種数１の曲線のガロワ点とガロワ群

新津高校

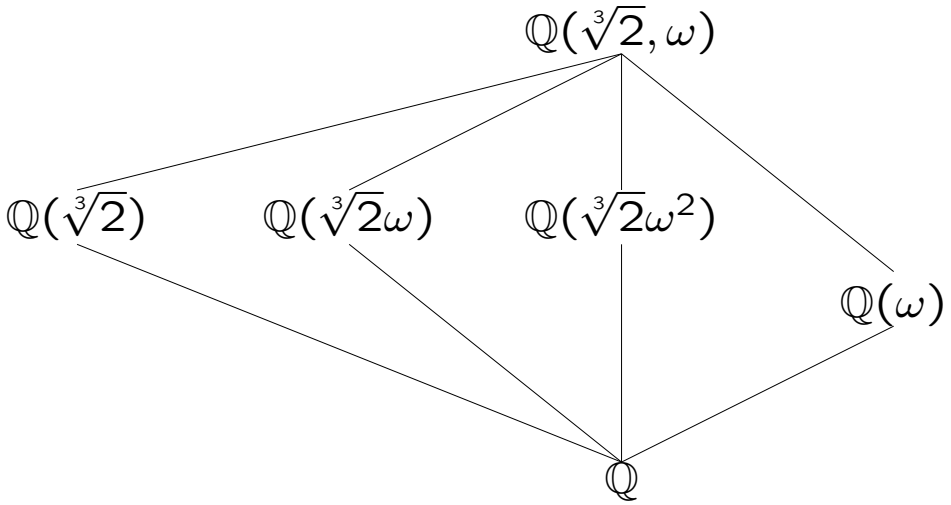
金沢光則

Galois 群は根の置換

$x^3 = 2$ $\qquad$ $x = \sqrt[3]{2},\ \sqrt[3]{2}\omega,\ \sqrt[3]{2}\omega^2$

$\mathbb{Q}(\sqrt[3]{2}, \omega)$: 最小分解体（根をすべて添加した体）このなかで根の置換が自己同型

体の拡大



文字にしよう

$x^3 = y$：代入するのは $\mathbb{C}$：$x = \sqrt[3]{y},\ \sqrt[3]{y}\omega,\ \sqrt[3]{y}\omega^2$

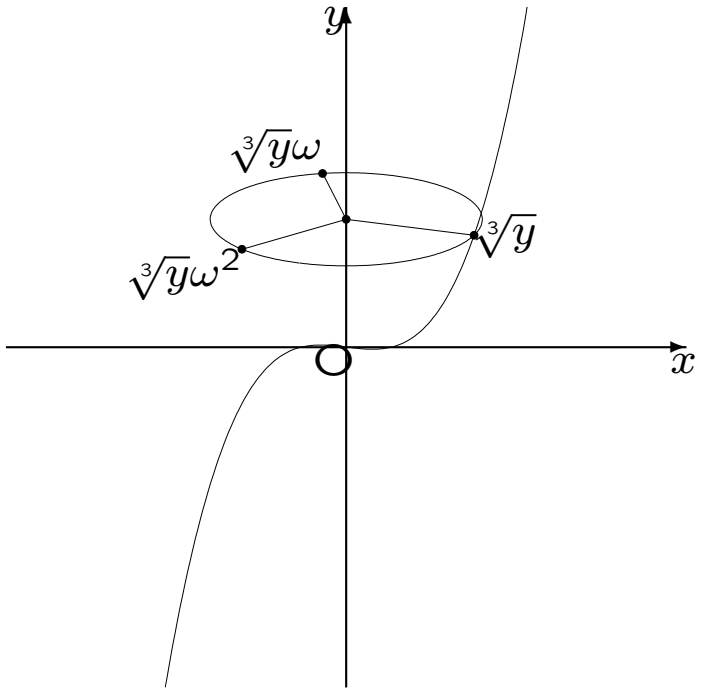
体の拡大は Galois 拡大

$\mathbb{C}(\sqrt[3]{y})$

$\mathbb{C}(y)$

代数幾何は、代数方程式で定義された図形を扱う。

根の置換は、曲線の自己同型を与える。(∞ からの射影)



