

楕円曲線の 5 等分点の体について

阪大理学部 広瀬 行夫 (Yukio Hirose)

代数体 K 上の非可解ガロワ拡大の最も単純な例は、 K -係数 5 次方程式の分解体すなわち S_5 (または A_5)-拡大で与えられる。一方 $l \neq 2, 3$ を素数とすると、 K 上の楕円曲線 E の l 等分点により生成される体は例外を除いて K 上の非可解ガロワ拡大 (そこでの "相互律" は E の Hasse-Weil zeta 関数によりだいたい統制されている) であり、特に E の 5 等分点で生成される体は高々 K 上の S_5 -拡大体の 4 次巡回拡大体となる。その S_5 -拡大体を与える 5 次方程式を具体的に決定したのがここの主要な結果である。

§0 結果

K を標数 0 の体, E を K 上の楕円曲線

$$E: y^2 = x^3 + Ax + B \quad (A, B \in K)$$

とし、 J_E を E の j -invariant $(= 2^8 3^3 A^3 / (4A^3 + 27B^2))$ とする。

素数 l を固定し、 $E[l]$ を E の l -torsion 元全体のなす部分群、

L は K に $\mathbb{E}[G]$ のすべての元の座標を K に付加した体 (" l 等分点の体 ") とする。

定理 $l=5$, $j_E \neq 0, 1728$ とする。 L は方程式

$$X^5 + 5X^4 + 40X^3 = j_E$$

の K 上の分解体の高々 4 次巡回拡大である。

$K = \mathbb{Q}$ (有理数体) とするとき、 L は 1 の原始 l 乗根を含む事が知られているから、 $L/\mathbb{Q}$ で L は分岐する。 L が $L/\mathbb{Q}$ で wildly ramify となる基準は Serre [1] により部分的に与えられているが、 $l=2, 3$ を除いて完全には知られていない。定理から、 $l=5$ の場合にだけ次の系を得た。結果はもちろん [1] と一致している。

系 $l=5$, $K = \mathbb{Q}_5$ (5-進体), $j_E \neq 0, 1728$ とし、整数 m , n はそれぞれ j_E , $j_E - 1728$ の 5 の order とする。このとき $L/\mathbb{Q}_5$ が wildly ramify とならない必要十分条件は、次のいずれかが成立する事である。

- i) $m \geq 2$ ii) $m \geq 3$
- iii) $m = n = 0$ かつ $j_E \equiv 7, 14, 21 \pmod{25}$
- iv) $5 \mid m < 0$ かつ $5^{-m} j_E \equiv \pm 1, \pm 7 \pmod{25}$

以下、定理の証明は §2 で、系の証明は §3 で行う。

記号 K は k の代数閉包、ガロワ拡大 F/k に対し $G(F/k)$ でそのガロワ群をあらわす。 $\mathbb{F}_2$, $GL_2(\mathbb{F}_2)$ はそれぞれ位数 2 の有限体と $\mathbb{F}_2$ 上の $(2,2)$ 型行列群をあらわす。 $GL_2^+(\mathbb{F}_2)$, $SL_2(\mathbb{F}_2)$ はそれぞれ 行列式 $\in \mathbb{F}_2^\times$, 行列式 = 1 なる元全体のなす $GL_2(\mathbb{F}_2)$ の部分群とする。自然数 n に対し、 S_n は n 次対称群とする。

