

S -整数環のアーベル拡大の normal basis について

学習院大学理学部 河本 史紀 (Fuminori Kawamoto)

CONTENTS

1. 問題と基礎事実	1
2. $S = \phi$ の場合	5
2.1. $k = \mathbb{Q}$ の場合 (Taylor の定理)	
2.2. $k \neq \mathbb{Q}$ かつ不分岐拡大の場合	
2.3. $k \neq \mathbb{Q}$ かつ分岐拡大の場合	
3. $S = \{p\}$ の場合	9
3.1. Kersten and Michaliček の定理	
3.2. Modular construction	
4. あとがき	10
5. おまけ	11
I. $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ の normal basis に関する論文	12
II. 関数体へのアナロジー	14
III. 成書と参考図書	14

1. 問題と基礎事実

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 (これらの記号は以後この意味で使う). 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. $S \subset \mathcal{P}_k$ は K/k において wildly ramified するすべての prime ideals を含んでいると仮定する. ここで, $\mathfrak{p} \in \mathcal{P}_k$ が K/k において wildly ramified するとは, e を $\mathfrak{p}$ の K/k における分岐指数とするとき (i.e., $\mathfrak{p}\mathfrak{o}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$), 剰余体 $\mathfrak{o}_k/\mathfrak{p}$ の標数は e を割ることで定義する. そうでないとき, $\mathfrak{p}$ は K/k において tamely ramified するという. 有限次拡大 N/k について, 今と同じように $\mathcal{P}_N$ 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 $M := \mathfrak{o}_k - \bigcup_{\mathfrak{p} \in \mathcal{P}_k - S} \mathfrak{p}$ 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). Dedekind 環の特徴付けの一つである “任意の 0 でない分数 ideal は可逆である” を (例えば) 考慮すれば, Dedekind 環の分数環は Dedekind 環である. したがって, $\mathfrak{o}_N(S)$ は Dedekind 環である. $\mathfrak{o}_N(S)$ 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.

$\mathfrak{o}_K(S)$ 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。

Definition 1.1. $\forall \mathfrak{p} \in \mathcal{P}_k - S$ に対して、 $\mathfrak{p}$ は K/k において不分岐であるとき (i.e., $\mathfrak{p}\mathfrak{o}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_g$), $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は不分岐拡大であると、ここでは仮に呼ぶことにする。そうでないとき、 $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は分岐拡大であるという。

Example 1.1. K/k が tamely ramified のとき、 $S := \phi$ 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。

Example 1.2. p を素数とする。 S として p の上にある $\mathfrak{o}_k$ の prime ideals 全体からなる有限集合をとると、 $\mathfrak{o}_K(S) = \mathfrak{o}_K[p^{-1}]$, $\mathfrak{o}_k(S) = \mathfrak{o}_k[p^{-1}]$ が成り立つ。

次の問題を考える:

Normal Basis 問題. $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ はいつ normal basis をもつか? もしもつならば normal basis の生成元を決めよ。

答えは当然ながら、Galois 群 G の構造と拡大 K/k および基礎体 k の数論的性質が関わってくるのだから、それを見極めるところに問題の面白さがある。現在あるアプローチのしかたは大まかに次のものがあると思う:

- (A) Fröhlich による “Hom-description” を使う ([Fr2]).
- (B) Brinkhuis による normal basis の存在条件付き埋め込み問題として扱う ([B3]). さらに彼による群環の torsion 元を用いる手法もある。
- (C) 環の Galois 拡大の理論を使う (Childs, Kersten, Michaliček, Greither 等の方法)。

ここではこの問題に関する結果の紹介をするが、次の点に留意された方がよい。

- (1) 数論の問題によくありがちなように、拡大次数 $[K : k]$ の偶奇によって問題の答えが質的に違ってくる。
- (2) この問題を解く最終段階では、 $[K : k]$ の素因子のあるべきを法として、単数の存在を調べる。そしてこれはとても難しい問いになることが多い。

normal basis 問題を考えるとき、 K/k の分岐に関する情報をまず考慮しなければならない (Theorem 1.3; 適当な文献を見つけられなかったので、この証明を書くことにしました)。

Lemma 1.1. A を Dedekind 環とし、その商体を L とする。 M/L を Galois 群 Γ をもつ有限次 Galois 拡大とし、 B を A の M における整閉包とする。このとき、次はすべて同値である。

- (i) B は A 上 tamely ramified である。
- (ii) $\text{Tr}_{M/L}(B) = A$, つまり $1 \in \text{Tr}_{M/L}(B)$ 。
- (iii) B は projective $A\Gamma$ -module である (ここで、 $A\Gamma$ は Γ の A 上の群環を表わす)。

PROOF. [CR, vol. I, p. 101, Exercise 4.13, 15] または [L, Ch. 9, Theorem 1.2]. $\square$

Proposition 1.2. $\mathfrak{p} \in \mathcal{P}_k$ とし, $\mathfrak{p}$ の上にある $\mathfrak{o}_K$ の *prime ideal* $\mathfrak{P}$ を 1 つとる. H を $\mathfrak{P}$ の K/k における分解群とする. K から $\mathfrak{P}$ による K の完備化 $K_{\mathfrak{P}}$ の中への k -同型を 1 つ固定し, $K \subset K_{\mathfrak{P}}$ とみなし, H を $\text{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ と同一視する. F を k の部分体とし, $P := \mathfrak{p} \cap F$ とおく. このとき, 次はすべて同値である.

- (i) $\mathfrak{o}_{K_{\mathfrak{P}}}$ は $\mathfrak{o}_{k_{\mathfrak{p}}}H$ -projective (ここで, $\mathfrak{o}_{k_{\mathfrak{p}}}$ は $k_{\mathfrak{p}}$ の付値環を表わす).
- (ii) $\mathfrak{o}_{K_{\mathfrak{P}}}$ は $\mathfrak{o}_{k_{\mathfrak{p}}}H$ -free. つまり, $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ は *normal integral basis* をもつ.
- (iii) $\mathfrak{o}_{K_{\mathfrak{P}}}$ は $\mathfrak{o}_{F_P}H$ -free.
- (iv) $\mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$ は $\mathfrak{o}_{F_P}G$ -free (作用は $(a \otimes x)^\lambda := \sum_{s \in G} a_s a \otimes x^s$ ($a \otimes x \in \mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$, $\lambda = \sum_{s \in G} a_s s \in \mathfrak{o}_{F_P}G$) により定義する).

