

ある生成的二面体群多項式の数論的性質について

東京都立大学・数学教室 小松 亨¹(Toru Komatsu)

Department of Mathematics,
Tokyo Metropolitan University

§ 1 導入.

本稿では, ある生成的巡回多項式から生成的二面体群多項式を構成しその多項式に関する数論的問題の解決について述べる. また全標数で利用可能な至る所生成的な多項式の構成についても触れる.

G を有限群とし k を体とする. r 変数有理関数体 $k(t)$, $t = (t_1, t_2, \dots, t_r)$ を係数環とする多項式環を $k(t)[X]$ と書く. 体 K 上のモニックな多項式 $F \in K[X]$ に対して K 上の F の最小分解体を $\text{Spl}_K F$ と書く.

定義 1.1. モニックな多項式 $F(t, X) \in k(t)[X]$ が次の条件を満たす時, $F(t, X)$ は G に対する k 上パラメトリックな多項式であるという.

- (i) 正則性: $\text{Spl}_{k(t)} F(t, X) \cap \bar{k} = k$ ($\bar{k}$ は k の代数的閉包),
- (ii) G 拡大: $\text{Spl}_{k(t)} F(t, X)$ が $k(t)$ のガロア拡大で $\text{Gal}(\text{Spl}_{k(t)} F(t, X)/k(t)) \simeq G$.

G に対する k 上パラメトリックな多項式 $F(t, X) \in k(t)[X]$ と k の拡大体 K に対して, K 上の F 実現射 $R_{F,K}$ を

$$R_{F,K}: \begin{array}{ccc} \mathbb{A}_K^r - \mathcal{P}_F & \rightarrow & \mathcal{G}\text{al}_K^G \\ a = (a_1, a_2, \dots, a_r) & \mapsto & \text{Spl}_K F(a, X) \end{array}$$

と定義する. ここで $\mathcal{P}_F$ を $F(t, X) = \sum_{i=0}^n c_i(t)X^i$ の係数 $c_i(t) \in k(t)$ の極集合の和集合とし, $\mathcal{G}\text{al}_K^G$ を

$$\{L/K : \text{ガロア拡大} \mid \text{Gal}(L/K) \simeq H, H : G \text{ の部分群} \}$$

とする.

定義 1.2. パラメトリックな多項式 $F(t, X) \in k(t)[X]$ が次の条件を満たす時, $F(t, X)$ は G に対する k 上生成的多項式であるという.

¹著者は日本学術振興会の援助を受けている.

(iii) 生成性: k の全ての拡大体 K に対して $R_{F,K}$ が全射.

注意 1.3. 上記の生成性の定義は DeMeyer[D] によるものである. 一方 (iii) の代わりに次の条件 (iii') で定義する流儀もある ([S] 参照).

(iii') 弱生成性: k の全ての拡大体 K に対して $R_{F,K}$ の像が gal_K^G を含む.

ここで $\text{gal}_K^G = \{L/K : \text{Gal}(L/K) \simeq G\}$ とする. 実はこの2種の定義は同値である, つまり (iii') ならば (iii) である (Kemper[Ke]).

例 1.4. (1) Artin-Schreier 多項式: 素数 p に対して $X^p - X - t$ は p 次巡回群 C_p に対する有限体 $\mathbb{F}_p$ 上の生成的多項式である.

(2) Kummer 多項式: n を正の整数とし, k を1の原始 n 乗根を持つ体とする. この時 $X^n - t$ は n 次巡回群 C_n に対する k 上の生成的多項式である.

注意 1.5. 多項式ではないが, Kummer-Artin-Schreier-Witt 理論という統一理論が関口氏と諏訪氏などによって知られている.

生成的多項式に関して次のような数論的問題が自然に考えられる.

問題 1.6. 生成的多項式 $F(t, X) \in k(t, X)$ と $a, a_1, a_2 \in A_K^* - \mathcal{P}_F$ に対して

- (1) 部分体問題: $R_{F,K}(a_1) \subseteq R_{F,K}(a_2)$ となる為の条件を a_1 と a_2 で表す.
- (2) 分岐群問題: 拡大 $R_{F,K}(a)/K$ の素イデアル $\mathfrak{p}$ での分岐群を $\mathfrak{p}$ と a から求める.

