種数１の曲線のガロワ点とガロワ群

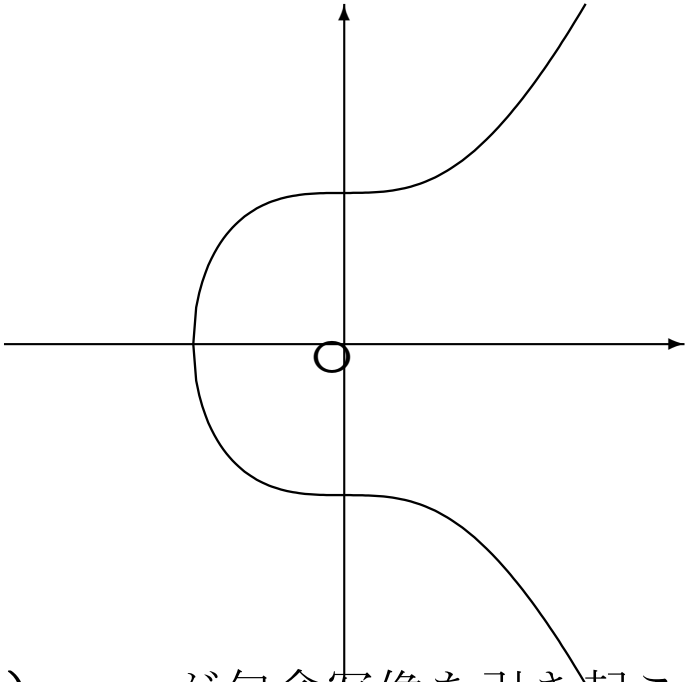
第１回：何をやったのか

第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定
第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

例１　楕円曲線への群 $\mathbb{Z}_3$ の作用（易）

$E : y^2 = x^3 + 1 \subset \mathbb{C}^2$: 楕円曲線とする



$\sigma : (x, y) \longrightarrow (e_3 x, y)$ によって、E に $G = \langle\sigma\rangle \cong \mathbb{Z}_3$ が作用する。$({e_3}^3 = 1, e_3 \neq 1)$

E の有理関数体 $\mathbb{C}(x, y) = Q(\mathbb{C}[X, Y]/(Y^2 - X^3 - 1))$ にも G が作用する。

$\sigma(x) = e_3 x$, $\sigma(y) = y$, $y \in \mathbb{C}(x, y)^G$ $\therefore$ $\mathbb{C}(x, y)^G = \mathbb{C}(y)$

$P = (1 : 0 : 0) \notin E$ を中心とする射影 $\pi_P : (x, y) \to y$ が包含写像を引き起こす。${\pi_P}^* : \mathbb{C}(y) = \mathbb{C}(x, y)^G \hookrightarrow \mathbb{C}(x, y)$

$\deg(x^3 - y^2 + 1) =^{\#} \mathbb{Z}_3$ より $\mathbb{C}(x, y)/\mathbb{C}(y)$ は３次のガロワ拡大、ガロワ群は $\mathbb{Z}_3$

例１　ガロワ点

図形でいうと、楕円曲線 $x^3 = y^2 - 1$ は、ガロワ点 $\mathrm{P} = (1 : 0 : 0)$ を持ち、そのガロワ群は $\mathbb{Z}_3$ である。

ガロワ点とガロワ群は対称性を表現している。

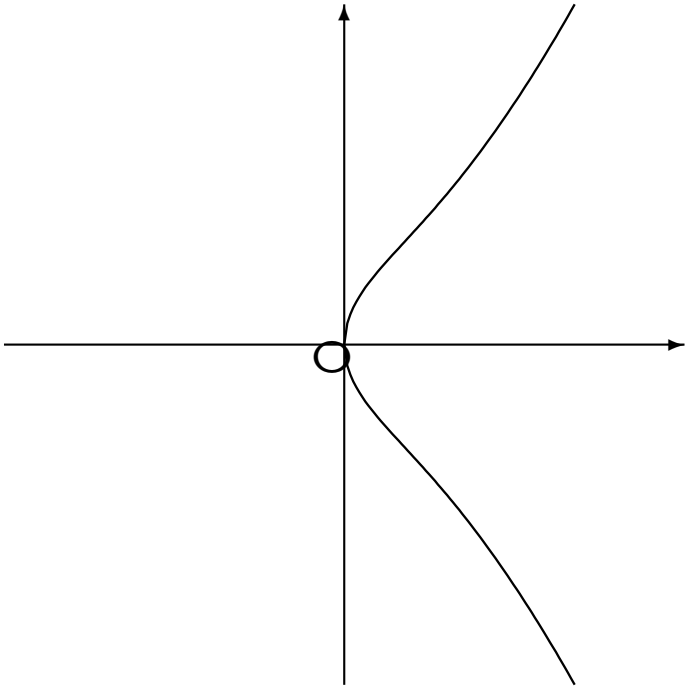
複素射影空間は、連比 $(a : b : c)$ 全体であり、$c \neq 0$ となる点全体が $(a : b : c) \longleftrightarrow (\frac{a}{c}, \frac{b}{c})$ これが有限部分の平面を表す。$c = 0$ は無限遠直線。

