数式処理 *J.JSSAC (2005)*
Vol. 11, No. 3,4, pp. 69 - 75

Noda2005 論文

一変数有理函数の函数合成積への分解について

村上 弘*

東京都立短期大学 経営情報学科

概　要

We consider the problem of the following: for the given non-constant univariate function F, determine whether there exist functions F_1 and F_2 such that $F = F_1 \circ F_2$ i.e. $F(x) = F_1(F_2(x))$ and if they exist construct them explicitly. This problem must be associated with a set of condition to what class of function for each F, F_1 and F_2 belongs. Solution for the following cases have already been known:

(1) F is a polynomial function and both F_1 and F_2 are also polynomial functions.
(2) F is a rational function and both F_1 and F_2 are also rational functions.

In this paper, in a manner as elementary as possible, the following two cases are treated:

(3) F is a rational function and F_1 is a rational function and F_2 is polynomial.
(4) F is a rational function and F_1 is a polynomial and F_2 is a rational function.

1　はじめに

「多項式を多項式の合成積に分解する問題」，および「有理函数を有理函数の合成積に分解する問題」は，参考文献に挙げたいくつかの論文により，既に解法が与えられている．

「多項式を多項式の合成積に分解する問題」については，[1, 13, 6, 8, 9, 2, 5, 12] ，および「有理函数を有理函数の合成積に分解する問題」については，[2, 4, 15, 14, 10] がある．更に「代数函数の分解の問題」については [7] がある．

本論文では，やや制限の強い形である「有理函数の多項式と有理函数の合成への分解」および「有理函数の有理函数と多項式の合成への分解」を見出す方法を扱う．問題の解法は初等的で具体的に構成が可能な方法として記述した．

2　有理函数の分解（有理函数と多項式の合成積への）

定数ではない有理函数 R が与えられたとき，有理函数 R_1 と多項式 P の合成積 $R = R_1 \circ P$ に分解できるか判定し，可能であるならば構成する問題を扱う．

まず R_1, P は定数ではないことはすぐにわかる．有理函数 R が互いに素な多項式 N, D により分数式として $R(x) \equiv N(x)/D(x)$ と書けて，有理函数 R_1 が互いに素な多項式 A, B により分数式と

*murakami@tmca.ac.jp

して，$R_1(y)\equiv A(y)/B(y)$ と書かれるとする．（但し，D, B は monic に規格化してあるとする．）合成積の関係を表すと，

$$\frac{N(x)}{D(x)} = \frac{A(P(x))}{B(P(x))}$$

である．$A(y), B(y)$ は互いに素な y の多項式だから，y の適当な多項式 $\alpha(y), \beta(y)$ をとると，$\alpha(y)A(y) + \beta(y)B(y) = 1$ が成り立つ．すると $\alpha(P(x))A(P(x)) + \beta(P(x))B(P(x)) = 1$ だから，x の多項式として $A(P(x))$ と $B(P(x))$ は互いに素であることがわかる．$N(x)$ と $D(x)$ も互いに素だから，適当な非零の定数 ρ により $N(x) = \rho\cdot A(P(x))$，$D(x) = \rho\cdot B(P(x))$ と書ける．

可逆一次変換による不定性を除く為に，P は monic で定数項は 0 と制限しよう．分母の多項式 $D(x)$, $B(x)$ も monic に規格化されていると仮定してある．すると，$D(x)$ と $\rho\cdot B(P(x))$ の主係数の比較から $\rho = 1$ だから，$N(x) = A(P(x))$，$D(x) = B(P(x))$ となる．

以上のことから「与えられた有理函数 R が有理函数 R_1 と多項式 P の合成積として $R = R_1\circ P$ と分解できるか」という問題は，「R の分子と分母の多項式 N と D が共通の多項式 P を右側因子に持つ多項式の合成積として分解できるか」，すなわち $N = A\circ P, D = B\circ P$ となるような多項式 A, B, P の組合せがあるかという問題に帰着する．（多項式の合成積分解の決定法は既に解決済みである．）

