数理解析研究所講究録
971巻 1996年 153-159

楕円曲線の3等分点の生成する局所体

香川大学 教育学部 数学教室 内藤 浩忠 (Hirotada NAITO)

§1 動機と記号

Eを有理数体 $\mathbf{Q}$ 上定義された楕円曲線とする。lを素数とするとき、E_lで Eの l等分点全体のなす集合を表す。それらの座標が生成する拡大体を $K_{(l)}=\mathbf{Q}(E_l)$ と書く。その $\mathbf{Q}$ 上の Galois 群を $G_{(l)}=Gal(K_{(l)}/\mathbf{Q})$ と書くと $E_l\cong\mathbf{F}_l\oplus\mathbf{F}_l$なので $G_{(l)}$は $GL_2(\mathbf{F}_l)$ の部分群になる。ここで $\mathbf{F}_l$は元の個数が l個の有限体を表し、GL_2は一般線型群を、SL_2は特殊線型群を表す。

ζ_lを 1 の原始 l乗根とすると 、$\zeta_l\in K_{(l)}$となり Galois 群の作用は $\zeta_l^{\sigma}=\zeta_l^{\det(\sigma)}$となることが知られている。したがって $G_{(l)}\cap SL_2(\mathbf{F}_l)$−固定体は $\mathbf{Q}(\zeta_l)$ となる。generic には $G_{(l)}=GL_2(\mathbf{F}_l)$ となる。

ここで $L(s,E/\mathbf{Q})=\sum_{n=1}^{\infty}a_nn^{-s}$を $E/\mathbf{Q}$ の Hasse-Weil zeta 関数とすると、この関数は等分点の体における素数の分解法則をわりあいよく記述する。このようなことは Shimura[7] で指摘されている。

$l=2$ の場合には、$GL_2(\mathbf{F}_2)\cong S_3$となる。ここで S_3は 3 次対称群である。ρを S_3の 2 次の既約表現として、$K_{(2)}/\mathbf{Q}$ のρに付随する Artin L 関数を $L(s,\rho)=\sum_{n=1}^{\infty}b_nn^{-s}$と書くと次の定理が成り立つ。

定理 (Koike [3])

good prime $p\neq 2$ に対して、$a_p\equiv b_p\ mod\ 2$ が成り立つ。

この定理は $K_{(2)}/\mathbf{Q}$ における素数の分解法則を記述している。一方、谷山−志村 予想によれば $L(s,E/\mathbf{Q})$ は適当な Nに対して重さ 2 の合同部分群$\Gamma_0(N)$ に関する尖点形式の L 関数に一致し、Deligne-Serre [1] の結果によれば $L(s,\rho)$ は適当な Mに対して重さ 1 の $\Gamma_1(M)$ に関する尖点形式の L 関数に一致する。a_nや b_nはそれらの尖点形式の Fourier 係数に一致するのでこの定理は 2 つの尖点形式に関する合同式と見ることもできる。

逆に $K/\mathbf{Q}$ を S_3-拡大とすると、Kはある 3 次方程式 $f(x)=0$ の分解体になる。このとき $E:y^2=f(x)$ とすると Eは楕円曲線になり、$K=\mathbf{Q}(E_2)$ となる。したがって上の定理は S_3- 拡大における分解法則を記述していることになる。

$l=3$ の場合には、次のような結果がある。ρを $GL_2(\mathbf{F}_3)$ の 2 次の既約表現として、$K_{(3)}/\mathbf{Q}$ のρに付随する Artin L 関数を $L(s,\rho)=\sum_{n=1}^{\infty}b_n n^{-s}$と書く。

定理 (Naito [5])
good prime $p\neq 3$ に対して、$a_p\equiv b_p \ mod\ \mathcal{P}_3$が成り立つ。
ここで $\mathcal{P}_3$は $\mathbf{Q}(\sqrt{-2})$ の 3 の上にある素イデアルである。

