虚数乗法を持つ楕円曲線における複素数倍写像の明示公式

柳内武志

早稲田大学大学院　基幹理工学研究科
数学応用数理専攻 橋本研究室　修士２年

講演の流れ

§1. **準備**

§2. **結果**

§3. **考察**

§1. 準備

楕円曲線

- k：(完全) 体　　$\overline{k}$：k の代数閉体
- E/k：k 上の楕円曲線　　O_E： E の基点
- $E(k)$：楕円曲線の k 有理点全体

Weierstrass 方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$a_1, a_2, a_3, a_4, a_6 \in k$$

$$\Downarrow \mathrm{char}(k) \neq 2 \text{ nor } 3$$

$$y^2 = x^3 + Ax + B \qquad A, B \in k$$

j 不変量・不変微分形式

- $j = j(E)$ ：E の j 不変量
- $\omega = \omega(E)$ ：E の不変微分形式

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

$$\omega = \frac{dx}{y}$$

$E_1/k, E_2/k$：楕円曲線

$$E_1 \cong_{\overline{k}} E_2 \iff j(E_1) = j(E_2)$$

$E/\mathbb{C}$の同型類

$$\begin{array}{ccccc}
\{\ \mathbb{C}\ \text{内の格子}\ \}/\sim & \longleftrightarrow & \mathbb{H}/\Gamma(1) & \longleftrightarrow & \mathbb{C} \\
\cup & & \cup & & \cup \\
\{\Lambda\} = \{\Lambda_\tau\} & \leftrightarrow & \tau & \leftrightarrow & j(\tau) \\
\updownarrow & & & & \updownarrow \\
\{\ E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\ \} & = & \{\ E : y^2 = x^3 - \frac{3j(\tau)}{j(\tau)-12^3}x + \frac{2j(\tau)}{j(\tau)-12^3}\ \} & & \\
\cap & & & & \\
\{\ \mathbb{C}\ \text{上の楕円曲線}\ \}/\simeq_{\mathbb{C}} & & & &
\end{array}$$

- $\Lambda_1 \sim \Lambda_2 \quad \Leftrightarrow \quad \exists c \in \mathbb{C} \quad \text{s.t.} \quad c\Lambda_1 = \Lambda_2$
- $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z} \qquad\qquad \Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\pm 1$
- $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots, \quad q = \mathrm{e}^{2\pi \mathrm{i} \tau}$

Mordell -Weil 群

- $+_E : E \times E \longrightarrow E\,;\ (P, Q) \mapsto P +_E Q$

$E(k)$: **アーベル群** (Mordell -Weil **群**)

定理 （Mordell -Weil）

k : **代数体（素体上有限生成な体）** ， E/k : **楕円曲線**

$$E(k) \simeq \mathbb{Z}^r \times G_{tors} \quad (\exists r \in \mathbb{Z}_{\geq 0}\ ,\ \exists G_{tors} : \textbf{有限群})$$

自己準同型写像

- E_1/k , E_2/k : 楕円曲線
- $\phi : E_1 \longrightarrow E_2$; 射

$$\phi : \text{同種写像} \overset{\text{def}}{\Longleftrightarrow} \phi(O_{E_1}) = O_{E_2}$$

$$\phi(P +_{E_1} Q) = \phi(P) +_{E_2} \phi(Q) \quad \forall P, \forall Q \in E_1$$

