非特異3次曲線の標準形

大塚美紀生

楕円曲線は今や代数曲線論の枠を越えて，整数論や暗号理論など他の専門分野への応用も目覚しく，多くの人々の関心を集めている。楕円曲線とは，非特異3次曲線のことであり，代数的には群構造を持つことが特徴である。

$x,\ y,\ z$ の斉次3次方程式は一般に

$$ax^3+bx^2y+cx^2z+dxy^2+exyz+fxz^2+gy^3+hy^2z+lyz^2+mz^3=0 \quad (1)$$

と表されるが，このままでは未知定数が多過ぎて，一般論を展開するには不都合である。そこで，非特異の仮定のもとで，適当に変数変換してどのような式に同値変形すればよいかという問題が生じるが，ワイエルシュトラスの $\wp$ 関数 $\wp(w)$[注1] が

$$\wp'(w)^2=4\wp(w)^3-g_2\wp(w)-g_3 \quad (g_2,\ g_3 \text{は定数})$$

を満たすことをモデルとして，ワイエルシュトラス標準形[注2]

$$y^2z=x^3+pxz^2+qz^3$$

に帰着させて考えることが多い。

定理の形にまとめると

定理　非特異3次曲線の方程式は，複素射影空間[注3]における適当な座標変換により，ワイエルシュトラス方程式

$$y^2z=x^3+pxz^2+qz^3$$

に帰着させることができる。

この定理は楕円曲線を学ぶ出発点の一つではあるが，大抵の代数曲線論(あるいは代数幾何学)の教科書では，一般次数の曲線に対する変曲点[注4]とベズーの定理[注5]という一般理論をまず学んでから証明している。もちろん，この定理の準備のためだけに一般理論を構築しているわけではないのだが，楕円曲線のみを学びたい者にとっては負担が大きいと言える。

本稿では，非特異3次曲線を直接考え，実際に変数を置き換えていくという初等的手法によりこの定理を証明する。

射影空間における曲線

本稿では，高校数学では登場しない用語も出てくるので，簡単にまとめておくことにする。数学についての知識のある方は，読み飛ばしていただいて差し支えない。

高校数学に出てくる座標空間 $\boldsymbol{R}^3 = \{(x,\ y,\ z) \mid x,\ y,\ z \in \boldsymbol{R}\}$ と同様に，座標を複素数にした 3 次元アフィン空間

$$\boldsymbol{C}^3 = \{(x,\ y,\ z) \mid x,\ y,\ z \in \boldsymbol{C}\}$$

も考えることができる。$\boldsymbol{C}^3$ から原点 $(0,\ 0,\ 0)$ を除いた集合において，0 でない定数倍を同一視して得られる空間

$$\boldsymbol{P_C}^2 = \{[X : Y : Z] \mid X,\ Y,\ Z \in \boldsymbol{C},\ (X,\ Y,\ Z) \neq (0,\ 0,\ 0)\}$$

を ($\boldsymbol{C}$ 上) 2 次元**射影空間**[注6]という。高校数学流に言えば，座標空間において原点を通る直線の方向ベクトルの集合と同じようなものである。

$\boldsymbol{P_C}^2$ に属する点 $[X : Y : Z]$ のうち $Z \neq 0$ であるものは $\boldsymbol{P_C}^2$ において $\left[\dfrac{X}{Z},\ \dfrac{Y}{Z},\ 1\right]$ と同じ点であるから，2 次元アフィン空間 $\boldsymbol{C}^2$ の点 $\left(\dfrac{X}{Z},\ \dfrac{Y}{Z}\right)$ と同一視できる。

$\boldsymbol{P_C}^2$ に属する点 $[X : Y : 0]$ は $(X,\ Y,\ 0) \neq (0,\ 0,\ 0)$ を満たすから $X \neq 0$ または $Y \neq 0$ であり，1 次元射影空間 $\boldsymbol{P_C}$ の点 $[X : Y]$ と同一視できる。したがって，

$\boldsymbol{P_C}^2$ は 2 次元アフィン空間 $\boldsymbol{C}^2$ と 1 次元射影空間 $\boldsymbol{P_C}$ を合わせた空間

