

与えられた p 群を Galois 群にもつ体の構成に
関する Šafarevič の方法について

早大理工 足立恒雄

東工大理 小松啓一

第一節 序

K を与えられた代数体, p を素数とする。さらに G を任意に与えられた (有限) p 群とする。

Scholz - Reichardt - Šafarevič の定理 K の Galois 拡大 K' が Galois 群 $\text{Gal}(K'/K)$ が G と同型なるものが無数に存在する。

この定理は p が奇素数であるとき Scholz によって証明され, Reichardt によって独立に, しかしやや後れて, 簡単な証明が与えられた。 $p=2$ の場合も含めた証明は 20 年たって Šafarevič ([1]) によって与えられた。 Scholz と Reichardt の方法は有理数体上に体を構成していき, それを K 上にスライドする方法である。 Šafarevič の方法は直接 K 上に構成するという点においても優れている。本記録の目的は Šafarevič の証明のミスとトリッキーなところ, 簡易化することである。

第二節 Scholz 拡大

K を基礎体 k の (有限次) p 拡大とし $\text{Gal}(K/k)$ を G とかく。
 $\hat{\varphi}: \hat{G} \rightarrow G$ を p 群 $\hat{G}$ から G の上への準同型写像とする。 $\hat{\varphi}$ の核 $\text{Ker } \hat{\varphi}$ が $\hat{G}$ の中心に含まれ, しかも基本 p 群, 即ち $(p, \dots, p)$ 型アベル群であるときに, $\hat{G}$ は G の中心拡大 (central extension) であるという。 $L \supset K \supset k$ なる体の列があ, $\Sigma \text{Gal}(L/k)$ が $\text{Gal}(K/k)$ の中心拡大であるとき, L/k は K/k の中心拡大であるという。とくに $\text{Ker } \varphi$ が p 次巡回群であるときは, 拡大は単純 (simple) であるという。

埋蔵問題 $(K/k, \varphi, \hat{G})$ が解けるとは, K を含む体 L が存在し $\hat{G}$ が $\text{Gal}(L/k)$ と同型になりある同型対応 $\hat{\varphi}: \hat{G} \rightarrow \text{Gal}(L/k)$ により $\varphi = \text{nat} \cdot \hat{\varphi}$ となるとき, 即ち右の図式が可換になる時にいう。
 nat は自然な全射を意味す。

$$\begin{array}{ccc} \hat{G} & \xrightarrow{\varphi} & G = \text{Gal}(L/k) \\ & \searrow \hat{\varphi} & \nearrow \text{nat} \\ & & \text{Gal}(L/k) \end{array}$$

一般に Ω を k 上の Galois 拡大であるとき, k 上の Galois 群が基本 p 群であるような Ω の最大部分体を Ω/k の p -台 (p -support) といって, $\Sigma(\Omega/k)$ と記す。 Ω が p 拡大であれば $\Sigma(\Omega/k)$ は $\text{Gal}(\Omega/k)$ の Frattini 部分群に対応する部分体である。

K/k が次の諸条件を満足するとき, K/k は Scholz 拡大である, 乃至 Scholz 型であるといわれる:

- (1) p の素因子はすべて K/k で完全分解する,
- (2) 無限素点はすべて K/k で不分岐である,
- (3) 分岐素点は K/k において相対次数 1 をもつ,
- (4) y を K/k で分岐する k の素点とすると

$$N_k y \equiv 1 \pmod{p^h}$$

となる, $\equiv$ は N_k は k からの絶対ノルムをあらわす。 h は十分大きな数である。

第三節 埋蔵問題の与える条件

本節では 1 の原始 p 乗根が k に含まれているものとする。

K/k が Scholz 型であるならば, G の任意の中心拡大 $\hat{G}$ に対して埋蔵問題 $(K/k, \varphi, \hat{G})$ は解ける。

概略の証明をあげる。 $\hat{G}$ が単純拡大であるときを証明すればよいことは群論的にすぐわかる。

また $\text{Ker } \varphi$ の生成元, $\{z^{a(\sigma_i)}\}$ を群拡大 $\hat{G} \rightarrow G$ に対応する因子団 α 一つとする。 z を 1 の原始 p 乗根, $\langle z \rangle$ を z の生成する巡回群とする。単射

$$\langle z \rangle \longrightarrow K^\times$$

から導かれる準同型写像

$$H^2(G, \langle z \rangle) \longrightarrow H^2(G, K^\times)$$

は K/k が Scholz 型であることにより, null map となる。

とわかる。従って $\exists \alpha_\sigma \in K^\times (\sigma \in G)$ s.t.

