数理解析研究所講究録
1154巻 2000年 1-9

The Iwasawa main conjecture and Gauss sums

都立大　青木 美穂 (Miho Aoki)

1 はじめに

p を奇素数とし, 以下固定する. $K/\mathbb{Q}$ を p が tamely ramified である虚な有限次 abel 拡大とし, $\Delta := \mathrm{Gal}(K/\mathbb{Q})$ とおく. K_∞/K を円分 $\mathbb{Z}_p$ 拡大, X を K_∞ の最大不分岐 abel pro-p 拡大の Galois 群とする. Iwasawa main conjecture は Δ の odd な指標 χ に対し, X の χ-part X_χ の特性イデアルが $\omega\chi^{-1}$ に付随する p 進 L 関数で書けることを主張している. ここで, $\omega : (\mathbb{Z}/p)^\times \to {\mathbb{Z}_p}^\times$ は Teichmüller 指標を表す.

Mazur と Wiles [MW] は, この Iwasawa main conjecture を保型形式を使い K_∞ の不分岐拡大を構成するという方法で証明した. その後 Rubin は Kolyvagin [K] が導入した 円単数の Euler system を用いて, この conjecture に新しい証明を与えた [R1]. Rubin は円単数を用いて, イデアル類群のプラスパートを調べ最後に双対性を使って上に述べたような Iwasawa main conjecture の対象とするマイナスパートへ移るという方法で証明を与えた. すなわち Rubin の証明は本来この conjecture の対象であるマイナスパートを直接扱うものではない.

ここでは円単数の代わりに Gauss 和 を用いて, イデアル類群のマイナスパートを直接扱い, p 進 L 関数との関係を調べる. その結果, この conjecture に対し新しい証明を与える. 証明で用いられる Gauss 和 の Euler system は円単数の Euler system と同様に Kolyvagin [K] が導入したもので Rubin [R2] は, この Gauss 和 の Euler system を用いて基礎体 K のイデアル類群のマイナスパートの構造を調べている. ここでは Gauss 和 の Euler system を K_∞/K の各中間体に対し組織的に用いて Iwasawa main conjecture に証明を与える.

2 Iwasawa main conjecture

この節では, Iwasawa main conjecture の formulation を与える. $K/\mathbb{Q}$ を前節のように p が tamely ramified である虚な有限次 abel 拡大とする. $\Delta := \mathrm{Gal}(K/\mathbb{Q})$ の任意の指標 χ に対し $\mathbb{Z}_p$ 上 χ の像で生成される環を $\mathcal{O}_\chi$, $\underline{\mathcal{O}_\chi}$ で χ を通し $\mathbb{Z}_p[\Delta]$- 加群と見なしたものを表すことにする. 任意の $\mathbb{Z}_p[\Delta]$- 加群 $\mathfrak{M}$ に対し $\mathcal{O}_\chi[\Delta]$- 加群 $\mathfrak{M}_\chi$ を以下のように定め $\mathfrak{M}$ の χ-part と呼ぶことにする. すなわち

$$\mathfrak{M}_\chi := \mathfrak{M} \otimes_{\mathbb{Z}_p[\Delta]} \underline{\mathcal{O}_\chi}$$

と定義する. 各 $m \geq 0$ に対し, K 上 p^m 次である K_∞/K の唯一の中間体を K_m とおく. A_m を K_m のイデアル類群の p-part とすると, 前節における K_∞ の最大不分岐 abel pro-p 拡大の Galois 群 X は類体論から A_m をノルムに関して射影極限をとったものになる. すなわち, $X = \varprojlim A_m$ である.

$$\Gamma_m := \mathrm{Gal}(K_m/K), \quad \Gamma := \mathrm{Gal}(K_\infty/K)$$

とおくと

$$\mathrm{Gal}(K_m/\mathbb{Q}) = \Delta \times \Gamma_m, \quad \mathrm{Gal}(K_\infty/\mathbb{Q}) = \Delta \times \Gamma$$

