楕円曲線とは何か?*

あと べ
$\mathrm{Tr}(\mathfrak{b})$

概 要

体 K 上の楕円曲線とは, $y^2 = f(x), f(x)$ は重根を持たない K-係数 3 次多項式で定義される曲線 (に無限遠点を付け加えたもの) のことである. 楕円曲線には, 自然に群構造が入ることが知られている. 代数幾何学の手法では, この群がどのような構造であるかを調べるのは難しい. ところが $\mathbb{C}$ 上の楕円曲線に限れば, 複素函数論の知識から, 楕円曲線がより簡単な群と同型であることを示すことが出来る. この講演では, その方法を紹介したい.

1 イントロ

体 $\mathbb{C}$ 上の楕円曲線とは, $y^2 = f(x), f(x)$ は重根を持たない $\mathbb{C}$-係数 3 次多項式で定義される曲線であるが, 変数変換により,x^2 の項は消せるので, 次の定義を採用する.

定義 1.1. $c_2, c_3 \in \mathbb{C}, c_2^3 - 27c_3^2 \neq 0$ を用いて,

$$\begin{aligned} E &= \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - c_2x - c_3\} \cup \{O_E\} \\ &= \{[x : y : z] \in \mathbb{CP}^2 \mid y^2z = 4x^3 - c_2xz^2 - c_3z^3\} \end{aligned}$$

と表される曲線を楕円曲線という.

注意 1.2.
(1) より本質的な定義もあるが, それはこの講演のネタバレを含むので, 今回は上の定義を採用する.
(2) 多項式 $4x^3 - c_2x - c_3$ が重根を持たないための必要十分条件が, $c_2^3 - 27c_3^2 \neq 0$ である.
(3) O_E は E の無限遠点である. 射影座標では, これは $[0 : 1 : 0]$ に対応する.

定理 1.3. E を $\mathbb{C}$ 上の楕円曲線とする. この時, 代数的な写像

$$\oplus \colon E \times E \to E$$

であって,$(E, \oplus, O_E)$ が Abel 群となるものが存在する.

*第 3 回関西すうがく徒のつどいにおいて発表された

証明の方法

(0) 信じて計算する.

(1) Max Noether の基本定理を用いる.

(2) Riemann-Roch の定理を認めて,Picard 群を用いる.

(3) 一意価定理を用いる.

(3) の方法は $\mathbb{C}$ 上の楕円曲線にしか適用出来ないが, 群構造が良く分かる. 以下, これの説明をする.

2 コンパクト Riemann 面からの準備

定義 2.1. Riemann 面とは, 連結な複素 1 次元多様体のこと.

例 2.2. $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ を Riemann 球面と言う.

定理 2.3. (開写像定理)

M, N をコンパクト Riemann 面とし, $f\colon M \to N$ を定数でない正則写像とする. この時,f は開写像である. 特に f は全射である.

M, N, f を上の通りとし,$f(p) = q$ とする. この時,p の開近傍 $U \subset M$,q の開近傍 V と $0 \in \mathbb{C}$ の開近傍 $U', V' \subset \mathbb{C}$ が存在して, 次の図式が可換となるような写像が取れる.

$$\begin{array}{ccccccc} M & \xleftarrow[open]{} & U & \xrightarrow{f} & V & \xrightarrow[open]{} & N \\ & & \cong\downarrow & \circlearrowleft & \downarrow\cong & & \\ \mathbb{C} & \xleftarrow[open]{} & \tilde{U} & \xrightarrow{\tilde{f}} & \tilde{V} & \xrightarrow[open]{} & \mathbb{C}, \end{array} \qquad \begin{array}{ccc} p & \longmapsto & q \\ \downarrow & & \downarrow \\ 0 & \longmapsto & 0. \end{array}$$

この時,$\tilde{f}\colon \tilde{U} \to \tilde{V}$ は正則写像なので,Taylor 展開

$$\tilde{f}(z) = \sum_{n=e_p}^{\infty} a_n z^n, \quad e_p \in \mathbb{Z}_{>0}, a_n \in \mathbb{C}, a_{e_p} \neq 0$$

を持つ. 整数 e_p は f と p のみに依存する. これを p における f の分岐指数と言う. この時, 次の定理が成り立つ.

定理 2.4. M, N, f は上の通りとし,$q \in N$ する. この時,

$$\sum_{p \in f^{-1}(\{q\})} e_p$$

は q によらず一定である. この値を f の次数と言い,$\deg(f)$ と書く.

