

円分体 $\mathbb{Q}(\mu_{p^n})$ の p 次不分岐巡回拡大の
相対正規整数環について

横浜市大・文理, 市村 文男 (Humio Ichimura)

§ 1 序文

代数体 K , その有限素点の有限集合 S , その有限次ガロア
拡大 $K/\bar{K}$ に対して, K が $\bar{K}$ 上 S -normal integral basis
(S -NIB) を持つとは, $\mathcal{O}_K(S)$ を自然に $\mathcal{O}_{\bar{K}}(S)[\text{Gal}(K/\bar{K})]$ 加群
とみた時, 自由になる事をいいます。なお, $\mathcal{O}_{\bar{K}}(S)$ 等は
 S -整数の環を表わします。 $K/\bar{K}$ が S -NIB を持てば, $K/\bar{K}$ は
(S の外で) 高々 tamely に分岐します (Noether) が, この二つの
条件の間にはかなりの gap があります。そこで, tamely より
強めて (S の外) 不分岐性と S -NIB の関係を考えます。

具体的には:

問題 Q $\bar{K}, S$ を上のとおり, G を有限群とします。
 $\bar{K}$ の S の外で不分岐な G 拡大全体のながで, S -NIB を持つもの
はどのくらい多いか, どのくらい例外的か? 代数体 $\bar{K}$ の

言葉で記述せよ。

まず、 G 拡大全体をとらえる必要がありますが、 G が $abel$ の場合には Kummer 理論が使えるので、以下 G は $abel$ とします。更に $k_1 \cap k_2 = \bar{k}$ とする $\bar{k}$ のガロア拡大 k_1, k_2 に対して、

$$k_1, k_2 / \bar{k} \text{ が } S\text{-NIB を持つ} \iff k_1, k_2 \text{ が } \bar{k} \text{ 上 } S\text{-NIB を持つ}$$

事が知られているので、以下、 G は p 中次巡回群とします。

(p : 素数) この時、除外因子 S が p 上の素点をすべて含むかどうかで様子がかなり異なります。§2 では、 S が p 上の素点全体の場合を、§3 では $S = \emptyset$ の場合を扱います。

§2 $S = p$ 上の素点全体の場合

$K/\bar{k}$ を p の外で不分岐な p 中次巡回拡大とします。これについて、 p -NIB を持つための、次の簡単な判定条件が、河本・小松 [8] で得られています。 $G = \text{Gal}(K/\bar{k})$ の指標 χ に対して、 K_χ を $\ker \chi$ の固定体、 g_χ を χ の位数、体 F について $F(\chi)$ を F に χ の値を追加した体とします。この時、

$$\begin{aligned} (*) \quad & K/\bar{k} \text{ が } p\text{-NIB を持つ} \\ \iff & \forall \chi \in \hat{G}, \exists p\text{-unit } \varepsilon \in \bar{k}(\chi) \text{ s.t. } K_\chi(\chi) = \bar{k}(\chi)(\varepsilon^{1/g_\chi}) \end{aligned}$$

これを用いると、問題Qに容易に答えられます。

例1 $\mu_{p^m} \subset \mathbb{F}$, $G = p^m$ -巡回群 の時

$$V' = \{ \alpha \in \mathbb{F}^\times \mid (\alpha) = \mathfrak{p} \alpha^{p^m}, \mathfrak{p} \text{ 上の素idealの積 } \{ \mathbb{F}^{\times p^m} / \mathbb{F}^{\times p^m} \}$$

$$\downarrow$$

$$\mathcal{E}' = E' / E'^{p^m}, \quad (E' = \mathbb{F} \text{ の } p\text{-unit の群})$$

とします。 $[\alpha] \in V' \longleftrightarrow \mathbb{F}(\alpha^{1/p^m}) / \mathbb{F}$ で、

V' と $\mathfrak{p}$ の外で不分岐、拡大次数 p^m の巡回拡大 $\{ \text{ガ} \}$ 1 対 1
に対応し、(*)より、 $[\alpha] \in V'$ に対して、

$$\mathbb{F}(\alpha^{1/p^m}) / \mathbb{F} \text{ が } p\text{-NIB を持つ} \iff [\alpha] \in \mathcal{E}'$$

とあります。従って、今の状況で、古典的な Kummer の完全列

$$(**) \quad 1 \rightarrow \mathcal{E}' \rightarrow V' \rightarrow {}_{p^m}\mathcal{U}'_{\mathbb{F}} \rightarrow 1$$

