

局所体の分岐定数 II

横浜国大 工 三木 博雄

p を任意の素数, $\mathbb{Q}_p$ を p 進数体とする。 $\mathbb{Q}_p$ の有限次代数拡大 K に対して, K の正規加法付値を ord_K , K の剰余体を $\bar{K}$ とあらしめ, $\text{ord}_K(p) = e$, $e/(p-1) = e'$ とおく。 K を G をガロア群にもつ K の有限次ガロア拡大とし, K の整数環を $\mathcal{O}_K$ とあらしめ。 このとき, 各整数 $i \geq -1$ に対して

$$G_i = \{ \sigma \in G \mid \text{ord}_K(\sigma \alpha - \alpha) \geq i+1 \quad (\forall \alpha \in \mathcal{O}_K) \}$$

とおいて, i 次の 分岐群 といわれる。

$$G = G_{-1} \supset G_0 \supset G_1 \supset \dots$$

$G_i \supsetneq G_{i+1}$ となる整数 i を 分岐定数 (ramification number) という。

$$\varphi(u) = \varphi_{K/\bar{K}}(u) = \begin{cases} u & (-1 \leq u \leq 0) \\ \frac{1}{g_0} (g_1 + \dots + g_m + (u-m)g_{m+1}) & (m \leq u \leq m+1, m \geq 0 \text{ 整数}) \end{cases}$$

とおく。 ただし $g_i = |G_i|$ (G_i の元の個数)。 i が分岐定数のとき, $\varphi(i)$ を upper ramification number または upper jump という。

う。 $K/\mathbb{K}$ の upper jump の全体を $\mathcal{T}(K/\mathbb{K})$ であらわす。これに関して次の Hasse-Arf の定理は重要である。

定理 1 ([3][1]; [10]). $K/\mathbb{K}$ がアーベル拡大ならば, $K/\mathbb{K}$ の upper jump は常に整数である。

この定理により, $\mathbb{K}_m/\mathbb{K}$ が完全分岐な p^m 次巡回拡大ならば $\mathcal{T}(\mathbb{K}_m/\mathbb{K})$ は m 個の自然数からなることがわかる。本稿において, 次の 2 つの問題を考える。

問題 1. $t_1 < t_2 < \dots < t_m$ を m 個の自然数とする。このとき $\mathcal{T}(\mathbb{K}_m/\mathbb{K}) = \{t_1, t_2, \dots, t_m\}$ となる完全分岐な p^m 次巡回拡大 $\mathbb{K}_m/\mathbb{K}$ が存在するための必要十分条件を求めること。 ($\mathbb{K}$ は固定しておく。)

問題 2. 上のような $\mathbb{K}_m$ の個数 $n_m = n(t_1, \dots, t_m)$ を求めること。

問題 1 は古典的であるが, $m=1$ の場合を除いては結果が得られたのは比較的最近である。分岐定数を考へに入れずに問題 2 と類似の問題を扱っているものとして例えば Krasner [4], Serre [11] がある。問題 2 は問題 1 の精密化になっていることに注意されたい。

まず問題 1 に関する結果から述べよう。Matsu ([6]) は ζ_s を $\zeta_s \in \mathbb{K}$ あるいは $\zeta_{s+1} \notin \mathbb{K}$ となる 1 の原始 p^s 乗根とするとき,

$$(d) \ s=0 \quad (e) \ s \geq 1 \text{ かつ } \text{ord}_{\mathbb{K}}(\zeta_s - 1) \not\equiv 0 \pmod{p}$$

の 2 つの場合に問題 1 を解決し、一般の場合はある種の複雑さから分岐定数のとりうる範囲は見通し難いと述べている、一方、Wyman ([13] [14]) と Tate ([12]) は独立に次の定理 2 に含まれるある必要条件を得、Tate はそれを p -divisible group に応用している。