とみることができる。ときには $Z = 1$ との交わりとして，慣れている $\boldsymbol{C}^2$ に帰着させて考えることもあるが，$X,\ Y,\ Z$ を同等にみることで方程式を処理しやすくしたり，$\boldsymbol{C}^2$ からでは気づきにくい本質をとらえるために射影空間を考えるのである。

射影空間における図形を表す多項式 $F(X,\ Y,\ Z)$ は，任意の定数 k に対して

$$F(kX,\ kY,\ kZ) = 0 \iff F(X,\ Y,\ Z) = 0$$

でなければないから，必然的にすべての項が同次となる。すべての項が同次である多項式を**斉次多項式**といい，斉次多項式で表される方程式を**斉次方程式**という。(1)は 3 次の斉次方程式である。斉次多項式でない多項式を非斉次多項式という。

$x,\ y,\ z$ の多項式 $f(x,\ y,\ z) = \sum_{i,\,j,\,k} x^i y^j z^k$ において $y,\ z$ を固定し，x だけの関数とみて微分することを x で **偏微分**するという。そのときの導関数を x による**偏導関数**といい，$f_x(x,\ y,\ z)$ で表す。y による偏導関数 $f_y(x,\ y,\ z)$，z による偏導関数 $f_z(x,\ y,\ z)$ も同様に定義される。

斉次方程式 $F(X,\ Y,\ Z) = 0$ で定義される曲線上の点 $\mathrm{P}(a,\ b,\ c)$ が

$$F_X(a,\ b,\ c) = F_Y(a,\ b,\ c) = F_Z(a,\ b,\ c) = 0$$

を満たすとき，P を**特異点**という。図形的に考えると，

$$F_X(a,\ b,\ c)X + F_Y(a,\ b,\ c)Y + F_Z(a,\ b,\ c)Z = 0$$

は点 P における曲線 $F(X,\ Y,\ Z) = 0$ の接線[注7]を表すから，特異点においては法線ベクトルが退化することを意味する。曲線が特異点を持たないとき，**非特異**であるという。

定理の証明

3 次斉次方程式は一般に

$$ax^3+bx^2y+cx^2z+dxy^2+exyz+fxz^2+gy^3+hy^2z+lyz^2+mz^3=0 \quad (1)$$

と表され，さらに非特異であることを仮定する。

適当な変数変換により，曲線(1)は点 $(0,\ 1,\ 0)$ を通るようにできるはずである。

$a=0$ のときは，x と y を入れ替える座標変換を行えば，

$$g=0$$

とできる。$ag\neq 0$ のとき

$$gy^3+dxy^2+bx^2y+ax^3=g(y-\alpha x)(y-\beta x)(y-\gamma x),\quad \alpha\beta\gamma\neq 0$$

を満たす複素数 $\alpha,\ \beta,\ \gamma$ が存在する。このとき，曲線(1)は点 $(1,\ \alpha,\ 0)$ を通るから，

$$(x,\ y)\to(y,\ x+\alpha y)$$

と変数変換すると，曲線(1)は点 $(0,\ 1,\ 0)$ を通る曲線となる。したがって，

$$g=0 \quad (2)$$

を満たす曲線に座標変換できる。

$l=0$ のときは，x と z を入れ替える座標変換を行えば，

$$b=0$$

とできる。$bl\neq 0$ ならば

$$b\alpha^2-e\alpha\beta+l\beta^2=0,\quad \alpha\beta\neq 0$$

を満たす複素数 $\alpha,\ \beta$ を定めることができて，

$$\begin{aligned} b(\alpha x)^2y+e(\alpha x)y(\beta z)+ly(\beta z)^2 &= y(b\alpha^2x^2+e\alpha\beta xz+l\beta^2z^2)\\ &= y\left\{b\alpha^2x^2+(b\alpha^2+l\beta^2)xz+l\beta^2z^2\right\}\\ &= y\left\{l\beta^2(x+z)^2+(b\alpha^2-l\beta^2)x(x+z)\right\}\end{aligned}$$

