代数体の底式と代数多様体の同伴形式

前田博信

代数体 K は，その整数の基底が知られている場合は，必要なだけ不定元を導入して底式を作り，その定義方程式である底方程式を mod p で還元して因数分解すれば，代数体の定義式の特異点解消をしなくても p の K における素因子分解が例外なく記述出来る．また，代数関数体は，ある既約なアフィン代数多様体 W の関数体とみなすとき，その生成点の座標と，必要なだけの不定元からなる 1 次形式を底式とみなして底方程式と同様の式を作ると，この式の係数を特殊化して（ここが代数体の場合の底方程式を mod p で還元することに相当する），因数分解すれば W 上の点がすべて記述できる．この両者の類似は（少なくとも最近では）あまり注意されていないようなので，ここで紹介したい．なお，後者の底方程式を射影代数多様体に拡張したものが同伴形式，別名 Chow 形式または Cayley 形式である．

1．特異点解消と底式．K を n 次代数体とする．K の主整数環 $\mathfrak{o}_K$ は階数が n の自由加群であるが，$\mathfrak{o}_K$ の基底であるような組 $\omega_1, \omega_2, \ldots, \omega_n$ があらかじめ知られているとする．このとき，$u_1, u_2, \ldots, u_n$ を不定元として，1 次形式 $\tau = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$ を K の底式 (Fundamentalform) とよび，τ の $\mathbf{Q}(u_1, u_2, \ldots, u_n)$ 上の定義方程式 $F(x; u_1, \ldots, u_n)$ を底方程式 (Fundamentalgleichung) とよぶ．各 ω_i の共役元を $\omega_i^{(j)}$ $(j = 1, \ldots, n)$ とすると

$$F(x;u) = \prod_{j=1}^{n} (x - u_1\omega_1^{(j)} - u_2\omega_2^{(j)} - \cdots - u_n\omega_n^{(j)})$$

となる．素数 p の K における分解が $p\mathfrak{o}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}$ であるならば，$F(x;u)$ の係数を mod p で還元した多項式の因数分解は

$$F(x;u) \equiv P_1(x;u)^{e_1} P_2(x;u)^{e_2} \cdots P_g(x;u)^{e_g} \pmod{p}$$

となる[1]．一方，p が K の定義方程式 $f(x)$ の判別式 Δ を高々1 回しか割らないならば，$f(x) \equiv P_1(x)^{e_1} P_2(x)^{e_2} \cdots P_g(x)^{e_g} \pmod{p}$ となるが，p が Δ を 2 回以上割る場合は p 上の特異点が存在する可能性があるため，その場合は $f(x)$ の特異点解消が必要であるが，特異点解消は単純な 2 次変換を繰り返すだけで計算出来る．

[1] Kurt Hensel, Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante, Crelle, 113 (1894).

例1. 簡単な4次体 $K=\mathbf{Q}(\sqrt{2},\sqrt{3})$ を考える. 定義方程式である x^2-2 と x^2-3 の判別式をみると, K において, 分岐しうる素数は2と3である. x^2-2 も x^2-3 も $\mathbf{Z}[x]$ の元としては非特異であるが, x^2-3 は $\mathbf{Z}[\sqrt{2}][x]$ の元としては $x^2-3=(x+1)^2-\sqrt{2}^2(x+1)-\sqrt{2}^2\in(x+1,\sqrt{2})^2$ となり特異点 $\mathfrak{m}=(x+1,\sqrt{2})$ をもつ[2]. この特異点 $\mathfrak{m}$ を中心とする2次変換による x^2-3 の固有変換は $\varphi(t)=t^2-\sqrt{2}t-1$ となり, これは非特異である. $\mathbf{Z}[\sqrt{2}][t]$ の元として, $\varphi(t)\equiv(t-1)^2 \bmod \sqrt{2}$ であるから K において, $\sqrt{2}=\mathfrak{p}^2$ すなわち, $2=\mathfrak{p}^4$ と完全分岐する. 一方, 3は $\mathbf{Z}[\sqrt{2}]$ においても素, すなわち, $3=\mathfrak{q}$, $N(\mathfrak{q})=3^2$ であり, $\varphi(t)\equiv(t-2\sqrt{2})^2 \bmod 3$ であるから, K において $\mathfrak{q}=\mathfrak{Q}^2$ すなわち, $3=\mathfrak{Q}^2$, $N(\mathfrak{Q})=3^2$ と分解することが分かる.

