数理解析研究所講究録 1376 巻 2004 年 20-31

Special elements and locally trivial cocycles in Iwasawa theory

広島大学・総合科学部　隅田 浩樹 (Hiroki Sumida-Takahashi)
Faculty of Integrated Arts and Sciences
Hiroshima University

1. Introduction

本稿のテーマについて文献をさかのぼってみると、岩澤健吉氏の1959年の論文[12, p.556]に以下のような記述を見つけることができる。氏が岩澤理論を創始された当初から、これらの問題に興味を持っておられたことが分かる。

"However, this last statement, on the rank of $\overline{E}_{n,0}$ is yet unproved, though it looks quite likely to be true. ⋯ (中略) ⋯ *It is also yet unknown whether or not ${}^iA(L/F)$ is regular for every even index i."*

ここで、pは素数、$F_n = \mathbf{Q}(\zeta_{p^{n+1}})$ (ζ_mは1の原始m乗根)、E_nをF_nの単数群、$F_{n,\mathfrak{p}_n}$をF_nのp上の唯一の素点$\mathfrak{p}_n$での完備化、$U_{n,0}$を$F_{n,\mathfrak{p}_n}$の主単数群、自然な埋め込み写像$d_n : F_n \hookrightarrow F_{n,\mathfrak{p}_n}$とするとき、$\overline{E}_{n,0}$は$d_n(E_n) \cap U_{n,0}$の$U_{n,0}$内における閉包である。また、$F = \cup_n F_n$、$L$を$F$上の最大不分岐アーベル$p$拡大とするとき、${}^iA(L/F)$はいわゆるΔ分解による$\mathrm{Gal}(L/F)$の$i$部分の指標群とする。さらに$A$が$n$-regularとは、$\Gamma_n = \mathrm{Gal}(F/F_n)$の位相生成元$\gamma_n$に対し$(\gamma_n - 1)A = A$となることであり、regularとは任意の$n$に対し$n$-regularであることをいう。

まず、最初の文は、次のLeopoldt予想に関する記述である。

Leopoldt予想　$\mathrm{rank}_{\mathbf{Z}} E_n = \mathrm{rank}_{\mathbf{Z}_p} \overline{E}_{n,0}$.

円分体の場合は、Bakerの定理のp進版の手法でAx氏[1], Brumer氏[2]により肯定的に解決された。このことと類体論によって、KをFの最大pの外不分岐アーベルp拡大とするとき、$A(K/F)$がregularであることが従う。

一方、後半の文は、未解決予想である次のVandiver予想とGreenberg予想に関連付けることができる。$F_n^+ = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$($F_n$の最大実部分体) とおく。

Vandiver予想　F_n^+の類数はpで割れない。(F_0^+の類数がpで割れなければ十分。)
$\Longleftrightarrow$　全ての偶数iに対し、${}^iA(L/F)$は自明である。

Greenberg予想　F_n^+の類数のp部分は$n \to \infty$で有界である。
$\Longleftrightarrow$　全ての偶数iに対し、${}^iA(L/F)$は有限である。

イデアル類群の有限性と類体論より、$A(L/F)$ が regular であることと $A(L/F)$ が p 可除加群であることは同値である。j が奇数のときは ${}^jA(L/F)$ は p 可除なので、偶数 i に対し ${}^iA(L/F)$ が p 可除かどうかが問題となっている。各々の p については、3つの可能性が考えられる。

・Vandiver 予想、従って Greenberg 予想も成立し、$A(L/F)$ は regular である。
・Vandiver 予想が不成立だが Greenberg 予想は成立し、$A(L/F)$ は regular ではない。
・Vandiver 予想、Greenberg 予想ともに不成立となる。$A(L/F)$ が regular かどうかはこの2つの予想からは決まらない。

$M(i)$ で M の i 回の Tate twist を表すことにする。コホモロジー群 $H^1(G_{\mathbf{Q}_\infty}, \mathbf{Q}_p/\mathbf{Z}_p(i))$ の言葉を用いると、${}^iA(K/F)$ は p の外 locally trivial cocycle の集合、${}^iA(L/F)$ は p も含めた locally trivial cocycle の集合と対応をつけることができる。次節に述べるように、一般に locally trivial cocycle はコホモロジー群の岩澤加群としての構造、特にねじれ加群に大きな影響を及ぼす。本稿のテーマは、大域体と局所体のガロア群の差異をあらわす非自明な locally trivial cocycle を、いかにして系統的かつ効率的に見つけるかということである。この節の最初に引用した岩澤氏の文章は次のように続いており、研究のヒントになっているのではないだろうか。

"Thus the regularity of the modules $A(K/F)$ and $A(L/F)$ (and also many important arithmetic properties of the cyclotomic fields F_n $(n \geq 0)$) essentially depends upon the structure of the G-group E, the group of units of the field F. But we leave the study of the structure of E to a future publication and mention here only the following fact: Let E^+ denote as before, the group of real units in E and E' the subgroup of E^+ generated by the so-called circular units. ⋯ "

注 以降の節では、この節における記号を必ずしも用いていない。

2. General setting

k を有限次代数体とし、$\mathrm{Gal}(\overline{k}/k)$ が連続に作用する $A \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^d$ に対し、$T = \varprojlim A[p^n]$、$V = T \otimes \mathbf{Q}_p$ とする。S は p, ∞ 上と $k(A)/k$ で分岐する k の全ての素点を含む集合とし、以下 S は有限集合であると仮定する。k_S を k 上最大 S の外不分岐な拡大として、$G = \mathrm{Gal}(k_S/k)$ とおく。k_∞ を $k \subseteq k_\infty \subseteq k_S$ となる k 上の p 進 Lie 拡大とし、$\Gamma = \mathrm{Gal}(k_\infty/k)$ とおく。k_n を $k \subseteq k_n \subseteq k_\infty$ であって、$G_n = \mathrm{Gal}(k_S/k_n)$ が $\cap_n G_n = G_\infty$ を満たすとき、次の Jannsen 氏のスペクトル系列が得られる [15, 20]。

$$E_2^{p,q} = E^p(H^q(G_\infty, A)^\vee) \Rightarrow \varprojlim H^{p+q}(G_n, T).$$

