ICOT Technical Report: TR-463

TR-463

代数的閉体上の多変数多項式の因数分解

横山　和弘、野呂　正行、竹島　卓

March, 1989

©1989, ICOT

ICOT
Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
Minato-ku Tokyo 108 Japan
(03) 456-3191～5
Telex ICOT J32964

Institute for New Generation Computer Technology

代数的閉体上の多変数多項式の因数分解

富士通・国際研 横山和弘 野呂正行 竹島卓

本論文では，多変数多項式を代数的閉体，すなわち複素数体，の上で因数分解するアルゴリズムを考察する．一般の代数的数を係数とする多変数多項式の因数分解は，基本は整数係数多項式の因数分解であることより，ひとたび整数係数の場合にアルゴリズムが得られれば，同様なアルゴリズムが存在することがわかる．そこで，我々は整数係数の場合を考察し，いくつかの方法を示す．

はじめに

以下，整数全体のなす環を $\mathbf{Z}$，有理数全体のなす体を $\mathbf{Q}$，実数全体のなす体を $\mathbf{R}$，複素数全体のなす体を $\mathbf{C}$ とする．$f(x_1,...,x_n)$ は変数を $x_1,...,x_n$ とする整数係数の多項式とする．f を $\mathbf{Z}$ で因数分解するアルゴリズムの研究は，一変数多項式の因数分解と並行して行われ，多くのアルゴリズムが発表されている．(Musser (1975), Wang (1978), Lenstra (1984a), Kaltofen (1985) 等を参照．) 更に，係数環を一般化した代数拡大体上の因数分解も数多く研究されている．(Trager (1976), Wang (1976), Lenstra (1984b) 等を参照．) 特に一変数の場合には，最小分解体を求めて，一次式に分解するアルゴリズム，すなわち，複素数体上での因数分解アルゴリズムも提案されている．(Trager (1976), Landau (1985), Yokoyama&Noro&Takeshima (1988).) しかしながら，多変数の場合には，指定された代数的拡大体の上での因数分解アルゴリズム (Wang (1976), Lenstra (1984b))，や絶対既約性の判定アルゴリズム (Heintz&Sieveking (1981), Kaltofen (1985), von zur Gathen (1985)) は研究されていても，複素数体上での因数分解アルゴリズムは研究されていない．しかも，複素数体上での因数分解は，パラメーター付の有理関数の積分において是非必要である．この観点より，我々は複素数体上の因数分解アルゴリズムの研究を行った．さらに，多変数多項式の因数分解は 2 変数の場合が本質的であることより，2 変数の場合を取り上げて議論する．

数学的基礎

f を整数係数 2 変数多項式とし，その変数を x,y とする．はじめから，f は $\mathbf{Q}$ 上で既約であると仮定してよい．f の $\mathbf{C}$ 上での因子 (既約であるとは限らない) を g，その共因子を h とする．すなわち，$f=g\cdot h$ である．

$$f(x,y)=\sum_{i=0}^{i=n}\sum_{j=0}^{j=m}f_{i,j}x^iy^j,$$

$$g(x,y)=\sum_{i=0}^{i=n'}\sum_{j=0}^{j=m'}g_{i,j}x^iy^j,$$

$$h(x,y)=\sum_{i=0}^{i=n-n'}\sum_{j=0}^{j=m-m'}h_{i,j}x^iy^j,$$

とおけば，$f_{i,j}\in\mathbf{Z}$，$g_{i,j},h_{i,j}\in\mathbf{C}$ であり，f が $\mathbf{Q}$ 上既約であることより，ある i,j に関して，$g_{i,j}\notin\mathbf{Q}$ である．さて，y に具体的な数値 a を代入してみると，以下になる．

$$f(x,a)=g(x,a)\cdot h(x,a).$$

これは，一変数多項式 $f(x,a)$ が $\mathbf{C}$ において，二つの因子 $g(x,a)$ と $h(x,a)$ とに分かれることに他ならない．したがって，$g(x,a)$ および $h(x,a)$ の各係数はすくなくとも $f(x,a)$ の最小分解体 $K_{f(x,a)}$ の元になることが判る．ここで，

$$g(x,a)=\sum_{i=0}^{i=n'} g_i(a)x^i$$

とおけば, 各係数 $g_i(a)$ は,

$$g_i(a)=\sum_{j=0}^{j=m'} g_{i,j}a^j$$

であることに注意する.