定義方程式は $X^3 = Y^2Z - Z^3$

関数は、$f(\frac{X}{Z}, \frac{Y}{Z})$ すなわち、$\dfrac{n\text{次の同次式}}{n\text{次の同次式}}$

例２　楕円曲線への群 $\mathbb{Z}_4$ の作用（易）

$E : y^2 = x^3 + x \subset \mathbb{C}^2$ ： 楕円曲線とする



$\sigma : (x, y) \longrightarrow (-x, e_4 y)$ によって、E に $G = \langle\sigma\rangle \cong \mathbb{Z}_4$ が作用する。

E の有理関数体 $\mathbb{C}(x, y) = Q(\mathbb{C}[X, Y]/(Y^2 - X^3 - X))$ にも G が作用する。

$\sigma(x) = -x,\ \sigma(y) = e_4 y$

$x\sigma(x) = -x^2 \in \mathbb{C}(x, y)^G$ ゆえ、$t = x^2 \in \mathbb{C}(x, y)^G$ とおく。

$y^2 = tx + x$ から $x = \dfrac{y^2}{t+1} \in \mathbb{C}(y, t)$ より $\mathbb{C}(x, y) = \mathbb{C}(y, t)/\mathbb{C}(t)$

例２　ガロワ点

$\pi_P{}^* : \mathbb{C}(t) = \mathbb{C}(x^2) = \mathbb{C}(x,y)^G \hookrightarrow \mathbb{C}(x,y) = \mathbb{C}(y,t)$

$P = (1:0:0)$ を中心とする射影 $\pi_P : (y,t) \to t$ から引き起こされる。

$$t = x^2 = \left(\frac{y^2}{t+1}\right)^2 \ \therefore y^4 = t(t+1)^2$$

deg $=^{\#} \mathbb{Z}_4$ だから、$\mathbb{C}(y,t)/\mathbb{C}(t)$ は４次のガロワ拡大： $y^4 = t(t+1)^2$

これは、既約多項式で、$\mathbb{C}(y,t) = \mathbb{C}(x,y)$ なので、$C : y^4 = t(t+1)^2$ は種数１の特異平面４次曲線で、ガロワ点 $P = (1:0:0) \notin C$ を持ち、ガロワ群は $\mathbb{Z}_4$ である。特異点は (y,t)=(0,−1)

例３　楕円曲線への群 $\mathbb{Z}_3{}^{\oplus 2}$ の作用(平行移動を含む)

$E : y^2 = x^3 + 1 \subset \mathbb{C}^2$: 楕円曲線とする

$$\sigma : (x, y) \longrightarrow (e_3 x, y), \quad \tau : (x, y) \longrightarrow \left(\frac{2 - 2y}{x^2}, \frac{y - 3}{y + 1} \right)$$

によって、E に $G = \langle \sigma, \tau \rangle \cong \mathbb{Z}_3{}^{\oplus 2}$ が作用する。$\mathbb{C}(x, y)$ にも作用する。

$$t = y + \tau(y) + \tau^2(y) = -y\tau(y)\tau^2(y) = \frac{y(y^2 - 9)}{y^2 - 1} \in \mathbb{C}(x, y)^G$$

$$y = \frac{t(y^2 - 1)}{y^2 - 9} = \frac{tx^3}{x^3 - 8} \in \mathbb{C}(x, t) \text{ より、} \mathbb{C}(x, y) = \mathbb{C}(x, t),$$

不変元を求める、生成することを示す、定義方程式を計算することが難しい。

例３　ガロワ点

$\sigma(x) = e_3 x,\ \tau(x) = \dfrac{2-2y}{x^2} = \dfrac{2((1-t)x^3-8)}{x^2(x^3-8)}.$

$\pi_P{}^* : \mathbb{C}(t) = \mathbb{C}\left(\dfrac{y(y^2-9)}{y^2-1}\right) = \mathbb{C}(x,y)^G \hookrightarrow \mathbb{C}(x,y) = \mathbb{C}(x,t)$

deg $=^{\#} G$ ゆえ$\mathbb{C}(x,t)/\mathbb{C}(t)$ はガロワ拡大： $x^9-(t^2+15)x^6+48x^3+64 = 0$

これは $P = (1:0:0)$ を中心とする射影 $\pi_P : (x,t) \to t$ から引き起こされる。

$C : x^9 - (t^2+15)x^6 + 48x^3 + 64 = 0$ は種数１の特異平面９次曲線で、特異点 (0 : 1 : 0), ガロワ点 P = (1 : 0 : 0) を持ち、ガロワ群は $\mathbb{Z}_3{}^{\oplus 2}$ である。