と分解する. 各 $m \geq 0$ に対し A_m は $\mathbb{Z}_p[\Delta \times \Gamma_m]$- 加群であるから, X は $\varprojlim \mathbb{Z}_p[\Delta \times \Gamma_m] = \mathbb{Z}_p[[\Gamma]][\Delta]$- 加群である. ここで, 完備群環 $\mathbb{Z}_p[[\Gamma]]$ は

$$\mathbb{Z}_p[[\Gamma]] := \varprojlim \mathbb{Z}_p[\Gamma_m]$$

で定義する.

$$\Lambda_\chi := \mathcal{O}_\chi[[\Gamma]] \simeq \mathcal{O}_\chi[[T]]$$

とおくと, $X_\chi = X \otimes_{\mathbb{Z}_p[\Delta]} \underline{\mathcal{O}_\chi}$ は $\Lambda_\chi[\Delta]$- 加群となる. ここで同型 $\mathcal{O}_\chi[[\Gamma]] \simeq \mathcal{O}_\chi[[T]]$ は Γ の位相的生成元 γ を一つ固定し, γ に $1+T$ を対応させて得られる. 1 節に現れた X_χ の特性イデアル $\mathrm{char}(X_\chi)$ を定義する. 岩澤先生の定理から, X_χ は有限生成 tortion Λ_χ- 加群であるから

$$X_\chi \sim \bigoplus_{j=1}^{k} \Lambda_\chi/f_j\Lambda_\chi, \qquad f_j \in \Lambda_\chi$$

と書ける. ここで, $\sim$ は有限のずれを無視した同型を表す. そこで, $\mathrm{char}(X_\chi)$ を $(\prod_{j=1}^{k} f_j)$ が Λ_χ の中で生成する単項イデアルとして定義する. すなわち,

$$\mathrm{char}(X_\chi) := (\prod_{j=1}^{k} f_j)$$

である. 一方, 岩澤先生は Kubota-Leopoldt の p 進 L 関数が巾級数の中に存在することを示した. すなわち Δ の任意の even な指標 $\chi(\neq \mathbf{1})$ に対し, 巾級数 $G_p(\chi, T) \in \Lambda_\chi \simeq \mathcal{O}_\chi[[T]]$ で以下を満たすものが存在する.

$$G_p(\chi, \kappa(\gamma)^s - 1) = L_p(\chi, s), \qquad\qquad s \in \mathbb{Z}_p$$

ここで $\kappa : \mathrm{Gal}(K_\infty/\mathbb{Q}) \to {\mathbb{Z}_p}^\times$ は円分指標であり, $L_p(\chi, s)$ は Kubota-Leopoldt の p 進 L 関数を表す. Iwasawa main conjecture とは以下のような主張である.

定理 2.1 [Iwasawa main conjecture] Δ の任意の odd な指標 $\chi(\neq \omega)$ に対し Λ_χ のイデアルとして以下の等式が成り立つ.

$$\mathrm{char}(X_\chi) = (G_p(\omega\chi^{-1}, T)).$$

以下で与える証明では, この定理の両辺に現れるイデアル類群のマイナスパートと p 進 L 関数とを直接関係づけていく. その両者の仲介役をなすのが Gauss 和 の Euler system である.

3 Gauss 和 の Euler system

この節では, Gauss 和 の Euler system について述べ, Gauss 和 がどの様にイデアル類群と p 進 L 関数との仲介役をするかという事について述べる. $F/\mathbb{Q}$ を任意の有限次 abel 拡大とし, その conductor を $N = p^t N_0$, $t \geq 0$, $p \nmid N_0$, $N_0 \not\equiv 2 \pmod 4$ とおく. $L := \mathbb{Q}(\mu_N)$ とおくと $F \subset L$ である. M を $M \geq p^t$ をみたす p の巾とし, 集合 S を以下で定める.