次に, 正の実数 M を以下のように定める.

$g_{i,j}$ の絶対値の最大値を A, 異なる二つの $g_{i,j}$ の差の絶対値の最小値を B としたときに, $M=4A/B$ と定義する.

Yokoyama&Noro&Takeshima (1988) より, 正数 M より大きい整数 a を代入したときに次が成り立つ.

$$\mathbf{Q}(g_{i,0},...,g_{i,m'})=\mathbf{Q}(g_i(a)) \text{ for } 0\le i\le n'.$$

したがって,

$$\mathbf{Q}(g_{0,0},...,g_{n',m'})=\mathbf{Q}(g_0(a),...,g_{n'}(a)).$$

これは, $f(x,y)=g(x,y)\cdot h(x,y)$ なる分解を与える代数拡大体 (K とおく) は $f(x,a)$ の最小分解体に含まれることを意味する. (求め方は Yokoyama&Noro&Takeshima (1988) を参照のこと.) $g(x,y)$ は $f(x,y)$ の任意の因子でよいことから, 以下が得られる.

補題 1. 十分大きい正の整数 a に関して, 2変数多項式 $f(x,y)$ の $\mathbf{C}$ 上の因数分解は, $f(x,a)$ の最小分解体 $K_{f(x,a)}$ 上での因数分解に等しい.

一方, $\mathbf{Q}(g_{i,0},...,g_{i,m'})$ の $\mathbf{Q}$ 上の拡大次数 n_i に注目すれば, Yokoyama&Noro&Takeshima (1988) により, $\{1,2,...,m'n_i\}$ の中に,

$$\mathbf{Q}(g_{i,0},...,g_{i,m'})=\mathbf{Q}(g_i(a))$$

なる a が存在することが判る. 同様の議論により, $\{1,2,...,n'm'n_i\}$ の中に,

$$\mathbf{Q}(g_{0,0},...,g_{n',m'})=\mathbf{Q}(g_0(a),...,g_{n'}(a))$$

なる a が存在することが判る. さらに, 各 n_i は $K_{f(x,a)}$ の $\mathbf{Q}$ 上の拡大次数を越えず, その拡大次数は $n!$ 以下である. また, $n'\le n$, $m'\le m$ であることから, 次が得られる.

補題 2. $\{1,2,...,nm(n!)\}$ の中に, ある a が存在して, 2変数多項式 $f(x,y)$ の $\mathbf{C}$ 上の因数分解は, $f(x,a)$ の最小分解体 $K_{f(x,a)}$ 上での因数分解に等しい.

さて, 再び等式

$$g_i(a)=\sum_{j=0}^{j=m'} g_{i,j}a^j \text{ for } 0\le i\le n',\ 0\le j\le m'$$

に注目すれば, 次の連立方程式が得られる.

$$\begin{pmatrix} g_0(a_0) & g_1(a_0) & \cdots & g_{n'}(a_0)\\ g_0(a_1) & g_1(a_1) & \cdots & g_{n'}(a_0)\\ \vdots & \vdots & \ddots & \vdots\\ g_0(a_{m'}) & g_1(a_{m'}) & \cdots & g_{n'}(a_{m'}) \end{pmatrix} = \begin{pmatrix} 1 & (a_0)^1 & \cdots & (a_0)^{m'}\\ 1 & (a_1)^1 & \cdots & (a_1)^{m'}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & (a_{m'})^1 & \cdots & (a_{m'})^{m'} \end{pmatrix} \cdot \begin{pmatrix} g_{0,0} & g_{1,0} & \cdots & g_{n',0}\\ g_{0,1} & g_{1,1} & \cdots & g_{n',1}\\ \vdots & \vdots & \ddots & \vdots\\ g_{0,m'} & g_{1,m'} & \cdots & g_{n',m'} \end{pmatrix}$$

ここで, $a_0,a_1,...,a_{m'}$ は, すべて異なる整数であるとする. 右辺の左の行列は Vandermonde の行列に他ならない. よって, 異なる $m'+1$ 個の a の値に対して, $g_i(a)$ が求まっていれば $g_{i,j}$ が解けることになる. これは, $f(x,y)=$

$g(x,y)\cdot h(x,y)$ なる分解を与える代数拡大体は $f(x,a_0),...,f(x,a_{m'})$ をすべて分解する体に含まれることを意味する. $m'\leq m$ であるから, m' の代わりに m を用いることができる. したがって, 次を得る.

