静岡県立大学
短期大学部
研究紀要第10号
1996年度

Thaine の annihilator と Gauss の和

舘 山 光 一

Thaine's annihilator and Gaussian sums

TATEYAMA, Koichi

1．序

1950 年代から展開された岩沢理論によって，円分体の整数論は飛躍的に発展し Mazur-Wiles の定理[M-W]によって一応の完成をみたように思われる。また，Thaine[Th]や Kolyvagin[R]の実円分体のイデアル類群の annihilator の構成は，難解な modular form や代数幾何からの解放の可能性を示し，円分体の理論をさらに完成度の高い理論への方向へと導いているように思える。ただ，Thaine や Kolyvagin の annihilator は従来の Gauss の和から Stickelberger element を取り出した方法とはかなり異なり，この2種類の annihilator の関係も判然とはしない。本稿の目的は，これらの一見異なるように思われる annihilator を統一的に構成する方法を示し，古典的な方法との関係を明らかにすることにある。

2．Teichmüller character

Stickelberger の定理は，Gauss の和の素イデアル分解を具体的に与えるものであるが，Gauss の和が素イデアルの何乗で割り切れるかは character が Teichmüller character の何乗で書けるかによって定まる。実は，この結果を一般化することができるのだが，その準備のためここではより一般的な場合を考えてみることにする。

まず p を奇素数とし k を $\mathbf{Q}_p$ 上の有限拡大体，$R=R_k$，$\mathfrak{p}=\mathfrak{p}_k$ をそれぞれ k の整数環，素イデアルとする。π を $\mathfrak{p}$ の uniformizing parameter とすると，次のような一変数の形式的べき級数 $[\pi](T)\in R[[T]]$ によって Lubin-Tate group G を定義することができる[L-T]。

$$[\pi](T)\equiv \pi T \mod \deg 2$$

$$[\pi](T)\equiv T^q \mod \pi$$

ここで，q は剰余体 R/π の元の数を表す。また，R の元 α に対して $[\alpha](T)\in R[[T]]$ を G の endomorphism とする。即ち，

$$[\alpha](G(X,Y))=G([\alpha](X),[\alpha](Y))$$

$$[\alpha](T)\equiv \alpha T \mod \deg 2$$

を満たすものである。また，k^{ac} を k を含む最小の代数閉体とするとき，

$$G_\pi = \{w \in k^{ac} : [\pi](w) = 0\}$$

$$K = k(G_\pi)$$

とする。Lubin-Tate の理論によれば，K/k はアーベル拡大となり，そのガロア群は剰余体 R/π の乗法群と同型になる。その対応は，

$$w^{\sigma\alpha} = [\alpha](w), \quad w \in G_\pi, \quad \sigma_\alpha \in \mathrm{Gal}(K/k)$$

で与えられる。k は 1 の $q-1$ 乗根を含むので，$\mathrm{Gal}(K/k)$ の character は k 上で実現することができるが，ここで，次の条件を満たす character ω を Teichmüller character と呼ぶことにする。

$$\omega(\sigma_\alpha) \equiv \alpha \mod \pi$$

このような character は存在し，$\mathrm{Gal}(K/k)$ の k 上の character group は ω で生成される位数 $q-1$ の巡回群となる。

K/k で $\mathbf{p}$ は完全分岐し，$\mathbf{p}$ の上のイデアル $\wp$ は $w \in G_\pi - \{0\}$ を uniformizing element とする単項イデアルとなる。従って，K の整数 β は k の整数を係数とする w-adic 展開が可能となり，$\beta^{\sigma-1} \mod \wp$ は $\mathrm{Gal}(K/k)$ の $R/\mathbf{p}$-value の character となる。$R/\mathbf{p}$ の乗法群は 1 の $q-1$ 乗根全体であるから，この character は $R^\times$ に持ち上げることができる。即ち，$\beta^{\sigma-1} \mod \wp$ は Teichmüller character ω を用いて表すことができる。次の命題 2.1 が 2 つの character の関係を具体的に示すものである。