定義 2.5. M をコンパクト Riemann 面とする. M から $\widehat{\mathbb{C}}$ への正則写像で恒等的に ∞ でないものを M 上の有理型函数と言う. M 上の有理型函数全体のなす体を $K(M)$ で表す.

命題 2.6. f をコンパクト Riemann 面 M 上の有理型函数で, 定数でないものとする. この時,

$$[K(M) : \mathbb{C}(f)] = \deg(f)$$

が成り立つ.

定理 2.7. (分離定理)

M をコンパクト Riemann 面とし,$p, q \in M$ とする. この時, 任意の $f \in K(M)$ に対して,$f(p) = f(q)$ が成り立つならば, $p = q$ である.

3 楕円函数

$\mathfrak{H} = \{z \in \mathbb{C} \,\big|\, \mathrm{Im} z > 0\}$ を上半平面と言う.

$\omega_1, \omega_2 \in \mathbb{C}, \omega_1/\omega_2 \in \mathfrak{H}$ の時, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ を $\mathbb{C}$ 内の格子と言う. $\mathbb{C}/\Lambda$ には自然にコンパクト Riemann 面の構造が入る.

定義 3.1. $\mathbb{C}$ 上の有理型函数 f が任意の $z \in \mathbb{C}$ と $\omega \in \Lambda$ に対して,

$$f(z + \omega) = f(z)$$

を満たす時,f を周期 Λ の楕円函数であると言う.

注意 3.2. 自然な 1 対 1 対応

$$\{ \text{周期}\Lambda\text{の楕円函数} \} \leftrightarrow K(\mathbb{C}/\Lambda)$$

がある.

定義 3.3. $\wp(z) = \wp(z; \Lambda)$ を次で定める.

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

これを Weierstrass の $\wp$-函数と言う.

定理 3.4. ($\wp$-函数の性質)

(1) $\wp, \wp'$ は $\mathbb{C} \setminus \Lambda$ 上, 局所一様絶対収束し, 周期 Λ の楕円函数を定める. 特に,Λ にのみ極を持つ.

(2) $k \geq 3$ に対して,

$$G_k = G_k(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-k}$$

とおく時,$\wp, \wp'$ の $z = 0$ での Laurent 展開は次のようになる.

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2} z^{2n},$$

$$\wp'(z) = -\frac{2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1) G_{2n+2} z^{2n-1}.$$

(3)

$$g_2 = g_2(\Lambda) = 60G_4 = 60 \sum_{\omega\in\Lambda,\omega\neq 0} \omega^{-4},$$
$$g_3 = g_3(\Lambda) = 140G_6 = 140 \sum_{\omega\in\Lambda,\omega\neq 0} \omega^{-6}$$

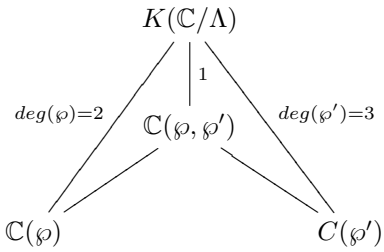
とおくと,$\wp, \wp'$ は次の関係式を満たす.

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

(4) 任意の格子 Λ に対して,$g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$.

定理 3.5. $K(C/\Lambda) = \mathbb{C}(\wp, \wp')$. 即ち, 格子 Λ を周期とする楕円函数は $\wp$ と $\wp'$ で表せる.

Proof. 定理 3.4(2) より,$\deg(\wp) = 2, \deg(\wp') = 3$ である. よって、主張は, 命題 2.6 から分かる.(下図参照)



□

定理 3.6. Λ が $\mathbb{C}$ 内の格子の時,

$$E[\Lambda] = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3\} \cup \{O_E\}$$

は $\mathbb{C}$ 上の楕円曲線であり, 写像

$$f\colon \mathbb{C}/\Lambda \to E[\Lambda]$$
$$z \mapsto (\wp(z), \wp'(z))$$

は全単射である. この写像を通して,$E[\Lambda]$ に群構造が入る.

Proof. $E[\Lambda]$ が楕円曲線であることは, 定理 3.4(4) から従う. また, そこから,$E[\Lambda]$ がコンパクトな複素 1 次元多様体であることも分かる.

Chow の定理より,$E[\Lambda]$ は複素多様体として連結であることが分かる. ゆえに $E[\Lambda]$ はコンパクト Riemann 面である.