補題 3. $a_0,a_1,...,a_m$ は, すべて異なる整数であるとし, $K_{f(x,a_i)}$ を $f(x,a_i)$ の最小分解体とする. さらに, L を $K_{f(x,a_0)},...,K_{f(x,a_m)}$ の合成体であるとする. このとき, 2 変数多項式 $f(x,y)$ の $\mathbf{C}$ 上の因数分解は, L での因数分解に等しい.

以上の補題より, 必要な代数的拡大体を計算し, 定められた代数的拡大体における因数分解法を適用することにより, 我々は, 2 変数多項式の因数分解ができる. 代数的拡大体を原始元により記述する場合には, Trager (1976), Landau (1985), Yokoyama&Noro&Takeshima (1988) を参照されたい. また, 定められた代数的拡大体上の因数分解法については, Wang (1976), Lenstra (1984b) 等が利用できる. このようにして, 代数的閉体上の因数分解が計算できる. しかし, 以上の方法は必要な拡大体の次数が大きいために, 実際の計算は不可能な場合が多いと考えられる. そこで, モジュラ計算等の工夫が必要になる.

モジュラ計算の試み

まず, 有限体への射影を考える. 以下, 位数が素数 p である有限体 $GF(p)$ を係数体とし, $\mathbf{Z}[x,y]$ から $GF(p)[x,y]$ への自然な射影を拡張する.

$f=g\cdot h$ を与える代数的拡大体を K とおく. K の原始元を一つ取り, それを α とし, α の最小多項式を F_α とおく. はじめから, F_α は monic かつ整数係数であると仮定してよい. このとき, 各 $g_{i,j}$ は α の有理数係数多項式として表すことができる. そこで, この多項式を $G_{i,j}(\alpha)$ とおくことにする. これより, g は次になる.

$$g(x,y)=\sum_{i=0}^{i=n'}\sum_{j=0}^{j=m'}G_{i,j}(\alpha)x^iy^j.$$

$h(x,y)$ に対しても, 同様に $H_{i,j}$ を定めておく. また, $f(x,y)$ の $GF(p)[x,y]$ での像を $\bar{f}(x,y)$ とおく. 仮定として, p が 各 $G_{i,j}[t]$ の係数の分母を割らないとする. 各 $G_{i,j}[t]$ は, Weinberger&Rothchild (1976) により, その共通の分母 D として, その二乗が F_α の discriminant を割るような最大の整数がとれる. discriminant 自身でもよいので, ここでは F_α の discriminant としてD を取ることにする. (discriminant は Resultant$(F_\alpha,dF_\alpha/dx)$ により計算される.) よって, 以下 p は discriminant D を割らない素数であると仮定する. 各 $G_{i,j}[t]$ の $GF(p)[t]$ での像を $\bar{G}_{i,j}[t]$ とおく. このとき, $\bar{g}(x,y;t)$ を以下に定義する.