定理 2 ([6] [5] [2]). $T(K_m/K) = \{t_1, \dots, t_m\}$ となる完全分岐な p^m 次巡回拡大 K_m/K が存在するためには、次の (i) ~ (iii) が必要である。

$$(i) \quad (a) \quad 1 \leq t_1 < e'p \text{ および } t_1 \not\equiv 0 \pmod{p}.$$

または

$$(b) \quad t_1 = e'p \quad (s=0 \text{ のときは (b) は省く}).$$

$$(ii) \quad t_i < e' \text{ ならば, 次の (c) ~ (e) のうちの 1 つが成立する。}$$

$$(c) \quad t_{i+1} = pt_i.$$

$$(d) \quad pt_i < t_{i+1} < e'p \text{ および } t_{i+1} \not\equiv 0 \pmod{p}$$

$$(e) \quad t_{i+1} = e'p \quad (s=0 \text{ のときは (e) は省く})$$

$$(iii) \quad t_i \geq e' \text{ ならば, } t_{i+1} = t_i + e.$$

Fontaine ([2]) は Artin 表現の有理性に関する Serre の予想の解決に上の定理 2 を用いている。Mazur ([6]) は 2 ページ目の下の 2 つの場合に定理 2 の (i) ~ (iii) と同値な条件を得ている。

以下, 定理2の条件(i)~(iii)をみたす数列 $t_1 < t_2 < t_3 < \dots$ を固定し, $t_i = 0$ ($i \leq 0$) とおく。 n を $t_n \geq \varepsilon'$ となる最小の自然数とする。 $n_m \neq 0$ となる最大の m を I とかけば, 問題1は次のようにいいかえられる。

問題1'. I を求めること。

この観点から, 先に述べた Maus の結果は次のように表される。(formulationはMausのと異なるが本質的には同じである)

定理3 ([6]). (i) $s=0$ ならば $I=\infty$ 。

(ii) $s \geq 1$ かつ $w \cdot \text{ord}_K(\zeta_s - 1) \neq 0 \pmod{p}$ ならば,

$$I = \begin{cases} j+s-1 & (\bar{K} = \mathbb{F}_p \text{ かつ } w \cdot \text{ord}_K(\zeta_s - 1) = t_j \text{ となる } t_j \text{ が存在するとき}) \\ \infty & (\text{そうでないとき}) \end{cases}$$

問題1'の部分的結果として, さらに次の Marshall の

定理4 ([5]). $n \leq I$.

があり, Nguyen-quang-do ([9]) が $\zeta_1 \in \mathbb{R}$ のときに別証明を与えている。

一般の場合は私 ([7][8]) が解答を与えた。結果は次のとおりである。 $s \geq 1$ のとき, $p^l \parallel \text{ord}_K(\zeta_s - 1)$ ならば,

$$(*) \quad \zeta_s = a_0^{p^l} a_1^{p^{l-1}} \cdots a_{l-1}^p a_0 \quad (a_i \in \mathbb{R}, \text{ord}_K(a_i - 1) \geq 1)$$

とかけられる。ただし $a_0, a_1, \dots, a_l$ は次の(1)~(3)をみたす。 $\lambda_i =$

$\text{ord}_*(a_i - 1)$ とおけば,

- (1) (a) $\lambda_l = e'p$ または (b) $\lambda_l < e'p$ および $\lambda_l \not\equiv 0 \pmod{p}$.
 (2) $a_i \neq 1$ および $0 \leq i \leq l-1$ ならば $\lambda_i \not\equiv 0 \pmod{p}$.
 (3) $a_i \neq 1, a_j \neq 1$ ($0 \leq j < i \leq l$) ならば $\lambda_i > p^{i-j} \lambda_j$.

λ_i ($0 \leq i \leq l$) は $\mathbb{R}$ に δ , τ - 意的に定まることを示され,
 従って $\mathbb{R}$ の一つの不変量である. これはある仮定のもとでは
 $\mathbb{R}/\mathbb{Q}$ の分岐の状態によって具体的に記述される.

$1 \leq j \leq n$ について次の条件 $P(j)$ を考える.

$P(j)$: $\{0, 1, \dots, l\}$ の部分集合 I_0 によって次の条件 (1), (2) をみたすものが存在する.

