数理解析研究所講究録
第 750 巻 1991 年 66-75

円分体の ideal 類群と保型形式及び K 群について

都立大・理 栗原 将人 (Masato Kurihara)

円分体は近代的整数論の発祥の地であり古い歴史を持つが、その理論は 発展の可能性を秘めた様々な理論の端的な例を与えると同時に それ自体の美しさによって今でも独特の位置を占めている[注]。ここでは岩澤理論とも密接に関連する円の p 分体のイデアル類群の p-part の構造について主に2つの方向から考えていく。すなわち円の p 分体の類群の構造についての有名な予想と $\mathbb{Z}$ の K 群，及び level 1 保型形式との関係について述べる。共に円の p 分体という有理数体の拡大体の話を下の体 $\mathbb{Q}$ (あるいは $\mathbb{Z}$) に落とした話であることに注意しておく。

1. 奇素数 (非正則素数) p に対して $K=\mathbb{Q}(\mu_p)$ を円の p 分体，$\Delta=\mathrm{Gal}(K/\mathbb{Q})$ をその Galois 群，A を K のイデアル類群の p-Sylow 部分群とする。Δ の位数は p と素だから A は Δ の

作用によって

$$A = \bigoplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} A^{[i]}$$

と分解される。ここに $\omega : \Delta = (\mathbb{Z}/p)^\times \longrightarrow \mathbb{Z}_p^\times$ を Teichmüller 指標として $A^{[i]} = \{x \in A \mid \sigma(x) = \omega^i(\sigma)x \text{ for all } \sigma \in \Delta\}$ である。$A^{[0]} = A^{[1]} = 0$ はすぐにわかる。また Mazur Wiles によって証明された Iwasawa's main conjecture の帰結として $j \not\equiv 1 \pmod{p-1}$ なる奇数 j に対し $\mathrm{ord}_p \# A^{[j]} = \mathrm{ord}_p L(0, \omega^{-j}) = \mathrm{ord}_p B_{1,\omega^{-j}}$ であることが知られている。ここに $L(s, \omega^{-j})$ は Dirichlet L 関数，$B_{1,\omega^{-j}}$ は generalized Bernoulli number である。なお最近 Kolyvagin は Gauss 和の Euler system を使って上の事実の main conjecture を経由しない証明を与えた。(偶数 i に対しても $A^{[i]}$ の位数を円単数を使って書くことができる。) しかしこのような zeta 関数の特殊値との関係だけからでは $A^{[i]}$ の構造はわからない。$A^{[i]}$ の構造についてはやや楽観的な次のような予想がある。

<u>予想 1.</u> (Kummer Vandiver) 偶数 i に対して $A^{[i]} = 0$

<u>予想 2.</u> j を $j \not\equiv 1 \pmod{p-1}$ なる奇数とすると

$$A^{[j]} \simeq \mathbb{Z}_p / B_{1,\omega^{-j}} \mathbb{Z}_p$$

よく知られているように予想 1 には理論的根拠は何もない。

ただこの予想が正しいとすると円分体論は著しく簡潔になるのである。duality により偶数 i に対する予想1は $j=1-i$ に対する予想2を導く。

岩澤理論との関係を一言述べておこう。$L/\mathbb{Q}(\mu_{p^\infty})$ を $\mathbb{Q}(\mu_{p^\infty})$ の最大不分岐 abel 拡大とする。main conjecture の述べるところは $\mathrm{Gal}(L/\mathbb{Q}(\mu_{p^\infty}))^-$ の"特性多項式"が p 進L関数であるということである。予想2が正しければ特性多項式がわかるだけでなく $\mathrm{Gal}(L/\mathbb{Q}(\mu_{p^\infty}))^-$ は $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]/(p$ 進 $L)$ と同型になる。以上の予想及び関連する事柄については岩澤先生の [1] にまとめられている。筆者の円分体論への興味はこのときの数理研における岩澤先生の簡潔にして感銘深い講演から始まった。この機会に岩澤先生並びにそのシンポジウムを組織された佐武先生，森田先生に感謝の気持を表したく思います。