Galois 群で対称性を見る

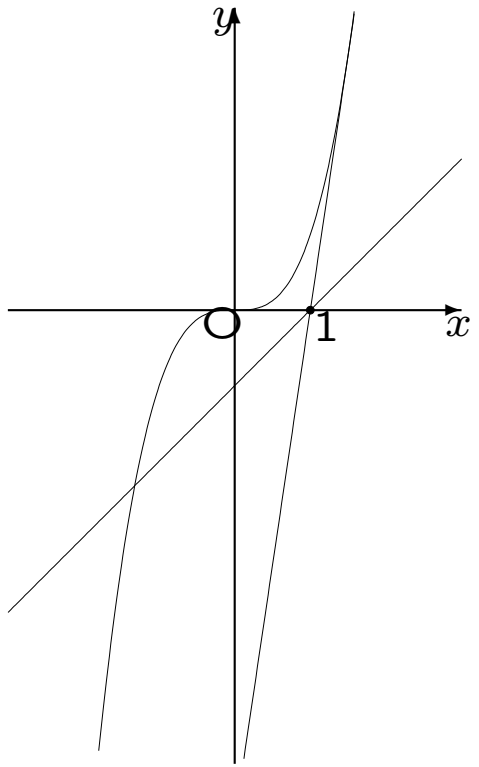
$y = x^3$ を点$(1,0)$からの射影でみる

交点は $x^3 - a(x-1) = 0$の根。aをyにして

$x^3 - yx + y = 0$

判別式 $D = y^2(4y - 27)$.

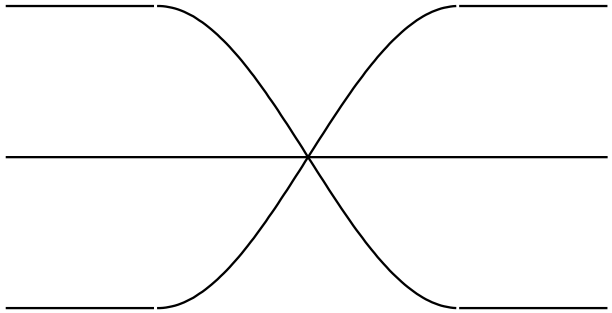
$y = \dfrac{27}{4}$のとき、$(x+3)(x-\frac{3}{2})^2 = 0$



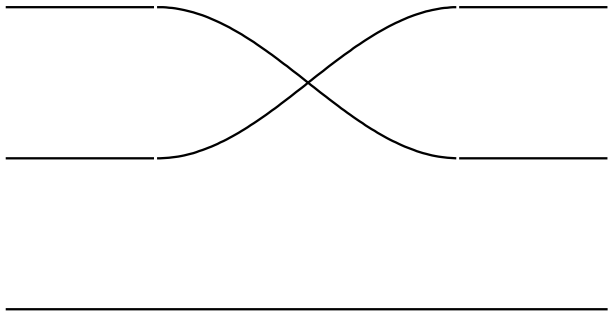
$x^3 = y$ はGalois だが、$x^3 - yx + y = 0$は根の置換が体の同型を与えないので、Galoisではない。