PROOF. (i) $\Rightarrow$ (ii). [CR, Theorem 32.1] による. これは E. Noether (1932) によって述べられ, Swan (1960) により証明された. 今の設定における直接的かつ単純な証明は [Ka3] にある.

(ii) $\Rightarrow$ (iii). $m := [k_{\mathfrak{p}} : F_P]$ とおく. $\mathfrak{o}_{k_{\mathfrak{p}}}$ は $\mathfrak{o}_{F_P}$ -free であるから, $\mathfrak{o}_{F_P}H$ -module としての自然な同型 $\mathfrak{o}_{k_{\mathfrak{p}}}H \cong (\mathfrak{o}_{F_P}H)^{(m)}$ (m 個の $\mathfrak{o}_{F_P}H$ の直和) があることからわかる.

(iii) $\Rightarrow$ (iv) $\Rightarrow$ (i) を示すために Galois algebra の言葉を使う (cf. [Fr2, Theorem 3 of Ch. I, Proposition 2.1 of Ch. III]).

Δ を $H \setminus G$ の完全代表系とし, $1 \in \Delta$ とする. K/k は Galois 拡大だから各 $\delta \in \Delta$ は K から $k_{\mathfrak{p}}$ の代数的閉包の完備化 $\bar{k}_{\mathfrak{p}}$ の中へのすべての k -同型をひきおこし, その像の $\bar{k}_{\mathfrak{p}}$ における閉包は $K_{\mathfrak{P}}$ と一致する. よって, $\forall \delta \in \Delta$ について, $k_{\mathfrak{p}}$ -algebra としての全射準同型 $1 \otimes \delta: k_{\mathfrak{p}} \otimes_k K \rightarrow K_{\mathfrak{P}}$, $a \otimes x \mapsto ax$ がある. 積写像をとると $k_{\mathfrak{p}}$ -algebra としての同型 $\varphi_1 := \prod_{\delta \in \Delta} (1 \otimes \delta): k_{\mathfrak{p}} \otimes_k K \cong \prod_{\delta \in \Delta} K_{\mathfrak{P}}$ を得る. ここで, $\prod_{\delta \in \Delta} K_{\mathfrak{P}}$ は Δ により index 付けられた $|\Delta|$ 個の $K_{\mathfrak{P}}$ の直積集合であり, 積位相が入った $k_{\mathfrak{p}}$ 上の位相線型空間である. $\prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}$ を Δ により index 付けられた $|\Delta|$ 個の $\mathfrak{o}_{K_{\mathfrak{P}}}$ の直積集合とすると, これは $\prod_{\delta \in \Delta} K_{\mathfrak{P}}$ の閉部分集合である. $\prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}$ の部分集合 $\varphi_1(\mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K)$ は $\prod_{\delta \in \Delta} K_{\mathfrak{P}}$ の free $\mathfrak{o}_{k_{\mathfrak{p}}}$ -submodule だから, これも $\prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}$ の閉部分集合である. 近似定理より, $\varphi_1(\mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K)$ の部分集合 $\varphi_1(\mathfrak{o}_K)$ は $\prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}$ の中で dense である. したがって, φ_1 は $\mathfrak{o}_{k_{\mathfrak{p}}}$ -algebra としての同型

$$\varphi_1: \mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K \cong \prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}, \quad a \otimes x \mapsto (ax^\delta)_{\delta \in \Delta}$$

をひきおこす. $\mathfrak{o}_{K_{\mathfrak{P}}}$ は $\mathfrak{o}_{k_{\mathfrak{p}}}H$ -module であり, 左乗積 (hg , $h \in H$, $g \in G$) により H は G に作用する. そこで,

$$\text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{P}}}) := \{ f: G \rightarrow \mathfrak{o}_{K_{\mathfrak{P}}} \text{ (map)} \mid f(g)^h = f(hg) \ (\forall h \in H, \forall g \in G) \}$$

とおく. これは pointwise multiplication により $\mathfrak{o}_{k_{\mathfrak{p}}}$ -algebra である. $\forall f \in \text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{P}}})$, $\forall \sigma \in G$ について,

$$f^\sigma(g) := f(g\sigma), \quad \forall g \in G$$

と定義すると, G は $\mathfrak{o}_{k_{\mathfrak{p}}}$ -algebra $\text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{P}}})$ に作用することがわかる.

$$\varphi_2: \text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{P}}}) \rightarrow \prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}, \quad f \mapsto (f(\delta))_{\delta \in \Delta}$$

は $\mathfrak{o}_{k_{\mathfrak{p}}}$ -algebra としての同型となる. 全射性を示すには $(\alpha_\delta)_{\delta \in \Delta} \in \prod_{\delta \in \Delta} \mathfrak{o}_{K_{\mathfrak{P}}}$ に対して, $g \in G$ を $g = h\delta$ ($h \in H$, $\delta \in \Delta$) とかき, $f(g) := \alpha_\delta^h$ とおけば, $f \in \text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{P}}})$ となる. $\Phi_1 := \varphi_2^{-1} \circ \varphi_1$ とおくと Φ_1 は G の作用を保つ (つ

まり, $a \otimes x \in \mathfrak{o}_{k_p} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$, $\sigma \in G$ について, $\Phi_1(a \otimes x^\sigma) = \Phi_1(a \otimes x)^\sigma$. ゆえに, $\mathfrak{o}_{k_p} G$ -module としての同型

$$\Phi_1 : \mathfrak{o}_{k_p} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K \cong \text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{p}}})$$

を得る. $\mathfrak{o}_{K_{\mathfrak{p}}}$ を左 $\mathfrak{o}_{F_P} H$ -module とみて, $\mathfrak{o}_{F_P} G$ を両側 $(\mathfrak{o}_{F_P} G, \mathfrak{o}_{F_P} H)$ -module とみることにし, tensor 積 $\mathfrak{o}_{F_P} G \otimes_{\mathfrak{o}_{F_P} H} \mathfrak{o}_{K_{\mathfrak{p}}}$ を定義する. $x \cdot (y \otimes \alpha) = xy \otimes \alpha$ ($x \in \mathfrak{o}_{F_P} G$, $y \otimes \alpha \in \mathfrak{o}_{F_P} G \otimes_{\mathfrak{o}_{F_P} H} \mathfrak{o}_{K_{\mathfrak{p}}}$) により, $\mathfrak{o}_{F_P} G \otimes_{\mathfrak{o}_{F_P} H} \mathfrak{o}_{K_{\mathfrak{p}}}$ は左 $\mathfrak{o}_{F_P} G$ -module となる.