ただし、$M^\vee = \mathrm{Hom}_{\mathbf{Z}_p}(M, \mathbf{Q}_p/\mathbf{Z}_p)$。この系列から以下の完全系列が得られる。

$$0 \longrightarrow E^1(H^0(G_\infty, A)^\vee) \longrightarrow \varprojlim H^1(G_n, T) \longrightarrow E^0(H^1(G_\infty, A)^\vee)$$
$$\longrightarrow E^2(H^0(G_\infty, A)^\vee) \longrightarrow (\varprojlim H^2(G_n, T))' \longrightarrow E^1(H^1(G_\infty, A)^\vee)$$
$$\longrightarrow E^3(H^0(G_\infty, A)^\vee) \longrightarrow 0.$$

ここで、$\Lambda = \mathbf{Z}_p[[\Gamma]]$, $E^i(M) = \mathrm{Ext}^i_\Lambda(M, \Lambda)$, $(\varprojlim_{\leftarrow} H^2(G_n, T))' = (\mathrm{Ker} : \varprojlim_{\leftarrow} H^2(G_n, T) \to E^0(H^2(G_\infty, A)^\vee))$ である。また、Poitou-Tate 氏らの双対系列より、以下の完全系列が得られる。

$$0 \longrightarrow \varprojlim P^0(G_n, T) \longrightarrow H^2(G_\infty, A^*)^\vee$$
$$\longrightarrow \varprojlim H^1(G_n, T) \longrightarrow \varprojlim P^1(G_n, T) \longrightarrow H^1(G_\infty, A^*)^\vee$$
$$\longrightarrow \varprojlim H^2(G_n, T) \longrightarrow \varprojlim P^2(G_n, T) \longrightarrow H^0(G_\infty, A^*)^\vee \longrightarrow 0.$$

ここで、$P^i(G_n, M) = \bigoplus_{v \in S}(\prod_{\eta|v} H^i(G_{n,\eta}, M))$,
$A^* = V^*/T^* = (\mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p(1)) \otimes \mathbf{Q}_p)/\mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p(1))$ である。

以下、$\Gamma \simeq \mathbf{Z}_p$ の場合 を考察する。この場合、M を有限生成 Λ 加群とするとき、$E^i(M)$ は以下のような対象に概ね対応している [14]。
$E^0(M) \longleftrightarrow \Lambda^{\mathrm{rank}_\Lambda M}$
$E^1(M) \longleftrightarrow \mathrm{tor}_\Lambda M + (\Lambda^{\mathrm{rank}_\Lambda M}$ と $M/\mathrm{tor}_\Lambda M$ との差)
$E^2(M) \longleftrightarrow M$ の最大有限 Λ 部分加群
$E^i(M) = 0 \quad (i \geq 3)$

まず、$H^1(G_\infty, A)$ の Λ-加群としての corank は、Euler-Poincaré 指標の計算により

$$\mathrm{corank}_\Lambda(H^1(G_\infty, A)) = r_2(k)d + \sum_{v:\mathrm{real}} d_v^- + \mathrm{corank}_\Lambda(H^2(G_\infty, A))$$

で与えられる [8]。ただし、$r_2(k)$ は k の虚素点の個数であり、k の実素点 v に対し v 上の複素共役元の作用により V を V^+ と V^- に分解し $d_v^\pm = \dim_{\mathbf{Q}_p} V^\pm$ としている。さらに、次の予想がある [7]。

Weak Leopoldt 予想 $H^2(G_\infty, A) \to P^2(G_\infty, A)$ は同型。

以下、この予想を A と A^* に対して仮定 する。すると、局所的な情報によって corank を表すことができる。

$$\mathrm{corank}_\Lambda(H^1(G_\infty, A)) = r_2(k)d + \sum_{v:\mathrm{real}} d_v^- + \mathrm{corank}_\Lambda(P^2(G_\infty, A)).$$

なお、k_∞/k で無限分解する有限素点があるとき、$\mathrm{corank}_\Lambda(P^2(G_\infty, A)) > 0$ となる場合があることに注意する。また、上の 2 つの完全系列と Weak Leopoldt 予想から

$$\mathrm{corank}_\Lambda(H^1(G_\infty, A)) = \mathrm{rank}_\Lambda(\varprojlim H^1(G_n, T)) = \mathrm{rank}_\Lambda(\mathrm{Ker} : \varprojlim P^1(G_n, T) \to H^1(G_\infty, A^*)^\vee)$$

$$= \mathrm{corank}_\Lambda(\mathrm{Coker}: H^1(G_\infty, A^*) \to P^1(G_\infty, A^*)).$$

さらに簡単のため、$\mathrm{corank}_\Lambda(P^2(G_\infty, A)) = 0$ を仮定する。$H^1(G_\infty, A)^\vee$ の Λ-torsion は、第一の完全系列からほぼ $\varprojlim H^2(G_n, T)$ に対応し、さらに第二の完全系列から以下の 2 つの加群に分けることができる。

$$\begin{aligned}(\mathrm{Im}: \varprojlim H^2(G_n,T) \to \varprojlim P^2(G_n,T)) &\simeq (\mathrm{Ker}: \varprojlim P^2(G_n,T) \to H^0(G_\infty, A^*)^\vee) \\ &\simeq (\mathrm{Coker}: H^0(G_\infty, A^*) \to P^0(G_\infty, A^*))^\vee.\end{aligned}$$

$$\begin{aligned}(\mathrm{Ker}: \varprojlim H^2(G_n,T) \to \varprojlim P^2(G_n,T)) &= (\mathrm{Im}: H^1(G_\infty, A^*)^\vee \to \varprojlim H^2(G_n,T)) \\ &\simeq (\mathrm{Coker}: \varprojlim P^1(G_n,T) \to H^1(G_\infty, A^*)^\vee) \\ &\simeq (\mathrm{Ker}: H^1(G_\infty, A^*) \to P^1(G_\infty, A^*))^\vee.\end{aligned}$$

