数理解析研究所講究録
942巻 1996年 112-123

GREENBERG予想と正規整数底

日大生産工・福田 隆

1. $\mathbb{Z}_p$-拡大と正規整数底

K/k を有限次代数体の有限 Galois 拡大とし、$G = Gal(K/k)$ を Galois 群とする。よく知られているように、K/k は正規底をもつ。すなわち $\{\alpha^\sigma \mid \sigma \in G\}$ が K の k 上の基底となるような$\alpha \in K$ が存在する。それでは整数環はどうだろうか。$\mathfrak{O}_K, \mathfrak{O}_k$ をそれぞれ K, k の整数環とする。$\{\alpha^\sigma \mid \sigma \in G\}$ が $\mathfrak{O}_K$ の $\mathfrak{O}_k$ 上の基底となるような $\alpha \in \mathfrak{O}_K$ が存在する時、K/k は正規整数底をもつという。正規整数底は存在することも存在しないこともある。例えば正規整数底をもつための必要条件として次の結果が知られている。

定理 1.1 (cf. [36]). *K/k が正規整数底をもてば K/k は tamely 分岐である。*

さて p を素数とし、K/k が $\mathbb{Z}_p$-拡大の場合を考えよう。K/k が $\mathbb{Z}_p$-拡大であるとは、K/k は Galois 拡大であり Galois 群 $Gal(K/k)$ が p-進整数環 $\mathbb{Z}_p$ の加法群に位相同型であることである。このとき自然数 n に対し、K/k は k 上の次数が p^n である中間体 k_n を唯一もち、k_n/k は巡回拡大である。K/k に対し正規整数底を考える場合、中間体 k_n/k に対し正規整数底を考えるのが自然であるが、ある自然数 n_0 が存在し、K/k_{n_0} では少くとも一つの p 上の素イデアルが完全分岐するので 定理1.1 により、十分大きな n に対して k_n/k は正規整数底をもたない。そこで $\mathbb{Z}_p$-拡大に対しては 正規 p-整数底を考える。

定義 1.2. *K/k を有限次 Galois 拡大とする。$\{\alpha^\sigma \mid \sigma \in Gal(K/k)\}$ が $\mathfrak{O}_K$ の $\mathfrak{O}_k$ 上の基底となるような $\alpha \in \mathfrak{O}_K$ が存在する時、K/k は正規 p-整数底をもつという。*

定義 1.3. *$k = k_0 \subset k_1 \subset \cdots \subset K$ を $\mathbb{Z}_p$-拡大とする。全ての $n \geqq 0$ に対し、k_n/k が正規 p-整数底をもつ時、K/k は正規 p-整数底をもつという。*

勝手な $\mathbb{Z}_p$-拡大 K/k は正規 p-整数底を持つことも持たないこともある。どのような $\mathbb{Z}_p$-拡大が正規 p-整数底を持つか考えることは次節で説明する Greenberg 予想と関連して重要である。まず次の事柄に注意する。

補題 1.4 (cf. [25]). k を有限次代数体、K_1/k, K_2/k を p の外で不分岐な巡回拡大で $K_1 \cap K_2 = k$ とする。K_1/k, K_2/k が正規 p-整数底を持てば K_1K_2/k も正規 p-整数底を持つ。

これから次がでる。

命題 1.5. K_1/k. K_2/k を $K_1 \cap K_2 = k$ なる $\mathbb{Z}_p$-拡大とする。K_1/k, K_2/k が共に正規 p-整数底を持てば K_1K_2/k に含まれる全ての $\mathbb{Z}_p$-拡大 K/k は正規 p-整数底を持つ。

$$q_n = \begin{cases} 2^{n+2} & \text{if } p = 2, \\ p^{n+1} & \text{if } p > 3. \end{cases}$$

とおき、$\mathbb{Q}_n$ を 1 の q_n-分体 $\mathbb{Q}(\zeta_{q_n})$ の部分体で $[\mathbb{Q}_n : \mathbb{Q}] = p^n$ なるものとするとき、$\mathbb{Q}_\infty = \cup\mathbb{Q}_n$ は $\mathbb{Q}$ の唯一の $\mathbb{Z}_p$-拡大となる。有限次代数体 k に対し、$k_\infty = k\mathbb{Q}_\infty$ は k の $\mathbb{Z}_p$-拡大であり、円分 $\mathbb{Z}_p$-拡大と呼ばれる。