$GL_2(\mathbf{F}_3)$ の 2 次の既約表現は 2 つあるがそれらは互いに複素共役になっている。3 の上の素イデアルも 2 つあるので、それらが 1 つづつ対応しているわけである。

しかし、$l=2$のときのような意味での逆がわからないので次のような問題を設定する。

問題 (G)
$K=\mathbf{Q}(E_3)$ となるような楕円曲線 $E/\mathbf{Q}$ が存在するような $GL_2(\mathbf{F}_3)$-拡大 $K/\mathbf{Q}$ を特徴づけよ。

まず、$K_{(3)}=\mathbf{Q}(E_3)$ で $Gal(K_{(3)}/\mathbf{Q})\cong GL_2(\mathbf{F}_3)$ となるときの中間体の様子を考察する。ここで楕円曲線 Eは方程式 $dy^2=4x^3-g_2x-g_3$で定義されているものとする。(ここで d,g_2,g_3は有理数。) $\Delta=g_2^3-27g_3^2$とおく。$M_{(3)}=\mathbf{Q}(E_3(x))$ とする。ここで $E_3(x)$ は E_3の x-座標を表す。このとき $M_{(3)}$は dに依らない。しかも $Gal(M_{(3)}/\mathbf{Q})\cong S_4$となる。ここで S_4は 4 次対称群で $PGL_2(\mathbf{F}_3)$ に同型である。実は、$M_{(3)}\supset\mathbf{Q}(\zeta_3,\Delta^{1/3})$ となっている。したがって問題の Kは $\mathbf{Q}(\zeta_3,\Delta^{1/3})$ という形の中間体を含まなくてはならない。しかし、それ以上のことは筆者は知らない。

§2 局所的なデータ

前のセクションで設定した問題を局所的に考える。すなわち $\mathbf{Q}$ のかわりの p-進体 $\mathbf{Q}_p$ 上で考える。

問題 (l)
$GL_2(\mathbf{F}_3)\supset G_p$を部分群とする。このとき $Gal(K_p/\mathbf{Q}_p)\cong G_p$なる拡大体 $K_p/\mathbf{Q}_p$に対して $K_p=\mathbf{Q}_p(E_3)$ となるような楕円曲線 $E/\mathbf{Q}_p$が存在するか？

これを次のような手順で考えていく。

*Step*1.
$GL_2(\mathbf{F}_3)$ の部分群 $G=G_p$を全て決める。

*Step*2.
$G_p\cap SL_2(\mathbf{F}_3)$ による固定体が $\mathbf{Q}_p(\zeta_3)$ となるような $\mathbf{Q}_p$上の G_p-拡大体 K_pを全て決める。このような K_pは有限個しかないので原理的には決定できる。

*Step*3.
上で決めた K_pに対して $K_p=\mathbf{Q}_p(E_3)$ となるような楕円曲線 Eを探す。

これを実行するには Serre-Tate[6] の結果と、次の 2 つの事実が有用である。

- $G_p \subset SL_2(\mathbf{F}_3) \iff \mathbf{Q}_p \ni \zeta_3 \iff p \equiv 1 \ mod\ 3$
- $\Delta^{1/3} \in \mathbf{Q}_p \iff 3 \nmid \sharp|G_p|$

*Step*1.の結果は次のとおりである。ここで C_n は位数 n の巡回群を表す。

(1). $G = GL_2(\mathbf{F}_3)$
これは $p = 2$ の場合しか起こらない。

(2). $G = SL_2(\mathbf{F}_3)$
これは楕円曲線の 3 等分点では生成されない。

(3). $G = B = \{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in GL_2(\mathbf{F}_3)\}$
$p \equiv 2 mod 3$ または $p = 3$ の場合しか起こらない。

(4-1). $G \cong S_3 = \{\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{F}_3)\}$ or $\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in GL_2(\mathbf{F}_3)\}$
$p \equiv 2 mod 3, p = 3$ の場合しか起こらない。

