

## 分岐条件の付いた埋め込み問題とその応用について

金沢大・自然 野村 明人 (Akito Nomura)

本稿の目的は、代数体上の不分岐非アーベル  $p$  拡大の存在について埋め込み問題の立場から考察することである。尚、詳しい証明に付いては [3][5] を参照してください。以下、 $p$  は常に奇素数を表すとする。

### §1 Introduction

$k$  を代数体、 $\mathfrak{G}$  を  $k$  の絶対ガロア群、即ち  $k$  の代数閉包の  $k$  上のガロア群、とする。  $K/k$  をガロア拡大とし、 $(\epsilon): 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(K/k) \rightarrow 1$  を中心拡大とする。このとき埋め込み問題  $(K/k, \epsilon)$  は、図式

$$\begin{array}{ccccccc}
 & & & & \mathfrak{G} & & \\
 & & & & \downarrow \varphi & & \\
 (\epsilon): 1 & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & E & \xrightarrow{j} & \text{Gal}(K/k) \longrightarrow 1
 \end{array} \tag{*}$$

で定義される。ここで  $\varphi$  は自然な全射を表す。 $\mathfrak{G}$  から  $E$  への連続な準同型  $\psi$  で、 $j \circ \psi = \varphi$  を満たすものを埋め込み問題  $(K/k, \epsilon)$  の solution と呼び、solution が存在するとき  $(K/k, \epsilon)$  は可解であると言う。さらに、solution  $\psi$  が全射のとき、 $\psi$  は proper solution であると言う。また、solution  $\psi$  に対して、 $\text{Ker } \psi$  に対応する  $k$  上のガロア拡大体を  $(K/k, \epsilon)$  の solution field と呼ぶ。 $(K/k, \epsilon)$  が proper solution を持つことは、

ガロア拡大  $L/K/k$  で自然な完全列  $1 \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(L/k) \rightarrow \text{Gal}(K/k) \rightarrow 1$  が  $(\varepsilon)$  と一致するようなものが存在することと同値である.

$k$  の素点  $q$  に対して,  $q$  による  $k$  の完備化を  $k_q$ ,  $k$  の  $K$  への延長による  $K$  の完備化を  $K_q$  で表す. このとき, 埋め込み問題  $(K/k, \varepsilon)$  の局所問題  $(K_q/k_q, \varepsilon_q)$  が次の図式で定義される.

$$\begin{array}{ccccccc}
 & & & & \mathfrak{S}_q & & \\
 & & & & \downarrow \varphi|_{\mathfrak{S}_q} & & \\
 (\varepsilon_q) : 1 & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & E_q & \xrightarrow{j|_{E_q}} & G_q \longrightarrow 1.
 \end{array}$$

ここで  $G_q$  は  $K_q/k_q$  のガロア群,  $\mathfrak{S}_q$  は  $k_q$  の絶対ガロア群,  $E_q$  は  $G_q$  の  $j$  による逆像を表す. また,  $(K_q/k_q, \varepsilon_q)$  に対する solution, solution field 等は,  $(K/k, \varepsilon)$  の場合と同様に定義される.

次は, 埋め込み問題において基本的な結果である.

**Fact 1(Ikeda[1])** 埋め込み問題  $(K/k, \varepsilon)$  は可解とする. このとき  $(K/k, \varepsilon)$  は proper solution を持つ.

**Fact 2(Neukirch[2])**  $k$  の任意の素点  $p$  に対して  $(K_p/k_p, \varepsilon_p)$  は可解とする. このとき  $(K/k, \varepsilon)$  は可解である.

**Fact 3(Neukirch[2])** 埋め込み問題  $(K/k, \varepsilon)$  は可解であるとする.  $S$  を  $k$  の素点の有限集合とし,  $S$  の元  $q$  に対して  $L(q)$  を  $(K_q/k_q, \varepsilon_q)$  の solution field とする.