2. $\mathbb{Z}$ を有理整数環，$K_*(\mathbb{Z})$ を $\mathbb{Z}$ の K 群とする。$K_n(\mathbb{Z})$ $(n\geqq 0)$ を知ることは K 理論の最も基本的な問題だと思われるが，現状ではその有限生成 abel 群であること (Quillen)，rank の計算 (Borel)，$n\leqq 5$ のときの結果 (Lee Szczarba 等) くらいしか知られていない。ここでは $K_n(\mathbb{Z})$ の torsion part $K_n(\mathbb{Z})_{tors}$ に対して次のように予想する。

<u>予想3</u>　$K_n(\mathbb{Z})_{tors}$ は 2-torsion を除いて巡回群である。

予想3は予想2を導く。もっと詳しく

予想4. $n \geqq 1$ に対して

1) $K_{4n}(\mathbb{Z}) \sim 0$

2) $K_{4n+1}(\mathbb{Z}) \sim \mathbb{Z}$

3) $K_{4n+2}(\mathbb{Z}) \sim \mathbb{Z}/N_{2n+2}\mathbb{Z}$

4) $K_{4n+3}(\mathbb{Z}) \sim \mathbb{Z}/D_{2n+2}\mathbb{Z}$

ここに $A \sim B$ は 2-torsion を除く同型を表す。また k を正の偶数としたとき N_k, D_k は

$$\zeta(1-k) = (-1)^{\frac{k}{2}} \frac{N_k}{D_k} \qquad (N_k, D_k) = 1$$

なる自然数。$\zeta(s)$ は Riemann zeta 関数。

定理1. (1) 予想4, 1) は予想1, 予想2を導く。より正確には $K_{4n}(\mathbb{Z})\{p\}$ ($K_{4n}(\mathbb{Z})$ の p-Sylow 部分群) $= 0$ であるとすると、$A^{[-2n]} = 0$ であり $A^{[2n+1]} \simeq \mathbb{Z}_p / B_{1,\omega^{-2n-1}} \mathbb{Z}_p$ となる。

(2) 予想4, 3) は予想2, $j = -2n-1$ を導く。

系. $A^{[p-3]} = 0$, $A^{[3]} \simeq \mathbb{Z}_p / B_{1,\omega^{-3}} \mathbb{Z}_p$.

これは Lee Szczarba Soulé の定理 $K_4(\mathbb{Z})\{p\} = 0$ $(p \geqq 5)$ と上の定理1 (1) からの帰結である。

定理1の証明は Chern class $K_{2r-2}(\mathbb{Z}) \longrightarrow H^2_{et}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p(r))$ の全

射性と同型

$$A^{[1-r]}/p \simeq H^2_{et}(\mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}/p(r))$$

による。

3. 上の系の応用をいくつか述べる。まず $A^{[p-3]}=0$ から伊原先生 [2] の Th. 6 の条件はすべて正しい。[2] の元となった [3] からひとつだけ結果を述べよう。a を $1 \leqslant a \leqslant p-2$ なる整数とし J を curve $y^p = x^a(1-x)$ の Jacobian, $J(\mathbb{Q}(\mu_p))\{p\}$ を J の $\mathbb{Q}(\mu_p)$ 有理点で位数が p 巾の元全体とする。$\pi = 1-\zeta_p$ (ζ_p : 1 の原始 p 乗根), $J[\pi^3]$ を $J(\overline{\mathbb{Q}})$ の π^3 等分点全体とする。(J は $\mathbb{Z}[\mu_p]$ の CM を持つ。) [3] Th. 1 では $J[\pi^3] \subset J(\mathbb{Q}(\mu_p))$ が示されていた。$A^{[p-3]}=0$ から

$$J(\mathbb{Q}(\mu_p))\{p\} = J[\pi^3] \left(\simeq (\mathbb{Z}/p)^{\oplus 3}\right)$$

がわかる。Jacobi 和，及び $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ の表現との関係について詳しくは [2] を見て頂きたい。

次に $A^{[3]} \simeq \mathbb{Z}_p/B_{1,\omega^{-3}}\mathbb{Z}_p$ の応用について述べる。Vandiver は Fermat の問題の第 1 の場合が誤っているとすると，つまり $x^p+y^p=z^p$, $p \nmid xyz$ なる自然数 x, y, z が存在すると仮定すると $p^2 \mid B_{(p-4)p+1}$ であることを示した。一方 Kummer の合同式から $B_{1,\omega^{-3}} \equiv -B_{(p-4)p+1}/((p-4)p+1) \pmod{p^2}$ である。従ってもし Fermat の問題の第 1 の場合が誤っているとすると $A^{[3]}$

