

Vandiver 予想と正規底について

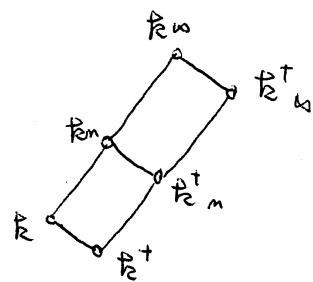
早大理工 小松啓一 (Keiichi Komatsu)

正の整数 n に対して, $\zeta_n = e^{\frac{2\pi i}{n}}$ とし, 奇素数 p に対して, $k = \mathbb{Q}(\zeta_p)$ とし, k^+ を k の最大実部分体, h_{k^+} を k^+ の類数とする。このとき p が h_{k^+} を割らないというのが Vandiver 予想である。さらに k の cyclotomic $\mathbb{Z}_p$ -拡大を k_∞ とする。この場合 $k_\infty = k(\{\zeta_{p^m}; \mathbb{Z} \ni m > 0\})$ となり $G(k_\infty/k) \cong \mathbb{Z}_p$ となっている。 k^+ の cyclotomic $\mathbb{Z}_p$ -拡大を k_∞^+ とすると

$$k^+ = k_0^+ \subset k_1^+ \subset \cdots \subset k_m^+ \subset \cdots \subset k_\infty^+$$

$$G(k_m^+/k^+) \cong \mathbb{Z}/p^m \mathbb{Z}$$

となる拡大体の列が存在する。



さらに A_m^+ を k_m^+ のイデアル類群の p -part とすれば, 岩沢の定理により, 0 以上の整数 $\lambda(k^+)$ と $\mu(k^+)$ および整数 $\nu(k^+)$ があり

$$\#A_m^+ = p^{\lambda(k^+)m + \mu(k^+)p^m + \nu(k^+)}$$

が十分大きな m に対して成立する。ただし $\#A_m^+$ は A_m^+ の位数を表すとする。このとき Ferrero - Washington [] により, $\mu(\mathbb{Q}^+) = 0$ が知られている。一方 Greenberg により $\lambda(\mathbb{Q}^+) = 0$ が予想されている。 p が $\ell_{\mathbb{Q}^+}$ を割らないならば $\lambda(\mathbb{Q}^+) = 0$ であることを注意しておく。

さて, 自然数 $m \leq n$ について A_m^+ から A_n^+ への自然な準同型があるが, それについての $\{A_m^+\}$ の inductive limit を $\varinjlim_m A_m^+ = A_\infty^+$ とする。このとき,

$\lambda(\mathbb{Q}^+) = 0 \iff A_\infty^+ = 0 \iff$ 任意の自然数 n と A_n^+ の任意の元 a について, a に属するイデアルは n より十分大なる m について ℓ_m^+ で単項化する。

$\mathbb{Q}_{\text{al}} = \mathbb{Q}(\{\zeta_n : \mathbb{Z} \ni n > 0\})$, $\mathbb{Q}_{\text{al}}^+$ を $\mathbb{Q}_{\text{al}}$ の最大実部分体 K を $\mathbb{Q}$ の有限次拡大体, C_K を K のイデアル類群とする。

$$C_{\mathbb{Q}_{\text{al}}^+} = \varinjlim_{\substack{\mathbb{Q}_{\text{al}}^+ \supset K \\ (K:\mathbb{Q}) < \infty}} C_K \quad \text{とする。}$$

このとき M. Kurihara [7] は次のような興味深い結果を得た。

Theorem 1. $C_{\mathbb{Q}_{\text{al}}^+}$ は trivial である。

この定理は ℓ_m^+ のイデアルは $\mathbb{Q}_{\text{al}}^+$ の十分大きな有限次

部分体で単項化していることをいっており, Greenberg 予想と比較して大変興味深い結果である。一方 $C_{\mathbb{Q}^{\text{ab}}}$ は大変大きな群になっていることを注意しておく。

次に $\mathbb{Z}_p$ -拡大の正規- p -基底と Vandiver 予想との関係について述べることにする。先ず有限次代数体 K を k の $\mathbb{Z}_p$ -拡大とし,

$$k = K_0 \subset K_1 \subset \cdots \subset K_m \subset \cdots \subset K \quad (K_m : k) = p^m$$

