Constructing PGL(2, 7)-extensions with restricted ramifications

東京理科大学　大学院理学研究科　数学専攻
鈴木望夢 (Nozomu SUZUKI)

概要

regular polynomial の特殊化と Newton polygon に関する手法を用いて, $\mathbb{Q}$ 上の PGL(2, 7) 拡大で，ただひとつの 2 次部分体上不分岐であるようなものを構成する．得られる拡大の 2 次体上の Galois 群は位数 168 の単純群 PSL(2, 7) である．

1　導入

有限群 G を与えたとき，G を Galois 群にもつ Galois 拡大，すなわち G 拡大が存在するか，という問題を**逆 Galois 問題**という．この問題は一般には未解決であるが，有理数体 $\mathbb{Q}$ 上の逆 Galois 問題では，例えば G が対称群や交代群であった場合に対して G 拡大が存在し，また，複素数体 $\mathbb{C}$ 上の一変数有理関数体 $\mathbb{C}(t)$ 上には任意の有限群 G に対して G 拡大が存在することが以前から知られている（[4]）．

一方，有理数体の有限次拡大，すなわち代数体の拡大は，一般に分岐する素点を少なくすることには限界があることが知られている．したがって代数体上の逆 Galois 問題では，分岐する素点を指定した拡大を構成する，分岐制限付きの逆 Galois 問題も重要である．例えば，有理数体上の拡大では，不分岐拡大が存在しないことが知られている．また，不分岐アーベル拡大は類体論によって説明される．

本研究では，正則拡大の特殊化を用いることで，$\mathbb{Q}$ 上のひとつの素数のみが分岐する PGL(2, 7) 拡大や，2 次部分体上が不分岐 PSL(2, 7) 拡大となる $\mathbb{Q}$ 上の PGL(2, 7) 拡大の族を構成した．これらの群は非 Abel 群であり，特に PSL(2, 7) は単純群である．代数体の拡大における素点の分岐を調べる手法は様々にあるが，本研究は Newton polygon を用いた手法のひとつである Ore の定理を用いている．

本レポートでは，証明に用いた Ore の定理に関する先行研究と主定理，及び主定理の証明の概略を述べ，最後に主定理を用いて得られる例を紹介する．

2　剛性の方法と Newton polygon

この節では，本研究の対象である正則 PGL$(2,7)$ の定義多項式について述べ，その後に主定理の証明に用いた事実を紹介する．

定義 2.1. L/K を体の分離拡大とする．K が L 内で代数的に閉じているとき，L/K を**正則拡大**という．

逆 Galois 問題に対する手法のひとつとして，次の Hilbert の既約性定理に基づいた正則拡大を用いる方法がある．

定理 2.2 ([6])**.** k を代数体とし，$K = k(T)$ を k 上の一変数有理関数体，L を k 上正則な K の有限次拡大とする．L/K の定義多項式を $f(T;X) \in K[X]$ とし，その K 上の *Galois* 群を G とする．このとき，$f(t;X) \in k[X]$ の k 上の *Galois* 群が G となる特殊化を与える $t \in k$ が無数に存在する．

本研究は次の多項式を基に行なっている：

$$F(T;X) := X^8 + X^7 + 7X^6 - T(X+1) \in \mathbb{Q}(T)[X]. \tag{1}$$

多項式 (1) の $\mathbb{Q}(T)$ 上の Galois 群は PGL$(2,7)$ である（cf.[4]）．この多項式は以下に述べる Riemann の存在定理と剛性の方法によって得られる．

定理 2.3 (**Riemann の存在定理**)**.** 有限群 G と正整数 r に対し，以下の *3* つの集合の間に一対一対応が存在する：

(i) G と同型な *Galois* 群をもつ $\mathbb{C}(T)$ 上の r 点分岐 *Galois* 拡大の同型類全体*,*
(ii) G と同型な *deck* 群をもつ $\mathbb{P}^1\mathbb{C}$ の r 点分岐 *Galois* 被覆の同型類全体*,*
(iii) G の共役類の組 $\mathcal{C} = (C_1, \ldots, C_r)$ に対し，

$$SNi(\mathcal{C}) := \{(g_1, \ldots, g_r) \mid g_i \in C_i, \langle g_1, \ldots, g_r \rangle = G, g_1 \cdots g_r = 1\}$$