と変形される。$(x,\ z)\to(\alpha x,\ \beta z)$ および $z\to z-x$ と変数変換すると，

$$bx^2y+exyz+lyz^2\to(b\alpha^2-l\beta^2)xyz+l\beta^2yz^2$$

と書き換えられるから，点 $(0,\ 1,\ 0)$ を通ることを保存したままで

$$b=0 \quad (3)$$

となるように変数変換できる。

(1)の左辺に (2), (3)を適用して

$$\varphi(x,\ y,\ z)=ax^3+cx^2z+dxy^2+exyz+fxz^2+hy^2z+lyz^2+mz^3$$

とおくと，

$$\begin{aligned}&\varphi_x(x,\ y,\ z)=3ax^2+2cxz+dy^2+eyz+fz^2,\quad \varphi_x(0,\ 1,\ 0)=d\\ &\varphi_y(x,\ y,\ z)=2dxy+exz+2hyz+lz^2,\quad \varphi_y(0,\ 1,\ 0)=0\\ &\varphi_z(x,\ y,\ z)=cx^2+exy+2fxz+hy^2+2lyz+3mz^2,\quad \varphi_z(0,\ 1,\ 0)=h\end{aligned}$$

点 $(0,\ 1,\ 0)$ は特異点ではないから，点 $(0,\ 1,\ 0)$ における接線

$$dx+hz=0 \ ^{注7}$$

が定まり，この接線が直線 $z=1$ になるように座標変換することができる。もう少し詳しく述べると，$h=0$ のときは非特異である仮定より $d\neq 0$ であるから，x を $x+z$

に置き換えることにより，これまでの性質を保存したまま

$$h \neq 0$$

とできて，$z \to \dfrac{z-dx}{h}$ と置き換えれば[注8]点 $(0,\ 1,\ 0)$ における接線は $z=1$ となり，

$$d=0,\quad h=1 \tag{4}$$

となるようにできる。

(2), (3), (4)を盛り込むと

$$\begin{aligned}\varphi(x,\ y,\ z) &= ax^3+cx^2z+fxz^2+z(y^2+exy+lyz)+mz^3\\ &= ax^3+cx^2z+fxz^2+z\Big(y+\frac{e}{2}x+\frac{l}{2}z\Big)^2-z\Big(\frac{e}{2}x+\frac{l}{2}z\Big)^2+mz^3\\ &= ax^3+\Big(c-\frac{e^2}{4}\Big)x^2z+\Big(f-\frac{el}{2}\Big)xz^2\\ &\qquad +z\Big(y+\frac{e}{2}x+\frac{l}{2}z\Big)^2+\Big(m-\frac{l^2}{4}\Big)z^3\end{aligned}$$

であり，$y \to y-\dfrac{e}{2}x-\dfrac{l}{2}z$ および $z \to -z$ により変数変換すると，$\varphi(x,\ y,\ z)=0$ は

$$y^2z = Ax^3+Bx^2z+Cxz^2+Dz^3 \quad (A,\ B,\ C,\ D \text{は定数})$$

に帰着される。

ここで，座標変換により曲線の非特異性が損なわれないことに注目して，$A \neq 0$ であることを示す。$A=0$ であるとすれば，

$$\begin{aligned}F(x,\ y,\ z) &= Bx^2z+Cxz^2+Dz^3-y^2z\\ F_x(x,\ y,\ z) &= 2Bxz+Cz^2\\ F_y(x,\ y,\ z) &= -2yz\\ F_z(x,\ y,\ z) &= Bx^2+2Cxz+3Dz^2-y^2\end{aligned}$$

をすべて 0 とするような $(x,\ y,\ z)$ が存在[注9]して，非特異であることに反するから

$$A \neq 0$$

よって，$A=\alpha^3$ となる 0 でない複素数 α が存在するから，$x \to \dfrac{x}{\alpha}$ と変換することにより，定数 $B,\ C,\ D$ を改めて

$$y^2z = x^3+Bx^2z+Cxz^2+Dz^3 \quad (B,\ C,\ D \text{は定数})$$

の形であると考えられる。右辺を立方完成すると

$$x^3+Bx^2z+Cxz^2+Dz^3 = \Big(x+\frac{B}{3}z\Big)^3+\Big(C-\frac{B^2}{3}\Big)xz^2+\Big(D-\frac{B^3}{27}\Big)z^3$$