やったこと

種数 1 の平面曲線 C はどんなガロワ点をもつか。その群と曲線の定義方程式を決定する。

平面楕円曲線の Weierstrass 標準形は、$y^2 = x^3 + 1$, $y^2 = x^3 + x$

これと双有理同値な曲線 C (有理関数体が一致する) に作用する有限群 G と不変元 t を使って、$\mathbb{C}(s,t) = \mathbb{C}(x,y)$ を満たし、$\mathbb{C}(s,t)/\mathbb{C}(t)$ がガロワ拡大となるような、G をすべて決定した。

すべての可換群 G に対して、定義方程式を決定した。いくつかの非可換群に対する定義方程式を決定した。次数は t を係数として、最高次係数が 1 で、t も変数とみて、最高次数が群の位数と一致する必要がある。

目標

無限体 k 上の超越拡大体 K は、純超越拡大体上の代数拡大（単拡大）となる。これは、射影空間内の超曲面（余次元1）を考えることである。代数拡大はガロワ群で調べるのが普通であり、代数多様体ではいろいろなことがわかっているので、体のガロワ拡大を代数多様体として調べることが目標である。

今回の方法は、曲線で、次数あるいは種数（非特異なら同じこと）を決め、非特異モデルに作用する群を定める。その群をガロワ群にもつ（特異）平面曲線を作る。

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。対称性は、分岐被覆で考えている。

なぜ？

なぜ種数１？　　なぜ楕円曲線と言わない？
なぜその標準形？　なぜその群？
なぜその作用？　　なにが新しいの？
ガロワ点てなに？　対称性はどこで出てくるの？
次の問題は？

Galois 点はどれだけあるか
Galois 群にはどんなものがあるか
Galois でないとき、Galois 閉包との関係は
異なる Galois 群をもつ曲線が存在するか？

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか

第２回：楕円曲線上の有限位数の自己同型

第３回：格子による自己同型の決定
第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

楕円曲線上の有限位数の自己同型

有理曲線（種数0）については、ほぼ終わり。次は楕円曲線（種数1）。

楕円曲線 E は、格子 $\mathcal{L}$ を用いて、$E = \mathbb{C}/\mathcal{L}$ と書ける。E は普遍被覆 $\mathbb{C}$ を持ち、同型 $\sigma : E \to E$ は、正則関数 $\tilde{\sigma} : \mathbb{C} \to \mathbb{C}$ $(\forall \lambda \in \mathcal{L} : \tilde{\sigma}(z+\lambda) - \tilde{\sigma}(z) \in \mathcal{L})$ に拡張できる。E は弧状連結、$\mathbb{C}$は弧状連結で単連結、射影は、局所同型。

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\sigma}} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ E & \xrightarrow{\sigma} & E \end{array}$$

$\sigma(z+\lambda) - \sigma(z)$ は離散集合 $\mathcal{L}$ に値をとる連続関数だから定数。

$\forall \lambda \in \mathcal{L} : \dfrac{d\sigma(z+\lambda)}{dz} = \dfrac{d\sigma(z)}{dz}$ なので、導関数はコンパクト多様体 E 上の正則関数となり、楕円曲線 E 上で定数。

これから、σ が１次式となる。

座標変換して(σ １つを考えているので)、$\sigma(z) = cz$ と書ける。

この c を決定する。

１次式の係数（１）

σ が有限位数をもつ同型だから、$\exists n \in \mathbb{N} : c^n = c.\ c \neq 0$ より、$|c| = 1.$

格子を $\mathcal{L} = \{m + n\omega \mid m, n \in \mathbb{Z}\}$ と表すとき、$c\mathcal{L} \subset \mathcal{L}$ から$\exists m_1, m_2, n_1, n_2 \in \mathbb{Z} : c = m_1 + m_2\omega, c\omega = n_1 + n_2\omega$

$m_2 = 0$ なら $c \in \mathbb{Z}$ であり、$m_2 \neq 0$ なら $c \cdot \dfrac{c - m_1}{m_2} = n_1 + n_2 \cdot \dfrac{c - m_1}{m_2}.$

これから、$c^2 - (m_1 + n_2)c - n_1m_2 + n_2m_1 = 0$

$c \in \mathbb{C},\ |c| = 1,\ c$は整数係数のモニック (最高次の係数=1) な２次方程式の解なので、$c = \pm 1,\ \pm i,\ \zeta_3,\ {\zeta_3}^2,$ これを示す。

１次式の係数（２）

$X^n - 1 = (X^2 - pX + q)f(X) + kX + l$ とおき、$X = c$を代入すると、c が複素数であることから、$k = l = 0$.

