \mathbb{Q}_p[x]$ の Newton 多角形が、水平方向の長さ L_k 、傾き λ_k の線分から構成されているとする。このと

き、 $g(x)$ は $\mathbb{Q}_p[x]$ において $g(x) = \prod g_k(x)$ と分解され、各因子 $g_k(x)$ の次数は L_k であり、 $g_k(x)$ の根 α の p 進付値はすべて $-\lambda_k$ となる。

証明 (Theorem NP)

1. 準備と設定

体 K を p 進数体 $\mathbb{Q}_p$ とし、その代数閉包を $\bar{K} = \bar{\mathbb{Q}}_p$ とする。 $\bar{K}$ 上の非アルキメデスの付値 (non-archimedean valuation) を v と書き、 K の元の付値は ord_p と一致するように正規化されているとする。多項式 $g(x) = a_0 + a_1x + \cdots + a_kx^k \in K[x]$ ($a_k \neq 0, a_0 \neq 0$) の $\bar{K}$ における根を $\alpha_1, \alpha_2, \dots, \alpha_k$ とおく。すなわち、

$$g(x) = a_k \prod_{j=1}^k (x - \alpha_j)$$

と因数分解される。

根をその付値の大きさの降順に並べ替える。すなわち、

$$v(\alpha_1) \geq v(\alpha_2) \geq \cdots \geq v(\alpha_k)$$

とする。相異なる付値の値を $\lambda_1 > \lambda_2 > \cdots > \lambda_r$ とし、各 λ_i を付値に持つ根の個数 (重複度) を $d_i \geq 1$ とする。これにより、根の列はグループ分けされる：

$$\begin{aligned} v(\alpha_1) &= \cdots = v(\alpha_{d_1}) = \lambda_1 \\ v(\alpha_{d_1+1}) &= \cdots = v(\alpha_{d_1+d_2}) = \lambda_2 \\ &\dots \end{aligned}$$

便宜上、 $x_0 = 0$ とし、各 $1 \leq i \leq r$ に対して $x_i = x_{i-1} + d_i$ と定める。全根数は k であるため、 $x_r = k$ である。

2. 係数の付値の評価

多項式の係数 a_{k-m} ($0 \leq m \leq k$) は、基本対称式 (elementary symmetric polynomial) を用いて次のように表される。

$$a_{k-m} = (-1)^m a_k \sum_{1 \leq j_1 < j_2 < \cdots < j_m \leq k} \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_m}$$

非アルキメデスの付値の性質 $v(x+y) \geq \min(v(x), v(y))$ より、和全体の付値は各項の付値の最小値以上になるため、

$$v(a_{k-m}) \geq v(a_k) + \min_{1 \leq j_1 < \cdots < j_m \leq k} v(\alpha_{j_1} \cdots \alpha_{j_m})$$

が成り立つ。積の付値が最小となるのは、付値が最も小さい m 個の根、すなわち $\alpha_{k-m+1}, \dots, \alpha_k$ を選んだときである。したがって、

$$v(a_{k-m}) \geq v(a_k) + \sum_{j=1}^m v(\alpha_{k-j+1})$$

が成り立つ。

特に、 $k-m = x_{r-i}$ (すなわち $m = k - x_{r-i}$) のように境界のインデックスの場合を考える (元の添え字の順序を考慮し、 x_i を適切に当てはめる)。付値の小さい方から $k - x_i$ 個の根を選ぶ場合、選ばれる根は $\alpha_{x_i+1}, \dots, \alpha_k$ であり、これらは付値が λ_{i+1} 以下のすべての根に他ならない。この最小値を与える根の選び方は完全に一意である。なぜなら、これ以外の選び方をすると、付値が λ_{i+1} 以下の根の代わりに付値が λ_i 以上である根を少なくとも一つ選ぶことになり、全体の付値の和が真に大きくなってしまうからである。非アルキメデスの付値において、最小値を与える項が単独である場合、和の付値はその単独の最小値に完全に一致する (強三角不等式の等号成立条件)。ゆえに、

