数論曲線の特異点に関するデデキントの結果

前田博信

2次式 t^2+3 は $t^2+3=(t+1)^2-2(t+1)+2^2$ となることから，整数係数の多項式環 $\mathbf{Z}[t]$ において，極大イデアル $\mathfrak{m}=(2,t+1)$ の平方 $\mathfrak{m}^2=(2^2,2(t+1),(t+1)^2)$ に含まれていることが分かる．3次式の例としては $t^3+8t+1=(t-2)^3+6(t-2)^2+20(t-2)+25\in(5,t-2)^2$ がある．このような現象を代数幾何学では多項式の定義する代数的集合が「特異点をもつ」という．特異点は無い方が都合がいいので，特異点に関する基本的な課題は非特異モデルの定式化と構成である．ここでは代数体の定義方程式について，その特異点を具体的に記述するデデキントの結果を紹介する．

$F(t)=t^n+a_1t^{n-1}+\cdots+a_n\in\mathbf{Z}[t]$ を整数係数で最高次係数が1の n 次で既約な1変数多項式とする．$F(t)$ の零点の1つ θ を $\mathbf{Q}$ に添加した代数体を $K=\mathbf{Q}(\theta)$ とし，K の主整数環を o_K とする．$\mathbf{Z}[t]$ の極大イデアル $\mathfrak{m}$ で $F(t)\in\mathfrak{m}^2$ をみたすものを $F(t)$ の特異点とよぶ．素数 p について，$f(t)\in\mathbf{Z}[t]$ の $\mathbf{F}_p[t]$ における像，すなわち係数を $\bmod p$ で考えた多項式を $\overline{f}(t)$ と表すことにすると，$\mathfrak{m}$ は適当な素数 p と，最高次係数が1の $P(t)\in\mathbf{Z}[t]$ で $\overline{P}(t)$ が既約なものとで生成される．このような $P(t)$ をデデキントは Primfunction とよんでいる．

極大イデアル $\mathfrak{m}=(p,P(t))$ について

$$F(t)\in\mathfrak{m}^2 \text{ ならば } \mathbf{F}_p[t] \text{ において } \overline{P}(t)^2 \mid \overline{F}(t)$$

となることは自明であるが，下で述べるデデキントの結果により

$$F(t)\in\mathfrak{m}^2 \text{ ならば } p^2 \mid \Delta(\theta) \quad (\Delta(\theta) \text{ は } \theta \text{ の判別式})$$

が成り立つ．$\Delta(\theta)$ は $F(t)$ と $F'(t)$ の終結式として計算でき，$\Delta(\theta)$ の各平方素因子 p に対して，$\overline{F}(t)$ の重複因子を求めれば特異点 $\mathfrak{m}$ の候補がすべて求められる．

例 (Dedekind[1]) $F(t)=t^4-t^3+t^2-2t+4$ を考える．$F(t)$ の判別式は $\Delta=11492=2^2\cdot13^2\cdot17$ である．$p=13$ のときは $F(t)\equiv(t^2+6t+2)^2 \bmod 13$ であるから，$\mathfrak{m}=(13,t^2+6t+2)$ は特異点の候補ではあるが，$F(t)\notin(13,t^2+6t+2)^2$ となり特異点にはならない．一方，$p=2$ に対しては，$\overline{F}(t)=t^2(t^2-t+1)$ となり，$F(t)\in(2,t)^2$ で

[1] Anzeige der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie, 1871年7月22日, Dedekind 全集 III, 論文番号 LV, 406頁参照. この例の存在は藤崎源二郎先生に教えていただきました.