$$\zeta_{\alpha(\sigma, \tau)} = \alpha_\sigma^\tau \alpha_{\sigma\tau}^{-1} \alpha_\tau$$

$$\therefore \alpha_{\sigma\tau}^p = \alpha_\sigma^{p\tau} \alpha_\tau^p$$

$H^1(G, K^\times) = 1$ だから $\exists \mu \in K^\times$ s.t.

$$\alpha_\sigma^p = \mu^{\sigma-1} \quad (\sigma \in G)$$

$K(\sqrt[p]{\mu})$ が求める解である。

$m \in \mathbb{F}^\times$ のとき μ のかわりに μm をとってよいことに注意すべきである。

$\alpha, \beta \in K^\times$ とする。 $\alpha\beta^{-1} \in K^{\times p}$ のとき

$$\alpha \approx \beta \quad \text{in } K$$

とわかる。 $\therefore$ $K^{\times p}$ はもちろん $\{\xi^p \mid \xi \in K^\times\}$ の元である。任意の $\sigma \in G$ に対して

$$\mu^\sigma \approx \mu \quad \text{in } K$$

となる $\mu \in K^\times$ を p-invariant number ということにする。 p-invariant numbers の全体のなす乗法群を部分群 $\mathbb{F}^\times K^{\times p}$ で商群をつくり、それを $M(K/\mathbb{F})$ とおくと上の命題によって

$$M(K/\mathbb{F}) \cong H^2(G, \mathbb{Z}/p)$$

なることがわかる。 $\mathbb{Z}/p$ は p-巡回群で G は $\mathbb{Z}/p$ に trivial に作用するものとする。

次に d 個の生成元をもつ自由群 F_d とおくと $\dots$

ただし $d = \dim^{(p)} H^1(G, \mathbb{Z}/p)$ とする。すると G は $\mathcal{S}_d$ の準同型像であるから, $\mathcal{S}_d/N \cong G$ とあらわせるような正規部分群 N が存在する。 $N' = N^p \cdot (N, \mathcal{S}_d)$ とおくとき(カロワ)コホモロロジー論でよく知られているように

$$H^2(G, \mathbb{Z}/p) \cong \text{Hom}^G(N, \mathbb{Z}/p) \cong C(N/N')$$

がなりたつ。ここに $C(N/N')$ は N/N' の指標群を表わす。

以上によつて2次の定理が示された:

定理1 $K/\mathbb{K}$ が Scholz 型であるとき,

$$H^2(G, \mathbb{Z}/p) \cong M(K/\mathbb{K}) \cong C(N/N')$$

$\mathcal{F}$ でもう2 $K/\mathbb{K}$ で分岐する $\mathbb{K}$ の素イデアル $\mathfrak{p}$ を表わす。 $\mathfrak{p}$ も $\mathcal{F}$ の上にある K の素イデアルの一つとする: $\mathfrak{p}|\mathcal{F}$

また π を $\mathfrak{p}$ でわれ, $\mathfrak{p}^2$ ではわれぬ $K^\times$ の元とする: $\mathfrak{p} \parallel \pi$
 $\mathfrak{p}^\sigma (\sigma \in G)$ に対して π は π^σ を用いることにする。よって

$$\left\{ \frac{\mu}{\mathfrak{p}} \right\} = \left(\frac{\mu, \pi}{\mathfrak{p}} \right)$$

とおく。右辺はノルム剰余記号である。

$$\left(\frac{\mu, \pi}{\mathfrak{p}} \right) = \left(\frac{\mu^\sigma, \pi^\sigma}{\mathfrak{p}^\sigma} \right) = \left(\frac{\mu, \pi^\sigma}{\mathfrak{p}^\sigma} \right) \quad (\sigma \in G)$$

である $\xrightarrow{\text{よって}}$ に留意する。もし $\mathfrak{p}$ が μ と素であれば, ノルム剰余記号の性質から

$$\left\{ \frac{\mu}{\mathfrak{f}} \right\} = \left(\frac{\mu}{\mathfrak{f}} \right)_K$$