定理 1.6 (cf. [27]). 有限次代数体 k に対し、円分 $\mathbb{Z}_p$-拡大 k_∞/k は正規 p-整数底を持つ。

$\mathbb{Z}_p$-拡大 K/k を持ち上げると正規 p-整数底を持ちやすくなることが次の定理からわかる (cf. [30])。

定理 1.7 (小松). F を虚 2 次体、p を奇素数とし、$k = F(p)$ を F の $mod\, p$ の *ray class field* とする。この時、任意の $\mathbb{Z}_p$-拡大 K/F に対し、Kk/k は正規 p-整数底を持つ。

これは次の定理から容易に導かれる。

定理 1.8 (小松). 前定理と同じ状況の下で、$L = F(mod\, p^n)$ を F の $mod\, p^n$ の *ray class field* とする。この時、任意の自然数 n に対し、L/k は正規 p-整数底を持つ。

保型関数の特殊値を用いて正規 p-整数底の生成元を具体的に構成しているので、この証明は大変興味深い。以下に概略を説明する。

定理1.8の証明の概略

まず $m \geqq 1$ に対し保型関数 f_m を構成する。$\mathbb{C}$ の格子 $\Omega = \mathbb{Z}\tau_1 + \mathbb{Z}\tau_2$ $(\mathrm{Im}(\tau_1/\tau_2) > 0)$ に対し、$\sigma_\Omega(z)$ を Wierstrass の σ-関数とし、

$$\eta_i = 2\frac{\sigma'_\Omega(\tau_i/2)}{\sigma_\Omega(\tau_i/2)}$$

とおく。$a_1, a_2 \in \mathbb{R}$ に対し、

$$f(a_1, a_2; \tau_1, \tau_2) = e^{-\frac{(a_1\eta_1 + a_2\eta_2)(a_1\tau_1 + a_2\tau_2)}{2}}\sigma_\Omega(a_1\tau_1 + a_2\tau_2)$$

とおき、整数 r, s, N に対し Siegel 関数 $g(\frac{r}{N}, \frac{s}{N})$ を

$$g(\frac{r}{N}, \frac{s}{N})(z) = 2\pi i e^{\pi i z/6} f(\frac{r}{N}, \frac{s}{N}; z, 1)\prod_{\nu=1}^{\infty}(1 - e^{2\pi i \nu z})^2$$

で定義する。さらに

$$\delta_p = \begin{cases} 12 & \text{if } p \neq 3, \\ 4 & \text{if } p = 3. \end{cases}$$

とし、

$$\tilde{g}(\frac{r}{p^m}, \frac{s}{p^m}) = g(\frac{r}{p^m}, \frac{s}{p^m})^{\delta_p}$$

とおく。$\tilde{g}(\frac{r}{p^m}, \frac{s}{p^m})$ は level p^{2m} の保型関数である。$(u, 2p^m) = 1$ の時 $\sigma_u \in G(\mathbb{Q}(\zeta_{2p^m})/\mathbb{Q})$ を $\zeta_{2p^m}^{\sigma_u} = \zeta_{2p^m}^u$ で定め、$\tilde{g}$ の ∞ における q-expansion の係数に σ_u を作用させることにより $\tilde{g}^{\sigma_u}$ を定義する。$\det A = u$ なる $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{Z})$ に対し、$A \equiv \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} A' \pmod{2p^m}$ なる $A' = \begin{pmatrix} a'_{11} & a'_{12} \\ a'_{21} & a'_{22} \end{pmatrix} \in SL_2(\mathbb{Z})$ をとり

$$\tilde{g}^A(z) = \tilde{g}^{\sigma_u}(\frac{a'_{11}z + a'_{12}}{a'_{21}z + a'_{22}})$$

で $\tilde{g}^A$ を定義する。さて $F = \mathbb{Q}(\sqrt{-d})$ とする。$d \equiv 1, 2 \pmod 4$ の場合を考える。$d \equiv 3 \pmod 4$ の場合も同様である。$\omega_1 = 1$, $\omega_2 = -\sqrt{-d}$ とおく。$S_m = \{(\alpha) \mid \alpha \in F,\ \alpha \equiv 1 \pmod{p^m}\}, k_m = k(\zeta_{p^m}), L' = F(\ \mathrm{mod}\ p^{2n})$ とおく。類体論と密度定理より

$$G(L'/k_{2n}) = < \left(\frac{L'/K}{(\alpha_1)}\right) >, \quad \alpha_1\bar{\alpha}_1 \equiv 1 \pmod{p^{2n}}, \quad \alpha_2 \equiv 1 + p \pmod{p^{2n}}$$

$$S_1/S_{2n} = < (\alpha_1)S_{2n}, (\alpha_2)S_{2n} > \simeq \mathbb{Z}/p^{2n-1}\mathbb{Z} \oplus \mathbb{Z}/p^{2n-1}\mathbb{Z}$$

