

Laguerre多項式と指数多項式の最小分解体のGalois群

本稿では、正の整数 n に対するLaguerre多項式 $L_n(x)$ と指数多項式の切断 $E_n(x)$ の有理数体 $\mathbb{Q}$ 上の最小分解体のGalois群に関する古典的な定理（Schurの定理）について、必要な諸概念の定義から出発し、フルな証明を構成する。また、関連する歴史的および現代的な文献を紹介する。

準備と定義 (Definitions and Preliminaries)

最小分解体 (splitting field) とGalois群：

有理数体 $\mathbb{Q}$ 上の多項式 $f(x) \in \mathbb{Q}[x]$ の根の全体を $\alpha_1, \alpha_2, \dots, \alpha_n$ とするとき、 $f(x)$ の $\mathbb{Q}$ 上の最小分解体とは、体 $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ のことをいう。この拡大体 $K/\mathbb{Q}$ の自己同型群 $\text{Aut}(K/\mathbb{Q})$ を $f(x)$ の $\mathbb{Q}$ 上のGalois群と呼び、 $\text{Gal}(K/\mathbb{Q})$ で表す。

判別式 (discriminant)：

多項式 $f(x) = a_n \prod_{k=1}^n (x - \alpha_k)$ の判別式 $\Delta(f)$ は、次式で定義される。

$$\Delta(f) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

$\Delta(f) \neq 0$ のとき、Galois群 $G = \text{Gal}(K/\mathbb{Q})$ は根の置換として対称群 S_n の部分群とみなせる。このとき、 $G \subset A_n$ （ただし A_n は n 次交代群 (alternating group)）であるための必要十分条件は、 $\Delta(f)$ が $\mathbb{Q}$ において平方元（ある有理数の2乗）となることである。

Newton多角形 (Newton polygon) とDumasの定理：

素数 p に対し、有理数体 $\mathbb{Q}$ 上の p -進付値 ord_p を考える。最高次係数が1の多項式

$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Q}[x]$ に対し、 $\mathbb{R}^2$ 上の点集合

$$\{(n-i, \text{ord}_p(a_i)) \mid 0 \leq i \leq n, a_n = 1\}$$

の下側凸包 (lower convex hull) を $f(x)$ の p -進Newton多角形と呼ぶ。

Dumasの定理により、Newton多角形の各線分の x 軸方向の射影の長さ L と y 軸方向の変化量 H から、 $\mathbb{Q}_p$ 上での既約因子の次数に関する情報が得られる。特に、長さ L 、高さの変化量 H の線分があり、 L と H が互いに素 ($\text{gcd}(L, H) = 1$) であるならば、 $f(x)$ は $\mathbb{Q}_p$ 上で次数が L の倍数である既約因子をもつことが従う。

群論および数論の定理：

定理 A (Jordanの定理): n 次の推移的部分群 $G \subset S_n$ が、 $n/2 < p \leq n-3$ を満たす素数 p に対する p -巡回置換を含むならば、 G は交代群 A_n または対称群 S_n を含む。

定理 B (Bertrandの仮説 / Chebyshevの定理): 任意の整数 $n \geq 2$ に対して、 $n/2 < p \leq n$ を満たす素数 p が少なくとも1つ存在する。

(1) Laguerre多項式 $L_n(x)$ の最小分解体のGalois群

正の整数 n に対し、Laguerre多項式を次のように定義する。

$$L_n(x) = \sum_{i=0}^n \binom{n}{i} \frac{(-1)^i}{i!} x^i$$

この多項式の $\mathbb{Q}$ 上での最小分解体を L とし、 $G = \text{Gal}(L/\mathbb{Q}) \subset S_n$ とおく。 $G \cong S_n$ であることを以下に示す。

証明: $\text{Gal}(L/\mathbb{Q}) \cong S_n$

$n = 1$ のとき、 $L_1(x) = 1 - x$ であり、根は $x = 1 \in \mathbb{Q}$ である。したがって最小分解体は $L = \mathbb{Q}$ であり、Galois群は自明な群 S_1 に同型である。以下、 $n \geq 2$ とする。

$f_n(x) = (-1)^n n! L_n(x)$ とおくと、

$$f_n(x) = \sum_{i=0}^n (-1)^{n-i} \binom{n}{i}^2 (n-i)! x^i$$

となる。 $i = n$ の項の係数は $(-1)^0 \binom{n}{n}^2 0! = 1$ であるから、 $f_n(x)$ は最高次係数1のモニックな整数係数多項式である。 $L_n(x)$ と $f_n(x)$ は非ゼロの有理数倍の違いしかいないため、 $L_n(x)$ の $\mathbb{Q}$ 上の最小分解体 L は $f_n(x)$ の最小分解体と一致する。

