代数体の付随するガロワ群による特徴付けについて

尾崎　学 (早稲田大学　基幹理工)

1. 序

本稿では，代数体の同型類と算術的同値類を付随するガロワ群で特徴付けるという問題を，近年筆者によって得られた結果も交えて概説する．

以下，有理数体の代数的閉包 $\overline{\mathbb{Q}}$ を一つ固定して，その部分体を**代数体**，特に $\mathbb{Q}$ 上有限次拡大である代数体を**有限次代数体**ということにする．そして，

$$\mathcal{A}_0 := \{\text{ 有限次代数体全体 }\} \subseteq \mathcal{A} := \{\text{ 代数体全体 }\}$$

とおく．

本稿では以下の 2 つの同値関係を考察する：

(1) 同型　$K_1 \simeq K_2$　　$(K_1, K_2 \in \mathcal{A})$

(2) 算術的同値　$K_1 \approx K_2 \overset{\text{def.}}{\Longleftrightarrow} \zeta_{K_1}(s) = \zeta_{K_2}(s)$　　$(K_1, K_2 \in \mathcal{A}_0)$

ここで，$F \in \mathcal{A}_0$ に対し，$\zeta_F(s) = \displaystyle\sum_{\mathfrak{a}} \frac{1}{[\mathcal{O}_F : \mathfrak{a}]^s}$ （$\mathfrak{a}$ は F の整数環 $\mathcal{O}_F$ の非零イデアル全体を亙る）は F の Dedekind zeta 函数を表す．

明らかに，$K_1, K_2 \in \mathcal{A}_0$ に対し，$K_1 \simeq K_2 \Longrightarrow K_1 \approx K_2$ であるから，$\simeq$ は $\approx$ よりも強い $\mathcal{A}_0$ 上の同値関係である．

以下の節で，代数体の同型類と算術的同値類がいかに Galois 群の言葉で特徴付けられるかについて解説する．

2. 算術的同値類の特徴付け

数論研究を生業にしている人は多かれ少なかれ，Dedekind zeta 函数 $\zeta_F(s)$ は有限次代数体 F のことを良く知っていると信じている．実際，$\zeta_F(s)$ から F の多くの算術的情報が復元される：

命題 1. $K_1, K_2 \in \mathcal{A}_0$, $K_1 \approx K_2$ とすると，以下が成立する．

(1) すべての素数の K_1 と K_2 における分解様式が一致する．即ち，任意の素数 p に対して，

$$p\mathcal{O}_{K_i} = \mathfrak{p}_{i1}^{e_{i1}} \mathfrak{p}_{i2}^{e_{i2}} \cdots \mathfrak{p}_{ig_i}^{e_{ig_i}}$$

を素イデアル分解とするとき，適当に素イデアルの番号付を選べば，$g_1 = g_2$，$[\mathcal{O}_{K_1}/\mathfrak{p}_{1j} : \mathbb{F}_p] = [\mathcal{O}_{K_2}/\mathfrak{p}_{2j} : \mathbb{F}_p]$ $(1 \leq i \leq g_1 = g_2)$ が成立する（この条件は $K_1 \approx K_2$ の必要十分条件である）．

(2) $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$．さらに K_1 と K_2 の実無限素点と複素無限素点の個数がそれぞれ一致する．

(3) $d_{K_1} = d_{K_2}$ （判別式）

(4) $\mathcal{O}_{K_1}^\times \simeq \mathcal{O}_{K_2}^\times$ （Abel 群として）

(5) h_{K_i} を K_i の類数，R_{K_i} を K_i の単数規準とするとき，$h_{K_1}R_{K_1} = h_{K_2}R_{K_2}$ が成立.

しかし，$\zeta_F(s)$ は F のすべてを知っているわけではない：

例 1. $K_1 := \mathbb{Q}(\sqrt[8]{-15})$，$K_2 := \mathbb{Q}(\sqrt[8]{-240})$ とおくと，$K_1 \approx K_2$ である．しかし，K_1 と K_2 は同型ではない．さらに，$h_{K_1} \neq h_{K_2}$，$R_{K_1} \neq R_{K_2}$ ([2]).