命題 2.1 β を $\mathrm{ord}_\wp \beta = n$ とする K の元とする。このとき，$\sigma \in \mathrm{Gal}(K/k)$ に対し

$$\beta^{\sigma-1} \equiv \omega^n(\sigma) \mod \wp$$

が成り立つ。

証明） w を $G_\pi - \{0\}$ の元とすると，$\mathrm{ord}_\wp w = 1$ であり $\mathrm{Gal}(K/k)$ の作用は

$$w^{\sigma\alpha} = [\alpha](w)$$

となる。従って，

$$w^{\sigma\alpha-1} \equiv \alpha \equiv \omega(\sigma_\alpha) \mod \wp$$

である。また，仮定より β は K の単数 u を用いて $\beta = w^n u$ と表すことができる。よって，

$$\beta^{\sigma-1} = \left(w^{\sigma-1}\right)^n u^{\sigma-1}$$

となるが，

$$u^{\sigma-1} \equiv 1 \mod \wp$$

より

$$\beta^{\sigma-1}\equiv\left(w^{\sigma-1}\right)^{n}\equiv\omega^{n}(\sigma) \mod \wp$$

となり，命題 2.1 は証明された。

注意）$G=\mathbf{G}_{\mathrm{m}}$ (formal multiplicative group)，$k=\mathbf{Q}_p$ とすれば $K=k(\zeta_p)$ であり，ω は通常の Teichmüller character である。以下，命題 2.1 はこの場合にだけ適応される。

3．単数群のコサイクル

k を有理数体上の有限次拡大体，p を k 上で完全分解する素数とする。また，$K=k(\zeta_p)$, $\Delta=\mathrm{Gal}(K/k)$ とすると $k\cap\mathbf{Q}(\zeta_p)=\mathbf{Q}$ より

$$\mathrm{Gal}(K/k)=\mathrm{Gal}(k\mathbf{Q}(\zeta_p)/k)\cong\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\cong(\mathbf{Z}/p)^{\times}$$

となる。ここで，E_K を K の単数群，$\mathrm{Z}^1(K/k, E_K)$ を 1 次元の cocycle group すなわち

$$\mathrm{Z}^1(K/k, E_K)=\{u_\sigma\in E_K : u_{\sigma\tau}=u_\sigma u_\tau^{\sigma},\ \sigma,\tau\in\Delta\}$$

とする。この cocycle $u=\{u_\sigma\}$ と K の元 θ に対して $g(u,\theta)$ を次のように定義する。

$$g(u,\theta)=\sum_{\sigma\in\Delta}u_\sigma\theta^{\sigma}$$

ここで，χ を値域が k に含まれるような Δ の指標とすると，χ は $\mathrm{Z}^1(K/k, E_K)$ の元であり，$g(\chi, \zeta_p)$ は通常の Gauss の和に一致する。Gauss の和の場合と同様に，K の p 上の素イデアルを $\wp$，$k\cap\wp=\mathbf{p}$ とする。素イデアル $\mathbf{p}$ は K で完全分岐するので，任意の $v\in E_K$，$\sigma\in\Delta$ に対して

$$v^{\sigma}\equiv v \mod \wp$$

となるから，$u=\{u_\sigma\}\in\mathrm{Z}^1(K/k, E_K)$ に対して

$$u_{\sigma\tau}\equiv u_\sigma u_\tau \mod \wp$$

より，$u_\sigma \bmod \wp$ は $\mathrm{Hom}(\Delta, R/\wp)\cong\mathrm{Hom}((\mathbf{Z}/p)^{\times}, R/\wp)$ の元となる。従って，$\wp$ に対応する Teichmüller $\omega=\omega_\wp$ と整数 m $(0\le m<p-1)$ が存在し

