3.　局所体のガロア群の構造について

朝田 衞（京都工芸繊維大学工芸科学研究科）

この講演では、岩澤全集の論文 [29]

On Galois groups of local fields, Trans. Amer. Math. Soc., **80** (1955), 448-469.

の紹介を行いました。

原論文の紹介、という趣旨から、主結果の内容やその証明方法だけでなく、用語や記号もなるべく原論文のままにするようにしましたが、一部の用語や記号については、現在の慣用に従っています。また、原論文では、代数的な準備を前半で行い、その後、それらを数論的な状況に適用して主結果の説明や証明に進む、という順序で書かれていますが、講演では、主結果の説明、その証明という順序で紹介しました。（Theorem, Lemma 等の番号は [29] のとおりにしましたので、説明の順序どおりではありません。）

以下は、ほぼ講演内容になっていますが、講演時には時間の関係で触れられなかったことを、本文中に、或いは註として、追加しました。

3.0　主結果（概要）

p を素数とし、$\mathbf{Q}_p$ を p 進体、Ω を $\mathbf{Q}_p$ の代数的閉包とし、以下、$\mathbf{Q}_p$ の拡大体はすべて Ω の中で考えます。

k を $\mathbf{Q}_p$ の有限次拡大体とし、T, V をそれぞれ拡大体 Ω/k の惰性体、分岐体とします。

この論文の結果は、k の絶対ガロア群 $\mathrm{Gal}(\Omega/k)$ に関するもので、大きく次の４つにまとめられます。

I　$\mathrm{Gal}(V/k)$ の位相群としての構造

II　$\mathrm{Gal}(\Omega/V)$ の位相群としての構造

III　短完全列

$$1 \longrightarrow \mathrm{Gal}(\Omega/V) \longrightarrow \mathrm{Gal}(\Omega/k) \longrightarrow \mathrm{Gal}(V/k) \longrightarrow 1$$

は split すること
IV Gal(Ω/V) のアーベル化群の Gal(V/k)-加群としての構造
いずれも基本的な結果ですが、主要な結果は **IV** でしょう。（論文にもそう書かれていますし、証明ももっとも込み入っています。）以下の 3.1 から 3.4 では、それぞれ **I** から **IV** の詳しい内容とその証明（の概略）を紹介します。

3.1 Gal(V/k) の位相群としての構造

(1-1) k の剰余体の元の個数を q とします。このとき、ガロア群 Gal(V/k) は、二つの元 σ, τ で生成され、一つの関係式 $\sigma\tau\sigma^{-1} = \tau^q$ で定義される profinite group と同型であり、σ は Gal(T/k) のフロベニウス置換を引き起こす元ととれる、というのが得られている結果です。

k の素元 π_1 をひとつ固定します。p と素な任意の正の整数 e について、1 の原始 e 乗根 ξ_e, π_1 の e 乗根 π_e を $e = e_1 e_2$ ならば $\xi_e^{e_1} = \xi_{e_2}$, $\pi_e^{e_1} = \pi_{e_2}$ が成り立つように定めます。

正の整数 f に対し、$e = q^f - 1$ とおき、k の拡大体 E_f, F_f を

$$E_f = k(\xi_e, \pi_e), \quad F_f = k(\xi_e)$$

により定めます。よく知られているように、

$$V = \bigcup F_f, \quad T = \bigcup E_f \tag{1.1}$$

が成り立ちます [1)] 。

従って、Gal(V/k) の元 σ', τ' で、p と素なすべての e について

$$\xi_e^{\sigma'} = \xi_e^q,\ \pi_e^{\sigma'} = \pi_e,\ \ \xi_e^{\tau'} = \xi_e,\ \pi_e^{\tau'} = \pi_e \xi_e$$