(1) $t_{j-i} = \lambda_{l-i}$ ($\forall i \in I_0$) および $t_{j-i} < \lambda_{l-i}$ ($i \in \{0, \dots, l\} - I_0$)

(2)
$$|I_0| = \begin{cases} \text{奇数} & (p=2) \\ 1 & (p \neq 2). \end{cases}$$

定理 5 ([7][8]). $s \geq 1$ のとき,

$$I = \begin{cases} j+s-1 & (\mathbb{R} = \mathbb{F}_p \text{ および } P(j) \text{ が成立する}) \\ n+s-1 & (\mathbb{R} \neq \mathbb{F}_p, t_n = \lambda_l = e'p \text{ および } t_{n-i} < \lambda_{l-i} \text{ } (1 \leq i \leq l)) \\ \infty & (\text{そうでないとき}). \end{cases}$$

$l=0$ のときが Matsu の結果 (定理 3 の (ii)) になっていること

とに注意されたい。前講演で述べられたように末吉豊氏によって定理5の別証明がえられている。

以下、問題2の解答を述べよう。この系として、定理5が導かれることに注意されたい。

$|\bar{k}| = p^f$, $d_m = f \cdot (t_m - [\frac{t_m-1}{p}]) - \delta_m + 1$ ($1 \leq m \leq n$) とおく。ただし δ_m は $t_{i+1} = p t_i$ ($1 \leq i \leq m-1$) となる i の個数で、 $[\]$ はガウスの記号である。

$$D_i = \begin{cases} p^{d_1} \alpha & (i=0) \\ (p^{d_i} - p^{d_{i-1}}) \alpha & (1 \leq i \leq n-1 \text{ かつ } t_{i+1} \neq p t_i) \\ p^{d_i} \alpha & (1 \leq i \leq n-1 \text{ かつ } t_{i+1} = p t_i) \\ p^{d-1} & (i \geq n) \end{cases}$$

とおく。ただし $\alpha = (p^f - 1) / (p - 1)$, $d = \dim_{\mathbb{F}_p} \mathbb{R}^* / \mathbb{R}^{*p}$ (これは $\zeta_1 \in \mathbb{R}$ または $\zeta_1 \in \mathbb{R}$ に従って $[\mathbb{R} : \mathbb{Q}_p] + 1$ または $[\mathbb{R} : \mathbb{Q}_p] + 2$ に等しい)。 $P_m = \prod_{i=0}^{m-1} D_i$ とおく。このとき、

定理6. $S=0$ ならば $\kappa_m = P_m$ ($m \geq 1$).

各 m ($0 \leq m \leq l$) について、 $t_{i_m} \leq \lambda_m < t_{i_m+1}$ をみたす i_m をとる ($\lambda_m = \infty$ のときは $i_m = \infty$ とする)。 $j_l = \text{Min}(i_l, i_{l-1}+1, \dots, i_0+1)$ とおく。各整数 $i \geq -1$ に対して、

$$f_i(x) = \begin{cases} 1 & (i = -1) \\ 0 & (i = 0) \\ x - x^2 + x^3 - \dots + (-1)^{i-1} x^i & (i \geq 1) \end{cases}$$

よって, 多項式 $f_i(x)$ を定義する。

$$\begin{aligned} h &= (t_{i_j} = \lambda_j \text{ あり } \vee j_l = i_j + (l-j) \text{ をみたす } j (0 \leq j \leq l) \text{ の個数}) - 1 \\ &= (\lambda_{l-j} = t_{j-l} \text{ をみたす } j (0 \leq j \leq l) \text{ の個数}) - 1 \end{aligned}$$

$$F = f_h \left(\frac{1}{p-1} \right)$$

とある。 $F=0$ であるためにはある j について $P(j)$ が成立することが必要十分で, このとき $j = j_l$ が成立する。

定理 7. $\bar{\mathbb{R}} = \mathbb{F}_p$ あり $\vee s \geq 1$ のとき,

$$n_m = \begin{cases} P_m & (1 \leq m \leq j_l + s - 1) \\ p^{-(m-s-j_l)} F P_m & (j_l + s \leq m) \end{cases}$$

$\bar{\mathbb{R}} \neq \mathbb{F}_p$ の場合の結果を述べるにはさらに記号が必要である。

$$b = p^{s-1} / (p^s - 1),$$

$$\begin{aligned} A = \{ 1 \leq j \leq n \mid t_{i_{l-m}} = \lambda_{l-m} \neq 0 \text{ あり } \vee j \leq \text{Min}(i_l, i_{l-1} + 1, \dots, i_{l-(m-1)} + (m-1)) \\ (\text{もし } m > 0) \text{ をみたすある } m (0 \leq m \leq l) \text{ が存在して} \\ j = i_{l-m} + m \text{ とかける} \} \end{aligned}$$