$$u_\sigma\equiv\omega^{-m}(\sigma) \mod \wp$$

と表すことができる。以下，この関係式を

$$u\equiv\omega^{-m} \mod \wp$$

と書くことにする。

定理 3.1 cocycle $u=\{u_\sigma\}\in\mathrm{Z}^1(K/k, E_K)$ が合同式 $u\equiv\omega^{-m} \mod \wp$ を満たすならば，

$$g(u,\theta)=0$$

または,

$$\mathrm{ord}_{\wp} g(u,\theta) \equiv m \mod p-1$$

である。

証明) $\tau \in \mathrm{Gal}(K/k)$ とすると, $g(u,\theta)$ への作用は

$$g(u,\theta)^{\tau} = \sum_{\sigma \in Gal(K/k)} u_{\sigma}^{\tau} \theta^{\sigma\tau} = \sum u_{\sigma\tau} u_{\tau}^{-1} \theta^{\sigma\tau} = u_{\tau}^{-1} g(u,\theta)$$

となる。ここで, $g(u,\theta) \neq 0$ であるならば, 仮定より

$$g(u,\theta)^{\tau-1} = u_{\tau}^{-1} \equiv \omega^{m}(\tau) \mod \wp$$

が成り立つ。k, K をそれぞれ素イデアル $\mathbf{p}$, $\wp$ で完備化したものを $k_{\mathbf{p}}$, $K_{\wp}$ とすると, $k_{\mathbf{p}} = \mathbf{Q}_p$, $K_{\wp} = \mathbf{Q}_p(\zeta_p)$ である。従って,

$$\mathrm{ord}_{\wp} g(u,\theta) = h$$

とすると, 命題 2.1 より

$$h \equiv m \mod p-1$$

である。これで, 定理 3.1 は証明された。

注意) 1. u を $Z^1(K/k, E_K)$ の元とすると, $g(u,\theta) \neq 0$ となる θ の存在はよく知られている。
2. $v \in E_K$ とすると, $u_{\sigma} v^{1-\sigma} \equiv u_{\sigma} \mod \wp$ より, $\mathrm{ord}_{\wp} g(u,\theta)$ は cocycle u の含まれる cohomology class に対して確定する。

4. Ideal annihilator

k を $\mathbf{Q}$ 上有限次 Galois 拡大, $G = \mathrm{Gal}(k/\mathbf{Q})$ とする。p は k 上完全分解する素数, $K = k(\zeta_p)$ とする。$u \in Z^1(K/k, E_K)$, $\tau \in \Delta = \mathrm{Gal}(K/k)$ とするとき,

$$g(u,\theta)^{\tau} = \sum_{\sigma \in \Delta} u_{\sigma}^{\tau} \theta^{\sigma\tau} = \sum_{\sigma \in \Delta} u_{\tau}^{-1} u_{\sigma\tau} \theta^{\sigma\tau} = u_{\tau}^{-1} g(u,\theta)$$

より, $g(u,\theta) \neq 0$ とすると単項イデアル $(g(u,\theta))$ は K/k で分岐するイデアルと k のイデアルの積となる。分岐するイデアルは p の上のイデアルだけであるから

$$(g(u,\theta)) = \mathfrak{J} \prod_{\wp | p} \wp^{n(\wp)}$$

と表すことができる。ここで, $\mathfrak{J}$ は p と素な k のイデアル, $n(\wp) \in \mathbf{Z}$ である。p 上のイデアル $\wp$ の指数 $n(\wp)$ は定理 3.1 により

$$u \equiv \omega_{\wp}^{-n(\wp)} \mod \wp$$

という合同式で定められる。u_{σ} は K の元なので, 直接 G の作用を考えることはできないが, cohomology class には Δ が trivial に作用し, さらに 3. の注意により上の合同式は class 内