写像 f は正則写像であり, 定数でない. ゆえに, 定理 2.3 より,f は全射である.

単射性は, 定理 3.5 と定理 2.7 から従う. □

定理 3.6 より,

$$\Phi\colon \{\mathbb{C} \text{ 内の格子 }\} \to \{\mathbb{C} \text{ 上の楕円曲線 }\}, \Lambda \mapsto E[\Lambda]$$

という写像が得られ, その像には群構造が入ることが分かった.

定理 1.3 を示すには,Φ の全射性が必要になる. これを保証するのが次の一意化定理である.

定理 3.7. (一意化定理)
$c_2^3 - 27c_3^2 \neq 0$ を満たす任意の複素数 c_2, c_3 に対して, $\mathbb{C}$ 内の格子 Λ で,

$$g_2(\Lambda) = c_2, g_3(\Lambda) = c_3$$

を満たすものがちょうど一つ存在する.

注意 3.8.
(1) 一意化定理は上の写像 Φ の全単射性を意味する.
(2) これにより, 楕円曲線は群として,$(\mathbb{R}/\mathbb{Z})^2$ と同型であることが分かる.
(3) $\wp$-函数の加法定理から, 楕円曲線の群法則が得られる.
(4) Φ の逆写像を楕円積分といい,

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \longleftrightarrow E$$

の時,ω_1, ω_2 を楕円曲線 E の周期と言う.

以下, 一意化定理の証明の概略を見る.

4 モジュラー函数

$\mathbb{C}$ 内の格子全体を定義域とする写像を考えるのは難しい. そこで, 特別な格子を考える.

$\tau \in \mathfrak{H}$ に対して,$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ とし,

$$G_k(\tau) = G_k(\Lambda_\tau) = \sum_{m,n\in\mathbb{Z},(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^k}$$

とおく. これは $k \geq 4$ の時, 局所絶対一様収束し,$\mathfrak{H}$ 上の正則関数を定める.

$\Lambda \cong \mathbb{Z}^2$ なので,$\mathrm{Aut}(\Lambda) = GL_2(\mathbb{Z})$ である. $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(Z)$ の時,

$$\gamma\Lambda_\tau = \mathbb{Z}(a\tau+b) + \mathbb{Z}(c\tau+d) = (c\tau+d)\Lambda_{\gamma(\tau)}$$

である. 但し,$\gamma(\tau) = \dfrac{a\tau+b}{c\tau+d}$ である.

$\mathrm{Im}(\gamma(\tau)) = \dfrac{\det(\gamma)}{|c\tau+d|}\mathrm{Im}(\tau)$ なので,$\gamma(\tau) \in \mathfrak{H} \Leftrightarrow \gamma \in SL_2(\mathbb{Z})$ である.
$\Gamma = SL_2(\mathbb{Z})$ とおくと $\gamma \in \Gamma$ の時,$\gamma\Lambda = \Lambda$ より次を得る.

$$G_k(\tau) = G_k((c\tau+d)\Lambda_{\gamma(\tau)}) = (c\tau+d)^{-k}G_k(\gamma(\tau)).$$

特に $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ として, $G_k(\tau+1) = G_k(\tau)$ を得る. ゆえに G_k は Fourier 展開が出来る.k が偶数の時, それは次で与えられることが知られている.

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

但し,ζ は Riemann の ζ 函数,$q = e^{2\pi i\tau}$, $\sigma_s(n) = \sum_{0<d|n} d^s$ である.

以上をまとめて次を得る.

命題 4.1. $k \geq 4$, 偶数の時,G_k は次を満たす.
(M-1) G_k は $\mathfrak{H}$ 上正則である.
(M-2) 任意の $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ と任意の $\tau \in \mathfrak{H}$ に対して,

$$G_k(\gamma(\tau)) = (c\tau+d)^k G_k(\tau)$$

が成り立つ.
(M-3) G_k は次の形の Fourier 展開を持つ.

$$G_k(\tau) = \sum_{n=0}^{\infty} a_n(G_k)q^n \quad , a_n(G_k) \in \mathbb{C}.$$

(M-1),(M-2),(M-3) を満たす $\mathfrak{H}$ 上の函数を重さ k, レベル 1 の正則モジュラー形式 (または, 重さ k の正則保型形式) と言う.