としたとき，$SNi(\mathcal{C})$ が空でないような $\mathcal{C}$ 全体．

剛性の方法を説明するために，共役類の有理性と，共役類の組の剛性を定義する．

定義 2.4. (i) G を有限群とし，C を G の共役類とする．C^k を $C^k = \{g^k \mid g \in C\}$ によって定める．$|G|$ と互いに素な 0 でない任意の整数 k に対し，$C = C^k$ が成り立つとき，C は有理性をもつという．

(ii) G を有限群とし，$\mathcal{C} = (C_1, \ldots, C_r)$ を G の共役類の組とする．G が (空でない) $SNi(\mathcal{C})$ に

$$G \times SNi(\mathcal{C}) \to SNi(\mathcal{C}) : (h, (g_1, \ldots, g_r)) \mapsto (g_1^h, \ldots, g_r^h)$$

によって単純かつ推移的に作用しているとき，$\mathcal{C}$ は剛性をもつという．

定理 2.5 (**剛性の方法**). 有限群 G の共役類の組 $\mathcal{C} = (C_1, \ldots, C_r)$ が剛性をもち，さらに各 C_i が有理性をもつとき，定理 *2.3* によって $\mathcal{C}$ に対応する $\mathbb{C}(T)$ 上の G 拡大，及び $\mathbb{P}^1\mathbb{C}$ 上の G 被覆は $\mathbb{Q}$ 上で定義される．

(1) の多項式 F の分解体は PGL$(2,7)$ の共役類の組 $(2^3 1^2, 61^2, 71)$ に対応し，剛性の方法によって $\mathbb{Q}$ 上で定義されることが確かめられる．ここで，共役類の組を表す数字は，共役類の元を互いに素なサイクルの積で表したときの各サイクルの長さを示したものである．また，この F によって定義される $\mathbb{Q}(T)$ の拡大 $L = \mathbb{Q}(T)[X]/(F(T;X))$ は種数 0 で，特に，$\mathbb{Q}$ 上の有理関数体である．関数体の種数は次の Riemann-Hurwitz の公式によって計算できる．

定理 2.6 (Riemann-Hurwitz の公式). G を S_n の推移的部分群とし，$\mathcal{C} = (C_1, \ldots, C_r)$ を剛性をもつ G の共役類の組とする．各 C_i が有理性をもつとし，$\mathcal{C}$ に対応する $\mathbb{Q}(t)$ の拡大を L，L の種数を g とする．このとき，

$$g = -(n-1) + \frac{1}{2}\sum_{i=1}^{r} \mathrm{ind}(C_i)$$

が成り立つ．ただし $\mathrm{ind}(C_i)$ は，C_i が互いに素な k 個のサイクルの積で表されるとき，$\mathrm{ind}(C_i) = n - k$ である．

次に，代数体での素数の分岐を調べる方法を紹介する．主定理の証明に用いた Ore の定理を述べるため，まず Newton 多角形を定義する．

定義 2.7 ([5]). p を素数とし，$f(X) = a_n X^n + \cdots + a_1 X + a_0$ を $\mathbb{Q}_p$ 上の n 次多項式で，$a_0 \neq 0$ をみたすものとする．このとき，f の（p **進**）**Newton 多角形**を次のようにして作られる折れ線として定める：

(i) 平面 $\mathbb{R}^2$ に点 $(i, v_p(a_i))$ $(i = 0, \ldots, n)$ をとる．ここで，v_p は $a = p^k b,\ \gcd(b,p) = 1$ としたとき，$v_p(a) = k$ で定める．

(ii) (i) でとった点をいくつか直線で結んで下に凸な折れ線を作る．ただし，折れ線は $(0, v_p(a_0))$ から $(n, v_p(a_n))$ までつながっているものとし，(i) でとったすべての点は折れ線上にあるか，折れ線より上に位置しているものとする．