を満たすものが一意的に定まります。(1.1) により、Gal(V/k) は σ', τ' により生成されます。また、この二つの元が関係式

$$\sigma'\tau'\sigma'^{-1} = \tau'^q$$

を満たすことも容易にわかります。
(1-2) 二つの元 α, β で生成され、ただ一つの関係式 $\alpha\beta\alpha^{-1} = \beta^q$ により定義される（抽象）群を J とし、Γ を J の profinite completion とします。J から Γ への標準準同型による α, β の像を、それぞれ σ, τ とすると、以上のことから、全射準同型

$$\psi : \Gamma \longrightarrow \mathrm{Gal}(V/k)$$

で $\psi(\sigma)=\sigma', \psi(\tau)=\tau'$ をみたすものが定まります。

よって、ψ が同型となることを示せばよいわけですが、それは次のようにしてわかります。$G_{e,f}$ を、二つの元 σ,τ で生成され、関係式 $\sigma\tau\sigma^{-1}=\tau^q, \sigma^f=1, \tau^e=1$ で定義される有限群（位数は ef で $q^f\equiv 1 \bmod e$) とすると、J の有限商群はこのような $G_{e,f}$ 全体となることがわかります。従って、Γ は $G_{e,f}$ 全体の射影極限になります：

$$\Gamma=\varprojlim G_{e,f}.$$

一方、$G_{e,f}$ は自然に $\mathrm{Gal}(E_f/k)$ と同型ですから、(1.1) により、ψ が同型となることが従います。

3.2 $\mathrm{Gal}(\Omega/V)$ の位相群としての構造

(2-1) ガロア群 $\mathrm{Gal}(\Omega/V)$ は、可算無限個の元で生成される free pro-p group と同型である、というのが得られている結果です。（生成元に canonical なものがあるわけではありません。）

これを証明するために、まず、岩澤全集の論文 [27]

> *On solvable extensions of algebraic number fields*, Ann. of Math.,(2) **58** (1953), 548-572.

から、結果を二つ引用します。（定理の番号は、[27] のとおり。）

Theorem 1 k を 1 の原始 p 乗根を含む体とする。このとき、embedding problem

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(K/k) & & \\ & & & & & & \big\downarrow \varphi & & \\ 1 & \longrightarrow & N & \longrightarrow & G & \stackrel{\alpha}{\longrightarrow} & G/N & \longrightarrow & 1 \end{array} \tag{2.1}$$

が任意の p-群 G について solution を持つ [2)] 為の条件は次の (i),(ii) である。

(i) 任意の有限次 p-拡大 K/k に対して、$H^2(\mathrm{Gal}(K/k),K^*)=\{0\}$

(ii) 体 k の乗法群 k^* の商群 $k^*/(k^*)^p$ は無限群である

次に、F を 可算無限個の元 x_i $(i=1,2,\dots)$ で生成される自由群、p を素数とします。pro-p 群 F_S を

$$F_S=\varprojlim F/N$$

と定義します。ここで、N は F/N が有限 p-群となるような正規部分群で、かつほとんどすべての x_i を含むものを動きます。そのような N は可算個ですから、

F_S の開部分群は可算個で、そのような位相群を separable topological group と呼びます。(代数体や局所体のガロア群として実現される profinite group は separable なものに限ります。) F_S を、$x_1, x_2, \ldots$ で生成される free pro-p group とよびます。

このとき、次の定理が成り立ちます。

Theorem 5 k を体、Σ を k の最大 pro p-拡大体とする。このとき、$\mathrm{Gal}(\Sigma/k)$ が F_S と同型となるための必要十分条件は、$\mathrm{Gal}(\Sigma/k)$ が separable で、かつ、任意の有限 p-群の短完全列と任意の全射準同型 φ に対して、embedding problem (2.1) が solution を持つことである。

補足 「pro-p」を「profinite」、「prosolvable」等に置き換えても同様の結果は成り立ちます。

(2-2) 上記の定理を $k = V$ について適用します。Ω は V の最大 pro-p 拡大体で、$\mathrm{Gal}(\Omega/V)$ は separable, また V は 1 の原始 p 乗根を含むことに注意します。

まず、V が T を含んでいることから、局所類体論により、任意の有限次 p-拡大 K/V に対して、

$$H^2(\mathrm{Gal}(K/V), K^*) = \{0\}$$

が成り立ちます。

次に、$V = \bigcup E_f$ であることから、$V^*/(V^*)^p$ が無限群であることも(容易に)わかりますので、Theorems 1, 5 により、$\mathrm{Gal}(\Omega/V)$ が F_S に同型であることが従うわけです。