$g_2(\tau) = 40G_4(\tau), g_3(\tau) = 140G_6(\tau), \Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$ とおく. 定理 3.4(4) より,$\Delta(\tau)$ は $\mathfrak{H}$ 上零点を持たない.

$$J(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)}$$

とおく.$J(\tau)$ をレベル 1 のモジュラー函数と呼ばれる函数の一つである. これは次を満たす.

定理 4.2. $J(\tau)$ は Γ-不変な $\mathfrak{H}$ 上の正則関数であり, 次の形の Fourier 展開を持つ.

$$J(\tau) = q^{-1}\left(1 + \sum_{n=1}^{\infty} c_n q^n\right) \quad , c_n \in \mathbb{Z}.$$

この函数の更なる情報を引き出すには, 定義域となる商空間 $\Gamma\backslash\mathfrak{H}$ を調べる必要がある. 基本領域を調べると次が分かる.

命題 4.3. $\Gamma\backslash\mathfrak{H}$ の代表系の閉包として, 次のものが取れる.

$$F = \left\{ \tau \in \mathfrak{H} \,\middle|\, -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq \frac{1}{2}, |\tau| \geq 1 \right\}.$$

商空間 $\Gamma\backslash\mathfrak{H}$ には,Riemann 面の構造が入りそうだが, この基本領域を見ると, それはコンパクトではなさそうである. しかしながら, 無限遠点をつけるとコンパクトになりそうである.

無限遠点 ∞ の Γ-軌道は, $\{\infty\} \cup \mathbb{Q}$ であるので, $\mathfrak{H}^* = \mathfrak{H} \cup \{\infty\} \cup \mathbb{Q}$ とおくと, Γ は $\mathfrak{H}^*$ に作用する. この時, 次が成り立つ.

定理 4.4. 商空間 $\Gamma\backslash\mathfrak{H}^*$ には自然なコンパクト Riemann 面の構造が入る.

例 4.5. $\infty \in \mathfrak{H}^*$ の基本近傍系として次のものを取る.

$$U_c = \{\infty\} \cup \{\tau \in \mathfrak{H} \mid \mathrm{Im}(\tau) > \mathrm{c}\} \quad , c > 0$$

計算により,

$$\begin{aligned} \{\gamma \in \Gamma \mid \gamma(U_1) \cap U_1 \neq \emptyset\} = \Gamma_\infty = \{\gamma \in \Gamma \mid \gamma(\infty) = \infty\} \\ = \left\{ \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| m \in \mathbb{Z} \right\} \end{aligned}$$

となることが分かる. この時,$D = \{\alpha \in \mathbb{C} \mid |\alpha| < e^{-2\pi}\}$ に対して,

$$\begin{array}{ccc} \Gamma\backslash\mathfrak{H}^* & & \mathbb{C} \\ \uparrow{\scriptstyle open} & & \uparrow{\scriptstyle open} \\ \Gamma_\infty\backslash U_1 & \xrightarrow{\cong} & D \end{array} \qquad , \Gamma_\infty \tau \longmapsto e^{2\pi i z}$$

により, 座標が入る.

定理 4.4 と定理 4.2 より次が分かる.

系 4.6. モジュラー函数 $J(\tau)$ はコンパクト Riemann 面 $\Gamma\backslash\mathfrak{H}^*$ 上の有理型函数であり, その次数は 1 である. 特に $J(\tau)$ は全単射

$$J \colon \Gamma\backslash\mathfrak{H} \to \mathbb{C}$$

を導く.

これから主定理が導かれる.

定理 4.7. (一意化定理)
$c_2^3 - 27c_3^2 \neq 0$ を満たす任意の複素数 c_2, c_3 に対して, $\mathbb{C}$ 内の格子 Λ で,

$$g_2(\Lambda) = c_2, g_3(\Lambda) = c_3$$

を満たすものがちょうど一つ存在する.

Proof. 存在性

$$A = 1728\frac{c_2^3}{c_2^3 - 27c_3^2} \in \mathbb{C}$$

とおく. 系 4.6 より,$\tau \in \mathfrak{H}$ で,$J(\tau) = A$ となるものが存在する.
まず,$c_2 \neq 0$ と仮定する.
$\alpha \in \mathbb{C}$ で,$g_2(\tau) = \alpha^4 c_2$ となるものを取る. この時,

$$1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = 1728\frac{c_2^3}{c_2^3 - 27c_3^2}, c_2 \neq 0$$

