Title	On a normal integral basis problem over cyclotomic $\mathbb{Z}_p$-extensions (Algebraic Number Theory and Related Topics)
Author(s)	市村, 文男
Citation	数理解析研究所講究録 (2003), 1324: 67-75
Issue Date	2003-05
URL	http://hdl.handle.net/2433/43147
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1324 巻 2003 年 67-75

On a normal integral basis problem over cyclotomic $\mathbb{Z}_p$-extensions

横浜市立大学数理科学教室 市村 文男 (Humio Ichimura)
Department of Mathematical Science,
Yokohama City University

§1 序文

講演ではまず Hilbert-Speiser の定理に関連するいくつかの話題を述べた後、特殊な設定の下ではあるが、ある種の素数次巡回拡大が normal integral basis を持つか否かを p 進 L 関数が生々しく支配している事を報告した。内容は私の論文 [1], [2], [3] にもとづいている。以下、記号を導入した上で、問題と得られた結果を述べる。

§2 設定と問題

代数体の有限次ガロア拡大 L/K が normal integral basis (NIB) を持つとは、O_L が群環 $O_K[\mathrm{Gal}(L/K)]$ 上 cyclic になる事を言う。ここで、O_K は K の整数環である。Noether により、L/K が NIB を持てば、L/K は tame である。NIB についての

古典的な問題のひとつは、tameなガロア拡大全体のなかでNIBを持つものがどのくらいあるかという問である。

以下、pを奇素数，Kをζ_pを含む虚アーベル体，K_∞/Kを円分$\mathbb{Z}_p$拡大，K_nをそのn番目の中間体とする。但し、$K_0=K$.

$S_n := \{a \in \mathcal{O}_{K_n} \mid a\mathcal{O}_{K_n} : \text{square free},\ a \equiv 1 \bmod \mathfrak{p},\ {}^\forall \mathfrak{p} | p\}$

とし、$a, b \in S_n$に対して$a \sim b$を$K_n(a^{1/p}) = K_n(b^{1/p})$となる事と定める。集合$\mathcal{S}_n, \mathcal{T}_n, \mathcal{N}_n$を次の様に定義する。

$\mathcal{S}_n := S_n/\sim$,

$\mathcal{T}_n := \{[a]_n \in \mathcal{S}_n \mid K_n(a^{1/p})/K_n : \text{tame}\}$,

$\mathcal{N}_n := \{\quad \text{〃} \quad \mid \quad \text{〃} \quad$: NIBを持つ$\}$.

Noetherにより、$\mathcal{N}_n \subseteq \mathcal{T}_n$である。$m>n$の時、自然な写像$K_n \to K_m$は単射$\mathcal{T}_n \to \mathcal{T}_m$を誘導するので、以下$\mathcal{T}_n \subseteq \mathcal{T}_m$とみなす。この時、$\mathcal{N}_n \subseteq \mathcal{N}_m$である。集合$\mathcal{T}_n \cap \mathcal{N}_m$は、$[a]_n \in \mathcal{T}_n$で$K_m(a^{1/p})/K_m$がNIBを持つもの全体である。

講演で扱った問題は次の2つである：

問1（古典的問題）$\mathcal{T}_n$内で$\mathcal{N}_n$はどのくらい大きいか小さいか？,

問2（単項化の問題）$m>n$の時、$\mathcal{T}_n \cap \mathcal{N}_m$は$\mathcal{T}_n$内でどのくらい大きいか小さいか？

