第2章

楕円曲線概論

梅垣 敦紀 (早稲田大学 理工学部)

§0. はじめに

この章では, 楕円曲線の基本的な事実をまとめてみることにする. また,「体 K が完全体である」ことを仮定する.

§1. 楕円曲線

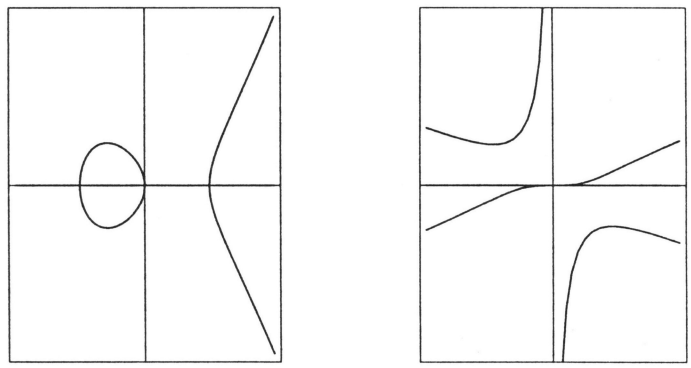
まず, 複素数体 $\mathbf{C}$ 上だけではなく, 一般の体 K 上における楕円曲線を定義する.

定義 1.1. 種数 1 の非特異曲線と基点 $O \in E$ の組 (E, O) を**楕円曲線**という. 体 K に対して, E が K 上定義されかつ $O \in E(K)$ となるとき, 楕円曲線 E は K **上定義される**といい, E/K とかく.

例 1.2. 以下の graph は楕円曲線

$$y^2z = x(x^2 - a^2z^2)$$

を (affine 平面に) 表したものである:



具体的に楕円曲線を扱う上では model を固定することが重要になる. $\mathbf{C}$ 上では Weierstraßの標準型といわれる model があることは既に知っている. 次の命題から, 一般の体 K 上においても標準的な model がとれることがわかる.

命題 1.3. 楕円曲線 E/K に対して,

$$(1) \qquad y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (a_1,\dots,a_6\in K)$$

という形の model が取れる. 逆に, model (1) をもつ曲線が非特異ならば, E は基点 $O=[0:1:0]$ をもつ楕円曲線である.

[証明]. Riemann-Roch の定理から, 任意の $n\in\mathbf{Z}_{>0}$ に対して,

$$l(n(O))=n$$

となることからわかる. 即ち, $x\in K(E)$ を適当にとって, $\{1,x\}$ が $L(2(O))$ の基底とできる. 同様に, $y\in K(E)$ を適当にとれば, $\{1,x,y\}$ が $L(3(O))$ の基底とできる. このとき, $L(6(O))$ には7つの函数 $\{1,x,y,x^2,xy,y^2,x^3\}$ が含まれるが, $l(6(O))=6$ より,

$$A_0^{(y)}y^2+A_1xy+A_3y=A_0^{(x)}x^3+A_2x^2+A_4x+A_6 \quad (A_1,\dots,A_4,A_0^{(y)},A_0^{(x)}\in K)$$

という線形な関係式が生じる. ここで, x^3,y^2 以外はそれぞれ O で異なる位数の極をもつから, $A_0^{(y)}A_0^{(x)}\neq 0$ であることに注意すると, (1) の形の式が得られる.

あとは, これが E の model となる, 即ち, 「$K(E)=K(x,y)$」 となることを確かめれば良い.

$$\phi\colon E\longrightarrow \mathbf{P}^1,\ x\mapsto [x:1]$$

を考えると, x の取り方から, x は O で2位の極を持ち, それ以外では極を持たないから,

$$\deg\phi=e(O)=2$$

より, $[K(E):K(x)]=2$ である. 一方, $[K(x,y):K(x)]=2$ だからよい. □

注意 1.4. 上述の (1) を **Weierstraß方程式**という.

上の命題で見たことから, 以下では Weierstraß方程式を model にもつ楕円曲線を取り扱って, 楕円曲線の性質を調べていくことにする.

model (1) をもつ曲線 E/K に対して,

$$\begin{aligned}
&b_2=a_1^2+4a_2,\ b_4=2a_4+a_1a_3,\ b_6=a_3^2+4a_6,\\
&b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2=\frac{b_2b_6-b_4^2}{8},\\
&c_4=b_2^2-24b_4,\\
&c_6=-b_2^3+36b_2b_4-216b_6,\\
&\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6=\frac{c_4^3-c_6^2}{1728},\\
&j=c_4^3/\Delta
\end{aligned}$$

とおく. Δ を E の**判別式**といい, $j=j(E)$ を E の j-**不変量**という. この Δ と j は重要な情報を保存しているが, それを見る前に, b_i,c_i 達の意味を確認したい.