一般に、後者の locally trivial な $H^1(G_\infty, A^*)$ の元を計算することは難しく、従って $H^1(G_\infty, A)^\vee$ の岩澤加群としての構造を決定することも難しい。次節以降では、k_∞ が $\mathbf{Q}$ の円分 $\mathbf{Z}_p$-拡大 $\mathbf{Q}_\infty$, even Dirichlet 指標 χ, $A = (\mathbf{Q}_p/\mathbf{Z}_p)(\chi)(i)$ という classical な場合に、どのようにしてこの群を調べるのかを述べたい。

3. Classical case

3.1. **Abelian extensions.** p を奇素数、$\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$ を以下固定する。χ を even Dirichlet 指標 ($\chi(-1) = 1$) とし、$k = k_\chi$ (χ に対応する実アーベル体) とする。$\omega = \omega_p$ を Teichmüller 指標とし、簡単のため、以下を仮定する。

(C1) $\quad k \cap \mathbf{Q}(\zeta_p) = \mathbf{Q} \quad$ and $\quad |\mathrm{Gal}(k/\mathbf{Q})|$ divides $p-1$.

S を $\mathbf{Q}_S \supset k(\zeta_p)$ となる $\mathbf{Q}$ の素点の集合とする。$G_\infty = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q}_\infty)$, $K = k(\zeta_p)$ とおき、$H_\infty = \mathrm{Gal}(\mathbf{Q}_S/K_\infty)$, $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ とする。$A = (\mathbf{Q}_p/\mathbf{Z}_p)(\chi)(i)$ (ガロア群の元 σ が $\chi(\sigma)\chi_{cycl}(\sigma)^i$ で作用) に対し、inflation-restriction 写像により、次の完全系列が得られる。

$$0 \longrightarrow H^1(\Delta, A^{H_\infty}) \longrightarrow H^1(G_\infty, A) \longrightarrow H^1(H_\infty, A)^\Delta \longrightarrow H^2(\Delta, A^{H_\infty}).$$

ここで、Δ の位数は p と素であるから、$H^1(G_\infty, A) \simeq H^1(H_\infty, A)^\Delta$ となる。Δ の指標 ψ に対し $e_\psi = \frac{1}{|\Delta|}\sum_{\delta\in\Delta}\psi(\delta)\delta^{-1} \in \mathbf{Z}_p[\Delta]$ と定める。$Z_\infty = (H_\infty/\overline{[H_\infty, H_\infty]}$ の pro-p 商) とおき、Δ-分解 $Z_\infty = \bigoplus e_\psi Z_\infty = \bigoplus Z_\infty^\psi$ と書くことにする。ここで、H_∞ は A に自明に作用するから、$i' \equiv i \bmod (p-1)$, $1 \le i' \le p-1$ として、

$$\begin{aligned}H^1(G_\infty, A) \simeq H^1(H_\infty, A)^\Delta &= \mathrm{Hom}_\Delta(Z_\infty, A) \\ &= \mathrm{Hom}_{\mathbf{Z}_p}(Z_\infty^{\chi\omega^{i'}}, A) = (Z_\infty^{\chi\omega^{i'}})^\vee(\chi)(i).\end{aligned}$$

このようにコホモロジー群を "素点の分岐に関する制限付きアーベル拡大のガロア群" を用いて表すことができる。以下、ガロア群の言葉で述べることにする。

M_∞^S を K_∞ 上最大 S の外不分岐アーベル p 拡大、M_∞ を K_∞ 上最大 p の外不分岐アーベル p 拡大、L_∞ を K_∞ 上最大不分岐アーベル p 拡大、L'_∞ を K_∞ 上全ての素点が完全分解する最大アーベル p 拡大とする。$Z_\infty = \mathrm{Gal}(M_\infty^S/K_\infty)$ であり、$Y_\infty = \mathrm{Gal}(M_\infty/K_\infty)$、$X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$、$X'_\infty = \mathrm{Gal}(L'_\infty/K_\infty)$ とおく。

ある素点に対する restriction 写像で trivial となる cocycle から生成される部分群に対応する拡大体では、その素点がその拡大において完全分解しており、逆のことも言える。さらに、$\mathbf{Q}_\infty$ において p 上以外の素点は剰余体の素体上の拡大次数が p^∞ となっていることに注意すると、完全分解であることと不分岐であることは一致する。さらに $\psi = \chi\omega^i$ に対し、以下を仮定する。

$$\text{(C2)} \qquad \psi(p) \neq 1 \quad \text{and} \quad \psi^*(p) = \psi^{-1}\omega(p) \neq 1.$$

前半の条件から p 上の素イデアルからのイデアル類群の (p,ψ)-部分への寄与は自明となる。そのため、$X_\infty^\psi \simeq X'^\psi_\infty$ が成立し、X_∞^ψ が目標の群となる。

$\psi = \chi\omega^i$ に対し i が奇数ならば、Mazur-Wiles 氏らによって証明された岩澤主予想によって、久保田-Leopoldt 氏らが構成した p 進 L 関数 $L_p(s,\psi^*)$ から定まる岩澤多項式により、X_∞^ψ の Λ 加群としての構造をほぼ記述できる [18]。たとえば、その次数は X_∞^ψ の $\mathbf{Z}_p$-rank を意味する。一方、$\psi = \chi\omega^i$ に対し i が偶数のときは、それほど容易ではない。この場合も岩澤主予想により $L_p(s,\psi)$ から定まる岩澤多項式により Y_∞^ψ の構造をほぼ記述できるが、目標の X_∞^ψ はその商である。Greenberg 予想はこの商が有限、正確に述べると Y_∞^ψ 内の p 上の素点の分岐群たちの合成が指数有限であることを意味している。