問2は、イデアル類群についての次の良く知られた事実を意識して設定した。A_nをK_nのイデアル類群のp-part,

$A_\infty = \varinjlim A_n$ をその順極限とする。これらの群は複素共役の作用で分解される。

事実 (i) $m>n$ の時、自然な写像 $A_n^- \to A_m^-$ は単射，

(ii) A_∞^- の構造は p 進 L 関数で記述される (Mazur-Wiles の定理)；

(iii) $A_\infty^+ = 0$ (Greenberg 予想)。

この事実の類似が成り立つかというのが問2の内容である。

§3 結果1

イデアル類群の場合と同じ様に J_n も複素共役の作用で分解したい。U_n を K_n の p での主 semi-local units の群とする。良く知られている様に、$[a]_n \in \mathcal{S}_n$ に対して、

$$[a]_n \in J_n \iff a \equiv u^p \bmod \pi^p,\ {}^\exists u \in U_n.$$

但し、$\pi = \zeta_p - 1$. そこで、

$$J_n^\pm := \{[a]_n \in J_n \mid a \equiv u^p \bmod \pi^p,\ {}^\exists u \in U_n^\pm\}$$

と定める。u として 1 をとれば、$J_n^+ \cap J_n^-$ が無限集合である事がわかる。しかし、実は $J_n^+ \cap J_n^- \subseteq N_n$ なので問題はない。

<u>命題1</u>　$p \nmid [K:\mathbb{Q}]$ の時、次が成り立つ：

(i) $J_0 = N_0$,

(ii) $J_n^- \cap N_n$ は J_n^- 内で"非常に小さい", ${}^\forall n \geq 1$,

(iii) $J_n \cap N_m \subseteq N_n$, $\forall m > n \geq 0$.

(iii) は、$A_n^- \to A_m^-$ の単射性の類似である。以下、J_n^+を扱う。次の仮定の下で話を進める。

(C1) $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ の exponent は $p-1$.

(C2) p 上の K の素点は唯一つ.

<u>命題2</u> (C1), (C2) の下で、$p \nmid h_K^- = h_K/h_{K^+} \Rightarrow J_n^+ \subseteq N_n$, $\forall n \geq 1$. 但し、h_Kは K の類数である。

この命題は、Kummer duality $p \nmid h_K^- \Rightarrow p \nmid h_{K^+}$ と良く似ている。以下、$p \mid h_K^-$ の場合を扱う。そのため、J_nをΔの作用でより細かく分解する。$\chi \in \hat{\Delta}$ を $\mathbb{Q}_p$-値の偶指標，$\chi^* = \omega\chi^{-1}$ をその双対とする。但し、ω は Δ の ζ_p への作用を表わす指標である。

$$J_n(\chi) := \{[a]_n \in J_n \mid a \equiv u^p \bmod \pi^p, \ \exists u \in U_n(\chi)\}$$

と定める。Δの自明な指標χ_0に対して、$A_n(\chi_0) = 0$ が知られている(Stickelbergerの定理)。これの類似として次が成り立つ。

<u>命題3</u> $J_n(\chi_0) \subseteq N_n$, $\forall n \geq 1$.

以下、$\chi \in \hat{\Delta}$を非自明な偶指標とする。(C1), (C2) に加えて

次を仮定する。

(C3) $A_0(\chi^*) \neq 0$.

$g_\chi(T) \in \Lambda = \mathbb{Z}_p[[T]]$ を p 進 L 関数 $L_p(s, \chi)$ に対応する巾級数とする； $g_\chi((1+p)^{1-s}-1) = L_p(s, \chi)$.

$P_\chi(T)$ を g_χ に付随する distinguished な多項式とする。$\lambda_\chi^* = \deg P_\chi$ とおく。(C3) より $\lambda_\chi^* \geqq 1$ である。I_n を $p^n, p^{n-1-j}T^{p^j}$ $(0 \leqq j \leqq n-1)$ で生成された Λ のイデアルとする。この時、次が成り立つ。

<u>定理1</u>　仮定 (C1)〜(C3) の下で更に $A_0(\chi) = 0$ と仮定する。

(1) $|J_n(\chi) \setminus N_n| = \infty$, $\forall n \geqq 1$.

(2) $p^{n-1}(p-1) \geqq \lambda_\chi^*$ の時： $J_n(\chi) \cap N_m \subseteq N_n$, $\forall m > n$.