となる $\alpha_1, \alpha_2 \in F$ がとれる。

$$\alpha_i \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = B(\alpha_i) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

で $B(\alpha_i) \in M_2(\mathbb{Z})$ を定義し、

$$f_m = \prod_{\nu=0}^{p^{m-1}-1} \tilde{g}^{B(\alpha_1)^\nu}(\frac{1}{p^m}, 0)$$

とおく。f_m は level p^{2m} の保型関数であり次の性質をみたす。

(i) f_m は上半平面に極および零点をもたない
(ii) f_m の ∞ における q-expansion の係数は $\mathbb{Z}[\zeta_{p^{2m}}]$ に含まれ、全てのカスプにおける q-expansion の最初の係数は p-単数である。

これより $f_m(\omega_1/\omega_2)$ は p-単数になる。また、$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{Z})$ $a_{12} \equiv a_{21} \equiv 0 \pmod{p^m}$, $a_{11} \equiv a_{22} \equiv 1 \pmod{p^m}$ に対し、

$$\tilde{g}^A(\frac{r}{p^m}, \frac{s}{p^m}) = e^{\frac{\delta p \pi i}{p^{2m}}(a_{12}r^2 + (a_{22}-a_{11})rs - a_{21}s^2)} \tilde{g}(\frac{r}{p^m}, \frac{s}{p^m})$$

であるから、$f_m^{B(\alpha_1)}/f_m$ は 1 の原始 p^m-乗根であり、$f_m^{B(\alpha_2)^{p^{m-1}}} = f_m$ となる。

$K'^{(m)}$ を $< (\frac{L'/K}{(\alpha_1)})^{p^{m-1}}, (\frac{L'/K}{(\alpha_2)}) >$ に対応する L'/k の中間体とすると、$G(L'/k_m) = < (\frac{L'/F}{\alpha_1}), (\frac{L'/F}{\alpha_2})^{p^{m-1}} >$, $F(\bmod p^m) = k_m K'^{(m)}$ である。

志村の相互法則より

$$f_m(\omega_1/\omega_2)^{(\frac{L'/F}{\alpha_1})} = f_m^{B(\alpha_1)}(\omega_1/\omega_2)$$

$$f_m(\omega_1/\omega_2)^{(\frac{L'/F}{\alpha_2})^{p^{m-1}}} = f_m^{B(\alpha_2)^{p^{m-1}}}(\omega_1/\omega_2) = f_m(\omega_1/\omega_2)$$

だから、$1 \leqq m \leqq n$ に対し、$f_m(\omega_1/\omega_2)^{p^m} \in k_m$, $k_m K'^{(m+1)} = k_m(f_m(\omega_1/\omega_2))$ となることがわかる。従って

補題 1.9 (cf. [26]). k を有限次代数体、p を奇素数とし、K/k を p の外で不分岐な有限巡回 p-拡大とする。$G(K/k)$ の指標 χ に対し、$Ker\,\chi$ に対応する K/k の中間体を k_χ で表し、$\nu_\chi = [k_\chi : k]$. $e_\chi = [k_\chi(\zeta_{\nu_\chi}) : k(\zeta_{\nu_\chi})]$ とする。任意の $\chi \neq 1$ に対し、$k_\chi(\zeta_{\nu_\chi}) = k(\zeta_{\nu_\chi})(\sqrt[e_\chi]{u_\chi})$ となる p-単数 $u_\chi \in k(\zeta_{\nu_\chi})$ が存在すれば K/k は正規 p-整数底をもつ。

より $K'^{(n+1)}/k$ は正規 p-整数底をもつ。定理1.6より k_{n+1}/k は正規 p-整数底をもつから、補題1.4より $F(\bmod p^{n+1})/k$ も正規 p-整数底をもつ。