あるから $\mathfrak{n}=(2,t)$ は（ただ1つの）特異点である．$\mathfrak{n}$ を中心とする2次変換 $u=t/2$ による $F(t)$ の固有変換は $F_1(u)=2^{-2}F(2u)=4u^4-2u^3+u^2-u+1\equiv u^2-u+1 \bmod 2$ となるから，$\mathfrak{o}_K$ において $(2)=\mathfrak{P}_1\mathfrak{P}_2, N(\mathfrak{P}_i)=2^2$ と分解することが分かる（図1）．

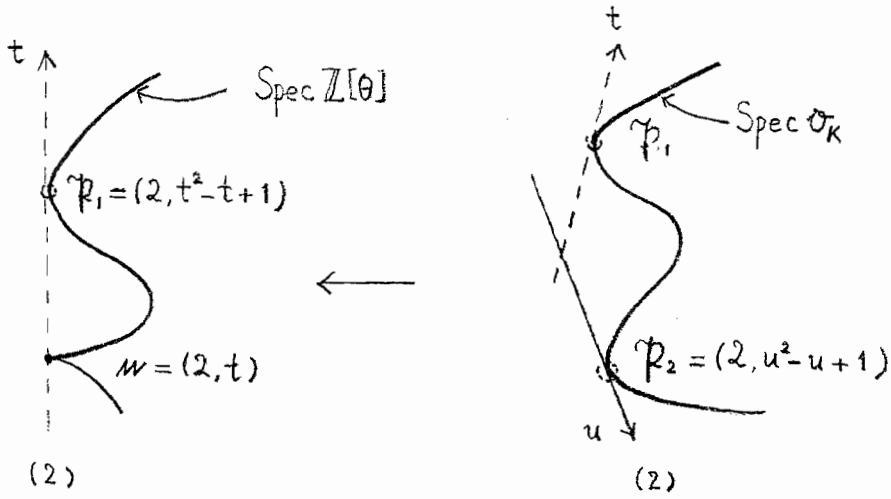

図1

デデキントがこのような例を構成したのは，代数体 K の主整数環 $\mathfrak{o}_K$ が，適当な定義方程式 $F(t)$ を用いて $\mathbf{Z}[t]/(F(t))=\mathbf{Z}[\theta]=\mathfrak{o}_K$ と表せるかどうかという問題に興味があったからである．上の例では，K において (2) が2つの2次の素イデアルに分解するが，$\mathbf{F}_2$ 上の既約な2次式は1つしかないから，どのような $F(t)$ を用いても $\mathbf{Z}[t]/(F(t))=\mathfrak{o}_K$ と表すことができない．デデキントは上の例のように，どのような $F(t)$ を用いても $\mathbf{Z}[t]/(F(t))=\mathfrak{o}_K$ と表せないための1つの「十分条件」として「$\mathfrak{o}_K$ の各元の判別式の共通の特異素因子（singuläre Primzahl），今日でいう仮因子，の存在」を突き止めた．上の例では2が仮因子である．しかし仮因子の存在は $\mathbf{Z}[t]/(F(t))=\mathfrak{o}_K$ と表せないことの必要条件ではない[2]．

その後デデキントは1878年に，個別の $F(t)$ に対しては「$\mathbf{Z}[t]/(F(t))=\mathbf{Z}[\theta]=\mathfrak{o}_K$ となることと $F(t)$ に特異点がないことが同値である」ことの証明を発表した．以下は，その論文「イデアルの理論と高次合同式の理論との関係について」[3] の最初の3節に解説をつけたものである．この論文には特異点という言葉こそ現れないが，実行している計算はまさしく特異点の計算である．

---

[2] Hasse の青本 H. Hasse, Zahlentheorie, Akademie-Verlag Berlin, 1949年, 335頁.

[3] Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Bd. 23, 3頁 – 38頁, 1878年1月5日.

§1

(この§ではディリクレの整数論講義[4] を引用して，後で必要な結果を要約している)
Ω を有理数体上 n 次の代数体，$\mathfrak{o}$ を Ω の中の全整数環とする．$\mathfrak{o}$ の $\mathbf{Z}$ 加群としての自由基底を $\omega_1, \omega_2, \ldots, \omega_n$ とする．Ω の判別式を $D = \Delta(\Omega)$ とする．$\theta \in \mathfrak{o}$ の判別式 $\Delta(\theta) = \Delta(1, \theta, \theta^2, \ldots, \theta^{n-1})$ に対して