§1 L/k の部分体

$E[L]$ は $G(K/k)$ の作用で固定されるから、 L/k はガロワ拡大で $G(L/k)$ の $E[L]$ への作用の表現

$$\rho: G(L/k) \longrightarrow \text{Aut}(E[L])$$

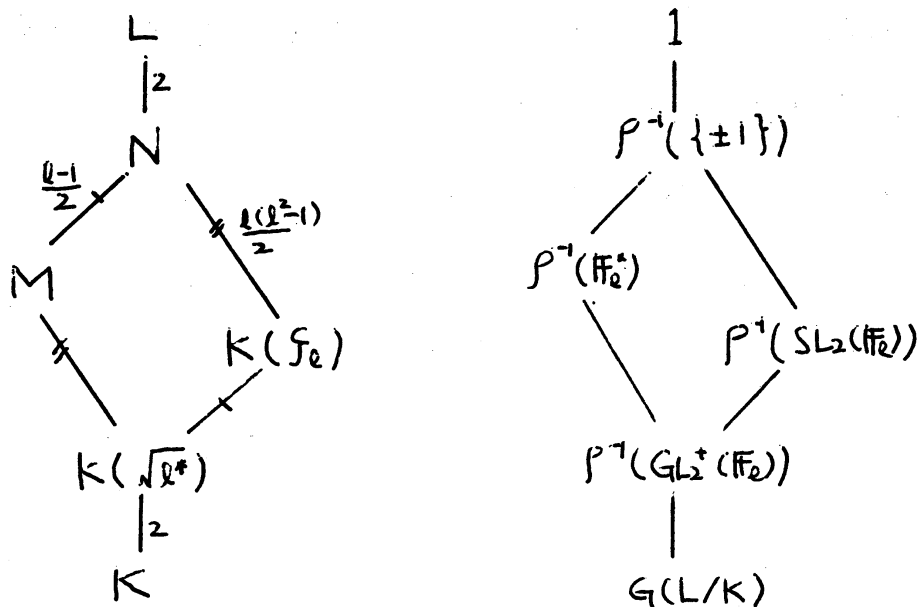
が得られる。 ρ は単射である。 $E[L]$ は加群として $\mathbb{F}_2 \oplus \mathbb{F}_2$ に同型であり、その $\mathbb{F}_2$ -basis を定めることにより $\text{Aut}(E[L])$ と $GL_2(\mathbb{F}_2)$ を同一視する。 M, N をそれぞれ $G(L/k)$ の部分群 $\rho^{-1}(\mathbb{F}_2)$, $\rho^{-1}(\{ \pm 1 \})$ に対応する L/k の部分体とする。 $\mathbb{F}_2$ は $GL_2(\mathbb{F}_2)$ の center だから、 $M/k, N/k$ はガロワ拡大である。次の事実が知られている。(cf. [2] "Weil-pairing.")

i) L は 1 の 2 乗根 ζ_2 を含む

ii) $\forall \sigma \in G(L/k)$ に対し、 $\zeta_2^\sigma = \zeta_2^{\det \rho(\sigma)}$

よって、 L/k の部分体と $G(L/k)$ の部分群の間に次の対応が

つく。(指数は $\ell \neq 2$ かつ P が全射のとき)



ここに、 $\ell^* = (-1)^{\frac{\ell-1}{2}} \ell$ (ただし、 $\ell = 2$ のとき $\ell^* = 1$)。

$G(M/K)$ の置換表現 $E[\ell]$ には $\ell+1$ 個の位数 ℓ の部分群

$$B = \{ B_1, \dots, B_{\ell+1} \}$$

が含まれており、 $G(L/K)$ が B に作用するが、この作用は P を通して $\text{Aut}(E[\ell]) = GL_2(\mathbb{F}_\ell)$ の B への作用に拡張される。

$GL_2(\mathbb{F}_\ell)$ の B への作用の表現を

$$\varphi: GL_2(\mathbb{F}_\ell) \longrightarrow \text{Aut}(B) \cong S_{\ell+1}$$

とおくと、 $\ker \varphi = \mathbb{F}_\ell^\times$ で、 P, φ から 単射準同型

$$G(M/K) \xhookrightarrow{P} PGL_2(\mathbb{F}_\ell) \xhookrightarrow{\varphi} S_{\ell+1}$$

