

S-整数環の分岐アーベル拡大の normal basis の非存在について

学習院大学理学部 河本 史紀 (Fuminori Kawamoto)

1. INTRODUCTION

k を有限次代数体, K/k を Galois 群 G をもつ有限次 Galois 拡大とする. k の整数環 \mathfrak{o}_k の 0 でない prime ideals 全体の集合を \mathcal{P}_k で表わす. $S \subset \mathcal{P}_k$ とする. 有限次拡大 N/k について, いまと同じように \mathcal{P}_N を定義し,

$$\mathfrak{o}_N(S) := \{ x \in N \mid \text{ord}_{\mathfrak{p}}(x) \geq 0 \ (\forall \mathfrak{p} \in \mathcal{P}_N \text{ s. t. } \mathfrak{p} \cap k \notin S) \}$$

とおく. \mathfrak{o}_k の (したがって \mathfrak{o}_N の) 乗法的部分集合 $M := \mathfrak{o}_k - \cup_{\mathfrak{p} \in \mathcal{P}_k - S} \mathfrak{p}$ をとると, $\mathfrak{o}_N(S) = M^{-1}\mathfrak{o}_N$ が成り立つ ($\mathfrak{p}_0 \in \mathcal{P}_k$, $S := \mathcal{P}_k - \{\mathfrak{p}_0\}$ とおくと, $\mathfrak{o}_k(S)$ は \mathfrak{o}_k の \mathfrak{p}_0 による局所化である). したがって, Dedekind 環の分数環は Dedekind 環であるから, $\mathfrak{o}_N(S)$ は Dedekind 環になる. また, $\mathfrak{o}_N(S)$ の 0 でないすべての prime ideal 全体は $\{ \mathfrak{P} \mathfrak{o}_N(S) \mid \mathfrak{P} \in \mathcal{P}_N, \mathfrak{P} \cap k \notin S \}$ となる. そこで, ($N = K$, k ととると) $\mathfrak{o}_K(S)$ は群環 $\mathfrak{o}_k(S)[G]$ 上の module とみれる. これが free module であるとき (体の有限次 Galois 拡大の normal basis theorem から free rank は 1 である), Dedekind 環の拡大 $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は normal basis をもつ という. このとき, $\mathfrak{o}_k(S)[G]$ -module としての同型 $\mathfrak{o}_k(S)[G] \cong \mathfrak{o}_K(S)$ による 1 の行き先 $\alpha \in \mathfrak{o}_K(S)$ を normal basis の生成元 と呼ぶ. つまり, $\{\alpha^s\}_{s \in G}$ は $\mathfrak{o}_K(S)$ の $\mathfrak{o}_k(S)$ -free basis である.

K/k が tamely ramified のとき, $S := \emptyset$ とすると, $\mathfrak{o}_K(S) = \mathfrak{o}_K$, $\mathfrak{o}_k(S) = \mathfrak{o}_k$. $\mathfrak{o}_K/\mathfrak{o}_k$ が normal basis をもつとき, 慣習に従って " K/k は normal integral basis をもつ" ということにする.

Definition 1.1. ある $\mathfrak{p} \in \mathcal{P}_k - S$ が K/k において分岐するとき (i.e., $\mathfrak{p} \mathfrak{o}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, $e > 1$), $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は分岐拡大であると, ここでは仮に呼ぶことにする.

いくつか知られている事柄を述べる.

Lemma 1.1. 次は同値である.

- (i) S は K/k において *wildly ramified* するすべての \mathfrak{o}_k の prime ideals を含んでいる.
- (ii) $\mathfrak{o}_K(S)$ は *projective $\mathfrak{o}_k(S)[G]$ -module* である.

したがって, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ が normal basis をもつならば Lemma 1.1, (ii) が成り立ち, S は Lemma 1.1, (i) をみたす.

- Remark 1.1.** (i) S は Lemma 1.1, (i) をみたと仮定する. このとき, ある $U \subset \mathcal{P}_k$, $|U| < \infty$ が存在して, $\mathfrak{o}_K(U \cup S)/\mathfrak{o}_k(U \cup S)$ は normal basis をもつ ([4, Proposition 1.1]). これは鈴木浩志さんが注意された.
- (ii) $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ が normal basis をもち, $S \subset T$ ならば (tensor 積 $\mathfrak{o}_k(T) \otimes_{\mathfrak{o}_k(S)}$ をとると) $\mathfrak{o}_K(T)/\mathfrak{o}_k(T)$ も normal basis をもつ.