が問題Qに対する解を与えます。但し、 $\mathcal{U}'_{\mathbb{F}}$ は $\mathbb{F}$ の p -ideal
類群, $V' \rightarrow {}_{p^m}\mathcal{U}'_{\mathbb{F}}$ は(数行前の記号で) $[\alpha] \rightarrow [\alpha]$ で定め
ます。

なお、Childs [1] は、別の手法で、問題Qに対して(**)と同
じ意味を持つ完全列を得ています。 $\mu_{p^m} \not\subset \mathbb{F}$ の場合は、

Greither [3] で扱われています。

例2 $\mathbb{Z}_p$ 拡大の p -NIB

$\mathbb{Z}_p$ 拡大 K/k が p -NIB を持つとは、 $\forall m \geq 0$ に対して m -th layer k_m が k 上 p -NIB を持つ事をいいます。判定条件(*)を用いると、これは、

$\forall m \geq 0, \exists p\text{-unit } \varepsilon \in k(\mu_{p^m})$ s.t. $k_m(\mu_{p^m}) = k(\mu_{p^m})(\varepsilon^{1/p^m})$ と同値にあります。この事と岩澤理論を用いて、 $G = \mathbb{Z}_p$ とした時の問題Qに対して次が得られています。

★ kersten-Michalek [9] (その上記の針での別証は、河本-小松[8])

$$\begin{aligned} & \mathbb{Q}(\mu_p) \text{ 上のすべての } \mathbb{Z}_p \text{ 拡大が } p\text{-NIB を持つ} \\ \iff & \forall m \geq 0 \text{ で } \mathcal{U}_{\mathbb{Q}(\mu_p)}^+ \rightarrow \mathcal{U}_{\mathbb{Q}(\mu_{p^m})}^+ \text{ は単射} \end{aligned}$$

また、Fleckinger - Nguyen Quang Do [6] は、 $\mathbb{Z}_p$ 拡大の場合に問題Qに対して(**)と同じ意味を持つ完全列を構成しました。

§3 $S' = \emptyset$ の場合

この場合は、§2と対照的に極くわかりな事しか得られていません。例えば、NIBを持つための判定条件も G が p 次巡回群の場合にしか得られていません。

この§では、 $k = \mathbb{Q}(\mu_{p^m})$, $S' = \emptyset$, $G = p$ 次巡回群 の場合に

問題Qとp進L関数の零点の“様子”,特に個数,との間には何かの関係がある事を報告します。

結果の主要な一部を述べると、

定理' p でのVandiver予想($p \nmid h(\mathbb{Q}(\cos 2\pi/p))$)を仮定する。 $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ の奇指標 ψ に対して、 λ_ψ を $\mathbb{Q}(\mu_p)$ の $\mathbb{Z}_p$ 拡大の岩澤入不変量の ψ 成分とする。この時、すべての奇指標 ψ に対して、 $p^{m-1}(p-1) \geq \lambda_\psi$ であれば、 $\mathbb{Q}(\mu_{p^{m+1}})$ のすべての p 次不分岐巡回拡大はNIBを持つ。(ここでは、 $m \geq 1$ としている。 $m=0$ の場合は、後述の定理(c)参照)

この事は、 $m \rightarrow \infty$ で、 $\mathbb{Q}(\mu_{p^m})$ の類群の p -rankは一定(ferrero-Washington [5])だが単数群は激しく大きくなるという事を反映しています。対照的に、単数を少ししか持たない、二次体長に対して、右上の二次不分岐拡大達の内NIBを持つものは高々ひとつです(Haggenmüller [7])。

Wagstaff [11], Ernvall-Metsänkylä [4] 達の計算により、 $p < 150000$ でVandiver予想が成立し、 $\lambda_\psi = 0, 1$ とある事が知られている。従って、定理', 後述の定理(c)によって、この範囲の p については、 $\forall m \geq 0$ で $\mathbb{Q}(\mu_{p^m})$ のすべての p 次不分岐巡回拡大はNIBを持ちます。なお、確率的な議論

によって、高々有限個の ψ すべてで、 $\lambda_\psi \leq 2$ とする事が予想されています。(Lang [10], Chap. 10 参照)

の p を除いて

結果をすべて記述するために記号をいくつか導入します。
 k を 1 の原始 p 乗根を含む代数体とし、 $\lambda = \zeta - 1$ とおきます。

$$V = \{ \alpha \in k^\times \mid \alpha \text{ は } p \text{ と素, singular かつ primär } \} \subset k^\times / k^{\times p}$$