2. GREENBERG 予想との関係

$\mathbb{Z}_p$-拡大に関しては岩澤健吉 (cf. [23]) により証明された次の結果が基本的である。

定理 2.1. $k = k_0 \subset k_1 \subset \cdots \subset K$ を $\mathbb{Z}_p$-拡大とし、p^{e_n} を k_n の類数の p-部分とする。この時、整数 $\mu = \mu_p(K/k) \geqq 0$, $\lambda = \lambda_p(K/k) \geqq 0$. $\nu = \nu_p(K/k)$ が存在し、十分大きな全ての n に対し、

$$e_n = \mu p^n + \lambda n + \nu$$

が成立する。

$\mu_p(K/k)$, $\lambda_p(K/k)$, $\nu_p(K/k)$ は K/k の岩澤不変量と呼ばれる。円分 $\mathbb{Z}_p$-拡大 k_∞/k に対する岩澤不変量は$\mu_p(k)$, $\lambda_p(k)$, $\nu_p(k)$ と書かれ、代数体 k の重要な不変量の一つと考えられている。$\mu_p(K/k)$ は一般には 0 にならないが、$\mu_p(k)$ は 0 であろうと予想されている。

予想 2.2. 任意の有限次代数体 k および任意の素数 p に対し、$\mu_p(k) = 0$。

この予想はまだ未解決であるが、Ferrero-Washington ([4]) により、$k/\mathbb{Q}$ がアーベル拡大の場合には証明されている。Greenberg([18]) により提起された次の問題は現在では Greenberg 予想と呼ばれている。

予想 2.3 (Greenberg 予想). 任意の有限次総実代数体 k および任意の素数 p に対し、$\mu_p(k) = \lambda_p(k) = 0$。

即ち、総実代数体 k の円分 $\mathbb{Z}_p$-拡大に対しては、中間体 k_n の類数の p-部分は有界であろうという予想である。この予想は、例えば $k/\mathbb{Q}$ がアーベル拡大の時、k の岩澤加群 (k_∞ の最大アーベル不分岐 p-拡大の k_∞ 上のガロア群) の minus part の特性多項式は、岩澤の主予想を通じて p-進 L-関数を記述する岩澤多項式と結び付いているが、plus part を記述すべき p-進 L-関数は Bernoulli 数の性質により恒等的に零になってしまうという事実に対応していると考えられる。また、Greenberg 予想から Mazur と Wiles によって証明された岩澤の主予想が導かれることも知られている (cf. [3], [17], [19])。

Greenberg 予想が成立する例も構成されており (cf. [18], [2])、特に k が実 2 次体の場合には詳しい数値実験が行われていた (cf. [8], [11], [13], [15])。更に最近数値実験に適した効率的な判定アルゴリズムが開発され (cf. [20], [21], [32], [33])、これまで不明だった $\lambda_3(\mathbb{Q}(\sqrt{254}))$ を含め、実例を計算するとことごとく予想が成立していることが確かめられている。ここ一年間のこのような進展により Greenberg 予想の正当性はかなり高くなったと考えられる。

さて、Greenberg 予想と正規整数底は Vandiver 予想に対する必要十分条件として Kersten と Michaliček により関係づけられた。

定理 2.4 (Kersten-Michaliček, [28]). p を奇素数、k^+ を p-分体 $\mathbb{Q}(\zeta_p)$ の最大実部分体、$h(k^+)$ を k^+ の類数とする。この時、

$$p \nmid h(k^+) \Longleftrightarrow \lambda_p(k^+) = 0 \text{ かつ } k \text{ の任意の } \mathbb{Z}_p\text{-拡大は正規 } p\text{-整数底をもつ}$$

環のガロア理論に基づいて証明される次の定理を認めれば $\Longleftarrow$ は以下のようにして示される。

定理 2.5 ([28]). $k_n = \mathbb{Q}(\zeta_{p^n})$ のイデアル類群の p-部分を A_n とし、$\iota_{0,n} : k_0 \longrightarrow k_n$ を埋め込みとする。この時、

$$k \text{ の全ての } \mathbb{Z}_p\text{-拡大は正規 } p\text{-整数底をもつ}$$

$$\Longleftrightarrow \text{全ての } n \geqq 0 \text{ に対し、} \iota_{0,n} : A_0 \longrightarrow A_n \text{ は単射}$$