ここでは [4] の結果の一部の紹介をする. その目的は K/k が Abel 拡大のとき, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ が normal basis をもたないための十分条件を与えることにある (Theorem 2.2). その動機の 1 つは Remark 1.1, (i) を眺めていて, 次のような漠然とした疑問を抱いたことにあった: “ S は Lemma 1.1, (i) をみたと十分大きな集合であり, かつ $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は normal basis をもたない”, をみたと拡大 K/k と S は作れるのだろうか? 実際, Proposition 2.3, 2.4 により, 有限次 tamely ramified Abel 拡大 K/k が存在して, \mathfrak{o}_k の prime ideals からなる有限集合の真の増大列 $\{S_n\}_{n \geq 1}$ ($S_n \subsetneq S_{n+1}$) があり, 各 $n \geq 1$ について, $\mathfrak{o}_K(S_n)/\mathfrak{o}_k(S_n)$ は normal basis をもたないことがわかる.

なお, normal basis 問題についてもっと知りたい方は [5] をご参照ください.

2. RESULT

この Section では, k は総実代数体または CM -体であり, かつ k/\mathbb{Q} は Galois 拡大であると仮定する. 奇素数 l は $k \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$ をみとし, これを一つ固定する. ここで, ζ_l は 1 の原始 l 乗根である. \mathcal{P}_k の部分集合をいくつか定義する. $\mathfrak{p} \nmid l$ をみとす \mathfrak{o}_k の prime ideal \mathfrak{p} について, $e_{\mathfrak{p}}$ で \mathfrak{p} の k/\mathbb{Q} における分岐指数を, $a_{\mathfrak{p}}$ (resp. $b_{\mathfrak{p}}$) で $\mathfrak{p} \cap \mathbb{Z}$ の k/\mathbb{Q} (resp. $\mathbb{Q}(\zeta_l)/\mathbb{Q}$) における相対次数を表わす.

$$\mathcal{X}_l := \{ \mathfrak{p} \in \mathcal{P}_k ; 2 \mid e_{\mathfrak{p}} \text{ かつ } \text{ord}_2(b_{\mathfrak{p}}) = 0 \}.$$

k が総実代数体のときは,

$$\mathcal{G}_{1,l} := \{ \mathfrak{p} \mid \mathfrak{p} \nmid l \text{ かつ } \text{ord}_2(a_{\mathfrak{p}}) + 1 \leq \text{ord}_2(b_{\mathfrak{p}}) \},$$

k が CM -体のときは, $k^+ := k \cap \mathbb{R}$ とおき,

$$\mathcal{G}_{21,l} := \{ \mathfrak{p} \mid \mathfrak{p} \nmid l \text{ かつ } \mathfrak{p} \text{ は } k/k^+ \text{ において分岐するかつ } \text{ord}_2(a_{\mathfrak{p}}) + 1 \leq \text{ord}_2(b_{\mathfrak{p}}) \},$$

$$\mathcal{G}_{22,l} := \{ \mathfrak{p} \mid \mathfrak{p} \nmid l \text{ かつ } \mathfrak{p} \text{ は } k/k^+ \text{ において惰性するかつ } \text{ord}_2(a_{\mathfrak{p}}) = \text{ord}_2(b_{\mathfrak{p}}) \}.$$

そこで, k が総実代数体のとき (resp. CM -体のとき), $\mathcal{G}_l := \mathcal{G}_{1,l}$ (resp. $:= \mathcal{G}_{21,l} \cup \mathcal{G}_{22,l}$) とおく.

Proposition 2.1. 上の述べた仮定と記号の下で次のことが成り立つ.

- (i) $\mathfrak{p} \in \mathcal{G}_l$ とする. このとき, $\mathfrak{P} \mid \mathfrak{p}$ をみとす $\forall \mathfrak{P} \in \mathcal{P}_{k(\zeta_l)}$ について, \mathfrak{P} は $k(\zeta_l)/k(\zeta_l)^+$ において不分解である.