は位数 p^2 の元を持つことになる。A が位数 p^2 の元を持つということは非常に強い条件であり，もちろん今まで知られている中ではこのような例は存在しない。なおこの Fermat の問題の第1の場合と Bernoulli 数の関係については最近岩澤先生と藤崎先生がもっと詳しく調べている。

4．保型形式に話を移そう。k を正の偶数とし，M_k で重さ k の $SL_2(\mathbb{Z})$ に関する保型形式全体のなす空間，M_k^0 で cusp forms 全体を表すことにする。$\mathbb{T}_k$ を $\mathrm{End}(M_k^0)$ の部分環で $\mathbb{Z}$ 上 Hecke 作用素 T_ℓ たちで生成される環とする。$\mathbb{T}_k$ は $\mathbb{Z}$ 上 finite でその rank は $\dim M_k^0$ に等しい。p を $p-1>k$ なる素数とする。$\mathbb{T}_k\otimes\mathbb{Z}_p$ を考えると これは $\mathbb{Z}_p$ 上 finite だから局所環の直和になる。

予想5．R を $\mathbb{T}_k\otimes\mathbb{Z}_p$ の ordinary な local component の局所環とすると R は1次元の Gorenstein 環である。

ここに R が ordinary とは m_R を R の極大 ideal としたとき T_p の R/m_R での像が0でないことと定義する。R が1次元の Gorenstein 環であることは $\mathrm{Hom}(R,\mathbb{Z}_p)$ が R 加群として R と同型であることと同値である。$f=\sum_{n\geq 1}a_n q^n$ を mod p eigenform $a_1=1$，$a_n\in F$（F：有限体$/\mathbb{F}_p$）とする。f に伴う表現を

$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$ とする。すなわち ρ_f は semi simple で $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell$, $\det(\rho_f(\mathrm{Frob}_\ell)) = \ell^{k-1}$ $(\ell \neq p)$。ρ_f が既約であれば f に対応する $\mathbb{T}_k \otimes \mathbb{Z}_p$ の local component $\mathbb{T}_f$ について上の予想は正しい。

予想5は予想2を導く。正確に述べよう。今 $A^{[1-k]} \neq 0$ と仮定する。従って $p \mid B_k$ となる。このとき Eisenstein series $G_k = \frac{1}{2}\zeta(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ は mod p cusp form になる。$\mathbb{T}^E$ を対応する $\mathbb{T}_k \otimes \mathbb{Z}_p$ の local component とする。すなわち $\mathbb{T}^E$ を極大 ideal $\mathfrak{m}$ が

$$\mathfrak{m} = (p,\ T_\ell - (1+\ell^{k-1}), \cdots)$$ (ℓ はすべての素数を動く)

で与えられる component とする。

<u>定理2</u>. (1) $\mathbb{T}^E$ が Gorenstein であれば $j = 1-k$ に対する予想2は正しい

(2) $\mathcal{I}$ を $T_\ell - (1+\ell^{k-1})$ (ℓ: 素数) たちで生成される $\mathbb{T}^E$ の ideal (Eisenstein ideal) とする。$p^n \| B_k$ とすると $\mathbb{T}^E/\mathcal{I} \simeq \mathbb{Z}/p^n$ であり、$\mathcal{I}/\mathcal{I}^2$ が位数 p^n の元を持てば $j = 1-k$ に対する予想2は正しい。

特に上から $\mathcal{I}$ が主 ideal であれば予想2が導かれることがわかる。また $d_{\mathbb{T}_k/\mathbb{Z}}$ を $\mathbb{T}_k$ の判別式としたとき、$p \nmid d_{\mathbb{T}_k/\mathbb{Z}}$ であれば $\mathbb{T}^E \simeq \mathbb{Z}_p$ であるから予想2は正しい。また G_k mod p の

標数0の normalized eigen cusp form への持ちあげが2つ以下しかなければ $\mathrm{rank}_{\mathbb{Z}_p} \mathbb{T}^E \leqq 2$ であるから やはり予想2が正しいことがわかる。

逆もほぼ成立する。

<u>定理3.</u> $i=2-k$ についての予想1を仮定する。このとき次は同値.

(1) $\mathbb{T}^E$ は Gorenstein

(2) $\mathfrak{I}$ は $\mathbb{T}^E$ の主 ideal.