複素共役写像 ρ は自然に A_n に作用するので、$A_n^- = A_n^{1-\rho}$, $A_n^+ = A_n^{1+\rho}$ とおく。$A_n = A_n^- \oplus A_n^+$ である。$\iota_{0,n} : A_0^- \longrightarrow A_n^-$ の単射性は岩澤 (cf. [23]) により知られているので、定理2.5では $\iota_{0,n} : A_0^+ \longrightarrow A_n^+$ の単射性が本質的である。k_n には p 上の素イデアルは一つしかないので次の補題がでる。

補題 2.6.

$$\text{全ての } n \geqq 0 \text{ に対し、} \iota_{0,n} : A_0 \longrightarrow A_n \text{ は単射}$$

$$\Longleftrightarrow \text{全ての } n \geqq m \geqq 0 \text{ に対し、} \iota_{m,n} : A_m \longrightarrow A_n \text{ は単射}$$

定理2.4の $\Longleftarrow$ の証明.

k の任意の $\mathbb{Z}_p$-拡大が正規 p-整数底をもち $A_0^+ \neq 1$ ならば$\lambda_p(k^+) \neq 0$ であることを示す。全ての $n \geqq 0$ に対し、ノルム写像 $N_{n+1,n} : A_{n+1}^+ \longrightarrow A_n^+$ は全射だから、$A_n^+ \neq 1$ である。また定理2.5、補題2.6より、全ての $n \geqq 0$ に対し、$i_{n,n+1} : A_n^+ \longrightarrow A_{n+1}^+$ は単射である。$i_{n,n+1}(A_n^+) = A_{n+1}^+$ と仮定すると、任意の $I \in A_n^+$ に対し $N_{n+1,n}(I') = I$ となる $I' \in A_{n+1}^+$ が存在し、さらに $i_{n,n+1}(J) = I'$ となる $J \in A_n^+$ が存在する。$I = N_{n+1,n}(I') = N_{n+1,n}(i_{n,n+1}(J)) = N_{n+1,n}(J) = J^p$ より $A_n^+ = (A_n^+)^p$ となる。$A_n^+ \neq 1$ だからこれは矛盾である。従って $i_{n,n+1}(A_n^+) \subsetneq A_{n+1}^+$ となり、$|A_n^+| < |A_{n+1}^+|$。故に $|A_n^+|$ は有界でない。ところが十分大きな全ての $n \geqq 0$ に対し、

$$|A_n^+| = p^{\mu_p(k^+)p^n + \lambda_p(k^+)n + \nu_p(k^+)}$$

であり、[4] より $\mu_p(k^+) = 0$ だから $\lambda_p(k^+) \neq 0$。

$\Longrightarrow$ については代数体の言葉による別証明と一般化が得られている。

定理 2.7 (河本-小松, [26]). p を奇素数、k を ζ_p を含むアーベル拡大で p が $k^+/\mathbb{Q}$ で不分解なものとする。この時、

$$p \nmid h(k^+) \Longrightarrow \lambda_p(k^+) = 0 \text{ かつ } k \text{ の任意の } \mathbb{Z}_p\text{-拡大は正規 } p\text{-整数底をもつ}$$

正規整数底の非存在を Greenberg 予想に対する必要条件として考察する試みもある。p を奇素数、F を虚 2 次体とする。K を F の全ての $\mathbb{Z}_p$-拡大の合併とし、$X = G(K/F)$ とおく。[1], [24] より $X \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ であり、複素共役写像 ρ を内部自己同型で X に作用させると $X = X^{1-\rho} \oplus X^{1+\rho}$ となる。$X^{1-\rho}$, $X^{1+\rho}$ に対応する K/F の中間体をそれぞれ F_∞, F_∞^- とする。F_∞, F_∞^- は $\mathbb{Q}$ 上ガロア拡大である F の $\mathbb{Z}_p$-拡大である。F_∞ は F の円分 $\mathbb{Z}_p$-拡大であり、F_∞^- は F の反円分 $\mathbb{Z}_p$-拡大と呼ばれる。

$k = F(\zeta_p)$, $\Delta = G(k/F)$ とおく。$\omega : \Delta \longrightarrow \mathbb{Z}_p^\times$ を Teichmüller 指標とし、

$$e_i = \frac{1}{|\Delta|} \sum_{g \in \Delta} \omega(g)^i g^{-1} \in \mathbb{Z}_p[\Delta]$$

