数理解析研究所講究録
1026巻 1998年 12-19

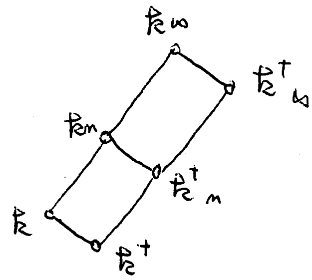
Vandiver 予想と正規底について

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 $k_\infty = k(\{\zeta_{p^n} ; \mathbb{Z} \ni n > 0\})$ 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

$$k^+ = k^+_0 \subset k^+_1 \subset \cdots \subset k^+_n \subset \cdots \subset k^+_\infty$$

$$G(k^+_n/k^+) \cong \mathbb{Z}/p^n\mathbb{Z}$$



となる拡大体の列が存在する。

さらに A^+_n を k^+_n 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

$$\# A^+_n = p^{\lambda(k^+)n + \mu(k^+)p^n + \nu(k^+)}$$

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

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

$\lambda(k^+)=0 \iff A_\infty^+=0 \iff$ 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 k_m^+ で単項化する。

$\mathbb{Q}_{ab}=\mathbb{Q}(\{\zeta_n : \mathbb{Z}\ni n>0\})$，$\mathbb{Q}_{ab}^+$ を $\mathbb{Q}_{ab}$ 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．

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

このとき M. Kurihara [7] は次のような興味深い結果を得た。

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

この定理は k_n^+ のイデアルは $\mathbb{Q}_{ab}^+$ 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 $C_{\mathbb{Q}^{ae}}$ 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。k を有限次代数体 K を k の $\mathbb{Z}_p$－拡大とし，

$$k = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K \qquad (K_n : k) = p^n$$

とする。

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

$\overset{\text{def.}}{\Longleftrightarrow}$ 任意の自然数 n に対して，$\mathcal{O}_{K_n}[\frac{1}{p}]$ の元 θ_n があって $\{\theta_n^{\tau}\}_{\tau \in G(K_n/k)}$ が $\mathcal{O}_{K_n}[\frac{1}{p}] / \mathcal{O}_{k}[\frac{1}{p}]$ の基底になっている。

このとき次の定理が成立する。

Theorem2(cf.[4]) p を奇素数，$\zeta_p = e^{\frac{2\pi i}{p}}$，$k = \mathbb{Q}(\zeta_p)$ $k^+ = k \cap \mathbb{R}$，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 $\frac{p+1}{2}$ この独立な $\mathbb{Z}_p$－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]) kを有限次代数体, k_∞をkのcyclotomic $\mathbb{Z}_p$-拡大とする。このときk_∞/kは正規-p基底をもつ。

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

Prop. 2より次がわかる。

Prop. 3. $p\equiv 3 \pmod{4}$ $p\neq 3$, ($\mathbb{Q}(\sqrt{-p})\subset\mathbb{Q}(\zeta_p)$となる) 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底や単数を Siegel modular 関数の特殊値でどのぐらい構成できるか。

以後 $\zeta = e^{\frac{2\pi i}{5}}$，$k = \mathbb{Q}(\zeta)$，正の整数 m に対して，$k(m)$ で 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，

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

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，$\mathrm{Ker}\,\tilde{\varphi}$ 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。

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

$$\mathfrak{z}_0 = \frac{1}{5}\begin{pmatrix} 2+\zeta-\zeta^2-2\zeta^4 & 2-\zeta+\zeta^2-2\zeta^3 \\ 2-\zeta+\zeta^2-2\zeta^3 & \zeta+2\zeta^2-2\zeta^3-\zeta^4 \end{pmatrix}$$ とおけば、

$\mathfrak{z}_0$ は $\mathfrak{S}_2$ の点で、$y^2=1-x^5$ の principal polarization をもった Jacobian variety にふずいした CM-point となる。

複素数 t に対して、$e(t)=e^{2\pi i t}$，$\mathfrak{z}\in\mathfrak{S}_2$，$r=\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}\in\mathbb{R}^2$

$s=\begin{pmatrix} s_1 \\ s_2 \end{pmatrix}\in\mathbb{R}^2$，$u=\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}\in\mathbb{C}^2$ とし，テータ関数を

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

とおき，

$$\Phi(\mathfrak{z};r,s)=\frac{2\Theta(0,\mathfrak{z};r,s)}{\Theta(0,\mathfrak{z};0,0)}$$ とおく。

然らば，正の整数 N に対して，$r,s\in\frac{1}{N}\mathbb{Z}^2$ のとき，$\Phi(\mathfrak{z};r,s)$ 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]) $\Phi_1(\mathfrak{z}_0)=\Phi\left(\mathfrak{z}_0;\begin{pmatrix} \frac{1}{p} \\ 0 \end{pmatrix},\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$，$\Phi_2(\mathfrak{z}_0)=\Phi\left(\mathfrak{z}_0;\begin{pmatrix} \frac{1}{p} \\ 0 \end{pmatrix},\begin{pmatrix} \frac{1}{p} \\ \frac{1}{p} \end{pmatrix}\right)$ とおく。このとき次が成立。

(1) $\Phi_i(\mathfrak{z}_0)\in\mathcal{O}_L \qquad i=1,2$

(2) $\Theta=\left(\sum_{\nu=0}^{p-1}\zeta_{p^2}^{\nu}\right)\left(\sum_{\nu=0}^{p-1}\Phi_1(\mathfrak{z}_0)^{\nu}\right)\left(\sum_{\nu=0}^{p-1}\Phi_2(\mathfrak{z}_0)^{\nu}\right)$ とおく。

$\Phi_1(\mathfrak{z}_0)\Phi_2(\mathfrak{z}_0)\neq 0$ ならば $\{\Theta^{\tau}\}_{\tau\in G(L/k(2p))}$ は $L/k(2p)$

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$\Phi_1(\mathfrak{z}_0)\Phi_2(\mathfrak{z}_0)\neq 0$を日大の福田隆氏に計算していただいた。$k(6)$の rank 19 の unit group も Φ 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., Michaličtk. J : $\mathbb{Z}_p$-extensions of complex multiplication fields. J. Number Theory 32 (1989) 131-150

[4] I. Kersten, J. Michaličtk : 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.