である。右辺は p 中剰余記号である。

$$\left(\frac{\mu}{\mathfrak{f}^\sigma} \right)_K = \left(\frac{\mu^\sigma}{\mathfrak{f}} \right)_K = \left(\frac{\mu}{\mathfrak{f}} \right)_K$$

に留意する。

次に μ の生成する単項イデアルを考えると, K で

$$(\mu) = \mathfrak{J} \mathfrak{m} \mathfrak{O}^p \quad \dots (*)$$

と分解される。ここに $\mathfrak{J}$ は $K/\mathfrak{k}$ で分岐する素イデアルの積で自共役, 即ち $\mathfrak{J}^\sigma = \mathfrak{J}$ ($\sigma \in G$) になりたつこと, $\mathfrak{m}$ は $\mathfrak{k}$ のイデアル, $\mathfrak{O}$ は K のイデアルである。こういう分解ができることは μ が p -invariant number であることから直ちに導かれることである。

補題 1 X を p -inv. number の類の一つとする: $X \in M(K/\mathfrak{k})$

X には次の性質をもつ μ が存在する:

(1) (μ) を $(*)$ の形にあらわすとき, $\mathfrak{O}$ は $K/\mathfrak{k}$ で分岐する素イデアルと素である,

(2) μ は p -hyperprimary かつ totally positive,

(3) $\left\{ \frac{\mu}{\mathfrak{f}} \right\} = 1$ かつ各分岐イデアル $\mathfrak{f}$ に対して

なりたつ。

証明は $K/\mathbb{F}$ が Scholz 型 であることと, μ のかわりに $\mu m \alpha^p$ ($m \in \mathbb{F}$, $\alpha \in K$) をとってよいことから, 合同式の解を求める方法で示される。

ζ_n を 1 の原始 p 乗根とし $\mathbb{F}(\zeta_n)$ の p -support を $\mathbb{F}_n$ とする。また $\Sigma(K/\mathbb{F})$ を Σ と略記する。 μ を補題 1 の諸条件を満たすようにとるときアル 4 = 記号

$$\left(\frac{\sum \mathbb{F}_n / \mathbb{F}}{m} \right)$$

は X の代表 μ のとり方によらない。よってこれを

$$(X)_{K/\mathbb{F}}$$

であらわすことにする。次の補題は明らかである：

補題 2 $(X_1 X_2)_{K/\mathbb{F}} = (X_1)_{K/\mathbb{F}} (X_2)_{K/\mathbb{F}}$

定理 2 $K/\mathbb{F}$ は Scholz 型 であるとする。 $(X)_{K/\mathbb{F}} = 1$ であれば, $\hat{G}$ を X に対対応する G の単純中心拡大とするとき, $(K/\mathbb{F}, \varphi, \hat{G})$ には Scholz 型 の解が存在する。

証明は [1] 参照。

系. $K/\mathbb{F}$ は Scholz 型 であるとする。 $X_1, \dots, X_r$ を $H^2(G, \mathbb{Z}/p)$ の基底とする。 $(X_1)_{K/\mathbb{F}} = \dots = (X_r)_{K/\mathbb{F}} = 1$ ならば,

任意の X に対する埋蔵問題は Scholz 型の解をもつ。

系は定理 2 と補題 2 とからあきらかである。

第四節 体の構成

$\mathbb{C} \in \mathbb{K}$ の場合を扱う。

S_d を d 個の文字 $s_1, \dots, s_d$ で生成される自由群とし、

$$N_d^{(0)} = S_d, \quad N_d^{(c+1)} = N_d^{(c)P}(N_d^{(c)}, S_d)$$

によって S_d の正規部分群 $N_d^{(c)}$ を定義する。さらに

$$G_d^{(c)} = S_d / N_d^{(c)}, \quad Z_d^{(c)} = N_d^{(c)} / N_d^{(c+1)}$$

と置く。 $K/\mathbb{K}$ は Galois 群 $G_d^{(c)}$ をもつ Scholz 型拡大であると仮定する。 δ が d にくらべて十分小なときには $K/\mathbb{K}$ の部分体 $\mathbb{C}$ で Galois 群 $G_\delta^{(c)}$ をもち invariant $(X)_{\mathbb{C}/\mathbb{K}}$ が任意の $X \in H^2(G_\delta^{(c)}, \mathbb{Z}/p)$ に対して 1 であるものが存在することを証明する。この目標である。