となるから，$x \to x-\dfrac{B}{3}z$ により変換して $p=C-\dfrac{B^2}{3}$，$q=D-\dfrac{B^3}{27}$ で置き換えると，方程式(1)は最終的に

$$y^2z = x^3+pxz^2+qz^3$$

と同値になるように座標変換される。 (証明おわり)

注 1　ワイエルシュトラスの $\wp$ 関数 $\wp(w)$ とは，

$$\wp(w) = \frac{1}{w^2} + \sum_{\alpha \in L'} \left\{ \frac{1}{(w-\alpha)^2} - \frac{1}{\alpha^2} \right\}$$

で定義される関数である。ここで，L' についての和は複素平面上のある格子 L の 0 以外のすべての数にわたる。複素平面上の **格子** L とは，複素平面上で線形独立な複素数 α_1，α_2 を用いて

$$L = \{ m\alpha_1 + n\alpha_2 \,\big|\, m,\ n \in \boldsymbol{Z} \}$$

と表される数集合のことである。

$$g_2 = 60 \sum_{\alpha \in L'} \frac{1}{\alpha^4},\quad g_3 = 140 \sum_{\alpha \in L'} \frac{1}{\alpha^6}$$

とおくとき，ワイエルシュトラスの $\wp$ 関数 $\wp(w)$ は

$$\wp'(w)^2 = 4\wp(w)^3 - g_2\wp(w) - g_3$$

を満たす。ワイエルシュトラスの $\wp$ 関数は楕円関数として重要な関数であるが，ここではこれ以上深入りはしない。関心を持たれた方は，[5] などの書物を参考にされたい。

注 2　高校数学の感覚では「別物」と思われるかも知れないが，

$$y^2z = x^3 + pxz^2 + qz^3$$

において $x \to \sqrt[3]{4}\, x$ と変数変換し，$p = -\dfrac{g_2}{\sqrt[3]{4}}$，$q = -g_3$ と置き換えれば

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

となるので，本質的には変わらないのである。

注 3　定理の証明の中で，代数方程式を満たす複素数の存在を用いているので，有理数や実数の範囲では必ずしも成り立たない。一方，複素数体を一般の代数的閉体しても，(代数方程式の解は存在するので)定理の証明はそのまま通用する。

注 4　代数幾何学において，**変曲点**とは，特異点ではなく接線との接触位数(接線の方程式と連立させたときの方程式の解の重複度)が 3 以上である点のことをいう。高校数学では，凹凸の変わり目を変曲点と呼んでいるので，少し意味がずれるので注意する。例えば，曲線 $y = x^4$ 上の原点は高校数学では変曲点ではないが，接触位数は 4 であるから，代数幾何学では変曲点と呼ぶ。

注 5　複素射影平面 $\boldsymbol{P_C}^2$ 上の m 次曲線 C_1 と n 次曲線 C_2 が共通成分を持たないとき，重複度も数えた C_1 と C_2 の交点数は mn となる。これを**ベズー(Bézout)の定理**という。高校数学の範囲では(微分法を用いない)代数曲線は 2 次以下しか扱わないので，ベズーの定理は直観的に明らかだと誤解されそうであるが，3 次以上になると格段に構造は難しくなる。

注 6　1 次元の射影空間を**射影直線**，2 次元の射影空間を**射影平面**と呼ぶこともある。空間の中での直線・平面との混同を避けるため，射影空間で通している。

注 7　射影空間に慣れていない人のために，接線について補足しておく。

射影平面(2 次元射影空間)上で，曲線 $F(X,\ Y,\ Z)=0$ の点 $(a,\ b,\ c)$ における接線を通常の座標空間における接平面として方程式を導くと，

$$F_X(a,\ b,\ c)(X-a)+F_Y(a,\ b,\ c)(Y-b)+F_Z(a,\ b,\ c)(Z-c)=0$$

となる。これを射影平面で考えれば接線の方程式のはずであるが，一見斉次式には見えない。実は，斉次多項式についてのオイラーの公式

$$XF_X(X,\ Y,\ Z)+YF_Y(X,\ Y,\ Z)+ZF_Z(X,\ Y,\ Z)=dF(X,\ Y,\ Z)$$
$$(d \text{ は } F(X,\ Y,\ Z) \text{ の次数})$$