$$\bar{g}(x,y;t)=\sum_{i=0}^{i=n'}\sum_{j=0}^{j=m'}\bar{G}_{i,j}(t)x^iy^j.$$

同様に $\bar{h}(x,y;t)$ を定義しておく. $F_\alpha[t]$ の $GF(p)[t]$ での像を $\bar{F}_\alpha$ とおき, $GF(p)$ の代数的閉包 $\bar{K}_p$ の中で β を $\bar{F}_\alpha(\beta)=0$になる様に取れば,

$$\bar{f}(x,y)=\bar{g}(x,y;\beta)\cdot\bar{h}(x,y;\beta)$$

なる等式が $GF(p)(\beta)$ 上でなりたつ.
一方, 有限体 $GF(p)(\beta)$ については, $\bar{F}_\alpha$ の根であることより, $\bar{F}_\alpha$ の $GF(p)$ 上でのある既約因子 F' の根となる. そこで, もしも, $\bar{F}_\alpha$ が $GF(p)$ 上で既約であるならば, $GF(p)$ の F_α の次数次 (これを N 次とする) の代数的拡大体 $GF(q)$ において

$$\bar{f}(x,y)=\bar{g}(x,y)\cdot\bar{h}(x,y)$$

となる因子分解ができることになる. この $GF(q)$ は $GF(p)$ 上既約な任意のN 次多項式により定義することができるから, 次の結果を得る.

補題 4. K の原始元として，その最小多項式の discriminant が p で割れず，かつその最小多項式が $GF(p)$ 上でも既約になる様なものが取りうる場合には，$GF(q)$ 上においても，$f = g \cdot h$ に対応する因数分解

$$\bar{f}(x,y) = \bar{g}(x,y) \cdot \bar{h}(x,y)$$

が存在する．ここで，$q = p^N$ であり，N は K の $\mathbf{Q}$ 上の拡大次数である．

次に，一般の場合について考える．補題 1 により，ある正の整数 M より大きい任意の整数 a に対して，$f(x,a)$ の最小分解体上で $f = g \cdot h$ なる因数分解ができていた．Yokoyama&Noro&Takeshima (1988) より，$f(x,a)$ の最小分解体の原始元の最小多項式を含む多項式 F を求める手続きが与えられている．そこでは，$f(x,a)$ の各係数より定まる正の整数 c を利用しているが，この計算をそのまま mod p 上にて行った場合に $GF(p)$ 上の対応する多項式が生成される．このときに，c として pで割れないように大きく取ってあれば (本当に，大きくできる)，$f(x,a)$ の最小多項式の $GF(p)[x,y]$ 上の像が得られる．したがって，その discriminant の mod p の値，すなわち D mod p も計算できることになる．(正しくは，求まる数は discriminant の倍数である．) さらに，D mod p は modulo p において同じ値を取る a, a' に対して不変であることも判る．そこで，$GF(p)[x,y]$ で考え，$\bar{a} = a$ mod p とおけば，$\bar{f}(x,\bar{a})$ の $GF(p)$ 上の最小分解体 $GF(q')$ とその原始元の最小多項式を含む多項式 F に相当する多項式 $\bar{F}$ が上述の手続きで計算でき，その discriminant も 計算される．(この場合の discriminant は $\bar{F}$ が無平方であるかどうかに対応している.)OOA この得られた多項式が無平方であるときに，$f = g \cdot h$ に対応する因数分解が存在することになる．

補題 5. $GF(p)$ の元を b とする．$\bar{f}(x,b)$ により定まる $\bar{F}$ が $GF(p)$ 上無平方であると仮定する．このとき，$\bar{f}(x,b)$ の $GF(p)$ 上の最小分解体を $GF(q')$とおけば $GF(q')$ 上で，

$$\bar{f}(x,y) = \bar{g}(x,y) \cdot \bar{h}(x,y)$$

なる因数分解が存在する．

補題 5 により，$f(x,y)$ が上記の $GF(q')$ 上で既約であった場合に，$f(x,y)$ が絶対既約であると判定できる．さらに，補題 5 での有限体上の因子を種として Hensel 構成で持ち上げて，$\mathbf{C}$ での因子の候補を作る方法も考えられる．ここで，有限体上の多変数多項式の因数分解法として von zur Gathen&Kaltofen (1985) または Lenstra (1985) が使えることを注意しておく．