被覆

Galois



Galois ではない



問題意識

Galois 点（射影の中心。体の拡大が Galois）がたくさんあると、図形の対称性は高い。Galois 群で、対称の形がわかる。

1. Galois 点はどれだけあるか

2. Galois 群にはどんなものがあるか

3. Galois でないとき、Galois 閉包との関係は

わかっていたこと（2に関して）

C ： 非特異平面代数曲線 次数$\geqq 3$ なら

ガロワ群は巡回群、位数＝次数

種数＝0（有理関数でパラメータ表示できる、実多様体としては球面）の曲線外の点（ガロワ点）のガロワ群は

Z_d, D_d, A_4, S_4, A_5 のみ。（多様体に作用するものすべて）

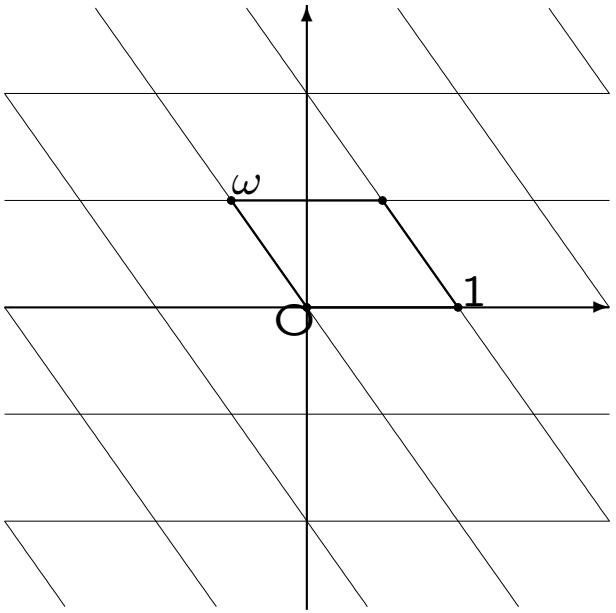
次は、種数１ ： 楕円曲線

楕円曲線 E

E は実多様体としてトーラス

問１　E に作用する自己同型群の有限部分群をすべて決定せよ。
問２　上の群を Galois 群にもつ平面曲線の定義方程式を作れ

$E = \mathbb{C}/\mathcal{L}$, $\mathcal{L} = \mathbb{Z} + \mathbb{Z}\omega$, $\omega \notin \mathbb{R}$



自己同型

$\mathrm{Auto}(\mathsf{E}) \ni \sigma : \mathsf{E} \to \mathsf{E}$

$\mathbb{C}$はEの普遍被覆。σ は$\mathbb{C}$上の正則関数

$\sigma(z+\lambda) - \sigma(z) \in \mathcal{L}$なので、定数

$\frac{d\sigma}{dz}(z+\lambda) = \frac{d\sigma}{dz}(z)$

$\frac{d\sigma}{dz}$はコンパクト多様体E上の正則関数なので定数

よって、$\sigma(z) = \alpha z + \beta$

α は回転を、βは平行移動を表す。

回転

$\alpha\mathcal{L} \subset \mathcal{L}$ から

$\alpha = m_1 + m_2\omega$, $\alpha\omega = n_1 + n_2\omega$, $\alpha^n z - z \in \mathcal{L}$ for some n. ωを消去して

$\alpha^2 - (m_1 + n_2)\alpha - m_2 n_1 = 0$, $\alpha^n = 1$ から、$\alpha = \zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_6$.

$\alpha \notin \mathbb{R}$ なら $\mathbb{Q}(\alpha) = \mathbb{Q}(\omega)$.

平行移動

$\beta(\iff z+\beta)$ は有限位数だから $\in \frac{1}{n}\mathcal{L}$ なので $\beta = \frac{a+b\omega}{n}$

有限群 G が、回転 $\sigma(z) = \omega z$ と平行移動 $\tau(z) = z + \beta$ を含むと、

$$\sigma\tau\sigma^{-1}(z) = \sigma\tau(\omega^{-1}z) = \sigma(\omega^{-1}z + \beta) = z + \omega\beta$$

平行移動が１つの元で生成されていれば、$\omega\beta = \lambda\beta$ $(\lambda \in \mathbb{C})$ となる。

これから、β, λ に制限が生じる。

例 1

回転が ω, 平行移動が $\frac{1+2\omega}{3}$

$$Z_3 \oplus Z_3 = \langle \omega, \tfrac{1+2\omega}{3} \rangle = \left\{ \omega^k z + l \cdot \tfrac{1+2\omega}{3} \right\}$$

$$\omega \cdot \tfrac{1+2\omega}{3} = \tfrac{\omega+2(-\omega-1)}{3} = \tfrac{-2-\omega}{3} = \tfrac{1+2\omega}{3}$$

$$\left\langle \omega, \tfrac{1-\omega}{9} \right\rangle = \left\langle \omega, \tfrac{\omega}{3}, \tfrac{1-\omega}{9} \right\rangle = \left\{ \omega^k z + l \cdot \tfrac{1}{9} + m \cdot \tfrac{\omega}{3} \right\} = Z_3 \ltimes (Z_9 \oplus Z_3)$$