なので, $g_3(\tau) = \pm\alpha^6 c_3$ が分かる. 必要なら,α を $\sqrt{-1}\alpha$ で取り替えて,

$$g_2(\tau) = \alpha^4 c_2, g_3(\tau) = \alpha^6 c_3$$

として良い. このような $\alpha \in \mathbb{C}$ は $c_2 = 0$ の時も取れる. この時,

$$c_2 = \alpha^{-4} g_2(\tau) = 40\alpha^{-4} \sum_{\omega \in \Lambda_\tau, \omega \neq 0} \omega^{-4} = g_2(\alpha\Lambda_\tau),$$
$$c_3 = \alpha^{-6} g_3(\tau) = 140\alpha^{-6} \sum_{\omega \in \Lambda_\tau, \omega \neq 0} \omega^{-6} = g_3(\alpha\Lambda_\tau).$$

従って, 格子 $\alpha\Lambda_\tau = \mathbb{Z}\alpha\tau + \mathbb{Z}\alpha$ が条件を満たす.
一意性
$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \Lambda' = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$ を格子, $\tau = \omega_1/\omega_2, \tau' = \omega_1'/\omega_2' \in \mathfrak{H}$ とし,

$$g_2(\Lambda) = g_2(\Lambda'), g_3(\Lambda) = g_3(\Lambda')$$

であると仮定する.
この時,$g_k(\tau) = \omega_2^{2k} g_k(\Lambda)$ などに注意すると,

$$J(\tau) = 1728\frac{{\omega_2}^{12} g_2(\Lambda)^3}{{\omega_2}^{12} g_2(\Lambda)^3 - 27\omega_2^{12} g_3(\Lambda)^2}$$
$$= 1728\frac{{\omega'}_2^{12} g_2(\Lambda')^3}{{\omega'}_2^{12} g_2(\Lambda')^3 - 27{\omega'}_2^{12} g_3(\Lambda')^2} = J(\tau')$$

となることが分かる. ゆえに系 4.6 より $\gamma \in \Gamma$ で, $\tau' = \gamma(\tau)$ となるものが取れる. この時,$\alpha \in \mathbb{C}^\times$ で, 次を満たすものが取れる.

$$\gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \alpha \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$$

ゆえに $\Lambda = \alpha\Lambda'$ なので, 次の等式を得る.

$$g_2(\Lambda') = g_2(\Lambda) = \alpha^{-4} g_2(\Lambda'), g_3(\Lambda') = g_3(\Lambda) = \alpha^{-6} g_3(\Lambda')$$

$(g_2(\Lambda'), g_3(\Lambda')) \neq (0,0)$ に注意して,3 つの場合に分ける.

case1 $g_2(\Lambda') \neq 0, g_3(\Lambda') \neq 0$ の場合

$\alpha^{-4} = \alpha^{-6} = 1$ より,$\alpha = \pm 1$ である. 従って,$\alpha\Lambda' = \Lambda'$ である.

case2 $g_2(\Lambda') = 0$ の場合

$J(\tau') = 0$ なので,$\tau' \in \Gamma\omega$ である. 但し,$\omega = \dfrac{-1+\sqrt{-3}}{2} \in \mathfrak{H}$ は 1 の原始 3 乗根である. ゆえに,Λ' は Λ_ω の定数倍なので ω で不変である.

一方,$g_3(\tau') \neq 0$ なので,$\alpha^6 = 1$ である. これを満たすのは,

$$\alpha = \pm 1, \pm\omega, \pm\omega^2$$

のみである. 従って,$\alpha\Lambda' = \Lambda'$ である.

case3 $g_3(\Lambda') = 0$ の場合

case2 において,ω を $i = \sqrt{-1}$ と置き換えれば良い.

以上より, どの場合でも,

$$\Lambda = \alpha\Lambda' = \Lambda'$$

となる. □

系 4.8. E を $\mathbb{C}$ 上の楕円曲線とし,$m \in \mathbb{Z}_{>0}$ とする. この時,m 倍写像

$$[m] \colon E \to E$$

は全射であって, その核は $(\mathbb{Z}/m\mathbb{Z})^2$ と同型である.

参考文献

[1] L.V. アールフォルス, 複素解析.

[2] W.Fulton,*Algebraic Curves.*

[3] 岩沢健吉, 代数函数論.

[4] S.Lang,*Elliptic Functions.*

[5] G.Shimura,*Introduction to Arithmetic Theory of Automorphic Functions.*

[6] J.H.Silverman*The Arithmetic of Elliptic Curves.*