数理解析研究所講究録
第230巻 1975年 1-12



# 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

## §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。

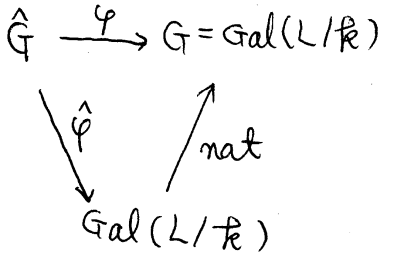
Scholz-Reichardt-Šafarevičの定理　$k$のGalois拡大$K$でGalois群$\mathrm{Gal}(K/k)$が$G$と同型なるものが無数に存在する。

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おき，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の証明のミスをとりのぞき，簡易化することである。

## §二節　Scholz拡大

$K$ を基礎体 $k$ の(有限次) $p$ 拡大とし $\mathrm{Gal}(K/k)$ を $G$ とかく。$\hat{\varphi}: \hat{G} \longrightarrow G$ を $p$ 群 $\hat{G}$ から $G$ の上への準同型写像とする。$\hat{\varphi}$ の核 $\mathrm{Ker}\,\hat{\varphi}$ が $\hat{G}$ の中心に含まれ，しかも基本 $p$ 群，即ち $(p,\cdots,p)$ 型アー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。$L \supset K \supset k$ なる体の列があって $\mathrm{Gal}(L/k)$ が $\mathrm{Gal}(K/k)$ 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 $\mathrm{Ker}\,\varphi$ 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 $L$ が存在して $\hat{G}$ が $\mathrm{Gal}(L/k)$ と同型になりある同型対応 $\hat{\varphi}: \hat{G} \longrightarrow \mathrm{Gal}(L/k)$ によって $\varphi = \mathrm{nat}\cdot\hat{\varphi}$ となるとき，即ち右の図式が可換になるときにいう。nat は自然な全射を意味する。




一般に $\Omega$ 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 $\Omega$ の最大部分体を $\Omega/k$ の $p$-台 ($p$-support) といって，$\Sigma(\Omega/k)$ と記す。$\Omega$ が $p$ 拡大であれば $\Sigma(\Omega/k)$ は $\mathrm{Gal}(\Omega/k)$ 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) $\mathfrak{p}$ を $K/k$ で分岐する $k$ の素点とすると

$$N_k \mathfrak{p} \equiv 1 \mod p^h$$

となる，ここに $N_k$ は $k$ からの絶対ノルムをあらわす。$h$ は十分大なる数である。

## 第三節 埋蔵問題のとける条件

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。

概略の証明をのべる。$\hat{G}$ 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。

$z$ を $\mathrm{Ker}\,\varphi$ の生成元，$\{z^{a(\sigma,\tau)}\}$ を群拡大 $\hat{G} \longrightarrow G$ に対応する因子団の一つとする。$\zeta$ を 1 の原始 $p$ 乗根，$\langle\zeta\rangle$ を $\zeta$ の生成する巡回群とする。単射

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

から導かれる準同型写像

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

は $K/k$ が Scholz 型であることによって，null map となるこ

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

$$\zeta^{a(\sigma,\tau)} = \alpha_\sigma^\tau \alpha_{\sigma\tau}^{-1} \alpha_\tau$$

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

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

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

$k(\sqrt[p]{\mu})$ が求める解である。

$m \in k^\times$ のとき $\mu$ のかわりに $\mu m$ をとってもよいことに注意すべきである。

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

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

とあらわす。ここに $K^{\times p}$ はもちろん $\{\xi^p \mid \xi \in K^\times\}$ のことである。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 <u>p- invariant number</u> ということにする。p-invariant numbers の全体のなす乗法群を部分群 $k^\times K^{\times p}$ で商群をつくり，それを $M(K/k)$ であらわすと上の命題によって

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

なることがわかる。$\mathbb{Z}/p$ は $p$ 次巡回群で $G$ 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を $S_d$ であらわす。~~すると~~

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

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

がなりたつ。ここに $C(N/N')$ は $N/N'$ の指標群を表わす。以上によって次の定理が示された：

<u>定理1</u>　$K/k$ が Scholz 型であるとき，

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

$\mathfrak{p}$ でもって $K/k$ で分岐する $k$ の素イデアルを表わす。$\mathfrak{P}$ を $\mathfrak{p}$ の上にある $K$ の素イデアルの一つとする：$\mathfrak{P}|\mathfrak{p}$

また $\Pi$ を $\mathfrak{P}$ でわれ，$\mathfrak{P}^2$ ではわれない $K$ の元とする：$\mathfrak{P} \| \Pi$

$\mathfrak{P}^\sigma$ ($\sigma \in G$) に対しては $\Pi^\sigma$ を用いることにする。そこで

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

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 ~~ことから~~ に留意する。もし $\mathfrak{P}$ が $\mu$ と素であれば，ノルム剰余記号の性質から

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

である。右辺は $\mathfrak{p}$ 中剰余記号である。

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

に留意する。

次に $\mu$ の生成する単項イデアルを考えると，$K$ で

$$(\mu) = \mathfrak{P}\mathfrak{M}\mathfrak{Q}^p \qquad \cdots\cdots (*)$$

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

<u>補題1</u>　$X$ を p-inv. number の類の一つとする：$X \in M(K/k)$
$X$ には次の性質をもつ $\mu$ が存在する：