$$\Delta(\theta) = \Delta(\Omega) k^2$$

となる有理整数 k がある．その絶対値を θ の指数 (Index) という．$k \neq 0$ のとき $1, \theta, \theta^2, \ldots, \theta^{n-1}$ は線形独立であり，θ は有理整数係数の既約な n 次の方程式

$$F(\theta) = \theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_n = 0$$

の根である．$\omega' = \varphi(\theta), \varphi(t) \in \mathbf{Z}[t]$ の形の元 ω' 全体のなす環 $\mathbf{Z}[\theta]$ を $\mathfrak{o}'$ とする．$\mathfrak{o}'$ は $\mathfrak{o}$ の部分環になる．このとき $\varphi(t)$ としては次数が $n-1$ 以下のものだけを考えればよい．$\mathfrak{o}'$ は $\mathbf{Z}$ 加群として $1, \theta, \theta^2, \ldots, \theta^{n-1}$ を自由基底にもつ．

さて，$p \nmid k$ となる素数 p を第1種 (erster Art)，$p \mid k$ となる素数 p を第2種 (zweiter Art) と呼ぶ．p が第1種のとき，$\mathfrak{o}'$ の元

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \ldots + x_{n-1}\theta^{n-1}$$

が $\omega' \in p\mathfrak{o}$ となるための必要十分条件は，係数 $x_0, x_1, x_2, \ldots, x_{n-1}$ がすべて p で割り切れることである．これは，k が $\mathfrak{o}' = \mathbf{Z} + \mathbf{Z}\theta + \cdots + \mathbf{Z}\theta^{n-1}$ から $\mathfrak{o} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \cdots + \mathbf{Z}\omega_n$ への $\mathbf{Z}$ 加群としての埋め込み写像 Φ の行列式の値であるから，$p \nmid k$ ならば Φ は $\bmod p$ で $\mathbf{F}_p$ 加群の同型 $\mathfrak{o}'/p\mathfrak{o}' = \mathbf{Z}[t]/(F(t), p) \to \mathfrak{o}/p\mathfrak{o}$ を引き起こすからである．

一方，p が第2種のときは，$\mathfrak{o}'$ の元

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \ldots + x_{n-1}\theta^{n-1}$$

であって，$\omega' \in p\mathfrak{o}$ をみたすが，係数 $x_0, x_1, x_2, \ldots, x_{n-1}$ のうちに p で割り切れないものが少なくとも1つあるものが存在する．これは上の埋め込み写像 Φ が $\bmod p$ で退化する，すなわち $\mathfrak{o}'/p\mathfrak{o}' = \mathbf{Z}[t]/(F(t), p) \to \mathfrak{o}/p\mathfrak{o}$ が自明でない核をもつから，その元の $\mathfrak{o}' = \mathbf{Z}[t]/(F(t))$ への持ち上げを ω' とすればよい．

---

[4] Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet, 2. Aufl., Vieweg und Sohn, Braunschweig, 1871 年.

§2

(この§の内容は良く知られている) 素数 p が第1種の場合に，p の $\mathfrak{o}$ における素イデアル分解

$$p\mathfrak{o} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_m^{e_m}$$

は $F = F(t)$ の $\mathbf{F}_p[t]$ における素因数分解

$$\overline{F}(t) = \overline{P}_1^{e_1}(t)\overline{P}_2^{e_2}(t)\dots\overline{P}_m^{e_m}(t)$$

で記述できることが示される．$\overline{P}_i(t)$ は最高次係数が1としてよい．これを次数が同じで最高次係数が1の整数係数多項式に持ち上げたものを $P_i = P_i(t)$ とすると，上の等式は

$$F \equiv P_1^{e_1}P_2^{e_2}\dots P_m^{e_m} \bmod p$$

と書いてもよい．$\mathfrak{o}$ の素イデアル $\mathfrak{p}_i$ は対応する $P_i(t)$ を用いて $p\mathfrak{o} + P_i(\theta)\mathfrak{o}$ と表すことができ，P_i の次数を f_i とすると $N(\mathfrak{p}_i) = p^{f_i}$ である．

§3

(ここに特異点の記述がある) §2 の $\overline{F}(t)$ の素因数分解を $\mathbf{Z}[t]$ に持ち上げて

$$F = P_1^{e_1}P_2^{e_2}\dots P_m^{e_m} - pM$$

とする．ここで次の定理 II[5] が成り立つ．

II. Ist der Index k der Zahl θ nicht theilbar durch p, so kann M nach dem Modul p durch keine Primfunction P theilbar sein, deren Quadrat in F aufgeht. (θ の指数 k が p で割り切れない場合は，mod p において，F の重複因子になるような既約因子 P で M を割るものはない.)