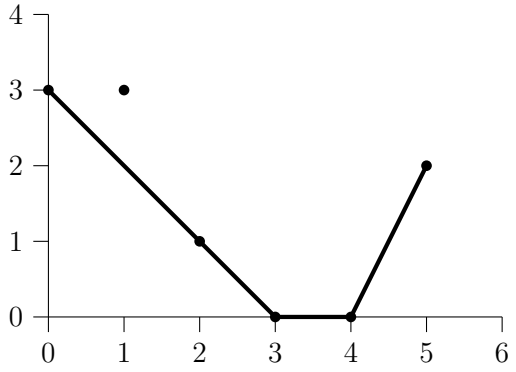

図 1　例 2.8 の f の 2 進 Newton 多角形

例 2.8. $f(X) = 4X^5 + X^4 + X^3 + 2X^2 + 8X + 8$ とし，$p = 2$ とする．このとき 2 進 Newton polygon は図 1 のようになる．

定義 2.9. p を素数，Γ を monic な多項式 $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ の p 進 Newton 多角形とし，Γ の辺のひとつを S とする． S の左端点の座標を (s, a_s) とする．S の横軸への射影の長さを E とし，縦軸への射影の長さを H とする．E と H の最大公約数を d とし，$h = H/d$, $e = E/d$ とおく．0 以上 d 以下の整数 i に対し，点 $(s + ei, v_p(a_s) - hi)$ をとる．このとき

$$b_i = \begin{cases} a_{s+ei}/p^{v_p(a_{s+ei})}, & \text{if } v_p(a_{s+ei}) = v_p(a_s) - hi, \\ 0, & \text{otherwise} \end{cases}$$

とする．これに対し，多項式 f_S を

$$f_S(Y) = \sum_{i=0}^{d} b_{d-i}Y^i$$

で定義する．これを S の **associated polynomial** とよぶ．f_S の判別式が p で割れないとき，f は S-regular であるといい，Γ のすべての辺 S に対して f が S-regular であるとき，f は Γ-regular であるという．

以上の準備の下で，次の Ore の定理が成り立つ．

定理 2.10 ([3]). *monic* な既約多項式 $f(X) \in \mathbb{Z}[X]$ とその根 θ をとり，$K = \mathbb{Q}(\theta)$, その整数環を O_K とする．素数 p をとり，f の p 進 *Newton polygon* を Γ とし，Γ の辺を $S_1, \ldots, S_l$ とする．各 S_i に対し，自然な射 $\mathbb{Z} \to \mathbb{F}_p$ によって f_{S_i} の係数を法 p で還元したものを $\overline{f_{S_i}}$ とし，$\mathbb{F}_p[X]$ 内での $\overline{f_{S_i}}$ の既約分解を

$$\overline{f_{S_i}}(X) = \varphi_{i,1}(X)^{e_{i,1}} \cdots \varphi_{i,k_i}(X)^{e_{i,k_i}}$$

とする．また，各 S_i の X 軸，Y 軸への射影の長さをそれぞれ E_i, H_i, その最大公約数を d_i とし，さらに $e_i = E_i/d_i$ とする．このとき p は K 内で

$$pO_K = \mathfrak{A}_1^{e_1} \cdots \mathfrak{A}_l^{e_l}$$

と分解され，さらに f が S_i-*regular* であるとき，

$$\mathfrak{A}_i = \mathfrak{p}_{i,1}^{e_{i,1}} \cdots \mathfrak{p}_{i,k_i}^{e_{i,k_i}}$$

と素イデアル分解される．

3 主定理と例

(1) の多項式 F を $t \in \mathbb{Q}$ で特殊化した多項式 $F(t; X)$ で定義される代数体を K_t とし，その $\mathbb{Q}$ 上の Galois 閉包, すなわち $F(t; X)$ の分解体を $\widetilde{K_t}$ とする．ここで, $\mathrm{Gal}(\widetilde{K_t}/\mathbb{Q})$ は $\mathrm{PGL}(2, 7)$ であると仮定する．本研究の主結果は次の定理である．

