P−1

2 次多項式の合成による既約多項式の構成

Construction of irreducible polynomials by composition of quadratic polynomials

◯若林岳洋 [1]
*Takehiro Wakabayashi[1]

Abstract: We construct irreducible polynomials in semigroups generated by quadratic polynomials under composition. We use an irreducibility test of Capelli, Siegel's theorem on integral points, as well as known results of arithmetic dynamics of quadratic polynomials.

1. はじめに

多項式が $\mathbb{Q}$ 上既約であることを単に**既約**であるということにする．ϕ の N 重合成を $\phi^{\circ N}$ で表す．ある $N \in \mathbb{N}$ に対し $\phi^{\circ N}(P) = P$ をみたす $P \in \mathbb{Q}$ を ϕ の $\mathbb{Q}$ 上の**周期点**といい，ϕ の $\mathbb{Q}$ 上の周期点全体の集合を $\mathrm{Per}(\phi, \mathbb{Q})$ で表す．ある $N \in \mathbb{Z}_{\geq 0}$ に対し $\phi^{\circ N}(P) \in \mathrm{Per}(\phi, \mathbb{Q})$ をみたす $P \in \mathbb{Q}$ を ϕ の $\mathbb{Q}$ 上の**前周期点**といい，ϕ の $\mathbb{Q}$ 上の前周期点全体の集合を $\mathrm{PrePer}(\phi, \mathbb{Q})$ で表す．

定義 1. 2 次多項式 $\phi_1 = x^2 + c_1, \phi_2 = x^2 + c_2$ に対し，ϕ_1, ϕ_2 が **exceptional pair** であるとは，
(1) ϕ_1 と ϕ_2 はともに有理平方である周期点をもつ．
(2) $\phi_1(\mathbb{Z}) \cap \mathrm{PrePer}(\phi_2, \mathbb{Q})$ と $\phi_2(\mathbb{Z}) \cap \mathrm{PrePer}(\phi_1, \mathbb{Q})$ はともに空でない．
をともにみたすことである．

次が本稿の主定理である．これは [1, Theorem 1.1] の証明から得られる主張である．

定理 2. $c_1, \ldots, c_s$ を異なる整数，$S = \{x^2 + c_1, \ldots, x^2 + c_s\}$ とし，$\phi_1 = x^2 + c_1, \phi_2 = x^2 + c_2$ が既約とする．また，ϕ_1, ϕ_2 は exceptional pair でないと仮定する．合成を演算として S によって生成される半群を M_S で表す．このとき $N \geq 2$ が存在し，$\{\phi_1^{\circ N} \circ \phi_2 \circ F \mid F \in M_S\}$ は既約多項式の集合となる．

注意 3. ϕ_1, ϕ_2 が exceptional pair であることと，c_1, c_2 のペア (c_1, c_2) か (c_2, c_1) が，$(-1, -3)$ またはある $s \in \mathbb{Z}$ に対して $(s^2 - s^4, -1 - s^2 - s^4)$ をみたすことは同値であることが知られている ([1, Theorem 1.2])．S が exceptional pair である既約多項式 ϕ_1, ϕ_2 を含む場合でも，定理 2 は成り立つが，一部別議論が必要である．

2. 定理 2 を示す準備

定義 4. $f_i \in S (1 \leq i \leq n)$ に対し，$g_n = f_1 \circ \cdots \circ f_n \in M_S$ の **adjusted critical orbit** とは，

$$-g_1(0), g_2(0), g_3(0), \ldots, g_n(0)$$

のことである．

命題 5 ([1, Proposition 2.1])**.** K は標数 2 でない体とする．ある $c_1, \ldots, c_n \in K$ に対し $f_i(x) = x^2 + c_i \in S$ とし，$g_n = f_1 \circ \cdots \circ f_n$ とおく．g_n の adjusted critical orbit が K における平方数でないならば，g_n は K 上既約である．