- (ii) k/\mathbb{Q} は Abel 拡大であるとし, k/\mathbb{Q} の判別式を d とする.
- (a) k が CM-体ならば $|\mathfrak{S}_\ell| = \infty$.
- (b) k が総実代数体のときは, “[$k : \mathbb{Q}$] は 2 ベキでなく, かつ $(d, \ell) = 1$ ”
または “ $\ell \equiv 1 \pmod{4}$ かつ $(d, \ell) = 1$ ” をみたすならば $|\mathfrak{S}_\ell| = \infty$.

PROOF. (i). \mathfrak{S}_ℓ の定義による.

(ii). Dirichlet の算術級数定理と Tchebotarev の密度定理を使う. \square

Theorem 2.2. 上の述べた仮定と記号の下で, $[k : \mathbb{Q}]$ は偶数であり, K/k を有限次 Abel 拡大とする. $\text{Gal}(K \cap \tilde{k}/k)$ は 2-group であると仮定し, $S \subset \mathfrak{S}_\ell$, $|S| < \infty$ とする. さらに, S に属さない \mathfrak{S}_ℓ の元 \mathfrak{p} が存在して, $\mathfrak{p} \nmid 2$ かつ $\ell \mid [K \cap k(\mathfrak{p}) : k]$ をみたすと仮定する. このとき, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は normal basis をもたない. ここで, \tilde{k} は k の Hilbert 類体, $k(\mathfrak{p})$ は k の mod \mathfrak{p} の the ray class field を表わす.

Remark 2.1. m を K/k の conductor とする. $\exists q \in \mathcal{P}_k - S$ s. t. $\text{ord}_q(m) \geq 2$ と仮定する. そのとき, q は K/k において wildly ramified であるから Lemma 1.1 より, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は normal basis をもたない. したがって, この仮定が成り立つときは, Theorem の主張は面白くない.

この証明の概略は Section 3 で述べるが, Theorem 2.2 より次の例を得る:

Proposition 2.3. p を奇素数, $k \subset K \subset \mathbb{Q}(\zeta_p)$, $[k : \mathbb{Q}]$ は偶数であるとする. そのとき, $\ell \mid [K : k]$ をみたす奇素数 ℓ が存在するならば, $\forall S \subset \mathfrak{S}_\ell$, $|S| < \infty$ に対して, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は normal basis をもたない. とくに, $S := \phi$ ととると, K/k は normal integral basis をもたない. また, k が総実かつ $[k : \mathbb{Q}]$ は 2 ベキのときには $\ell \equiv 1 \pmod{4}$ ととれるならば, Proposition 2.1, (ii) により \mathfrak{S}_ℓ は常に無限集合である.

PROOF. Theorem 2.2 の仮定にある \mathfrak{p} として, \mathfrak{p} の上にある唯一つの \mathfrak{o}_k の prime ideal をとればよい. \square

Proposition 2.4. k を $[\tilde{k} : k]$ が 2 ベキである 2 次体, \mathfrak{p} を k/\mathbb{Q} において分岐する \mathfrak{o}_k の prime ideal とする. $\ell \mid ((N\mathfrak{p} - 1)/w_{\mathfrak{p}})$ をみたす奇素数 ℓ が存在すると仮定する. ここで, $w_{\mathfrak{p}} := |(\mathfrak{o}_k^\times + \mathfrak{p})/\mathfrak{p}|$. このとき, $\forall S \subset \mathfrak{S}_\ell$, $|S| < \infty$ に対して, $\mathfrak{o}_{k(\mathfrak{p})}(S)/\mathfrak{o}_k(S)$ は normal basis をもたない. とくに, $S := \phi$ ととると, $k(\mathfrak{p})/k$ は normal integral basis をもたない. また, k が実 2 次体のときには, ℓ は k/\mathbb{Q} の判別式と素であり, かつ $\ell \equiv 1 \pmod{4}$ ととれるならば, Proposition 2.1, (ii) により \mathfrak{S}_ℓ は常に無限集合である.