3.2. **Special elements and a criterion.** 自明でない偶指標 ψ の conductor を f とし、$f_0 = \mathrm{l.c.m}(f,p)$, $f_n = f_0 p^n$ とおく。さらに、$F_n = \mathbf{Q}(\zeta_{f_n}) \supseteq K_n = K\mathbf{Q}_n \supset k_n = k\mathbf{Q}_n$ とする。ただし、$\mathbf{Q} \subseteq \mathbf{Q}_n \subseteq \mathbf{Q}_\infty$ で $[\mathbf{Q}_n : \mathbf{Q}] = p^n$ であるものとする。$\Gamma = \mathrm{Gal}(K_\infty/K)$ の位相生成元 γ_0 としてすべての n に対して $\zeta_{f_n}^{\gamma_0} = \zeta_{f_n}^{1+f_0}$ となるものとし、対応 $\gamma_0 \leftrightarrow 1+T$ により完備群環 $\mathbf{Z}_p[[\Gamma]]$ と形式べき級数環 $\Lambda = \mathbf{Z}_p[[T]]$ の位相同型対応を得て、$\mathbf{Z}_p[[\Gamma]]$-加群を Λ-加群とみなすことができる。$A_n = A_n(K)$ を K_n のイデアル類群の p 部分とする。ψ を $\mathrm{Gal}(K/\mathbf{Q})$ の指標で $\mathrm{Gal}(K/k)$ の元に対して自明であるとするとき、$p \nmid [K:k]$ より $N_{K_n/k_n} : A_n(K)^\psi \to A_n(k)^\psi$ は同型になることに注意する。我々の興味の対象は、$X_\infty^\psi = \varprojlim A_n^\psi$ (相対ノルムによる逆極限) という Λ-加群である。(類体論により $\mathrm{Gal}(L_\infty/K_\infty)^\psi$ と同型である。) ψ を Δ の偶指標とするとき、以下を満たす $G_\psi(T), G_\psi^*(T) \in \Lambda$ が unique に存在する [13]。

$$L_p(s,\psi) = G_\psi((1+f_0)^{1-s}-1), \quad L_p(s,\psi) = G_\psi^*((1+f_0)^s - 1) \quad \text{for all } s \in \mathbf{Z}_p.$$

p 進 Weierstrass の準備定理より、$G_\psi(T) = p^\mu g_\psi(T)u(T)$, $G_\psi^*(T) = p^\mu g_\psi^*(T)u^*(T)$ と表される。ここで、μ は非負整数、$g_\psi(T), g_\psi^*(T) \in \mathbf{Z}_p[T]$ は distinguished polynomial、$u(T), u^*(T) \in \Lambda^\times$ である。Ferrero-Washington 氏らの定理により、$\mu = 0$ が証明されている [4]。一般の場合の判定法を述べると煩雑になるので、ここでは次の条件をおく (cf. [19])。

$$\text{(C3)} \qquad g_\psi(T) = T - \alpha, \quad \alpha \in p\mathbf{Z}_p, \qquad \alpha \not\equiv 0,\ f_0 \bmod p^2$$

なお、このとき $g_\psi^*(T) = T - \alpha^*$, $\alpha^* = \frac{f_0 - \alpha}{1+\alpha}$ となる。この条件の下で、次を満たす多項式 $Y_n(T), Y_n^*(T) \in \mathbf{Z}[T]$ を定める。

$$Y_n(T) \equiv \frac{(1+T)^{p^n} - (1+\alpha)^{p^n}}{T - \alpha} \bmod p^{n+1}, \qquad Y_n^*(T) \equiv \frac{(1+T)^{p^n} - (1+\alpha^*)^{p^n}}{T - \alpha^*} \bmod p^{n+1}.$$

また、$\mathbf{e}_{\psi,n} \in \mathbf{Z}[\Delta]$ を $\mathbf{e}_{\psi,n} \equiv e_\psi \bmod p^{n+1}$ を満たし、係数和が 0 となるように定める。

Special element I: Circular unit

$$c_n = (N_{F_n/K_n}(1 - \zeta_{f_n}))^{\mathbf{e}_{\psi,n}} \in K_n^\times.$$

[10, 11] において以下の定理を得た。

定理 (市村-S) $0 \le x \le n+1$ に対し、

$$|A_n^\psi| \ge p^x \iff c_n^{Y_n(T)} \in (K_n^\times)^{p^x}$$

$$\iff \iota_{\mathfrak{L}}(c_n^{Y_n(T)}) \in (K_{n,\mathfrak{L}}^\times)^{p^x} \textit{ for every prime ideal } \mathfrak{L} \nmid p.$$

ただし、$\iota_{\mathfrak{L}} : K_n \hookrightarrow K_{n,\mathfrak{L}}$ は自然な inclusion である。

右辺下の circular unit の局所的な性質を調べることにより、$|A_n^\psi|$ の上界が得られる可能性がある。実際に、判別式が小さい実二次体 k、小さな素数 p に対して判定法を試したところ、調べた全ての範囲において $|A_n|$ の上界が得られた。しかしながら、あくまでこれは上界なので、厳密には A_n が自明かどうかも確定できない。

p と k_n の拡大次数が小さいときには、以下のような手法がある [17]。$G(X)$ を $\varepsilon = c_n^{Y_n(T)}$ に対する $\mathbf{Q}$ 上の最小多項式とする。もし ε が p^x 乗の元であるならば $\prod_{\sigma \in \mathrm{Gal}(K_n/\mathbf{Q})}(X - \sqrt[p^x]{\varepsilon^\sigma})$ の積を精密に計算すれば整数係数の多項式 $H(X)$ に近くなるはずである。そこで、$H(X)$ で $G(X^{p^x})$ を割り切ることができるならば ε の p^x 乗根の存在が確認される。しかしながら、この手法は p や k_n の拡大次数が大きいとき、$G(X), H(X)$ の係数が大きくなり実行が難しい。例えば、$p < 12,000,000$ まで Vandiver 予想が確かめられているが [3]、それより大きな素数で予想成立が怪しい例があったとしても、この方法で不成立の確認をするのはまず不可能であろう。また、実は Minkowski bound から有限個の素イデアル $\mathfrak{L}$ で上記の判定法を試せばよいのであるが、その数は膨大であり実用的ではない。以上のことを考慮に入れて、上記の判定法を基礎にし、円分体のもうひとつの特殊元である Gauss sum をさらに用いた判定法を与えた。