$\delta < d$ とし、 $\{s_1, \dots, s_d\}$ を δ 個の空でない部分集合 $\mathcal{S}^{(j)}$ ($j=1, \dots, \delta$) の disjoint union にわける：

$$\{s_1, \dots, s_d\} = \bigcup_{j=1}^{\delta} \mathcal{S}^{(j)}, \quad \mathcal{S}^{(j)} \cap \mathcal{S}^{(j')} = \emptyset \quad (j \neq j')$$

この分割は今後固定しておく。

$\mathcal{S}^{(j)}$ を $\mathcal{S}^{(j)}$ の空でない部分集合とする。 $j=1, \dots, \delta$

$S^{(j)}$ に属する元はすべて t_j に, $S^{(j)} - S^{(j)}$ に属する元はすべて単位元 1 に写すことにより得られる S_d から, $t_1, \dots, t_g$ により生成される自由群 S_g への準同型写像を考える。このような型の準同型写像は標準的であると称される。 S を標準的な準同型写像: $S_d \longrightarrow S_g$ とすると, S から $G_d^{(c)}$ から $G_g^{(c)}$ への, また $Z_d^{(c)}$ から $Z_g^{(c)}$ への準同型写像が誘導される。これも S であるから, $S: Z_d^{(c)} \longrightarrow Z_g^{(c)}$ が全射であるから, 単射: $C(Z_g^{(c)}) \longrightarrow C(Z_d^{(c)})$ が得られる。これも S であるから:

$$X^S(x) = X(x^S) \quad \text{for } x \in Z_g^{(c)}, x \in Z_d^{(c)}$$

K^S によって $S: G_d^{(c)} \longrightarrow G_g^{(c)}$ の kernel によってうごかなる元 a なる K の部分体をあらわす。その図式

$$\begin{array}{ccc} C(Z_g^{(c)}) & \xrightarrow{S} & C(Z_d^{(c)}) \\ \downarrow \wr & & \downarrow \wr \\ M(K^S/k) & \xrightarrow{\text{inj}} & M(K/k) \end{array}$$

が可換であることがわかる。

$S_1, \dots, S_m$ を標準的な準同型写像とする。各 j に対して

$$S_\lambda^{(j)} \cap S_\mu^{(j)} = \emptyset \quad (\lambda, \mu = 1, \dots, m), \lambda \neq \mu$$

がみたされるべき, 独立であるといわれる。 $S_\lambda^{(j)}$ は, もちろん, $S^{(j)}$ の部分集合で t_j に写像される元の全体を意味する。

α とし $j = 1, 2, \dots, d$ に対して

$$(S_1 * \dots * S_m)^{(j)} = S_1^{(j)} \cup \dots \cup S_m^{(j)}$$

と定義すれば, 新しい標準的準同型写像 $S_1 * \dots * S_m$ がえられる。 $\Sigma \in K/k$ の p -support とし,

$$\Sigma = k(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_d}).$$

$$(\sqrt{\alpha_\nu})^{\delta_\mu} = \zeta^{\delta_{\nu\mu}} \sqrt{\alpha_\nu}$$

となるように $\alpha_1, \dots, \alpha_d \in k$ をえらぶ。 $\zeta = \zeta_{p^m}$ は Kronecker $\alpha \delta$ である。 Σ を標準的準同型写像とすると, $\alpha_{S^{(j)}} = \prod_{S_\nu \in S^{(j)}} \alpha_\nu$ とおくと

$$\Sigma^S = k(\sqrt{\alpha_{S^{(1)}}}, \dots, \sqrt{\alpha_{S^{(d)}}})$$

とかけると, Σ^S は K^S/k の p -support である。

いま $X \in C(Z_S^{(j)})$ をえらんで固定する。 X^S に対応する $C(Z_d^{(j)})$ の元とする。 X^S に属する補題 1 を満足する p -inv. number in K を μ_S とする。 $(\mu_S) \approx \mathcal{I}_S m_S$ in K とき S に対して

$$\left[\left(\frac{\alpha_{S^{(1)}}}{m_S} \right)_k, \dots, \left(\frac{\alpha_{S^{(d)}}}{m_S} \right)_k, \left(\frac{k_2/k}{m_S} \right) \right] \in G_S'' \times G(k_2/k)$$