次数の比較からは $\deg N = \deg A\cdot \deg P$，$\deg D = \deg B\cdot \deg P$ が必要である．合成積演算の単元である一次多項式は含めないので $\deg(P) > 1$ とする．$\deg P$ を $\gcd(\deg N, \deg D)$ の約数として可能性をすべて列挙して仮定し，N と D の多項式としての合成積分解が共通な右側因子の多項式 P により $N = A\circ P, D = B\circ P$ と書けたとする．そのとき $R_1(y) = A(y)/B(y)$ と置くと，与えられた有理函数 $R(x) = N(x)/D(x)$ は合成積への分解 $R = R_1\circ P$ を持つ．

注意:多項式 N, D, P の x による微分を N_x, D_x, P_x と書き，$A(y), B(y)$ の y による微分を A_y, B_y と書くと，$N_x(x) = P_x(x)A_y(P(x))$, $D_x(x) = P_x(x)B_y(P(x))$ であるから P_x は $G\equiv \gcd_x(N_x, D_x)$ の因子でなければならない．

以下，議論の簡単の為に体の標数は 0 とする．例えば，多項式 G が定数ならば P_x は高々一次多項式であり，分解は自明なものになる．ランダムに選ばれた多項式 N, D に対しては，ほとんどの場合に G は定数となるから，この予備試験は効率が良い．多項式 G の次数が低い場合には，G の因数分解も手間が少ないので G を割り切る因子として P_x の候補を列挙し調べることも考えられる．その場合の候補は，条件 $\deg P_x + 1 = \deg P(> 1)$ が $\gcd(\deg N, \deg D)$ の約数である，を満たすものに限定できる．P の定数項は 0 だから P_x から P が決まる．

3 有理函数の分解（多項式と有理函数の合成積への）

今度は，ある与えられた定数函数ではない有理函数 R が多項式 P と有理函数 R_2 の合成積 $R = P\circ R_2$ として表せるかという問題を扱う．

R が互いに素な多項式 N, D により $R(x)\equiv N(x)/D(x)$ と書かれるとし，さらに R_2 も互いに素な多項式 A, B により $R_2(x)\equiv A(x)/B(x)$ と書かれるとする．多項式の係数は体 K に含まれるとする．一般性を失わずに分母の多項式 D, B は monic とする．

3.1 問題は $\deg N \leq \deg D$ に制限できる

最初から $\deg N \leq \deg D$ なら何もしなくてよい.

そこで $\deg N > \deg D$ とする．その場合には，分母の定数項が非零なら $x' = x$ とし，分母の定数項が零ならば x の適当なシフト $x' = x - x_0$ を行なって分母の定数項を非零にする．その後に $x' = 1/t$ と置いて R を変換した有理函数 $R'(t)$ は，t についての分子の次数が分母の次数以下となる．（注意:ここでのプライムは導函数を意味しない）

証明　$x' = x - x_0$ により $N(x) = N'(x')$, $D(x) = D'(x')$, $\deg N' = \deg N$, $\deg D' = \deg D$. さらに $N'(x')$ は x' の丁度 δ-巾 ($\delta \geq 0$) で割り切れるとすると $N'(x') = N'(1/t) = N''(t)/t^{\deg N}$, $\deg N'' = \deg N - \delta$ で，$N''(t)$ の定数項は非零．また $D'(x')$ は構成より定数項が非零で x' では割れないから，$D'(x') = D'(1/t) = D''(t)/t^{\deg D}$，$\deg D'' = \deg D$ で，$D''(t)$ の定数項は非零．すると，$\deg N - \deg D$ だから $R'(t) = N''(t)/\left\{t^{(\deg N - \deg D)} \cdot D''(t)\right\}$ となる．この有理函数 $R'(t)$ の分数表現の式は既約で，分子の次数は $\deg N - \delta$ であり，分母の次数は $(\deg N - \deg D) + \deg D = \deg N$ となる．よって t の有理函数 $R'(t)$ の分子の次数は分母の次数以下となる． ∎

R から R' を作ることは, 右から可逆な分数一次変換 L を合成することにあたる．もしも合成分解 $R = P \circ R_2$ が存在すれば，その両辺に対して L を右から合成して $R' = (R \circ L) = P \circ (R_2 \circ L) = P \circ R_2'$ である.