(4-2). $G \cong C_6 = \langle\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}\rangle$
$p \equiv 1 mod 3$ の場合しか起こらない。

(5). $G \cong C_3 = \langle\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle$
$p \equiv 1 mod 3$ の場合しか起こらない。

(6). $G \cong SD_{16} = \langle a = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}\rangle$
$a^8 = b^2 = 1, b^{-1}ab = a^3$
$p = 2$ しか起こらない。

(7-1). $G \cong C_8 = \langle\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\rangle$
$p \equiv 2 mod 3$ の場合しか起こらない。

(7-2). $G \cong D_8 = \langle a = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, b = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}\rangle$
$a^4 = b^2 = 1, b^{-1}ab = a^{-1}$
$p \equiv 2 mod 3$ の場合しか起こらない。
しかも $p \equiv 3 mod 4$ または $p = 2$ でなければならない。

(7-3). $G \cong Q_8 = SD_{16} \cap SL_2(\mathbf{F}_3) = \langle\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\rangle$
$p \equiv 1 mod 3$ の場合しか起こらない。
しかも $p \equiv 3 mod 4$ でなければならない。

(8-1). $G \cong C_4 = \langle \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \rangle$

$p \equiv 1 mod 3$ の場合しか起こらない。

(8-2). $G \cong V_4 (\cong C_2 \oplus C_2 = \langle \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$

$p \equiv 2 mod 3 (p \neq 2)$ または $p = 3$ のときしか起こらない。

(9). $G \cong C_2 = \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ or $\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$

(10). $G = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \}$

$p \equiv 1 mod 3$ の場合しか起こらない。

次に、*Step.2* を実行するわけだが、その前に次の用語を導入しておく。

定義 $\{G_p, I_p, V_p\}$ が、ramification triple of $GL_2(\mathbf{F}_3)$ とは、

1. $G_p \subset GL_2(\mathbf{F}_3)$,
2. $G_p \rhd I_p$ かつ G_p/I_pは巡回群、
3. $G_p \rhd V_p$ かつ I_p/V_pは巡回群で、 $\sharp|I_p/V_p|$ は $p^{\sharp|I_p/V_p|} - 1$ を割り、
4. V_p は p-群である。

$G_p = Gal(K_p/\mathbf{Q}_p) \subset GL_2(\mathbf{F}_3)$ のとき、I_pを惰性群、V_pを高次分岐群とすれば、$\{G_p, I_p, V_p\}$ は、ramification triple of $GL_2(\mathbf{F}_3)$ となる。

$p \neq 2, 3$ のときは、$V_p = \{1\}$ なので *Step.2* は易しくなっている。*Step.2* の結果は省略させていただく。((7-2) については Naito[4]、(7-3) については Fujisaki[2] 参照。)

最後に *Step.3* を実行する。*Step.2* で得られた各 K_pに対して、楕円曲線 Eを探す。そのためには具体的に 3 等分点の方程式を書き下す。それは次のとおりである。

楕円曲線を $E : dy^2 = 4x^3 - g_2x - g_3$ とすると、3 等分点の x−座標の方程式は

$f(x) = x^4 - \frac{g_2}{2}x^2 - g_3x - \frac{{g_2}^2}{48}$

$= (x^2 - \sqrt{\frac{g_2 - \Delta^{1/3}}{3}}x - \frac{2\Delta^{1/3} + g_2}{12} - \frac{g_3}{2\sqrt{\frac{g_2 - \Delta^{1/3}}{3}}})$

$\times (x^2 + \sqrt{\frac{g_2 - \Delta^{1/3}}{3}}x - \frac{2\Delta^{1/3} + g_2}{12} + \frac{g_3}{2\sqrt{\frac{g_2 - \Delta^{1/3}}{3}}})$

で与えられる。ここで$\Delta = {g_2}^3 - 27{g_3}^2$とする。

結果としては、$p \neq 2$ のときは *Step.2* で求めた全ての K_pに対して $K_p = \mathbf{Q}_p(E_3)$ となるような楕円曲線 Eが見つかった。しかし $p = 2$ のときにはそうはいかなかった。