注意 1.5. $\mathrm{char}(K) \neq 2$ とする. E/K の model (1) に対して,

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{2}$$

の形に変換できる. $\mathrm{char}(K) \neq 2,3$ とする. E/K の model (1) に対して,

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{3}$$

の形に変換できる.

特に, (3) は $\mathbf{C}$ 上の楕円曲線のときに現れた**Weierstraßの標準型**であることを確認しておく.

楕円曲線の Weierstraß方程式の取り方は unique では無いが, model の取り替えは線形変数変換でできることが保証される.

命題 1.6. 楕円曲線 E/K の model (1) を固定する. E の任意のもう1つの model

$$Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6' \quad (a_1', \ldots, a_6' \in K) \tag{4}$$

に対して, $u \in K^\times$, $r,s,t \in K$ を用いて

$$\begin{cases} x = u^2X + r \\ y = u^3Y + su^2X + t \end{cases} \tag{5}$$

の形の線形変数変換で変換できる.

[証明]. $\{1,x\},\{1,X\}$ はともに $L(2(O))$ の基底であって, $\{1,x,y\},\{1,X,Y\}$ はともに $L(3(O))$ の基底である. ゆえに, ある $u_1,u_2 \in K^\times$, $r,s_2,t \in K$ を用いて,

$$\begin{cases} x = u_1X + r \\ y = u_2Y + s_2X + t \end{cases}$$

とかける. ここで, X,Y は (4) を満たすから, $u_1^3 = u_2^2$ より,

$$u = \frac{u_2}{u_1},\ s = \frac{s_2}{u^2}$$

と置けばよい. □

変換 (5) は明らかに曲線の間の morphism であって, 同じ model をもつことは (K 上の) 同型という言葉と矛盾していない. また, 変換 (5) はしばしば行われるから, 係数や不変量をまとめて計算しておく.

注意 1.7. 曲線 E/K の model (1) を固定する. このとき, (5) の変換で得られる新しい model (4) との間に, 以下の関係がある:

$$\begin{aligned}
ua_1' &= a_1 + 2s, \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\
u^3a_3' &= a_3 + ra_1 + 2t, \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,
\end{aligned}$$

$$
\begin{aligned}
u^2 b_2' &= b_2 + 12r, \\
u^4 b_4' &= b_4 + r b_2 + 6r^2, \\
u^6 b_6' &= b_6 + 2r b_4 + r^2 b_2 + 4r^3, \\
u^8 b_8' &= b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4, \\
u^4 c_4' &= c_4, \\
u^6 c_6' &= c_6, \\
u^{12}\Delta' &= \Delta, \\
j' &= j.
\end{aligned}
$$

次に, 判別式 Δ の性質を見る.

命題 1.8. model (1) をもつ曲線 E/K に対して,

$$E \text{ が非特異} \iff \Delta \neq 0$$

が成り立つ.

[証明]. E が特異点を持つとする. その特異点を原点 $(0,0)$ に移すと (Δ が 0 であるかどうかはこの変換で変わらないことに注意する), $a_3 = a_4 = a_6 = 0$ だから,

$$y^2 + a_1 xy = x^3 + a_2 x^2$$

について考えれば良いが, このとき, $b_4 = b_6 = 0$ より, $\Delta = 0$ がわかる.

次に, 逆を示すために, 「$\Delta = 0$」を仮定する. 簡単のため「$\mathrm{char}(K) \neq 2$」とする.

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

を考えれば良いが,

$$(\text{右辺 } 4x^3 + b_2 x^2 + 2b_4 x + b_6 \text{ の判別式}) = 16\Delta = 0$$

より, $f(x)$ は重根 α をもつ. このとき, $(\alpha, 0)$ は特異点である. □

上の命題から, 楕円曲線という言葉を用いるときは非特異, 即ち, $\Delta \neq 0$ が仮定されているから, $\Delta = 0$ の曲線を考えることは無意味と感じるかも知れない. しかしながら, 例えば K が代数体の場合では reduction を考えたとき非常に重要になる.

命題 1.9. model (1) をもつ曲線 E/K に対して, $\Delta = 0$ ならば, 次数 1 の有理射 $E \longrightarrow \mathbf{P}^1$ が存在する.