証明. 数学的帰納法．$n = 1$ のとき，$-g_1(0) = -c_1$ が K における平方数でなければ，$g_1(x) = x^2 - (-c_1)$ は K 上既約な 2 次多項式である．$n \geq 2$ に対して，$n - 1$ まで主張が成り立ち，$-g_1(0), g_2(0), \ldots, g_n(0)$ が K における平方数でないと仮定する．帰納法の仮定より，$g_{n-1}(x)$ は K 上既約である．いま $\alpha \in \bar{K}$ を $g_{n-1}(x)$ の任意の根とし，$f_n(x) - \alpha$ が $K(\alpha)$ 上可約だと仮定する．このとき $\alpha - c_n$ は $K(\alpha)$ における平方数である．一方，$g_{n-1}(x)$ は K 上既約なので，モニック多項式 $g_{n-1}(x + c_n) \in K[x]$ は $\alpha - c_n$ の K 上の最小多項式だとわかる．よって，ノルムを計算すると，$N_{K(\alpha)/K}(\alpha - c_n) = N_{K(\alpha - c_n)/K}(\alpha - c_n) = (-1)^{2^{n-1}} g_{n-1}(0 + c_n) = g_{n-1}(f_n(0)) = g_n(0)$．ここで，平方数のノルムは平方数であることに注意すると，$g_n(0)$ は K における平方数となる．これは仮定に反するので，$f_n(x) - \alpha$ は $K(\alpha)$ 上既約である．従って，次の Capelli の補題により，$g_n = g_{n-1} \circ f_n$ は K 上既約となる．　□

補題 6 (Capelli の補題)**.** K を体，$f, g \in K[x], \beta \in \bar{K}$ を f の根とする．このとき $f \circ g$ が K 上既約であることと，f が K 上既約かつ $g - \beta$ が $K(\beta)$ 上既約であることは同値．

定義 7. $P \in \mathbb{P}^N(\mathbb{Q})$ に対し，P の**高さ**とは，$h(P) = \log \max |x_i|$ のことである．ここで，$P = [x_0 : \cdots : x_N]$ で $x_i \in \mathbb{Z}$ と $\gcd(x_0, \ldots, x_N) = 1$ をみたす．$\phi : \mathbb{P}^N(\mathbb{Q}) \to \mathbb{P}^N(\mathbb{Q})$ を次数 $d \geq 2$ の射とする．このとき，任意の $P \in \mathbb{P}^N(\mathbb{Q})$ に対して $\hat{h}_\phi(P) = \lim_{n \to \infty} \frac{h(\phi^{\circ n}(x))}{d^n}$ と定めると極限は存在する．この $\hat{h}_\phi$ を ϕ に関する**標準的高さ**という．

補題 8 ([1, Lemma 3.1])**.** ある $c \in \mathbb{Z} \backslash \{0, -1\}$ に対し $\phi(x) = x^2 + c$ とする．このとき $N = N_\phi \geq 2$ が存在し，$a \in \mathbb{Z}$ に対して $\phi^{\circ N}(a)$ が平方数ならば，$\phi^{\circ N}(a)$ は周期点となる．

1: 日大理工・院 (前)・数学

証明. まず超楕円曲線 $C_\phi : Y^2 = \phi^{\circ 2}(X) = X^4 + 2cX^2 + c^2 + c$ を考える．$\phi^{\circ 2}$ の判別式は $4^4c^2(c^2+c)$ であり，$c \neq 0, -1$ なので 0 にならない．よって，C の種数は 1 である．Siegel の定理より，C は有限個の整数点をもつ．従って，ある $x, y \in \mathbb{Z}$ に対して $(x, y) \in C$ ならば，$\hat{h}_\phi(x) < B$ をみたす正の定数 B が選べる．Northcott の定理より，$\hat{h}^{\min}_{\phi,\mathbb{Q}} = \min\{\hat{h}_\phi(b) \mid b \in \mathbb{Q}, \hat{h}_\phi(b) > 0\}$ は 0 より大きい値になる．次に，必要があれば B を大きく取り直して $B \geq \hat{h}^{\min}_{\phi,\mathbb{Q}}$ とし，$N = N_\phi = \lceil \log_2 \frac{B}{\hat{h}^{\min}_{\phi,\mathbb{Q}}} \rceil + 2$ と定める．$N_\phi \geq 2$ である．ここで，ある $y \in \mathbb{Z}$ を用いて $\phi^{\circ N}(a) = y^2$ と表せるなら，$(X, Y) = (\phi^{\circ (N-2)}(a), y)$ は C 上の整数点であり，