続いて定理 III[6] で，逆も正しいことが示される．

III. Ist M durch keine solche Primfunction P theilbar (mod. p), deren Quadrat zugleich in F aufgeht, so ist der Index k der Zahl θ nicht theilbar durch p. (mod p において，F の重複因子になるような既約因子 P で M の因子になるものがなければ，θ の指数 k は p で割り切れない.)

II の証明：$\overline{F}(t) = \overline{S}(t)\overline{P}(t)^e$ ($e \geqq 2$, $\overline{P}(t)$ と $\overline{S}(t)$ は互いに素) と分解すると仮定する．$p \nmid k$ であるから，§2 により，$\mathfrak{o}_K$ の素イデアルを $\mathfrak{p} = (p, P(\theta))$ とすると，$p\mathfrak{o}_K =$

5) 上記論文 3) の §3, 17 頁参照.
6) 上記論文 3) の §3, 19 頁参照.

$\mathfrak{a}\mathfrak{p}^e$ ($\mathfrak{a}$ と $\mathfrak{p}$ は互いに素) と分解する．$\overline{S}(t)$, $\overline{P}(t)$ の $\mathbf{Z}[t]$ への持ち上げで最高次係数が 1 となるものをそれぞれ $S(t)$, $P(t)$ とすると，$\mathbf{Z}[t]$ において $F(t)=S(t)P(t)^e-pM(t)$ と表すことができ，t に θ を代入して $\mathfrak{o}_K$ における等式

$$S(\theta)P(\theta)^e=pM(\theta)$$

を得る．この左辺は丁度 $\mathfrak{p}^e$ で割り切れるから，$\mathfrak{p}\nmid M(\theta)$ が分かる．これは $\mathbf{F}_p[t]$ において $\overline{P}(t)\nmid\overline{M}(t)$ を意味する（証明終り）．

III の証明：$p\mid k$ であるから，環 $\mathbf{Z}[t]/(F(t),p)$ の 0 でない元で環 $\mathfrak{o}_K/p\mathfrak{o}_K$ に写すと 0 になるものがある．すなわち次数が $n-1$ 以下で定数ではなく最高次係数が 1 の元 $\varphi(t)\in\mathbf{Z}[t]$ であって，$\overline{\varphi}(t)\neq 0$ かつ $\varphi(\theta)\in p\mathfrak{o}_K$ をみたすものが存在する．さて $\overline{\varphi}(t)$ と $\overline{F}(t)$ の最大公約式を考える．mod p でこの最大公約式となるような，次数が $n-1$ 以下で最高次係数が 1 の元 $A(t)\in\mathbf{Z}[t]$ を選ぶことができる．$A(t)$ は $\mathbf{Z}[t]$ において $A(t)=\varphi(t)\varphi_1(t)+F(t)\varphi_2(t)+p\varphi_3(t)$ $(\varphi_1(t),\varphi_2(t),\varphi_3(t)\in\mathbf{Z}[t])$ と表すことができる．ここで t に θ を代入すると $A(\theta)=\varphi(\theta)\varphi_1(\theta)+p\varphi_3(\theta)\in p\mathfrak{o}_K$ となる．特に $A(t)$ は定数ではないことが分かる．また θ の共役元 $\theta^{(i)}$ についても $A(\theta^{(i)})\in p\mathfrak{o}_{K^{(i)}}$ となるので，$A(\theta)$ の $\mathbf{Z}$ 上の最小多項式は

$$A(\theta)^s+ph_1A(\theta)^{s-1}+p^2h_2A(\theta)^{s-2}+\cdots+p^sh_s=0\ ,\ {}^\forall h_i\in\mathbf{Z} \tag{1}$$