すると有理函数 $R'(t)$ の分解 $R' = P \circ R_2'$ には，$R = P \circ R_2$, $R_2 = R_2' \circ L^{-1}$ が対応する．このことから，合成積への分解 $R = P \circ R_2$ を考察するときには，問題を前処理により $\deg N \leq \deg D$ の場合に帰着できる．以下の考察では有理函数は $\deg N \leq \deg D$ を最初から満たすとしてよい.

3.2 考察は $\deg A < \deg B$ に限定できる

$\deg A > \deg B$ なら $\deg P > 0$ だから $\deg N > \deg D$ になる．$\deg P = 0$ は R が定数なので除外してある．それゆえ $\deg N \leq \deg D$ ならば $\deg A \leq \deg B$ でなければならない.

$\deg A = \deg B > 0$ ならば, A の主係数を $c \neq 0$ とすると, $A' = A - cB$ とすると, $A/B = c + A'/B$ で, $\deg A' < \deg B$ である．$P(c+y) = P'(y)$ とおくと $n = \deg P = \deg P'$ である．（$\deg A = \deg B = 0$ は R が定数となるから除外する.）$R = P(A/B) = P(c + A'/B) = P'(A'/B)$ により $\deg A = \deg B$ を満たす解があれば，$\deg A' < \deg B$ を満たす解がある.

よって最初から $\deg A < \deg B$ の場合に限定してよい.

3.3 考察を $\deg N < \deg D$, $P(0) = 0$ に限定できる

$\deg N = \deg D$ の場合は，R から定数 $\ell c(N)/\ell c(D)$ を引くと，$\deg N < \deg D$ の場合に帰着できる．これは多項式 P の定数項を変更することに相当する．逆に，P の定数項を変更すると，$\deg N < \deg D$ の場合を $\deg N = \deg D$ の場合に変更できる．このことから，以下では最初から $\deg N < \deg D$ としてよい．さらに，$x \to \infty$ では $\deg A < \deg B$ により $y = A/B \to 0$，さらに $\deg N < \deg D$ により $R = N/D \to 0$ である．したがって $P(0) = 0$，つまり多項式 P の定数項は 0 になる．そこで，以下では $y = 0$ が $P(y)$ のちょうど m-位の零点 ($m > 0$) とする．（無限遠 ∞ の使用や極限操作を避けるには $x \to \infty$ の代わりに $x = 1/t$ と変数を置換した式を整理して $t = 0$ に置く.）

3.4 多項式 B の決定

条件 $R = P \circ R_2$ を多項式の関係で表すと，

$$\frac{N}{D} = P\left(\frac{A}{B}\right) = \frac{\widehat{P}(A,B)}{B^n}\,.$$

但し $P(y)$ は一次多項式ではないとし，n は $\deg D$ の約数．$\deg P = n > 1$ で主係数 $p_n = \ell c(P) \neq 0$, $y = 0$ がちょうど m-位の零点だとすると $p_m \neq 0$ で，

$$P(y) \equiv \sum_{i=m(>0)}^{n} p_i y^i = p_m y^m + \cdots + p_n y^n\,,$$

$\widehat{P}$ の定義は

$$\widehat{P}(A,B) \equiv \sum_{i=m}^{n} p_i A^i B^{n-i} = p_m A^m B^{n-m} + \cdots + p_n A^n\,.$$

A^n と B は互いに素で，$p_n \neq 0$ だから，$\widehat{P}(A,B)$ と B は互いに素．よって $\widehat{P}(A,B)$ と B^n も互いに素．N と D も互いに素だから，上の有理式の関係を多項式の関係に書くと，ある非零な定数 ρ によって

$$N = \rho \cdot \widehat{P}(A,B)\,,\ D = \rho \cdot B^n$$

となるが，B, D は予め monic としてあるので，D と $\rho \cdot B^n$ の主係数の比較から，$\rho = 1$ が判明し，

$$N = \widehat{P}(A,B)\,,\ D = B^n$$

となる．monic 多項式 D が体 K の係数を持つ多項式のちょうど n-巾であることが必要で，D の n-巾根の monic 多項式が B である．

n-巾根の計算は $x = 1/t$ とし，t の多項式 D', B' の定義を

$$D'(t) \equiv t^{\deg D} D(1/t)\,,\ B'(t) \equiv t^{(\deg D)/n} B(1/t)$$

とすると（注意:ここのプライムは導函数の意味ではない），関係は $(B')^n = D'$ となる．変数 x の多項式の主係数は変数 t の多項式の定数項だから，$B'(0) = 1$ になる．

n が 体 K の標数で割れなければ，巾級数に対する Newton 法を用いて初期値を 1 から始めて反復法により D' の n-巾根として t の巾級数の形で B' が高速に求められる．