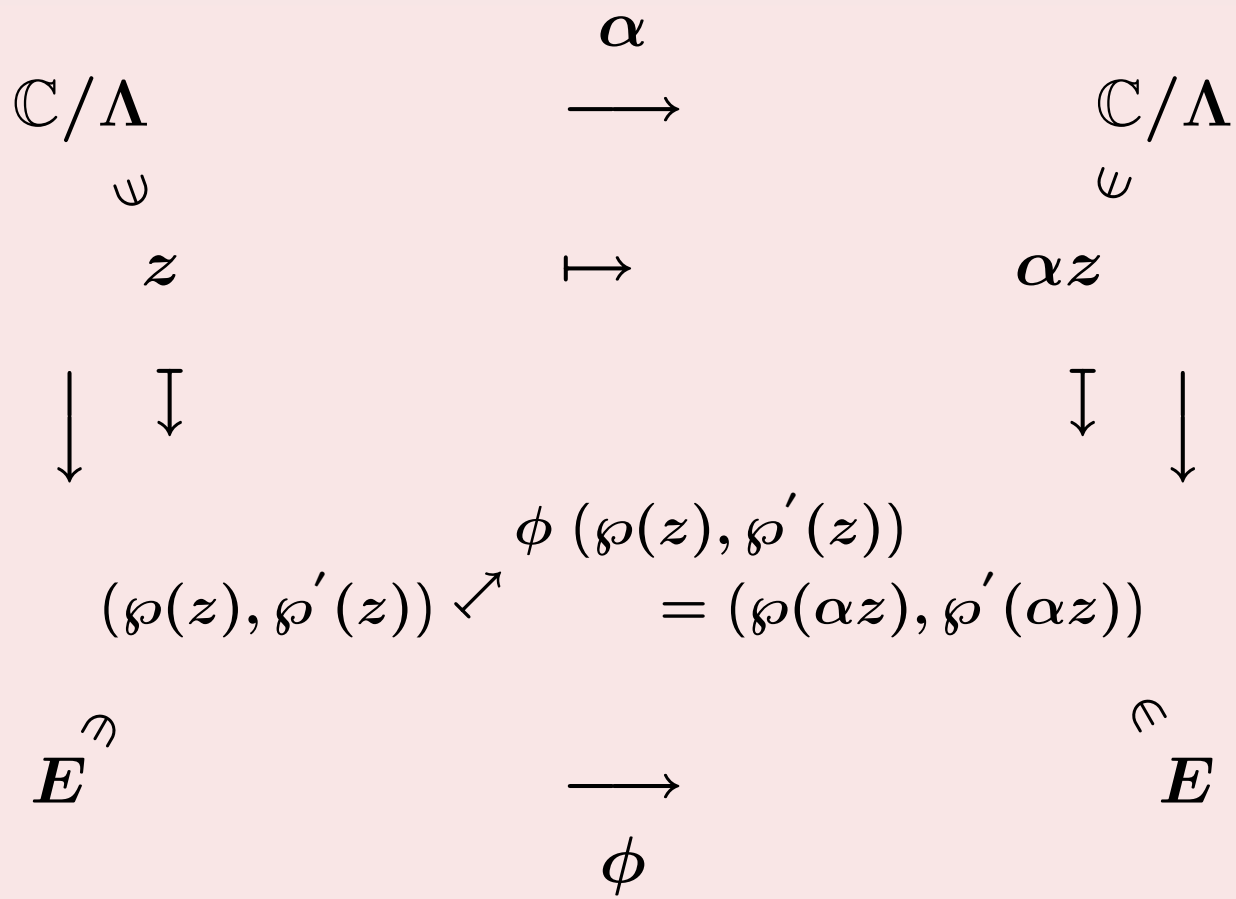
- $\mathrm{Hom}(E_1, E_2) = \{\ \phi : E_1 \to E_2;$ 同種写像 $\}$

$$\mathrm{Hom}(E_1, E_2) : \text{自由}\ \mathbb{Z}\ \text{加群}, \quad \mathrm{rank}(\mathrm{Hom}(E_1, E_2)) \leq 4$$

- $\mathrm{End}(E) = \{\ \phi : E \to E;$ 同種写像 $\}$: E の自己準同型環

$$\mathrm{char}(k) = 0 \ \Rightarrow \mathrm{rank}(\mathrm{End}(E)) \leq 2$$
$$\text{i.e. } k = \mathbb{C} \ \Rightarrow \mathrm{rank}(\mathrm{End}(E)) = 1 \text{ or } 2$$

$\mathbb{C}$ 上の楕円曲線



虚数乗法をもつ楕円曲線

$$\mathrm{End}(E) \xrightarrow{\sim} \mathcal{O} \hookrightarrow K \hookrightarrow \mathbb{C}$$

$$[\overline{\alpha}] = \overline{[\alpha]} \qquad \alpha \in \mathbb{C}$$

$$[\alpha^{\sigma}] = [\alpha]^{\sigma} \qquad \langle \sigma \rangle = \mathrm{Gal}(K/Q)$$

$$\begin{array}{ccccc}
\mathrm{End}(E) & & \longleftrightarrow & & \mathcal{O} \\
\ni & [\alpha] & \leftrightarrow & \alpha & \in \\
\downarrow & \downarrow & \searrow & \downarrow & \downarrow \\
 & \overline{[\alpha]} = [\overline{\alpha}] & \leftrightarrow & \overline{\alpha} & \in \\
\ni & & & & \\
\mathrm{End}(E) & & \longleftrightarrow & & \mathcal{O}
\end{array}$$