§ 2 ある生成的巡回多項式の数論.

n を3以上の整数とし, k を標数が0または n と互いに素な体とする. $\zeta \in k^{\text{sep}}$ を1の原始 n 乗根とし $\omega = \zeta^{-1} + \zeta$ とする. 以下本稿では $\omega \in k$ を仮定する.

$$F(s, X) = \frac{\zeta^{-1}(X - \zeta)^n - \zeta(X - \zeta^{-1})^n}{\zeta^{-1} - \zeta} - s \frac{(X - \zeta)^n - (X - \zeta^{-1})^n}{\zeta^{-1} - \zeta}$$

と定義する.

定理 2.1(陸名 [R]). $F(s, X)$ は C_n に対する k 上パラメトリックな多項式である. n が奇数の時 $F(s, X)$ は C_n に対する k 上生成的多項式である.

この多項式 $F(s, X)$ に関する数論的問題は以下のような議論から解決出来る ([K] 参照). k の拡大体 K に対して $\mathbb{P}_K^1 - \{\zeta, \zeta^{-1}\} = K \cup \{\infty\} - \{\zeta, \zeta^{-1}\}$ を T_K と書く. $s_1, s_2 \in T_K$ に対して

$$s_1 +_T s_2 = \frac{s_1 s_2 - 1}{s_1 + s_2 - \omega}$$

と定義する. この時 T_K は演算 $+$ を持つ 1 次元トーラスである. 整数 m に対して $s + s + \cdots + s$ (m 項和) を $[m]_T(s)$ と書き $[m]_T T_K = \{[m]_T(s) | s \in T_K\}$ とする.

定理 2.2([K]).

$$0 \rightarrow T_K/[n]_T T_K \xrightarrow{\delta} \text{Hom}_{\text{cont}}(\text{Gal}(K^{\text{sep}}/K), \mathcal{C}_n) \rightarrow \mathfrak{C} \rightarrow 0 \quad (\text{完全}),$$

ここで

$$\mathfrak{C} = \begin{cases} \text{Coker}(\text{Norm} : K(\zeta)^\times \rightarrow K^\times) & n \text{ が偶数であり } \zeta \notin K \text{ の時,} \\ 0 & \text{それ以外,} \end{cases}$$

とする.

補題 2.3. $F(s, X) = 0$ と $[n]_T X = s$ は同値. 特に $a \in K - \{\zeta, \zeta^{-1}\}$ に対して $R_{F,K}(a) = \text{Spl}_K F(a, X)$ は $(K^{\text{sep}})^{\text{Ker} \delta(a)}$ に等しい.

定理 2.2 の写像 δ の単射性から $F(s, X)$ の部分体問題が解決される.

命題 2.4. $a_1, a_2 \in K - \{\zeta, \zeta^{-1}\}$ に対して $R_{F,K}(a_1) \subseteq R_{F,K}(a_2)$ である事は

$$a_1 \in \langle a_2 \rangle_T + [n]_T T_K = \{[m]_T a_2 + [n]_T a | m \in \mathbb{Z}, a \in T_K\}$$

と同値である.

注意 2.5. 定理 2.2 の写像 δ が全射である事 ($\mathfrak{C} = 0$) は多項式 $F(s, X)$ の生成性と同値である.

注意 2.6. 小川氏も別の動機づけから定理 2.2 と同様な結果を得ている ([O] 参照).

T_K の n 等分元全体を $T_K[n]_T$ と書く.

補題 2.7. $T_K[n]_T = \langle -1 \rangle_T = \{\infty, -1, 0, \dots, \omega, \omega + 1\}$.

補題 2.8. $a \in T_K - \{\zeta, \zeta^{-1}\}$ に対して $m = \min\{j : n \text{ の正の約数 } |[j]_T a \in [n]_T T_K\}$ とすると $[R_{F,K}(a) : K] = m$ であり, $\text{Gal}(R_{F,K}(a)/K) = \langle \sigma_{n/m} \rangle$ である. また $F(a, x) = 0$ を満たす $x \in K^{\text{sep}}$ に関して $R_{F,K}(a) = K(x)$ であり, $\sigma_{n/m}(x) = x + \frac{1}{T} [n/m]_T (-1)$ である.

§ 3 二面体群多項式の構成.