$$B > \hat{h}_\phi(\phi^{\circ (N-2)}(a)) = 2^{N-2}\hat{h}_\phi(a) \tag{1}$$

をみたす．

$a \notin \mathrm{PrePer}(\phi, \mathbb{Q})$ とすると，[4, Theorem 3.22] より $\hat{h}_\phi(a) > 0$．よって，$\hat{h}^{\min}_{\phi,\mathbb{Q}} \leq \hat{h}_\phi(a)$ となるので，(1) より $N < \log_2 \frac{B}{\hat{h}^{\min}_{\phi,\mathbb{Q}}} + 2$ となる．しかし，これは $N = \lceil \log_2 \frac{B}{\hat{h}^{\min}_{\phi,\mathbb{Q}}} \rceil + 2 \geq \log_2 \frac{B}{\hat{h}^{\min}_{\phi,\mathbb{Q}}} + 2$ に反する．従って，$a \in \mathrm{PrePer}(\phi, \mathbb{Q})$ である．[4, Exercise 2.20] より，$\phi \in \mathbb{Z}[x] (\deg \phi \geq 2)$ がモニックで $P \in \mathrm{Per}(\phi, \mathbb{Q})$ ならば，$P \in \mathbb{Z}$ かつ P の周期は $1, 2, 4$ のいずれかである．[2, Theorem 4] より，$x^2 + c \in \mathbb{Q}[x]$ は周期 4 の有理周期点をもたない．従って，$\phi(x) = x^2 + c \in \mathbb{Z}[x]$ のすべての有理周期点は整数点であり，周期は 1 か 2 である．次に [3, Theorem 3, (6)] より，$\phi^{\circ 2}(a)$ は周期点となる．よって，$N \geq 2$ なので $\phi^{\circ N}(a) \in \mathbb{Z}$ は周期点となる．□

命題 9 ([1, Proposition 3.2])**.** 異なる $c_1, c_2 \in \mathbb{Z}\backslash\{0, -1\}$ に対して $\phi_1(x) = x^2 + c_1, \phi_2(x) = x^2 + c_2$ とする．さらに ϕ_1, ϕ_2 は exceptional pair でないと仮定する．このとき，次のうち少なくとも 1 つが成り立つ．

(1) $N \geq 2$ が存在し，任意の $b \in \mathbb{Z}$ に対して $\phi_1^{\circ N}(\phi_2(b))$ は (有理) 平方数でない．

(2) $N \geq 2$ が存在し，任意の $b \in \mathbb{Z}$ に対して $\phi_2^{\circ N}(\phi_1(b))$ は (有理) 平方数でない．

証明. ϕ_1, ϕ_2 に対して，それぞれ補題 8 のような自然数 N_1, N_2 をとる．命題 9 の (1) と (2) がともに成り立たないとすると，$b_1, b_2 \in \mathbb{Z}$ が存在し，$\phi_1^{\circ N_1}(\phi_2(b_1))$ と $\phi_2^{\circ N_2}(\phi_1(b_2))$ がともに (有理) 平方数となる．よって，$a_1 = \phi_2(b_1), a_2 = \phi_1(b_2)$ とおくと，補題 8 より $\phi_1^{\circ N_1}(a_1), \phi_2^{\circ N_2}(a_2)$ は，それぞれ ϕ_1, ϕ_2 の周期点．さらに，$a_1 \in \phi_2(\mathbb{Z}) \cap \mathrm{PrePer}(\phi_1, \mathbb{Q})$ かつ $a_2 \in \phi_1(\mathbb{Z}) \cap \mathrm{PrePer}(\phi_2, \mathbb{Q})$ である．従って，ϕ_1, ϕ_2 は exceptional pair であるが，これは矛盾．□