例 2

回転が ω, 平行移動が $\frac{1+3\omega}{7}$

$$Z_3 \ltimes Z_7 = \left\langle \omega, \frac{1+3\omega}{7} \right\rangle = \left\{ \omega^k z + l \cdot \frac{1+3\omega}{7} \right\}$$

$$\omega \cdot \frac{1+3\omega}{7} = \frac{\omega+3(-\omega-1)}{7} = \frac{-3-2\omega}{7} = \frac{4+5\omega}{7} = 4 \cdot \frac{1+3\omega}{7}$$

$$\sigma\tau(z) = \sigma(z + \frac{1+3\omega}{7}) = \omega z + \omega \cdot \frac{1+3\omega}{7} = \omega z + 4 \cdot \frac{1+3\omega}{7}$$

$$\tau\sigma(z) = \tau(\omega z) = \omega z + \frac{1+3\omega}{7}$$

$$\left\langle \omega, \frac{1+2\omega}{7} \right\rangle = Z_3 \ltimes \mathcal{L} = Z_3 \ltimes (Z_7^{\oplus 7})$$

Eの有限自己同型群

$Z_l \ltimes (Z_n \oplus Z_m)$ $(l = 1, 2, 3, 4, 6,\ m|n)$

$l = 3, 6$ のとき $\frac{n}{m} = qp_1 \cdots p_k$, $(q = 1$ or 3 , p_i is odd prime $\equiv 1$ $(3))$

$l = 4$ のとき $\frac{n}{m} = qp_1 \cdots p_k$, $(q = 1$ or 2 , p_i is odd prime $\equiv 1$ $(4))$

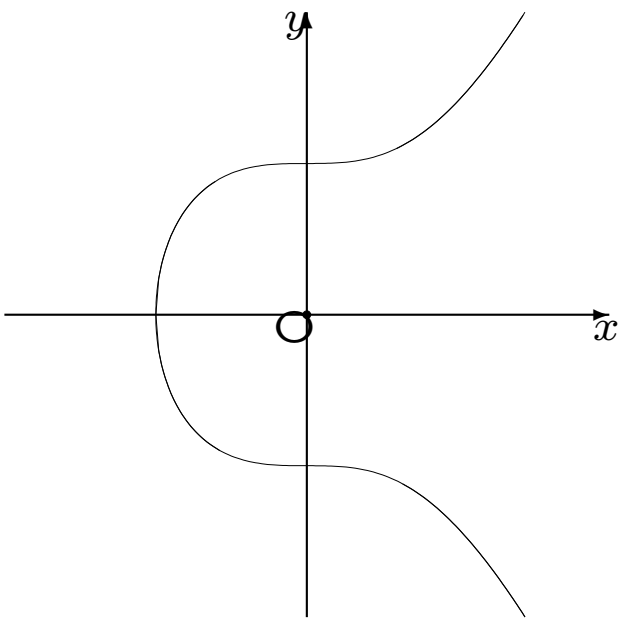
可換群はこれだけ

Z_2, $Z_2{}^{\oplus 2}$, $Z_2{}^{\oplus 3}$, Z_3, $Z_3{}^{\oplus 2}$, $Z_4 \oplus Z_2$, Z_4, Z_6