多項式 $H(u, Z)$ を

$$H(u, Z) = Z^n - un^2 \prod_{1 \leq i \leq n-1} (Z - \eta_i)$$

と定義する. ここで $\eta_i = (\zeta^{-1} - \zeta)^2 / (\zeta^i + \zeta^{-i} - 2) \in k$ とする.

定理 3.1. n が奇数の時 $H(u, Z)$ は n 次二面体群 $\mathcal{D}_n$ に対する k 上生成的多項式である.

定理 3.1 の証明の概略. 今 s, u, x, z を 4 つの不定元とし関係式 $F(s, x) = 0$ 及び $H(u, z) = 0$ を満たしているとする. この時 $F(s, x)$ は s に関して 1 次多項式であるので s は x の有理式で表す事ができ, その式を $s = f(x) \in k(x)$ と書く. u, z に関しても同様に $u = h(z) \in k(z)$ とする. ここで $B(X) = X^2 - \omega X + 1 \in k[X]$ と定義し, 関係式 $B(x) = z$ を満たすとする. この時 $B(s) = u$ となる事が分かる. 以上の関係式により 4 つの関数体 $k(s), k(u), k(x), k(z)$ の間に関係が出来た.

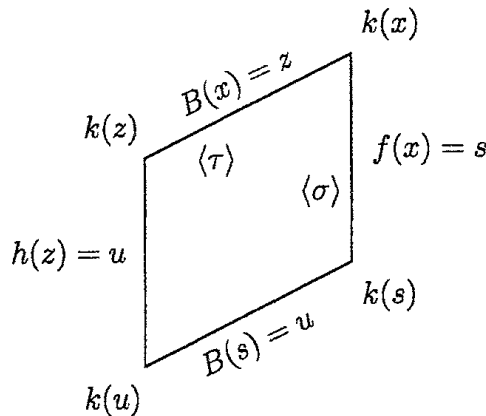


図 A

拡大 $k(x)/k(s)$ は §2 で述べたように n 次巡回拡大であり $\text{Gal}(k(x)/k(s)) = \langle \sigma \rangle$, $\sigma(x) = x + \frac{(-1)}{T} = (-x-1)/(x-1-\omega)$ である. 拡大 $k(x)/k(z)$ は 2 次巡回拡大であり $\text{Gal}(k(x)/k(z)) = \langle \tau \rangle$, $\tau(x) = [-1]_T x = -x + \omega$ である. また拡大 $k(s)/k(u)$ も 2 次巡回拡大であり $\text{Gal}(k(s)/k(u)) = \langle \tau|_{k(s)} \rangle$, $\tau(s) = [-1]_T s = -s + \omega$ である. 従って $[k(x) : k(u)] = [k(x) : k(s)][k(s) : k(u)] = 2n$ である. 体 $k(u)$ から見た $k(x)$ の共役体は $k(x)$ 自身の他に $\text{Spl}_{k(s)}(F(\tau(s), X))$ が存在する. $\tau(s) = [-1]_T(s)$ より $F(s, X) = \prod_{1 \leq i \leq n} (X - x_i)$ とした時 $F(\tau(s), X) = \prod_{1 \leq i \leq n} (X - [-1]_T x_i)$ である. よって $k(x)/k(u)$ はガロア拡大であり $\text{Gal}(k(x)/k(u)) \supseteq \langle \sigma, \tau \rangle$ である. 定義から $\# \langle \sigma \rangle = n$, $\# \langle \tau \rangle = 2$, $\sigma^i \tau = \tau \sigma^{-i}$ であるので $\langle \sigma, \tau \rangle \simeq \mathcal{D}_n$ である. 従って $[k(x) : k(u)] = \# \langle \sigma, \tau \rangle = 2n$ より $\text{Gal}(k(x)/k(u)) = \langle \sigma, \tau \rangle$ が分かる. 今 $k(z) =$

