Title	分岐条件の付いた埋め込み問題とその応用について(代数的整数論における最近の話題)
Author(s)	野村, 明人
Citation	数理解析研究所講究録 (1992), 797: 17-24
Issue Date	1992-08
URL	http://hdl.handle.net/2433/82784
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
第 797 巻 1992 年 17-24

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，$(\varepsilon): 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(K/k) \to 1$ を中心拡大とする．このとき埋め込み問題 $(K/k, \varepsilon)$ は，図式

$$
\begin{array}{ccccccccc}
 & & & & & & \mathfrak{G} & & \\
 & & & & & & \downarrow{\scriptstyle\varphi} & & \\
(\varepsilon): 1 & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & E & \xrightarrow{j} & \mathrm{Gal}(K/k) & \longrightarrow & 1
\end{array}
\qquad (*)
$$

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

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

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

$$
\begin{tikzcd}
 & & & \mathfrak{G}_\mathfrak{q} \arrow[d, "\varphi|_{\mathfrak{G}_\mathfrak{q}}"] & \\
(\varepsilon_\mathfrak{q}) : 1 \arrow[r] & \mathbf{Z}/p\mathbf{Z} \arrow[r] & E_\mathfrak{q} \arrow[r, "j|_{E_\mathfrak{q}}"] & G_\mathfrak{q} \arrow[r] & 1.
\end{tikzcd}
$$

ここで $G_\mathfrak{q}$ は $K_\mathfrak{q}/\boldsymbol{k}_\mathfrak{q}$ のガロア群, $\mathfrak{G}_\mathfrak{q}$ は $\boldsymbol{k}_\mathfrak{q}$ の絶対ガロア群, $E_\mathfrak{q}$ は $G_\mathfrak{q}$ の j による逆像を表す. また, $(K_\mathfrak{q}/\boldsymbol{k}_\mathfrak{q}, \varepsilon_\mathfrak{q})$ に対する solution, solution field 等は, $(K/\boldsymbol{k}, \varepsilon)$ 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 $(K/\boldsymbol{k}, \varepsilon)$ は可解とする. このとき $(K/\boldsymbol{k}, \varepsilon)$ は proper solution を持つ.

Fact 2(Neukirch[2]) $\boldsymbol{k}$ の任意の素点 $\mathfrak{p}$ に対して $(K_\mathfrak{p}/\boldsymbol{k}_\mathfrak{p}, \varepsilon_\mathfrak{p})$ は可解とする. このとき $(K/\boldsymbol{k}, \varepsilon)$ は可解である.

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

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

§2 Main theorem

$(K/\boldsymbol{k},\varepsilon)$ 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 $(K/\boldsymbol{k},\varepsilon,\emptyset)$ を次のように定義する．

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

(1) ψ は $(K/\boldsymbol{k},\varepsilon)$ の solution,

(2) ψ 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ψ が全射のとき，ψ 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 $K/\boldsymbol{k}/\mathbf{Q}$ は条件

(1)$[\boldsymbol{k}:\mathbf{Q}]$ は p と素,

(2)$K/\boldsymbol{k}$ は不分岐 p 拡大,

を満たすとし，$(\varepsilon): 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(K/\mathbf{Q}) \to 1$ を，split しない中心拡大とする．このとき $(K/\mathbf{Q},\varepsilon,\emptyset)$ 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，$(K/\mathbf{Q},\varepsilon)$ は可解である．次に条件(1)(2) に注意すると，**Fact 3** を用いて $(K/\mathbf{Q},\varepsilon)$ 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 ψ とし，$\mathfrak{G}$, 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 $H^2(\mathrm{Gal(K/}\mathbf{Q}), \mathbf{Z}/p\mathbf{Z}) \to H^2(G(p), \mathbf{Z}/p\mathbf{Z})$ が 1 対 1 であることより，$1 \to \mathbf{Z}/p\mathbf{Z} \to E(p) \to G(p) \to 1$ 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，$\psi|_{\mathfrak{G}(p)}\colon \mathfrak{G}(p) \to E(p)$ は全射である．従って $\psi : \mathfrak{G} \to E$ も全射となり，ψ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 $\mathfrak{q}_1$ が L_1/K で分岐しているとする． $\mathfrak{q}_1$ の $K, \mathbf{Q}$ への制限をそれぞれ $\mathfrak{q}, q$ とし，$K_\mathfrak{q}$ に含まれる $\mathbf{Q}_q$ 上の最大 p 拡大を F とすると $1 \to \mathrm{Gal}(L_{1\mathfrak{q}_1}/K_\mathfrak{q}) \to \mathrm{Gal}(L_{1\mathfrak{q}_1}/F) \to \mathrm{Gal}(K_\mathfrak{q}/F) \to 1$ は split し，$\mathfrak{q}$ 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 $N_{F/\mathbf{Q}_q}(\bar{q}) \equiv 1$ (mod. p). 今 $F/\mathbf{Q}_q$ は p 拡大だから $q \equiv 1$ (mod. p) を得る．

そこで T を $\mathbf{Q}(\zeta_q)$ の p 次部分体，$\tilde{\mathfrak{q}}$ を $\mathfrak{q}$ の $T\cdot L_1$ への延長とし，$\tilde{\mathfrak{q}}$ 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 $\mathrm{Gal}(L/k)$ が

$$\left\langle \alpha,\gamma \,|\, \alpha^p=\beta^p=\gamma^p=1, \gamma^{-1}\alpha\gamma=\alpha\beta, \beta^{-1}\alpha\beta=\alpha, \beta^{-1}\gamma\beta=\gamma \right\rangle$$

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 $\mathrm{Gal}(K/\mathbf{Q})$ は

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

と同型になることがわかる．そこで

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

に対して，split しない中心拡大

$$1 \longrightarrow <\beta> \longrightarrow E \xrightarrow{j} G \longrightarrow 1$$

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 ψ を持つ．　ψ 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，$p^f \equiv 1$ (mod. p) 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 $\mathrm{Gal}(k/\mathbf{Q})$ は $\mathrm{Gal}(K/k)$ に作用し，群環 $\mathbf{F}_p[\mathrm{Gal}(k/\mathbf{Q})]$ の構造を調べることにより，p–rank $\mathrm{Gal}(K/k)=fl^j$ 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，

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

今 f が偶数だから

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

一方，

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

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

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

がわかり，

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

を得る．よって split しない中心拡大

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

が存在し，Theorem 1 よりガロア拡大 $L_1/K/\mathbf{Q}$ で $\mathrm{Gal}(L_1/\mathbf{Q})$ 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

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

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.Wasington, Class Numbers of the Simplest Cubic Fields, Math.Comp.**48** (1987), 371–384.