方法は、まず K_pの部分体で3等分点の x-座標で生成されるべき中間体に対して、それが上の方程式 $f(x)=0$ の分解体となるように、g_2, g_3を p 巾に関する合同条件で求める。x-座標の体は d に依らないことが有効である。その中間体を K_pまで延ばすときに d をうまく取り直すわけである。

$G_p = C_8$のときを例にとって説明する。4次体が共通な2つの C_8-拡大体を合成するとその Galois 群は $C_8 \times C_2$に同型になり、それは2つの C_8-拡大体を含む。同時に3つの2次拡大体を含むわけだが、それらを $\mathbf{Q}_p(\zeta_3) = \mathbf{Q}_p(\sqrt{-3}), \mathbf{Q}_p(\sqrt{d}), \mathbf{Q}_p(\sqrt{-3d})$ とするとき、この d を使って楕円曲線を取り直せばもう一方の C_4-拡大体が作られる。

$\mathbf{Q}_p(\zeta_3)$ を含む C_4-拡大は $p \equiv 3 \ mod\ 4$ のときは1個、その他のときは2個ある。それぞれは C_8-拡大に、pが奇素数のときは2個ずつ、$p=2$のときは4個ずつ延長できる。したがって $\mathbf{Q}_p(\zeta_3)$ を含む C_4-拡大が楕円曲線の3等分点の x-座標で生成されることを示せば、あとは d を適当に見つけることにより C_8-拡大体が楕円曲線の3等分点で生成されることがわかる。

$p=2$ の場合について結果を述べる。

•$G_2 = GL_2(\mathbf{F}_3)$ のとき。

まず、S_4-拡大体を考える。[8] によれば、$\mathbf{Q}_2$上の S_4-拡大体は3つあり、explicit に与えている。そのうちの1つは $GL_2(\mathbf{F}_3)$-拡大に延びない。残りの2つは4つづつ $GL_2(\mathbf{F}_3)$-拡大に延びる。これらはいずれも楕円曲線の3-等分点により生成されていることがわかった。

•$G_2 = SD_{16}$のとき。

$\mathbf{Q}_2$上の SD_{16}-拡大体は、、$\mathbf{Q}_2(\sqrt{-1})$ 上の8次巡回拡大となるものが4つあり、$\mathbf{Q}_2(\sqrt{-5})$ 上の8次巡回拡大となるものが4つある。いずれも $\mathbf{Q}_2$上の D_8-拡大体の2次拡大として得られる。($\mathbf{Q}_2$上の D_8-拡大体は [4] で決定済み。) 1つの D_8-拡大体から2つづつの SD_{16}-拡大体に延びる。

このうち $\mathbf{Q}_2(\sqrt{2+\sqrt{-1}}, \sqrt{5}) = \mathbf{Q}_2(\sqrt{2+\sqrt{-3}}, \sqrt{-1})$ という D_8-拡大体は楕円曲線の3等分点の x-座標からは来ないことが、計算によりわかった。その他の SD_{16}-拡大体は楕円曲線の3等分点から生成されることもわかった。したがって $\mathbf{Q}_2(\sqrt{-5})$ 上の8次巡回拡大となるような SD_{16}-拡大体のうち半分が楕円曲線の3等分点から生成されるわけである。

その他の場合にはすべて $K_2 = \mathbf{Q}_2(E_3)$ となる楕円曲線 Eが見つかった。

§3 応用

定理

Sを素数からなる有限集合とし、$S \ni p$ に対して $\{G_p, I_p, V_p\}$ を ramification triple of $GL_2(\mathbf{F}_3)$ で、

$$\begin{cases} G_p \subset SL_2(\mathbf{F}_3) & p \equiv 1 \ mod\ 3, \\ G_p \not\subset SL_2(\mathbf{F}_3) & \text{その他} \end{cases}$$