斉次多項式と変数変換による簡約化

特殊な工夫として，次にあげる変数変換による簡約化がある．2 変数多項式 $f(x,y)$ が斉次の場合には，次がいえる．

補題 二変数多項式 $f(x,y)$ が斉次の場合には，$f(x,1)$ の最小分解体 $K_{f(x,1)}$ の上で，$f(x,y)$ は 1 次式にの積に分解される．すなわち，

$$f(x,y) = \prod_{i=1}^{i=n}(x - c_i y),$$

ここで，

$$f(x,1) = \prod_{i=1}^{i=n}(x - c_i),$$

である．

では，斉次でないときにはどうなるのであろうか？まず，一般の斉次ではない 2 変数多項式 $f(x,y)$ について，次の斉次化をおこなう．

$$f_h(x,y,z) = z^s f(x/z, y/z).$$

ここで，s =total degree $f(x,y)$ である．

このとき，新たにできた 3 変数多項式 $f_h(x,y,z)$ に対して次が成り立つ．

補題 7. $f(x,y)$ の $\mathbb{C}$ における因数分解と $f_h(x,y,z)$ の $\mathbb{C}$ における因数分解とに次の対応がある.

$g(x,y,z)$ が $f_h(x,y,z)$ の既約因子であるための必要十分条件は $g(x,y,1)$ が $f(x,y)$ の既約因子である.

この補題により, $f(x,y)$ の因数分解は新たにできた 3 変数多項式 $f_h(x,y,z)$ の因数分解に帰着される. さらに, $f_h(x,y,z)$ の因数分解は $f_h(x,1,z)$ の因数分解とも同等であることより, $f_h(x,y,z)$ において, 次数が一番多い変数に 1 を代入してできる多項式を因数分解するのが有効であることになる. そこで, $\mathrm{degree}_z\, f_h(x,y,z)$ を t とおくとき, t が n,m より小さい場合は, z を主変数とする 2 変数多項式 $f_h(x,1,z)$ を因数分解すればよいことになる. これを, 変数変換による簡約と呼ぶことにする.

例 $f(x,y)=x^5-y^5$ は $\mathbb{C}$ の上で以下に分解される.

$$f(x,y)=(x-y)(x-y\omega)(x-y\omega^2)(x-y\omega^3)(x-y\omega^4).$$

ここで, ω は 1 の原始 5 乗根である.

しかし, $g(x,y)=x^5-y^4$ は $\mathbb{C}$ の上で既約であることが以下で示すことができる.

$g_h(x,y,z)=x^5-y^4z$ であり, z に関して 1 次であることから, $g_h(x,y,z)$ は $\mathbb{C}$ 上既約である.

参考文献

von zur Gathen J. (1985), Irreduciblity of multivariate polynomials, J. Comput. System Sci. 31, 225-264.

von zur Gathen J., Kaltofen E. (1985), factorization of multivariate polynomials over finite fields, math. Comp. 45, 251-261.

Heintz J., Sieveking M. (1981), Absolute primality of polynomials is decidable in random polynomial time in the number of variables, Lecture Note in Computer Science 115, pp.16-25, Springer-Verlag, New York.

Kaltofen E. (1985), Effective Hilbert irreduciblity, Inform. Contr. 66, 123-137.

Landau S. (1982), Factoring polynomials over algebraic number fields, SIAM. J. Comput. 14, 184-195.

Lenstra A. K. (1984a), Factoring multivariate integral polynomials, Theoret. Comput. Sci. 34, 207-213.

Lenstra A. K. (1984b), Factoring multivariate polynomials over algebraic number fields, Lecture Note in Computer Science 176, 389-396.

Lenstra A. K. (1985), Factoring multivariate polynomials over finite fields, J. Comput. System Sci. 30, 235-248.

Musser D. (1975), Multivariate polynomial factorization, J. ACM. 22, 291-308.

Trager B. M. (1976), Algebraic factoring and rational integration. proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation.

Wang P. S. (1976), Factoring multivariate polynomials over algebraic number fields, Math. Comp. 30, 324-336.

Wang P. S. (1978), An improvement multivariate polynomial factoring algorithm, Math. Comp. 32, 1215-1231.

Weinberger P. J., Rothchild L. P. (1976), Factoring polynomials over algebraic number fields, ACM Trans. Math. Soft. 2, 335-350.

Yokoyama K., Noro M., Takeshima T. (1988), Computing primitive elements of extension fields, to appear in J. Symbolic Computation.