$$\varphi_3 : \text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{p}}}) \longrightarrow \mathfrak{o}_{F_P} G \otimes_{\mathfrak{o}_{F_P} H} \mathfrak{o}_{K_{\mathfrak{p}}}, \quad f \longmapsto \sum_{\delta \in \Delta} \delta^{-1} \otimes f(\delta)$$

は $\mathfrak{o}_{F_P} G$ -module としての同型になる ($\{\delta^{-1}\}_{\delta \in \Delta}$ は G/H の完全代表系になることから, $x \in \mathfrak{o}_{F_P} G \otimes_{\mathfrak{o}_{F_P} H} \mathfrak{o}_{K_{\mathfrak{p}}}$ に対して, $x = \sum_{\delta \in \Delta} \delta^{-1} \otimes \alpha_\delta$, $\alpha_\delta \in \mathfrak{o}_{K_{\mathfrak{p}}}$ と一意にかけることを使う). また, φ_3 は $H \setminus G$ の完全代表系 Δ のとり方によらないこともわかる. したがって, $\mathfrak{o}_{F_P} G$ -module としての同型

$$\Phi_2 := \varphi_3 \circ \Phi_1 : \mathfrak{o}_{k_p} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K \cong \mathfrak{o}_{F_P} G \otimes_{\mathfrak{o}_{F_P} H} \mathfrak{o}_{K_{\mathfrak{p}}}$$

を得る.

(iii) $\Rightarrow$ (iv). $\mathfrak{o}_{F_P} G$ -module としての同型 Φ_2 を使えばよい.

(iv) $\Rightarrow$ (i). $\mathfrak{o}_{F_P} G$ -module としての同型 Φ_1 を使うと, $\text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{p}}})$ は $\mathfrak{o}_{F_P} G$ -free である. $m := [k_p : F_P]$ とおくと, その $\mathfrak{o}_{F_P} G$ -free basis $\{f_1, \dots, f_m\}$ がとれる. よって, $1 = \sum_{i=1}^m f_i^{\lambda_i}$, $\lambda_i \in \mathfrak{o}_{F_P} G$ ($1 \leq i \leq m$) と一意にかけられる. $g \in G$ について, $1 = 1^g = \sum_{i=1}^m f_i^{g\lambda_i}$. したがって, $\lambda_i = g\lambda_i$ ($\forall g \in G$). よって, $N := \sum_{g \in G} g$ とおくと, $\exists a_i \in \mathfrak{o}_{F_P}$ s. t. $\lambda_i = a_i N$. ゆえに, $F := \sum_{i=1}^m a_i f_i \in \text{Map}_H(G, \mathfrak{o}_{K_{\mathfrak{p}}})$ とすると, $1 = F^N$ を得る. よって,

$$1 = F^N(1) = \sum_{g \in G} F(g) = \sum_{\delta \in \Delta} \sum_{h \in H} F(h\delta) = \sum_{\delta \in \Delta} \sum_{h \in H} F(\delta)^h.$$

したがって, ある $\delta \in \Delta$ について, $\sum_{h \in H} F(\delta)^h = \text{Tr}_{K_{\mathfrak{p}}/k_p}(F(\delta)) \in \mathfrak{o}_{k_p}^\times$.

$\therefore \text{Tr}_{K_{\mathfrak{p}}/k_p}(\mathfrak{o}_{K_{\mathfrak{p}}}) = \mathfrak{o}_{k_p}$. Lemma 1.1, (ii) $\Rightarrow$ (iii) より, $\mathfrak{o}_{K_{\mathfrak{p}}}$ は $\mathfrak{o}_{k_p} H$ -projective である. $\square$

Definition 1.2. R を Dedekind 環, G を有限群とし, $\Lambda := RG$ とおく. M を Λ -lattice, すなわち, 有限生成 Λ -module かつ R -projective (これは R が Dedekind 環だから R -torsion free を意味する) とする. R の 0 でない prime ideal 全体を $\mathcal{P}_R$ で表わし, $P \in \mathcal{P}_R$ に対して, R_P で R の P による完備化とし, $M_P := R_P \otimes_R M$ とおく ($\Lambda_P \cong R_P G$). このとき, M は rank n の locally free Λ -module であるとは, $M_P \cong (\Lambda_P)^{(n)}$ ($\forall P \in \mathcal{P}_R$) が成り立つことで定義する. ここで, $(\Lambda_P)^{(n)}$ は n 個の Λ_P の直和である.

Theorem 1.3. $S \subset \mathcal{P}_k$ とする. F を k の部分体とし, $S_0 := \{ \mathfrak{p} \cap F \mid \mathfrak{p} \in S \}$ とおき, 先と同じように $\mathfrak{o}_F(S_0)$ を定義する. S は S_0 の上にある $\mathfrak{o}_k$ の prime ideal 全体の集合と一致すると仮定する (つまり, $\mathfrak{o}_F(S_0) \subset \mathfrak{o}_k(S)$ が成り立つ). したがって, $\mathfrak{o}_K(S)$ は $\mathfrak{o}_F(S_0)[G]$ -module となる. このとき, 次はすべて同値である.

- (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) $\text{Tr}_{K/k}(\mathfrak{o}_K(S)) = \mathfrak{o}_k(S)$.

- (iii) $\mathfrak{o}_K(S)$ は *projective* $\mathfrak{o}_k(S)[G]$ -module である.
- (iv) $\mathfrak{o}_K(S)$ は *rank* $[k : F]$ の *locally free* $\mathfrak{o}_F(S_0)[G]$ -module である.

PROOF. (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii). Lemma 1.1 による.

(i) $\Rightarrow$ (iv). まず, 次のことに注意する.