(3) $p^{n-1}(p-1) \leqq \lambda_\chi^* \leqq p^n$ の時：

　(i) $|J_n(\chi) \setminus N_{n+1}| = \infty$,

　(ii) $T^{p^n - \lambda_\chi^*} P_\chi \notin I_n \Rightarrow |(J_n(\chi) \cap N_{n+1}) \setminus N_n| = \infty$,

　　　〃 $\in I_n \Rightarrow J_n(\chi) \cap N_{n+1} \subseteq N_n$.

(4) $p^n \leqq \lambda_\chi^*$ の時：

　(i) $p \,\|\, P_\chi(0) \Rightarrow J_n(\chi) \subseteq N_{n+1}$,

　　$p^2 \mid P_\chi(0) \Rightarrow |J_n(\chi) \setminus N_{n+1}| = \infty$,

　(ii) $P_\chi \notin I_{n+1} \Rightarrow |(J_n(\chi) \cap N_{n+1}) \setminus N_n| = \infty$

　　$P_\chi \in I_{n+1} \Rightarrow J_n(\chi) \cap N_{n+1} \subseteq N_n$.

(5) $m > n \geqq 1$ に対して、

$$J_n(\chi) \not\subseteq N_{m-1} \text{ だが } J_n(\chi) \subseteq N_m$$
$$\Longleftrightarrow \text{(i) } \lambda_\chi^* \geqq p^n, \text{ (ii) } p^{m-n} \| P_\chi(0), \text{ (iii) } P_\chi \in (p^{m-n}, I_m).$$

(2)により、大きいnに対しては"単項化"の現象は起こらない。つまり、Greenberg予想の類似は整数環では成り立たない。(3)～(5)では、小さいnに対しては"単項化"の現象が起こり得て、実際に起こるかどうかをp進L関数$P_\chi(T)$が支配している事をいっている。

例（陽田浩樹氏による）$p=3$, $K=\mathbb{Q}(\sqrt{-3}, \sqrt{d})$, $d>0$ とする。χをΔの唯一の非自明偶指標とする。

$d=269681$ で $(n, m)=(1,2),(2,3)$ で (5)の(i),(ii),(iii)の条件がみたされている，

$d=9340977$ で $(n, m)=(1,3)$ で (5)の(i),(ii),(iii)の条件が成立。

§4 結果2（主結果）

E_n, C_nをそれぞれK_nの単数群，円単数群とし、$\mathcal{E}_n=\overline{E_n \cap U_n}$, $\mathcal{C}_n=\overline{C_n \cap U_n}$とする。$U_n^{(1)}=\{u \in U_n \mid u \equiv 1 \bmod \pi\}$とする。§3で述べた様に、$[a]_n \in \mathcal{S}_n$に対して、$[a]_n \in J_n \Leftrightarrow a \equiv u^p \bmod \pi^p$, $\exists u \in U_n$である。この$u=u_a$は$U_n^{(1)}$を法として一意的に定まる。次の主張が、問1,問2と岩澤理論をつなぐ橋であ

る。

<u>Key Lemma</u>　$[a]_n \in J_n$ に対して、

$$[a]_n \in N_n \Longleftrightarrow a \equiv \varepsilon^p \bmod \pi^p,\ {}^{\exists}\varepsilon \in \mathcal{E}_n$$
$$(\Longleftrightarrow u_a \in \mathcal{E}_n \mathcal{U}_n^{(1)}).$$

この補題により、$m \geqq n$ に対して、

$$(*)\quad [a]_n \in N_m \Longleftrightarrow u_a \in \mathcal{E}_m \mathcal{U}_m^{(1)}$$

である。そこで写像 θ_n を

$$\theta_n : J_n^+ \longrightarrow (\mathcal{U}_n / \mathcal{E}_n \mathcal{U}_n^{(1)})^+,\ [a]_n \longmapsto \overline{u_a}$$