従って，$\approx$ は $\simeq$ よりも真に弱い $\mathcal{A}_0$ 上の同値関係である．

それでは，有限次代数体の同型と算術的同値の差はどの程度なのであろうか．それを理解するために，函数体での類似を見てみる．F_1，F_2 を標数 l の有限体 $\mathbb{F}$ 上の 1 変数代数函数体として，C_1，C_2 を $\mathbb{F}$ 上の代数曲線で，それぞれの $\mathbb{F}$ 上函数体が F_1 と F_2 になるものとする．そして，$\zeta_{F_i}(s)$ を F_i の Dedekind zeta 函数とする．このとき，つぎが知られている：

定理 1 ((1)$\Longleftrightarrow$(3) は Weil, (2) との同値性は Tate[11])**.** つぎは同値である：
(1) $\zeta_{F_1}(s) = \zeta_{F_2}(s)$
(2) C_i の Jacobi 多様体 $\mathrm{Jac}(C_i)$（$i = 1, 2$）の間に $\mathbb{F}$ 上の同種写像 $\mathrm{Jac}(C_1) \sim \mathrm{Jac}(C_2)$ が存在する．
(3) p を l と異なる素数として，$X_{\overline{\mathbb{F}}F_i}(p)$ を $\overline{\mathbb{F}}F_i$ 上の最大不分岐 abel p-拡大の Galois 群とする（類体論よりこれは Tate 加群 $\varprojlim \mathrm{Jac}(C_i)[p^n]$ と自然に同型）．このとき，$\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \simeq \mathrm{Gal}(\overline{\mathbb{F}}F_i/F_i)$-加群として

$$X_{F_1}(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq X_{F_2}(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

が成立.

従って函数体の世界での算術的同値は即ち，Jacobi 多様体の同種であるから，代数体における同型と算術的同値の差は，函数体における Jacobi 多様体の同型と同種の差の類似として捉えることができる．

代数体の世界では Jacobi 多様体そのものの良い類似物は知られていないが，Tate 加群の良い類似物があり，それと Dedekind zeta 函数との関係の類似が追求されている——それが**岩澤理論**である．ここで円分的 $\mathbb{Z}_p$-拡大の岩澤理論について簡単に説明する．k を有限次代数体，素数 p を一つ固定しておく．函数体の係数拡大 $\overline{\mathbb{F}}F_i$ の類似物として $K := k(\mu_{p^\infty})$（μ_{p^∞} は 1 の p 冪乗根全体）を採る（本来であれば 1 の冪乗根全てを添加した拡大を考えたいところだが，現時点でその方向での類似の追求はうまくいっていない）．

$X_K(p)$ を K 上の最大不分岐 abel p-拡大 $L_K(p)/K$ の Galois 群，$X_{K,\{p\}}(p)$ を K 上の最大 p-分岐 abel p-拡大 $M_K(p)/K$ の Galois 群（「p-分岐」は「p 上に無い素点はすべて不分岐」の意）とする．

このとき，$\mathrm{Gal}(K/k) \simeq \mathrm{Gal}(k(\mu_p)/k) \times \mathrm{Gal}(K/k(\mu_p))$ が $\mathrm{Gal}(L_K(p)/k)$ 乃至は $\mathrm{Gal}(M_K(p)/k)$ の内部自己同型を通じて $X_K(p)$ 及び $X_{K,\{p\}}(p)$ に作用する．ここで，有限個の例外の p を除けば，$\mathrm{Gal}(k(\mu_{p^\infty})/k) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) =: G_p$ に注意.