$$\mathsf{S} := \{\ n \in \mathbb{N} \mid n \text{ は square free かつ}$$
$$\text{任意の } n \text{ の素因子 } \ell \text{ は合同式 } \ell \equiv 1 \pmod{MN_0} \text{ をみたす.}\}$$

$n \in \mathrm{S}$ に対し $r \equiv 1 \pmod{nN}$ となる素数 r をとり r の上にある $L(\mu_n)$ の素イデアル $\mathfrak{R}$ を一つ固定する. character $\varepsilon_{n,\mathfrak{R}} : (\mathbb{Z}/r)^\times \to \mu_{nN}$ を以下をみたすものとして定義する.

$$\varepsilon_{n,\mathfrak{R}}(a) \equiv a^{-\frac{r-1}{nN}} \mod \mathfrak{R}$$

この時, Gauss 和 $g(n, \mathfrak{R}, \zeta_r)$ を以下で定義する.

定義 3.1 (Gauss 和)

$$g(n, \mathfrak{R}, \zeta_r) = \sum_{a=1}^{r-1} \varepsilon_{n,\mathfrak{R}}(a) {\zeta_r}^a \qquad \in L(\mu_{rn})^\times .$$

次に, この Gauss 和 $g(n, \mathfrak{R}, \zeta_r)$ から $F(\mu_n)^\times$ の元を定義する. $\delta \in \mathrm{Gal}(L/\mathbb{Q})$ を固定し, $\tilde{\delta} \in \mathrm{Gal}(\mathbb{Q}(\mu_{NM})/\mathbb{Q})$ をその延長とする. 各 $n \in \mathrm{S}$ に対し, $b_n \in \mathbb{N}$ を以下で定める.

$$\begin{array}{ccccccc} \mathrm{Gal}(\mathbb{Q}(\mu_{nNM})/\mathbb{Q}) \cong & (\mathbb{Z}/nNM)^\times & \cong & \mathrm{Gal}(\mathbb{Q}(\mu_{NM})/\mathbb{Q}) & \times & \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \\ & b_n & \mapsto & (\quad \tilde{\delta} & , & 1 \quad) . \end{array}$$

このとき, 任意の $\zeta \in \mu_{nNM}$ に対し $\zeta^{\tilde{\delta}} = \zeta^{b_n}$ が成り立つ.

$$\alpha(n, \mathfrak{R}) = g(n, \mathfrak{R}, \zeta_r)^{\delta - b_n} \qquad \in L(\mu_n)^\times$$

とおき, さらに $\mathfrak{R}$ の下にある $F(\mu_n)$ の素イデアル $\mathfrak{r}$ に対し

$$\alpha(n, \mathfrak{r}) = N_{L/F}\, \alpha(n, \mathfrak{R}) \qquad \in F(\mu_n)^\times$$

と定義する. ここで $N_{L/F} : L(\mu_n)^\times \to F(\mu_n)^\times$ はノルム写像を表す. $\alpha(n, \mathfrak{r})$ は $\mathfrak{R}$ のとり方によらず well-defined に定まることが確かめられる. これら $\alpha(n, \mathfrak{r})$ は Euler system をなし, かつそれぞれがイデアル類群, p 進 L 関数の両者に関係していることから Iwasawa main conjecture を証明するための細かな情報を与えてくれる. 実際にどのように $\alpha(n, \mathfrak{r})$ がイデアル類群と p 進 L 関数に関係しているのかを次にみていく. はじめに $n \in \mathrm{S}$ に対し Stickelberger element $\theta(n)$ を以下で定義する.