定理 3.1. n を 6 と互いに素な整数とし，m を $7n$ と互いに素な整数とする．このとき次が成り立つ：

(i) $(7^7n^6 + 108m^7)/p$ が平方数となるような素数 p が存在するとき，$t = 7^7n^6/m^7$ とすれば $K_t/\mathbb{Q}$ は p 外不分岐である．

(ii) $t = 7^7n^3/m^7$ とすれば，$\widetilde{K_t}/\mathbb{Q}$ はただひとつの 2 次部分体上不分岐な PGL(2, 7) 拡大である．

以下に主結果の証明の概略を述べる．

まず，PGL(2, 7) 拡大での素数の分解群と惰性群を考えることで，次の補題を得る．

補題 3.2. p を素数とする．p が $\widetilde{K_t}/\mathbb{Q}$ で不分岐であることと，$K_t/\mathbb{Q}$ で不分岐であることは同値である．また，p が $K_t/\mathbb{Q}$ で *tame* に分岐するとき，p の上の $\mathbb{Q}(\sqrt{D_{K_t}})$ の素イデアルが $\widetilde{K_t}/\mathbb{Q}(\sqrt{D_{K_t}})$ で不分岐である必要十分条件は $v_p(D_{K_t}) = 0$ または 3 であることである．

この補題により，定理 3.1 を示すためには，$K_t/\mathbb{Q}$ での素数の分岐を調べれば十分であることがわかる．

簡単のため，$m = 1$, すなわち t が整数であると仮定する．多項式 (1) の X に関する判別式が $-7^7T^5(T + 108)^3$ であることから，7, 及び t と $t + 108$ の素因数について調べれば良い．7 と t に関しては，Ore の定理を用いることで次の命題が得られる．

命題 3.3. t を 6 と互いに素な整数とする．p を t の 7 でない素因数としたとき，$(6, v_p(t)) = 3 \Leftrightarrow v_p(D_{K_t}) = 3$ であり，$(6, v_p(t)) = 6 \Leftrightarrow v_p(D_{K_t}) = 0$ である．さらに 7^7 が t を割り切るとき，$(6, v_7(t)-1) = 3 \Leftrightarrow v_7(D_{K_t}) = 3$ であり，$(6, v_7(t)-1) = 6 \Leftrightarrow v_7(D_{K_t}) = 0$ である．

$t + 108$ に関しては次の命題が得られる．

命題 3.4. t を 0 でない整数とし，$(t + 108, 42) = 1$ とする．素数 p が $t + 108$ を割り切るとき，$v_p(D_{K_t}) \leq 3$ で，$v_p(D_{K_t}) = 0$ であることの必要十分条件は $v_p(t + 108)$ が偶数であることである．

この命題は Dedekind による多項式の分解と素数の分解に関する定理と Hensel の補題を用いることで証明できる．

命題 3.3, 3.4 により，定理 3.1 の $m = 1$ の場合についての証明が完了した．m が一般の場合については，Ore の定理を $\mathbb{Q}$ 係数の場合に拡張したものを考える必要がある．実際 Ore の定理は多項式が $\mathbb{Q}$ 係数の場合にも成立することが確認でき，命題 3.3, 3.4 は $t \in \mathbb{Q}$ の場合にも同様の結果が証明できる．定理 3.1 を証明するためには，さらに m の素因数についても考える必要がある．再び Ore の定理を用いることで，次の命題を得る．

命題 3.5. n, m, t を定理 *3.1* と同じものとし，p を m の素因数とする．p が $K_t/\mathbb{Q}$ で不分岐であるための必要十分条件は $v_p(m)$ が 7 で割り切れることである．さらに p が $K_t/\mathbb{Q}$ で分岐するとき，$v_p(D_{K_t}) = 6$ である．