函数体の場合，$\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ の Frobenius 自己同型の $X_{\overline{\mathbb{F}}F_i}(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ への作用の特性多項式 $\Phi(X)$ が本質的に $\zeta_{F_i}(s)$ に一致するのであった（Weil）．同様のことが代数体のこの枠組みでも k が総実有限次代数体の場合 にには成立する（岩澤主予想＝Wiles の定理）．即ち，$\mathbb{Q}_p$ 上の有限次線型空間 $(X_K(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_P)^- := (1-J)(X_K(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_P)$ （$J \in \mathrm{Gal}(k(\mu_p)/k)$ は複素共役）あるいは，$(X_{K,\{p\}}(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_P)^+ := (1+J)(X_K(p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_P)$ への $\mathrm{Gal}(K/k(\mu_p)) \simeq \mathbb{Z}_p$ の生成元の作用の特性多項式 $P_p(X)$（岩澤多項式）が，Dedekind zeta 函数の負の整数点での値を p-進補間して得られる p-進 zeta 函数の零点で記述される．ここで，函数体の場合と決定的に異なるのは，函数体の場合には一つのの固定された素数 $p \neq l$ についての Frobenius 自己同型の特性多項式 $\Phi(X)$ から zeta 函数が完全に復元される，つまり zeta 函数は本質的に多項式であるが，代数体の場合には岩澤多項式 $P_p(X)$ から p-進 zeta 函数は復元できない．代数体の p-進 zeta も Dedekind zeta も多項式からかけ離れた函数だからである．従って，代数体に於いて定理 1 のそのままの類似は成立しないのであるが，次の定理が示すように，p を殆どすべての素数を走らすことで，岩澤多項式から Dedekind zeta を復元し，類似の結果を得ることができる：

定理 2 (足立-小松 [1](1987), J.Oh[9](1998)).
k_1，k_2 を総実有限次代数体とすると，次は同値：

(1) $k_1 \approx k_2$

(2) 有限個の例外を除いたすべての素数 p について，

$$X_{k_1(\mu_{p^\infty})}(p)^- \simeq X_{k_1(\mu_{p^\infty})}(p)^- \quad (\mathbb{Z}_p[[G_p]]\text{-加群として})$$

(3)　有限個の例外を除いたすべての素数 p について，

$$X_{k_1(\mu_{p^\infty}),\ \{p\}}(p)^+ \simeq X_{k_1(\mu_{p^\infty}),\ \{p\}}(p)^+ \quad (\mathbb{Z}_p[[G_p]]\text{-加群として})$$

注意 1. 実際には，(2) の同型の条件を "擬同型 $X_{k_1(\mu_{p^\infty})}(p)^- \sim X_{k_2(\mu_{p^\infty})}(p)^-$（$\mathbb{Z}_p[[G_p]]$-加群として）" に変えたもの（擬同型とは，核と余核が有限であるような準同型である），あるいは "$-$" を外したものも同様に同値である．(3) についても同様（"$+$" を外す）．

定理 2 の証明の概略を説明しよう．(1) $\Longleftrightarrow$ (2) の証明が本質的で，(2) と (3) は Kummer 双対性から概ね同値であることが従う．$\Longrightarrow$ 部分は次の群論的な命題から従う：

命題 2.　(1) $k_1, k_2 \in \mathcal{A}_0$ とする．$N \subseteq \overline{\mathbb{Q}}$ を k_1k_2 を含むような任意の $\mathbb{Q}$ 上の有限次 Galois 拡大として，$G := \mathrm{Gal}(N/\mathbb{Q})$, $H_1 := \mathrm{Gal}(N/k_1)$, $H_2 := \mathrm{Gal}(N/k_2)$ とおく．

このとき $k_1 \approx k_2$ であるための必要十分条件は，全単射 $f : H_1 \longrightarrow H_2$ と $\{\sigma_h \,|\, h \in H_1\} \subseteq G$ で $f(h) = \sigma_h h \sigma_h^{-1}$ $(\forall h \in H_1)$ をみたすものが存在することである.（G の 2 つの部分群 H_1 と H_2 がこのような性質を持つとき，H_1 と H_2 は **Gassmann 同値**と言われる.）

(2)　G を有限群，Δ を群，p を $\#G$ と素な素数，M を $\mathbb{Z}_p[G \times \Delta]$-加群とする．このとき，$G$ の Gassmann 同値な部分群 H_1, H_2 に対して，

$$M_{H_1} \simeq M_{H_2} \quad (\mathbb{Z}_p[\Delta]\text{-加群として})$$

ここで $M_H := M/\sum_{h\in H}(h-1)M$ は M の最大 H-不変商.