[証明]. 特異点は K 上定義されることに注意する. 特異点を $(0,0)$ に移せば, $a_1, a_2 \in K$, $a_3 = a_4 = a_6 = 0$ を仮定して良い, 即ち,

$$y^2 + a_1 xy = x^3 + a_2 x^2$$

として良い.

$$\phi\colon E \longrightarrow \mathbf{P}^1,\ (x,y) \mapsto [x:y]$$

を考えると, $t = \dfrac{y}{x}$ に対して,

$$t^2 + a_1 t = x + a_2$$

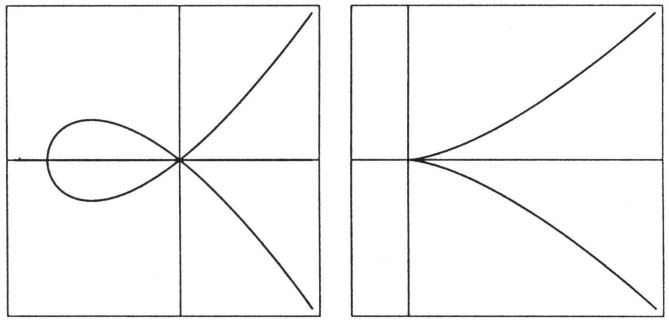
が成り立つから, $x \in K(t)$, よって, $y \in K(t)$ だから, $\deg \phi = 1$ が成り立つ. □

$\Delta = 0$ のとき, 以下のように, 特異点の状況が Weierstraß方程式の係数から簡単に判別できることに注意する.

注意 1.10. model (1) をもつ曲線 E/K に対して, 「$\Delta = 0$」を仮定する. このとき,

$$\text{特異点が node である} \iff c_4 \neq 0,$$
$$\text{特異点が cusp である} \iff c_4 = 0$$

がいえる.



node　　cusp

図 1. node & cusp

C 上において, j-不変量が楕円曲線の同型類を定めていることは知っている. 一般の体 K 上においても同様に, j-不変量は代数閉体 $\overline{K}$ 上の同型類を定めることが分かる.

命題 1.11. 楕円曲線 $E, E'/K$ に対して,

$$E \text{ と } E' \text{ が } \overline{K} \text{ 上同型} \iff j(E) = j(E')$$

が成り立つ.

[証明]. E と E' が $\overline{K}$ 上同型であるとき, 注意 1.7 より, $j(E) = j(E')$ となることは明らか.

逆に, 「$j(E) = j(E')$」とする. 「$\mathrm{char}(K) \neq 2, 3$」のとき, E, E' の Weierstraß方程式として,

$$E\colon y^2 = x^3 + Ax + B$$
$$E'\colon y^2 = x^3 + A'x + B'$$

をとって, $u \in \overline{K}^{\times}$ を

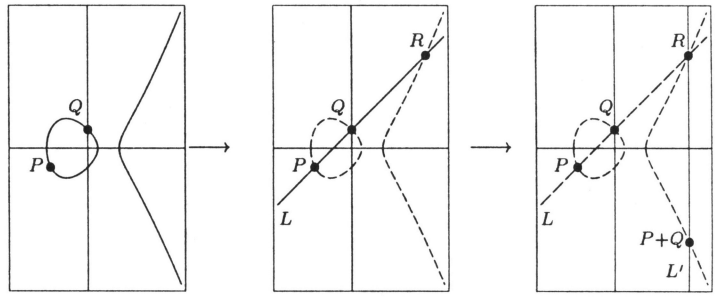
$$u = \begin{cases} (B/B')^{1/6} & j = 0 (\Longleftrightarrow A = 0) \text{ のとき}, \\ (A/A')^{1/6} & j = 1728 (\Longleftrightarrow B = 0) \text{ のとき}, \\ (A/A')^{1/6} = (B/B')^{1/6} & \text{それ以外のとき}, \end{cases}$$

とするとき, $(x, y) \mapsto (u^2 x, u^3 y)$ という変換を考えれば良い. □

§2. 群構造

C 上で楕円曲線が群構造をもつことは知っている. 任意の体 K 上の楕円曲線も同様に群構造をもつ.

命題 2.1. E/K を model (1) で定義される楕円曲線として, $P, Q \in E(\overline{K})$ とする. L を P と Q を結ぶ直線 ($P = Q$ ならば P における接線) として, R を E と L との交点とする. さらに R と O を結ぶ直線 L' の交点を $P + Q$ とする.



このとき, この加法に関して, E 上の点は Abel 群をなす.