一方, $t^2-\sqrt{2}t-1=0$ の根は $\dfrac{\sqrt{2}\pm\sqrt{6}}{2}=\dfrac{1\pm\sqrt{3}}{\sqrt{2}}$ であるから, $\mathfrak{o}_K$ の整数基として, $1,\sqrt{2},\sqrt{3},\dfrac{1+\sqrt{3}}{\sqrt{2}}$ をとることが出来る. このときの K の底式は $\tau=u_1+\sqrt{2}u_2+\sqrt{3}u_3+\dfrac{1+\sqrt{3}}{\sqrt{2}}u_4$ となり, 底方程式を計算すると, $f(x;u)=x^4-4u_1x^3+(6u_1^2-4u_2^2-6u_3^2-4u_2u_4-4u_4^2)x^2+(-4u_1^3+8u_1u_2^2+12u_1u_3^2+8u_1u_2u_4+24u_2u_3u_4+8u_1u_4^2+12u_2u_4^2)x+u_1^4+4u_2^4+9u_3^4+u_4^4-4u_1^2u_2^2+6u_1^2u_3^2-12u_2^2u_3^2-4u_1^2u_4^2-12u_3^2u_4^2-4u_1^2u_2u_4+8u_2^3u_4-24u_1u_2u_3u_4-12u_2u_3^2u_4-12u_1u_3u_4^2-4u_2u_4^3$ となる. $f(x;u)\equiv(x+u_1+u_3+u_4)^4 \bmod 2$ より, $2=\mathfrak{p}^4$ となり, $f(x;u)\equiv(x^2+u_1x+u_2^2+u_2u_4+u_4^2)^2 \bmod 3$ より, $3=\mathfrak{Q}^2$ $(N(\mathfrak{Q})=3^2)$ となることが再確認された.

このように, 整数基を求めるには特異点を解消するよりも多くの計算が必要であるが, 得られる情報は多い. しかし, 素因子分解を求めるだけなら特異点解消の計算だけで十分である.

例2. $f(x)=x^5+10x^3-10x^2+35x-18$ を借用して[3] 特異点の様子を見てみよう. $f(x)$ の判別式は $2^6\cdot5^8\cdot11^2$ であるから, 特異点は, あるとすると, $p=2,5$ または11の上である. $f(x)\equiv x(x+1)^4 \bmod 2$ であるが $f(-1)=-37\times2\not\equiv0 \bmod 2^2$ であるから $p=2$ 上の特異点は存在しない. 次に $f(x)\equiv(x+2)^5 \bmod 5$ であるが $f(-2)=-48\times5\not\equiv0 \bmod 5^2$ であるから $p=5$ の上にも特異点はない. $p=11$ のときは, $f(x)\equiv(x+3)^2(x+5)(4+x^2) \bmod 11$ であるが $f(-3)=-6\times11^2\equiv0 \bmod 11^2$ であるから特異点 $\mathfrak{m}=(x+3,11)$ がある. ここで単項変換を実行するため, $\dfrac{x+3}{11}=u$, $\dfrac{11}{x+3}=v$ とおく. $A=\mathbf{Z}[x,u]$ における f の固有変換は $f_1=11^{-2}f=1331u^5-1815u^4+1100u^3-370u^2+70u-6$ であり非特異である. A においては $(11,f_1)=(11,4(u^2+u+4))$

[2] 前田博信, Dedekind の3次体の整数環について, 数学, 57巻, 2005年1月号.

[3] Joe Buhler, Icosahedral Galois Representations, Lect. Notes in Math., vol. 654 (1978), Springer, の136頁の表にある最初の式.