$$\lambda(j) = \# \{ i \mid 1 \leq i \leq j \text{ あり } \vee i \in A \}.$$

とあけは,

定理 8. $s \geq 1$ および $\bar{K} \neq \mathbb{F}_p$ とする。 $\lambda \notin \{t_1, \dots, t_n\}$ または $t_{j_\lambda} = \lambda \neq e'p$ ならば,

$$n_m = \begin{cases} P_m & (1 \leq m \leq j_\lambda + s - 1) \\ b^{\lambda(m-s)} P_m & (m = j_\lambda + s) \\ p^{-(m-s-j_\lambda - \lambda(m-s)+s)} b^{\lambda(m-s)} P_m & (j_\lambda + s + 1 \leq m) \end{cases}$$

ただし

$$\delta = \begin{cases} 1 & (j_\lambda = n \text{ および } j_\lambda \in A) \\ 0 & (\text{それ以外}) \end{cases}$$

定理 9. $s \geq 1$ および $\bar{K} \neq \mathbb{F}_p$ とする。 $t_{j_\lambda} = \lambda = e'p$ および $j_\lambda = n$ ならば,

(i) $1 \leq m < s+n$ ならば,

$$n_m = \begin{cases} P_m & (1 \leq m \leq j_\lambda + s - 1) \\ b^{\lambda(m-s)} P_m & (m = j_\lambda + s) \\ p^{-(m-s-j_\lambda - \lambda(m-s))} b^{\lambda(m-s)} P_m & (j_\lambda + s + 1 \leq m < s+n) \end{cases}$$

(ii) $m \geq s+n$ ならば,

$$n_m = \begin{cases} 0 & (j_\lambda = n \notin A) \\ c_1 p^{-(m-s-n)} P_m & (j_\lambda = n \in A) \\ c_1 b^{\lambda(n)-1} p^{-(m-s-n)} P_m & (j_\lambda + 1 = n \in A) \\ c_1 b^{\lambda(n)-1} p^{-(m-s-j_\lambda - \lambda(n))} P_m & (j_\lambda + 2 \leq n \in A) \end{cases}$$

$$\begin{cases} c_2 b^{\lambda^{(n)}} p^{-(m-s-n)} P_m & (j_k+1 = n \notin A) \\ c_2 b^{\lambda^{(n)}} p^{-(m-s-j_k-\lambda^{(n)}-1)} P_m & (j_k+2 \leq n \notin A) \end{cases}$$

$\in \mathbb{Z}$, $c_1 = (p-1)(1-b)$, $c_2 = (p-1)(1-p^{-1})$.

文 献

- [1] C. Art, Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper, J. reine angew. Math. 181 (1939), 1-44.
- [2] J.-M. Fontaine, Groupes de ramification et représentations d'Artin, Ann. Scient. Éc. Norm. Sup. 4 (1971), 337-392.
- [3] H. Hasse, Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper, J. Fac. Sci. Imp. Univ. Tokyo Sec. I, 2 (1934), 477-498.
- [4] M. Krasner, Nombre des extensions d'un degré donné d'un corps p -adique, Colloque CNRS n°143, Clermont-Ferrand, 1966, p. 143-169.
- [5] M. A. Marshall, Ramification groups of abelian local field extensions, Canad. J. Math. 23 (1971), 271-281.
- [6] E. Maus, Existenz p -adischer Zahlkörper zu vorgegebenem Verzweigungsverhalten, Dissertation, Ham-

burg 1965.

- [7] H. Miki, 局所体の分岐定数について, 第25回代数学シンポジウム報告集, 北大 1979.
- [8] H. Miki, On the ramification numbers of cyclic p -extensions over local fields, to appear in J. reine angew. Math.
- [9] T. Nguyen-quang-do, Filtration de K^*/K^{*p} et ramification sauvage, Acta Arith. 30 (1976), 323-340.
- [10] J.-P. Serre, Corps locaux, Paris 1962; 2nd Ed. 1968.
- [11] J.-P. Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, C. R. Acad. Sci. Paris, Série A, 286 (1978), 1031-1036.
- [12] J. Tate, p -divisible groups, Proc. of a conference on local fields, Driebergen 1966.
- [13] B. F. Wyman, Wild ramification in cyclic extensions of complete fields, Ph. D. Thesis, Berkeley 1966.
- [14] B. F. Wyman, Wildly ramified gamma extensions, Amer. J. of Math. 91 (1969), 135-152.