が induce される。 $\ell = 2, 3$ を除けば、 φ は全射でない。 $\ell = 5$ のとき、 $PGL_2(\mathbb{F}_5) \cong S_5$ が群論の一般論から知られているので、 M/K は高々 S_5 -拡大である。

命題 1 $j_E \neq 0$, 1728 とする。 K' を K の部分体、 E' を K' 上の楕円曲線とし、 E から M, N を定義したのと同様に E' に対し M', N' を定義する。このとき

$$j_E = j_{E'} \Rightarrow M = KM', N = KN'$$

証明は、 $j_E = j_{E'}$ から E と E' が K 上同型なる事と、 $j_E \neq 0$, 1728 から $\text{Aut}(E), \text{Aut}(E') = \{\pm 1\}$ なる事から容易に従う。

§2 定理の証明

以下 $\ell = 5$, $j_E \neq 0$, 1728 とする。 M の定義方程式が定理の方程式なる事を示せばよい。命題 1 により定理の証明のためには、 K, E を次の形

$$K = \mathbb{Q}(C) \quad (C \neq 0, 1)$$

$$E = E_C: y^2 = x^3 - 3Cx - 2C \quad (C = j_E / (j_E - 1728))$$

に制限して十分である。次の補題が基本的である。

補題 Λ を index の集合の集合の集合

$$\Lambda = \left\{ \{i, j\}, \{k, l\}, \{m, n\} \mid \{i, j, k, l, m, n\} = \{1, 2, \dots, 6\} \right\}$$

とおく。 $|\Lambda| = 15$ で、 S_6 を Λ に対し自然に作用させる。このとき、 §1 の γ を通して得られる $\text{PG}_2(\mathbb{F}_5)$ の Λ への作用に關し、次が成立する。

1) Λ の推移域分解は

$$\Lambda = \Lambda_1 \cup \Lambda_2 \quad ; \quad |\Lambda_1| = 5, \quad |\Lambda_2| = 10$$

$$\Lambda_1 = \{ \{i, j\}, \{k, l\}, \{m, n\} \in \Lambda \mid (i, j)(k, l)(m, n) \notin \mathcal{P}(\mathrm{PGL}_2(\mathbb{F}_5)) \}$$

2) $\mathrm{PGL}_2(\mathbb{F}_5)$ の Λ_1 への作用は faithful すなわち,

$$\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathrm{Aut} \Lambda_1 \cong S_5$$

証明 補題の証明は計算機で行われた。■

今、各 $i = 1, \dots, 6$ に対し、

$$w_i \stackrel{\text{def}}{=} \frac{1}{4} \sum_{0 \neq p \in B_i} x(p) \quad (x(p) \text{ は } p \text{ の } x \text{ 座標})$$

各 $\lambda = \{ \{i, j\}, \{k, l\}, \{m, n\} \} \in \Lambda$ に対し、

$$u_\lambda \stackrel{\text{def}}{=} w_i w_j + w_k w_l + w_m w_n$$

と定める。明らかに $w_i \in M$ で $\sigma \in G(L/k)$ に対し $\sigma(B_i)$

$= \sigma(B_j)$ ならば $\sigma(w_i) = w_j$, $(\varphi \circ \rho(\sigma))(i) = j$ である。

よって補題の 1) により

$$h(x) \stackrel{\text{def}}{=} \prod_{\lambda \in \Lambda_1} (x - u_\lambda)$$

は k -係数 5 次多項式で、補題の 2) により $u_\lambda, \lambda \in \Lambda_1$

が互いに異なる限りとあって、 $h(x)$ は M を定義する多項式

である。ところで、 C を不定元にとれば、15 次多項式 $H(x)$

$\stackrel{\text{def}}{=} \prod_{\lambda \in \Lambda} (x - u_\lambda)$ は次節にのべる方法により、 X と C の $\mathbb{Q}$

