数理解析研究所講究録
440巻 1981年 26-35

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$\bar{k}$であらわし，$\mathrm{ord}_k(p)=e$，$e/(p-1)=e'$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$\mathcal{O}_K$であらわす。このとき，各整数$i \geqq -1$に対して

$$G_i=\{\sigma \in G \mid \mathrm{ord}_K(a^\sigma - a) \geqq i+1 \quad (\forall a \in \mathcal{O}_K)\}$$

とおいて，i次の<u>分岐群</u>といわれる。

$$G=G_{-1} \supset G_0 \supset G_1 \supset \cdots \quad 。$$

$G_i \supsetneqq G_{i+1}$となる整数iを<u>分岐定数</u>(ramification number)という.

$$\varphi(u)=\varphi_{K/k}(u)=\begin{cases} u & (-1 \leqq u \leqq 0) \\ \dfrac{1}{g_0}(g_1+\cdots+g_m+(u-m)g_{m+1}) & \left(\begin{matrix} m \leqq u \leqq m+1 \\ m \geqq 0 \text{ 整数} \end{matrix}\right) \end{cases}$$

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<u>upper ramification number</u>または<u>upper jump</u>とい

う。K/k の upper jumps の全体を $T(K/k)$ 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/k がアーベル拡大ならば, K/k の upper jumps は常に整数である。

この定理により, k_m/k が完全分岐な p^m 次巡回拡大ならば $T(k_m/k)$ 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. $t_1 < t_2 < \cdots < t_m$ を m 個の自然数とする。このとき $T(k_m/k) = \{t_1, t_2, \cdots, t_m\}$ となる完全分岐な p^m 次巡回拡大 k_m/k が存在するための必要十分条件を求めること。(k は固定しておく。)

問題2. 上のような k_m の個数 $n_m = n(t_1, \cdots, t_m)$ 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。分岐定数を考えに入れない問題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。Maus ([6]) は ζ_s を $\zeta_s \in k$ および $\zeta_{s+1} \notin k$ となる1の原始 p^s 乗根とするとき,

(a) $s=0$ (b) $s \geq 1$ および $\mathrm{ord}_k(\zeta_s - 1) \not\equiv 0 \pmod{p}$

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 へ応用している。

<u>定理２</u>（[6][5][2]）．$T(k_m/k)=\{t_1,\cdots,t_m\}$ 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)　(a) $1 \leqq t_1 < e'p$ および $t_1 \not\equiv 0 \pmod p$．

またば

　(b) $t_1 = e'p$　（$s=0$ のときは (b) は省く）．

(ii)　$t_i < e'$ ならば，次の(c)〜(e)のうちの一つが成立する。

　(c) $t_{i+1} = pt_i$

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

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

(iii)　$t_i \geqq e'$ 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。Maus（[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 $t_1 < t_2 < t_3 < \cdots$ を固定し，$t_i = 0$ $(i \leqq 0)$ とおく。n を $t_n \geqq e'$ 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) $s \geqq 1$ および $\mathrm{ord}_k(\zeta_s - 1) \not\equiv 0 \pmod p$ ならば，

$$I = \begin{cases} j+s-1 & (\bar{k}=\mathbb{F}_p \text{ および } \mathrm{ord}_k(\zeta_s-1)=t_j \text{ となる } {}^{\exists}t_j \text{ が存在するとき}) \\ \infty & (\text{そうでないとき}) \end{cases}$$

問題1′の部分的結果として，さらに次の Marshall の

定理4([5]). $n \leqq I$.

があり，Nguyen-quang-do([9])が $\zeta_1 \in k$ 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。$s \geqq 1$ のとき，$p^l \| \mathrm{ord}_k(\zeta_s - 1)$ ならば，

$$(*) \quad \zeta_s = a_0^{p^l} a_1^{p^{l-1}} \cdots a_{l-1}^{p} a_0 \qquad (a_i \in k,\ \mathrm{ord}_k(a_i - 1) \geqq 1)$$

とかける。ただし $a_0, a_1, \cdots, a_l$ は次の(1)～(3)をみたす。$\lambda_i =$

$\mathrm{ord}_k(a_i-1)$ 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 $0 \leqq i \leqq l-1$ ならば $\lambda_i \not\equiv 0 \pmod p$.