とする。

Def. $\mathbb{Z}_p$ -拡大 K/k が正規- p -基底を持つ。

($\stackrel{\text{def.}}{\Leftrightarrow}$) 任意の自然数 m に対して, $\mathcal{O}_{K_m}[\frac{1}{p}]$ の元 θ_m があつて $\{\theta_m^{\tau}\}_{\tau \in G(K_m/k)}$ が $\mathcal{O}_{K_m}[\frac{1}{p}]/\mathcal{O}_k[\frac{1}{p}]$ の基底になっている。

このとき次の定理が成立する。

Theorem 2 (cf. [4]) p は奇素数, $\zeta_p = e^{\frac{2\pi i}{p}}$, $k = \mathbb{Q}(\zeta_p)$

$k^+ = k \cap \mathbb{R}$, h_{k^+} を k^+ の類数とする。このとき次は同値

(1) p は h_{k^+} を割らない。

(2) $\lambda(k^+) = 0$ で k の $\frac{p+1}{2}$ の独立な $\mathbb{Z}_p$ -拡大がすべて正規- p -基底をもつ。

上の定理から Vandiver 予想の研究にとって $\mathbb{Z}_p$ -拡大の正規- p -基底の研究が大切であることがわかる。これについて以下に述べる事が知られている。

Prop. 1. (cf. [3]) $\mathbb{K}$ を有限次代数体, $\mathbb{K}_\infty$ を $\mathbb{K}$ の cyclotomic $\mathbb{Z}_p$ -拡大とする。このとき $\mathbb{K}_\infty/\mathbb{K}$ は正規- p -基底をもつ。

Prop. 2. (cf. [2], [5]) $\mathbb{K}$ を虚 2 次体, $\tilde{\mathbb{K}}$ を $\mathbb{K}$ の絶対類体, K を $\mathbb{K}$ の $\mathbb{Z}_p$ -拡大, このとき $p \neq 3$ ならば, $K\tilde{\mathbb{K}}/\mathbb{K}$ は正規- p -基底をもつ。

Prop. 2 より 次かわかる。

Prop. 3. $p \equiv 3 \pmod{4}$ $p \neq 3$, ($\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$ と仮定)
 K を $\mathbb{Q}(\sqrt{p})$ の $\mathbb{Z}_p$ -拡大とすれば, $K\mathbb{Q}(\sqrt{p})/\mathbb{Q}(\sqrt{p})$ は正規- p -基底をもつ。

Prop. 2 の証明には, modular units がもちいられる。このことから, 次の問題を考えることは意味があるように思われる。

問題 虚アーベル体のアーベル拡大の正規基底や単数を Siegel modular 関数の特殊値でどのくらい構成できるか。

以後 $\zeta = e^{\frac{2\pi i}{5}}$, $k = \mathbb{Q}(\zeta)$, 正の整数 m に対して,
 $k(m)$ を k の mod m の ray class field を表すとする。さらに
 $S_m = \{ a \in k^\times ; a \equiv 1 \pmod{m} \}$, $\tilde{S}_m = \{ (a) : a \in S_m \}$

$G(k/\mathbb{Q})$ の元 σ で $\zeta^\sigma = \zeta^2$ となるものを固定し, $k^\times$ の自己準同型 φ を $\varphi(a) = a^{1+\sigma^3}$ $a \in k^\times$ で定める。さらに U を k の単数群とする。このとき,

$$G(k(2p^2)/k(2p)) \cong \tilde{S}_{2p}/\tilde{S}_{2p^2} \cong S_{2p}/S_{2p^2}(S_{2p} \cap U)$$

となる。 $H = S_{2p^2}(S_{2p} \cap U)$ とおけば, $\varphi(H) \subset H$ となり,

$$\text{準同型 } \tilde{\varphi} : S_{2p}/H \rightarrow S_{2p}/H \quad \text{が} \quad \tilde{\varphi}(aH) = \varphi(a)H$$