N を命題 2 と同様とすれば，$p \nmid \#\mathrm{Gal}(N/\mathbb{Q})$ のとき

$$X_{N(\mu_{p^\infty})}(p)_{\mathrm{Gal}(N(\mu_{p^\infty})/k_i(\mu_{p^\infty}))} \simeq X_{k_i(\mu_{p^\infty})}(p) \quad (i = 1, 2)$$

なので，この命題を $G = \mathrm{Gal}(N(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^\infty}))$, $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}), H_i = \mathrm{Gal}(N(\mu_{p^\infty})/k_i(\mu_{p^\infty}))$, $M = X_{N(\mu_{p^\infty})}(p)$ に適用すると（有限個の例外の素数 p を除いて，

$$\mathrm{Gal}(N(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathrm{Gal}(N(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^\infty})) \times \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}),$$
$$\mathrm{Gal}(N(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^\infty})) \simeq \mathrm{Gal}(N/\mathbb{Q})$$

に注意），定理 2 の (1) $\Longrightarrow$ (2) が従う.

(2) $\Longrightarrow$ (1) は，上述の岩澤主予想（Wiles の定理）を用いる：有限個の例外を除いたすべて素数 p についての $X_{k_i(\mu_{p^\infty})}(p)^-$ の構造から，有理数 $\zeta_{k_i}(1-n)$ $(n \in \mathbb{Z}_{\geq 1})$ の p 進絶対値を，有限個の例外の素数 p を除いて知ることができる．このことから，Dedekind zeta 函数の函数等式と解析的手法を駆使して，$\zeta_{k_1}(s) = \zeta_{k_2}(s)$ を導くことができる.

定理 2 は (2) $\Longrightarrow$ (1) の部分で総実代数体の岩澤主予想（Wiles の定理）を用いているので，総実でない一般の有限次代数体についてそのままの形では一般化されていない．しかし，少し弱い形であれば，一般の有限次代数体についても成立する：

命題 3 (O.). $k_1,\ k_2 \in \mathcal{A}_0$ とすると次は同値：

(1) $k_1 \approx k_2$,

(2) 有限個の例外を除いたすべての素数 p について，
$(X_{k_1(\mu_{p^\infty}),\{p\}}(p)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p)^{\omega_p} \simeq (X_{k_1(\mu_{p^\infty}),\{p\}}(p)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p)^{\omega_p}$（$\mathbb{Q}_p[G_p]$-加群として）
ここで，$\omega_p : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^\times$ は円分指標で，$\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})]$-加群 X に対し，$X^{\omega_p} := \left(\frac{1}{p-1}\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})}\omega_p(\sigma)\sigma^{-1}\right)X$.

注意 2. 実際には，(2) の同型の条件を "$X_{k_1(\mu_{p^\infty}),\{p\}}(p)^{\omega_p} \simeq X_{k_2(\mu_{p^\infty}),\{p\}}(p)^{\omega_p}$（$\mathbb{Z}_p[[G_p]]$-加群として）" に変えたもの，あるいは "$\omega_p$" を外したものも同様に同値である．

定理 2 と命題 3 は，有限次代数体 k の無限次拡大 $L_{k(\mu_{p^\infty})}(p)/k$ あるいは $M_{k(\mu_{p^\infty})}(p)/k$ の Galois 群の族が k の算術的同値類を特徴付けるという結果であったが，もっと小さい制限分拡大の Galois 群の族によっても，特徴付けることができる．以下，一般に $F \in \mathcal{A}$ と素数 p, 素数の集合 S に対して，$X_{F,S}(p)$ で F 上の最大 S-分岐 abel p-拡大（「S-分岐」は S に含まれる素数上の F の素点以外はすべて不分岐の意）を表す．