で定める。θ_n は全射である事，各類 $\bar{u} \in (\mathcal{U}_n/\mathcal{E}_n \mathcal{U}_n^{(1)})^+$ に対して $\theta_n^{-1}(\bar{u})$ が無限集合になる事が容易にわかる。(*) にかんがみ

$$H_{n,m} = \ker(\mathcal{U}_n \longrightarrow \mathcal{U}_m / \mathcal{E}_m \mathcal{U}_m^{(1)},\ u \mapsto u \bmod \mathcal{E}_m \mathcal{U}_m^{(1)})^+$$

とおく。容易に、$H_{n,m} \subseteq H_{n,m+1}$、(*) より、

$$J_n^+ \cap N_n = \theta_n^{-1}(\bar{1})$$
$$J_n^+ \cap N_m = \theta_n^{-1}(\overline{H_{n,m}}) \quad (\text{但し、} \overline{H_{n,m}} = H_{n,m} \bmod \mathcal{E}_n \mathcal{U}_n^{(1)})$$

となる。従って、問1, 問2は、filtration

$$(\mathcal{U}_n^{(1)}\mathcal{E}_n)(\chi) = H_{n,n}(\chi) \subseteq H_{n,n+1}(\chi) \subseteq \cdots \subseteq H_{n,m}(\chi) \subseteq \cdots \quad \subseteq \mathcal{U}_n(\chi)$$

を調べよという問題に帰着する。$\mathcal{U}_n$ について次の事が知られている。$\omega_m = (1+T)^{p^m} - 1$, $\nu_{n,m} = \omega_m/\omega_n$ $(m \geqq n)$ とおく。

(1)　$\mathcal{U}_n(\chi) \simeq \Lambda/(\omega_n)$,

(2) $\mathcal{H}_n^{(1)}(\chi) \simeq I_n/(\omega_n)$,

(3) $\lambda_0(\chi)=0 \Rightarrow \mathcal{E}_n(\chi) = \mathcal{E}_n(\chi) \simeq (P_\chi, \omega_n)/(\omega_n)$.

従って、

$G_{n,n} = (P_\chi, I_n)$,

$G_{n,m} = \ker(\Lambda \longrightarrow \Lambda/G_{m,m}\,;\ x \longmapsto \overline{\nu_{n,m}x})$, $m>n$

とおくと、$H_{n,m}(\chi) \simeq G_{n,m}/(\omega_n)$, $\forall m \geq n$, となり、結局、我々の問題は、Λのイデアルのfiltration

$G_{n,n} \subseteq G_{n,n+1} \subseteq \cdots \subseteq G_{n,m} \subseteq \cdots \subseteq \Lambda$

を調べる事に帰着する。

<u>定理2</u> 以上の設定の下で次が成り立つ.

(1) 商 $G_{n,m+1}/G_{n,m}$ はΛ加群としてcyclicであり、そのΛ上の生成元は$P_\chi(T)$から出発して$m-n$に関して"帰納的"に計算できる。

(2) $m=n$とする.

$h_\chi = (P_\chi - T^{\lambda_\chi^*})/p$,

$p^n \leq \lambda_\chi^* \Rightarrow A = h_\chi$, $p^n \geq \lambda_\chi^* \Rightarrow A = T^{p^n-\lambda_\chi^*}h_\chi$ とおくと、

$G_{n,n+1}/G_{n,n}$ はΛ上Aの類で生成される。

定理1の大部分は定理2をもとにした多少の計算によって得られる。

参考文献

[1] H. Ichimura, Note on the ring of integers of a Kummer extension of prime degree, III, Proc. Japan Acad., 77A (2001), 71-73.

[2] H. Ichimura, On a normal integral basis problem over cyclotomic $\mathbb{Z}_p$-extensions, II, J. Number Theory, 96 (2002), 105-132.

[3] H. Ichimura, On some ideals of the p-adic power series ring arising from a normal integral basis problem, 投稿中.