補題 10 ([1, Lemma 3.4])**.** ある $c \in \mathbb{Z}\backslash\{0, -1\}$ に対し，$\phi(x) = x^2 + c$ を既約とする．このとき，任意の $n \geq 1$ に対し $\phi^{\circ n}$ の adjusted critical orbit は (有理) 平方数でない．

証明. $\phi(x) = x^2 + c$ が既約なので，$-c$ は平方数でない．$c_1 = -c$, $c_{i+1} = \phi(c_i)$ とおく $(i \geq 1)$．このとき，$c_{i+1} = \phi(c_i) = \cdots = \phi^{\circ i}(c_1) = \phi^{\circ i}(-c) = \phi^{\circ i}(c) = \phi^{\circ (i+1)}(0)$ が成り立つ．よって，$c_i (1 \leq i \leq n)$ は $\phi^{\circ n}$ の adjusted critical orbit である．

まず，任意の $i (1 \leq i \leq n)$ に対して $c_i \geq |c|$ が成り立つことを示す．$i = 1$ のときは $c_1 = -c$ なので明らか．$c_{i-1} \geq |c|$ が成り立つと仮定すると，i のとき，$c_i = \phi(c_{i-1}) = c_{i-1}^2 + c \geq |c|^2 + c$ となる．ここで，$c > 0$ のときは $|c|^2 + c = |c|^2 + |c| > |c|$．よって，$|c_i|^2 = c_i^2 < c_i^2 + c = c_{i+1} = c_i^2 + |c| < c_i^2 + |c_i| = |c_i|^2 + |c_i| = |c_i|(|c_i| + 1) < (|c_i| + 1)^2$ となる．しかし，連続する 2 つの整数の 2 乗の間に平方数はないので，$c_{i+1} (1 \leq i \leq n-1)$ は平方数でない．$c \leq -2$ のときは $|c|^2 + c = |c|^2 - |c| = |c|(|c| - 1) \geq |c|$．よって，$|c_i|^2 > |c_i|^2 + c = c_i^2 + c = c_{i+1} = |c_i|^2 - |c| \geq |c_i|^2 - |c_i| = |c_i|(|c_i| - 1) > (|c_i| - 1)^2$ となる．上と同様の議論より，$c_{i+1} (1 \leq i \leq n-1)$ は平方数でない．よって，$c_i (1 \leq i \leq n)$ は平方数でない．□

3. 定理 2 の証明

証明. まず $c_1, c_2 \in \mathbb{Z}\backslash\{0, -1\}$ である．なぜなら，もし $c_i = 0, -1$ だと $\phi_i = x^2 = x \cdot x$, $x^2 - 1 = (x+1)(x-1)$ となり，ϕ_i の既約性に反する．

ϕ_1, ϕ_2 が exceptional pair でないので，命題 9 より (必要があれば添え字をつけ直して) 自然数 $N \geq 2$ が存在し，

$$\text{任意の } b \in \mathbb{Z} \text{ に対して} \phi_1^{\circ N} \circ \phi_2(b) \text{ は平方数でない．} \tag{2}$$

ここで，$f = \phi_1^{\circ N} \circ \phi_2 \circ F$ の adjusted critical orbit を考える．まず，補題 10 より $-\phi_1(0) = -c_1, \phi_1^{\circ 2}(0), \ldots, \phi_1^{\circ N}(0)$ は平方数でない．また，(2) より，$\phi_1^{\circ N}(\phi_2(0)), \phi_1^{\circ N}(\phi_2(F(0)))$ は平方数でない ($F \in \mathbb{Z}[x]$ に注意)．よって，命題 5 より，$f = \phi_1^{\circ N} \circ \phi_2 \circ F$ は既約．□

4. 参考文献

[1] W. Hindes, R. Jacobs, P. Ye, Irreducible polynomials in quadratic semigroups, Journal of Number Theory, Vol. 248: 208-241, 2023.

[2] P. Morton, Arithmetic properties of periodic points of quadratic maps, II, Acta Arith. 87 (2): 89-102, 1998.

[3] B. Poonen, The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture. Math. Z. 228: 11-29, 1998.

[4] J. H. Silverman, The Arithmetic of Dynamical Systems, vol. 241, Springer GTM, New York, 2007.