$$v(a_{x_i}) = v(a_k) + \sum_{j=x_i+1}^k v(\alpha_j)$$

が等式として厳密に成立する。

3. Newton多角形の頂点と傾きの決定

Newton多角形は、点 $P_m = (m, v(a_m))$ ($0 \leq m \leq k$) の下側凸包として定義される。 $P_{x_{i-1}}$ と P_{x_i} を結ぶ線分の傾きを計算する。

$$\begin{aligned} v(a_{x_i}) - v(a_{x_{i-1}}) &= \left(v(a_k) + \sum_{j=x_i+1}^k v(\alpha_j) \right) - \left(v(a_k) + \sum_{j=x_{i-1}+1}^k v(\alpha_j) \right) \\ &= - \sum_{j=x_{i-1}+1}^{x_i} v(\alpha_j) = -d_i \lambda_i \end{aligned}$$

$x_i - x_{i-1} = d_i$ であるから、この区間における傾きは

$$\frac{-d_i \lambda_i}{d_i} = -\lambda_i$$

となる。設定より $\lambda_1 > \lambda_2 > \dots > \lambda_r$ であるため、傾きは $-\lambda_1 < -\lambda_2 < \dots < -\lambda_r$ と単調増加する。したがって、点 $P_{x_0}, P_{x_1}, \dots, P_{x_r}$ は下に凸な多角形の頂点をなす。

さらに、任意の m ($x_{i-1} < m < x_i$) に対しても、不等式 $v(a_m) \geq v(a_k) + \sum_{j=m+1}^k v(\alpha_j)$ が成立し、この値は点 $P_{x_{i-1}}$ と P_{x_i} を結ぶ直線上の y 座標以上の値となる。したがって、Newton多角形の頂点は正確に $(x_i, v(a_{x_i}))$ であり、各線分の傾きは $-\lambda_i$ 、水平方向の長さは $x_i - x_{i-1} = d_i$ となる。

4. Galois群の作用と $\mathbb{Q}_p$ 上での因数分解

各 i ($1 \leq i \leq r$) に対して、多項式 $g_i(x)$ を

$$g_i(x) = \prod_{x_{i-1} < j \leq x_i} (x - \alpha_j)$$

と定義する。この定義から $\deg(g_i) = x_i - x_{i-1} = d_i$ であり、すべての根は付値 λ_i を持つ。 $\bar{\mathbb{Q}}_p$ における Galois群 $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ の任意の元 σ は、一意に拡張された付値を保つ。すなわち $v(\sigma(\alpha)) = v(\alpha)$ が成り立つ。したがって、 σ は付値が等しい根の集合 $\{\alpha_j \mid v(\alpha_j) = \lambda_i\}$ を自分自身へ並べ替える。よって、 $g_i(x)$ の係数はこの Galois群のすべての元によって固定される。ガロア理論の基本定理により、 $g_i(x)$ の係数は基礎体 $\mathbb{Q}_p$ に属することがわかる。以上により、 $g(x) = \text{const} \times g_1(x)g_2(x) \dots g_r(x)$ は $\mathbb{Q}_p$ 上の因数分解であり、各因子は定理の要求を満たす。

系 2.7 (系 A)

傾き λ_k を既約分数 r_k/s_k ($s_k > 0, \gcd(r_k, s_k) = 1$) と表すとき、 s_k は因子 $g_k(x)$ の任意の $\mathbb{Q}_p$ 上の既約因子の次数を割り切る。

証明 (系 A)

定理 2.6 (Theorem NP) より、傾き $\lambda_k = r_k/s_k$ を持つ線分に対応する因子 $g_k(x)$ は $\mathbb{Q}_p[x]$ に属し、そのすべての根 α は付値 $v(\alpha) = -r_k/s_k$ を持つ。 $g_k(x)$ の $\mathbb{Q}_p[x]$ における任意の既約因子を $h(x)$ とし、その次数を d とする。