3.3 短完全列の splitting について

(3-1) Γ を、σ, τ で生成され、関係式 $\sigma\tau\sigma^{-1} = \tau^q$ により定義される profinite group とします。Γ_0 を τ で生成される Γ の閉部分群 とすると、Γ_0 は 正規部分群で、

$$\Gamma_0 \simeq \widehat{\mathbf{Z}}^{(p')}, \quad \Gamma/\Gamma_0 \simeq \widehat{\mathbf{Z}}$$

が成り立ちます。ただし、$\widehat{\mathbf{Z}}$ は加法群 $\mathbf{Z}$ の profinite completion, $\widehat{\mathbf{Z}}^{(p')}$ は加法群 $\mathbf{Z}$ を、指数が有限で、かつ p と素な部分群全体で completion した群を表します。

短完全列の splitting を示すためには、もう少し一般に次の Lemma を示せば十分です。

Lemma 4　G を profinite group とし、N を G の閉正規部分群で、$G/N = \Gamma$ かつ N は pro-p 群なるものとする。このとき、G の閉部分群 H で、$H \cap N = \{1\}$ かつ $G = HN$ を満たすものが存在する。

(3-2) Lemma 4 の証明には、次の Lemma を用います。

Lemma 5　G を profinite group とし、N を G の閉正規部分群で、"N の位数と N の指数は互いに素"[3] とする。このとき、次の (i),(ii) が成り立つ。
(i) G の閉部分群 H で、$H \cap N = \{1\}$ かつ $G = HN$ を満たすものが存在する。
(ii) N 又は G/N が可解群ならば、(i) の閉部分群 H は共役を除いて一意的である。

この証明は、G が有限群の場合に帰着します。G が有限群の場合は、Schur-Zassenhaus の定理とも呼ばれます。この場合は、仮定より N の位数、G/N の位数の少なくとも一方は奇数ですから、Feit-Thompson の定理によれば、N, G/N のいずれかは可解群となり、(ii) の仮定ははずすことができます。ただし、Feit-Thompson の定理の論文は 1963 年で、この論文より後です。

Lemma 5 を用いると、Lemma 4 の証明は次のようになります。

まず、G' を G の正規部分群で、N を含み $G'/N = \Gamma_0$ となるものとします。N の位数と N の指数は互いに素なので、Lemma 5 により、

$$H_1 \cap N = \{1\},\ G' = H_1 N$$

を満たすものが存在します。

次に、G/G' は $\widehat{\mathbf{Z}}$ に同型ですから、G の元 a で、$a \bmod G'$ が G/G' を（位相群として）生成するものがあります。a で生成される G の部分群 $<a>$ と H_1 との積 $<a> H_1$ が splitting を与えていればよいのですが、必ずしもそうはなっていないので、以下のようにして a を取替えます。

$$H_2 = aH_1a^{-1}$$

とおくと、H_2 も G'/N の splitting を与えることは容易にわかりますので、Lemma 4 (ii) により、$H_1 = bH_2b^{-1}$ を満たす G' の元 b があります。従って $H_1 = (ba)H_1(ba)^{-1}$, 即ち、ba は H_1 を normalize します。これより、（a を ba に取り替えて）$H = <ba> H_1$ とおくと、H が splitting を与えること、即ち、$H \cap N = \{1\}, G = HN$ となることがわかります。
(3-3) 講演では触れることができませんでしたが、この結果の意義を少し補足しておきます。

証明からもわかるように、短完全列

$$1 \longrightarrow \mathrm{Gal}(\Omega/V) \longrightarrow \mathrm{Gal}(\Omega/k) \longrightarrow \Gamma \longrightarrow 1$$

の splitting は canonical なものがあるわけではありません。しかし、とにかく splitting があることから、Γ を（splitting を通して、共役により）Gal(Ω/V) に作用させることができます。これにより、Gal(Ω/V) は、「作用域 Γ を持つ pro-p 群」となるわけです。この論文の主要な結果は、Gal(Ω/V) のアーベル化群への、Γ の作用を決めたものですが、Gal(Ω/V) 自身の「作用域 Γ を持つ pro-p 群」としての構造の研究 4) は、その後、H. Koch[HK65] へと受け継がれて行きます。