整数係数の多項式を、モニックな整数係数の多項式で割ると、商と余りも整数係数の多項式になるので

$X^n - 1 = (X^2 - pX + q)(X^{n-2} + \cdots + a)$ であるが、定数項は $qa = -1$ となり、$q = \pm 1$. よって $q = c \cdot \bar{c} = |c|^2 = 1$ かつ $c + \bar{c} = p \in \mathbb{Z}$. これを満たすのは、$p = -2, -1, 0, 1, 2$ から、$c = -1, \pm {e_3}^2, \pm i, \pm e_3, 1$

$c = \pm 1,\ \pm\sqrt{-1}$ $(\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-1})$: 虚数乗法をもつ)

$c = \pm 1,\ \dfrac{\pm 1 \pm \sqrt{-3}}{2}$ $(\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$: 虚数乗法をもつ)

$c = \pm 1$ (otherwise)

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型

第３回：格子による自己同型の決定

第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

格子による自己同型の決定

G を E の自己同型よりなる有限群とする。

前回の話より、$G \ni \sigma$ は $\sigma(z) = cz + d$ $(c = \pm 1,\ \pm i,\ \pm e_3)$ と書ける。

cについての制限は、$E = \mathbb{C}/\mathcal{L}$ $(\mathcal{L} = \{a + b\omega \mid a, b \in \mathbb{Z}\})$ と書いたとき、$c\mathcal{L} \subset \mathcal{L}$ なので$c = a + b\omega$, $c\omega = a' + b'\omega$ となることから出たが、このとき、cが虚数なら$\mathbb{Q}(c) = \mathbb{Q}(\omega)$ である。したがって、$\mathcal{L}$ のωによって、cの値が制限される。

$\varphi : G \to \mathbb{C} :\ cz + d \to c$ とすると、$\varphi(G)$ は $\mathbb{C}$ の単位円周上の有限集合でできた群なので、原始元が存在する。それを c とし、座標変換をすることにより、$G \ni \sigma :\ \sigma(z) = cz$ としてよい。

このとき次は split exact sequence なので $G \cong G_0 \ltimes G_T$. G_0, G_T は可換群。

平行移動 1

$1 \to G_T(= \mathrm{Ker}\varphi) \longrightarrow G \xrightarrow{\varphi} G_0(= \mathrm{Im}\varphi) \to 1$

G_T は平行移動を表す。G_T の元は $z + d$ と書けるが、これを d と表す。

G_T の元は有限位数をもつので、$d = \dfrac{a + b\omega}{n}$ $(a, b \in \mathbb{Z})$ と書いてよい。

ここで、(a, b) と n は共通因数をもたないとしてよい。

$\psi : G_T \to \mathbb{C} : \dfrac{a + b\omega}{n} \to \dfrac{a}{n}$

の像は、$[0, 1)$ で、差が整数のとき同一視することで群を成している。

$\frac{a}{n} > 0$ の元があれば、正で最小のものが生成元になっているので、それに対応する G_T の元を d_0 とする。

平行移動２

$G_T/\langle d_0\rangle$は、有限群であり、$b\omega$とかけるので、もし$G_T \neq \langle d_0\rangle$ なら原始元がある。

$\frac{a}{n} > 0$ の元がないときも含めて、

$G_T = 1,$

$\cong \mathbb{Z}_n (= \langle \frac{a}{n} + \frac{b}{n}\omega \rangle),$

$\cong \mathbb{Z}_n \oplus \mathbb{Z}_m \ (= \langle \frac{a}{n} + \frac{b}{n}\omega, \frac{1}{m}\omega \rangle) \cdots Ⓐ$

有限群 $G = \mathbb{Z}_n \oplus \mathbb{Z}_m = \langle x, y \rangle$ のとき、

$ord(x+y) = L.C.M(ord(x), ord(y))$ ゆえ Ⓐ において $m \mid n$ としてよい。

平行移動３

σ を G_0 の生成元とする。$G_T \ni \tau$ に対して

$$\sigma\tau\sigma^{-1}(z) = \sigma\tau(c^{-1}z) = \sigma(c^{-1}z + d) = z + cd$$

より G_T は G_0 の元による内部自己同型によって不変なので、$G_T \supset \langle \tau, \sigma\tau\sigma^{-1} \rangle$

G_T が１次元のとき、$d = \dfrac{a + b\omega}{n}$ を原始元とすると、$cd = \lambda d$ $(k \in \mathbb{Z})$ となる。可換群となるのは $cd = d$ すなわち $\lambda = 1$ のとき。

$\omega = c = e_3$ のとき、$\omega \cdot \frac{a+b\omega}{n} = \lambda \cdot \frac{a+b\omega}{n} \quad \therefore \frac{a\omega+b(-\omega-1)}{n} = \frac{\lambda a+\lambda b\omega}{n}$

有限群G

$-b \equiv \lambda a \mod n,\ a - b \equiv \lambda b \mod n$

これから $(\lambda^2 + \lambda + 1)a \equiv 0,\ (\lambda^2 + \lambda + 1)b \equiv 0 \mod n$ となる。

(a, b) はnと共通因数をもたないので、$n \mid \lambda^2 + \lambda + 1$

$\omega = c = e_4$ のときは同様に $n|1 + \lambda^2$. 他の場合も同様。

$c = -1$ のときは、$n \mid \lambda + 1$.