-係数多項式として実際に具体的に計算される。そこで、 $H(x)$

が具体的にわか、たものとして、話を進める。 $H(x)$ は実際には、5次と10次の多項式に $\mathbb{Q}(c)[x]$ で因数分解され、それらは C が不定元なる限り $\mathbb{Q}(c)$ 上既約である。5次の成分の x を仮に (x と c の多項式である意味も含めて) $h_1(x, c)$ とかけば、 C が $\mathbb{Q}$ 上超越的ならば明らかに $h_1(c, x)$ は $h(x)$ と一致する。又、 C が $\mathbb{Q}$ 上代数的であ、ても、 C に収束する $\mathbb{C}$ - $\overline{\mathbb{Q}}$ ($\mathbb{C}$ は複素数体) の数列 $\{c_n\}$ をとると、 E_{c_n} に対し定義される $h(x)$ ($= h_1(c_n, x)$) が $E_{\mathbb{C}}$ に対し定義される $h(x)$ に (係数ごと) 収束するのは明らかなので、この場合 $h(x) = h_1(c, x)$ を得る。適当な x の $\mathbb{Q}(c)$ 上の一次分数変換により、 $h_1(c, x)$ は定理の方程式に変形される。又、定理の方程式の判別式は (すべての $\lambda \neq 0, 1/2$ に対し) 0 でない事も容易に確かめられるから、 $u_\lambda; \lambda \in \mathbb{A}^1$ は互いに異なる。よ、て定理の方程式の k 上の分解体は M である。■

$H(x)$ の計算 計算結果は繁雑なので、ここでは計算手順のみを述べる。実行は計算機による数式処理で行われた。計算は次の3段階に分けられる。1) "5等分多項式" の計算 2) $g(x) \stackrel{\text{def}}{=} \prod_{i=1}^6 (x - \omega_i)$ の計算 3) $H(x)$ の計算

1) "5等分多項式" $P, Q \in E$ に対し、 $x(p) = x(q)$

$\Leftrightarrow P = \pm Q$ だから

$$f(x) \triangleq \prod (X - x) ; x \in \{x(p) ; 0 \neq p \in E[5]\}$$

は K -係数 12 次の多項式で、その分解体は N である。これを 5 等分多項式と呼ぶ。E の加法公式から、 $P = (x, y) \in E$ に対し

$$x(2p) = \frac{x^4 + 6Cx^2 + 16Cx + 9}{4y^2} \quad \rightarrow -32C^2 + 27C^3$$

$$x(3p) = x - \frac{8y^2(x^6 - 15Cx^4 - 40Cx^3 - 45C^2x^2 - 24C^2x)}{(3x^4 - 18Cx^2 - 24Cx - 9C^2)^2}$$

である。 $x(2p) = x(3p)$ ($\Leftrightarrow p \in E[5]$) において、 y^2 に $x^3 - 3Cx - 2C$ を代入すれば $f(x)$ を得る。

2) $g(x)$ の計算 $1 \leq i \leq 6$, $0 \neq p \in B_i$ に対し、

$$w_i = \frac{1}{2} (x(p) + x(2p)) = a(x(p)) / b(x(p))$$

$$\text{すなわち、} a(x) = 5x^4 - 6Cx^2 + 8Cx + 9C^2$$

$$b(x) = 8(x^3 - 3Cx - 2C)$$

となる事が容易に確かめられる。 $b(x) = 0$ の根は E の 2 等分点の x 座標であるから、 $b(x)$ と $f(x)$ は $K[X]$ で互いに素である。従って互除法を用いて、 $b(x)t(x) \equiv 1 \pmod{f(x)}$ なる $t(x) \in K[X]$ が求まる。 $w(x) = a(x)t(x)$ において、 $m = 1, \dots, 6$ に対し、 $w(x)^m$ を $f(x) = 0$ で環元する事により、 $w_m(x) \equiv w(x)^m \pmod{f(x)}$, $\deg w_m(x) \leq 11$ なる $w_m(x) \in K[X]$ が求まる。しからば $1 \leq i \leq 6$, $0 \neq p \in B_i$ に対し、