定義 3.2 (Stickelberger element)

$$\theta(n) = (\delta - b_n) \sum_{\substack{a=1 \\ (a,nN)=1}}^{nN} \frac{a}{nN} {\tau_a}^{-1} \qquad \in \mathbb{Z}[\mathrm{Gal}(L(\mu_n)/\mathbb{Q})].$$

ここで $\tau_a \in \mathrm{Gal}(L(\mu_n)/\mathbb{Q})$ は任意の $\zeta \in \mu_{nN}$ に対し $\zeta^{\tau_a} = \zeta^a$ をみたす元である. 各 Galois 群の元を $F(\mu_n)$ に制限することにより $\theta(n) \in \mathbb{Z}[\mathrm{Gal}(F(\mu_n)/\mathbb{Q})]$ とみなす. 岩澤先生の定理より, この Stickelberger element は p 進 L 関数を構成することが分かる. また Stickelberger element はイデアル類群の annihilator であることを主張する以下の定理が知られている.

定理 3.3 (Stickelberger)

$$(\alpha(n, \mathfrak{r})) = \theta(n)\mathfrak{r}$$

すなわち, イデアル類群と p 進 L 関数を構成する $\theta(n)$ の両者に Gauss 和 $\alpha(n, \mathfrak{r})$ は関係している:

$$F(\mu_n)\ \text{のイデアル} \quad \underset{\alpha(n,\mathfrak{r})}{\longleftrightarrow} \quad \theta(n)$$

我々が知りたいのは F のイデアルの情報である (後で F として, 円分 $\mathbb{Z}_p$ 拡大 K_∞/K の各中間体 K_m をとる). そこで, 上の関係と類似した F での図式:

$$F\ \text{のイデアル} \quad \underset{\kappa(n,\rho)}{\longleftrightarrow} \quad \delta(n)$$

を作る. $\delta(n)$, $\kappa(n, \rho)$ の説明をする. 任意の素数 $\ell \in \mathrm{S}$ に対し σ_ℓ を $\mathrm{Gal}(F(\mu_\ell)/F) \simeq (\mathbb{Z}/\ell)^\times$ の生成元とし,

$$D_\ell = \sum_{i=0}^{\ell-2} i {\sigma_\ell}^i$$

とおく. 自然数 $n \in \mathrm{S}$ に対しては,

$$D_n = \prod_{\ell | n} D_\ell$$

で定義する. 前に定義した Stickelberger element $\theta(n)$ に対し

$$D_n\theta(n) \quad \in N_n\{(\mathbb{Z}/M)[\mathrm{Gal}(F/\mathbb{Q})]\}$$

であることが確かめられる. ここで N_n はノルム $N_n = \sum \tau,\ \tau \in \mathrm{Gal}(F(\mu_n)/F)$ を表す. そこで $\delta(n) \in (\mathbb{Z}/M)[\mathrm{Gal}(F/\mathbb{Q})]$ を以下で定義する.

$$D_n\theta(n) = N_n\delta(n).$$

次に $\kappa(n,\rho)$ の説明をする. これを定義するために $F/\mathbb{Q}$ は虚な有限次 abel 拡大という仮定をおく.

$$\mathrm{Gal}(F/\mathbb{Q}) \simeq \Delta \times G_p, \quad p \nmid |\Delta|, \quad G_p : p \text{ 群}$$

とおき, $\chi(\neq \omega)$ を Δ の odd な指標とする. この時, 任意の $\mathbb{Z}_p[\Delta]$- 加群 $\mathfrak{M}$ に対し functor $\mathfrak{M} \mapsto \mathfrak{M}_\chi := \mathfrak{M} \otimes_{\mathbb{Z}_p[\Delta]} \underline{\mathcal{O}_\chi}$ は exact となる. $a \in \mathfrak{M}$ の像を $a_\chi \in \mathfrak{M}_\chi$ とおくことにする.