定理 3 (東海林-O.[3](2013)). $k_1,\ k_2 \in \mathcal{A}_0$ とする．l_0 を，$l_0 > [k_i : \mathbb{Q}]\ (i=1,2)$, $l_0 \nmid h_{k_1}h_{k_2}d_{k_1}d_{k_2}$ をみたすような固定された素数とする．このとき次は同値：

(1) $k_1 \approx k_2$,

(2) 任意の素数の集合 S に対して，
$$X_{k_1,S}(l_0) \simeq X_{k_2,S}(l_0),$$

(3) 有限個の例外を除くすべての素数 p に対して，
$$X_{k_1,\{p\}}(l_0)/l_0 \simeq X_{k_2,\{p\}}(l_0)/l_0.$$

この定理により，有限 Galois 群の族 $\{X_{k,\{p\}}(l_0)/l_0 \,|\, p \text{ は素数}\}$ が $k \in \mathcal{A}_0$ の算術的同値類を特徴付けることがわかる．

(1) $\Longrightarrow$ (2), (3) は命題 2 から直ちに従う．(2) $\Longrightarrow$ (1) の証明には次の定理を用いる：

定理 4 (Stuart-Perlis[10])．　$k_1,\ k_2 \in \mathcal{A}_0$ に対して，次は同値：

(1)　$k_1 \approx k_2$,

(2)　有限個の例外を除くすべての素数 p について，k_1 と k_2 に於ける p 上の素点の個数が一致する．

$X_{k,\{p\}}(l_0)/l_0$ は類体論により k における p 上の素点の個数と関連はあるが，単数群の影響によりこの群から直ちにその素点の個数が復元されるわけではない．しかし，技術的な方法より，殆ど全ての p について定理 3(2) の同型がが成立していることを利用すると，この困難は克服できて．定理 4 より (1) が導かれる．

3. 同型類の特徴付け

有限次代数体の Galois 群による特徴付けについては，Neukirch-内田の定理として名高い次の定理がある．以下，$F \in \mathcal{A}$ に対し，$G_F := \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ を F の絶対 Galois 群とする．

定理 5 (Jürgen Neukirch[4], 内田興二 [6]，池田正験 [7]，岩澤健吉 [8])．$k_1,\ k_2 \in \mathcal{A}_0$ について，$\varphi : G_{k_1} \simeq G_{k_2}$ を位相群同型とする．このとき，$\alpha \in G_{\mathbb{Q}}$ で，

$$\alpha(k_1) = k_2,\ \varphi(\sigma) = \alpha\sigma\alpha^{-1}\ (\forall\sigma \in G_{k_1})$$

を満たすものが一意に存在する．特に $k_1 \simeq k_2$ である．

この定理の系として，絶対 Galois 群の自己同型に関する次の事実が得られる：

系 1．　$k \in \mathcal{A}_0$ に対して，

$$\mathrm{Aut}(k) \simeq \mathrm{Out}(G_k),\quad g \mapsto (\sigma \mapsto \overline{g}\sigma\overline{g}^{-1}) \mod \mathrm{Inn}(G_k)$$

ここで，$\mathrm{Aut}(k)$ は k の自己同型群，$\mathrm{Out}(G_k)$ は G_k の外部自己同型群，$\mathrm{Inn}(G_k)$ は G_k の内部自己同型群，$g \in \mathrm{Aut}(k)$ に対して，$\overline{g}$ は $\overline{g}|_k = g$ なる $G_{\mathbb{Q}}$ の元とする．特に $\mathrm{Out}(G_{\mathbb{Q}}) = 1$ である．

ここで定理 5 の成立の経緯について簡単に説明する．まず初めに Neukirch が以下で説明するような基本的な成果を挙げた後に，それを基にして内田興二が定理の主張を証明した．同時期に池田は内田とは独立に系 1 の証明を完成させ，岩澤は池田の証明の手法で定理 5 を示すことができることを指摘した．