$\#G_0 = 1$ のとき、$G = G_T = \mathbb{Z}_n,\ \mathbb{Z}_n \oplus \mathbb{Z}_m\ (m \mid n)$

$\#G_0 = 2$ のとき、$G = Z_2,\ Z_2 \ltimes \mathbb{Z}_n,\ Z_2 \ltimes (\mathbb{Z}_n \oplus \mathbb{Z}_m)\ (m \mid n)$

$\#G_0 > 2$ のとき、$G = G_0,\ G_0 \ltimes \mathbb{Z}_n,\ G_0 \ltimes (\mathbb{Z}_n \oplus \mathbb{Z}_m)\ (m \mid n)$, n,mは...

可換群

$\#G_0 = 1$ のとき、$G = G_T = \mathbb{Z}_n,\ \mathbb{Z}_n \oplus \mathbb{Z}_m\ (m \mid n)$

$\#G_0 = 2$ のとき、$G = Z_2,\ Z_2^{\oplus 2},\ Z_2^{\oplus 3}$

$\#G_0 > 2$ のとき、$G = G_0,\ Z_3^{\oplus 2},\ Z_4 \oplus \mathbb{Z}_2$

$\#G_0 > 2$ のとき、n の条件は難しい。

きちんと判定できないか？　が次回の話題。

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定

第４回：平行移動の条件と数論

第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

平行移動の条件と数論

有理整数 k が存在して $n \mid 1 + k^2$ が成り立つのは、n が４で割ると１余る有理整数の積かまたはその２倍である。

有理整数 k が存在して $n \mid 1 + k + k^2$ が成り立つのは、n が３で割ると１余る有理整数の積かまたはその３倍である。

前半の証明 1

$\mathbb{Z}[\sqrt{-1}]$ はユークリッド整域なのでUFD。$n = p_1 \cdots p_l$ を $\mathbb{Z}$ での素因数分解とする。

$n = p_1 \cdots p_l \mid (1 - k\sqrt{-1})(1 + k\sqrt{-1})$

p_j が、$\mathbb{Z}[\sqrt{-1}]$ で素数とする。$1 - k\sqrt{-1}$ の因子としてよい。$p_j(a + b\sqrt{-1}) = 1 - k\sqrt{-1}$ と書けるので、$ap_j = 1$ となり、$p_j = \pm 1$ となって矛盾。

よって、p_j は $\mathbb{Z}[\sqrt{-1}]$ で素数でないので 2 または、4 で割った余りが 1 の素数。

さらに、2^2 が n の約数になると、$2 = (1+\sqrt{-1})(1-\sqrt{-1})$, $(1+\sqrt{-1})^2 = 2\sqrt{-1}$, $(1-\sqrt{-1})^2 = -2\sqrt{-1}$ ゆえ、2がnの約数となり、上と同様に矛盾する。よって、2^2 は n の約数にはならない。

4で割ると1余る奇素数 p は,任意の$m \in \mathbb{Z}_{\geqq 0}$ に対して$p^{2^m} = a^2 + b^2$, $ab \neq 0$, $(a, b) = 1$ と書ける。

前半の証明２

$a, b, c, d \in \mathbb{Z}$ が $(a, b) = 1$, $(c, d) = 1$, $(a^2 + b^2, c^2 + d^2) = 1$ のとき $(a^2 + b^2)(c^2 + d^2) = A^2 + B^2$, $A, B \in \mathbb{Z}$, $(A, B) = 1$ となる。

$a^2 + b^2$ $(a, b) = 1$ は、ある $A \in \mathbb{Z}$ が存在して $1 + A^2$ の約数となる。

n を素因数分解して、２以外の素数のべきを 2^m に増やした数を N とする。この N に対して成り立つことが証明できる。

後半の証明 1

$1+k+k^2$ は奇数。$\mathbb{Z}[\sqrt{-3}]$ はユークリッド整域なのでUFD。$n = p_1 \cdots p_l$ を $\mathbb{Z}$ での素因数分解とする。

$n = p_1 \cdots p_l \mid (1-ke_3)(1-ke_3{}^2) \mid (2+k-k\sqrt{-3})(2+k+k\sqrt{-3})$

p_j が、$\mathbb{Z}[\sqrt{-3}]$ で素数とする。$2+k-k\sqrt{-3}$ の因子としてよい。$p_j(a+b\sqrt{-3}) = 2+k-k\sqrt{-3}$ と書けるので、$ap_j = 2+k$, $bp_j = -k$. $\therefore (a+b)p_j = 2$. p_j は奇数なので、矛盾。

よって、p_j は $\mathbb{Z}[\sqrt{-3}]$ で素数でないので 3 または、3 で割った余りが 1 の素数。

さらに、3^2 が n の約数になると、3 が $2+k-k\sqrt{-3}$ か $2+k+k\sqrt{-3}$ の約数となる。上と同じ理由により矛盾。よって、3^2 は n の約数にはならない。

3で割ると1余る奇素数 p は,任意の$m \in \mathbb{Z}_{\geqq 0}$ に対して$p^{2^m} = a^2+3b^2$, $ab \neq 0$, $(a,b) = 1$ と書ける。