$\alpha(n,\mathfrak{r}) \in F(\mu_n)^\times$ に対し,

$$\alpha(n,\mathfrak{r})^{D_n} \in [F(\mu_n)^\times/(F(\mu_n)^\times)^M]^{G_n}, \qquad G_n = \mathrm{Gal}(F(\mu_n)/F)$$

が成り立つので ρ を $\mathfrak{r}$ の下にある F の素イデアルとし $\kappa(n,\rho) \in (F^\times/(F^\times)^M)_\chi$ を以下で定める.

$$\begin{array}{ccc} (F^\times/(F^\times)^M)_\chi & \simeq & ([F(\mu_n)^\times/(F(\mu_n)^\times)^M]^{G_n})_\chi \\ & & \\ \kappa(n,\rho) & \mapsto & (\alpha(n,\mathfrak{r})^{D_n})_\chi \end{array}$$

$\kappa(n,\rho)$ は $\mathfrak{r}$ のとり方によらず定まる. $\mathcal{L} := \oplus_\lambda \mathbb{Z}\lambda$ を F のイデアル群とし, 単項イデアル $(x) \in \mathcal{L}$ の $\mathcal{L}/M\mathcal{L}$ での像を $[x]$ とおく. ρ, $\delta(n)$, $\kappa(n,\rho)$ の間には Stickelberger の定理 (定理 3.3) と類似した以下の関係式が $(\mathcal{L}/M\mathcal{L})_\chi$ において成り立つ.

$$[\kappa(n,\rho)] = \delta(n)_\chi\rho_\chi + (\ n \text{ を割る素数イデアルの成分 }).$$

この関係式が今回の証明において重要な役割をする.

4 証明の概略

$K/\mathbb{Q}$ を虚な有限次 abel 拡大とし K^+ で K の最大実部分体を表すことにする. ここで以下の仮定をおく.

仮定
I. $p \nmid [K:\mathbb{Q}]$.
II. p の上の任意の素イデアルは K/K^+ で不分解.

$\chi(\neq \omega)$ を odd な第一種の指標, すなわち χ の conductor f_χ は $f_\chi = p^a N_0$, $a = 0$ or 1, $p \nmid N_0$, $N_0 \not\equiv 2 \pmod 4$ という形に書けているとする. K_χ を χ の kernel に対応する体とする. $K = K_\chi(\mu_p)$ とし, χ を $\Delta := \mathrm{Gal}(K/\mathbb{Q})$ の指標とみなした場合を示せば十分であることが確かめられる. この時, 円分 $\mathbb{Z}_p$ 拡大 K_∞/K の各中間体 K_m の conductor は $p^{m+1}N_0$ となる. 中間体 K_m を一つ固定し, p の巾 M を十分大きくとる. この K_m に対し3節の結果を用いると任意の $n \in \mathrm{S}$ に対し $\delta(n) \in (\mathbb{Z}/M)[\mathrm{Gal}(K_m/\mathbb{Q})]$ が定まる. 分解

$$\mathrm{Gal}(K_m/\mathbb{Q}) \simeq \Delta \times \Gamma_m$$

より

$$\delta(n)_\chi \quad \in (\mathbb{Z}/M)[\mathrm{Gal}(K_m/\mathbb{Q})]_\chi \simeq (\mathcal{O}_\chi/M)[\Gamma_m] \simeq \Lambda_\chi/(M, \omega_m)$$

である. ここで多項式 ω_m は $\omega_m := (1+T)^{p^m} - 1$ で定義する.

定義 4.1 任意の $n' \in \mathrm{S}$ に対し, 集合 $\{\ \delta(n)_\chi \mid n$ は n' の約数 $\}$ で生成される $R_{m\chi} := \Lambda_\chi/(M, \omega_m)$ のイデアルを $T_{n'}{}^\chi$ とおく.

定義より $T_1{}^\chi = (\delta(1)_\chi)$ であるが h_0 を $G_p(\omega\chi^{-1}, T)$ の $R_{m\chi}$ での像とおくと, Stickelberger element が p 進 L 関数を構成することから $T_1{}^\chi = (\delta(1)_\chi) = (h_0)$ が成り立つ. 2節で述べたように, $X_\chi \sim \oplus_{j=1}^k \Lambda_\chi/f_j\Lambda_\chi$, $f_j \in \Lambda_\chi$ が成り立つが, イデアル類群と関係する f_j は, Stickelberger element から構成された $\delta(n)_\chi$ と以下のように関係づけられることが示される.