虚数乗法をもつ楕円曲線

$$[\alpha]^*\omega = \alpha\omega \quad (\forall \alpha \in \mathcal{O},\ \forall \omega \in \Omega_E)$$

$$j \in \mathcal{O}_{\overline{\mathbb{Q}}}$$

$K(j) : K$ の Hilbert 類体

$$[\mathbb{Q}(j) : \mathbb{Q}] = [K(j) : K] = \sharp Cl_K$$

$$\begin{array}{ccc} \{\ \mathcal{O}_K \text{ に虚数乗法をもつ楕円曲線}\ \}/\simeq_{\mathbb{C}} & \longleftrightarrow & Cl_K \\ \cup & & \cup \\ \{\ E_{\mathfrak{a}}\ \} & \leftrightarrow & \{\ \mathfrak{a}\ \} \end{array}$$

整数倍写像の明示公式

$$
\begin{aligned}
\psi_1 &= 1, \quad \psi_2 = 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)
\end{aligned}
$$

$$
\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && m \geq 2 \\
2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) && m \geq 2
\end{aligned}
$$

$$
\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m-1}\psi_{m+1} && m \geq 1 \\
4y\omega_m &= \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 && m \geq 1
\end{aligned}
$$

$$
[n](x,y) = \left(\frac{\phi_n(x,y)}{\psi_n^2(x,y)} \ , \ \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right) \qquad n \in \mathbb{Z}_{\geq 1}
$$

$$
[-1](x,y) = (x,-y)
$$

§2. 結果

類数１の虚二次体

類数１の虚二次体

$$K_d = \mathbb{Q}(\sqrt{-d})\ , \quad d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

- $$\alpha_d = \begin{cases} \sqrt{-d} & \dots \ d = 1, 2 \\ \frac{1+\sqrt{-d}}{2} & \dots \ otherwise \end{cases}$$
- $\{\ 1\ ,\ \alpha_d\}$: $\mathcal{O}_{K_d}$の基底

j 不変量

d	$j(\alpha_d)$	Factors of $j(\alpha_d)$
1	1728	$2^6 \cdot 3^3$
2	8000	$2^6 \cdot 5^3$
3	0	0
7	-3375	$-1 \cdot 3^3 \cdot 5^3$
11	-32768	$-1 \cdot 2^{15}$
19	-884736	$-1 \cdot 2^{15} \cdot 3^3$
43	-884736000	$-1 \cdot 2^{18} \cdot 3^3 \cdot 5^3$
67	-147197952000	$-1 \cdot 2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
163	-262537412640768000	$-1 \cdot 2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Weierstrass 方程式

$$E_d : y^2 = x^3 + A_d x + B_d \ ; \quad \mathrm{End}(E_d) = \mathcal{O}_{K_d}$$

$$\begin{aligned}
E_1 &: y^2 = x^3 - x, \\
E_2 &: y^2 = x^3 - 30x + 56, \\
E_3 &: y^2 = x^3 + 1, \\
E_7 &: y^2 = x^3 - 35x + 98, \\
E_{11} &: y^2 = x^3 - 264x + 1694, \\
E_{19} &: y^2 = x^3 - 152x + 722, \\
E_{43} &: y^2 = x^3 - 3440x + 77658, \\
E_{67} &: y^2 = x^3 - 29480x + 1948226, \\
E_{163} &: y^2 = x^3 - 8697680x + 9873093538.
\end{aligned}$$

主結果

各 E_d について，α_d 倍写像は次のように表せる：

$$[\alpha_d](x,y) = \left(\frac{1}{\alpha_d^2} \left(x + \frac{\phi_{\alpha_d}(x)}{\psi_{\alpha_d}^2(x)} \right), \frac{y}{\alpha_d^3} \left(1 + \frac{\omega_{\alpha_d}(x)}{\psi_{\alpha_d}^3(x)} \right) \right)$$

$$\psi_{\alpha_d},\ \phi_{\alpha_d},\ \omega_{\alpha_d} \in \mathcal{O}_{K_d}[x]$$