の cocycle の選び方に依存しない。また，p 上のイデアルは K/k で分岐するので Δ は trivial に作用する。従って，上の合同式に G を作用させることができる。p 上のイデアル $\wp$ を一つ固定すると，p 上のイデアルは $\wp^{\gamma}(\gamma\in G)$ と表すことができる。いま，

$$u^{\gamma}\equiv\omega_{\wp}{}^{-n(\gamma)} \mod \wp$$

によって $n(\gamma)\ (0\le n(\gamma)<p-1)$ を定めると，

$$(g(u,\theta))=\mathfrak{I}\wp^{a(\mathbf{p},u)}$$

と表される。ここで，$\mathbf{p}=\wp\cap k$

$$a(\mathbf{p},u)=\sum_{\gamma\in G}n(\gamma)\gamma^{-1}$$

である。よって，$g(u,\theta)$ のノルムを考えることにより，次の定理が証明された。

定理 4.1 I_k, P_k をそれぞれ k のイデアル群，単項イデアル群とすると，

$$\mathbf{p}^{a(\mathbf{p},u)}\in P_k I_k^{p-1}$$

が成立する。

$a(\mathbf{p},u)$ は，本質的にイデアル $\mathbf{p}$ に依存する。従って，k のイデアル類群の exponent が $p-1$ の約数であっても $\mathbf{p}$ を含む類以外を零化するかどうかはわからない。$\mathbf{p}$ に依存しないものが得られるならば，イデアル類群全体を零化することになる。以下述べる Stickelberger element の場合はそのような例となっている。

$m=p-1$(p を奇素数とする)とし，また，m が 4 で割り切れない場合 $f=\dfrac{m}{2}$，その他は $f=m$ とする。体 K，k をそれぞれ $k=\mathbf{Q}(\zeta_f)$，$K=k(\zeta_p)$ とする。K/k は Kummer 拡大となるので k の元 α が存在し $K=k(\sqrt[f]{\alpha})$ と表すことができる。ここで，χ を α に対応する Kummer character とする。即ち，

$$\chi(\sigma)=\left(\sqrt[f]{\alpha}\right)^{\sigma-1}\qquad \sigma\in \mathrm{Gal}(K/k)$$

とする。χ は exponent が m であるから，$Z^1(K/k, E_K)$ の元となる。さらに，$g(\chi,\zeta_p)$ は 0 にならないことが知られているので，$g(\chi,\zeta_p)$ の素イデアル分解から annihilator が構成できる。$\mathrm{Gal}(k/\mathbf{Q})$ と $(\mathbf{Z}/f)^{\times}$ との同型写像を

$$\zeta^{\sigma_a}_f=\zeta^{a}_f$$

で定めると，cocycle χ への $\mathrm{Gal}(k/\mathbf{Q})$ の作用は

$$\chi^{\sigma_a}=\chi^a$$

となり，χ に対応する annihilator は

$$a(\mathfrak{p},\chi)=\sum_{a=1}^{p-1} a\sigma_a^{-1}$$

である。もちろん，これが Stickelberger element である。

次に円単数からの構成法を示す。記号を多少変更して，l を f を割る奇数，

$k=\mathbf{Q}(\zeta_l)$，$K=k(\zeta_p)$，$\varepsilon=\zeta_p\zeta_l-1$ とすると，

$$N_{K/k}(\varepsilon)=\frac{\zeta_l^{p}-1}{\zeta_l-1}=1$$

より，ε に対応する cocycle $u\in Z^1(K/k, E_K)$ が存在する。K の素数 p 上の素イデアルの 1 つを $\wp$ とすると，

$$\varepsilon\equiv\zeta_l-1 \mod \wp$$

となる。ここで，$\wp$ で定まる Teichmüller character を ω，$\mathrm{Gal}(K/k)$ の生成元を σ とすると，

$$\varepsilon\equiv\zeta_l-1\equiv\omega^h(\sigma) \mod \wp$$

となる整数 h が m を法として定まる。このとき，$u\equiv\omega^h \mod \wp$ である。このようにして定まる h を $l(\zeta_l-1,\sigma,\wp)$ と書くことにすると，

$$\sum_{\tau\in Gal(k/\mathbf{Q})} l(\zeta_l^{\tau}-1,\sigma,\wp)\tau^{-1}$$

が $\mathfrak{p}=\wp\cap k$ の annihilator となる。また，$\mathrm{Gal}(K/k)$ の生成元の取り方を変えると $\mathbf{Z}/m$ の単数倍となるだけであるから，記号を簡単にして