(3) $\mathfrak{I}/\mathfrak{I}^2$ は位数 p^n の元を持つ. $(p^n \| B_k)$

(4) $j=1-k$ に対して予想2が正しい。

特に予想1（Vandiver予想）が一般に正しければ Eisenstein ideal $\mathfrak{I}$ は主 idealである。

重さ2，指標 ω^{k-2} の $\Gamma_1(p)$ に関する保型形式に対しても同様なことはできる。

5. Ribetは[4]で円分体に関する結果を得るために保型形式に伴う Galois 表現を効果的に用いた。これはその後のこの種の議論の出発点となったが，ここでも上の定理を得るために保型形式に伴う p 進表現，すなわち etale cohomology

$W = H^1_{par}(M_N \otimes \overline{\mathbb{Q}}, \mathrm{Sym}^{k-2} R^1 f_* \mathbb{Z}_p(k-1))^{GL_2(\mathbb{Z}/N)}$ （M_N: level $\Gamma(N)$ を持つ

楕円曲線の moduli space, f: universal elliptic curve) の $\mathbb{T}^E$ component W^E を考える。ここでは定理2.(1)の証明の概略を与えることにする。$\mathbb{T}^E$ が Gorenstein ということは W^E が $\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{T}^E)$ なる2次元表現であることを保証する。これは p の外で不分岐である。今 I を $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の p での惰性群とすると上の表現の I への制限は $\begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix}$ χ: cyclotomic character となっている。(ここまでは保型形式に伴う p 進表現の一般論) さて Eisenstein ideal $\mathcal{I}$ に対し

$$\rho_E \bmod \mathcal{I} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{T}^E/\mathcal{I}) \simeq GL_2(\mathbb{Z}/p^n)$$

を考えると この分解群 D への制限は split $\begin{pmatrix} \chi^{k-1} & 0 \\ 0 & 1 \end{pmatrix}$ しており さらに $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 全体の表現としても $\begin{pmatrix} \chi^{k-1} & 0 \\ * & 1 \end{pmatrix}$, $* \notin p\cdot(\mathbb{Z}/p^n)$ なる型であることが示せる。(ただし正確には $\mathbb{T}^E \neq \mathbb{Z}_p$ と仮定した。$\mathbb{T}^E = \mathbb{Z}_p$ のときはもっと簡単で (その必要はないと思うのだが) lattice をとり直せば上のようにできる。) 従って $(\rho_E \bmod \mathcal{I}) \otimes \chi^{1-k}$ は $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{p}]}(\mathbb{Z}/p^n, \mathbb{Z}/p^n(1-k)) \simeq H^1_{et}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(1-k))$ の元で p での分解群に制限すると trivial になってしまう位数 p^n の元を与える。つまり

$$\mathrm{Ker}\,(H^1_{et}(\mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}/p^n(1-k)) \longrightarrow H^1(\mathbb{Q}_p, \mathbb{Z}/p^n(1-k)))$$

の位数 p^n の元を与えることになる。Tate Poitou の duality によって上の群は $H^2_{et}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(k))$ の双対と同型。一方 Iwasawa's main conjecture により $\# H^2_{et}(\mathbb{Z}[\frac{1}{p}]\ \mathbb{Z}/p^n(k)) = p^n$ である。従っ

て $H^2_{et}(\mathbb{Z}[\frac{1}{p}]\ \mathbb{Z}/p^n(k)) \simeq \mathbb{Z}/p^n$ でなければならず，これは $H^2_{et}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p(k)) \simeq \mathbb{Z}/p$ を導く。このことと 2. で述べた同型 $A^{[1-k]}/p \simeq H^2_{et}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p(k))$ とから $A^{[1-k]}$ が巡回群であることが従うのである。

References

[1] 岩澤健吉，円分体に関するいくつかの問題，数理研講究録 658，p. 43 − 55

[2] Y. Ihara, Profinite braid groups, Galois representations and Complex multiplications, Ann. of Math. 123, p. 43 − 106

[3] R. Greenberg, On the Jacobian variety of some algebraic curves, Compos. Math. 42, p. 345 − 359

[4] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. math. 34, p. 151 − 162

(注) この書き出しの文章の一部は K. Iwasawa Ann. of Math. (1959) p. 530−561 から引用させて頂いた。