後半の証明２

$a, b, c, d \in \mathbb{Z}$ が $(a, b) = 1$, $(c, d) = 1$, $(a^2 + 3b^2, c^2 + 3d^2) = 1$ のとき $(a^2 + 3b^2)(c^2 + 3d^2) = A^2 + 3B^2$, $A, B \in \mathbb{Z}$, $(A, B) = 1$ となる。

奇数 $a^2 + 3b^2$ $(a, b) = 1$ は、ある $A \in \mathbb{Z}$ が存在して $1 + A + A^2$ の約数となる。

$a^2 + 3b^2 = (a + b + 2be_3)(\overline{a + b + 2be_3})$ が奇素数で、$(a, b) = 1$ だから $(a+b, 2b) = 1$ なので$(a+b)x+2by = 1$ と書ける。$(a+b+2be_3)(x-ye_3) = 1 - Ae_3$, $(1 - Ae_3)(\overline{1 - Ae_3}) = 1 + A + A^2$

n を素因数分解して、3以外の素数のべきを2^mに増やした数を N とする。この N に対して成り立つことが証明できる。

次回は、群の楕円曲線への作用を考える。

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定
第４回：平行移動の条件と数論

第５回：図形としての楕円曲線と自己同型の回転

第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

図形としての楕円曲線と自己同型の回転

束 $\mathcal{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ に対して、$\wp(z) = \dfrac{1}{z^2} + \displaystyle\sum_{\zeta\in\mathcal{L}\setminus\{0\}} \left\{ \frac{1}{(z-\zeta)^2} - \frac{1}{\zeta^2} \right\}$ を Weierstrass のペー関数という。

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

$$\Phi : \mathbb{C}/\mathcal{L} \longrightarrow \Phi(\mathbb{C}/\mathcal{L}) \subset \mathbb{P}^2(\mathbb{C}) \qquad z \to \begin{cases} (\wp(z) : \wp'(z) : 1) & (z \neq 0) \\ (0:1:0) & (z = 0) \end{cases}$$

像の方程式は、$y^2 = 4(x-u_1)(x-u_2)(x-u_3)$

ただし、$u_1 = \wp\left(\dfrac{\omega_1}{2}\right)$, $u_2 = \wp\left(\dfrac{\omega_2}{2}\right)$, $u_3 = \wp\left(\dfrac{\omega_1}{2} + \dfrac{\omega_2}{2}\right)$

回転 1

Weierstrass の標準形：$\mathbb{C}/(1,\zeta_3)$：$y^2 = x^3 + 1$, $\mathbb{C}/(1,i)$：$y^2 = x^3 + x$

$\mathbb{Z}_2$ の作用は、$\sigma(z) = -z$ なので、$\sigma(x) = \wp(-z) = x$, $\sigma(y) = \wp'(-z) = -y$

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

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

$\mathbb{Z}_4$ は $y^2 = x^3 + x$ に作用し、$\sigma(z) = e_2 z$ なので、$\sigma(x) = \wp(e_2 z) = -x$, $\sigma(y) = \wp'(e_2 z) = e_2 y$

$$\wp(e_2 z) = \frac{1}{(e_2 z)^2} + \sum_{e_2\zeta\in\mathcal{L}\setminus\{0\}} \left\{ \frac{1}{(e_2 z - e_2\zeta)^2} - \frac{1}{(e_2\zeta)^2} \right\} = -\wp(z)$$

回転 2

$\wp'(e_2 z) = -2\sum_{e_2\zeta\in\mathcal{L}} \frac{1}{(e_2 z - e_2\zeta)^3} = e_2\wp'(z)$

$\mathbb{Z}_3$ は $y^2 = x^3 + 1$ に作用し、$\sigma(z) = e_3 z$ なので、$\sigma(x) = \wp(e_3 z) = e_3 x$,
$\sigma(y) = \wp'(e_3 z) = y$

$\wp(e_3 z) = \frac{1}{(e_3 z)^2} + \sum_{e_3\zeta\in\mathcal{L}\setminus\{0\}} \left\{ \frac{1}{(e_3 z - e_3\zeta)^2} - \frac{1}{(e_3\zeta)^2} \right\} = e_3\wp(z)$

$\wp'(e_3 z) = -2\sum_{e_3\zeta\in\mathcal{L}} \frac{1}{(e_3 z - e_3\zeta)^3} = \wp'(z)$

$\mathbb{Z}_6$ は $y^2 = x^3 + 1$ に作用し、$\sigma(z) = -e_3 z$ なので、$\sigma(x) = \wp(-e_3 z) = e_3 x$,
$\sigma(y) = \wp'(-e_3 z) = -y$

このやり方で、平行移動を計算することは非常に困難である。

実は、楕円曲線には加法群の構造がある。それは、複素平面上の加法を引き継いでいる。次回は、曲線上の加法を見てみよう。

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定
第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転