となる．この極大イデアルを $\mathfrak{P}_1$ とおく．次に $B=\mathbf{Z}[x,v]$ における f の固有変換は $f_2=(x+3)^{-2}f=(x+3)^3-15(x+3)^2+100(x+3)-370+70v-6v^2$ となり非特異である．$11=(x+3)v$ に注意すると，B において $(11,f_2)=(x+3,f_2)\cap(v,f_2)=(x+3,5(v^2+3v+3))\cap(v,(x+3)+2)\cap(v,(x+3)^2+5(x+3)+2)$ と3つの極大イデアルに分解するが，$\mathbf{Z}[x,u,v]$ において $(x+3,5(v^2+3v+3))=(11,4(u^2+u+4))=\mathfrak{P}_1$ であるから，$\mathfrak{P}_2=(v,(x+3)^2+5(x+3)+2),\mathfrak{q}=(v,(x+3)+2)$ とおくと，$V(f_1)\cup V(f_2)$ 上の閉点として $(11)=\mathfrak{P}_1\mathfrak{P}_2\mathfrak{q}$，すなわち $p=11$ は K で不分岐である（図1）．

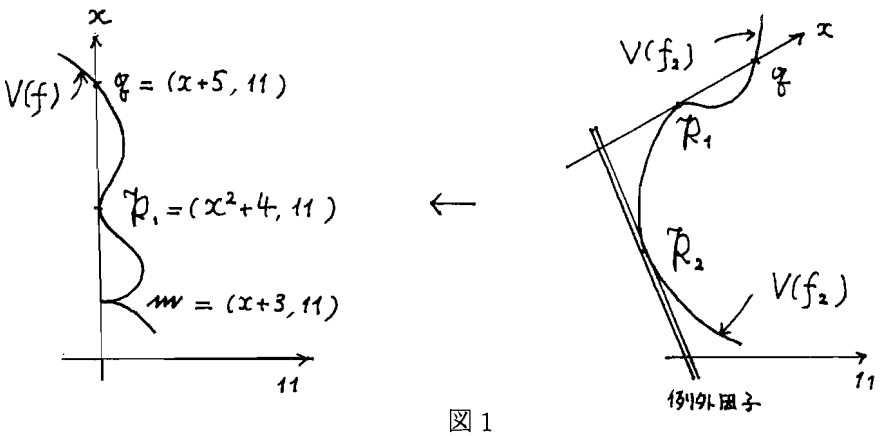

図1

2．同伴形式．次に K を基礎体 k 上の r 次元代数関数体とする．K は，$\xi_1,\xi_2,\ldots,\xi_r$ が k 上代数的独立で，$\xi_{r+1},\ldots,\xi_n$ は $k[\xi_1,\xi_2,\ldots,\xi_r]$ 上の整元となるような $(\xi_1,\xi_2,\ldots,\xi_n)$ を生成点とするアフィン代数多様体 W の有理関数体としてよい（Noetherの正規化）．そこで，$u_{r+1},\ldots,u_n$ を不定元とし，底式に相当する1次形式 $\tau=u_{r+1}\xi_{r+1}+\cdots+u_n\xi_n$ を考える．τ は $\tilde{k}=k(\xi_1,\ldots,\xi_r,u_{r+1},\ldots,u_n)$ 上の整元であるから，その定義式を $f(x;\xi,u)$ とする．各 ξ_i に η_i を代入して $f(x;\eta,u)$ を因数分解したものを

$$f(x;\eta_1,\ldots,\eta_r,u_{r+1},\ldots,u_n)=\prod_{i=1}^{m}(x-u_{r+1}\eta_{r+1}^{(i)}-\cdots-u_n\eta_n^{(i)})$$

とすると，点 $(\eta_1,\ldots,\eta_r)$ の上の点 $(\eta_1,\ldots,\eta_r,\eta_{r+1}^{(i)},\ldots,\eta_n^{(i)})$ が得られる．逆に，点 $(\eta_1,\ldots,\eta_r)$ 上にある W の点はこのような因数分解により例外なく得られる[4]．なお，必要に応じて係数体を拡大するため，得られた点は k 有理点とは限らない．

例3．ξ_1,ξ_2 が k 上代数的独立で，$\xi_3^2-\xi_1=0,\xi_4^2-\xi_2=0,\xi_5^2-\xi_1\xi_2=0$ のとき，$(\xi_1,\xi_2,\xi_3,\xi_4,\xi_5)$ を生成点とする2次元アフィン代数多様体を考える．$\tau=u_3\xi_3+$

[4] B. L. van der Waerden, ZAG III, Math. Ann., 108(1933).