注意 2.2. 上の加法を Weierstraß 方程式 (1) の係数を用いて表すと:
$P_0 = (x_0, y_0)$ に対して, 逆元は

$$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3),$$

であって, $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ に対して, 和は $x_1 = x_2$ かつ $2y_2 + a_1 x_1 + a_3 = 0$ のときは $P_1 + P_2 = O$ であって, そうでないときは

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \text{ のとき}, \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & x_1 = x_2 \text{ のとき}, \end{cases}$$

$$\nu = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & x_1 \neq x_2 \text{ のとき}, \\ \dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3} & x_1 = x_2 \text{ のとき}, \end{cases}$$

とするとき,

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

で定まる.

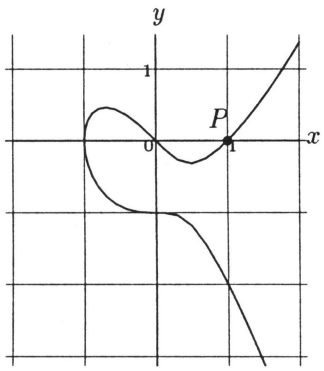
和の座標は係数と元の点の座標のみから決まるから, 次がわかる.

注意 2.3. 注意 2.2 から, 任意の拡大 L/K に対して, $E(L)$ は $E(\overline{K})$ の部分群になることに注意する.

例 2.4. 楕円曲線

$$y^2 + xy + y = x^3 - x$$

を考える. $P = (1,0)$ とするとき, $2P, 3P, \ldots$ と順に求めていくと, $6P = O$ となることが確認できる.



§3. Isogeny

前節で楕円曲線は群の構造を持つことをみた. 群において, 準同型写像は重要な役割を果たした. そこで, 楕円曲線に付随する群の間の準同型写像となるものが興味の対象となるが, 特に, 曲線の morphism でもあるようなものを考える.

§3.1. isogeny

まず, isogeny の定義をしておく.

定義 3.1. $E_1, E_2/K$ を楕円曲線とする. このとき, morphism

$$\phi : E_1 \longrightarrow E_2$$

が $\phi(O_{E_1}) = O_{E_2}$ を満たすとき, ϕ を E_1 と E_2 の間の **isogeny** といい, E_1 と E_2 の間の isogeny のなす群を $\mathrm{Hom}(E_1, E_2)$ で表す.

また, $\phi(E_1) \neq \{O_{E_2}\}$ を満たす isogeny ϕ が存在するとき, E_1 と E_2 は **isogenous** であるといい, $E_1 \sim E_2$ で表す.

群 $\mathrm{Hom}(E_1, E_2)$ において, 加法が

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

で与えられ, 明らかに可換であることを確認しておく.

定義 3.2. isogeny ϕ が, morphism として体 K 上定義されるとき, ϕ は K **上定義される**といい, それらがなす $\mathrm{Hom}(E_1, E_2)$ の部分群を $\mathrm{Hom}_K(E_1, E_2)$ で表す.

同様に, E_1 と E_2 が isogenous であるとき, その間の isogeny が K 上定義されるとき, K **上 isogenous** であるといい, $E_1 \underset{K}{\sim} E_2$ と表す.

代数曲線の一般論から次の事実は保証されている:

注意 3.3. $\phi(E_1) \neq \{O_{E_2}\}$ であるとき, smooth な曲線の間の morphism であるから, ϕ は全射であることに注意する.

上の定義と注意から, isogeny は準同型であることが分かる:

定理 3.4. $\phi \in \mathrm{Hom}(E_1, E_2)$ に対して, $P, Q \in E_1$ とするとき,

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

を満たす. 即ち, isogeny ϕ は群準同型である.

[証明]. ϕ が定数写像, 即ち, 任意の $P \in E_1$ に対して $\phi(P) = O$ となるときは明らか.

ϕ が定数写像でないときも, 明らかに,

$$\phi_*\colon \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2),\ \left[\sum n_i(P_i)\right] \mapsto \left[\sum n_i(\phi(P_i))\right]$$

は hom であって, 同型

$$f_i\colon E_i \xrightarrow{\sim} \mathrm{Pic}^0(E_i),\ P \mapsto [(P) - (O)] \quad (i = 1, 2)$$

を考えると, 図式

$$\begin{array}{ccc} E_1 & \xrightarrow[\sim]{f_1} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \xrightarrow[f_2]{\sim} & \mathrm{Pic}^0(E_2) \end{array} \tag{6}$$

が可換になるから, ϕ は準同型である. □

準同型に対して, その kernel で割った商群を考えることができる. その商群に対応する楕円曲線が存在するかどうかは非常に興味深い.