の形になる．したがって $\mathbf{Z}[t]$ において

$$A(t)^s+ph_1A(t)^{s-1}+p^2h_2A(t)^{s-2}+\cdots+p^sh_s=F(t)G(t) \tag{2}$$

と表され，$\mathbf{F}_p[t]$ において

$$\overline{A}(t)^s=\overline{F}(t)\overline{G}(t) \tag{3}$$

が成り立つ．一方 $\mathbf{Z}[t]$ において

$$F(t)=A(t)B(t)-pM(t) \tag{4}$$

と表されるから，t に θ を代入して

$$A(\theta)B(\theta)=pM(\theta) \tag{5}$$

が得られる．また（4）の両辺の次数を比較して，$B(t)$ も定数でないことが分かる．さて（1）に $B(\theta)^s$ をかけると

$$\{A(\theta)B(\theta)\}^s+ph_1B(\theta)\{A(\theta)B(\theta)\}^{s-1}+\cdots+p^sh_sB(\theta)^s=0 \tag{6}$$

となる.（6）に（5）を代入して p^s で割ると

$$M(\theta)^s + h_1 B(\theta) M(\theta)^{s-1} + \cdots + h_s B(\theta)^s = 0 \tag{7}$$

となる．すなわち $\mathbf{Z}[t]$ において

$$M(t)^s + h_1 B(t) M(t)^{s-1} + \cdots + h_s B(t)^s = F(t)H(t) = A(t)B(t)H(t) - pM(t)H(t) \tag{8}$$

と表される.（8）から $\overline{B}(t) | \overline{M}(t)^s$ が分かる.

$\overline{B}(t)$ は定数ではないから，最高次係数が 1 で定数ではない元 $P(t) \in \mathbf{Z}[t]$ を，$\overline{P}(t)$ が $\overline{B}(t)$ の既約因子になるように選ぶ.（4）より $\overline{B}(t) | \overline{F}(t)$ であり,（3）より $\overline{P}(t)$ は $\overline{A}(t)$ の因子にもなっていることが分かる．したがって，

$$\overline{P}(t)^2 \mid \overline{F}(t) \text{ かつ } \overline{P}(t) \mid \overline{M}(t)$$

が成り立つ（証明終り）.

上の証明から，$\mathbf{Z}[t]$ において $A(t) = P(t)A_1(t) + pA_2(t)$，$B(t) = P(t)B_1(t) + pB_2(t)$，$M(t) = P(t)M_1(t) + pM_2(t)$ と表されることが分かる．これらをすべて（4）に代入すると，$\mathbf{Z}[t]$ において $F(t) = P(t)^2 A_1(t)B_1(t) + pP(t)\{A_1(t)B_2(t) + A_2(t)B_1(t) + M_1(t)\} + p^2 M_2(t) \in (p, P(t))^2$ が成り立つことが分かる．したがって，定理 II と定理 III は

II. $p \nmid k$ ならば，$F(t) \in \mathfrak{m}^2$ となる極大イデアル $\mathfrak{m} = (p, P(t))$ は存在しない

III. $p \mid k$ ならば $F(t) \in \mathfrak{m}^2$ となる極大イデアル $\mathfrak{m} = (p, P(t))$ が存在する

と書き換えられる．k の値はすぐには分からないが，$\Delta(\theta) = \Delta(\Omega)k^2$ であるから，$p \mid k$ となる p は $\Delta(\theta)$ の平方素因子の 1 つである．また $k^2 = 1$ と $\mathfrak{o} = \mathbf{Z}[\theta]$ は同値であるからデデキントの結果は

「$\mathbf{Z}[\theta]$ が $\mathfrak{o}$ の真の部分環であることと $F(t)$ に特異点が存在することは同値」

と言い換えることができる．これらの結果を用いると p の Ω における素イデアル分解が定義方程式の特異点を中心とする 2 次変換と合同式の計算だけで，すなわち $\mathfrak{o}$ の整数基底や判別式を用いずに，初等的に求めることができる[7].

[7] 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.