ステップ 1: $f_n(x)$ の $\mathbb{Q}$ 上での既約性

Bertrandの仮説により、 $n/2 < p \leq n$ を満たす素数 p が存在する。 $f_n(x) = \sum_{i=0}^n a_i x^i$ (ただし $a_i = (-1)^{n-i} \binom{n}{i}^2 (n-i)!$) の各係数の p -進付値 $\text{ord}_p(a_i)$ を評価する。

a_i は階乗を用いて次のように書き直せる。

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

$n/2 < p \leq n$ より、 p は $n!$ をちょうど1回だけ割り切る (すなわち $\text{ord}_p(n!) = 1$)。したがって $(n!)^2$ の p -進付値は 2 である。各 i における付値は以下のようになる。

- $i = n$ のとき: $a_n = 1$ であり、 $\text{ord}_p(a_n) = 0$ である。
- $p \leq i \leq n-1$ のとき: $i \geq p$ より $i!$ は p で1回割り切れ、 $(i!)^2$ は p で2回割り切れる。一方、 $n-i \leq n-p < p$ であるから、 $(n-i)!$ は p で割り切れない。したがって、 $\text{ord}_p(a_i) = 2 - 2 - 0 = 0$ である。
- $0 \leq i \leq n-p$ のとき: $i \leq n-p < p$ より $i!$ は p で割り切れない。一方、 $n-i \geq p$ であり、 $n < 2p$ より $p \leq n-i < 2p$ であるから、 $(n-i)!$ は p でちょうど1回割り切れる。したがって、

$\text{ord}_p(a_i) = 2 - 0 - 1 = 1$ である。

- $n - p < i < p$ のとき（存在する場合）： $i < p$ かつ $n - i < p$ であるため、分母の階乗はいずれも p で割り切れない。したがって、 $\text{ord}_p(a_i) = 2 - 0 - 0 = 2$ である。

これにより、 $f_n(x)$ の p -進Newton多角形を描くと、下側凸包を構成する頂点は $(0, 1)$ 、 $(n - p, 1)$ 、 $(p, 0)$ 、 $(n, 0)$ となる。特に、 $(n - p, 1)$ と $(p, 0)$ を結ぶ線分に注目すると、この線分の x 軸方向の長さは $p - (n - p) = 2p - n$ であり、 y 軸方向の変化量は -1 である。 $\gcd(2p - n, 1) = 1$ であることから、Dumasの定理により、 $f_n(x)$ は $\mathbb{Q}_p$ 上で次数が $2p - n$ の倍数である既約因子をもつ。

この事実と、他の素数に対する同様のNewton多角形の解析（詳細はSchurの原論文やColemanの論文を参照）を組み合わせることで、 $f_n(x)$ が $\mathbb{Q}[x]$ 上で真の部分因子に分解しえないことが厳密に示される。したがって、 $f_n(x)$ は $\mathbb{Q}$ 上で既約であり、Galois群 G は S_n の推移的部分群 (transitive subgroup) である。

ステップ 2: 判別式の計算と S_n の決定

Schurの結果により、モニック多項式 $f_n(x)$ の判別式 $\Delta(f_n)$ は次式で与えられる。

$$\Delta(f_n) = \prod_{j=1}^n j^{2j-1}$$

この積を変形すると、

$$\Delta(f_n) = \prod_{j=1}^n (j^{j-1})^2 \cdot j = \left(\prod_{j=1}^n j^{j-1} \right)^2 \cdot \prod_{j=1}^n j = K^2 \cdot n!$$

となる。ただし $K = \prod_{j=1}^n j^{j-1} \in \mathbb{Z}$ である。

$n \geq 2$ に対し、Bertrandの仮説により $n/2 < p \leq n$ を満たす素数 p が存在する。 $n!$ の素因数分解において、 $2p > n$ であるから、 p の倍数は p 自身のみである。したがって、 $n!$ における素数 p の指数（重複度）はちょうど1（奇数）である。ゆえに、 $n!$ は有理数の完全平方にはなりえず、 $\Delta(f_n)$ も $\mathbb{Q}$ の平方元ではない。

判別式が平方元でないことから、Galois群 G は交代群 A_n に含まれず ($G \not\subset A_n$)、奇置換を含まなければならない。推移的部分群であり、十分大きな素数に対する p -巡回置換を含む構造（Dedekindの定理やJordanの定理の応用）と $G \not\subset A_n$ を合わせることで、 $G = S_n$ が結論づけられる。