3.4 Gal(Ω/V) のアーベル化群の Γ-加群としての構造

(4-1) 3.1 と少し記号が変わりますが、まず、$e = q^f - 1$ とし、ξ を 1 の原始 e 乗根、$F = k(\xi)$ とします。π は k の素元の e 乗根とし、$E = k(\xi, \pi)$ とします。このとき、E は k のガロア拡大体で、ガロア群 G は、二つの元 σ, τ で生成され、関係式 $\sigma\tau\sigma^{-1} = \tau^q, \sigma^f = 1, \tau^e = 1$ で定義される有限群（位数は ef で $q^f \equiv 1 \bmod e$）になっています。

以下、次の二つの仮定が満たされる状況で考えます。

仮定 1　E は 1 の原始 p 乗根を含む。

仮定 2　E に含まれる 1 の p べき乗根の群の位数を p^k、w を 1 の原始 p^k 乗根とすると、p は拡大次数 $[E : k(w)]$ を割る。($p = 2$ の場合は 4 が $[E : k(w)]$ を割る。)

Gal(Ω/V) のアーベル化群を、以下、Gal(Ω/V)^{ab} と書きます。これには Γ (= Gal(V/k)) が自然に作用し、Γ-加群となりますが、その構造は次の 3 つのステップにより決定されています。

1　E の主単数群を $U_1 = \{a \in E^* \ a \equiv 1 \bmod \pi\ \}$ とするとき、U_1/U_1^p の $\mathbf{F}_p[G]$-加群としての構造の決定

これを得るための数論的な道具は、U_1 の自然なフィルトレーションについての Hasse の研究結果です。それ以外に、特別な $\mathbf{F}_p[G]$-加群の構造を決定する代数的な議論が必要です。

2　U_1 の $\mathbf{Z}_p[G]$-加群としての構造の決定

これは **1** の結果をもとにして、代数的な議論だけで得られます。

3　Gal(Ω/V)^{ab} の Γ-加群としての構造の決定

これは **2** の結果をもとにして、局所類体論を V/k の有限次中間体すべてに適用することで得られます。

(4-2) **1** の結果を得るために必要な、単数群のフィルトレーションについての Hasse の研究結果をまとめておきます。(Hasse[Hasse80]Ch.15.)

k の $\mathbf{Q}_p$ 上の拡大次数を m, 絶対分岐指数を e_0, 剰余拡大次数を f_0 とし、剰余体の元の個数を（以前のとおり）q とします。従って $m = e_0 f_0, q = p^{f_0}$ で

す。E の素元は π, 絶対分岐指数は ee_0 ですが、E が 1 の原始 p 乗根を含むという仮定により、$p-1$ が ee_0 を割ることに注意しておきます。

乗法群 E^* の部分群の減少列 $U_i (i = 1, 2, \dots)$ を

$$U_i = \{a \in E^* \ a \equiv 1 \bmod \pi^i \ \}$$

と定め、u を U_1 から U_1 への p 乗写像（群準同型）とします。E の整数環を O とし、U_i の元 a を $a = 1 + t\pi^i$ $(t \in O)$ と表すと（二項展開により）

$$u(a) = 1 + tp\pi^i + \cdots + t^p \pi^{pi}$$

となりますが、加法付値の値は、$p\pi^i$ が $i + ee_0$, π^{pi} が pi で中間の項の値は $i + ee_0$ より大きい。そこで、$\lambda(i) = Min\{pi, i + ee_0\}$ とおくと、これより、まず次の (0) が従います。

(0) $u(U_i) \subset U_{\lambda(i)}$, $u(U_{i+1}) \subset U_{\lambda(i)+1}$

従って u は準同型 $u_i : U_i/U_{i+1} \to U_{\lambda(i)}/U_{\lambda(i)+1}$ を誘導します。

(1) $i \neq s$ のとき、u_i は bijective.

これは U_i/U_{i+1} の元 $\bar{a}$ に対応する $O/(\pi)$ の元 $\bar{t}$ の対応を見ればよい。

(2) $i > sp$ のとき $U_i \subset U_1^p$.

$i - ee_0 > sp - ee_0 = s$ だから (1) により u_{i-ee_0} が bijective であることから従います。

(3) $i = s$ のとき、$\mathrm{Ker} u_i \simeq \mathbf{Z}/p\mathbf{Z}$.

