数理解析研究所講究録
797巻 1992年 153-161

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

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/kに対して、Kがk上S-*normal integral basis* (S-NIB)を持つとは、$\mathcal{O}_K(S)$を自然に$\mathcal{O}_k(S)[\mathrm{Gal}(K/k)]$加群とみた時、自由になる事をいいます。なお、$\mathcal{O}_k(S)$等は$S$-整数の環を表わします。$K/k$が$S$-NIBを持てば、$K/k$は($S$の外で)高々tamelyに分岐します(Noether)が、この2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の外の)不分岐性とS-NIBの関係を考えます。具体的には:

<u>問題Q</u>　k, Sを上のとおり, Gを有限群とします。kのSの外で不分岐なG拡大全体のなかで、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kの

言葉で記述せよ。

先ず、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 $k_1 \cap k_2 = k$ となる k のガロア拡大 k_1, k_2 に対して、

$$k_1k_2/k \text{ が S-NIB を持つ} \iff k_1, k_2 \text{ が } k \text{ 上 S-NIB を持つ}$$

事が知られているので、以下、Gはp巾次巡回群とします。（p：素数）この時、除外因子Sがp上の素点をすべて含むか否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 $S=\phi$ の場合を扱います。

§2　S = p上の素点全体の場合

K/k をpの外で不分岐なp巾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。$G = Gal(K/k)$ 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 の値を添加した体とします。この時、

(*)　K/k が p-NIB を持つ

$$\iff \forall \chi \in \hat{G},\ {}^{\exists}\text{p-unit } \varepsilon \in k(\chi) \text{ s.t. } k_\chi(\chi) = k(\chi)(\varepsilon^{1/g_\chi})$$

これを用いると、問題Qに容易に答えられます。

例1　$\mu_{p^n} \subset k$, $G = p^n$次巡回群　の時

$V' = \{\alpha \in k^\times \mid (\alpha) = {}^\exists \mathfrak{a}^{p^n} \times$ p上の素idealの積$\} k^{\times p^n} / k^{\times p^n}$

$\cup$

$\mathcal{E}' = E' / E'^{p^n}$　($E' = k$のp-unitの群)

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

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

$k(\alpha^{1/p^n})/k$ が p-NIBを持つ $\Longleftrightarrow [\alpha] \in \mathcal{E}'$

となります。従って、今の状況で、古典的なKummerの完全列

$$(**) \qquad 1 \longrightarrow \mathcal{E}' \longrightarrow V' \longrightarrow {}_{p^n}Cl'_k \longrightarrow 1$$

が問題Qに対する解を与えます。但し、Cl'_k はkのp-ideal類群，$V' \longrightarrow {}_{p^n}Cl'_k$ は(数行前の記号で)$[\alpha] \longrightarrow [\mathfrak{a}]$ 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。$\mu_{p^n} \not\subset k$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、$\forall n \geq 0$ に対して n-th layer k_n 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、

$\forall n \geq 0,\ {}^{\exists} p\text{-unit}\ \varepsilon \in k(\mu_{p^n})$ s.t. $k_n(\mu_{p^n}) = k(\mu_{p^n})(\varepsilon^{1/p^n})$

と同値になります。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-Michaliček [9]（その上記方針での別証は、河本-小松 [8]）

$\mathbb{Q}(\mu_p)$ 上のすべての $\mathbb{Z}_p$ 拡大が p-NIB を持つ

$\iff \forall n \geq 0$ で $\mathcal{C}^{+}_{\mathbb{Q}(\mu_p)} \longrightarrow \mathcal{C}^{+}_{\mathbb{Q}(\mu_{p^n})}$ は単射

なお、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　$S' = \phi$ の場合

この場合は、§2と対照的に極くわずか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、$k = \mathbb{Q}(\mu_{p^n})$, $S' = \phi$, $G = p$ 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，との間になにがし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、

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

この事は、$n \to \infty$ で、$\mathbb{Q}(\mu_{p^n})$ 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、2次体 k に対して、k 上の2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、$\lambda_\psi = 0, 1$ とな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、$\forall n \geq 0$ で $\mathbb{Q}(\mu_{p^n})$ のすべての p 次不分岐巡回拡大は NIB を持ちます。なお、確率論的な議論

によって、高々有限個のpを除いてすべてのψで、$\lambda_\psi \leq 2$ となる事が予想されています。(Lang [10], Chap. 10 参照)

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ζを含む代数体とし、$\lambda=\zeta-1$ とおきます。

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

$\cup$

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

とします。

但し、pと素な数αに対して、αがsingulär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、

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

$[\alpha]\in V$ に対して、

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

が知られています。

従って、$k=k_n=\mathbb{Q}(\mu_{p^{n+1}})$に対する$V$, $\mathcal{E}$ をV_n, $\mathcal{E}_n$とかけば、問題Qは、$V_n=\mathcal{E}_n$か？ という問になります。

V_n, $\mathcal{E}_n$ は、$\Delta=Gal(k_0/\mathbb{Q})$ $(\hookrightarrow Gal(k_n/\mathbb{Q}))$ の作用で固有空間

分解して考えます。$\mathcal{E}_n^- = \{1\}$, $V_n(\chi_0) = \{1\}$ (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 とかきます。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 polyn., $u_\psi \in \mathbb{Z}_p[[t]]^\times$ と一意的に分解されます。

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

A_n: p^n, $p^{n-1-j} t^{p^j}$ $(0 \le j \le n-1)$ で生成される $\mathbb{Z}_p[t]$ の ideal とします。

この時、

<u>定理</u> 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) $p^{n-1}(p-1) \ge \lambda_\psi$ の時、$V_n(\chi) = \mathcal{E}_n(\chi)$。

(b) $p^{n-1}(p-1) < \lambda_\psi < p^n$ の時、

$$V_n(\chi) = \mathcal{E}_n(\chi) \iff t^{p^n - \lambda_\psi} \cdot H_\psi(t) \in pA_n$$

(c) $p^n \le \lambda_\psi$ の時、

$$V_n(\chi) = \mathcal{E}_n(\chi) \iff H_\psi(t) \in pA_n$$

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. Haggenmüller : 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. Michaliček : 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