定理 4.2 以下の性質を満たす素数の集合 $\{r_j\}_{1\le j\le k}$ が存在する.
$n_j = r_1 \ldots r_j$ とおくと, ある $h_j \in T_{n_j}{}^{\chi}$ が存在し $R_{m\chi}$ において次の関係式を満たす.

$$f_j h_j = \eta h_{j-1}.$$

ここで η は p の巾であり, 全ての中間体 K_m に対し共通にとれる. (ただし M は η より十分大きくとれる.)

この定理は Cheboterev の密度定理と, Gauss 和 の Euler system を用いて h_j を帰納的に構成していくという方法で示される. 具体的に述べると, $h_{j-1} \in T_{n_{j-1}}{}^{\chi}$ を生成元を用いて

$$h_{j-1} = \sum_{n|n_{j-1}} g_n \delta(n)_{\chi}, \quad g_n \in R_{m\chi}$$

と書いた時, 適当な K_m の素イデアル λ を選び,

$$\beta := \prod_{n|n_{j-1}} \kappa(n,\lambda)^{g_n},$$

$$W := \beta R_{m\chi} \subset (K_m{}^{\times}/(K_m{}^{\times})^M)_{\chi}$$

とおき, ある種の条件をみたす $R_{m\chi}$- 準同型 $\psi : W \to R_{m\chi}$ を構成する. $h_j = \psi(\beta)$ とおくと, この h_j は $h_j \in T_{n_j}{}^{\chi}$ かつ $f_j h_j = \eta h_{j-1}$ を満たすことが示せる.

定理 4.2 の h_j の極限をとり Ferrero-Washington の定理 [FW] から $p \nmid f_j$ が成り立つことを用いると Λ_{χ} の元 $\vartheta_j{}^{\chi}$ が以下のように得られる.

定理 4.3 任意の j, $1 \le j \le k$ に対し, Λ_{χ} の元 $\vartheta_j{}^{\chi}$ で $f_j = \vartheta_{j-1}{}^{\chi}/\vartheta_j{}^{\chi}$ となるものが存在する.

ここで, $\vartheta_0{}^{\chi} = G_p(\omega\chi^{-1}, T)$ である.

定理 4.3 からイデアルの包含関係

$$\mathrm{char}(X_{\chi}) \supset (G_p(\omega\chi^{-1}, T))$$

が導かれ, 類数公式を用いた岩澤先生による手法を使うと, 定理 2.1 [Iwasawa main conjecture] が示される.

参考文献

[A] M. Aoki, The Iwasawa main conjecture and Gauss sums, in preparation.

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. 109 (1979), 377-395.

[G] C. Greither, Class groups of abelian fields and the main conjecture, Ann. Inst. Fourier (Grenoble), 42 (1992), 449-499.

[I] K. Iwasawa, Lectures on p-adic L-functions, Princeton, Princeton Univ. Press and Univ. of Tokyo Press (1972).

[K] V. Kolyvagin, Euler systems, The Grothendieck Festschrift II, Progr. Math.87(1990), Birkhäuser, 435-483.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. math. 76 (1984), 179-330.

[R1] K. Rubin, The main conjecture, Appendix to S.Lang, Cyclotomic Fields I and II, Springer (1990).

[R2] K. Rubin, Kolyvagin's system of Gauss sums, Arithemetic Algebraic Geometry, Progr.Math.89(1991), Birkhäuser, 309-324.

[W] L. Washington, Introduction to Cyclotomic Fields, 2nd ed, GTM83, Springer (1997).

Department of Mathematics, Tokyo Metropolitan University, Minami-Ohsawa 1-1, Hachioji, Tokyo, 192-0397 Japan

E-mail address: maoki@comp.metro-u.ac.jp