命題 3.5. E を楕円曲線として, T を E の有限部分群とする. このとき,

$$\ker\phi = T$$

を満たす楕円曲線 E' と isogeny $\phi \in \mathrm{Hom}(E, E')$ が唯 1 つ存在する.

注意 3.6. 命題 3.5 の E' を E/T で表す.

例えば, 例 2.4 の E と P に対して,

$$E/\langle 3P\rangle : Y^2+XY+Y=X^3-11X+12$$

であって,

$$\phi : \begin{cases} X=\dfrac{x^2+x+2}{x+1}, \\ Y=\dfrac{(x^2+2x-1)y-2(x+1)}{(x+1)^2} \end{cases}$$

となる. 同様に,

$$E/\langle 2P\rangle : Y^2+XY+Y=X^3+4X-6$$

に対しては,

$$\phi : \begin{cases} X=\dfrac{x^3-x+1}{x^2}, \\ Y=\dfrac{(x^3+x-2)y+x^2-x-1}{x^3} \end{cases}$$

であって,

$$E/\langle P\rangle : Y^2+XY+Y=X^3-36X-70$$

に対しては,

$$\phi : \begin{cases} X=\dfrac{x^6-x^5+6x^4+3x^3-2x+1}{(x-1)^2x^2(x+1)}, \\ Y=\dfrac{(x^4-4x^3-1)(x^2+x+2)(x^2+2x-1)}{(x-1)^3x^3(x+1)^2}y \\ \qquad -\dfrac{(x+1)(7x^6+3x^5+7x^4-4x^3+3x^2+x-1)}{(x-1)^3x^3(x+1)^2} \end{cases}$$

となる.

§3.2. 自己準同型

一般の群に対して, 自己準同型を考えることができた. 楕円曲線の場合にも同様のことを考える. 特に, 合成によって積を定めることで, それらは環をなすが, その構造が個々の楕円曲線のもつ重要な性質の一つとなる.

定義 3.7. E を楕円曲線とする. このとき, $\mathrm{End}(E)=\mathrm{Hom}(E,E)$ を E の**自己準同型環**という.

$\mathrm{End}(E)$ の元で isogeny として K 上定義されるもののなす部分環を $\mathrm{End}_K(E)$ で表す.

注意 3.8. $\mathrm{End}(E)$ の元の例として, $m\in\mathbf{Z}$ とするとき,

$$[m] : E \longrightarrow E, \quad P \mapsto \underbrace{P+\cdots+P}_{m \text{ times}}$$

で与えられる m-倍 isogeny $[m]$ がある.

楕円曲線の自己準同型環の構造について以下のことが分かる.

命題 3.9. E を楕円曲線とする. このとき, $\mathrm{End}(E)$ は torsion-free $\mathbf{Z}$-加群の構造を持ち, かつ標数 0 の整域である.

注意 3.10. $\mathrm{End}(E)$ は $\mathbf{Z}$ に同型な部分環を含む.

より詳しく, 楕円曲線の自己準同型環は 3 つのタイプに類別される.

定理 3.11. 楕円曲線 E/K に対して, $\mathrm{End}(E)$ は $\mathbf{Z}$, 虚 2 次体の整環, $\mathbf{Q}$ 上の 4 元数環の整環のいずれかに同型である.

注意 3.12. $\mathrm{char}(K) = 0$ とする. このとき, $\mathrm{End}(E)$ は 4 元数環の整環にはなり得ない. 特に, $\mathrm{End}(E)$ が虚 2 次体の整環と同型であるとき, E は**虚数乗法**をもつという.

§3.3. dual isogeny

今までは, 楕円曲線が群構造をもつことから自然に派生する話題だったが, dual isogeny は楕円曲線のもつ著しい特徴である.

定理 3.13. $\phi \in \mathrm{Hom}(E_1, E_2)$ を次数 m の isogeny とする. このとき,

$$\widehat{\phi} \circ \phi = [m] \tag{7}$$

となる isogeny $\widehat{\phi} \in \mathrm{Hom}(E_2, E_1)$ が唯 1 つ存在する.

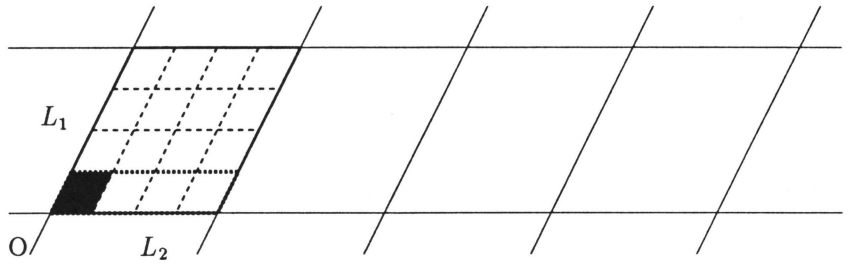
定義 3.14. $\phi \in \mathrm{Hom}(E_1, E_2)$ とする. 定理 3.13 で定まる isogeny $\widehat{\phi}$ を ϕ の **dual isogeny** という.