$k(x)^{(r)}$ より $k(z)/k(u)$ は非ガロア拡大であり そのガロア閉包は $k(x)$ である. 実際 $F(s, X) = \prod_{1 \leq i \leq n} (X - x_i)$ とした時 $H(u, Z) = \prod_{1 \leq i \leq n} (X - B(x_i))$ である. 従って $\text{Spl}_{k(u)} H(u, Z) = k(x)$ であり, $H(u, Z)$ は $\mathcal{D}_n$ に対する k 上パラメトリックな多項式である事が分かった. $H(u, Z)$ の生成性の証明は $F(s, X)$ の生成性を利用する. 以下 n は奇数である事に注意する. 体 K を k の拡大とし L/K はガロア拡大で $\text{Gal}(L/K) \simeq \mathcal{D}_n$ とする. この時 L/K の中間体 M で $\text{Gal}(L/M) \simeq \mathcal{C}_n$ となる体が存在する. 今 $F(s, X)$ の生成性から $\text{Spl}_M F(a, X) = L$ となる $a \in M$ が存在する. そして $B(a - \rho(a)) = c$ (ρ は $\text{Gal}(M/K)$ の生成元) とおくと, $c \in K$ であり $\text{Spl}_K H(c, X) = L$ が証明出来る. これで $H(u, Z)$ の (弱) 生成性が示された. $\square$

注意 3.2. 構成法 (図 A) から $H(u, Z)$ に関する数論的問題は $F(s, X)$ の数論的問題へ帰着出来る. 構成法が明示的である事からその帰着は容易であり, $F(s, X)$ の数論的問題は **[K]** で解決されている.

§ 4 知られている多項式との関係.

n が奇数の場合は以下の生成的巡回多項式 $P(c, Y)$ 及び生成的二面体群多項式 $R(c, Y)$ が橋本氏と三宅氏によって与えられていた (**[HM]** 参照). 本稿の多項式 $F(s, X)$ は $P(c, Y)$ の改良版である (**[R]** 参照).

$$P(c, Y) = \frac{(Y - \zeta)^n + (Y - \zeta^{-1})^n}{2} - c \prod_{0 \leq j \leq n-1} (-\xi_j Y + \xi_{j+1}),$$

$$R(c, Y) = \prod_{0 \leq j \leq n-1} (Y - \xi_j \xi_{j+1}) + c.$$

ここで $\xi_j = (\zeta^j - \zeta^{-j})/(\zeta - \zeta^{-1}) \in \mathbb{Q}$ とする.

定理 4.1(橋本-三宅 **[HM]**). 体 k は標数 0 であり n は奇数とする. この時 $P(c, Y)$ は $\mathcal{C}_n$ に対する k 上の生成的多項式である. $R(c, Y)$ は $\mathcal{D}_n$ に対する k 上の生成的多項式である.

補題 4.2. 標数 0 の体 k 上 $R(c, Y)$ と $H(u, Z)$ は同値である. つまり $R(c, Y)$ の c に u の高々 1 次分数変換を代入し, Y に Z の高々 1 次分数変換を代入した有理式の分子が $H(u, Z)$ の定数 ($k^\times$ の元) 倍に等しい.

しかし $H(u, Z)$ は前節 §3 で述べたように数論的問題を解く上で扱い易く, さらに次のような数論的応用上良い性質を持つ.

命題 4.3. n を奇素数とし $k = \mathbb{Q}(\omega)$ とする. k の拡大体 K の元 u に対して $un^2 \in O_K$ と仮定する. $z_j \in \bar{K}$ を $H(u, Z) = \prod_{1 \leq j \leq n} (Z - z_j)$ とし $L = \text{Spl}_K H(u, Z)$ とする. この時 $\{z_j - \eta_i | 1 \leq i \leq n-1, 1 \leq j \leq n\} \subset O_L^\times$.

注意 4.4. 関係式 $\prod_{1 \leq j \leq n} (z_j - \eta_i) = -\eta_i^n$ 及び $z_j - \eta_i = z_j - \eta_{n-i}$ があるので $\{z_j - \eta_i | 1 \leq i \leq n-1, 1 \leq j \leq n\}$ が乗法的に生成する $O_L^\times / O_K^\times$ の部分群の次元は高々 $(n-1)^2/2$ である.

§ 5 至る所生成的な多項式.

G を有限体とし k を有限次代数体とする. O_k の素イデアル $\mathfrak{p}$ に対して剰余体 $O_k/\mathfrak{p}$ を $\mathbb{F}_p$ と書く.

定義 5.1. モニックな多項式 $F(t, X) \in k(t)[X]$ が次の条件を満たす時, $F(t, X)$ は G に対する k 上至る所生成的な多項式であるという.