$l(\zeta_l-1,\sigma,\wp)=l(\zeta_l-1,\mathfrak{p})$ とすると

$$\eta(\zeta_l,\mathfrak{p})=\sum_{a\in(\mathbf{Z}/l)^{\times}} l(\zeta_l^{a}-1,\mathfrak{p})\sigma_a^{-1}$$

が $\mathfrak{p}$ の annihilator となる。即ち，

$$\mathfrak{p}^{\eta(\zeta_l,\mathfrak{p})}\in I_k^{p-1}P_k$$

が成り立つ。ただし，$\eta(\zeta_l,\mathfrak{p})$ の係数は $\mathbf{Z}/m$ なので，$\mathbf{Z}$ に持ち上げて作用させるものとする。

$l(\zeta_l-1,\mathfrak{p})$ は k の $\mathfrak{p}$-unit に対して定義することができる。$R=R_k$ を k の整数環とすると，$R/\mathfrak{p}$ の乗法群は $\omega(\sigma) \mod \mathfrak{p}$ で生成される巡回群であることから，β を $\mathfrak{p}$-unit とすると，$h=l(\beta,\mathfrak{p})$ を

$$\beta\equiv\omega^h(\sigma) \mod \mathfrak{p}$$

で定まるものと定義する。即ち，k の $\mathbf{p}$-unit から $\mathbf{Z}/m$ への準同型である。次の各等式は，容易に証明される。本質的には初等整数論で出てくる，原始根を底としたときの指数 Ind と同じである [T] 。

1. $l(\alpha\beta, \mathbf{p}) = l(\alpha, \mathbf{p}) + l(\beta, \mathbf{p})$　α, β は $\mathbf{p}$-unit
2. $l(\alpha^r, \mathbf{p}) = r\, l(\alpha, \mathbf{p})$　　$r \in \mathbf{Z}$
3. $l(\alpha, \mathbf{p}) = l(\beta, \mathbf{p}) \iff \alpha \equiv \beta \mod \mathbf{p}$

また，k の $\mathbf{p}$ による完備化を $k_{\mathbf{p}}$，$k_{\mathbf{p}}$ の単数群を U とおくと，上の $l(\alpha, \mathbf{p})$ は U からの写像とすることができる。

ここで，更に l を奇素数とすると k は l–分体となる。$E = E_k$ を k の単数群，$C = C_k$ を円単数で生成される E の部分群とする。即ち，C は E の有限位数の部分群で，次のような単数で生成されている。

$$\left\{ \frac{\zeta_l^{\,a}-1}{\zeta_l-1} : a \in (\mathbf{Z}/l)^{\times} \right\}$$

$N = l^t$ を $t > \mathrm{ord}_l(E:C)$ となるように十分大きくとると，E/CE^N と E/C の l–Sylow 群は同型となる。E/CE^N は l–群であるから，$\mathbf{Z}_l[\mathrm{Gal}(k/\mathbf{Q})]$–module と考えると，次のように直交分解される。

$$E/CE^N = \bigoplus_{\chi} E(\chi)$$

ここで，χ は $\mathrm{Gal}(k/\mathbf{Q})$ の $\mathbf{Z}_l^{\times}$ への指標で，$E(\chi)$ は

$$E(\chi) = \{\eta \in E/CE^N : \eta^{\sigma} = \eta^{\chi(\sigma)}\}$$

である。特に，$\chi \neq$ 単位指標, χ(複素共役) $= 1$ とすると，次の各巡回群の生成元が取れる。

$$\varepsilon \in E(\chi), \quad u = \prod_{\sigma \in Gal(k/Q)} (\zeta_l^{\sigma}-1)^{\chi^{-1}(\sigma)} \in E(\chi) \cap CE^N/E^N$$