- (i) $\Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}_k - S : \mathfrak{p}$ は K/k において tamely ramified する.
- $\Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}_k - S \ \forall \mathfrak{P} \in \mathcal{P}_K : \mathfrak{P} \mid \mathfrak{p}$ かつ $\mathfrak{p}$ は $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ において tamely ramified する.
- $\Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}_k - S \ \forall \mathfrak{P} \in \mathcal{P}_K : \mathfrak{P} \mid \mathfrak{p}$ かつ $\mathfrak{o}_{K_{\mathfrak{P}}}$ は $\mathfrak{o}_{k_{\mathfrak{p}}}[Gal(K_{\mathfrak{P}}/k_{\mathfrak{p}})]$ -projective である. ($\because$ Lemma 1.1, (i) $\Leftrightarrow$ (iii))
- $\Leftrightarrow \forall P \in \mathcal{P}_F - S_0 \ \forall \mathfrak{p} \in \mathcal{P}_k : \mathfrak{p} \mid P$ かつ $\mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$ は $\mathfrak{o}_{F_P} G$ -free である. ($\because S_0$ に関する仮定と Proposition 1.2, (i) $\Leftrightarrow$ (iv))

$M := \mathfrak{o}_F - \bigcup_{P \in \mathcal{P}_F - S_0} P$ とおくと S_0 に関する仮定から, $\mathfrak{o}_F(S_0) = M^{-1} \mathfrak{o}_F$, $\mathfrak{o}_K(S) = M^{-1} \mathfrak{o}_K$ が成り立つ. $P \in \mathcal{P}_F - S_0$ とする. そのとき, $\mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F} \mathfrak{o}_F(S_0) = \mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F} \mathfrak{o}_F = \mathfrak{o}_{F_P}$ より, $\mathfrak{o}_F(S_0)$ の P による完備化は $\mathfrak{o}_{F_P}$ になる. したがって,

$$\begin{aligned} \mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F(S_0)} \mathfrak{o}_K(S) &= (\mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F} \mathfrak{o}_F(S_0)) \otimes_{\mathfrak{o}_F(S_0)} \mathfrak{o}_K(S) = \mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F} \mathfrak{o}_K(S) \\ &= \mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F} \mathfrak{o}_K = (\mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F} \mathfrak{o}_k) \otimes_{\mathfrak{o}_k} \mathfrak{o}_K \\ &= (\bigoplus_{\mathfrak{p} \mid P} \mathfrak{o}_{k_{\mathfrak{p}}}) \otimes_{\mathfrak{o}_k} \mathfrak{o}_K = \bigoplus_{\mathfrak{p} \mid P} (\mathfrak{o}_{k_{\mathfrak{p}}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K). \end{aligned}$$

これらのことと仮定より, $\mathfrak{o}_{F_P} \otimes_{\mathfrak{o}_F(S_0)} \mathfrak{o}_K(S)$ は $\mathfrak{o}_{F_P} G$ -free である. よって, $\mathfrak{o}_K(S)$ は $\mathfrak{o}_F(S_0)[G]$ -locally free である.

(iv) $\Rightarrow$ (iii). 仮定と [CR, (31.3), (ii)] より, $\mathfrak{o}_K(S)$ は *projective* $\mathfrak{o}_F(S_0)[G]$ -module である. よって, (tensor 積 $\mathfrak{o}_k(S) \otimes_{\mathfrak{o}_F(S_0)}$ をとることにより) $\mathfrak{o}_K(S)$ は $\mathfrak{o}_k(S)[G]$ -projective となる. $\square$

Remark 1.1. K/k を有限次 Abel 拡大とし, m で K/k の conductor を表わす. そのとき類体論より, Theorem 1.3, (i) は $\text{ord}_{\mathfrak{p}}(m) \geq 2$ をみたす $\mathfrak{p} \in \mathcal{P}_k$ はすべて S の元であることを意味する ([Iw, Lemma 7.14]).

したがって, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ が normal basis をもつならば Theorem 1.3, (iii) が成り立ち, よって他のすべての条件も成り立つ. それで, S は (i) をみたすと始めに仮定しておいたのである. また, $F = k$ ととり, Proposition 1.2, (iv) を用いると, 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 をもつことが示せる ([Ka6, Proposition 1.1]). これは鈴木浩志さんが注意された.

Remark 1.2. 簡単なことだが次の注意をする. $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ 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.

2. $S = \phi$ の場合

この Section において, K/k は tamely ramified であると仮定する (cf. Example 1.1). よって, Theorem 1.3 より, $\mathfrak{o}_K$ は rank 1 の locally free $\mathfrak{o}_k G$ -module である. さらに, $F = \mathbb{Q}$, $S = \phi$ として Theorem 1.3, (iv) を使うと, $\mathfrak{o}_K$ は rank $[k : \mathbb{Q}]$ の locally free $\mathbb{Z}G$ -module でもある.

2.1. $k = \mathbb{Q}$ の場合 (Taylor の定理). R をその商体 F が有限次代数体である Dedekind 環とし, G を有限群とする (したがって, FG は半単純環である). locally free RG -modules 全体の作る圏と Grothendieck 群を各々 $\mathcal{C}$, $K_0(RG)$ で表わす. $K_0(RG)$ の元は $[X] - [RG^{(n)}]$ ($X \in \mathcal{C}$, $n \geq 0$) の形にかかる (RG -locally free ならば RG -projective である). [CR, (31.14)] より, $M \in \mathcal{C}$ に対して, RG の locally free 左 ideal $I \in \mathcal{C}$ があって,

$$(2.1) \quad M \cong RG^{(m-1)} \oplus I, \quad m := \text{rank } M$$

とかける. $K_0(RG) \rightarrow \mathbb{N}$, $[Y] \mapsto \text{rank } Y$ から群準同型写像 $K_0(RG) \rightarrow \mathbb{Z}$ が定義される. この kernel を RG の locally free class group と呼び, $\text{Cl}(RG)$ で表わす. よって, $\text{Cl}(RG)$ の元は $[M] - [RG^{(m)}]$ の形であり, (2.1) より, これは $[I] - [RG]$ に等しい (cf. [CR, (39.12)]). それで, $\{[I] \in K_0(RG) \mid I \text{ は } RG \text{ の locally free 左 ideal}\}$ により, $\text{Cl}(RG)$ を定義する場合もある ([CR, §49]). $\text{Cl}(RG)$ は Jordan-Zassenhaus の定理より有限 Abel 群になる ([CR, (39.13)]). ところで, $[M] - [RG^{(m)}] = 0 \iff M$ と $RG^{(m)}$ は RG -stably isomorphic (M は RG -stably free であるという), i.e., $M \oplus RG^{(k)} \cong RG^{(m+k)}$ ($\exists k \geq 0$). これは $M \oplus RG$ が RG -free になることと同値である ([CR, (41.20)]).

