

志村の楕円曲線のある等分点が生ずる代数体

京大教養部 山内正敏

§ 1. 志村の楕円曲線

q を $q \equiv 1 \pmod{4}$ なる素数で, χ を導手 q の指標で位数 2 のもの, つまり $\chi(*) = \left(\frac{*}{q}\right)$, level q の合同部分群 $\Gamma_0(q)$ に関する, 重さ 2 の指標 χ に属する Nebentype の cusp forms の空間を $\mathcal{S}_{2,\chi} = \mathcal{S}_2(\Gamma_0(q), \chi)$ とします。今 $\mathcal{S}_{2,\chi}$ の元 $f(z) = 1 + \sum_{n=2}^{\infty} a_n e^{2\pi i n z}$ は, $\mathcal{S}_{2,\chi}$ に働く全てのヘッケ作用素 T_m, χ の同時固有函数であるとし, K を有理数体 $\mathbb{Q}$ 上フーリエ係数 a_n ($n=2,3,\dots$) が生成する有限次代数体とします。志村理論 [1. Chap. 7] によると, この $f(z)$ に対し $\mathbb{Q}$ 上定義されたアーベル多様体 $A = A_f$ を構成出来, この A は (i) $\dim A = [K:\mathbb{Q}]$ (ii) $\text{End}_{\mathbb{Q}}(A)$ は自然に K を含む, という性質をもちます。更に重要な事に, (iii) 実 2 次体 $k = \mathbb{Q}(\sqrt{q})$ 上定義された A の自己同型 μ が存在し, $\mu^2 = \text{id}$, $\mu^\varepsilon = -\mu$ ($\text{id} \neq \varepsilon \in \text{gal}(k/\mathbb{Q})$) が成立します。

この μ を使って $B = (1 + \mu)A$ という A のアーベル部分多様体を考えると B は $k = \mathbb{Q}(\sqrt{p})$ 上定義されていて,

$A \sim B \times B^E$ と k 上 isogenous の意味で分解されます。

B は更に k 上分解されて 1 次元の因子をもてば, その 1 次元因子の事を "志村の楕円曲線" と呼ぶことにします。特に

$\dim B = 1$ の時 B 自身が志村の楕円曲線となります。こ

うなるのは $q = 29, 37, 41$ の時に限ります。ここでは,

$q = 29, 37$ を扱います。以後 $\dim B = 1$ とします。

l を 1 つの素数とし, K_l (或いは K_{l^∞}) を B の位数 l (或いは 位数 l の) の点の座標を定義体 k に添加して出来る有限次 (或いは無限次) ガロワ拡大体とすると, $\text{End}_{\mathbb{Q}}(B) = \mathbb{Q}$ ということがわかっていきますから

$$R_\infty: \text{Gal}(K_{l^\infty}/k) \longrightarrow \text{GL}_2(\mathbb{Z}_l)$$

$$R_1: \text{Gal}(K_l/k) \longrightarrow \text{GL}_2(\mathbb{Z}/l\mathbb{Z})$$

なるガロワ群の表現 R_∞, R_1 が得られます。この時 R_∞, R_1 を

$$(*) \quad R_\infty(\sigma) \equiv R_1(\sigma') \pmod{l}, \quad (\sigma' \text{ は } \sigma \text{ の } K_l \text{ への制限})$$

となる様にとることが出来ますからその様にと、おきます。

l をある特殊な素数にした時の $\text{Gal}(K_l/k)$ を決め, K_l を explicit に書くことが目的です。

素数 p ($\neq l, q$) の上にある K_l の 1 つの素因子を $\mathfrak{p}$, $\mathfrak{p}$ の K_{l^∞} への延長の 1 つを $\mathfrak{P}$ とし, $\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{P}}$ を夫々のフロベ

ニウス自己同型とすると

$$(**) \quad \det(I_2 - X R_\infty(\sigma_p)) = \begin{cases} 1 - a_p X + p X^2 & , \chi(p)=1 \\ 1 - (a_p^2 + 2p) X + p^2 X^2 & , \chi(p)=-1 \end{cases}$$

となっています。[1. (7.6.15)] (＊), (＊＊) により K_L/k の素イデアル分解が $a_p \pmod{l}$ の値でわかるわけです。

§2. a_p に関する1つの合同式 (土井氏による。)

χ を今迄通りとし, $B_{n,\chi}$ を一般化されたベルヌイ数とします。つまり,

$$F_\chi(t) = \sum_{a=1}^q \frac{\chi(a)t \cdot e^{at}}{e^{qt}-1}$$

を母函数とし

$$F_\chi(t) = \sum_{n=1}^{\infty} B_{n,\chi} \cdot \frac{t^n}{n!}$$

で得られる数 $B_{n,\chi}$ です。この時, 一般に重さ w の Nebentypen type の cusp forms の空間 $\mathcal{S}_w(\Gamma_0(q), \chi)$ に働くハッケ作用素 $T_{p,\chi}$ と一般化されたベルヌイ数 $B_{w,\chi}$ との間になりたつ次の合同式を土井氏は証明しました。(未発表)

$$(\star) \quad \det(I + \chi(p)p^{w-1}I - T_{p,\chi}) \equiv 0 \pmod{l}.$$

(ここで l は有理数 $w^{-1} B_{w,\chi}$ の分子の奇素因子)