$i = s$ ならば、

$$u_i(a) \equiv 1 + tp\pi^i + t^p \pi^{pi} \bmod \pi^{\lambda(i)+1}$$

が成り立ちます。$-p = \varepsilon\pi^{ee_0}$ （ε : 単数）とおくと、U_i/U_{i+1} の元 $\bar{a}$ に対応する $O/(\pi)$ の元 $\bar{t}$ の u_i による行く先は $\bar{t}^p - \bar{\varepsilon}\bar{t}$ となります。合同式 $t^p - \varepsilon t \equiv 0 \bmod \pi$ が自明でない解を持つことがわかるので（ $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p((-p)^{1/p-1})$ を用いる)、これより (3) が従います。

次に、$V_i = U_i U_1^p$ $(i = 1, 2, \dots)$ とおくと、$\{V_i\}$ は U_1 の G-不変なフィルトレーション（減少列）で、(2) により $V_{sp+1} = U_1^p$ です；

$$U_1 = V_1 \supset \cdots \supset V_{sp} \supset V_{sp+1} = U_1^p.$$

それゆえ、$\{V_i/V_{i+1}\}$ は U_1/U_1^p のフィルトレーションの successive quotient ですが、これについて次が成り立ちます。

p が i を割らないとき $V_i/V_{i+1} \simeq U_i/U_{i+1}$. （容易）

p が i を割り、$i \neq sp$ のとき [5]、$V_i/V_{i+1} = \{1\}$. （(1) による）

$i = sp$ のとき、$V_{sp}/V_{sp+1} \simeq \mathbf{Z}/p\mathbf{Z}$. （(3) による）

さて、U_i/U_{i+1} は G-加群ですが、具体的には、以下のような G-加群になっています。

U_i/U_{i+1} は $\bar{a}$ に $\bar{t}$ を対応させることで、加法群としては $\mathbf{F}_{q^f}$ に同型です。G の元 σ, τ の作用を見ると、

$$\sigma(a) \equiv 1 + t^q \pi^i \bmod \pi^{i+1},\ \tau(a) \equiv 1 + \eta^i t \pi^i \bmod \pi^{i+1}$$

となることは容易にわかります。従って、加法群 $\mathbf{F}_{q^f}$ に、

$$\sigma(a) = a^q,\ \tau(a) = \eta^i a \tag{4.1}$$

により G-加群としたものを A_i と書くと、G-加群として

$$U_i/U_{i+1} \simeq A_i$$

となります [6)]。

$M = U_1/V_{sp}$ とおくと、これは $\mathbf{F}_p[G]$-加群ですが、以上により、M は次の性質を持つことが従います。

M は $\mathbf{F}_p[G]$-部分加群のフィルトレーション（減少列）

$$M = M_0 \supset M_1 \supset \cdots \supset M_r = \{0\}$$

で、$M_{l-1}/M_l \simeq A_{i_l}$ を満たすものが存在する。ただし、$i_1 < i_2 < \cdots < i_r, (r = ee_0)$ は $1 \leq i < sp, (i,p) = 1$ を満たす自然数全体。
このとき、次の Lemma が成り立ちます。

Lemma 1 上の性質を持つ $\mathbf{F}_p[G]$-加群 M は $\mathbf{F}_p[G]^{\oplus e_0 f_0}$ に同型である。

一般には、$\mathbf{F}_p[G]$-加群は完全可約ではない（G の位数が p で割れる場合もある）にもかかわらず、M の構造がフィルトレーションの successive quotients の情報だけから決定される、というのは奇妙に思われるかも知れませんが、そのからくりは以下の証明をたどるとわかります。

なお、U_1/U_1^p については、 $\mathbf{F}_p[G]^{\oplus e_0 f_0}$ と 1 次元加群との直和となることが示されます（詳細略）。
Lemma 1 の証明の概略を述べます。
(i) $M \otimes \bar{\mathbf{F}}_p$ が $\mathbf{F}_p[G]^{\oplus e_0 f_0} \otimes \bar{\mathbf{F}}_p$ に同型であることを示せばよい。
(ii) $M \otimes \bar{\mathbf{F}}_p$ のフィルトレーションの successive quotient は $\{A_{i_l} \otimes \bar{\mathbf{F}}_p\}$.
(iii) G-加群 A_i は、加法群 $\mathbf{F}_{q^f}$ に、(4.1) により G が作用しているものでした。これより、$A_i \otimes \bar{\mathbf{F}}_p$ の $\bar{\mathbf{F}}_p$-basis $a'_1, \ldots, a'_{ff_0}$ （添字は mod ff_0）で、