とおく。この時次の結果が知られている。

定理 2.8 ([12]). p, F, k を上の通りとし、A^+ を k^+ のイデアル類群の p-部分とする。更に p は $F/\mathbb{Q}$ で惰性し、$(A^+)^{e_1} \neq 1$ と仮定する。この時、$\lambda_p(k^+) = 0$ ならば F_∞^-/F は正規 p-整数底をもたない。

$p = 3$ の場合には Greenberg 予想と正規整数底の関係がよりはっきりとした形で与えられる。$k = \mathbb{Q}(\sqrt{d})$ を実 2 次体とし、$k^- = \mathbb{Q}(\sqrt{-3d})$ とする。円分 $\mathbb{Z}_3$-拡大 k_∞/k の中間体 k_n のイデアル類群の 3-部分を A_n とする。[4] により $\mu_3(k) = 0$ だから、Greenberg 予想は次のように言い換えることができる。

定理 2.9 (Greenberg). 3 が k で不分解の時、

$$\lambda_3(k) = 0 \Longleftrightarrow \text{ある } n \geqq 0 \text{ に対し、} A_0 \longrightarrow A_n \text{ は } 0\text{-}map$$

一方、正規整数底に関しては次が成り立つ。

定理 2.10 (Kersten, Michaliček, Fleckinger, Nguyen Quang Do, 小松, 福田). 3 が kk^- で不分解の時、

$$\text{反円分 } \mathbb{Z}_3\text{-拡大 } k_\infty^-/k^- \text{ が正規 3-整数底をもつ}$$

$$\Longleftrightarrow \text{全ての } n \geqq 0 \text{ に対し、} A_0 \longrightarrow A_n \text{ は単射}$$

定理2.9と定理2.10から、Greenberg 予想より弱い次の予想が考えられる。

予想 2.11 (小松). 3 が kk^- で不分解で k の類数が 3 で割れれば反円分 $\mathbb{Z}_3$-拡大 k_∞^-/k^- は正規 3-整数底をもたない。

3. 相対単数群との関係

この節の内容に関しては [9] を参照。k を実2次体、p を奇素数とし、$\mathbb{Q}=\mathbb{Q}_0\subset\mathbb{Q}_1\subset\cdots\subset\mathbb{Q}_\infty$, $k=k_0\subset k_1\subset\cdots\subset k_\infty$ を円分 $\mathbb{Z}_p$-拡大とする。$k_n=k\mathbb{Q}_n$ である。$E(k_n)$ で k_n の単数群、A_n で k_n のイデアル類群の p-部分を表す。

定義 3.1. $E_{n,R}=\{\varepsilon\in E(k_n)\mid N_{k_n/\mathbb{Q}_n}(\varepsilon)=\pm1,\ N_{k_n/\mathbb{Q}_n}(\varepsilon)=\pm1\}$ を k_n の相対単数群と呼ぶ。

$E_{n,R}$ の free rank は p^n-1 である。$E(k_n)$ に対しては Minkowski 単数の存在が知られているが、$E_{n,R}$ に対しても同様のことが成り立つ。

補題 3.2. ある $\varepsilon\in E_{n,R}$ が存在し、$(E_{n,R}:<\varepsilon^\sigma\mid\sigma\in G(k_n/\mathbb{Q})>)<\infty$ となる。

$G(k_n/\mathbb{Q})$ の生成元 σ を固定し、$\varepsilon\in E(k_n)$ に対し $e_i=e^{\sigma^i}$ と書くことにする。$r=p^n-1$ とおく。次の補題が成り立つので、次の定義は自然である。

補題 3.3. $\varepsilon\in E_{n,R}$ に対し、$\varepsilon_r=\pm(\varepsilon_1\varepsilon_3\cdots\varepsilon_{r-1})(\varepsilon_0\varepsilon_2\cdots\varepsilon_{r-2})^{-1}$

定義 3.4. $(E_{n,R}:<-1,\varepsilon_0,\varepsilon_1,\cdots,e_{r-1}>)$ が有限で p と素になる $\varepsilon\in E_{n,R}$ が存在する時、$E_{n,R}$ は p-正規底を持つという。