(g_0) 標数 0: $F(t, X)$ は G に対する k 上の生成的多項式,

(g_p) 正標数: O_k の全ての素イデアル $\mathfrak{p}$ に対して, $F(t, X) \bmod \mathfrak{p}$ が定義され,
 $F(t, X) \bmod \mathfrak{p}$ は G に対する $\mathbb{F}_p$ 上の生成的多項式.

$F(s, X), H(u, Z)$ を §2, 3 で扱った多項式とする. n を奇素数 l とし $k = \mathbb{Q}(\omega)$ 上の多項式 $\Omega_{C_l}(s, X), \Omega_{D_l}(u, Z)$ を

$$\Omega_{C_l}(s, X) = F(s/l, X), \quad \Omega_{D_l}(u, Z) = H(u/l^2, Z)$$

と定義する.

定理 5.2. $\Omega_{C_l}(s, X)$ は C_l に対する $\mathbb{Q}(\omega)$ 上至る所生成的な多項式である. $\Omega_{D_l}(u, Z)$ は D_l に対する $\mathbb{Q}(\omega)$ 上至る所生成的な多項式である.

補題 4.2 と同様にして $\Omega_{D_l}(u, Z)$ と $R(c, Y)$ が全標数で同値である事が分かる. 従って定理 5.2 から次が分かる.

系 5.3. $R(c, Y)$ は D_l に対する $\mathbb{Q}(\omega)$ 上至る所生成的な多項式である.

§ 6 よく知られている多項式との関係.

k を標数 0 の体とする. $\text{cheb}(Y)$ を n 次の Chebyshev 多項式とする,

$$\text{cheb}(Y) = \cos(n \cos^{-1}(Y)) = (-2)^{n-1} \prod_{0 \leq j \leq n-1} \left(Y - \frac{\zeta^j + \zeta^{-j}}{2} \right) + 1.$$

補題 6.1. 多項式 $H(u, Z)$ と $\text{cheb}(Y) - t$ は k 上同値である.

系 6.2. $\text{cheb}(Y) - t$ は $\mathcal{D}_n$ に対する $\mathbb{Q}(\omega)$ 上生成的な多項式である.

注意 6.3. 体 $\text{Spl}(X^n - t)$ に ζ が含まれる事と同様にして体 $\text{Spl}(\text{cheb}(Y) - t)$ に ω が含まれる.

拡大 $\text{Spl}_{k(t)}(\text{cheb}(Y) - t)/k(t)$ の中間体は $t = \cos \theta$ の場合に制限すると次のように表す事が出来る. ここで $\psi(X) = (X + \omega^2/2 - 2)/X$, $\beta = \psi \circ B$ とし, $\sigma(\theta) = \theta + 2\pi$, $\tau(\theta) = -\theta$ である.

$$\begin{array}{c}
 y = \cos \frac{\theta}{n} \quad k(y) \quad \beta(x) = y \quad k(x) \quad x = \frac{\sin(\frac{\theta}{2n} - \frac{2\pi}{n})}{\sin \frac{\theta}{2n}} \\
 \text{cheb}(y) = t \quad \langle \tau \rangle \quad f(x) = s \\
 t = \cos \theta \quad k(t) \quad \beta(s) = t \quad k(s) \quad s = \frac{\sin(\frac{\theta}{2} - \frac{2\pi}{n})}{\sin \frac{\theta}{2}}
 \end{array}$$

§ 7 例.

(1) $l = 3$ の時 $\omega + 1 = 0$, $\eta_1 = 1$ である.

$$\begin{aligned}
 \Omega_{\mathcal{C}_3}(s; X) &= X^3 - sX^2 - (s+3)X - 1, \\
 \Omega_{\mathcal{D}_3}(u; Z) &= Z^3 - u(Z-1)^2 \\
 &= Z^3 - uZ^2 + 2uZ - u, \\
 \Omega_{\mathcal{D}_3}(u; Z + \eta_1) &= (Z+1)^3 - uZ^2 \\
 &= Z^3 - (u-3)Z^2 + 3Z + 1.
 \end{aligned}$$

(2) $l = 5$ の時 $\omega^2 + \omega - 1 = 0$, $\eta_1 = \omega + 2$, $\eta_2 = 1$ である.