最後に，定理 3.1 の適用例を与える．定理の条件を満たす t に対して K_t の判別式を計算し，定理の結果を確認する．

表 1　定理 3.1 (i) の例

n	m	$D_{K_{7^7n^6/m^7}}$
1	-12	13869011721^3
1	-11	184151637^3
1	-5	145053^3
1	-4	1945929^3
1	-3	-11627^3
1	-2	-1809719^3
1	1	-1823651^3
1	2	-1837367^3
1	10	-11080823543^3
1	12	-13870658807^3
5	-9	-112351298723^3
5	3	-112868095571^3
5	6	-112898092463^3
5	8	-113094351791^3
5	12	-116737694639^3
7	-6	-196858777319^3
7	-2	-196888996583^3
7	3	-196889246603^3
7	4	-196890779879^3
7	8	-197115502823^3
11	-13	-114521798207873
11	-4	-114589548911513
11	-2	-114589566467993
11	6	-114589868937113
11	13	-114657335004593
13	-15	-139566319517873
13	-5	-139750763267873
13	-1	-139750847641793
13	3	-139750850004833

表 2　定理 3.1 (ii) の例

n	m	$D_{K_{7^7n^3/m^7}}$
1	-6	$15^3 \cdot 11^3 \cdot 31^3 \cdot 47^3 \cdot 367^3$
1	-5	145053^3
1	-4	1945929^3
1	-3	-11627^3
1	-2	-1809719^3
1	-1	$-15^3 \cdot 37^3 \cdot 4451^3$
1	1	-1823651^3
1	2	-1837367^3
1	3	$-167^3 \cdot 15817^3$
1	4	$-15^3 \cdot 89^3 \cdot 5827^3$
1	5	$-111^3 \cdot 841913^3$
1	6	$-1139^3 \cdot 223429^3$
5	-6	$-15^3 \cdot 31^3 \cdot 2345477^3$
5	-4	$-15^3 \cdot 317^3 \cdot 319159^3$
5	-3	$-15^3 \cdot 397^3 \cdot 258707^3$
5	-2	$-15^3 \cdot 73^3 \cdot 149^3 \cdot 9463^3$
5	-1	$-15^3 \cdot 79^3 \cdot 1303073^3$
5	1	$-15^3 \cdot 11^3 \cdot 13^3 \cdot 139^3 \cdot 5179^3$
5	2	$-15^3 \cdot 29^3 \cdot 41^3 \cdot 131^3 \cdot 661^3$
5	3	$-15^3 \cdot 29^3 \cdot 293^3 \cdot 12143^3$
5	4	$-15^3 \cdot 104712347^3$
5	6	$-15^3 \cdot 1481^3 \cdot 89923^3$
7	-6	$-17^3 \cdot 409^3 \cdot 616729^3$
7	-5	$-17^3 \cdot 16381^3 \cdot 16729^3$
7	-4	$-17^3 \cdot 11^3 \cdot 23^3 \cdot 1109509^3$
7	-3	$-17^3 \cdot 19^3 \cdot 859^3 \cdot 17293^3$
7	-2	$-17^3 \cdot 173^3 \cdot 65309^3$
7	-1	$-17^3 \cdot 13^3 \cdot 21728857^3$
7	1	$-17^3 \cdot 1693^3 \cdot 166849^3$
7	2	$-17^3 \cdot 313^3 \cdot 902521^3$
7	3	$-15^3 \cdot 7^3 \cdot 17^3 \cdot 857^3 \cdot 3881^3$
7	4	$-17^3 \cdot 547^3 \cdot 519643^3$
7	5	$-17^3 \cdot 290912749^3$
7	6	$-17^3 \cdot 467^3 \cdot 669611^3$

参考文献

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] M. Kida and N. Suzuki. Constructing PGL$(2,7)$-extensions with restricted ramifications. preprint.

[3] P. Llorente, E. Nart, and N. Vila. Decomposition of primes in number fields defined by trinomials. *Sém. Théor. Nombres Bordeaux (2)*, 3(1):27–41, 1991.

[4] G. Malle and B. H. Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[5] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[6] H. Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.

[7] 鈴木望夢． PGL$(2,7)$ 多項式の明示的な構成とその特殊化で得られる多項式の数論について． Master's thesis, 東京理科大学， 2023.