$\dim B = 1$ つまり $\dim \mathcal{S}_{2,\chi} = 2$ の時, ハッケ作用素 $T_{m,\chi}$ ($m=1, 2, \dots$) についての同時固有函数 $f(z) = 1 + \sum_{n=2}^{\infty} a_n e^{2\pi i n z}$ のフーリエ係数 a_p について土井氏の

合同式 (★) は

$$(\star\star) \begin{cases} 1+p-a_p \equiv 0 \pmod{l} & \text{if } \chi(p)=1 \\ (1-p)^2 - a_p^2 \equiv 0 \pmod{l} & \text{if } \chi(p)=-1 \end{cases}$$

ということを意味します。 $q=29, 37$ の時 $B_{2,\chi}$ は
夫々 $12, 20$ ですから 上の合同式 (★) の l として
夫々 $3, 5$ がとれます。 この l についての l 等分体の
体 K_l をきめるわけです。

§3 K_l の決定 ($q=29, 37$ の場合)

(★) の左辺は (**) の右辺に $\chi=1$ を代入したものです
から (*) を合わせて考えると、結局 K_l でのフロベニウス
自己同型 σ_p の R_1 による像 $R_1(\sigma_p)$ は $GL_2(\mathbb{Z}/l\mathbb{Z})$
の元として、いつも固有値 1 をもっています。こういう事から

$R_1(\text{Gal}(K_l/k))$ が決まります。更に K_l/k での分岐の状
態を調べる事により K_l を explicit に求める事が出来ます。
結局まとめると、

定理 $q=29, 37$ の時 l を夫々 $l=3, 5$ として、

$$(i) \quad \text{Gal}(K_l/k) \cong \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{Z}/l\mathbb{Z}) \mid \begin{matrix} b \in \mathbb{Z}/l\mathbb{Z} \\ d \in (\mathbb{Z}/l\mathbb{Z})^\times \end{matrix} \right\}$$

更に K_{l^∞} についていえば、

$$(i)' \quad \text{Gal}(K_{\ell^{\infty}}/k) \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{Z}_{\ell}) \mid \begin{array}{l} a-1 \in \ell\mathbb{Z}_{\ell} \\ c \in \ell\mathbb{Z}_{\ell} \\ b \in \mathbb{Z}_{\ell} \\ d \in \mathbb{Z}_{\ell}^{\times} \end{array} \right\}$$

$$(ii) \quad K_{\ell} = k(\zeta_{\ell}, \sqrt[\ell]{\varepsilon_q})$$

ここで ζ_{ℓ} は 1 の原始 ℓ 乗根, ε_q は $k = \mathbb{Q}(\sqrt{q})$ の基本単数。

(i), (ii) についての証明は [2] にあります。(i)' については、まず $\text{Gal}(K_{\ell^2}/k)$ を決めておいて、G. Shimura, A reciprocity law in non-solvable extensions, J. Reine Angew. Math., 221 (1966), 209-220. にある Lemma 5. を modify して得られます。

[注意]

(1). $B_{2,\chi} \equiv 0 \pmod{\ell}$ であると $k(\zeta_{\ell})$ の類数は ℓ で割れます。(斎藤氏に教えて頂いた。) 円分体の類数に関するクンマーのクライテリオンに相当する事実です。従って $k(\zeta_{\ell})$ の上に ℓ 次不分岐巡回拡大が存在します。 $q=29$ の時 K_{ℓ} が丁度それになっています。しかし $q=37$ のときはそうではありません。一般に $B_{2,\chi} \equiv 0 \pmod{5}$ ならば $k(\zeta_5, \sqrt[5]{\varepsilon_{5q}})/k(\zeta_5)$ が、5次不分岐巡回拡大である⁷⁾。ということがいえます。 $(\varepsilon_{5q}: \mathbb{Q}(\sqrt{5q}) \text{ の基本単数})$

(2) アーベル多様体の次元 > 1 の時、同様な等分点についての拡大体を調べようとする、2-等分点を考えるのが自然です。(1: a_n ($n=2, 3, \dots$) が生成する体のある素イデアル).
 すると、この時は 合同式 (※) では少し不十分で、もっと精密化する必要があります。($1+p-a_p \equiv 0 \pmod{1}$ という様な合同式の証明が必要) それらは 最近、太田氏と小池氏によって独立に証明が得られています。従って $q=67, 73$ 等の Neben type についての K_L の決定が 柴原氏によって得られています。

参考文献

- [1]. G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, No.11 Iwanami Shoten and Princeton University Press, 1971.
- [2]. M. Yamauchi, On the fields generated by certain points of finite order on Shimura's elliptic curves, J. Math. Kyoto Univ., 14(1974) 243-255.