$u_4\xi_4+u_5\xi_5$ の底方程式は $f(x;\xi_1,\xi_2,u_3,u_4,u_5)=x^4-2(\xi_1u_3^2+\xi_2u_4^2+\xi_1\xi_2u_5^2)x^2-8\xi_1\xi_2u_3u_4u_5x+\xi_1^2u_3^4+\xi_2^2u_4^4+\xi_1^2\xi_2^2u_5^4-2\xi_1\xi_2u_3^2u_4^2-2\xi_1^2\xi_2u_3^2u_5^2-2\xi_1\xi_2^2u_4^2u_5^2$ となる.

1937 年に van der Waerden はこの底方程式を射影代数多様体に拡張した[5]. 体 k 上の n 次元射影空間 S_n に入っている r 次元の既約な射影代数多様体 W を考える. $(x_0,x_1,\ldots,x_n)$ を同次座標とする. 不定元 $\{u_j^{(i)}\}$ を係数とする r 個の超平面 $u_0^{(i)}x_0+u_1^{(i)}x_1+\cdots+u_n^{(i)}x_n=0\ (i=1,\ldots,r)$ と W との（適当な拡大体上での）交点は g 個の閉点 $(p_0^{(l)},\ldots,p_n^{(l)})\ (l=1,\ldots,g)$ となる. これらの点の座標の 1 次結合の積

$$F(u)=\prod_{l=1}^{g}\left(u_0p_0^{(l)}+u_1p_1^{(l)}+\cdots+u_np_n^{(l)}\right)$$

をつくり, $\{u_j^{(i)}\}$ の多項式とみたものを W の同伴形式（zugeordnete Form）とよぶ. $F(u)$ は定数倍を除き W によって一意的に決まるため, $F(u)$ の係数からなる同次座標は, S_n の中にある r 次元の W を特定することができ, W のモジュラスとよばれる.

例 4. $n=3$ とし, W は異なる 2 点 $y=(y_0,y_1,y_2,y_3)$, $z=(z_0,z_1,z_2,z_3)$ を通る直線とする. S_3 は 4 次元ベクトル空間 V の中の射線の全体とみなせるから, W に対応するのは V の部分空間であって, y と z で張られるもの $\lambda y+\mu z$ の全体である. この中で不定元を係数とする超平面 $H:u_0x_0+u_1x_1+u_2x_2+u_3x_3=0$ 上にあるものは, $u_0(\lambda y_0+\mu z_0)+u_1(\lambda y_1+\mu z_1)+u_2(\lambda y_2+\mu z_2)+u_3(\lambda y_3+\mu z_3)=\lambda(u_0y_0+u_1y_1+u_2y_2+u_3y_3)+\mu(u_0z_0+u_1z_1+u_2z_2+u_3z_3)=0$ をみたすから, $\lambda=u_0z_0+u_1z_1+u_2z_2+u_3z_3$, $\mu=-(u_0y_0+u_1y_1+u_2y_2+u_3y_3)$ とおいたものである. すなわち, H と W の交点 p の第 i 座標は $p_i=\lambda y_i+\mu z_i=(u_0z_0+u_1z_1+u_2z_2+u_3z_3)y_i-(u_0y_0+u_1y_1+u_2y_2+u_3y_3)z_i$ となるから W の同伴形式 $F(v)$ は

$$\prod_{j=0}^{3}v_jp_j=\prod_{j=0}^{3}v_j\left\{(u_0z_0+u_1z_1+u_2z_2+u_3z_3)y_i-(u_0y_0+u_1y_1+u_2y_2+u_3y_3)z_i\right\}$$

となり展開すると

$$F(v)=\sum_{j=0}^{3}\sum_{k=0}^{3}(y_jz_k-y_kz_j)v_ju_k$$

となる. 係数はプリュッカーの S_1 座標[6] とよばれ, これが W のモジュラスである.

同伴形式, すなわちモジュラスは既約成分が等次元の代数的集合にも拡張され, 例えば, 高々通常 2 重点のみをもつ（安定）平面代数曲線のモジュラスの全体は射影代数多様体になることが知られている[7].

---

[5] B. L. van der Waerden und W.-L. Chow, ZAG IX, Math. Ann., 113(1937).

[6] B. L. ファン・デル・ヴェルデン, 代数幾何学入門, シュプリンガー東京 (1991).

[7] B. L. van der Waerden, ZAG XI, Math. Ann., 114(1937).