により induce される。このとき $\tilde{\varphi}(S_{2p}/H) \cong (\mathbb{Z}/p\mathbb{Z})^3$ がわかり, $\text{Ker } \tilde{\varphi}$ に対応する類体を L とすれば,

$$G(L/k(2p)) \cong (\mathbb{Z}/p\mathbb{Z})^3$$

となる。

$\mathcal{H}_2 = \{ z \in M_2(\mathbb{C}) ; {}^t z = z, \text{ Im } z \text{ は positive definite} \}$
 を degree 2 の Siegel 上半空間とする。さらに,

$$z_0 = \frac{1}{5} \begin{pmatrix} 2+y-y^2-2y^4 & 2-y+y^2-2y^3 \\ 2-y+y^2-2y^3 & y+2y^2-2y^3-y^4 \end{pmatrix} \quad \text{とおけば,}$$

z_0 は $\mathcal{F}_2$ の点で, $y^2=1-x^5$ の principal polarization をとった Jacobian variety にふたつとした CM-point となる。

複素数 t に対して, $e(t) = e^{2\pi i t}$, $z \in \mathcal{F}_2$, $t = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \in \mathbb{R}^2$

$\Delta = \begin{pmatrix} \Delta_1 \\ \Delta_2 \end{pmatrix} \in \mathbb{R}^2$, $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \in \mathbb{C}^2$ とし, テータ関数を

$$\Theta(u, z; t, \Delta) = \sum_{x \in \mathbb{Z}^2} e\left(\frac{1}{2} t(x+t)z(x+t) + t(x+t)(u+\Delta)\right)$$

とおき,

$$\Phi(z; t, \Delta) = \frac{2\Theta(0, z; t, \Delta)}{\Theta(0, z; 0, 0)} \quad \text{とおく。}$$

然らば, 正の整数 N に対して, $t, \Delta \in \frac{1}{N}\mathbb{Z}^2$ のとき,

$\Phi(z; t, \Delta)$ は レベル $2N^2$ の Siegel modular function

となる。このとき次の定理が得られる。

Theorem 3 ([6]) $\Phi_1(z_0) = \Phi(z_0; \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix})$,

$\Phi_2(z_0) = \Phi(z_0; \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix})$ とおく。このとき次が成立。

$$(1) \quad \Phi_i(z_0) \in \mathcal{O}_{\mathbb{K}} L \quad i=1, 2$$

$$(2) \quad \Theta = \left(\sum_{\nu=0}^{p-1} \zeta_{p^2}^{\nu} \right) \left(\sum_{\nu=0}^{p-1} \Phi_1(z_0)^{\nu} \right) \left(\sum_{\nu=0}^{p-1} \Phi_2(z_0)^{\nu} \right) \quad \text{とおく。}$$

$\Phi_1(z_0)\Phi_2(z_0) \neq 0$ ならば $\{\Theta^z\}_{z \in G(L/\mathbb{K}(2P))}$ は $L/\mathbb{K}(2P)$

の正規底である。

証明には [1] と [8] の結果をもちいる。 $p=3$ のとき $\varpi_1(\zeta_9)\varpi_2(\zeta_9) \neq 0$ を 日大の福田隆氏に計算していただいた。 $\mathbb{Q}(\zeta_9)$ の rank 19 の unit group も ϖ をもちいて構成できる。

References

[1] J. Igusa : Modular forms and projective invariants, Amer. J. Math., 89 (1967) 817-855

[2] T. Ito : A construction of normal bases over the Hilbert p -class field of imaginary quadratic fields, to appear in Proc. Japan Acad.

[3] Kersten, I., Michaličková, J : $\mathbb{Z}_p$ -extensions of complex multiplication fields.

J. Number Theory 32 (1989) 131-150

[4] I. Kersten, J. Michaličková : On Vandiver's conjecture and $\mathbb{Z}_p$ -extensions of $\mathbb{Q}(\zeta_{p^n})$, J. Number Theory 32 (1989), 371-386

[5] K. Komatsu : Normal basis and Greenberg's conjecture, Math. Ann. 300 (1994), 157-163

[6] K. Komatsu : Construction of normal bases ~~of~~ by special values of Siegel modular functions, preprint

[7] M. Kurihara : Notes on the ideal class groups of real

abelian fields, Preprint

[8] G. Shimura: Theta functions with complex multiplication,
Duke Math. J., 43 (1976), 673-696.