$$w_i^m = w_m(x(p))$$

である。今、任意の多項式 $F(x) \in K[X]$ と $m \in \mathbb{Z}$ に対し、

$$[m]_F \stackrel{\text{def}}{=} \sum_{F(x)=0} x^m$$

と定める。Newton の公式を用いれば $g(x)$ を求めるためには、 $[m]_g$; $m=1, \dots, 6$ を $[]_F$ であらわす事を考えればよい。 $W_m(x) = \sum_{j=0}^6 a_j^{(m)} x^j$ とおけば

$$\begin{aligned} [m]_g &= \sum_{i=1}^6 w_i^m = \sum_{i=1}^6 \left(\frac{1}{4} \sum_{0 \neq p \in B_i} W_m(\lambda(p)) \right) \\ &= \frac{1}{2} \sum_{f(x)=0} W_m(x) = \frac{1}{2} \sum_{j=0}^6 a_j^{(m)} [j]_f \end{aligned}$$

$$\left(\begin{array}{l} \text{以上の方法により、} \\ g(x) = X^6 - C(15X^4 + 40X^3 + 45CX^2 + 24CX + 5C). \end{array} \right)$$

3) $H(x)$ の計算 常識的には $H(x)$ を $w_1, \dots, w_6, x$ の多項式に展開して x^m の係数を $w_1, \dots, w_6$ の基本対称式であらわす事をやればよいのだが、それでは計算があまりにどう大となるので 2) と同様 $[]_H$ を $[]_f$ であらわす事を考える。そのためには、更に次の公式が必要である。

$$\left(\begin{array}{l} \text{(公式) 多項式 } F(x) = \prod_{i=1}^n (x - \lambda_i) \text{ に対し、 } [\dots]_F \text{ を} \\ \text{漸化式 } [k_1, \dots, k_d, k]_F \stackrel{\text{def}}{=} [k_1, \dots, k_d]_F [k]_F \\ \quad - \sum_{i=1}^n [k_1, \dots, k_{i-1}, k_i + k, k_{i+1}, \dots, k_d]_F \\ \text{により定める。このとき } 1 \leq d \leq n \text{ に対し} \\ \sum_{\sigma \in S_n} \lambda_{\sigma(1)}^{k_1} \cdots \lambda_{\sigma(d)}^{k_d} = (n-d)! [k_1, \dots, k_n]_F \end{array} \right)$$

証明は帰納法によれば容易なので省略する。公式を用いて $[m]_H$ は次の様に計算される。

$$[m]_H = \sum_{\lambda \in A} u_\lambda^m = \frac{15}{15 \cdot 6!} \sum_{\sigma \in S_6} (w_{\sigma(1)} w_{\sigma(2)} + w_{\sigma(3)} w_{\sigma(4)} + w_{\sigma(5)} w_{\sigma(6)})^m$$

$$= \frac{1}{48} \sum_{\substack{p+q+r=m \\ p,q,r \geq 0}} \frac{m!}{p!q!r!} \sum_{\sigma} w_{\sigma(1)}^p w_{\sigma(2)}^p w_{\sigma(3)}^q w_{\sigma(4)}^q w_{\sigma(5)}^r w_{\sigma(6)}^r$$

$$= \frac{m!}{24} \sum_{p,q,r} \frac{g(0)^r}{p!q!r!} [p-r, p-r, q-r, q-r]_g$$

$[p-r, p-r, q-r, q-r]_g$ は $[p-r]_g, [2q-2r]_g$ 等々であら
わされ、 $[m]_H$ を $[]_g$ として計算する事ができる。

§3 系の証明

次の4つの場合: 1) $m > 0$, 2) $n > 0$, 3) $m = n = 0$, 4)
 $m = n < 0$ に分けて、下の命題2を $p=5$, $k=\mathbb{Q}_5$, $F(x)$
 $= X^5 + 5X^4 + 40X^3 - d$ において適用すれば容易に証明され
る。■