このとき  $(K/k, \epsilon)$  の solution field  $L$  で,  $S$  の元  $q$  による  $L$  の完備化が  $L(q)$  と一致するものが存在する.

## §2 Main theorem

$(K/k, \epsilon)$  を, 図式 (\*) で定義される埋め込み問題とする. そこで分岐条件の付いた埋め込み問題  $(K/k, \epsilon, \emptyset)$  を次のように定義する.

**Definition**  $(K/k, \epsilon, \emptyset)$  は  $(K/k, \epsilon)$  と同じ図式 (\*) で定義される.  $\mathcal{O}$  から  $E$  への連続な準同型  $\psi$  が  $(K/k, \epsilon, \emptyset)$  の solution であるとは, 条件

- (1)  $\psi$  は  $(K/k, \epsilon)$  の solution,
- (2)  $\psi$  に対応する solution field は  $K$  上不分岐,

を満たすことである. さらに  $\psi$  が全射のとき,  $\psi$  は proper solution であるという.

このとき次の結果が得られた.

**Theorem 1** ガロア拡大  $K/k/\mathbf{Q}$  は条件

- (1)  $[k : \mathbf{Q}]$  は  $p$  と素,
- (2)  $K/k$  は不分岐  $p$  拡大,

を満たすとし,  $(\epsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(K/\mathbf{Q}) \rightarrow 1$  を, split しない中心拡大とする. このとき  $(K/\mathbf{Q}, \epsilon, \emptyset)$  は proper solution を持つ.

(証明の概略) 先ず, 埋め込み問題の一般論から,  $(K/\mathbf{Q}, \epsilon)$  は可解である. 次に条件

(1)(2) に注意すると, Fact 3 を用いて  $(K/\mathbf{Q}, \epsilon)$  の solution field  $L_1$  で  $L_1/K$  では,

$p$  の因子が不分岐なものが存在することが解る。このとき  $L_1$  は、 $(K/\mathbf{Q}, \varepsilon)$  の proper solution を与える。実際、 $L_1$  に対応する soluiton を  $\psi$  とし、 $\mathfrak{G}, \text{Gal}(K/\mathbf{Q}), E$  の  $p$ -Sylow 群をそれぞれ  $\mathfrak{G}(p), G(p), E(p)$  とすると、制限写像  $H^2(\text{Gal}(K/\mathbf{Q}), \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(G(p), \mathbf{Z}/p\mathbf{Z})$  が 1 対 1 であることより、 $1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E(p) \rightarrow G(p) \rightarrow 1$  が split しないことがわかる。よって、 $E(p)$  と  $G(p)$  の極小生成系の元の個数は等しく、 $\psi|_{\mathfrak{G}(p)}: \mathfrak{G}(p) \rightarrow E(p)$  は全射である。従って  $\psi: \mathfrak{G} \rightarrow E$  も全射となり、 $\psi$  は  $(K/\mathbf{Q}, \varepsilon)$  の proper solution である。 $L_1/K$  が不分岐ならば  $L_1$  が求めるガロア拡大体である。そこで  $L_1$  の素点  $q_1$  が  $L_1/K$  で分岐しているとする。 $q_1$  の  $K, \mathbf{Q}$  への制限をそれぞれ  $q, \mathfrak{q}$  とし、 $K_q$  に含まれる  $\mathbf{Q}_q$  上の最大  $p$  拡大を  $F$  とすると  $1 \rightarrow \text{Gal}(L_{1q_1}/K_q) \rightarrow \text{Gal}(L_{1q_1}/F) \rightarrow \text{Gal}(K_q/F) \rightarrow 1$  は split し、 $q$  の  $F$  への制限  $\bar{q}$  は  $F$  上の  $p$  次巡回拡大で分岐する。よって  $N_{F/\mathbf{Q}_q}(\bar{q}) \equiv 1 \pmod{p}$ 。今  $F/\mathbf{Q}_q$  は  $p$  拡大だから  $q \equiv 1 \pmod{p}$  を得る。