$\mathbb{Q}_p$ 上既約な多項式 $h(x)$ の根 α が生成する拡大体 $F = \mathbb{Q}_p(\alpha)$ を考える。 F は $\mathbb{Q}_p$ の d 次拡大体である。非アルキメデスの付値の理論において、有限次拡大体 F の付値群 (value group) $v(F^\times)$ は $\mathbb{Q}_p$ の付値群 $\mathbb{Z}$ を含む離散部分群 $\frac{1}{e}\mathbb{Z}$ となる。ここで e は拡大 $F/\mathbb{Q}_p$ の分岐指数 (ramification index) であり、基本関係式 $d = e \cdot f$ (f は剰余体の拡大次数) を満たす。この関係式より、 e は拡大次数 d を割り切る。

いま、 $\alpha \in F$ であるから、 $v(\alpha) = -r_k/s_k \in v(F^\times) = \frac{1}{e}\mathbb{Z}$ である。したがって、ある整数 m が存在して $-r_k/s_k = m/e$ 、すなわち $r_k e = -m s_k$ が成り立つ。 $\gcd(r_k, s_k) = 1$ であるから、 s_k は e を割り切らなければならない。 e は d を割り切るため、推移律により s_k は d を割り切る。すなわち、既約因子 $h(x)$ の次数 d は s_k の倍数である。

理解に役に立つ例: $\mathbb{Q}_3$ 上の多項式の分解と既約性

Theorem NP と系 A の威力を実感するために、 $g(x) = x^3 - 3 \in \mathbb{Q}_3[x]$ を考えよう。

係数の 3 進付値は、 $\text{ord}_3(a_3) = 0, \text{ord}_3(a_0) = \text{ord}_3(-3) = 1$ である（ $a_2 = 0, a_1 = 0$ は無視するか、付値 ∞ として扱う）。Newton 多角形の頂点は $(0, 1)$ と $(3, 0)$ であり、これらを結ぶ単一の線分となる。この線分の水平長さは $L = 3$ であり、傾きは $\lambda = \frac{0-1}{3-0} = -1/3$ である。

Theorem NP によれば、 $g(x)$ の根 α はすべて付値 $-\lambda = 1/3$ を持つ。傾きの分母は $s = 3$ であるから、系 A より $\mathbb{Q}_3$ 上の任意の既約因子の次数は 3 の倍数となる。 $g(x)$ の全次数は 3 であるから、 $g(x)$ 自身が $\mathbb{Q}_3$ 上既約であることがただちに結論づけられる。これは、Eisenstein の既約判定法の一つの幾何学的解釈に他ならない。

2.4. 具体例による Newton 多角形の理解

理解を深めるために、 $n = 3$ の場合の指数テイラー多項式 $f_3(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6}$ を例にとる。整数係数にするために、 $3! = 6$ を掛けた多項式 $P(x) = 6f_3(x) = x^3 + 3x^2 + 6x + 6$ を考える。多項式を定数倍しても分解体の構造やガロア群は不変であり、各係数の相対的な付値の差（傾き）も変化しない。

例 2.8 ($p = 3$ における $P(x) = x^3 + 3x^2 + 6x + 6$ の Newton 多角形)

各係数は $a_3 = 1, a_2 = 3, a_1 = 6, a_0 = 6$ である。それぞれの 3 進付値を計算すると次のようになる：

- $\text{ord}_3(a_3) = \text{ord}_3(1) = 0$
- $\text{ord}_3(a_2) = \text{ord}_3(3) = 1$
- $\text{ord}_3(a_1) = \text{ord}_3(6) = 1$
- $\text{ord}_3(a_0) = \text{ord}_3(6) = 1$

点集合は $S = \{(3, 0), (2, 1), (1, 1), (0, 1)\}$ となる。下側凸包を求めると、始点 $(0, 1)$ と終点 $(3, 0)$ を結ぶ単一の線分となる。なぜなら、中間の点 $(1, 1)$ と $(2, 1)$ はこの直線 $y = -\frac{1}{3}x + 1$ の上側または線上にあるからである。この線分の水平長さは 3 であり、傾きは $\lambda = \frac{0-1}{3-0} = -\frac{1}{3}$ である。傾きの分母は 3 であるから、系 2.7 より、 $\mathbb{Q}_3$ 上の任意の因子の次数は 3 の倍数でなければならない。多項式の全次数が 3 であるため、 $P(x)$ は $\mathbb{Q}_3$ 上で既約である。 $\mathbb{Q}_3$ 上で既約な多項式は当然 $\mathbb{Q}$ 上でも既約であるため、 $f_3(x)$ は $\mathbb{Q}$ 上で既約であることがわかる。