Proposition 2.4 と関連する Gómez Ayala と Schertz [2] の結果を紹介しておく. 重複するかもしれないが, 少し記号を導入する. F を任意の有限次代数体とし, m を

\mathfrak{o}_F の ideal とする. $F(\mathfrak{m})$ で F の mod \mathfrak{m} の the ray class field を表わし, $w_{\mathfrak{m}}$ を $(\mathfrak{o}_F/\mathfrak{m})^\times$ の部分群 $(\mathfrak{o}_F^\times + \mathfrak{m})/\mathfrak{m}$ の位数とすると,

$$[F(\mathfrak{m}) : F] = h_F \frac{\varphi(\mathfrak{m})}{w_{\mathfrak{m}}},$$

ここで, φ は Euler 関数であり, h_F は F の類数である. F の ideal 群

$$H_F := \{ (\alpha)\mathfrak{o}_F \mid \alpha \in F^\times, \alpha \equiv 1 \pmod{4} \}$$

を使う. 彼らが出発点としたのは次の命題である (このような形で明記はされていない).

Proposition 2.5. k を有限次代数体とし, K/k は 2 次拡大とする. K/k において分岐する \mathfrak{o}_k のすべての prime ideals を $\mathfrak{p}_1, \dots, \mathfrak{p}_u$ ($u \geq 0$) で表わす. このとき,

K/k は normal integral basis をもつ.

$$\iff \exists d \in \mathfrak{o}_k \text{ s. t. } K = k(\sqrt{d}), \quad d \equiv 1 \pmod{4}, \quad (d)\mathfrak{o}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_u.$$

さらにこれが成り立つとき, $\frac{1+\sqrt{d}}{2}$ は K/k の normal integral basis の生成元になる.

これを使って次の結果を示している:

Proposition 2.6. $F := \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$, $m < 0$, m は square-free とする.

(i) ([2, Satz 1]) $m = -2, -11, -19, -43, -67, -163$ のとき (したがって, $h_F = 1$, $\mathfrak{o}_F^\times = \{\pm 1\}$),

$$(2.1) \quad \mathfrak{p} \nmid 2, \quad 2 \mid ((N\mathfrak{p} - 1)/2), \quad \mathfrak{p} \notin H_F$$

をみたす \mathfrak{o}_F の prime ideals \mathfrak{p} は無限個あり, この \mathfrak{p} について, $F(\mathfrak{p})/F$ は normal integral basis をもたない.

(ii) ([2, Satz 2]) $m = -2, -11$ のとき,

$$\mathfrak{p} \nmid 6, \quad \mathfrak{p}\mathfrak{o}_{F(3)} \notin H_{F(3)}$$

をみたす \mathfrak{o}_F の prime ideals \mathfrak{p} は無限個あり, この \mathfrak{p} について, $F(3\mathfrak{p})/F(3)$ は normal integral basis をもたない.

Remark 2.2. $m = -11, -19, -43, -67, -163$ とする. そのとき, F/\mathbb{Q} において分岐する \mathfrak{o}_F の prime ideal \mathfrak{p} (i.e., $\mathfrak{p} \mid m$) に対して, 各 m について各々 $\ell = 5, 3, 3$ (または 7), 3 (または 11), 3 が Proposition 2.4 の仮定をみたすから, $F(\mathfrak{p})/F$ は normal integral basis をもたない. そして, この \mathfrak{p} は (2.1) の真ん中の条件をみたさないので, Proposition 2.4 と Proposition 2.6, (i) の主張は独立である.

3. OUTLINE OF PROOF

Lemma 1.1 より, S は条件 Lemma 1.1, (i) をみたと仮定してよい. $L := K \cap k(\mathfrak{p})$ とおく. $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は normal basis をもつと仮定する. したがって, $\mathfrak{o}_L(S)/\mathfrak{o}_k(S)$ も normal basis をもつ. S の外で仮定された tameness より, $\mathrm{Tr}_{L/k}(\alpha) = 1$ をみたとす $\mathfrak{o}_L(S)/\mathfrak{o}_k(S)$ の normal basis の生成元 α をとることができる. $\ell \mid [L:k]$ より, 位数 ℓ の $\mathrm{Gal}(L/k)$ の指標 χ が存在する. そこで, k_χ を $\mathrm{Ker} \chi$ の L/k における固定体とすると, k_χ/k は ℓ 次巡回拡大である. そのとき, \mathfrak{p} は k_χ/k において分岐する. もしそうでないならば, $L \subset k(\mathfrak{p})$ により k_χ/k において分岐する可能性のある素点は \mathfrak{p} のみだから, $k_\chi \subset \tilde{k}$ を得る. これは $\mathrm{Gal}(K \cap \tilde{k}/k)$ が 2-group であることに反するからである. また, $k_\chi \subset k(\mathfrak{p})$ より, さらに \mathfrak{p} は k_χ/k において tamely ramified である. \mathfrak{p} は k_χ/k において完全分岐することを使うと, α の resolvent の素因子分解は次のようになる:

$$(3.1) \quad (\langle \alpha, \chi \rangle)^\ell \mathfrak{o}_{k(\zeta_\ell)}(S) = \mathfrak{P}^\theta,$$