そこで  $T$  を  $\mathbf{Q}(\zeta_q)$  の  $p$  次部分体、 $\bar{q}$  を  $q$  の  $T \cdot L_1$  への延長とし、 $\bar{q}$  の  $T \cdot L_1/K$  における惰性体を  $L_2$  とする。このとき  $L_2$  は条件

- (a)  $L_2$  は  $(K/\mathbf{Q}, \varepsilon)$  の solution field,
- (b)  $L_2/K$  で  $q$  の因子は不分岐,
- (c)  $L_1/K$  で分岐しない素点は  $L_2/K$  でも分岐しない,

を満たす。従ってこの操作を続けると求めるガロア拡大が得られる。(証終)

### §3 Applications

この節では, **Theorem 1** の応用について述べる. 先ず2次体上の不分岐非アーベル  $p$  拡大の存在について次が言える.

**Theorem 2**  $k$  を2次体,  $p$  を奇素数とし,  $k$  のイデアル類群の  $p$ -rank が2以上であるとする. このとき不分岐ガロア拡大  $L/k$  で  $\text{Gal}(L/k)$  が

$$\langle \alpha, \gamma \mid \alpha^p = \beta^p = \gamma^p = 1, \gamma^{-1}\alpha\gamma = \alpha\beta, \beta^{-1}\alpha\beta = \alpha, \beta^{-1}\gamma\beta = \gamma \rangle$$

と同型なものが存在する.

(証明) 仮定より, 不分岐ガロア拡大  $K/k$  でそのガロア群が  $(\mathbf{Z}/p\mathbf{Z})^2$  と同型なものが存在する. このとき  $K$  は  $\mathbf{Q}$  上のガロア拡大で  $\text{Gal}(K/\mathbf{Q})$  は

$$G = \langle u, v, w \mid u^p = v^p = w^2 = 1, w^{-1}uw = u^{-1}, w^{-1}vw = v^{-1}, v^{-1}uv = u \rangle$$

と同型になることがわかる. そこで

$$E = \left\langle \alpha, \gamma, \delta \mid \begin{array}{l} \alpha^p = \beta^p = \gamma^p = \delta^2 = 1, \gamma^{-1}\alpha\gamma = \alpha\beta, \beta^{-1}\alpha\beta = \alpha, \\ \beta^{-1}\gamma\beta = \gamma, \delta^{-1}\alpha\delta = \alpha^{-1}, \delta^{-1}\beta\delta = \beta, \delta^{-1}\gamma\delta = \gamma^{-1} \end{array} \right\rangle$$

に対して, split しない中心拡大

$$1 \longrightarrow \langle \beta \rangle \longrightarrow E \xrightarrow{j} G \longrightarrow 1$$

を考える. ここで  $j$  は  $\alpha \mapsto u, \gamma \mapsto v, \delta \mapsto w$  で定義される準同型である. このとき **Theorem 1** より埋め込み問題  $(K/\mathbf{Q}, \varepsilon, \emptyset)$  は proper solution  $\psi$  を持つ.  $\psi$  に対応する solution field を  $L$  とすると  $L/k$  が求めるガロア拡大である.(証終)

次に Hilbert  $p$ -類体の類数の  $p$  可除性についての応用例をあげる.

**Theorem 3**  $l, p$  を異なる奇素数とし,  $p^f \equiv 1 \pmod{l}$  を満たす最小の自然数  $f$  は偶数であると仮定する. さらに,  $k/\mathbf{Q}$  はアーベル  $l$  拡大とする. このとき  $k$  の類数が  $p$  で割り切れるならば,  $k$  の最大不分岐アーベル  $p$  拡大体の類数もまた  $p$  で割り切れる.

(証明)  $k$  の類数が  $p$  で割り切れることより, ガロア拡大  $K/k/\mathbf{Q}$  で次の条件

(a)(b) を満たすものが存在する.