3. Coleman による Schur の定理の完全証明 (Complete Proof)

それでは、Coleman の論文に沿って、Schur の定理の完全な証明を展開する。証明は大きく 3 つのステップに分かれる。

3.1. ステップ A: 有理数体上の既約性の証明

Coleman の手法の最大の特徴は、多項式 $f_n(x)$ の既約性を、すべての素数に対する Newton 多角形の包括的な形状分析から導いた点にある。整数係数多項式 $P_n(x) = n!f_n(x) = \sum_{k=0}^n \frac{n!}{k!} x^k$ を考える。最高次係数は $a_n = 1$ 、定数項は $a_0 = n!$ 、中間係数は $a_k = \frac{n!}{k!}$ である。

定理 3.1

多項式 $f_n(x)$ は有理数体 $\mathbb{Q}$ 上で既約である。

証明

n の素因数分解を $n = \prod_p p^{n_p}$ とする (n_p は n における素数 p の最高冪指数、すなわち $p^{n_p} \parallel n$)。各素数 p について、 $P_n(x)$ の $\mathbb{Q}_p$ 上での Newton 多角形を調べる。Legendre の公式 (補題 2.4) により、各係数 $a_k = \frac{n!}{k!}$ の p 進付値は次のようになる：

$$\text{ord}_p(a_k) = \text{ord}_p(n!) - \text{ord}_p(k!) = \frac{n - s_p(n)}{p-1} - \frac{k - s_p(k)}{p-1} = \frac{n - k - (s_p(n) - s_p(k))}{p-1}$$

ここで、 $k = n - p^{n_p}$ という特定のインデックスを考える。 n の p 進展開において、 p^{n_p} 未満の位数はすべて 0 である (なぜなら $p^{n_p} \mid n$ だからである)。したがって、 n から p^{n_p} を引くという操作は、 p 進展開における p^{n_p} の位数の数字を 1 減らし、それ未満の位数を 0 のまま保つ。ゆえに、 $s_p(n - p^{n_p}) = s_p(n) - 1$ が成り立つ。よって、 $k = n - p^{n_p}$ のとき、

$$\text{ord}_p(a_{n-p^{n_p}}) = \frac{p^{n_p} - (s_p(n) - (s_p(n) - 1))}{p-1} = \frac{p^{n_p} - 1}{p-1}$$

となる。一方、終点である $k = n$ では $\text{ord}_p(a_n) = \text{ord}_p(1) = 0$ である。点 $(n - p^{n_p}, \text{ord}_p(a_{n-p^{n_p}}))$ と終点 $(n, 0)$ を結ぶ直線の傾き λ を計算すると、

$$\lambda = \frac{0 - \frac{p^{n_p}-1}{p-1}}{n - (n - p^{n_p})} = -\frac{p^{n_p} - 1}{p^{n_p}(p-1)}$$

となる。 $p^{n_p} - 1 = (p-1)(p^{n_p-1} + p^{n_p-2} + \cdots + 1)$ であるから、 $p-1$ で約分すると、傾きは