第６回：楕円曲線上の加法

第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

楕円曲線上の加法

楕円曲線 E は3次曲線なので、直線と3点で交わる（Bezout's の定理）。E 上の2点A, Bを結んだ直線との3番目の交点を C′ とし、x 軸に関して対称な点を C とする。(A, B) に対して C を対応させる2項演算は、和を定義する。これを座標で計算する。$(a,b)+(c,d)=(e,f)$ とすると、

$y^2=x^3+x$ の場合は、$e=\dfrac{(a+c)(ac+1)-2bd}{(a-c)^2}$,

$$f=\frac{(3a^2c+c+a^3+3a)d-(c^3+3ac^2+3c+a)b}{(a-c)^3}.$$

$y^2=x^3+1$ の場合は、$e=\dfrac{-2bd+ac^2+a^2c+2}{(a-c)^2}$,

$$f=\frac{(3a^2c+a^3+4)d-bc^3-3abc^2-4b}{(a-c)^3}.$$

楕円曲線上の２倍点

接線との交点を使うことにより、２倍点の公式を得る。

$y^2 = x^3 + x$ の場合は、

$$2(a,b) = \left(\frac{(a^2-1)^2}{4b^2}, \frac{a^6+5a^4-5a^2-1}{8b^3} \right)$$

$y^2 = x^3 + 1$ の場合は、

$$2(a,b) = \left(\frac{a(b^2-9)^2}{4b^2}, \frac{b^4+18b^2-27}{8b^3} \right)$$

有限位数の有理点

$E : y^2 = x^3 + ax^2 + bx + c$

に対して、$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ とおくと、点 (x, y) が有限位数の有理点ならx,yはともに整数であり、$y = 0$ ($\Longleftrightarrow$ $2P = 0$) または $y \mid D$.

$E : y^2 = x^3 + x$ では、(0,0):位数２

$E : y^2 = x^3 + 1$ では、$(-1, 0)$:位数２、(0,1),(2,3):位数３、(2,3):位数６

次回は、曲線上の加法構造を使って、群の作用を表現する。

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定
第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法

第７回：楕円曲線の加法と平行移動

第８回：楕円曲線上の因子
第９回：例

新津高校　金沢光則

楕円曲線の加法と平行移動

位数2の点は、$y=0$ で求められる。$y^2=x^3+x$ の場合は、(0,0),(e_4,0),($-e_4$,0) の３点。

$$(x,y)+(0,0)=\left(\frac{1}{x},-\frac{y}{x^2}\right)=(\tau_1(x),\tau_2(y))$$

$$(x,y)+(e_4,0)=\left(\frac{e_4(x+e_4)}{x-e_4},\frac{2y}{(x-e_4)^2}\right)=(\tau_2(x),\tau_2(y)).$$

$$(x,y)+(-e_4,0)=\left(-\frac{e_4(x-e_4)}{x+e_4},\frac{2y}{(x+e_4)^2}\right)=(\tau_3(x),\tau_3(y)).$$

$x+\tau_2(x)=\frac{x^2-1}{x-e_4}\in\mathbb{C}(x,y)^{\langle\tau_2\rangle}$. τ_1 では、次数の条件を満たさない。

平行移動２

$y^2 = x^3 + 1$ では、

$4(0,1) = 2(0,1) + 2(0,1) = 2(0,-1) = (0,1)$

から、$3(0,1) = O$

$$(x,y) + (0,1) = \left(\frac{2-2y}{x^2}, \frac{x^3+4-4y}{x^3}\right) = \left(\frac{2-2y}{x^2}, \frac{y-3}{y+1}\right) = (\tau(x), \tau(y))$$

$$x + \tau(x) + \tau^2(x) = \frac{y+3}{x^2} \in \mathbb{C}(x,y)^{\langle\tau\rangle}$$

τ_1 と τ_2

τ_2 を使って、$\mathbb{Z}_2{}^{\oplus 2}$ の作用をもつ曲線の定義方程式を得る。

$4s^4 - 4(e_4t + 2)s^3 - (t^2 + 4(2 + e_4)t - 8(1 - e_4))s^2 + 2(2e_4t^2 + (2 - e_2)t - 2(1 - 2e_4))s + (t^3 + 4t^2 - 3e_4t^2 + 4t + 8e_4t - 3) = 0$

τ_1 を使うと、

$y^4 + (2t - t^3)y^2 + t^2 = 0$ となる。

$E : y^2 = x^3 + x \longrightarrow y^4 + (2t - t^3)y^2 + t^2 = 0 : (x, y) \longrightarrow (y, \frac{y^2}{x^2}) : (0, 1) \longrightarrow (1, \infty) = (0 : 1 : 0)$: 内ガロワ点

次回は、群をガロワ群に持つ曲線の定義方程式を得るために、曲線上の因子を計算する。

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定
第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動