$\mathbf{C}$ 上の楕円曲線については, dual isogeny を以下の様に視覚的に捉えることができる.

注意 3.15. $\mathbf{C}$ 上では以下の様にして、dual isogeny が得られる:
L_1, L_2 を E_1, E_2 に対応する格子とする. このとき, $\phi \in \mathrm{Hom}(E_1, E_2)$ に対応して, 包含関係 $L_1 < L_2$ がある. 一方, $mL_2 < L_1$ だから, これに対応する map を ψ とすれば, 図式

$$\begin{array}{ccc} \mathbf{C}/L_1 & \xrightarrow{[m]} & \mathbf{C}/L_1 \\ {\scriptstyle\phi}\downarrow & & \uparrow{\scriptstyle\psi} \\ \mathbf{C}/L_2 & \xrightarrow[m]{\sim} & \mathbf{C}/mL_2, \quad z \pmod{L_2} \mapsto mz \pmod{mL_2} \end{array}$$

は可換である. したがって, $\widehat{\phi} = \psi \circ m$ としてとればよい.



注意 3.16. dual isogeny の存在から, 定義 3.1 で定義した isogenous $E_1 \sim E_2$ は同値関係であることがわかる.

命題 3.17. $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, $m = \deg \phi$ とする. このとき,

(1) $\widehat{\phi} \circ \phi = [m]_{E_1}$, $\phi \circ \widehat{\phi} = [m]_{E_2}$;
(2) $\widehat{(\phi \circ \psi)} = \widehat{\psi} \circ \widehat{\phi}$, $\widehat{(\phi + \psi)} = \widehat{\phi} + \widehat{\psi}$,
(3) $\deg \widehat{\phi} = \deg \phi$,
(4) $\widehat{\widehat{\phi}} = \phi$.
(5) $\widehat{[m]} = [m]$, $\deg \widehat{[m]} = \deg[m] = m^2$,

[証明]. (1):

$$(\phi \circ \widehat{\phi}) \circ \phi = \phi \circ [m]_{E_1} = [m]_{E_2} \circ \phi$$

からわかる.
(2): 前半は明らか. 後半は認めることにする.
(5): (2) より, 前半は

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$$

が induction でいえるから OK. 後半は, 今示したことから,

$$[m] \circ \widehat{[m]} = [m^2]$$

より, isogeny の定義に戻れば, $\deg [m] = m^2$ がわかる.
(3): (5) より, $\deg(\widehat{\phi} \circ \phi) = \deg[m] = m^2$ より, $\deg(\widehat{\phi}) = m$ となる.
(4):

$$\widehat{\phi} \circ \phi = [m] = \widehat{[m]} = \widehat{\widehat{\phi} \circ \phi} = \widehat{\phi} \circ \widehat{\widehat{\phi}}$$

より, OK. □

§3.4. 自己同型

自己同型という言葉は2通りの意味で使われる. まず, 楕円曲線の群構造を含めた意味での自己同型を考える.

定義 3.18. $\mathrm{End}(E)$ の単元のなす群を $\mathrm{Aut}(E)$ で表し, E の**自己同型群**という. さらに, $\mathrm{End}_K(E)$ の単元のなす群を $\mathrm{Aut}_K(E)$ で表す.

この自己同型群は j-不変量と定義体 K の標数によって完全に記述できる.

定理 3.19. E/K を楕円曲線とする. このとき,

$$\#\mathrm{Aut}(E) = \begin{cases} 2 & j(E) \neq 0, 1728 \text{ のとき}, \\ 4 & j(E) = 1728,\ \mathrm{char}(K) \neq 2,3 \text{ のとき}, \\ 6 & j(E) = 0,\ \mathrm{char}(K) \neq 2,3 \text{ のとき}, \\ 12 & j(E) = 0 = 1728,\ \mathrm{char}(K) = 3 \text{ のとき}, \\ 24 & j(E) = 0 = 1728,\ \mathrm{char}(K) = 2 \text{ のとき}, \end{cases}$$

が成り立つ.