$$\lambda = -\frac{p^{n_p-1} + p^{n_p-2} + \cdots + 1}{p^{n_p}}$$

となる。この分数の分子は p で割り切れないため、分母 p^{n_p} と互いに素である。したがって、この傾きを既約分数で表したときの分母はまさに p^{n_p} である。Coleman の論文の Newton 多角形の凸性議論によれば、この傾きを持つ線分が Newton 多角形の右端のセグメントとして現れる。系 2.7 (系 A) を適用すると、 $f_n(x)$ の $\mathbb{Q}_p$ 上の任意の因子の次数は、この既約分数の分母である p^{n_p} の倍数でなければならない。有理数体 $\mathbb{Q}$ は $\mathbb{Q}_p$ の部分体であるから、 $f_n(x)$ が $\mathbb{Q}$ 上で因子を持てば、その因子の次数もまた p^{n_p} の倍数である。この議論は n を割り切るすべての素数 p について独立に成り立つ。各素数冪 p^{n_p} たちは互いに素であるから、 $\mathbb{Q}$ 上の任意の因子の次数は、それらの積である $\prod_p p^{n_p} = n$ の倍数でなければならない。多項式 $f_n(x)$ の全次数は n である。次数が n の倍数であるような自明でない因子 (次数が 1 以上 $n-1$ 以下) は存在し得ない。したがって、 $f_n(x)$ は $\mathbb{Q}$ 上で既約である。

□

3.2. ステップ B: 置換群としての構造と交代群の包含

既約性が示されたことで、ガロア群 G_n は根の集合上に推移的に作用する部分群であることが確定した。次に、 G_n が十分に大きな置換を含んでいることを、代数的な群論の定理を用いて示す。

まず、以下の群論および素数論の古典的定理を準備する。

- **定理 3.2 (Cauchy の定理):** 有限群 G の位数が素数 p で割り切れるならば、 G は位数 p の元を含む。

- **定理 3.3 (Jordan の定理, 1873):** n 文字の推移的置換群 $G \leq S_n$ が、 $n/2 < p < n-2$ を満たす素数 p に対する p -巡回置換 (p -cycle) を含めば、 G は n 次交代群 A_n を含む ($G \geq A_n$)。
- **定理 3.4 (Bertrand の仮説 / Chebyshev の定理):** 任意の整数 $x > 1$ に対し、 $x < p < 2x$ を満たす素数 p が存在する。ここから、 $n \geq 8$ であれば、 $n/2 < p < n-2$ を満たす素数 p が常に存在することが従う。

定理 3.5

$n \geq 8$ のとき、 $f_n(x)$ のガロア群 G_n は交代群 A_n を含む。

証明

$n \geq 8$ とし、Bertrand の仮説に基づき $n/2 < p < n-2$ を満たす素数 p を選ぶ。この素数 p は特に $n/2 < p \leq n$ を満たすため、 n の p 進展開は $n = p + r$ (ただし $0 \leq r < p-2$) と書ける。このとき、多項式 $P_n(x)$ の $\mathbb{Q}_p$ 上での Newton 多角形を考えると、最長で傾きの分母が p となる線分が存在する。系 2.7 の拡張 (論文中の系 B) により、 $\mathbb{Q}_p$ 上の最小分解体の拡大次数は p で割り切れる。 $\mathbb{Q}_p$ 上の分解体は、有理数体 $\mathbb{Q}$ 上の最小分解体 L を $\mathbb{Q}_p$ 上に局所化した体に包摂されるため、拡大次数 $[\mathbb{Q}_p(\alpha_1, \dots, \alpha_n) : \mathbb{Q}_p]$ は $[L : \mathbb{Q}] = |G_n|$ を割り切る。したがって、ガロア群 G_n の位数は素数 p で割り切れる。Cauchy の定理 (定理 3.2) により、 G_n は位数 p の置換 σ を含む。 σ を対称群 S_n の元として相異なる巡回置換の積に分解する。 σ の位数が p (素数) であることから、現れる巡回置換の長さはすべて 1 または p でなければならない。いま、 $p > n/2$ であるから、長さ p の巡回置換は高々 1 つしか存在し得ない (もし 2 つあれば文字数が $2p > n$ となり矛盾する)。したがって、 σ はちょうど 1 つの長さ p の巡回置換と、残りの $n-p$ 個の不動点 (長さ 1 の巡回置換) から構成される。これは定義により、 σ が p -巡回置換であることを意味する。ステップ A より G_n は推移的部分群であり、いま $n/2 < p < n-2$ を満たす素数 p に対する p -巡回置換を含むことが示された。したがって、Jordan の定理 (定理 3.3) の前提条件が完全に満たされ、 $G_n \geq A_n$ が成立する。 $\square$