Special element II: Gauss sum $\tilde{\mathfrak{L}}$ を F_n の素イデアルとし、$\chi_{\tilde{\mathfrak{L}}} : (\mathcal{O}_{F_n}/\tilde{\mathfrak{L}})^\times \to \langle \zeta_{f_n} \rangle$, s.t. $\chi_{\tilde{\mathfrak{L}}}(y) \equiv y^{(N\tilde{\mathfrak{L}}-1)/f_n} \bmod \tilde{\mathfrak{L}}$ とする。($\mathcal{O}_{F_n}$ は F_n の整数環。)

$$g_n'(\tilde{\mathfrak{L}}) = -\sum_{y \in (\mathcal{O}_{F_n}/\tilde{\mathfrak{L}})^\times} \chi_{\tilde{\mathfrak{L}}}(y) \zeta_l^{Tr(y)}$$

と定める。K_n のイデアル $\mathfrak{A}$ に対し、$\mathfrak{A}\mathcal{O}_{F_n} = \prod_{i=1}^{r} \tilde{\mathfrak{L}}_i^{e_i}$ となるとき、$f' = f_0/p$ として

$$g_n(\mathfrak{A}) = \left(\prod_{i=1}^{r} g_n'(\tilde{\mathfrak{L}}_i)^{e_i} \right)^{f' \mathbf{e}_{\psi^*,n}} \in K_n^{\times}$$

と定める (cf. [9])。

定理 $0 \leq x \leq n+1$ に対し、

$$|A_n^{\psi}| \geq p^x \iff \iota_{\mathfrak{L}}(c_n^{Y_n(T)}) \in (K_{n,\mathfrak{L}}^{\times})^{p^x} \quad \textit{for a prime ideal } \mathfrak{L} \nmid p \textit{ s.t.}$$
$$(1)\ \mathfrak{L} \textit{ splits completely in } K_n/\mathbf{Q}, \textit{ and}$$
$$(2)\ \iota_{\mathfrak{L}^*}(g_0(N_{K_n/K_0}\mathfrak{L})) \notin (K_{0,\mathfrak{L}^*}^{\times})^p \textit{ for a prime ideal } \mathfrak{L}^* \nmid p\mathfrak{L}.$$

Chebotarev の密度定理より (1)(2) を満たす $\mathfrak{L}$ と $\mathfrak{L}^*$ が存在する。よって、右辺の局所的な条件を調べることにより、$|A_n^{\psi}|$ の正確な値を知ることができる。

証明の概略を以下に述べる。岩澤主予想と条件 (C1)(C2) から、求めたい A_n^{ψ} と $(\mathcal{E}_n/\mathcal{C}_n)^{\psi}$ の位数は一致する。ただし、E_n は K_n の単数群、C_n は circular unit のなす群、$\mathcal{E}_n = \overline{d_n(E_n) \cap U_{n,0}}$, $\mathcal{C}_n = \overline{d_n(C_n) \cap U_{n,0}}$ (Introduction と同様に定義) である。そこで、$c_n^{Y_n(T)}$ を用いて、$(\mathcal{E}_n/\mathcal{C}_n)^{\psi}$ の差を求める。これは、$c_n^{Y_n(T)}$ が大域的に何乗の元なのかで決まる。ここで、$c_n^{Y_n(T)}$ は、K_∞ において局所的には p^{n+1} 乗の元、$g_n(\mathfrak{L})^{Y_n^*(T)}$ は p の外では p^{n+1} 乗の元 (コホモロジー群では (p の外)locally trivial な元に対応) となっていることが重要である。すなわち、それぞれの元の p^{n+1}-乗根は不分岐拡大、p の外不分岐拡大に入っている。条件 (C3) からこれらの拡大は巡回拡大である。$\mathfrak{L}$, $\mathfrak{L}^*$ の Frobenius 写像がそれぞれのそれぞれのアーベル拡大のガロア群たちを生成すると仮定する。このとき、$c_n^{Y_n(T)}$, $g_n(\mathfrak{L})^{Y_n^*(T)}$ がそれぞれ大域的に何乗の元になっているかは、$\mathfrak{L}$, $\mathfrak{L}^*$ における局所的な情報と一致する。一方、類体論により、定理内の Gauss sum に関する条件は $\mathfrak{L}$, $\mathfrak{L}^*$ の Frobenius 写像がガロア群たちの生成元になっていることと同値である。以上により、circular unit, Gauss sum の局所的な情報から大域的な情報を導くことが示せる。

General setting においても、十分大きな体 K_n' で考えると $A[p^{n+1}]$ への作用は自明であり、locally trivial な cocycle の集合は不分岐アーベル拡大のガロア群から作られる加群のある商と対応する。K_n' の p の外不分岐なアーベル拡大は、単数とイデアル類群の元を用いて Kummer 拡大により表すことができる。そのため、いかに円分体におけるような理想的な状況ー explicit な元の存在ーを得ることができるかが、この方法での具体的な計算の鍵となる。