$$\begin{aligned}
 \Omega_{\mathcal{C}_5}(s; X) &= X^5 - sX^4 + 2(\omega s - 5)X^3 + 2\omega(s+5)X^2 - (s-5\omega)X - 1, \\
 \Omega_{\mathcal{D}_5}(u; Z) &= Z^5 - u(Z - (\omega+2))^2(Z-1)^2 \\
 &= Z^5 - uZ^4 + 2(\omega+3)uZ^3 - 7(\omega+2)uZ^2 + 2(4\omega+7)uZ \\
 &\quad - (3\omega+5)u, \\
 \Omega_{\mathcal{D}_5}(u; Z + \eta_1) &= (Z + \omega + 2)^5 - uZ^2(Z + \omega + 1)^2 \\
 &= Z^5 - (u - 5(\omega+2))Z^4 - (2(\omega+1)u - 10(3\omega+5))Z^3 \\
 &\quad - ((\omega+2)u - 10(8\omega+13))Z^2 + 5(21\omega+34)Z + 55\omega + 89, \\
 \Omega_{\mathcal{D}_5}(u; Z + \eta_2) &= (Z+1)^5 - u(Z - (\omega+1))^2Z^2 \\
 &= Z^5 - (u-5)Z^4 + (2(\omega+1)u+10)Z^3 - ((\omega+2)u-10)Z^2 \\
 &\quad + 5Z + 1.
 \end{aligned}$$

(3) $l = 7$ の時 $\omega^3 + \omega^2 - 2\omega - 1 = 0$, $\eta_1 = \omega + 2$, $\eta_2 = 1$, $\eta_3 = -2\omega^2 - \omega + 5$ である.

$$\Omega_{C_7}(s; X) = X^7 - sX^6 + 3(\omega s - 7)X^5 - 5((\omega^2 - 1)s - 7\omega)X^4 \\ - 5(\omega^2 - 1)(s + 7)X^3 + 3(\omega s - 7(\omega^2 - 1))X^2 - (s - 7\omega)X - 1,$$

$$\Omega_{D_7}(u; Z) = Z^7 - u(Z - (\omega + 2))^2(Z - 1)^2(Z - (-2\omega^2 - \omega + 5)) \\ = Z^7 - uZ^6 - 4(\omega^2 - 4)uZ^5 + 6(5\omega^2 + \omega - 15)uZ^4 \\ - 30(3\omega^2 + \omega - 8)uZ^3 + 11(12\omega^2 + 5\omega - 30)uZ^2 \\ - 2(47\omega^2 + 22\omega - 113)uZ + (26\omega^2 + 13\omega - 61)u,$$

$$\Omega_{D_7}(u; Z + \eta_2) = (Z + 1)^7 - u(Z - (\omega + 1))^2Z^2(Z - (-2\omega^2 - \omega + 4)) \\ = Z^7 - (u - 7)Z^6 - ((4\omega^2 - 10)u - 21)Z^5 \\ + ((10\omega^2 + 6\omega - 25)u + 35)Z^4 \\ - ((10\omega^2 + 6\omega - 20)u - 35)Z^3 \\ + ((2\omega^2 + \omega - 5)u + 21)Z^2 + 7Z + 1.$$

References

- [D] F. R. DeMeyer, *Generic polynomials*, J. Algebra **84** (1983), 441–448.
- [HM] K. Hashimoto, K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications (Kyoto, 1997), 165–181, Dev. Math., 2, Kluwer Acad. Publ., Dordrecht, 1999.
- [HR] K. Hashimoto, Y. Rikuna, *On generic families of cyclic polynomials with even degree*, Manuscripta Math. **107** (2002), 283–288.
- [Ke] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141.
- [K] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), 265–279.
- [O] H. Ogawa, *Quadratic reduction of multiplicative group and its applications*, (Japanese) Algebraic number theory and related topics (Kyoto, 2002). Surikaisekikenkyusho Kokyuroku **1324** (2003), 217–224.
- [R] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), 2215–2218.
- [S] D. J. Saltman, *Generic Galois extensions*, Proc. Nat. Acad. Sci. U.S.A. **77** (1980), 1250–1251.

小松 亨

〒192-0397 東京都八王子市南大沢 1-1

東京都立大学大学院理学研究科数学教室

E-mail: trkomatu@comp.metro-u.ac.jp

Toru Komatsu

Department of Mathematics, Tokyo Metropolitan University,

1-1 Minami-Osawa, Hachioji-shi, Tokyo 192-0397, Japan.