以下で定理 5 の証明の概略を説明しよう．すべての基本は次の Neukirch の定理である：

定理 6. $1 \neq H \subseteq G_{\mathbb{Q}}$ を閉部分群とする．ある局所体 $\mathbb{Q}_p \subseteq \kappa \subseteq \overline{\mathbb{Q}}_p$ で，ある素数 $q \neq 2$ に対して $q^\infty \nmid [\kappa : \mathbb{Q}_p]$ （即ち，$\mathbb{Q}_p \subseteq M \subseteq \kappa$ で，$[M : \mathbb{Q}_p] < \infty$ なる M たちについて，$[M : \mathbb{Q}_p]$ の q-部分が有界）なるものについて，$H \simeq G_\kappa$ が成立しているものとする．このとき，$\overline{\mathbb{Q}}$ の素点 $\mathfrak{P}$ で、$H \subseteq D_{\mathbb{Q},\mathfrak{P}}$ なるものが一意に存在する．ここで，$F \in \mathcal{A}$ と $\overline{\mathbb{Q}}$ の素点 $\mathfrak{P}$ に対して，$D_{F,\mathfrak{P}}$ は $\mathfrak{P}$ に関する G_F の分解部分群を表す．特に $[\kappa : \mathbb{Q}_p] < \infty$ の場合には，$\mathfrak{P}$ は p の上の素点である．

この定理の系として，次が得られる：

系 2. $k \in \mathcal{A}_0$, p を素数とする．このとき，$\{D_{k,\mathfrak{P}} \,|\, \mathfrak{P}|p\}$ は $\{H \subseteq G_k \,|\, \exists\kappa/\mathbb{Q}_p : \text{有限次} : H \simeq G_\kappa\}$ の包含関係に関する極大元全体と一致する．

この系から，G_k の p 上の素点に関する分解部分群たちは，G_k の群論的構造のみから完全に定まることがわかる．言い換えると各素点の分解群は既に群 G_k の構造の中に “encode” されている ([5, p.786])．これはある意味で絶対 Galois 群が「素数のことを知っている」とも解釈できる．例えば Dirichlet の算術級数定理は定理 5 を用いることにより，$G_{\mathbb{Q}}$ の群構造に encode されていることが判る．とは言えども，例えば Riemann 予想などが encode されているかどうかは謎である（これは半分は冗談です）．

さて，系 2 から，各素数 p について

$$\{\varphi(D_{k_1,\mathfrak{P}}) \,|\, \mathfrak{P}|p\} = \{D_{k_2,\mathfrak{P}} \,|\, \mathfrak{P}|p\} \tag{1}$$

が従う．素数 p の k_i での分解様式は，G_{k_i} の部分群の族 $\{D_{k_1,\mathfrak{P}} \,|\, \mathfrak{P}|p\}$ から決定されるので，(1) と命題 1 より，$k_1 \approx k_2$ が得られる（Neukirch）．

内田はこの Neukirch の結果を基にして，巧妙な群論的方法で定理 5 を得た：Neukirch の結果より，任意の有限次拡大 K_1/k_1 に対し，K_2/k_2 を $\varphi(G_{K_1}) = G_{K_2}$ なる有限次拡大とすれば，$K_1 \approx K_2$ が従う．特に $N/\mathbb{Q}$ が $k_1k_2 \subseteq N$ であるような有限次 Galois 拡大のとき，N と算術的同値な有限次代数体は N 自身のみなので（これは命題 2(1) で $k_1/\mathbb{Q}$ を Galois とすれば，H_1 は G の正規部分群なので，$H_1 = H_2$ となることから従う），$\varphi(G_N) = G_N$ となる．よって，φ は，有限群の同型 $\varphi_N : \mathrm{Gal}(N/k_1) \simeq \mathrm{Gal}(N/k_2)$ を誘導する．しかも，上に述べたことと命題 2 より，φ_N は任意の部分群 $H \subseteq \mathrm{Gal}(N/k_1)$ について H と $\varphi_N(H)$ が $\mathrm{Gal}(N/\mathbb{Q})$ の部分群として Gassmann 同値になるという強い性質を持っていることが判る．この事実を足掛かりとして，内田は φ_N が実際に $\mathrm{Gal}(N/\mathbb{Q})$ の内部自己同型から誘導されることを示し，結局 φ が $G_{\mathbb{Q}}$ の内部自己同型から来ていることを証明したのである．