$B'(t)$ の巾級数が $(\deg D)/n$-次多項式なら $B(x)$ が決まるが，$B'(t)$ の巾級数が $(\deg D)/n$-次までで切れなければ $B(x)$ の解は無い．

> 注: 体の標数が 0 でなく n が体の標数で割り切れる場合は，n-巾根を求めるのに Newton 法を（導函数が恒等零になるので）直接使えない．n が標数のちょうど e-巾の数 q で割れるとし $n = qn'$ と置くとき，

$$D(x) = (B(x))^n = \{(B(x))^q\}^{n'} = \left(\widehat{B}(x^q)\right)^{n'}$$

但し，$(B(x))^q = \widehat{B}(x^q)$ で，$B(x) = \sum_{i=0}^{\deg B} b_i x^i$ のとき，$\widehat{B}(s) = \sum_{i=0}^{\deg B} (b_i)^q s^i$．$D(x)$ は x^q の多項式 $\widehat{D}(x^q)$ であることが必要で，そのとき $s = x^q$ と置くと，

$$(\widehat{B}(s))^{n'} = \widehat{D}(s)$$

$\widehat{B}(x)$ と $\widehat{D}(s)$ は monic で，n' は体の標数と素だから，$\widehat{D}$ の n'-巾根となる $\widehat{B}$ が（存在すれば）Newton 法で求められる．さらに $B(x)$ が存在するためには $\widehat{B}(s)$ の全ての係数が体 K の元の q-巾として表せることが必要充分である．

3.5 多項式 A の候補の決定

関係 $N = \widehat{P}(A, B)$ から多項式 A を解くことが残っている．A は 0 ではないから monic とする．（係数の規格化は，R_2 の左側からの可逆一次変換の合成だから無視できる．）

$\deg A < \deg B$ が仮定できることは示してあるので $\widehat{P}(A, B)$ の各項 $p_k A^k B^{n-k}$, $(1 \le k \le n)$ は，$p_k \neq 0$ なら k が小さいものほど次数が高いとしてよい．

$m > 0$ を $p_k \neq 0$ を満たす k の最小値とすると，次数の比較から $\deg N = (n-m)\deg B + m \deg A$ であり，$m = (\deg D - \deg N)/(\deg B - \deg A)$ でなければならない．

係数 $p_0, \cdots, p_{m-1}$ は零で，$p_m \neq 0$ であり，$\ell c(B) = 1$ で $\ell c(A) = 1$ だから，$\ell c(N) = p_m$ である．さらに，

$$N = \sum_{i=m(>0)}^{n} p_i A^i B^{n-i}$$

であり，A, B は互いに素だから，N は A のちょうど m-巾 $(m > 0)$ で割り切れる．

以上のことから，「体 K 上での一変数多項式の因数分解」を用いると，

- A の係数は体 K に属し，monic である．
- $\deg A < \deg B$ を満たす．
- A は N をちょうど m-巾で割る．

という条件を満たす多項式 m と A の候補をすべて列挙することができる．

3.6 多項式 $P(y)$ の係数決定の一方法

上の条件を満たす B, m, A の候補の組が与えられたとき，以下の手順により関係 $N = \widehat{P}(A, B) = \sum_{i=m}^{n} p_i A^i B^{n-i}$ を満たすように多項式 $P(y) = \sum_{i=m}^{n} p_i y^i$ の係数である p_i を決めると，P の存在判定と存在する場合の構成ができる．