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

(2)　$\mu$ は p-hyperprimary かつ totally positive，

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

なりたつ。

証明は $K/k$ が Scholz 型であることと，$\mu$ のかわりに $\mu m \alpha^p$ ($m \in k$, $\alpha \in K$) 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。

$\zeta_n$ を 1 の原始 $p^n$ 乗根とし $k(\zeta_n)$ の $p$-support を $k_n$ とする。また $\Sigma(K/k)$ を $\Sigma$ と略記する。$\mu$ を補題 1 の諸条件をみたすようにとるときアルチン記号

$$\left( \frac{\Sigma k_n / k}{\mathfrak{m}} \right)$$

は $\mathfrak{m}$ の代表 $\mu$ のとり方によらない。そこでこれを

$$(X)_{K/k}$$

であらわすことにする。次の補題は明らかである：

補題 2　$(X_1 X_2)_{K/k} = (X_1)_{K/k} (X_2)_{K/k}$

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

証明は [1] 参照。

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

任意の $X$ に対応する埋蔵問題は 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

$\zeta \in k$ の場合を扱う。

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

$$N_d^{(0)} = S_d, \qquad N_d^{(c+1)} = N_d^{(c)p}(N_d^{(c)}, S_d)$$

によって $S_d$ の正規部分群 $N_d^{(c)}$ を定義する。さらに

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

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

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

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

この分割は今後固定しておく。

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

$S^{(j)}$ に属する元はすべて $t_j$ に，$\mathcal{S}^{(j)} - S^{(j)}$ に属する元はすべて単位元 1 に写すことによって得られる $S_d$ から，$t_1, \cdots, t_g$ によって生成される自由群 $S_g$ 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。これらもすべて $S$ であらわす。$S: Z_d^{(c)} \longrightarrow Z_g^{(c)}$ 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 $S$ であらわそう：

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

$K^S$ でもって $S: G_d^{(c)} \longrightarrow G_g^{(c)}$ の kernel によってうごかない元のなす $K$ の部分体をあらわす。すると図式

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

が可換であることがわかる。

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

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

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

このとき $j=1,2,\cdots,\delta$ に対して

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

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

$$\Sigma=k(\sqrt[p]{\alpha_1},\cdots,\sqrt[p]{\alpha_d}),$$

$$(\sqrt[p]{\alpha_\nu})^{S_\mu}=\zeta^{\delta_{\nu\mu}}\sqrt[p]{\alpha_\nu}$$

となるように $\alpha_1,\cdots,\alpha_d\ (\in k)$ をえらぶ。ここに $\delta_{\nu\mu}$ は Kronecker の $\delta$ である。そこで $S$ を標準的準同型写像とするとき，$\alpha_{S^{(j)}}=\prod_{S_\nu\in S^{(j)}}\alpha_\nu$ とおくと

$$\Sigma^S=k(\sqrt[p]{\alpha_{S^{(1)}}},\cdots,\sqrt[p]{\alpha_{S^{(\delta)}}})$$

とかける，ここに $\Sigma^S$ は $K^S/k$ の p-support である。

いま $X\in C(Z_\delta^{(1)})$ をえらんで固定する。$X^S$ を対応する $C(Z_d^{(1)})$ 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 $\mu_S$ とする。$(\mu_S)\approx\vartheta_S\mathfrak{m}_S$ in $K$ のとき $S$ に対して

$$\left[\left(\frac{\alpha_{S^{(1)}}}{\mathfrak{m}_S}\right)_k,\cdots,\left(\frac{\alpha_{S^{(\delta)}}}{\mathfrak{m}_S}\right)_k,\left(\frac{k_k/k}{\mathfrak{m}_S}\right)\right]\in G_\delta^{(1)}\times G(k_k/k)$$

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 ~~$(X^S)_k$~~ $(X)_{K^S/k}=1$ である。

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

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

のなりたつことをいう。ここに$(j_1, \cdots, j_k)$は$(1, \cdots, n+1)$の空でないsubsetをうごく。

定理3　$C(Z_S^{(c)})$の任意のえXに対して

$$\deg \chi(S) \leqq c+1$$

証明. $S_1, \cdots, S_{c+2}$が独立であるとする。

$$\prod_{j_1<\cdots<j_k} \chi(S_{j_1}*\cdots*S_{j_k})^{(-1)^k} = \prod_{j_1<\cdots<j_k} \left[ \left( \frac{\alpha(S_{j_1}*\cdots*S_{j_k})^{(1)}}{m_{S_{j_1}*\cdots*S_{j_k}}} \right)^{(-1)^k}, \cdots, \left( \frac{f_{k_k}/f}{m_{S_{j_1}*\cdots*S_{j_k}}} \right)^{(-1)^k} \right]$$

第1成分に注目する.

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

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

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

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

ところで$S_0, S_1, \cdots, S_{c+1}$が独立のとき

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

である（[1] 参照），故に補題2によって

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

他の成分についても同様であるから証明された。

$d$ が $\delta$ に対して十分大なるときには定理3から

$$\chi_i(S) = 1 \qquad (i = 1, 2, \cdots, r)$$

（ここに $\chi_1, \cdots, \chi_r$ は $(Z_\delta^{(1)})$ の基底である。）となるような $S$ の存在が証明される。（[1], Theorem 3）

$\mathfrak{k} \neq \mathfrak{k}$ の場合の考察は略すが，結果だけのべると Scholz 型拡大 $K/\mathfrak{k}$ に対して，任意の埋蔵問題 $(K/\mathfrak{k}, \varphi, \hat{G})$ 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