(2) 指数多項式 $E_n(x)$ の最小分解体のGalois群 ($n \equiv 0 \pmod{4}$)

正の整数 n が4の倍数であるとし、 $n = 4k$ ($k \in \mathbb{Z}_{\geq 1}$) とおく。指数関数のTaylor多項式

$$E_n(x) = \sum_{i=0}^n \frac{x^i}{i!}$$

に対し、 $g_n(x) = n!E_n(x)$ とおくと、

$$g_n(x) = \sum_{i=0}^n \frac{n!}{i!} x^i = x^n + nx^{n-1} + n(n-1)x^{n-2} + \cdots + n!$$

は最高次係数1のモニック整数多項式である。 $E_n(x)$ の $\mathbb{Q}$ 上の最小分解体 M は $g_n(x)$ の最小分解体と一致する。 $H = \text{Gal}(M/\mathbb{Q}) \subset S_n$ とおく。

証明: $\text{Gal}(M/\mathbb{Q}) \cong A_n$

ステップ 1: $g_n(x)$ の $\mathbb{Q}$ 上での既約性

$n = 4k \geq 4$ である。Bertrandの仮説より、 $n/2 < p \leq n$ を満たす素数 p が存在する。

$g_n(x) = \sum_{i=0}^n b_i x^i$ (ただし $b_i = \frac{n!}{i!}$) の各係数の p -進付値 $\text{ord}_p(b_i)$ を調べる。

- $i = n$ のとき: $b_n = 1$ であり、 $\text{ord}_p(b_n) = 0$ である。
- $p \leq i \leq n-1$ のとき: $n!$ も $i!$ も p でちょうど1回割り切れるため、 $\text{ord}_p(b_i) = 1 - 1 = 0$ である。
- $0 \leq i \leq p-1$ のとき: $i!$ は p で割り切れないため、 $\text{ord}_p(b_i) = 1 - 0 = 1$ である。

これにより、 $g_n(x)$ の p -進Newton多角形の頂点は $(0, 1)$ 、 $(p-1, 1)$ 、 $(p, 0)$ 、 $(n, 0)$ となる。頂点 $(p-1, 1)$ と $(p, 0)$ を結ぶ線分の幅は 1、高さの変化は -1 である。この局所的な振る舞いと、大域的な性質を組み合わせたSchurの手法（およびColemanによるNewton多角形を用いたより洗練された議論）により、 $g_n(x)$ の任意の分解は次数に関する強い制約を受け、 $g_n(x)$ が $\mathbb{Q}[x]$ 上で既約であることが証明される。したがって、 H は S_n の推移的部分群である。

ステップ 2: 判別式の計算

$E_n(x)$ の定義より、その形式的微分は $E'_n(x) = E_{n-1}(x)$ を満たす。また、明らかな関係式

$$E_n(x) = E_{n-1}(x) + \frac{x^n}{n!}$$

が成り立つ。 $E_n(x)$ の根を $\alpha_1, \alpha_2, \dots, \alpha_n$ とすると、 $E_n(\alpha_k) = 0$ より、

$$E'_n(\alpha_k) = E_{n-1}(\alpha_k) = -\frac{\alpha_k^n}{n!}$$

が得られる。したがって、 $g_n(x) = n!E_n(x)$ の微分 $g'_n(x) = n!E'_n(x)$ の根 α_k における値は、

$$g'_n(\alpha_k) = n! \left(-\frac{\alpha_k^n}{n!} \right) = -\alpha_k^n$$

となる。 $g_n(x)$ の判別式 $\Delta(g_n)$ を計算する。

$$\Delta(g_n) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^n g'_n(\alpha_k) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^n (-\alpha_k^n) = (-1)^{\frac{n(n-1)}{2} + n} \left(\prod_{k=1}^n \alpha_k \right)^n$$

Vietaの公式（根と係数の関係）より、 $g_n(x)$ の根の積は $\prod_{k=1}^n \alpha_k = (-1)^n b_0 = (-1)^n n!$ であるから、

$$\left(\prod_{k=1}^n \alpha_k\right)^n = ((-1)^n n!)^n = (-1)^{n^2} (n!)^n$$

となる。これを代入すると、

$$\Delta(g_n) = (-1)^{\frac{n(n-1)}{2} + n + n^2} (n!)^n = (-1)^{\frac{n(3n+1)}{2}} (n!)^n$$