定理 5 を無限次代数体も含む代数体のクラスに拡張する試みについて説明する．その前に少し記号の準備をする．素数 p と $n \geq 1$ に対して，

$$\Pi_{p,n} := \{l \mid l \text{ は素数，} \ l \equiv 1 \pmod{p^n}, \ p^{\frac{l-1}{p}} \not\equiv 1 \pmod{l}\}$$
$$\Pi_n := \{l \mid l \text{ は素数，} \ l \equiv 1 \pmod{n}\}$$

とおく．そして，$\mathcal{F} \subseteq \mathcal{A}$ を，以下の 2 条件をみたす $F \in \mathcal{A}$ 全体の集合とする：

- 部分体 $F_0 \subseteq F$ で，$F_0/\mathbb{Q}$ は Galois 拡大，$[F : F_0] < \infty$ となるものが存在する．
- 任意の素数 p と整数 $n \geq 1$ に対して，$l_1, l_2 \nmid [F : \mathbb{Q}]$（すなわち，任意の $\mathbb{Q}$ 上有限次部分体 $M \subseteq F$ に対して，$l_1, l_2 \nmid [M : \mathbb{Q}]$）なる $l_1 \in \Pi_{p,n}$ と $l_2 \in \Pi_n$ が存在する．

ここで，$\mathcal{A}_0 \subseteq \mathcal{F}$ に注意しよう．このとき，定理 5 の一般化である次の定理を得る：

定理 7. $K_1, K_2 \in \mathcal{F}$ に対して，$\varphi : G_{K_1} \simeq G_{K_2}$ を位相群同型とする．このとき，$\alpha \in G_{\mathbb{Q}}$ で，

$$\alpha(K_1) = K_2, \quad \varphi(\sigma) = \alpha\sigma\alpha^{-1} \ (\forall\sigma \in G_{K_1})$$

を満たすものが一意に存在する．特に $K_1 \simeq K_1$ である．

証明の概略について説明しよう．証明の土台は定理 5 同様，定理 6 及びその系である．まず，それらから次の補題が得られる：

補題 1. S, T を任意の素数の集合とする．定理 7 の仮定の下で，$G^T_{K_i,S}$ $(i = 1, 2)$ を K_i 上の最大 S-分岐 T-分解拡大（即ち，S 上にない素点は不分岐かつ T 上にある素点はすべて完全分解するような最大拡大）の Galois 群とするとき，$G^T_{K_1,S} \simeq G^T_{K_2,S}$ が成立する．

この補題をうまく運用すると，Galois 拡大 $F/\mathbb{Q}$ で，$F \subseteq K_1 \cap K_2$ かつ $[K_i : F] < \infty$ $(i = 1, 2)$ なるものが存在することがわかる．

有限次拡大 M_1/K_1 に対し，M_2/K_2 を $\varphi(G_{M_1}) = G_{M_2}$ なる有限次拡大，$N/\mathbb{Q}$ を $M_1M_2 \subseteq N$ なる Galois 拡大で，$[N : F] < \infty$ なるものとする．このとき，有限次 Galois 拡大 $N_0/\mathbb{Q}$ で $N_0 \subseteq N$ かつ制限写像が同型 $\pi : \mathrm{Gal}(N/F) \simeq \mathrm{Gal}(N_0/F_0)$ $(F_0 := N_0 \cap F)$ を誘導するものが存在する．このとき $M_{i,0} := N_0^{\pi(\mathrm{Gal}(N/M_i))}$ $(i = 1, 2)$ とおけば，$M_{1,0} \approx M_{2,0}$ が補題 1 と次を用いることで証明できる：