$\uparrow$

$$E = \{ \varepsilon \in E_k \mid \varepsilon \equiv 1 \pmod{\lambda^p} \} \quad (E_k = k \text{ の単数群})$$

とします。

但し、 p と素な数 α に対して、 α が singular とは、 (α) が k の ideal の p 乗になっている事、primär とは、 $\alpha \equiv x^p \pmod{\lambda^p}$ が k に解を持つ事をいいます。

$\alpha \in k^\times$ に対して、

$$k(\alpha^{1/p})/k : \text{不分離} \iff [\alpha] \in V \quad (\text{Furtwängler})$$

$[\alpha] \in V$ に対して、

$$k(\alpha^{1/p})/k \text{ が NIB を持つ} \iff [\alpha] \in E \quad (\text{Chilès [2]})$$

が知られています。

従って、 $k = k_m = \mathbb{Q}(\mu_{p^{m+1}})$ に対する V, E を V_m, E_m とかけば、

問題 Q は、 $V_m = E_m$ か? という問になります。

V_m, E_m は、 $\Delta = \text{Gal}(k_0/\mathbb{Q}) (\subset \text{Gal}(k_m/\mathbb{Q}))$ の作用で固有空間

分解して考えます。 $\mathcal{E}_m^- = \{1\}$, $V_m(\chi_0) = \{1\}$ (χ_0 は Δ の自明な指標) は良く知られています。 Δ の円分指標を ω とがります。 Δ の ω と異なる奇指標 ψ に対して, $g_\psi(t) (\in \mathbb{Z}_p[[t]])$ を p 進 L 関数 $L_p(s, \omega\psi^{-1})$ に対応する巾級数とします:

$$g_\psi((1+p)^s - 1) = L_p(s, \omega\psi^{-1}).$$

$g_\psi((1+t)^{-1} - 1) = h_\psi(t) u_\psi(t)$, h_ψ : distinguished poly., $u_\psi \in \mathbb{Z}_p[[t]]^\times$ と一意的に分解されます。

$$\lambda_\psi := \deg h_\psi, \quad H_\psi(t) := h_\psi(t) - t^{\lambda_\psi} (\in {}_p\mathbb{Z}_p[[t]])$$

$A_m := p^m, p^{m-1-j} \cdot t^{p^j} (0 \leq j \leq m-1)$ で生成される $\mathbb{Z}_p[[t]]$ の ideal とします。

この時、

定理 Vandiver 予想を仮定する。 Δ の非自明な偶指標 χ に対して, $\psi = \omega\chi^{-1}$ とおく。

$$(a) \quad p^{m-1}(p-1) \geq \lambda_\psi \text{ の時, } V_m(\chi) = \mathcal{E}_m(\chi).$$

$$(b) \quad p^{m-1}(p-1) < \lambda_\psi < p^m \text{ の時,}$$

$$V_m(\chi) = \mathcal{E}_m(\chi) \iff t^{p^m - \lambda_\psi} \cdot H_\psi(t) \in pA_m$$

$$(c) \quad p^m \leq \lambda_\psi \text{ の時,}$$

$$V_m(\chi) = \mathcal{E}_m(\chi) \iff H_\psi(t) \in pA_m$$

文献

- [1] L.N. Childs : Abelian Galois extensions of rings containing roots of unity, Illinois J. Math., 15, 1971
- [2] ——— : The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc., 35, 1977
- [3] C. Greither : Cyclic Galois extensions and normal bases, Trans. A.M.S., 326, 1991
- [4] R. Ernvall and T. Metsänkylä : Cyclotomic invariants for primes between 125000 and 150000, Math. Comp., 56, 1991
- [5] B. Ferrero and L.C. Washington : The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. Math., 109, 1979
- [6] V. Fleckinger et T. Nguyen Quang Do : Bases normales, unités et conjecture faibles de Leopoldt, Manus. Math., 71, 1991
- [7] R. Hagenmüller : Diskriminanten und Picard-Invarianten freier quadratischer Erweiterungen, Manus. Math., 36, 1981
- [8] F. Kawamoto and K. Komatsu : Normal bases and $\mathbb{Z}_p$ -extensions, preprint, (1991)
- [9] I. Kersten and J. Michalek : On Vandiver's conjecture and $\mathbb{Z}_p$ -extensions of $\mathbb{Q}(\mu_p^n)$, J. Number Th., 32, 1989
- [10] S. Lang : Cyclotomic Fields, Vol II, Springer

[11] S.S. Wagstaff : The irregular primes up to 125000,
Math. Comp., 32, 1978