(3) $a_i \neq 1$, $a_j \neq 1$ $(0 \leqq j < i \leqq l)$ ならば $\lambda_i > p^{i-j}\lambda_j$.

λ_i $(0 \leqq i \leqq l)$ は k によって一意的に定まることが示され，従って k の一つの不変量である．これはある仮定のもとでは $k/\mathbb{Q}$ の分岐の状態によって具体的に記述される。

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

$P(j)$: $\{0, 1, \cdots, l\}$ の部分集合 $^{\exists}I_0$ で次の条件(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 $t_{j-i} < \lambda_{l-i}$ $({}^{\forall} i \in \{0, \cdots, l\} - I_0)$

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

定理 5 ([7][8]). $s \geqq 1$ のとき，

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

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

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。これの系として，定理5が導かれることに注意されたい。

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

$$D_i = \begin{cases} p^{d_1} a & (i = 0) \\ (p^{d_i} - p^{d_{i-1}}) a & (1 \leqq i \leqq n-1 \text{ および } t_{i+1} \neq p t_i) \\ p^{d_i} a & (1 \leqq i \leqq n-1 \text{ および } t_{i+1} = p t_i) \\ p^{d-1} & (i \geqq n) \end{cases}$$

とおく。ただし $a = (p^f - 1)/(p-1)$, $d = \dim_{\mathbb{F}_p} k^{\times}/k^{\times p}$ (これは $\zeta_1 \notin k$ または $\zeta_1 \in k$ に従って $[k : \mathbb{Q}_p] + 1$ または $[k : \mathbb{Q}_p] + 2$ 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 $n_m = P_m$ $(m \geqq 1)$.

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

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

によって，多項式 $f_i(x)$ を定義する。

$$h = (t_{i_j} = \lambda_j \text{ および } j_\ell = i_j + (\ell - j) \text{ をみたす } j\ (0 \leqq j \leqq \ell) \text{ の個数}) - 1$$

$$= (\lambda_{\ell-j} = t_{j_\ell - j} \text{ をみたす } j\ (0 \leqq j \leqq \ell) \text{ の個数}) - 1$$

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

とおく。$F = 0$ 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 $j = j_\ell$ が成立する。

<u>定理 7.</u> $k = \mathbb{F}_p$ および $s \geqq 1$ のとき，

$$n_m = \begin{cases} P_m & (1 \leqq m \leqq j_\ell + s - 1) \\ p^{-(m-s-j_\ell)} F P_m & (j_\ell + s \leqq m) \end{cases} .$$

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

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

$A = \{ 1 \leqq j \leqq n \mid t_{i_{\ell-m}} = \lambda_{\ell-m} \neq ep$ および $j \leqq \mathrm{Min}(i_\ell, i_{\ell-1}+1, \cdots, i_{\ell-(m-1)} + (m-1))$ $(\text{if } m > 0)$ をみたすある $\exists m\ (0 \leqq m \leqq \ell)$ が存在して $j = i_{\ell-m} + m$ とかける $\}$,

$\lambda(j) = \# \{ i \mid 1 \leqq i \leqq j$ および $i \in A \}$.

とおけば，

__定理8.__ $s \geqq 1$ および $\overline{R} \neq \mathbb{F}_p$ とする。$\lambda_\ell \notin \{t_1, \cdots, t_n\}$ または $t_{i_\ell} = \lambda_\ell \neq e'p$ ならば，

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

ただし

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

__定理9.__ $s \geqq 1$ および $\overline{R} \neq \mathbb{F}_p$ とする。$t_{i_\ell} = \lambda_\ell = e'p$ および $j_\ell = n$ ならば，

(i) $1 \leqq m < s + n$ ならば，

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

(ii) $m \geqq s + n$ ならば，

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

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

ただし，$c_1 = (p-1)(1-b)$，$c_2 = (p-1)(1-p^{-1})$。

文献

[1] C. Arf, 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 $\mathfrak{p}$-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 $\mathfrak{p}$-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; 2-nd 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.