3.3. Computation of Gauss sums. 前小節の判定法における重要な点の1つは、$g_n(\mathfrak{L})$ を用いずとも $g_0(N_{K_n/K_0}\mathfrak{L})$ を用いるだけで十分ということである。これは、Λ-加群に関する中山の補題による。このことにより、計算すべき Gauss sum の共役元たちの個数が減少する。もう一つの重要な点は、その Gauss sum の共役元たちの $\mathfrak{L}^*$ を法とした値を Fast Fourier Transform を用いて高速に計算できるということである。これは、Gauss

sum が特殊な形をした大域元であることによる。以下、より詳しく $g_n(\mathfrak{L})^{Y_n^*(T)} \bmod \mathfrak{L}^*$ の計算方法を述べる。l (resp. l^*) を $l \equiv 1 \bmod f_n$ (resp. $l^* \equiv 1 \bmod f_n l$) となる素数、g (resp. g^*) をそれぞれの素数の原始根とする。s (resp. t) を $s \equiv g^{*(l^*-1)/f_n} \bmod l^*$ (resp. $t \equiv g^{*(l^*-1)/l} \bmod l^*$) をみたす整数とする。このとき、ある K_n のイデアル $\mathfrak{L}|l$ と $K_n(\zeta_l)$ のイデアル $\mathfrak{L}^*|l^*$ に対し、$s \equiv \chi_{\mathfrak{L}}(g) \bmod \mathfrak{L}^*$ かつ $t \equiv \zeta_l \bmod \mathfrak{L}^*$ となる。ここで、$Y_n^*(T) = \sum_{j=0}^{p^n-1} a_j(1+T)^j = \sum_{j=0}^{p^n-1} a_j \gamma_0^j, \quad a_j \in \mathbf{Z}$ とする。また、$\mathrm{Gal}(K_n/K_0)$ (resp. $\mathrm{Gal}(K_n/\mathbf{Q}_n)$) を $\mathrm{Gal}(K_n(\zeta_l)/K_0(\zeta_l))$ (resp. $\mathrm{Gal}(K_n(\zeta_l)/\mathbf{Q}_n(\zeta_l))$) と同一視する。さらに $\mathfrak{A}_n$ を $(\mathbf{Z}/f_n l\mathbf{Z})^\times$ の部分群で $\mathrm{Gal}(\mathbf{Q}(\zeta_{f_n l})/\mathbf{Q}_n(\zeta_l))$ に対応するものとする。$\mathrm{Gal}(\mathbf{Q}(\zeta_{f_n l})/\mathbf{Q}_n(\zeta_l))$ への元の拡張をとることにより、$\left(\sum_{\tau \in \mathrm{Gal}(\mathbf{Q}(\zeta_{f_n})/K_n)} \tau\right) \mathbf{e}_{\Psi^*,n} = \sum_{m \in \mathfrak{A}_n} b_m \tau_m, \quad b_m \in \mathbf{Z}$ と表す。このとき、Gauss sum は以下のように表される。

$$
\begin{aligned}
g_n(\mathfrak{L})^{Y_n^*(T)} &= \left(\prod_{j=0}^{p^n-1} \left(\prod_{m \in \mathfrak{A}_n} \left(- \sum_{y \in (\mathcal{O}_n/\mathfrak{L})^\times} \chi_{\mathfrak{L}}(y) \zeta_l^y \right)^{b_m \tau_m} \right)^{a_j \gamma_0^j} \right)^{f'} \\
&\equiv \left(\prod_{0 \le j < p^n,\, m \in \mathfrak{A}_n} \left(- \sum_{i=0}^{l-2} s^{m(1+f_0)^j i} t^{g^i} \right)^{b_m a_j} \right)^{f'} \bmod \mathfrak{L}^*.
\end{aligned}
$$

以上を計算するためには、次の Discrete Fourier Transform を計算できれば良い。

$$
F(w) = \sum_{0 \le v < z} \zeta_z^{wv} f(v) = \zeta_{2z}^{w^2} \sum_{0 \le v < z} \zeta_{2z}^{-(v-w)^2} (\zeta_{2z}^{v^2} f(v)).
$$

ただし、$0 \le w < z$, $z = f_n$ であり、$f(v) = \sum_{0 \le i \le l-2,\, i \equiv v \bmod f_n} t^{g^i}$ とする。ここで、$l^* \equiv 1 \bmod 2 f_n l$ を仮定すれば、

$$
\sum_{i=0}^{n'-1} a_i x^i \sum_{j=0}^{n'-1} b_j x^j = \sum_{k=0}^{n'-1} \left(\sum_{i=0}^{n'-1} a_{i \bmod n'} b_{(k-i) \bmod n'} \right) x^k \in (\mathbf{Z}/l^*\mathbf{Z})[x]/(x^{n'}-1),
$$

であるから、上記の convolution を多項式の乗算、あるいは整数の乗算を用いて計算できる。Fast Fourier Transform を繰り返し用いることにより、Schönhage-Strassen 氏らは 2 つの n-bit の自然数の乗算を $O(n \log n \log\log n)$ 回のステップで計算できることを示した (cf. [16, 4.3.3])。こういった方法により、十分なメモリを備えた計算機を用いれば、求めたい Gauss sum を高速に計算することができる。

4. Numerical examples

$k = \mathbf{Q}(\sqrt{D})$, $D > 0$ は k の判別式とする。χ_D を k に付随する非自明な Dirichlet 指標とする。$1 < D < 200$, $5 \le p < 10000$ の範囲で、$K = k(\zeta_p)$, $\psi = \chi_D \omega^i$, $A_n(K)^\psi$ に対する岩澤不変量 $\lambda_p(\psi)$, $\nu_p(\psi)$ を計算した。$\tilde{\lambda}_p(\chi_D \omega^i) := \deg(g_{\chi_D \omega^i}(T)) = \lambda_p(\chi_D \omega^{p-i})$ となることに注意する。$2 \le i \le p-3$ (i は偶数) の範囲では、(C2) を満たす $(p, \chi_D \omega^i)$ の個数は 171,981,262 であり、そのうち $\tilde{\lambda}_p(\chi_D \omega^i) = 1$ となるものは 37,140、$\tilde{\lambda}_p(\chi_D \omega^i) = 2$ となるものは 46、$\tilde{\lambda}_p(\chi_D \omega^i) = 3$ となるものは 1 あり、残りは $\tilde{\lambda}_p(\chi_D \omega^i) = 0$ となっている。(C2)(C3) を満たさないものや $i = 0$ となるものについても、p 単数を用いた Greenberg 予

想の判定法 (cf. [5, 6]) や本稿の定理の一般的な version を用いることにより、以下の結果を得た。

命題 $\lambda_p(\mathbf{Q}(\sqrt{D}, \zeta_p + \zeta_p^{-1})) = 0$ for all $1 < D < 200$ and $5 \leq p < 10000$.