確認事項

- $\mathrm{End}(E)$ の元であること :

$$X = \frac{1}{\alpha_d^2}\left(x + \frac{\phi_{\alpha_d}(x)}{\psi_{\alpha_d}^2(x)}\right), Y = \frac{y}{\alpha_d^3}\left(1 + \frac{\omega_{\alpha_d}(x)}{\psi_{\alpha_d}^3(x)}\right) \text{として},$$

$$Y^2 = X^3 + A_d X + B_d$$

- α_d 倍写像であること :

$$[\alpha_d][\overline{\alpha_d}] = [\alpha_d \overline{\alpha_d}]$$

- 埋め込み方も考慮に入れる場合 :

$$[\alpha]^* \omega = \alpha\omega \quad \Leftrightarrow \quad \frac{dX}{Y} = \alpha_d \frac{dx}{y}$$

例 $(d = 1, 2, 3)$

$$[\alpha_1](x, y) = (-x,\ \alpha_1 y) \quad \Leftrightarrow \quad [\mathrm{i}](x, y) = (-x,\ \mathrm{i}y)$$

$$[\alpha_3](x, y) = (\alpha_3 x,\ y) \quad \Leftrightarrow \quad [\omega](x, y) = (\omega x,\ y)$$

$$[\alpha_2](x, y) = \left(\frac{1}{\alpha_2^2}\left(x + \frac{-36(x-4)}{(x-4)^2}\right), \frac{y}{\alpha_2^3}\left(1 + \frac{-18(x-4)}{(x-4)^3}\right)\right)$$

$$= \left(-\frac{1}{2}\left(x - \frac{36}{(x-4)}\right), -\frac{y}{2\sqrt{-2}}\left(1 - \frac{18}{(x-4)^2}\right)\right)$$

例 $(d = 43)$

$$\psi_{43} = \alpha_{43}x^5 - 12(21\alpha_{43} + 11)x^4 + 172(134\alpha_{43} + 121)x^3 - 3784(263\alpha_{43} + 320)x^2 + 29584(699\alpha_{43} + 1045)x - 59168(2826\alpha_{43} + 4951)$$

$$\begin{aligned}\phi_{43} = {} & 344(22(29\alpha_{43} - 88)x^9 + (619641 - 233211\alpha_{43})x^8 + 3784(9936\alpha_{43} - 23045)x^7 \\ & -8944(392131\alpha_{43} - 791164)x^6 + 59168(3525891\alpha_{43} - 6159571)x^5 \\ & -29584(277458944\alpha_{43} - 416931603)x^4 + 20353792(10500091\alpha_{43} - 13445696)x^3 \\ & -40707584(87263617\alpha_{43} - 93970855)x^2 + 2625639168(13032756\alpha_{43} - 11580809)x \\ & -875213056(166383621\alpha_{43} - 118657286))\end{aligned}$$

$$\begin{aligned}\omega_{43} = {} & 688((649\alpha_{43} + 3509)x^{13} + 363(730\alpha_{43} + 4279)x^{12} - 4120776(12\alpha_{43} + 77)x^{11} \\ & +516(10766883\alpha_{43} + 76903057)x^{10} - 59168(7036286\alpha_{43} + 57389409)x^9 \\ & +355008(61228382\alpha_{43} + 592271339)x^8 - 30530688(26155900\alpha_{43} + 317859729)x^7 \\ & +15265344(1319129386\alpha_{43} + 22162728049)x^6 \\ & -1312819584(240772331\alpha_{43} + 6789516888)x^5 \\ & +3500852224(532901684\alpha_{43} + 50071254101)x^4 \\ & +75268322816(476338494\alpha_{43} - 3322173649 3)x^3 \\ & -1806439747584(527103790\alpha_{43} - 13555658919)x^2 \\ & +12946151524352(711380145\alpha_{43} - 11387935757)x \\ & -51784606097408(673230288\alpha_{43} - 7951005307))\end{aligned}$$

§3. 考察

アルゴリズム

1. $n = |\alpha_d|^2$ 等分多項式 ψ_n を求める．
2. ψ_n を $\mathbb{Q}$ 上で因数分解し，該当する $\mathbb{Q}$ 上既約多項式 ψ' を選ぶ．
3. ψ' を K_d 上で因数分解し，該当する K_d 上既約多項式を ψ_{α_d} とする．
4. 係数が決まっていない多項式 ϕ' を用意し，
   $\Phi(x) = \frac{1}{\alpha_d^2}\left(x + \frac{\phi'(x)}{\psi_{\alpha_d}^2(x)}\right)$ を $\overline{\Phi}$ の x に代入して，
   通分した後の分母を ψ_n' とする．
5. ψ_n' と ψ_n が一致するような ϕ' を ϕ_{α_d} とする．
6. ψ_{α_d} と ϕ_{α_d}' から x 成分を構成し，y 成分は不変微分を使って求める．