さて $E_{n,R,p^n}=\{\varepsilon\in E_{n,R}\mid\varepsilon^{1+\sigma}\in E_{n,R}^{p^n}\}$ とし、

$$V_n=E_{n,R,p^n}/E_{n,R}^{p^n},\quad r(V_n)=\dim_{\mathbb{F}_p}(V_n/V_n^p)$$

とおく。

命題 3.5. 全ての $n\geqq0$ に対し $|V_n|=p^n$ である。$r(V_n)$ は単調増加で有界である。

V_n のアーベル群としての構造は $E_{n,R}$ のガロア加群としての構造と関係があり、更に Greenberg 予想とも関係している。

命題 3.6. V_n は巡回群 $\Longleftrightarrow$ $E_{n,R}$ は p-正規底を持つ

定理 3.7. p が k で不分解の時、

全ての $n\geqq0$ に対し V_n は巡回群 $\Longleftrightarrow$ 全ての $n\geqq0$ に対し $A_0\longrightarrow A_n$ は単射

例えば $p=3$, $k=\mathbb{Q}(\sqrt{257})$ の時、V_1 は 3 次巡回群だが $A_0 \longrightarrow A_1$ は単射ではないから、"全ての" は必要である。前節の結果と合わせると次の定理が得られる。

定理 3.8. 3 が kk^- で不分解の時、次は同値。
(1) 反円分 $\mathbb{Z}_3$-拡大 k_∞^-/k^- は正規 3-整数底をもつ
(2) 全ての $n \geqq 0$ に対し、$A_0 \longrightarrow A_n$ は単射
(3) 全ての $n \geqq 0$ に対し $E_{n,R}$ は 3-正規底を持つ
(4) 全ての $n \geqq 0$ に対し V_n は巡回群

4. Example

$p=3$ で k が実 2 次体の場合の例を紹介しよう。

例 1. $k=\mathbb{Q}(\sqrt{2})$ とする。$3 \nmid h(k)$ だから$\lambda_3(k)=0$ であり、定理3.8により k_∞^-/k^- は正規 3-整数底をもつ。

例 2. $k=\mathbb{Q}(\sqrt{254})$ とする。$A_0 \simeq \mathbb{Z}/3\mathbb{Z}$ であり、$A_0 \longrightarrow A_3$ は単射である。$A_0 \longrightarrow A_4$ も単射である可能性が高い。最近 Kraft, Scooh, 市村, 隅田, 栗原氏により $A_0 \longrightarrow A_5$ が 0-map であることが示された。従って $\lambda_3(k)=0$ である。k_∞^-/k^- は正規 3-整数底をもたない。

例 3. $k=\mathbb{Q}(\sqrt{1937})$ とする。$A_0 \simeq \mathbb{Z}/3\mathbb{Z}$ である。$V_2 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ であることが判り、これより $A_0 \longrightarrow A_2$ が 0-map であることも判る。従って定理2.9より $\lambda_3(k)=0$ がわかる。k_∞^-/k^- は正規 3-整数底をもたない。

例 4. $k=\mathbb{Q}(\sqrt{32009})$ とする。$A_0 \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ である。$|\mathrm{Ker}(A_0 \longrightarrow A_1)|=3$ より k_∞^-/k^- は正規 3-整数底をもたないことがわかり、$|\mathrm{Ker}(A_0 \longrightarrow A_2)|=9$ より $\lambda_3(k)=0$ がわかる。これは巡回群でない A_0 に対し $\lambda_3(k)=0$ がわかる例として興味深い。3 が k で分解する時の同様の例は [16] で与えられている。

例 5. $k=\mathbb{Q}(\sqrt{53678})$ とする。$A_0 \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ である。$|\mathrm{Ker}(A_0 \longrightarrow A_1)|=1$, $|\mathrm{Ker}(A_0 \longrightarrow A_2)|=3$ より k_∞^-/k^- は正規 3-整数底をもたないことがわかる。$\lambda_3(k)=0$ かどうかは不明である。

注. $k=\mathbb{Q}(\sqrt{53678})$ に関しては 1995 年 11 月 1 日の時点では$\lambda_3(k)=0$ かどうか不明だったが、1995 年 12 月 13 日に数理研で開かれた「代数的整数論とフェルマーの問題研究集会」に於いて、市村-隅田氏により $\lambda_3(k)=0$ であることが報告された。