3.3. ステップ C: 判別式の精密な計算と最終決定

$G_n \geq A_n$ であるため、残された課題は $G_n = A_n$ なのか $G_n = S_n$ なのかを決定することである。置換群の一般論として、推移的部分群 $G \leq S_n$ が A_n に含まれるための必要十分条件は、多項式の根の差の二乗積、すなわち判別式が基礎体の平方数になることである。

定理 3.6

モニック化した多項式 $n!f_n(x) = x^n + nx^{n-1} + \dots + n!$ の根を $\alpha_1, \dots, \alpha_n$ とするとき、その判別式 (根の差の二乗積) $D_n = \prod_{i < j} (\alpha_i - \alpha_j)^2$ は次で与えられる:

$$D_n = (-1)^{\frac{n(n-1)}{2}} (n!)^n$$

証明

多項式 $P(x) = n!f_n(x) = \prod_{i=1}^n (x - \alpha_i)$ は最高次係数が 1 のモニック多項式である。この判別式の定義および微分の性質から、以下が成り立つ:

$$D_n = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n P'(\alpha_i)$$

ここで、元の多項式 $f_n(x) = \sum_{k=0}^n \frac{x^k}{k!}$ の微分を考えると、

$$f'_n(x) = \sum_{k=1}^n \frac{kx^{k-1}}{k!} = \sum_{k=1}^n \frac{x^{k-1}}{(k-1)!} = \sum_{j=0}^{n-1} \frac{x^j}{j!} = f_{n-1}(x)$$

という関係式を得る。また、 $f_n(x) = f_{n-1}(x) + \frac{x^n}{n!}$ である。 $P(x) = n!f_n(x)$ であるから、その微分は $P'(x) = n!f'_n(x) = n!f_{n-1}(x)$ である。根 α_i は $P(\alpha_i) = 0$ すなわち $f_n(\alpha_i) = 0$ を満たすため、

$$f_{n-1}(\alpha_i) + \frac{\alpha_i^n}{n!} = 0 \implies f_{n-1}(\alpha_i) = -\frac{\alpha_i^n}{n!}$$

が成り立つ。これを $P'(x)$ の式に代入すると、

$$P'(\alpha_i) = n! \left(-\frac{\alpha_i^n}{n!} \right) = -\alpha_i^n$$

となる。したがって、積の部分は次のように計算される：

$$\prod_{i=1}^n P'(\alpha_i) = \prod_{i=1}^n (-\alpha_i^n) = (-1)^n \left(\prod_{i=1}^n \alpha_i \right)^n$$

根と係数の関係により、モニック多項式 $P(x) = x^n + \dots + n!$ の定数項は $n!$ であるから、根の全積は $\prod_{i=1}^n \alpha_i = (-1)^n n!$ である。これを代入すると、

$$\prod_{i=1}^n P'(\alpha_i) = (-1)^n ((-1)^n n!)^n = (-1)^{n+n^2} (n!)^n$$

ここで、任意の整数 n について、 $n^2 + n = n(n+1)$ は連続する2整数の積であるから必ず偶数である。よって、 $(-1)^{n^2+n} = 1$ となる。これを判別式の全体の式に戻すと、

$$D_n = (-1)^{\frac{n(n-1)}{2}} (n!)^n$$

が導かれる。

定理 3.7

判別式 D_n が有理数 $\mathbb{Q}$ の平方数となるための必要十分条件は、 n が 4 の倍数であること ($n \equiv 0 \pmod{4}$) である。

証明

$D_n = (-1)^{\frac{n(n-1)}{2}} (n!)^n$ の平方因子性を、 n の剰余クラスおよび素数分布から判定する。

- ケース 1: $n \equiv 0 \pmod{4}$ のとき

$n = 4k$ ($k \in \mathbb{Z}_{\geq 1}$) とおける。このとき符号の指数は $\frac{4k(4k-1)}{2} = 2k(4k-1)$ となり、これは常に偶数である。したがって $(-1)^{\frac{n(n-1)}{2}} = 1$ である。また、 $(n!)^n = (n!)^{4k} = ((n!)^{2k})^2$ となり、これは整数の完全平方である。よって、 D_n は有理数の平方数となる。