例　$K = \mathbb{Q}(\sqrt{-5})$（類数 2）の場合

- $\beta = \sqrt{-5}$

$$K_\beta = \mathbb{Q}(\beta), \qquad \mathcal{O}_{K_\beta} = \mathbb{Z} + \beta\mathbb{Z}$$

$h_{K_\beta} = 2$, $j(\beta) : x^2 - 1264000x - 681472000 = 0$ の根

$$[\beta](x, y) = \left(\frac{1}{\beta^2} \left(x + \frac{\phi_\beta(x)}{\psi_\beta^2(x)} \right), \frac{y}{\beta^3} \left(1 + \frac{\omega_\beta(x)}{\psi_\beta^3(x)} \right) \right)$$

$$\psi_\beta,\ \phi_\beta,\ \omega_\beta \in \mathcal{O}_{K_\beta}[x]$$

例　$K = \mathbb{Q}(\sqrt{-5})$（類数 2）の場合

$$E_{\beta,1} : y^2 = x^3 - 15(21650 + 5967\sqrt{5})x + 4180(21650 + 5967\sqrt{5})$$

$$\psi_\beta = -x^2 + (695 + 225\sqrt{5})x - 129925 - 90738\sqrt{5}$$

$$\begin{aligned}\phi_\beta = {} & 72(21650 + 5967\sqrt{5})x^3 - 1080(1393000 + 786741\sqrt{5})x^2 \\ & +1080(639113791 + 352507230\sqrt{5})x \\ & -9000(11488491805 + 6471088308\sqrt{5})\end{aligned}$$

$$\begin{aligned}\omega_\beta = {} & 72(21650 + 5967\sqrt{5})x^4 - 360(4006075 + 2916783\sqrt{5})x^3 \\ & +1080(813332477 + 509573655\sqrt{5})x^2 \\ & -1800(88716208049 + 88359212745\sqrt{5})x \\ & +360(34326214125625 + 4274162432726\sqrt{5})\end{aligned}$$

例　$K = \mathbb{Q}(\sqrt{-5})$（類数 2）の場合

$$E_{\beta,2} : y^2 = x^3 - 15(21650 - 5967\sqrt{5})x + 4180(21650 - 5967\sqrt{5})$$

$$\psi_\beta = x^2 + (-695 + 225\sqrt{5})x + 129925 - 90738\sqrt{5}$$

$$\begin{aligned}\phi_\beta = {} & 72(21650 - 5967\sqrt{5})x^3 - 1080(1393000 - 786741\sqrt{5})x^2 \\ & +1080(639113791 - 352507230\sqrt{5})x \\ & -9000(11488491805 - 6471088308\sqrt{5})\end{aligned}$$

$$\begin{aligned}\omega_\beta = {} & 72(-21650 + 5967\sqrt{5})x^4 - 360(-4006075 + 2916783\sqrt{5})x^3 \\ & +1080(-813332477 + 509573655\sqrt{5})x^2 \\ & -1800(-88716208049 + 88359212745\sqrt{5})x \\ & +360(-34326214125625 + 4274162443272\sqrt{5})\end{aligned}$$

例　$\mathbb{Q}(\sqrt{-1})$ の（極大でない）整環

- $\gamma = 1 + 2\sqrt{-1}$

$$K_\gamma = \mathbb{Q}(\sqrt{-1}), \qquad \mathcal{O}_\gamma = \mathbb{Z} + \gamma\mathbb{Z}$$

$$\sharp Pic(\mathcal{O}_\gamma) = 1, \qquad j(\gamma) = 287496$$

$$E_\gamma : y^2 = x^3 - 11x + 14$$

$$\psi_\gamma = \gamma x^2 + (-3\gamma - 5)x + 2\gamma + 9$$

$$\phi_\gamma = 44(\gamma + 5)x^3 - 12(13\gamma + 105)x^2 + 4(33\gamma + 581)x + 12(\gamma - 115)$$

$$\omega_\gamma = -44(9\gamma - 35)x^4 + 2000(\gamma - 5)x^3 + (23640 - 2856\gamma)x^2 - 176(\gamma + 135)x + 2132\gamma + 8260$$