ここで, \mathfrak{P} は \mathfrak{p} の上の $\mathfrak{o}_{k(\zeta_\ell)}$ のある prime ideal, θ は Stickelberger element (仮定: $k \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$ より, $\mathrm{Gal}(k(\zeta_\ell)/k) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ であるから, $\theta \in \mathbb{Z}[\mathrm{Gal}(k(\zeta_\ell)/k)]$ とみれる) であり, $\langle \alpha, \chi \rangle := \sum_{s \in \mathrm{Gal}(L/k)} \chi(s^{-1}) \alpha^s$ とおく. (3.1) の右辺は Stickelberger の定理が主張する Gauss 和の素因子分解と似ているので, α の resolvent から決まる $k(\zeta_\ell)$ のある元と Jacobi 和たちのある積との間の関係式を得る. この関係式から Brinkhuis [1, Theorem 2] のテクニックを使うと矛盾を導くことができる (したがって, Theorem 2.2 は Brinkhuis の定理の 1 つの一般化とみなせる; まだ使っていない仮定 “[$k : \mathbb{Q}$] は偶数である, $\mathfrak{p} \in T_\ell$, $\mathfrak{p} \nmid 2$ ” をこのとき使う). その際, 次の単数に関する事実を本質的に使う: $\forall \varepsilon \in \mathfrak{o}_{k(\zeta_\ell)}(S)^\times$ について, $\varepsilon/\bar{\varepsilon}$ は 1 のべき根になる. ここで, $\bar{\varepsilon}$ は ε の複素共役であり, このことは CM -体の単数に関するよく知られた事実の S -単数への拡張になっている.

PROOF. $F := k(\zeta_\ell)$ とおく. W_F を F 中の 1 のべき根全体, \tilde{S} を S 上にある \mathfrak{o}_F の prime ideals 全体からなる有限集合, \tilde{S}_∞ を F の無限素点全体とし, $T := \tilde{S} \cup \tilde{S}_\infty$, $t := |T|$ とおく. Dirichlet の単数定理により, 群準同型写像

$$f: \mathfrak{o}_F(S)^\times \longrightarrow \mathbb{R}^t, \quad u \longmapsto (\log |u|_q)_{q \in T}$$

の像で生成される部分空間は $(t-1)$ 次元であり, $\mathrm{Ker} f = W_F$ である. k は総実代数体または CM -体であるから, F は CM -体になる. さらに, Proposition 2.1, (i) より複素共役は \tilde{S} に trivially に作用している. したがって, $\bar{\varepsilon} \in \mathfrak{o}_F(S)^\times$. $\therefore \varepsilon/\bar{\varepsilon} \in \mathfrak{o}_F(S)^\times$. また, $|\varepsilon/\bar{\varepsilon}|_q = 1 \quad (\forall q \in \tilde{S}), \quad |\varepsilon/\bar{\varepsilon}|_q = 1 \quad (\forall q \in \tilde{S}_\infty)$. ゆえに, $\varepsilon/\bar{\varepsilon} \in \mathrm{Ker} f = W_F$ を得る. \square

REFERENCES

1. J. Brinkhuis, *Galois modules and embedding problems*, J. Reine Angew. Math. **346** (1984), 141–165.
2. E. J. Gómez Ayala and R. Schertz, *Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Number Theory **44** (1993), 41–46.
3. F. Kawamoto and K. Komatsu, *Normal bases and \mathbb{Z}_p -extensions*, J. Algebra **163** (1994), 335–347.
4. F. Kawamoto, *On normal bases of some ring extensions in number fields I*, to appear in Tokyo J. Math..
5. ———, *S -整数環のアーベル拡大の normal basis について*, 数理解析研究所講究録 “群スキームの変形と整数論への応用”.