$$\sigma^{-1}(a'_{j-f_0}) = a'_j,\ \tau(a'_j) = (\eta^i)^{p^j} a'_j$$

を満たすものが存在することが従います。($(\eta^i)^p, (\eta^i)^{p^2}, \ldots, (\eta^i)^{p^{ff_0}}$ が η^i の $\mathbf{F}_p$-共役であることと、$\tau(x) = \eta^t x$ より $\tau(\sigma^{-1}(x)) = (\eta^t)^q(\sigma^{-1}(x))$ となっていることに注意。)
(iv) $\bar{\mathbf{F}}_p[G]$-加群

$$A_{i_l} \otimes \bar{\mathbf{F}}_p,\ i_1 < i_2 < \cdots < i_{ee_0}\ (1 \le i < sp, (i,p) = 1)$$

の上記の basis 全部を（ τ の）固有値 η^t $(0 \le t < e)$ で分類する。個数を数えると、t に無関係に、それぞれ $e_0 f_0 f$ 個ずつあることがわかります 7) 。
(v) τ で生成される G の部分群を N とします。N は e 次巡回群で、e は p と素です。従って、G-加群 $\bar{\mathbf{F}}_p[G]$ を N-加群とみなすと、それは完全可約で、$\bar{\mathbf{F}}_p[N]^{\oplus f}$ に同型であり、

$$(\bigoplus_{t=0}^{e-1} V_t)^{\oplus f}$$

と直和分解されます。ここで、V_t は部分 N-加群で、η^t-固有空間です。そして、σ は族 $\{V_t\}$ には、$\sigma^{-1}(V_t) = V_{qt}$ で作用します。
(vi) (iii), (iv), (v) から、$\bigoplus_{i_l}(A_{i_l} \otimes \bar{\mathbf{F}}_p)$ と $\bar{\mathbf{F}}_p[G]^{\oplus e_0 f_0}$ は同型であることがわかります。特に、$A_{i_l} \otimes \bar{\mathbf{F}}_p$ は（自由加群の直和因子なので）射影的であることがわかります。
(vii) (ii) 及び $A_{i_l} \otimes \bar{\mathbf{F}}_p$ の射影性より、$M \otimes \bar{\mathbf{F}}_p$ が $\mathbf{F}_p[G]^{\oplus e_0 f_0} \otimes \bar{\mathbf{F}}_p$ に同型であることが従います。
(4-3) **1** の結果に基づき、純粋に代数的な議論で、U_1 が $\mathbf{Z}_p[G]$-加群として、$(m+1)$ 個の生成元を持ち（$m = e_0 f_0$）、2 個の関係式で定義されることが導かれます。

この証明については、時間の関係もあり、省略させていただきました。**1**、**2** の証明はずいぶんと込み入ったものですが、その後、もっと簡単な証明が得られており、関係式の数も 1 個（基礎体が 1 の p 乗根を含まなければ 0 個、即ち自由加群)）でよいことがわかっています。(Jannsen[Jann82], §2 参照。)
(4-4) ガロア群 $\mathrm{Gal}(\Omega/V)^{ab}$ の Γ-加群としての構造は、U_1 の $\mathbf{Z}_p[G]$-加群としての構造がわかったことを用いて、局所類体論により得られます。最終的な結果は Theorem 3 として、$\mathrm{Gal}(\Omega/V)^{ab}$ の指標群の言葉で書かれています。$\mathrm{Gal}(\Omega/V)^{ab}$ 自身について言えば次のようになります。

Theorem 3 $\mathrm{Gal}(\Omega/V)^{ab}$ は Γ-加群として、$\mathbf{Z}_p \bigoplus \mathbf{Z}_p[[\Gamma]]^{\oplus m}$（$\mathbf{Z}_p[[\Gamma]]$: Γ の $\mathbf{Z}_p$ 上の完備群環）と同型である。

講演でも述べましたが、これはちょっとおかしいのではないか、と思います。というのは、$\mathrm{Gal}(\Omega/V)^{ab}$ の Γ-coinvariant と対応する部分体 K を考えると、ま