を対応づける写像を考える。これを $X(S)$ であらわそう。

$X(S) = 1$ ならば ~~$(X)_{K^S/k}$~~ $(X)_{K^S/k} = 1$ である。

$X(S)$ が $\deg \leq m$ であるとは, 任意の独立な標準的準同型写像 $S_1, \dots, S_{m+1}$ に対して

$$\prod_{j_1 < \dots < j_k} X(S_{j_1} * \dots * S_{j_k})^{(-1)^k} = 1$$

のなりたつことをいふ。こゝに $(j_1, \dots, j_k)$ は $(1, \dots, n)$ の空でない subset をいう。

定理 3 $C(Z_f^{(c)})$ の任意の元 X に対し

$$\deg X(S) \leq c+1$$

証明. $S_1, \dots, S_{c+2}$ が独立であるとき。

$$\prod_{j_1 < \dots < j_k} X(S_{j_1} * \dots * S_{j_k})^{(-1)^k} = \prod_{j_1 < \dots < j_k} \left[\left(\frac{\alpha(S_{j_1} * \dots * S_{j_k})^{(1)}}{m_{S_{j_1} * \dots * S_{j_k}}} \right)^{(-1)^k}, \dots, \left(\frac{f_k/f}{m_{S_{j_1} * \dots * S_{j_k}}} \right)^{(-1)^k} \right]$$

より成分に注目する。

$$\prod_{j_1 < \dots < j_k} \left(\frac{\alpha(S_{j_1} * \dots * S_{j_k})^{(1)}}{m_{S_{j_1} * \dots * S_{j_k}}} \right)^{(-1)^k} = \prod_{j_1 < \dots < j_k} \prod_{r=1}^k \left(\frac{\alpha_{S_{j_k}}^{(1)}}{m_{S_{j_1} * \dots * S_{j_k}}} \right)^{(-1)^k}$$

$$= \prod_{j_1 < \dots < j_k} \prod_{r=1}^k \left(\frac{\alpha_{S_{j_r}}^{(1)}}{m_{S_{j_r} * S_{j_1} * \dots * S_{j_k}}} \right)^{(-1)^k} \quad (\because S_{j_1} * \dots * S_{j_k} = S_{j_r} * S_{j_1} * \dots * S_{j_k})$$

$$= \prod_{j=1}^{c+2} \prod_{j_1 < \dots < j_{k-1}} \left(\frac{\alpha_{S_j}^{(1)}}{m_{S_j * S_{j_1} * \dots * S_{j_{k-1}}}} \right)^{(-1)^{k-1}}$$

$$= \prod_{j=1}^{c+2} \left(\frac{\alpha_{S_j}^{(1)}}{\prod_{j_1 < \dots < j_{k-1}} m_{S_j * S_{j_1} * \dots * S_{j_{k-1}}}} \right)^{(-1)^{k-1}}$$

よって $S_0, S_1, \dots, S_{c+1}$ が独立であるとき

$$\prod_{j_1 < \dots < j_k} X^{S_0 * S_{j_1} * \dots * S_{j_k}} (-1)^k = 1$$

である ([1] 参照), 故に補題 2 によって

$$\left(\frac{\alpha_{S_j^{(1)}}}{\prod_{j_1 < \dots < j_k} m_{S_j * S_{j_1} * \dots * S_{j_{k-1}}} (-1)^{k-1}} \right) = 1$$

他の成分についても同様であるから証明された。

d が δ に対して十分大なるときには定理 3 から

$$X_i(S) = 1 \quad (i=1, 2, \dots, r)$$

(Σ に $X_1, \dots, X_r$ は $(\mathbb{Z}_\delta^{(r)})$ の基底である。) となるような α の存在が証明される。 ([1], Theorem 3)

もし $\mathbb{F}$ の場合の考察は略すか, 結果だけみると Scholz 型拡大 $K/\mathbb{F}$ に対して, 任意の埋蔵問題 $(K/\mathbb{F}, \varphi, \hat{G})$ は Scholz 型の解をもつので, 本稿後半部のような群論的考察は不要となる。

文 献

- [1] Šafarevič, On the Construction of fields with a given Galois group of order l^a , Amer. Math. Soc. Transl. (2) 4 (1956) 107-142