命題2 $p \in$ 素数, k を p -進体 $\mathbb{Q}_p$ の有限次拡大体, v を
 k の指数付値で $v(k^\times) = \mathbb{Z}$ とする。 $F(x) \in k$ -係数, p -次
, monic なる多項式でその判別式 $\text{disc } F \neq 0$ とする。 Ω を
 $F(x)$ の k 上の分解体とするとき、下の手順 (0) ~ (3) を有
限回ループする事により

(*) Ω/k は wildly ramify

になるか否かを判別できる。

(0) a_i ($i=1, \dots, p$) を $F(x)$ の X^{p-i} の係数, $N =$
 $v(a_p)$ と定める。

(1) $1 \leq i \leq p-1$ かつ $v(a_i) \leq \frac{i}{p}n$ ならば(*)でない。

その他の場合,

(2) $p + N$ ならば (*) である。

その他の場合,

(3) $v(x^p + a_p) > N$ なる $x \in k$ がとれ、 $F(x)$ を $F(x+x)$ に置きかえて (1) へ戻る。

証明 π を k の素元、また v は Ω 上まで拡張しておく。まず手順の各段階の正当性を示す。

(1) の正当性: (*) であるとする ($1 \leq i \leq p-1, v(a_i) > \frac{i}{p}N$ を示す)。 $F(x)$ は k 上既約となり、 $F(x)$ の任意の根 α に対し $v(\alpha) = \frac{N}{p}$ 。故に $1 \leq i \leq p, v(a_i) \geq \frac{i}{p}N$ 。よって $p + N$ ならば $1 \leq i \leq p-1, v(a_i) > \frac{i}{p}N$ 。 $p \nmid N$ とする。 $G(x) = F(\pi^{\frac{N}{p}}x) / \pi^N$ は整係数, monic でその根 β は Ω の整数。 $k(\beta)/k$ は totally ramify される residue class degree は 1。よって k の整数 r が存在して $v(\beta-r) > 0$ 共役をとれば $G(x)$ の他の根 β' に対しても $v(\beta'-r) > 0$ となる。よって $G(x) \equiv x^p - r^p \pmod{\pi}$ すなわち $1 \leq i \leq p-1, v(a_i) > \frac{i}{p}N$ である。

(2) の正当性: $v(a_i) > \frac{i}{p}N$ ($i=1, \dots, p-1$), $p+n$ とし (*) を示す。 $F(x)$ の Newton polygon をみれば $F(x)$ は k 上既約がわかり、 $F(x)$ の根 α に対し $v(\alpha) = \frac{N}{p}$ 。よって (*) である。

(3)の正当性: $p \nmid N$ なるとき $v(x^p + a_p) > N$ なる $x \in k$ は $y^p \equiv a_p / \pi^N$ なる y をとって $x = \pi^{\frac{N}{p}} y$ とおけばとれる。

(0)~(3) のループが有限回で止まることの証明: (3)の時点 k において考えると, $p \nmid N$ で, $1 \leq i \leq p-1$ に対し, $v(a_i) > \frac{i}{p} N$ である。よって $G(X) = F(\pi^{\frac{N}{p}} X) / \pi^N$ は整係数, monic で, $0 \leq v(\text{disc } G) = v(\text{disc } F) - N(p-1)$ すなわち, $N \leq v(\text{disc } F) / (p-1) (< \infty)$ 。一方, $v(x^p + a_p) > N$ より $v(F(x)) > N$ となり, 次回のループにおいて N は増大している。 $v(\text{disc } F)$ はループを重ねる度に不変であるから, ループは有限回で止まらねばならない。 ■

文献

- [1] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math. 15 (1972), 259-331
- [2] J. H. Silverman "The Arithmetic of elliptic curves," Graduate texts in mathematics 106, Springer-Verlag