特に, 定義体の標数が $2,3$ では無いときは, 自己同型の元を簡潔かつ具体的にかくことができる.

注意 3.20. $\mathrm{char}(K) \neq 2,3$ のとき, E の model として,

$$y^2 = x^3 + Ax + B$$

をとると,

$$\begin{aligned} \mathrm{Aut}(E) &= \begin{cases} \langle [-1] \colon (x,y) \mapsto (x,-y) \rangle & j \neq 0, 1728 \text{ のとき}, \\ \langle [i] \colon (x,y) \mapsto (-x, iy) \rangle & j = 1728\ (B = 0) \text{ のとき}, \\ \langle [-1] \rangle \times \langle [\omega] \colon (x,y) \mapsto (\omega x, y) \rangle & j = 0\ (A = 0) \text{ のとき}, \end{cases} \\ &\cong \mu_n \quad (n := \#\mathrm{Aut}(E)) \end{aligned}$$

である. さらに, この同型は G_K-加群としての同型である.

次に, 群構造を無視して, 曲線としての自己同型群をみる. この群の構造は今見た群としての自己同型群 $\mathrm{Aut}(E)$ を用いて記述できる.

定義 3.21. 楕円曲線 E/K に対して, (曲線としての) $\overline{K}$ 上の同型 $E \longrightarrow E$ のなす群を $\mathrm{Isom}(E)$ で表す.

注意 3.22. $\mathrm{Aut}(E) < \mathrm{Isom}(E)$ であって, $\mathrm{Aut}(E) \neq \mathrm{Isom}(E)$ であることに注意する. 例えば, 任意の $P \in E(\overline{K})$ に対して,

$$\tau_P \colon E \longrightarrow E,\ Q \mapsto Q + P$$

を考えると, $\tau_P \in \mathrm{Isom}(E)$ であるが, $\tau_P \notin \mathrm{Aut}(E)$ である.

命題 3.23.

$$E(\overline{K}) \times \mathrm{Aut}(E) \longrightarrow \mathrm{Isom}(E), \quad (P, \alpha) \mapsto \tau_P \circ \alpha$$

は(集合として)全単射である.

さらに, 演算を

$$(P, \alpha) \cdot (Q, \beta) = (P + \alpha(Q), \alpha \circ \beta)$$

で定義することによって, 群の同型

$$E(\overline{K}) \rtimes \mathrm{Aut}(E) \xrightarrow{\sim} \mathrm{Isom}(E),$$

が得られる.

[証明]. $\phi \in \mathrm{Isom}(E)$ に対して, $\tau_{-\phi(O)} \circ \phi$ を考えると, これは $\mathrm{Aut}(E)$ の元であって,

$$\phi = \tau_{-\phi(O)} \circ (\tau_{-\phi(O)} \circ \phi)$$

と書けるから, 上の写像は全射である.

$\tau_P \circ \alpha = \tau_Q \circ \beta$ とする. このとき, O を代入すると, $P = Q$ だから, $\alpha = \beta$ となり, 単射がわかる.

さらに,

$$(\tau_P \circ \alpha) \circ (\tau_Q \circ \beta) = (\tau_P \circ \tau_{\alpha Q}) \circ (\alpha \circ \beta)$$

より, 群の同型がいえた. □

§4. Tate 加群

楕円曲線において, 決まった位数をもつ点は部分群をなす. 明らかにこの部分群は体 K の絶対 Galois 群の作用で閉じている. この性質から非常に興味深い対象となる. 詳しい話は, 後に譲ることにして, ここではこの部分群の構造を把握することにする.

命題 4.1. E/K を楕円曲線として, $m \in \mathbf{Z}_{>0}$, $p = \mathrm{char}(K)$ とする. $p = 0$ または $(m, p) = 1$ ならば,

$$E[m] \cong (\mathbf{Z}/m\mathbf{Z})^{\oplus 2} \tag{8}$$

が成り立つ.

また, $p > 0$ のとき,

$$E[p^e] \cong \{0\} \text{ または } (\mathbf{Z}/p^e\mathbf{Z}) \tag{9}$$

が成り立つ.

[証明]. ϕ を p-Frobenius 写像とすると,

$$\#E[p^e] = \deg_s[p^e] = \deg_s(\hat{\phi})^e$$

となるから,

$$E[p^e] \cong \begin{cases} \{0\} & \hat{\phi} \text{ が非分離的であるとき,} \\ \mathbf{Z}/p^e\mathbf{Z} & \hat{\phi} \text{ が分離的であるとき,} \end{cases}$$

となる. □

素数 l に対して, l 冪位数をもつ点のなす群 $E[l^n]$ の間に, $[l]$-倍 isogeny で定まる準同型

$$E[l^{n+1}] \longrightarrow E[l^n]$$

がある. この系列は射影系をなすから, この系列を 1 組にして考える.