FG が Eichler 条件 ([CR, §51A]) をみたすとき, RG -stably free と RG -free は同意語になる ([CR, (49.29), (51.24)]). G は奇数位数または Abel 群ならば FG は Eichler 条件をみたす ([CR, (51.2), (51.3)]).

Fröhlich は $\text{Cl}(RG)$ を “Hom-description” の言葉で表現することにより扱いやすいものになっている ([Fr2, Ch. I, Theorem 1], [CR, (52.11)], [T4, Ch. 1, Theorem 3.5], [Sn1, 4.2.28]).

G の各複素既約指標 χ に対して, 拡張された Artin L -関数 $\Lambda(s, \chi)$ が定義され, それは $\mathbb{C}$ 上の有理型関数であり, 関数等式 $\Lambda(s, \chi) = W(\chi) \Lambda(1-s, \bar{\chi})$ をみたす. $W(\chi)$ は χ の Artin root number と呼ばれ, symplectic 既約指標 χ (つまり, その値は実数であるが, その対応する表現は $\mathbb{R}$ 上実現可能でない既約指標のこと ([Se, p. 131])) に対しては $W(\chi)$ の値は ± 1 をとる. この $W(\chi)$ たちと Hom-description を使って, Cassou-Noguès は $\text{Cl}(\mathbb{Z}G)$ の元 $t(W)$ を定義した. その定義より $2 \cdot t(W) = 0$ をみたす. Taylor は次のことを示した:

Theorem 2.1. ([T1, Theorem 1]) K/k を Galois 群 G をもつ有限次 tamely ramified Galois 拡大とし, $m := [k : \mathbb{Q}]$ とおく.

- (i) $[o_K] - [\mathbb{Z}G^{(m)}] = t(W)$ が成り立つ. とくに, $[o_K \oplus o_K] = [\mathbb{Z}G^{(2m)}]$ となり, $o_K \oplus o_K$ は $\mathbb{Z}G$ -stably free である. また, $[o_K] = [\mathbb{Z}G^{(m)}]$ となるための障害は G の symplectic 既約指標の Artin root number たちの符号のみであることがわかる.
- (ii) G は奇数位数または Abel 群ならば o_K は free $\mathbb{Z}G$ -module である. とくに, このとき, $k = \mathbb{Q}$ ととると, K/k は normal integral basis をもつ.

PROOF. (ii). G の仮定より, G は symplectic 既約指標をもたないので ([Se, p. 133, 練習問題 1]), $t(W) = 0$ である. よって, o_K は $\mathbb{Z}G$ -stably free である. さらに, $\mathbb{Q}G$ は Eichler 条件をみたすので, o_K は $\mathbb{Z}G$ -free となる. $\square$

Remark 2.1. (ii) は古典的結果 Hilbert-Speiser の定理 ([L, Ch. 9, Theorem 3.4], [CT, Ch. I, Theorem 3.8]) を含んでいる.

Taylor の定理の解説として, 整数表現の専門家である宮田武彦氏の論説 “整数環のガロワ加群としての構造” がある. 私はそのコピーを持っているが, 掲載されている研究集会の報告集を確認できなかった.

2.2. $k \neq \mathbb{Q}$ かつ不分岐拡大の場合. 群環の torsion 元を使うことにより, Brinkhuis は次のことを示した (cf. Proposition 5.2).

- Theorem 2.2.** (i) ([B7, (1.6)]) k を CM -体または総実代数体とし, K/k を *normal integral basis* をもつ有限次 (すべての有限素点において) 不分岐 $Abel$ 拡大とする. このとき, K/k^+ は *Galois* 拡大であり, かつ $\rho s \rho^{-1} = s^{-1}$ ($\forall s \in \text{Gal}(K/k)$) をみたす. ここで $k^+ := k \cap \mathbb{R}$ とおき, ρ は $\mathbb{C}$ の複素共役の K への制限を表わす.
- (ii) ([B6, Corollary 2.10] または [B7, Corollary 2.1]) k を総実代数体とし, K/k を *normal integral basis* をもつ有限次不分岐 $Abel$ 拡大とする. このとき, $\text{Gal}(K/k)$ は $(2, \dots, 2)$ 型である. つまり, K は k の 2 次拡大たちの合成体になっている.
- (iii) ([B7, Corollary 2.3]) k を CM -体とし, K/k を *normal integral basis* をもつ有限次不分岐 $Abel$ 拡大とする. Artin 写像により K に対応する Cl_k の部分群を N とする. また, 自然な写像 $f: Cl_{k^+} \rightarrow Cl_k$, $c(a) \mapsto c(a\sigma_k)$ を考える. このとき, $\text{Im } f \subset N$.
- (iv) ([B7, Corollary 2.4]) k を CM -体とし, $\bar{k}$ を k の Hilbert 類体とする. このとき, $\bar{k}/k$ が *normal integral basis* をもつならば $h_{k^+} = 1$ または 2 (円分体 $k = \mathbb{Q}(\zeta_n)$ のときは $h_{k^+} = 1$ である).

上の (ii) において, *normal integral basis* をもつ $(2, \dots, 2)$ 型拡大 K/k の例も, そうでない例もある. この結果 (ii) のもっと詳しい内容を [B6, Corollary 2.10] において与えている: K を Galois 群 G をもつ総実代数体 k 上の有限次不分岐 $Abel$ 拡大とする. そのとき, $[o_K] - [o_k G]$ は $\text{Cl}(o_k G)$ の元であり, その位数を $\text{ord}(o_K)$ で表わす. e を G の exponent とする. このとき, $\text{ord}(o_K) = e$ または $e/2$. とくに, $[K : k]$ が奇数ならば $\text{ord}(o_K) = e$ となる.

次の結果は基礎体として, もっとも代表的な CM -体である虚 2 次体をとって, さらに詳しく調べている.