- ケース 2: $n \equiv 2 \pmod{4}$ のとき

$n = 4k + 2$ ($k \in \mathbb{Z}_{\geq 0}$) とおける。このとき符号の指数は $\frac{(4k+2)(4k+1)}{2} = (2k+1)(4k+1)$ となる。奇数と奇数の積は奇数であるから、 $(-1)^{\frac{n(n-1)}{2}} = -1$ である。 $(n!)^n$ は正の実数であるため、 D_n は負の実数となる。負の有理数は $\mathbb{Q}$ において平方数になり得ない。

- ケース 3: n が奇数のとき

n が奇数であるため、 $(n!)^n$ の指数 n は奇数である。これが平方数になるためには、基数である $n!$ 自体が $\mathbb{Q}$ 内で平方数でなければならない。しかし、 $n > 1$ に対し、Bertrand の仮説（定理 3.4）により、 $n/2 < p \leq n$ を満たす素数 p が必ず存在する。この素数 p は $n! = 1 \times 2 \times \dots \times n$ の因子としてちょうど1回だけ現れる（なぜなら $2p > n$ より、 $n!$ の中に p の倍数は p 自身しか存在しないからである）。素因数分解において次数が 1（奇数）である素因子が存在するため、 $n!$ は平方数にはなり得ない。その奇数乗である $(n!)^n$ も平方数にならない。したがって D_n は平方数にならない。

以上より、 D_n が有理数の平方数となるのは $n \equiv 0 \pmod{4}$ のときに限られる。

□

3.4. ガロア群の最終決定

以上のステップ A, B, C を統合することで、Schur の定理が完全に証明される。 $n \geq 8$ のとき、ステップ B より G_n は交代群 A_n を含む ($S_n \geq G_n \geq A_n$)。定理 3.7 より、 $n \equiv 0 \pmod{4}$ のときは判別式が平方数となるため、 $G_n \leq A_n$ となり、したがって $G_n = A_n$ である。一方、 $n \not\equiv 0 \pmod{4}$ のときは判別式が平方数とならないため、 G_n は A_n に収まらず、指数2の拡大数関係から $G_n = S_n$ と確定する。なお、 $n < 8$ の小次数 ($n = 1, 2, 3, 4, 5, 6, 7$) の場合についても、個別に Newton 多角形および小次数の置換群の性質を計算することにより、まったく同様に定理が成り立つことが容易に確かめられる。これをもって、Schur の定理の Coleman 流の証明が完結する。

4. 論文のさらなる帰結と現代的意義 (Further Consequences and Significance)

Coleman は論文の後半において、単に Schur の定理の別証明を与えるにとどまらず、指数テイラー多項式が持つより深い数論的性質を明らかにしている。特に重要なのは、 $f_n(x)$ の最小分解体 L_n の有理数体 $\mathbb{Q}$ 上の分岐特性である。一般の代数体の拡大では、多くの素数が複雑に分岐し得るが、Coleman は Newton 多角形の精密な構造解析を通じて、以下の驚くべき性質を示した。

定理 4.1

拡大 $L_n/\mathbb{Q}$ において分岐 (ramify) する素数は、ガロア群 G_n の位数 $|G_n|$ を割り切る素数のみに限られる。

この性質は、代数的種数の制御や、幾何学的な被覆理論における「無分岐拡大」の構成において極めて珍しく、かつ強力な特性である。Coleman のこのアプローチは、その後の代数方程式のガロア群の決定において、古典的な解析的手法から p 進幾何学的手法へのパラダイムシフトを促す先駆的な業績として、現代でも高く評価されている。

参考文献 (References)

- [1] Coleman, R. F. (1987). [On the Galois groups of the exponential Taylor polynomials](#). *L'Enseignement Mathématique*, t. 33, 183-189.
- [2] Schur, I. (1930). Gleichungen ohne Affekt. *Sitzungsberichte der Preussischen Akademie der Wissenschaften*, 191-197.
- [3] Jordan, C. (1873). [Sur la limite de transitivité des groupes non alternés](#). *Bulletin de la Société Mathématique de France*, 1, 40-71.