従って 整数 $h = h(\chi)$ が存在し，$\varepsilon^h = u$ 即ち，ε の代表元を ε_1 とすると，

$$\varepsilon_1^h \equiv \prod_{\sigma} (\zeta_l^{\sigma}-1)^{\chi^{-1}(\sigma)} \mod E^N$$

という関係式が成立する。記号の乱用となるが，$s = \mathrm{ord}_l\ m$ のとき $l(\ \ , \mathbf{p})$ と自然な写像

$$\mathbf{Z}/m \longrightarrow \mathbf{Z}/l^s$$

との合成を $\mathrm{Ind}_l(\ \ , \mathbf{p})$ とすると，

$$h\mathrm{Ind}_l(\varepsilon_1, \mathbf{p}) = \sum_{\sigma} \chi^{-1}(\sigma)\mathrm{Ind}_l(\zeta_l^{\sigma}-1, \mathbf{p}) + N\mathrm{Ind}_l(\kappa, \mathbf{p})$$

となる。ここで，$\kappa \in E$ である。$\mathrm{ord}_l N > \mathrm{ord}_l m$ となるようにとると，

$$h\mathrm{Ind}_l(\varepsilon_1, \mathbf{p}) = \sum_{\sigma} \chi^{-1}(\sigma)\mathrm{Ind}_l(\zeta_l^{\sigma} - 1, \mathbf{p})$$

となり，実の二次体の類数公式のような関係式が導かれる。右辺は

$\mathbf{Z}/l^s[\mathrm{Gal}(k/\mathbf{Q})]$ の元

$$\sum_{a\in(\mathbf{Z}/l)^{\times}} \mathrm{Ind}_l(\zeta_l^{a}-1, \mathbf{p})\sigma_a^{-1}$$

の，χ–成分である。もちろんこの元は，イデアル類群の l-Sylow 群に作用させた場合，annihilator

$$\eta(\zeta_l, \mathbf{p}) = \sum_{a\in(\mathbf{Z}/l)^{\times}} l(\zeta_l^{a}-1, \mathbf{p})\sigma_a^{-1}$$

と同じ作用となる。これで，Thaine [Th] の annihilator を explicit な形での構成が完了し，単数群の index との関係が明らかになった。

5．まとめ

いままでの記号をそのまま使用して大ざっぱにまとめると，次のようになる。円分体 $\mathbf{Q}(\zeta_l)$のイデアル類群の l-Sylow 群の –eigenspace A^- の annihilator は

$$\sum_{a=1}^{l-1} \mathrm{Ind}_l(\zeta_l^{a}, \mathbf{p})\sigma_a^{-1} = \sum_{a=1}^{l-1} a\sigma_a^{-1}$$

であり，+eigenspace A^+ の annihilator は

$$\sum_{a=1}^{l-1} \mathrm{Ind}_l(\zeta_l^{a}-1, \mathbf{p})\sigma_a^{-1}$$

となる。A^- の場合は，うまい具合に素イデアル $\mathbf{p}$ に依存しない形になっていることがわかる。ただ，共に単数群から導かれているにもかかわらず、微妙に様子が異なっている。例えば，A^+ の場合は annihilator は円単数から導かれ，A^+ と E/C の l-Sylow 群の各 χ–component の位数が等しいことが知られているが[M-W]，A^- の場合はそのような対象を単数群から見いだすことはできない。統一的な annihilator にはもう一歩先があるような気がする。

参考文献

[L-T] J. Lubin and J. Tate, Formal complex multiplication in local fields, Ann. of Math. 8(1965) pp. 380-387

[M-W] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**, Invent. Math. 76 (1984) pp. 179-330

[R] K. Rubin, The Main Conjecture, (S.Lang, Cyclotomic Fields Ⅰ and Ⅱ, Combined Second Edition, Springer-Verlag, 1990, Appendix)

[T] 高木貞治，初等整数論講義，共立出版

[Th] F. Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. 128(1988) pp. 1 -18

［1996 年 10 月 30 日　受理］