$U_m \Leftarrow N/A^m$ と置く；
以下の処理を $i = m, \ldots, n$ について順番に行う：
- U_i の次数が高々 $\{(n-i)\deg B\}$ でなければ失敗;
- U_i の $\{(n-i)\deg B\}$ 次の係数を p_i とする;
- $U_i - p_i B^{n-i}$ がAで割り切れなければ失敗;
- $U_{i+1} \Leftarrow (U_i - p_i B^{n-i})/A$ とする;

多項式 $P(y)$ の係数 $p_i, (i = m, \ldots, n)$ が途中で失敗せずに求まったら，$R(x) = N(x)/D(x) = P(y)$, $y = R_2(x) = A(x)/B(x)$ と分解される．すなわち $R = P \circ R_2$ となる組合せが得られる．可能な分解を全て得るには，A の候補全てについて調べる必要がある．

4 後書き

「有理函数を多項式と有理函数の合成積に分解する問題」あるいは「有理函数を有理函数と多項式の合成積に分解する問題」は，（多項式は有理函数でもあるから）どちらも「有理函数を有理函数の合成積に分解する問題」として解いた後に，因子の片方が多項式と（一次多項式と一次分数式による変換に関して）同値であるかの判定を加えることに帰着可能ではあるが，それよりも本論文のように特殊性を用いて専用の扱いをする方が効率的と思われる．

数式処理としては，有理函数以外の函数や，多変数化された問題（既に [1] で部分的に扱われている），連立化された問題などに扱う対象の範囲を拡げることが興味深い．

参 考 文 献

[1] V. S. Alagar and Mai Thanh. Fast polynomial decomposition algorithms. *Proc. EUROCAL'85*, Vol.2, Springer-Verlag, Lect. Notes in Comput. Sci. **204**, April 1-3, 1985, 150–153.

[2] Franz Binder. Polynomial Decompositions - Theoretical Results and Algorithms. DIPLOMARBEIT, Angefertigt am Institut für Mathematik der Technisch-Naturwissenschaftlichen Fakultät der Johannes Kepler Universität Linz, 1995, URL=citeseer.ist.psu.edu/86494.html.

[3] Franz Binder, Characterization Of Polynomial Prime Bidecompositions - A Simplified Proof. URL="citeseer.ist.psu.edu/479486.html".

[4] Franz Binder. Fast Computations in the Lattice of Polynomial Rational Function Fields. *Proc. ISSAC '96*, ACM, July 24-26, 1996, 43–48.

[5] Robert M. Corless, Mark W. Giesbrecht and David J. Jaffrey. Approximate Polynomial Decomposition. *Proc. ISSAC '99*, ACM, 1999, 213–219.

[6] Dexter Kozen and Susan Landau. Polynomial Decomposition Algorithms. *J. Symb. Comput.*, **7**(5), 1989, 445–456.

[7] Dexter Kozen, Susan Landau, and Richard Zippel. Decomposition of Algebraic Functions(1994). *J. Symb. Comput.*, **22**(3), 1996, 235–246.

[8] J. von zur Gathen. Functional decomposition of polynomials: the tame case. *J. Symb. Comput.*, **9**(3), March 1990, 281–299.

[9] J. von zur Gathen. Functional decomposition of polynomials: the wild case. *J. Symb. Comput.*, **10**(5), Nov 1990, 437–452.

[10] Jaime Gutierrez and Tomas Recio. A practical implementation of two rational function decomposition algorithms. *Proc. ISSAC '92*, ACM, July 27-29, 1992, 152–157.

[11] Jürgen Weiß. Homogeneous Decomposition of Polynomials. *Proc. ISSAC '92*, ACM, 1992, 146–151.

[12] Franz Winkler. Polynomial Algorithms in Computer Algebra. Texts and Monographs in

Symb. Comput., Springer-Verlag, Wien New York, 1996,
Chapter 6,"Decomposition of polynomials", 151–156.

[13] David R. Barton and Richard Zippel. Polynomial Decomposition Algorithms. *J. Symb. Comput.*, **1**(2), June 1985, 159-168.

[14] Richard Zippel. Rational function decomposition. *Proc. ISSAC '91*, ACM, July 15-17, 1991, 1–6.

[15] Richard Zippel. Functional Decomposition(1996). Cornell University, Ithaca, NY, URL="citeseer.ist.psu.edu/zippel96functional.html".