となるものを与えておく。

このとき次のような $\mathbf{Q}$ 上の Galois 拡大体 Kが無限個存在する。

1. $Gal(K/\mathbf{Q}) \cong GL_2(\mathbf{F}_3)$,
2. $K \ni \zeta_3$ かつ $\zeta_3^{\sigma} = \zeta_3^{det\sigma}, (\sigma \in Gal(K/\mathbf{Q}))$,
3. $S \ni p$ に対して $K/\mathbf{Q}$ の分解群が G_pで、惰性群が I_pで高次分岐群が V_pにそれぞれ共役になる。

証明の概略。

§2 において、楕円曲線 Eは p 巾を法とする合同条件で取っていたので、$p \in S$に対しては 3 番目の性質は満たすようにできる。$p = 2$ のときは楕円曲線が見つからない SD_{16}-拡大体があるが、$\mathbf{Q}_2(\sqrt{-5})$ 上 8 次巡回拡大になる SD_{16}-拡大体は全て G_p, I_p, V_pが一致するので、この条件を満たすように作ることができる。

$S \not\ni q_1, q_2$という素数に対して $G_{q_1} = C_8, G_{q_2} = B$としておけば、これらを含む $GL_2(\mathbf{F}_3)$ の部分群は全体しかないので 1 番目の性質が言える。

2 番目の性質は、楕円曲線の等分点の性質から明らかである。

無限個存在することは次のようにすれば言える。もしこのような拡大体が有限個しかないとする。それらを $K_1, \cdots, K_t$とする。p_iを $K_i/\mathbf{Q}$で完全分解する素数とする。このとき新たな Sとして $p_1, \cdots, p_t$を含むように取り、$G_{p_i} \neq \{1\}$ としておいて、上のような拡大体 $K/\mathbf{Q}$を構成すればこれは $K_1, \cdots, K_t$のいずれとも異なる。したがって無限個存在する。

数値例

Kを、方程式 $x^4 - 6x^2 - 312x + 477 = 0$ の $\mathbf{Q}$ 上の分解体とする。この方程式の判別式は $D = -2^{18} \cdot 3^5 \cdot 5^2 \cdot 13^2$となる。$K \supset \mathbf{Q}(\zeta_3, \sqrt[3]{5})$ を満たし、$Gal(K/\mathbf{Q}) \cong S_4$となるが、$K \otimes_{\mathbf{Q}} \mathbf{Q}_2 = \mathbf{Q}_2(\sqrt{2+\sqrt{-3}}, \sqrt{-1})$ なので、§2 のデータより楕円曲線の 3 等分点の x-座標からは生成されない。

したがって $\mathbf{Q}(\zeta_3, \sqrt[3]{m})$ という形の中間体を含むという条件だけでは、楕円曲線の 3 等分点から生成されるということは言えない。あとどのような条件を付け加えればよいのかが今後の課題である。

参考文献

[1] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup. (4), **7** (1974), 507-530.

[2] G. Fujisaki, *A remark on quaternion extensions of the rational p-adic field*, Proc. Japan Acad., **66** (1990), 257-259.

[3] M. Koike, *Higher reciprocity law, modular forms of weight 1 and elliptic curves*, Nagoya Math. J., **98** (1985), 109-115.

[4] H. Naito, *Dihedral extensions of degree* 8 *over the rational p-adic fields*, Proc. Japan Acad., **71** (1995), 17-18.

[5] H. Naito, *A congruence between the coefficients of the L-series which are related to an elliptic curve and the algebraic number field generated by its 3-division points*, Mem. Fac. Edu. Kagawa Univ., **37** (1987), 43-45.

[6] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492-517.

[7] G. Shimura, *A reciprocity law in non-solvable extensions*, J. Reine Angew. Math., **221** (1966), 209-220.

[8] A. Weil, *Exercises dyadiques*, Invent.Math. **27** (1974), 1-22.