ず K は k 上のガロア拡大ですが、Lemma 4 により $\mathrm{Gal}(K/k)$ は $\mathrm{Gal}(K/V)$ と $\Gamma = \mathrm{Gal}(V/k)$ との半直積となります。ところが、Γ は $\mathrm{Gal}(K/V)$ に自明に作用するので、結局 $\mathrm{Gal}(K/k)$ は $\mathrm{Gal}(K/V)$ と $\Gamma = \mathrm{Gal}(V/k)$ との直積です。

従って、k 上のアーベル拡大体 K_0 で、$K = K_0V,\ V \cap K_0 = k$ となるものが存在します。Theorem 3 によれば、$\mathrm{Gal}(K_0/k) \simeq \mathbf{Z}_p^{\oplus(m+1)}$ ですが、局所類体論からは $\mathbf{Z}_p^{\oplus m}$ となるはずです。（いろいろと文献を調べましたが、このことについて触れてあるものは見つかりませんでした。私の考え違いかも知れません。どなたかご教示下さい。）

(4-5) Serre[Serre94], Ch.III §4.2 に言及されていることですが、この論文の結果から、k の絶対ガロア群 $\mathrm{Gal}(\Omega/k)$ が、位相群として有限生成であることが従います。実際、まず、$\mathrm{Gal}(\Omega/V)^{ab}$ の Γ-加群としての有限個の生成元をとり、それらの σ, τ 共役全体の $\mathrm{Gal}(\Omega/V)$ への延長を考えます。Theorem 3 により、これら有限個の $\mathrm{Gal}(\Omega/V)$ の元は $\mathrm{Gal}(\Omega/V)^{ab}$ への像が $\mathrm{Gal}(\Omega/V)^{ab}$ を生成しています。従って、$\mathrm{Gal}(\Omega/V)$ が pro-p 群であることから、$\mathrm{Gal}(\Omega/V)$ を生成します。（Burnside の基底定理（の pro-p 版）、[Serre94], Ch.I Prop.25] 参照。）従って、$\mathrm{Gal}(\Omega/V)$ は有限生成で、$\mathrm{Gal}(V/k)$ の有限生成性（σ, τ で生成される）と合わせて、絶対ガロア群 $\mathrm{Gal}(\Omega/k)$ の有限生成性がわかります。

3.5 註

1) $T = \bigcup E_f$ については、例えば Neukirch, Schmidt, Wingberg[NSW08], VII §5 参照。

2) embedding problem とは、ガロア拡大 K/k, 同型 φ, および群の短完全列の組のことを言い、それが solution を持つとは、K を含む k 上のガロア拡大体 L と同型 $\mathrm{Gal}(L/K) \to N,\ \mathrm{Gal}(L/k) \to G$ で、可換図式

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(L/k) & \longrightarrow & \mathrm{Gal}(K/k) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\varphi} & & \\
1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\alpha} & G/N & \longrightarrow & 1
\end{array}$$

が成り立つようなものが存在することを言う。

3) G の任意の有限商群 $\bar{G}$ に対して、N の $\bar{G}$ への像 $\bar{N}$ の位数と指数が互いに素であること。

4) 原論文では、この作用を決めるのは "different problem" と思われる、と書かれていますが（p.464 l.7 ）、これは difficult problem の誤植だろうと思います。(Review（C. Chevalley）でも difficult problem となっています。）

5) 原論文 p.460 l.-1 の $1 \leq i \leq sp$ は正しくは $1 \leq i < sp$.

6) 原論文 p.461 l.6 の $i = 1, \ldots, r$ は $j = 1, \ldots, r$ の誤植。
7) 原論文 p.450 l.12 の $i|p$ は $p|i$ の誤植。

参考文献

[Hasse80] H. Hasse, *Number Theory*, Springer 1980.

[Jann82] U. Jannsen, *Über Galoisgruppen lokaler Körper*, Invent. math. **70**(1982), 53-69.

[HK65] Helmut Koch, *Über Galoissche Gruppen von p-adischen Zahlkörpern*, Math. Nachr. **29**(1965), 77-111.

[NSW08] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Springer 2008 (2nd edition).

[Serre94] J.P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics **5**, Springer 1994 (5th edition).