Theorem 2.3. ([B8, Theorem]) $k := \mathbb{Q}(\sqrt{-d})$ とし, $d > 0$, $d \in \mathbb{Z}$ は square-free かつ $d \neq 3$ とする.

- (i) k の上の *normal integral basis* をもつ不分岐 3 次巡回拡大は存在したとしても一つのみである.
- (ii) $m \in \mathbb{Z}$ は “ $\forall n \in \mathbb{Z} : m \neq n^3 - n^2$ ” をみたすとする. K を $f(X) := X^3 - X^2 - m$ の $\mathbb{Q}$ 上の最小分解体とすると, $K/\mathbb{Q}(\sqrt{-27m^2 - 4m})$ は不分岐 3 次巡回拡大かつ *normal integral basis* をもつ. ここで $\mathbb{Q}(\sqrt{-27m^2 - 4m})$ は虚 2 次体で, $\mathbb{Q}(\sqrt{-3})$ とは異なる. *normal integral basis* は f の根たちで与えられる.
- (iii) *normal integral basis* をもつ不分岐 3 次巡回拡大 K/k は (ii) で与えられたものに限る. つまり, ある $m \in \mathbb{Z}$ が存在して, K は $X^3 - X^2 - m$ の $\mathbb{Q}$ 上の最小分解体であり, $k = \mathbb{Q}(\sqrt{-27m^2 - 4m})$ となる.
- (iv) ζ_3 を 1 の原始 3 乗根とする. このとき,

$$\begin{aligned} & \text{normal integral basis をもつ不分岐 3 次巡回拡大 } K/k \text{ が存在する} \\ \iff & \exists \epsilon \in o_{\mathbb{Q}(\sqrt{3d})}^\times \text{ s. t. } \epsilon \equiv 1 \pmod{(\zeta_3 - 1)^3} \text{ かつ } \epsilon \notin \mathbb{Q}(\sqrt{3d})^{\times 3}. \end{aligned}$$

彼の初期の仕事には次の結果もある.

Theorem 2.4. ([B2, Theorem 4.1]) k は CM -体または総実代数体とし, k はその部分体 F 上の $Galois$ 拡大であるとする. K/k は有限次 $Abel$ 拡大であり, かつ K は F 上の $Galois$ 拡大である. $Galois$ 群の群拡大 $1 \rightarrow Gal(K/k) \rightarrow Gal(K/F) \rightarrow Gal(k/F) \rightarrow 1$ は *split* せず, 拡大次数 $[K : k]$ または $[k : F]$ が奇数になっていると仮定する. このとき, K/k は *normal integral basis* をもたない.

この証明は *normal integral basis* の存在条件付き埋め込み問題を考えることによりなされている (cf. [B1], [B3]). なお, [B2], [B3] について, 竹内光弘氏の論説 “ガロワ加群と埋め込み問題について, 数理解析研究所講究録 549 (1985)” がある. また, この Brinkhuis のアプローチに沿う, 2 次拡大を扱った結果として, [M1], [M2] もある.

p を奇素数とし, $k := \mathbb{Q}(\zeta_p)$ とする. [T3, Theorem 2] において, k 上の p 次不分岐巡回拡大の *normal integral basis* の存在と p 進 L -関数の $s = 1$ における値との関係が *principal homogeneous space* の言葉を用いて与えられている (cf. [T5]). [Ic1], [Ic2] においては同様の拡張された結果が得られている. ここは市村さん自身の講演を聞くのが一番であるから, これ以上述べない. ただ, 彼は次の Childs の定理を出発点にしていることを注意する. この結果は環論的手法を使っているが, その証明を読むと代数体の言葉だけで書き直すことができる.

Proposition 2.5. ([Ch, Theorem B]) p を素数, k を有限次代数体とし, $\zeta_p \in k$ と仮定する. K/k は p 次不分岐巡回 *Kummer* 拡大とする. このとき,

K/k は *normal integral basis* をもつ.

$$\iff \exists \varepsilon \in \mathfrak{o}_k^\times \text{ s. t. } K = k(\varepsilon^{1/p}), \quad \varepsilon \equiv 1 \pmod{(\zeta_p - 1)^p}.$$

さらにこれが成り立つとき, $\eta := \varepsilon^{1/p}$ とおくと, $(1/p) \sum_{i=0}^{p-1} \eta^i$ は K/k の *normal integral basis* の生成元になる.

素数次 *Kummer* 拡大が *normal integral basis* をもつための (不分岐拡大に限定しない) 必要十分条件は [Ka4, Theorem 6] において与えた (cf. [Go]). その方法は, 奥津さんによって定義された divisor polynomial ([Oku] (cf. [Ka5])) を用いて, まず *integral basis* の形を決め, 次に Fröhlich による “Hom-description” を使って計算により決定した. それが有効であることを示す例は [Ka1], [Ka2], [Ka4, Ch. IV] にある.

p を素数とし, $\mathcal{G}$ を $(p, \dots, p)$ 型 $Abel$ 群とする. 基礎体 k を固定して,

K/k : 有限次 tamely ramified $Abel$ 拡大, $Gal(K/k) \cong \mathcal{G}$

をみたま K を動かして, $[\mathfrak{o}_K]$ からなる $Cl(\mathfrak{o}_K G)$ の部分集合を $R(\mathfrak{o}_K G)$ で表わす ($Cl(\mathfrak{o}_K G)$ は $\mathfrak{o}_K G$ の locally free 左 ideal たちで定義している). [Mc] においては $R(\mathfrak{o}_K G)$ を解析している (cf. [So]). とくに $R(\mathfrak{o}_K G)$ は $Cl(\mathfrak{o}_K G)$ の部分群をなす. また, “宮本雅彦, クンマー拡大の $Galois$ module structure, 数理解析研究所講究録 549 (1985)” も参照のこと.

2.3. $k \neq \mathbb{Q}$ かつ分岐拡大の場合. $\mathbb{Q}$ 上の $\text{mod } p\infty$ の ray class field $\mathbb{Q}(\zeta_p)$ の中の *normal integral basis* は [Co1], [Co2], [B4, Theorem 2] において扱われた. それは次のように拡張できる. $\mathbb{Q}$ 上の $Abel$ 拡大 K を扱うとき, resolvent と Gauss sum が結びつくことを示し, Stickelberger の定理と [KK, Theorem 2.10, Remark 2.11] を用いて証明された.