補題 2. q を $\#\mathrm{Gal}(N_0/\mathbb{Q}) \mid q - 1.$ なる素数とする．
もしも任意の有限 $\mathbb{F}_q[\mathrm{Gal}(N_0/\mathbb{Q})]$-加群 Y について，

$$Y_{\mathrm{Gal}(N_0/M_{1,0})} \simeq Y_{\mathrm{Gal}(N_0/M_{2,0})} \quad (\mathbb{F}_q\text{-加群として})$$

が成立すれば，$M_{1,0}$ と $M_{2,0}$ は算術的同値である．

任意の有限 $\mathbb{F}_q[\mathrm{Gal}(N_0/\mathbb{Q})]$-加群 Y はある素数の集合 S, T に関する $X^T_{N_0,S}(q)$ として実現され，さらに S, T をうまく選べば，$X^T_{N_0,S}(q) \simeq X^T_{N,S}(q)$ とできる．ここで，補題 1 より，

$$X^T_{N_0,S}(q)_{\mathrm{Gal}(N_0/M_{i,0})} \simeq X^T_{N,S}(q)_{\mathrm{Gal}(N/M_i)} \simeq X^T_{M_i,S}(q) \quad (i=1,2)$$

は互いに同型であるから，補題 2 より $M_{1,0} \approx M_{2,0}$ が従う．

よって，定理 5 の証明と同様に，φ が有限群の同型

$$\varphi_{N_0} : \mathrm{Gal}(N_0/k_1) \simeq \mathrm{Gal}(N_0/k_2), \quad (k_i := N_0^{\pi(\mathrm{Gal}(N/K_i))} \ (i=1,2))$$

を誘導して，内田の手法によりこの同型 φ_{N_0} が $\mathrm{Gal}(N_0/\mathbb{Q})$ の内部自己同型から誘導されることも判る．そして，結局 φ 自身が $G_{\mathbb{Q}}$ の内部自己同型から来ていることを示すことができる．

References

[1] N.Adachi, K.Komatsu, The maximal p-extensions and zeta-functions of algebraic number fields. Mem. School Sci. Engrg. Waseda Univ.**51** (1987), 25–31.

[2] B.de Smit, R.Perlis, Zeta functions do not determine class numbers. Bull. Amer. Math. Soc. (N.S.) **31** (1994), no. 2, 213–215.

[3] M.Tohkailin, M.Ozaki, Characterization of arithmetical equivalence of number fields by Galois groups with restricted ramification, Tokyo J. Math. **36** (2013), no. 2, 347–354.

[4] J.Neukirch, Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkrper, Invent. Math. **6** (1969), 296–314.

[5] J.Neukirch, A.Schmidt, K.Wingberg, Cohomology of number fields (2nd edition), Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, 2008.

[6] K.Uchida, Isomorphisms of Galois groups. J. Math. Soc. Japan **28** (1976), no. 4, 617–620.

[7] M.Ikeda, Completeness of the absolute Galois group of the rational number field. J. Reine Angew. Math. **291** (1977), 1–22.

[8] K.Iwasawa, Automorphisms of Galois groups over number fields (1975) (未刊行), 岩澤健吉全集第 2 巻.

[9] J.Oh, On zeta functions and Iwasawa modules, Trans. Amer. Math. Soc. **350** (1998), no. 9, 3639–3655.

[10] D.Stuart, R.Perlis, A new characterization of arithmetic equivalence, J. Number Theory **53** (1995), no. 2, 300–308.

[11] J.Tate, Endomorphisms of abelian varieties over finite fields. Invent. Math. **2** (1966) 134–144.

早稲田大学理工学術院基幹理工学部数学科

尾崎　学

e-mail: ozaki@waseda.jp