第８回：楕円曲線上の因子

第９回：例

新津高校　金沢光則

楕円曲線上の因子 1

$E : y^2 = x^3 + 1$ 上で、因子 (x) を計算する。

$E : Y^2Z = X^3 + Z^3$ と射影平面上の式で考える。

$(x) = \left(\frac{X}{Z}\right)$ なので、$X = 0$ のときと $Z = 0$ のときを考える。

$X = 0$ のとき、$(Y - Z)(Y + Z)Z = 0$ から、

交点は (0:1:1), (0:−1:1), (0:1:0)

$Z = 0$ のとき、$X = 0$ から交点は (0:1:0)

楕円曲線上の因子２

点 (0:1:1) では、$Z = 1$ で考えて、$y = x^3 + 1$ 上の点 (0,1) において、(x) の係数を求める。平行移動して、y を $y - 1$ に置き換えると、$y = x^3$ 上の点 (0,0) における正則パラメータは x なので、(x) の係数は１である。

点 (0:−1:1) では、$Z = 1$ で考えて、$y = x^3 + 1$ 上の点 (0,−1) において、(x) の係数を求める。平行移動して、y を $y + 1$ に置き換えると、$y = x^3$ 上の点 (0,0) における正則パラメータは x なので、(x) の係数は１である。

点 (0:1:0) では、$Y = 1$ で考えて、$z = x^3 + z^3$ 上の点 (0,0) において、(x) の係数を求める。$x^3 = z(1 - z^2)$ で、$1 - z^2$ は可逆元だから、正則パラメータは x, $z \sim x^3$. よって、$\left(\frac{X}{Z}\right) = \left(\frac{x}{z}\right) = (x^{-2}) = -2(x)$

楕円曲線上の因子３

$(x)_0 = (0:1:1) + (0:-1:1)$, $(x)_\infty = 2(0:1:0)$

よって $(x) = -2(0:1:0) + (0:1:1) + (0:-1:1)$

$(y) = (\frac{Y}{Z})$, $Z = 0$ とすると $X = 0$ なので $Y = 1$ として、$x^3 = z - z^3$ ゆえ、正則パラメータは　x なので、$(\frac{1}{z}) = (x^{-3}) = -3(x)$.

よって $(y)_\infty = 3(0:1:0)$ から

$(x) + (y)_\infty = (0:1:0) + (0:1:1) + (0:-1:1) \geqq 0$

次回は、群を具体的に決めて、それに対する曲線の定義方程式を求める。

種数１の曲線のガロワ点とガロワ群

第１回：何をやったのか
第２回：楕円曲線上の有限位数の自己同型
第３回：格子による自己同型の決定
第４回：平行移動の条件と数論
第５回：図形としての楕円曲線と自己同型の回転
第６回：楕円曲線上の加法
第７回：楕円曲線の加法と平行移動
第８回：楕円曲線上の因子

第９回：例

新津高校　金沢光則

非可換の例 ： D_3

$E : y^2 = x^3 + 1 \cdots ①$, $\sigma(x) = x$, $\sigma(y) = -y$, $\tau(x) = \frac{2-2y}{x^2}$, $\tau(y) = \frac{y-3}{y+1}$

$t = x + \tau(x) + \tau^2(x) = \frac{y^2+3}{x^2}(\cdots ②) \in \mathbb{C}(x,y)^{\langle\sigma,\tau\rangle}$

$(t)_\infty = 2(0:1:0) + 2(0:1:1) + 2(0:-1:1)$,

$(x) = -2(0:1:0) + (0:1:1) + (0:-1:1)$,

$(y) = -3(0:1:0) + (-1:0:1) + (-e_3:0:1) + (-{e_3}^2:0:1)$

よって $\left(\frac{y}{x}\right) + (t)_\infty > 0$

そこで、$s = \frac{y}{x} \cdots ③$ とおくと、①，②，③ から y を消去して $tx^2 = x^3 + 4 \cdots ④$, $s^2x^2 = x^3 + 1 \cdots ⑤$. x について次数下げを行うと、$x^2 = \frac{3}{t-s^2}$. さらに 次数下げを行い、$x = \frac{4s^2-t}{3} \in \mathbb{C}(s,t)$. よって、$y = sx \in \mathbb{C}(s,t)$.

④，⑤ から 終結式により x を消去して

$$16s^6 - 24s^4t + 9s^2t^2 - t^3 + 27 = 0$$

次の仕事

(1) もっと大きな非可換群の例を作る
(2) 種数２以上の曲線に対して研究する
(3) 有理関数体とそのガロワ閉包の関係

終結式 resultant

$f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m,\ g(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_m & & \\ & a_0 & a_1 & \cdots & a_m & \\ & & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_n & & \\ & b_0 & b_1 & \cdots & b_n & \\ & & b_0 & b_1 & \cdots & b_n \end{vmatrix} = {a_0}^n {b_0}^m \Pi(\alpha_i - \beta_j)$$

$f(x) = 0$ の解を α_i, $g(x) = 0$ の解を β_j とする。

$R(f,g) = 0 \iff f(x) = 0, g(x) = 0$ が共通解をもつ。

連立方程式から 1 文字を消去するために使える。

$R(f, f') \sim$ 判別式