$\tilde{\lambda}_p(\chi_D\omega^i) = 1$ かつ $\nu_p(\chi_D\omega^i) > 0$

D	p	i	D	p	i	D	p	i
12	701	542	21	199	150	33	53	30
37	43	32	53	1033	564	69	19	14
85	3697	3086	88	71	26	101	5333	2770
104	19	14	113	43	32	113	3373	1602
124	197	126	124	239	48	129	67	28
140	4751	120	141	5431	4826	149	43	32
149	71	16	149	229	182	157	401	56
161	101	22	168	37	22	172	73	10
173	7	4	173	43	32	173	101	42
177	17	6	181	71	52	181	6991	1628
185	827	354	188	1621	168	197	521	372

$\tilde{\lambda}_p(\chi_D\omega^i) = 2$

D	p	i	D	p	i	D	p	i
8	1151	842	21	11	4	24	29	4
24	181	84	29	569	64	37	5	2
37	89	66	37	3251	1094	40	257	232
44	653	448	53	193	14	56	1663	616
60	1277	582	60	1481	986	92	5	2
97	271	94	104	19	14	104	7919	4386
105	373	340	109	131	100	109	293	132
109	373	128	124	733	58	124	2111	1480
129	23	4	133	911	196	136	71	20
137	17	8	140	23	10	140	367	292
141	113	108	141	5939	2938	145	43	28
145	61	58	145	167	128	145	4157	3528
149	5	2	149	509	426	161	2389	646
165	11	2	172	13	10	172	47	38
173	7	4	177	157	48	181	223	26
185	17	6						

$\tilde{\lambda}_p(\chi_D\omega^i) = 3$

D	p	i	D	p	i
165	23	6	185	17	10

$\tilde{\lambda}_p(\chi_D\omega^i) = 1$ かつ $v_p(\alpha) = e > 1$

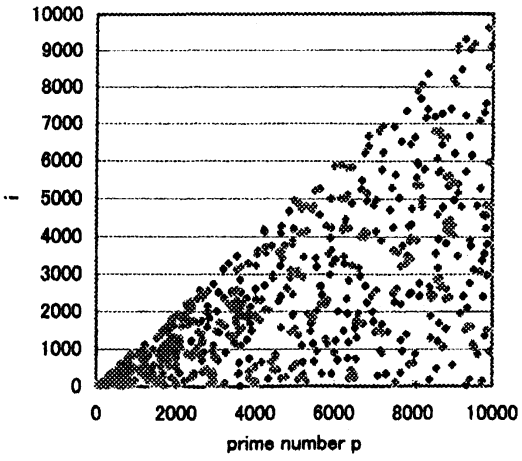
D	p	i	D	p	i	D	p	i
8	59	36	17	61	32	21	149	128
28	977	828	33	59	42	37	1091	812
41	7	4	41	283	102	44	787	148
53	7	2	53	1879	1158	57	2161	758
61	17	4	61	1747	1270	76	191	84
89	41	10	92	181	124	97	17	4
105	769	524	105	1453	162	120	2749	2196
124	41	30	140	107	74	149	797	140
149	2767	2178	152	17	12	168	43	10
173	13	4	177	31	24	184	373	72
193	7873	1886						

$\tilde{\lambda}_p(\chi_D\omega^i) = 1$ かつ $v_p(\alpha^*) = e^* > 1$

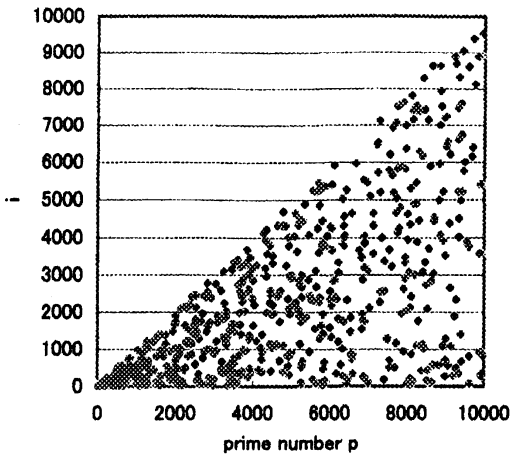
D	p	i	D	p	i	D	p	i
8	2221	1600	13	109	6	17	1319	88
28	223	126	33	31	24	33	1777	1184
41	19	12	41	421	126	60	19	14
61	7481	3516	73	11	2	73	1487	808
76	1451	418	76	4283	3484	97	367	26
109	41	32	133	1061	446	136	449	284
152	41	2	152	4027	3108	156	4637	2280
157	8221	582	165	29	26	165	89	66
165	1229	48	172	11	4	172	1487	900
177	337	74	184	1171	464	185	167	68
188	89	76						

$D = 1$ に対しては、$p < 12,000,000$ まで調べられたにもかかわらず、$\nu_p(\omega^i) > 0$ や $\lambda_p(\omega^i) > 1$ などの実例が得られなかった [3]。一方、D を上記の範囲で調べると、$p < 10,000$ の範囲でも上記の表の通りいくつかの実例が得られる。その個数は、Washington[21, pp.158–159] の naive な議論で予測された数とそれほど異ならない。ただし、素数がさらに大きい場合にどうなるかを予測することについては、まだ慎重にならざるを得ない。