Theorem 2.6. ([Ka6, Theorem 5.3]) p を奇素数とし, $k \subset K \subset \mathbb{Q}(\zeta_p)$ とする. $n := [K : k] > 1$, $m := [k : \mathbb{Q}] > 1$ と仮定する. このとき,

- (I) 次の 3 つの場合を除くと, K/k は *normal integral basis* をもたない:
 - (i) m は偶数かつ 2 のべきでなく, かつ $n = 2$.
 - (ii) m と n は共に 2 のべきである.
 - (iii) m は奇数であり, かつ $n = 2$.
- (II) (I-iii) の場合において, K/k は *normal integral basis* をもつ.

Remark 2.2. $p \equiv 1 \pmod{4}$ とし, $K := \mathbb{Q}(\zeta_p)$, $k := \mathbb{Q}(\zeta_p)^+$ ととると, $n = 2$ かつ m は偶数であり, ζ_p は K/k の *normal integral basis* の生成元であることはすぐわかるので, これは (I-i, ii) の場合の 1 つの例を与える. (I-ii) の場合において $n = 2$ ならば, 岩沢の定理より $2 \nmid h_k$ であることに注意して, K/k は *normal integral basis* をもつことが示せる. 他の場合はまだ未解決である.

分岐拡大について次のような例があることを注意しておきたい ([Ka6, Theorem 4.1]). Cf. Theorem 2.2, [GS].

Proposition 2.7. ([Ka6, Proposition 4.5]) k を $[\tilde{k} : k]$ が 2 べきである 2 次体とし, $\mathfrak{p}$ を $k/\mathbb{Q}$ において分岐する $\mathfrak{o}_k$ の *prime ideal* とする. ここで, $\tilde{k}$ は k の *Hilbert* 類体であり, k の $\text{mod } \mathfrak{p}$ の *ray class field* を $k(\mathfrak{p})$ により表わし, $w_{\mathfrak{p}} := |(\mathfrak{o}_k^{\times} + \mathfrak{p})/\mathfrak{p}|$ とおく. いま, $\ell \mid ((N_{\mathfrak{p}} - 1)/w_{\mathfrak{p}})$ をみたす奇素数 ℓ が存在すると仮定する. ℓ に対して具体的に述べないが, ある $\mathfrak{S}_{\ell} \subset \mathcal{P}_k$ を定義することができる (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, 密度定理より $\mathfrak{S}_{\ell}$ は常に無限集合になる). 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.

3. $S = \{p\}$ の場合

標題の意味は次の定義からくる (cf. Example 1.2).

Definition 3.1. k を有限次代数体, p を素数, L/k を $\mathbb{Z}_p$ -拡大とする. そのとき, L/k の各 n -layer L_n について, $\mathfrak{o}_{L_n}[p^{-1}]/\mathfrak{o}_k[p^{-1}]$ が *normal basis* をもつとき, L/k は *normal basis* をもつという.

$\mathbb{Z}_p$ -拡大 L/k において分岐する *prime ideal* は p の上にあるものに限り, 少なくとも 1 つは分岐し, しかも *wildly ramified* する. したがって, ある n_0 があって, $\forall n \geq n_0$ に対して L_n/k は *normal integral basis* をもたない (Theorem 1.3). しかし, p の上にある *prime ideal* を用いて整数環を少し膨らませれば, *normal basis* をもつ可能性は残る. 実際, L/k が *cyclotomic* $\mathbb{Z}_p$ -拡大のときは *normal basis* をもつ ([KM1, Theorem 2.1], [Gr2, Ch. I, Proposition 2.4], [KK, Remark 3.4]).

3.1. Kersten and Michaliček の定理. 次の結果 [KM2, Theorem 3.1, 3.3] は大変興味深いものであった:

Theorem 3.1. p を奇素数とし, $k := \mathbb{Q}(\zeta_{p^n})$ とする. h_{k^+} を k の最大実部分体 k^+ の類数とし, λ^+ を k^+ の *cyclotomic* $\mathbb{Z}_p$ -拡大の岩澤 λ -不変量とする. このとき,

$$p \nmid h_{k^+} \iff \lambda^+ = 0 \text{ かつ } k \text{ の任意の } \mathbb{Z}_p\text{-拡大 } L/k \text{ は } \textit{normal basis} \text{ をもつ.}$$

左辺は Kummer-Vandiver 予想と同値である. $(\Rightarrow)$ の証明は環論的手法が使われている. 代数体の言葉を使って証明を与えることもでき, “ $k/\mathbb{Q}$ は Abel 拡大, $\zeta_p \in k$, p は $k^+/\mathbb{Q}$ で不分解” という仮定の下でも $(\Rightarrow)$ は成り立つ ([KK, Theorem 4.6]).

F を虚 2 次体とし, $k := F(\zeta_p)$ とおく. normal basis をもつ F の $\mathbb{Z}_p$ -拡大の存在と k^+ の cyclotomic $\mathbb{Z}_p$ -拡大の岩澤 λ -不変量との関連については [FK] を見よ. これは Theorem 3.1, $(\Leftarrow)$ の証明を参考にしている. とくに, 3 は $F/\mathbb{Q}$ において惰性し, $3 \mid h_{k^+}$ と仮定すると, もし F のすべての $\mathbb{Z}_3$ -拡大が normal basis をもつならば, k^+ の cyclotomic $\mathbb{Z}_3$ -拡大の岩澤 λ -不変量が消えないことが従う (独立に [FN] においても示されている). これは Greenberg 予想: “任意の総実代数体 N と任意の素数 p に対して, N の cyclotomic $\mathbb{Z}_p$ -拡大の岩澤 λ -不変量 $\lambda_p(N)$ は 0 になる” を否定する命題である. しかし, F のすべての $\mathbb{Z}_3$ -拡大が normal basis をもつか否かはわかっていない.