方程式

$y^2 = x^3 + 1$

楕円曲線： Weierstrassの標準形 $y^2 = x^3 + ax + b$



トーラスと Weierstrass の標準形は $\wp$ 関数でつながっているが、使うのは難しい

$\mathbb{C}/(1, \omega) \to y^2 = x^3 + ax + b$

$z \to (\wp(z), \wp'(z))$

$$\wp(z) = \frac{1}{z^2} + \sum_{\zeta \in \mathcal{L} \setminus \{0\}} \left\{ \frac{1}{(z-\zeta)^2} - \frac{1}{\zeta^2} \right\}$$

$$\wp'(z) = -2 \sum_{\zeta \in \mathcal{L}} \frac{1}{(z-\zeta)^3}$$

曲線への作用

$z \to (\wp(z), \wp'(z))$:

$$\wp(z) = \frac{1}{z^2} + \sum_{\zeta \in \mathcal{L} \setminus \{0\}} \left\{ \frac{1}{(z-\zeta)^2} - \frac{1}{\zeta^2} \right\}$$

$$\wp'(z) = -2 \sum_{\zeta \in \mathcal{L}} \frac{1}{(z-\zeta)^3}$$

$\mathcal{L} = \mathbb{C}/(1, \omega) \iff y^2 = x^3 + 1$
$\sigma(z) = -z : (x, y) \to (x, -y)$

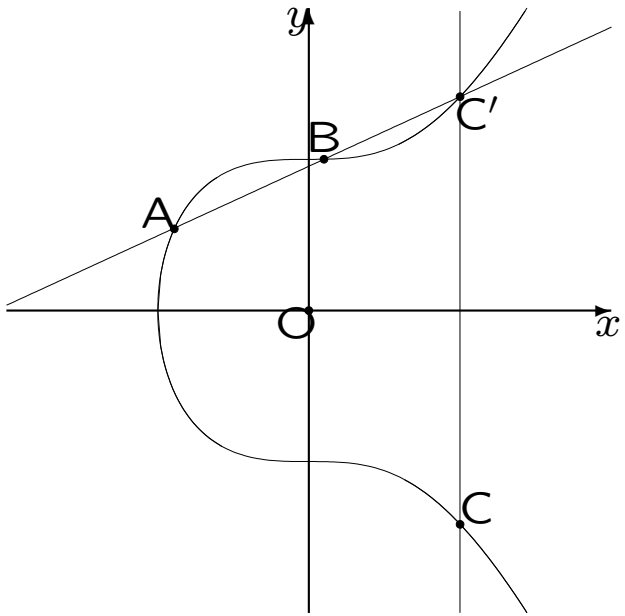
$\sigma(z) = \omega z : (x, y) \to (\omega x, y)$
$\sigma(z) = -\omega z : (x, y) \to (\omega x, -y)$

$\mathcal{L} = \mathbb{C}/(1, i) \iff y^2 = x^3 + x$
$\sigma(z) = -z : (x, y) \to (x, -y)$
$\sigma(z) = iz : (x, y) \to (-x, iy)$

平行移動はこの対応では難しい

曲線上の点の和

$y^2 = x^3 + 1$



A+B=C という演算がある。これはそのまま、トーラスでの複素数の和

位数nの平行移動 β には、位数 n の点 P の和が対応する

$(x, y) + P = (\tau(x), \tau(y))$

	$y^2 = x^3 + x$	$y^2 = x^3 + 1$
2位	(0,0),$(i,0)$,$(-i,0)$	$(-1,0)$, $(-\omega,0)$, $(-\omega^2,0)$
3位		(0,3)
4位	$(\pm 1, \pm\sqrt{2})$	