定義 4.2. E/K を楕円曲線として, l を素数とする. このとき, $[l]$-倍写像による射影極限

$$T_l(E) = \varprojlim_n E[l^n]$$

を E の (l-進) **Tate 加群**という.

この Tate 加群の構造は上の命題からすぐにわかる.

命題 4.3. E/K を楕円曲線として, l を素数とする. $\mathbf{Z}_l$-加群として,

$$T_l(E) \cong \begin{cases} \mathbf{Z}_l^{\oplus 2} & l \neq \mathrm{char}(K) \text{ のとき,} \\ \{0\} \text{ または } \mathbf{Z}_l & l = \mathrm{char}(K) > 0 \text{ のとき.} \end{cases} \tag{10}$$

§5. Twist

今までに見たように, 代数閉体上においては, 楕円曲線の同型類を j のみで簡単に表すことができた. しかし, 定義体 K が閉体ではない場合, K 上の同型類を考えてみると j だけでは記述できない. そこで, twist と呼ばれる概念を導入する.

定義 5.1. 楕円曲線 E/K を固定する. 楕円曲線 E'/K が $j(E') = j(E)$ を満たすとき, E' を E の **twist** という. また, 集合 $\mathrm{Twist}^0(E/K)$ を

$$\mathrm{Twist}^0(E/K) := \{E' : E \text{ の twist}\}/K \text{ 上の同型}$$

で定義する.

twist という言葉のもつイメージは次の命題から理解できるであろう.

命題 5.2. 「$\mathrm{char}(K) \neq 2, 3$」 を仮定して,

$$n = \begin{cases} 2 & j(E) \neq 0, 1728 \text{ のとき,} \\ 4 & j(E) = 1728 \text{ のとき,} \\ 6 & j(E) = 0 \text{ のとき,} \end{cases}$$

とする. このとき, $\mathrm{Twist}^0(E/K)$ は $K^\times/K^{\times n}$ と同一視できる. さらに, E/K の model として,

$$E\colon y^2 = x^3 + Ax + B \quad (A, B \in K) \tag{11}$$

をとると, この同一視は $D \in K^\times/K^{\times n}$ に対して,

$$E_D\colon \begin{cases} y^2 = x^3 + D^2Ax + D^3B & j(E) \neq 0, 1728 \text{ のとき}, \\ y^2 = x^3 + DAx & j(E) = 1728 \text{ のとき}, \\ y^2 = x^3 + DB & j(E) = 0 \text{ のとき}, \end{cases}$$

に対応させることによって得られる.

[証明]. $[E'] \in \mathrm{Twist}^0(E/K)$ に対して, 楕円曲線 E' と $\overline{K}$ 上の同型 $\phi : E' \longrightarrow E$ の組の類と自然に見做せるから,

$$\mathrm{Twist}^0(E/K) \longrightarrow H^1(G_K, \mathrm{Aut}(E)),\ [E'] \mapsto [\xi_\sigma = (\sigma \mapsto \phi^\sigma \circ \phi^{-1})]$$

が定まり, これは全単射である. 注意 3.20 で見たように, $\mathrm{Aut}(E) \cong \mu_n$ は G_K-加群の同型だから, Hilbert Satz 90 を用いて,

$$\mathrm{Twist}^0(E/K) = H^1(G_K, \mathrm{Aut}(E)) \cong H^1(G_K, \mu_n) \cong K^\times/K^{\times n}$$

となることがわかる.

次に, この同型の対応を調べる. 「$j \neq 0, 1728$」とする. ここで, $K(\sqrt{D})/K$ に対応する 2 次指標

$$\chi\colon G_K \longrightarrow \langle \pm 1 \rangle \cong \mu_2,\ \sigma \mapsto \frac{\sigma(\sqrt{D})}{\sqrt{D}}$$

を考えて,

$$[\xi_\sigma\colon \sigma \mapsto [\chi(\sigma)]] \in H^1(G_K, \mathrm{Aut}(E))$$

をとる. (11) に対して, $\sigma(x) = x, \sigma(y) = \chi(\sigma)\, y$ だから,

$$X = x,\ Y = \frac{1}{\sqrt{D}}\, y$$

を考えると, X, Y は G_K-不変だから, $X, Y \in K(E)$ であって,

$$DY^2 = X^3 + AX + B$$

を満たす. □