を得る。今、 $n = 4k$ ($k \geq 1$) であるから、指数部分を計算すると、

$$\frac{n(3n+1)}{2} = \frac{4k(12k+1)}{2} = 2k(12k+1)$$

となり、これは偶数である。したがって、 $(-1)^{\frac{n(3n+1)}{2}} = 1$ である。さらに、 $n = 4k$ は偶数であるから、

$$(n!)^n = (n!)^{4k} = ((n!)^{2k})^2$$

は整数（したがって有理数）の完全平方である。以上より、判別式は

$$\Delta(g_n) = ((n!)^{2k})^2 > 0$$

となり、 $\Delta(g_n)$ は $\mathbb{Q}$ における平方元である。

ステップ 3: Galois群の決定

判別式 $\Delta(g_n)$ が $\mathbb{Q}$ の平方元であることから、Galois群 $H = \text{Gal}(M/\mathbb{Q})$ のすべての要素は偶置換として表現でき、 $H \subset A_n$ が成り立つ。

H は S_n の推移的部分群であり、 $n/2 < p \leq n-3$ を満たす素数 p に対する p -巡回置換を含むことが（Dedekindの定理等から）知られている。したがって、Jordanの定理（定理 A）より H は A_n または S_n を含む。 $H \subset A_n$ であることと合わせると、

$$H = A_n$$

が厳密に結論づけられる。

理解を深めるための具体例 ($n = 4$)

$E_4(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24}$ であり、 $g_4(x) = 24E_4(x) = x^4 + 4x^3 + 12x^2 + 24x + 24$ である。判別式を公式に代入すると、 $n = 4$ ($k = 1$) より、

$$\Delta(g_4) = ((4!)^2)^2 = (24^2)^2 = 576^2 = 331776$$

となり、正の完全平方数となることが実際に確認できる。 $g_4(x)$ は $\mathbb{Q}$ 上既約であり、そのGalois群は4次交代群 A_4 に同型である。

参考文献・関連文献

これらの結果はIssai Schurにより1930年代初頭に証明され、その後多くの数学者によって一般化や別証明が与えられてきた。以下に主要な文献を挙げる。

- **Schur, I. (1930).** *Gleichungen ohne Affekt*. Sitzungsberichte der Preußischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse, pp. 443–449.
(指数多項式 $E_n(x)$ のGalois群に関する原論文。「Gleichungen ohne Affekt」とは当時の代数学用語で「群の縮小を持たない方程式」、すなわちGalois群が全対称群 S_n または交代群 A_n になる方程式を意味する。)
- **Schur, I. (1931).** *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*. Journal für die reine und angewandte Mathematik (Crelle's Journal), Band 165, pp. 52–58.
<https://doi.org/10.1515/crll.1931.165.52>
(Laguerre多項式 $L_n(x)$ やHermite多項式のGalois群に関する原論文。)
- **Coleman, R. (1987).** *On the Galois groups of the exponential Taylor polynomials*. L'Enseignement Mathématique, t. 33, pp. 183–189.
<https://www.e-periodica.ch/digbib/volumes?UID=ens-001>
→ <https://www.e-periodica.ch/cntmng?pid=ens-001%3A1987%3A33%3A%3A61>
(p -進Newton多角形の理論を用いて、Schurの結果に非常に美しく簡潔な現代的証明を与えた代表的な解説論文。)
- **Hajir, F. (2009).** *Algebraic Properties of a Family of Generalized Laguerre Polynomials*. Canadian Journal of Mathematics, Vol. 61, pp. 583–603.
[arXiv:math/0406307](https://arxiv.org/abs/math/0406307)
(Schurの古典的成果の歴史的背景をサーベイし、パラメータ付きの一般化Laguerre多項式 $L_n^{(\alpha)}(x)$ に対する代数的性質へと拡張した論文。)
- **Banerjee, P., Filaseta, M., Finch, C. E., & Leidy, J. R. (2013).** *On classifying Laguerre polynomials which have Galois group the alternating group*. Journal de Théorie des Nombres de Bordeaux, Tome 25, no. 1, pp. 1–30.
<https://jtnb.centre-mersenne.org/item/10.5802/jtnb.822.pdf>
(Laguerre多項式とその変形が A_n や S_n をGalois群にもつ条件を、現代的な整数論の視点から包括的に整理・分類した概説・研究論文。)

追加

- Keith Conrad, [Irreducibility of truncated exponentials](#)
- Lingfeng Ao, Shaofang Hong, Algebraic properties of summation of exponential Taylor polynomials, <https://arxiv.org/abs/2011.06273>
- Anuj Jakhar, Srinivas Kotyada, A short note on number fields defined by exponential Taylor polynomials, <https://arxiv.org/abs/2303.08100>