References

1. A. Brumer, *On the units of algebraic number fields*, Mathematika **14**, 121–124 (1967)
2. A . Candiotii, *Computations of Iwasawa invariants and K_2*, Compositio Math. **29**, 89–111 (1974)
3. J. Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic Number Fields (Durham Symposium, 1975, ed. by A. Fröloch), 269–353, Academic Press, 1977.
4. B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109**, 377–395 (1979)
5. V. Fleckinger and T. Nguyen Quang Do, *Bases normales unités et conjecture faible de leopoldt*, Manus. Math. **71**, 183–195 (1991)
6. T. Fukuda, *Iwasawa λ-invariants of certain real quadratic fields*, Proc. Japan Acad. **65A**, 260–262 (1989)
7. T. Fukuda, *emarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. **70A**, 264–266 (1994)
8. T. Fukuda, *Cyclotomic units and Greenberg's conjecture for real quadratic fields*, to appear in Math. Comp.
9. T. Fukuda, *Greenberg's conjecture and relative unit groups for real quadratic fields*, preprint (1996)
10. T. Fukuda and K. Komatsu, *On the λ invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Number Theory **23**, 238–242 (1986)
11. T. Fukuda and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan **38**, 95–102 (1986)
12. T. Fukuda and K. Komatsu, *Normal bases and λ-invariants of number fields*, Proc. Japan Acad. **67A**, 243–245 (1991)
13. T. Fukuda and K. Komatsu, *A capitulation problem and Greenberg's conjecture on real quadratic fields*, to appear in Math. Comp.
14. T. Fukuda, K. Komatsu and H. Wada, *A remark on the λ-invariants of real quadratic fields*, Proc. Japan Acad. **62A**, 318–319 (1986)
15. T. Fukuda and H. Taya, *The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arith. **LXIX.3**, 277–292 (1995)
16. T. Fukuda and H. Taya, *Computational research of Greenberg's conjecture for real quadratic fields*, Mem. School Sci. Eng., Waseda Univ. **58**, 175–203 (1994)
17. R. Greenberg, *On p-adic L-functions and cyclotomic fields*, Amer. J. Math. 98 (1974), 61–77.
18. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.

19. R. Greenberg, *On p-adic L-functions and cyclotomic fields II*, Nagoya Math. J. 67 (1977), 139–158.
20. H. Ichimura and H. Sumida, *On the Iwasawa λ-invariants of certain real abelian fields*, preprint (1995)
21. H. Ichimura and H. Sumida, *On the Iwasawa λ-invariants of certain real abelian fields II*, preprint (1995)
22. H. Ichimura and H. Sumida, *On the Iwasawa λ-invariant of the real p-cyclotomic field*, preprint (1995)
23. K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65**, 183–226 (1959)
24. K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. **98**, 246–326 (1973)
25. F. Kawamoto, *On normal integral bases*, Tokyo J. Math. **7**, 221–231 (1984)
26. F. Kawamoto and K. Komatsu, *Normal bases and $\mathbb{Z}_p$-extensions*, J. Algebra **163**, 335–347 (1994)
27. I. Kersten and J. Michaliček, *$\mathbb{Z}_p$-extensions of complex multiplication fields*, J. Number theory **32**, 131–150 (1989)
28. I. Kersten and J. Michaliček, *On Vandiver's conjecture and Z_p-extensions of $\mathbb{Q}(\zeta_{p^n})$*, J. Number theory **32**, 371–386 (1989)
29. K. Komatsu, *Modular construction of normal basis*, J. Math. Soc. Japan **46**, 235–243 (1994)
30. K. Komatsu, *Normal basis and Greenberg's conjecture*, Math. Ann., **300**, 157–163 (1994)
31. J. Kraft, *Iwasawa invariants of CM fields*, J. Number Theory **32**, 65–77 (1989)
32. J. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97**, 135–155 (1995)
33. M. Kurihara, *The Iwasawa λ invariants of real abelian fields and the cyclotomic elements*, preprint (1995)
34. B. Mazur and A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. 76 (1984), 179.
35. M. Ozaki and H. Taya, *A note on Greenberg's conjecture of real abelian number fields*, Manuscripta Math. **88**, 311–210 (1995)
36. A. Speiser, *Gruppendeterminante und Körperdiskriminante*, Math. Ann. **77**, 546–562 (1916)
37. H. Sumida, *Greenberg's conjecture and the Iwasawa polynomial*, preprint (1995)
38. H. Taya, *On the Iwasawa λ-invariants of real quadratic fields*, Tokyo J. Math. **16**, 121–130 (1993)

39. H. Taya, *Computation of $\mathbb{Z}_3$-invariants of real quadratic fields*, to appear in Math. Comp.
40. H. Taya, *On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields*, to appear in Acta Math.
41. A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. 131 (1990), 493–540.