(a)  $K/k$  は不分岐初等アーベル  $p$  拡大.

(b) ガロア拡大  $K'/k/\mathbf{Q}$  で  $k \subsetneq K' \subsetneq K$  を満たすものは存在しない.

このとき  $\text{Gal}(k/\mathbf{Q})$  は  $\text{Gal}(K/k)$  に作用し, 群環  $\mathbf{F}_p[\text{Gal}(k/\mathbf{Q})]$  の構造を調べることにより,  $p\text{-rank Gal}(K/k) = fl^j$  を満たす非負の整数  $j$  が存在することがわかる (cf.[5;Theorem 9]). よって,

$$H^2(\text{Gal}(K/k), \mathbf{Z}/p\mathbf{Z}) \cong (\mathbf{Z}/p\mathbf{Z})^{\frac{fl^j(fl^j+1)}{2}}.$$

今  $f$  が偶数だから

$$p^{\frac{fl^j(fl^j+1)}{2}} \not\equiv 1 \pmod{l}.$$

一方,

$$H^2(\text{Gal}(K/\mathbf{Q}), \mathbf{Z}/p\mathbf{Z}) \cong H^2(\text{Gal}(K/k), \mathbf{Z}/p\mathbf{Z})^{\text{Gal}(k/\mathbf{Q})}.$$

そこで  $\text{Gal}(k/\mathbf{Q})$  の  $H^2(\text{Gal}(K/k), \mathbf{Z}/p\mathbf{Z})$  への作用に関する軌道分解を考えると

$$H^2(\text{Gal}(K/k), \mathbf{Z}/p\mathbf{Z})^{\text{Gal}(k/\mathbf{Q})} \neq 0$$

がわかり,

$$H^2(\text{Gal}(K/\mathbf{Q}), \mathbf{Z}/p\mathbf{Z}) \neq 0$$

を得る. よって **split** しない中心拡大

$$(\varepsilon): 1 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow E \longrightarrow \text{Gal}(K/\mathbf{Q}) \longrightarrow 1$$

が存在し, **Theorem 1** よりガロア拡大  $L_1/K/\mathbf{Q}$  で  $\text{Gal}(L_1/\mathbf{Q})$  が  $E$  と同型かつ

$L_1/k$  が不分岐  $p$  拡大となるものが存在する. もし  $L_1/k$  がアーベル拡大ならば

$$H^2(\text{Gal}(L_1/\mathbf{Q}), \mathbf{Z}/p\mathbf{Z}) \neq 0$$

であることが同様に示される. 従って同じ操作を繰り返すことによりガロア拡大  $L/k/\mathbf{Q}$

で,  $L/k$  が不分岐非アーベル  $p$  拡大となるものが存在する. よって  $k$  の最大不分岐

アーベル  $p$  拡大体の類数は  $p$  で割り切れる. (証終)

**Remark.** 任意の素数  $p$  に対して, 類数が  $p$  で割り切れるような  $\mathbf{Q}$  上の 3 次巡回

拡大体が無限個存在することが知られている (cf. [6] [7]). よって **Theorem**

**3** の仮定を満たすような  $k$  は確かに存在する.

## References

- [1].M.Ikeda, Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem, Hamb.Abh.**24**(1960),126–131.
- [2].J.Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math.**21**(1973),59–116.
- [3].A.Nomura, On the existence of unramified  $p$ -extensions, Osaka J.Math.**28** (1991), 55–62
- [4].A.Nomura, On imbedding problems with ramification conditions and their applications, Dissertation, Kanazawa University,1991
- [5].A.Nomura, A remark on the class number of Hilbert's class fields (preprint).
- [6].K.Uchida, Class numbers of cubic cyclic fields, J.Math.Soc.Japan **26** No.3 (1974), 447–453.
- [7].L.Washington, Class Numbers of the Simplest Cubic Fields, Math.Comp.**48** (1987), 371–384.