から，定数項について

$$-F_X(a,\ b,\ c)a-F_Y(a,\ b,\ c)b-F_Z(a,\ b,\ c)c=dF(a,\ b,\ c)=0$$

が成り立ち，射影曲線 $F(X,\ Y,\ Z)=0$ の点 $(a,\ b,\ c)$ における接線の方程式は

$$F_X(a,\ b,\ c)X+F_Y(a,\ b,\ c)Y+F_Z(a,\ b,\ c)Z=0$$

と表される。

なお，上述のオイラーの公式については，各項ごとに示されれば十分であるが，意外と簡単に確かめられる。

$$G(X,\ Y,\ Z)=X^iY^jZ^k \quad (i\geqq 0,\ \ j\geqq 0,\ \ k\geqq 0,\ \ i+j+k=d)$$

とすると，

$$G_X(X,\ Y,\ Z)=iX^{i-1}Y^jZ^k$$
$$G_Y(X,\ Y,\ Z)=X^i(jY^{j-1})Z^k$$
$$G_Z(X,\ Y,\ Z)=X^iY^j(kZ^{k-1})$$

であるから，

$$\begin{aligned}&XG_X(X,\ Y,\ Z)+YG_Y(X,\ Y,\ Z)+ZG_Z(X,\ Y,\ Z)\\&=X\cdot iX^{i-1}Y^jZ^k+Y\cdot X^i(jY^{j-1})Z^k+Z\cdot X^iY^j(kZ^{k-1})\\&=(i+j+k)X^iY^jZ^k\\&=dG(X,\ Y,\ Z)\end{aligned}$$

注 8　$z'=dx+hz\ (h\neq 0)$ とおくと，$z=\dfrac{z'-dx}{h}$ である。

この変数変換で，変換前の d と変換後の d を混同して $d=0$ に帰着できないと錯覚してしまいそうであるが，x と $z'(=dx+hz)$ の線形結合で表示していることに注意しなければならない。実際，$s,\ t$ を複素定数として

$$dx+hz=sx+t(dx+hz)=(s+dt)x+htz$$

とおくと，

$$s+dt=d \text{ かつ } ht=h \text{ かつ } h\neq 0$$

より，$s=0,\ t=1$ となることがわかる。

注 9　具体的に計算すると，

$$F(x,\ y,\ 0) = F_x(x,\ y,\ 0) = F_y(x,\ y,\ 0) = 0,$$
$$F_z(x,\ y,\ 0) = Bx^2 - y^2$$

$\beta^2 = B$ を満たす複素数 β が存在して

$$F_z(1,\ \beta,\ 0) = B\cdot 1^2 - \beta^2 = 0,\quad (1,\ \beta,\ 0) \neq (0,\ 0,\ 0)$$

したがって，$A = 0$ ならば特異点 $(1,\ \beta,\ 0)$ が存在してしまう。

参考文献

[1] R. Akhtar, *An Introduction to Elliptic Curves*,
Algebra Short Course (SUMSRI) Miami University (2002)
http://www.theoremoftheday.org/Docs/RezaAkhtar.pdf

[2] C. C. Gibson, *Elementary Geometry of Algebraic Curves*, Cambridge (1998)

[3] 長岡亮介，線型代数入門講義，東京図書 (2010)

[4] 永田雅宜，高校生のための代数幾何，現代数学社 (1997)

[5] S. Lang, *Elliptic Functions*, Addison-Wesley (1973)

[6] 志賀啓成，複素解析学， 培風館 (1997)

[7] *inflection points and canonical forms of non-singular cubic curves* (2013)
http://planetmath.org/inflectionpointsandcanonicalformsofnonsingularcubiccurves

2013.8.21