定義方程式を作る

(1) 楕円曲線 E と有限自己同型群 G を選ぶ

(2) E 上の有限位数の点を用いた平行移動を用意する

(3) G の作用で不変な有理関数 $t \in \mathbb{C}(x,y)^G$ を見つける

(4) $(s) + (t)_\infty \geqq 0$ となる有理関数 s を見つける ← (7) の十分条件

(5) $\mathbb{C}(s,t) = \mathbb{C}(x,y)$ を確かめる

(6) s と t の既約方程式を見つける

(7) (6) の多項式が s について、最高次係数が 1 で、次数が G の位数と同じことを確かめる

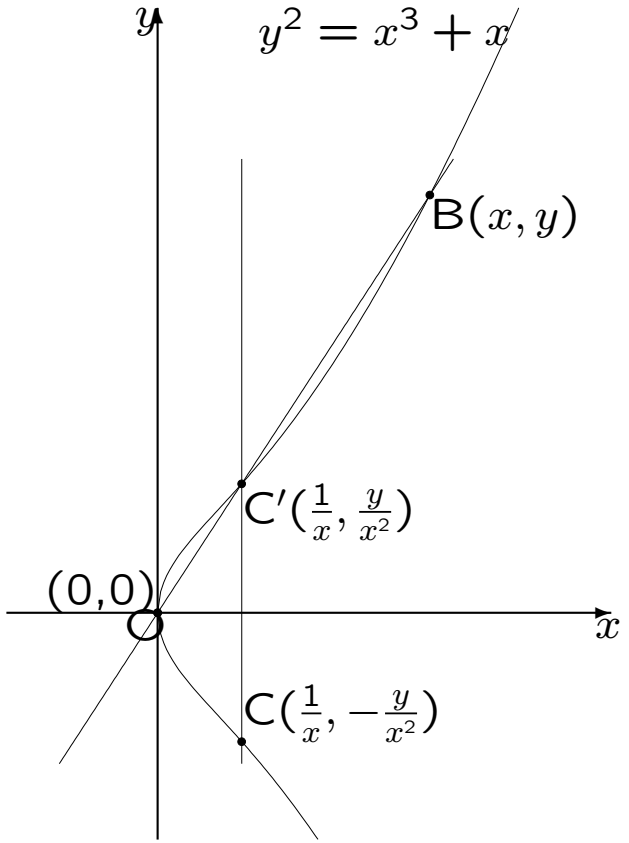
例$(Z_4 \oplus Z_2)$を作る

E：$y^2 = x^3 + x$, $\sigma(x) = -x$, $\sigma(y) = iy$, 平行移動は位数2 (0,0)

$$(x, y) + (0, 0) = \left(\frac{1}{x}, -\frac{y}{x^2}\right) = (\tau(x), \tau(y))$$

$$\mathbb{C}(x, y)^{\langle\sigma,\tau\rangle} \ni x^2 + \frac{1}{x^2} = \frac{x^6+x^2}{x^4} = \frac{y^4}{x^4} - 2$$

$t = \frac{y^4}{x^4}$ とおく。



極、零点、因子

$t = \frac{y^4}{x^4} = \frac{Y^4}{X^4}$

$y^2 = x^3 + x$ を$\mathbb{C}P^2$で考え、$Y^2Z = X^3 + XZ^2$とする。

$X = 0$とすると、$Y^2Z = 0$ ゆえ $(X : Y : Z) = (0 : 0 : 1),\ (0 : 1 : 0)$.

前者をP, 後者をQ

Pの近くで、$y^2 = x^3 + x = x(x^2 + 1) \sim x$ ゆえ正則パラメータはyで、$t = y^{-4}$
ゆえtはPで4位の極

同様にして $(t)_\infty = 4(0 : 0 : 1) + 4(0 : 1 : 0)$,

$(y) = -3(0 : 1 : 0) + (0 : 0 : 1) + (i : 0 : 1) + (-i : 0 : 1)$ で $(y) + (t)_\infty \geqq 0$

生成元：$\mathbb{C}(t,y)=\mathbb{C}(x,y)$

$tx^4=y^4,\ x^3=y^2-x$　：　次数下げを行う

$x^3=y^2-x,\ t(y^2x-x^2)=y^4\Rightarrow x^2=y^2x-\frac{y^4}{t}$

$x^2=y^2x-\frac{y^4}{t},\ y^2x^2-\frac{y^4x}{t}=y^2-x\Rightarrow y^2x^2=(\frac{y^4}{t}-1)x+y^2$

$\therefore x=\frac{\frac{y^4}{t}+1}{y^2-\frac{y^2}{t}+\frac{1}{y^2}}\in\mathbb{C}(t,y)$

これを直前の式に代入して

$y^8-(t^3-4t^2+2t)y^4+t^2=0$ を得る。yは$\mathbb{C}(t)$上８次既約方程式の根。

得た定義方程式

すべての可換群に対応するもの ： $Z_2^{\oplus 2}$ は難しい

非可換群では

D_3, D_4, $BD_{2\times 4}$

Thank you!