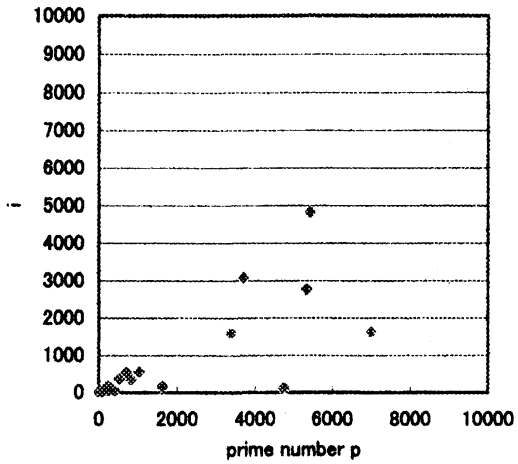
D=1, irregular prime numbers



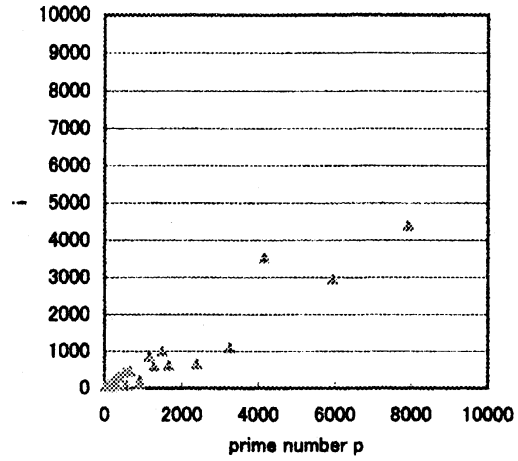
D=5



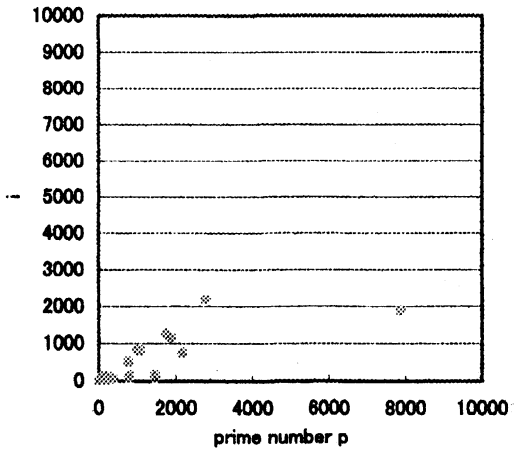
$\nu > 0$



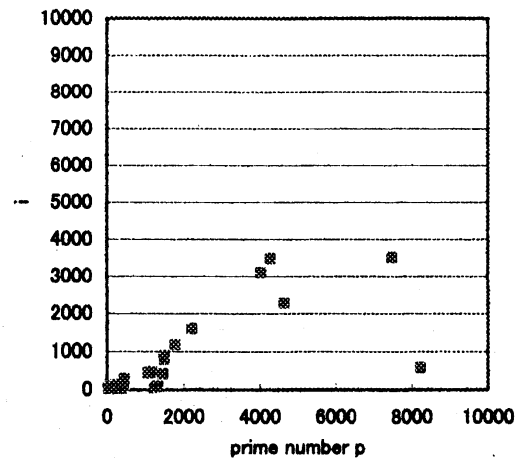
$\lambda > 1$



$\nu(\alpha) > 1$



$\nu(\alpha') > 1$



なお、$D=8, p=34,301, i=114$ に対し、$\nu_p(\chi_D\omega^i)>0$ という例がその後得られた。

今回は classical な対象に対してのみ計算しており、他のさまざまな対象に対する計算は今後の課題である。例えば、K 上の楕円曲線 E の p べき等分点を A とするとき、有理点 $E(K_n)$ のランクが十分大きければ、それらの有理点を用いて locally trivial cocycle が構成される。他にどのような寄与があり得るのかは、興味深い問題である。

References

1. J. Ax, *On the units of an algebraic number field*, Illinois J. Math. **9** (1965), 584–589.
2. A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.
3. J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and A. M. Shokrollahi, *Irregular primes and cyclotomic invariants to* 12 *million*, J. Symbolic Comput. **31** (2001), 89–96.
4. B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.
5. T. Fukuda and K. Komatsu, *On $\mathbf{Z}_p$-extensions of real quadratic fields*, J. Math.Soc.Japan **38** (1986), 95–102.
6. T. Fukuda and H. Taya, *The Iwasawa λ-invariants of $\mathbf{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), 277–292.
7. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
8. ———, *The structure of Selmer groups*, Proceedings Natl. Acad. of Science **94** (1997), 11125–11128.
9. H. Ichimura, *Local units modulo Gauss sums*, J. Number Theory **68** (1998), 36–56.
10. H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*, Internat. J. Math. **7** (1996), 721–744.
11. ———, *On the Iwasawa invariants of certain real abelian fields*, Tôhoku Math. J. **49** (1997), 203–215.
12. K. Iwasawa, *On the theory of cyclotomic fields*, Ann. of Math.,(2) **70** (1959), 530–561.
13. ———, *Lectures on p-adic L-functions*, Ann. of Math. Stud., vol. 74, Princeton Univ. Press: Princeton, N.J., 1972.
14. U. Jannsen, *Iwasawa modules up to isomorphism*, vol. 17, pp. 171–207, Algebraic number theory, Adv. Stud. in Pure Math., 17, 1989.
15. ———, *A spectral sequence for Iwasawa adjoints*, preprint http://www.mathematik.uni-regensburg.de/Jannsen/#Preprints (1994).
16. E. Knuth, *The art of computer programming, vol. 2: Seminumerical algorithms. 2nd edition*, Addison-Wesley Publishing Co., Reading, Mass,, 1981.
17. J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.
18. B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.
19. H. Sumida-Takahashi, *Computation of iwasawa invariants of certain real abelian fields*, J. Number Theory **105** (2004), 235–250.
20. O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. **4** (2002), 271–311.
21. L. Washington, *Introduction to cyclotomic fields. second edition*, Graduate Texts in Math., vol. 83, Springer-Verlag: New York, 1997.