3.2. Modular construction. 虚数乗法論を用いて normal basis の生成元を具体的に保型関数の特殊値として与えることにより, 次のことが証明されている:

Theorem 3.2. ([Ko1]) F を虚 2 次体とし, p は奇素数であり, $F/\mathbb{Q}$ において完全分解する. $\mathfrak{p}$ を p の上の $\mathfrak{o}_F$ の prime ideal とする. $m \in \mathbb{N}$ とし, $K := F(\mathfrak{p}^{[5m/2]})$, $k := F(\mathfrak{p}^m)$ とおく. ここで $[\cdot]$ は Gauss 記号である. このとき, $\mathfrak{o}_K[p^{-1}]/\mathfrak{o}_k[p^{-1}]$ は normal basis をもつ.

上は [T2, Corollary 4] の結果 ($K := F(\mathfrak{p}^{2m})$ とする) の拡張になっている.

Theorem 3.3. ([Ko2]) F を虚 2 次体, p を奇素数とし, $k := F(p)$ (F の mod p の ray class field) とする.

- (i) $m \in \mathbb{N}$ とし, $K := F(p^m)$ とおくと, $\mathfrak{o}_K[p^{-1}]/\mathfrak{o}_k[p^{-1}]$ は normal basis をもつ.
- (ii) L を F の任意の $\mathbb{Z}_p$ -拡大とすると, $\mathbb{Z}_p$ -拡大 Lk/k は normal basis をもつ.

Remark 3.1. 3 は $F/\mathbb{Q}$ において惰性するとし, L/F を F の任意の $\mathbb{Z}_3$ -拡大とする. いま, $3 \nmid [F(3) : F]$ と仮定する. そのとき, Theorem 3.3, (ii) と Lemma 5.3, (iii) より, L/F は normal basis をもつ. 一方, 仮定より, $3 \nmid h_F$. よって, Reflection theorem より $3 \nmid h_{F(\zeta_3)^+}$ を得る. したがって, Theorem 3.3 は F の $\mathbb{Z}_p$ -拡大の normal basis を調べる試みとしてはまだ不十分である.

4. あとがき

以上が現在知られている normal basis 問題に関する結果である. 基礎体が $\mathbb{Q}$ とは異なるとき, まだまだ十分に結果がないのが実状である. もっともっと結果が出てくれば, Taylor の定理のように, 背後に系統的なものが現れてくることもありうると思う. ですから, 興味のある方はこの問題に参加して頂ければ幸いです.

原稿を書く段階で, 相羽さん, 市村さん, 小松さんから助言を頂きました. どうもありがとうございました.

5. おまけ

normal basis 問題を考えるとき, 簡単だが注意すべき事柄について述べる. k を有限次代数体, K/k を Galois 群 G をもつ有限次 Galois 拡大とし, $S \subset \mathcal{P}_k$ とする.

Lemma 5.1. M/k は Galois 拡大であり, $k \subset M \subset K$ をみたすとする. このとき, $\alpha \in \mathfrak{o}_K(S)$ は $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ の normal basis の生成元であるならば, $\text{Tr}_{K/M}(\alpha)$ は $\mathfrak{o}_M(S)/\mathfrak{o}_k(S)$ の normal basis の生成元になる.

G は環 KG に次のし方で作用する: $\forall s \in G, \forall x = \sum_{t \in G} a_t t \in KG$ に対して,

$$x^s := \sum_{t \in G} a_t^s t \in KG.$$

また, $\hat{x} := \sum_{t \in G} a_t t^{-1}$ とおく. $\beta \in K$ に対して, $R(\beta) = R_G(\beta) := \sum_{t \in G} \alpha^t t^{-1}$ (resolvent) と定義し, $\hat{R}(\beta) := \widehat{R(\beta)}$ と略記する. 次のことはすぐわかる.

$$(5.1) \quad x^s = x \cdot s \ (\forall s \in G) \iff \exists \alpha \in K \text{ s. t. } x = R(\alpha).$$

次の命題は Theorem 2.2, 2.3 の証明の出発点である. それは $S = \phi$ のときに述べられているが, 証明は同じである.

Proposition 5.2. ([B4, Proposition 1.1]) $\alpha \in \mathfrak{o}_K(S)$ とする. このとき, 次は同値である:

- (i) $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ は不分岐かつ α は normal basis の生成元である.
- (ii) $\exists \beta \in \mathfrak{o}_K(S) \text{ s. t. } R(\alpha)\hat{R}(\beta) = 1.$

Remark 5.1. G が Abel 群のとき, 条件 (ii) は $R(\alpha) \in \mathfrak{o}_K(S)[G]^\times$ と同値である.

Lemma 5.3. K_i/k ($i = 1, 2$) を Galois 群 G_i をもつ n_i 次 Galois 拡大とし, $K_1 \cap K_2 = k$ と仮定する.

- (i) $\mathfrak{o}_{K_i}(S)/\mathfrak{o}_k(S)$ は不分岐かつ $\alpha_i \in \mathfrak{o}_{K_i}(S)$ は normal basis の生成元であるとする ($i = 1, 2$). このとき, $\alpha_1 \alpha_2$ は $\mathfrak{o}_{K_1 K_2}(S)/\mathfrak{o}_k(S)$ の normal basis の生成元である.
- (ii) $\mathfrak{o}_{K_1}(S)/\mathfrak{o}_k(S)$ は不分岐かつ $\alpha_1 \in \mathfrak{o}_{K_1}(S)$ は normal basis の生成元であるとする. このとき, α_1 は $\mathfrak{o}_{K_1 K_2}(S)/\mathfrak{o}_{K_2}(S)$ の normal basis の生成元でもある.
- (iii) G_1 は Abel 群であり, $(n_1, n_2) = 1$ と仮定する. このとき, $\mathfrak{o}_{K_1 K_2}(S)/\mathfrak{o}_{K_2}(S)$ は不分岐かつ normal basis をもつならば $\mathfrak{o}_{K_1}(S)/\mathfrak{o}_k(S)$ も不分岐かつ normal basis をもつ.

PROOF. $\mathcal{G} := \text{Gal}(K_1 K_2/k)$ とおく. いま, 群 $\mathcal{G}$ は係数への作用により環 $(K_1 K_2)[\mathcal{G}]$ へ作用している. 自然な同型 $\mathcal{G} \cong G_1 \times G_2$ により両辺を同一視する. そのとき, G_1 と G_2 の元は可換であり, $G_1 = \text{Gal}(K_1 K_2/K_2)$, $G_2 = \text{Gal}(K_1 K_2/K_1)$ となる. (i), (ii) はすぐわかるので, (iii) のみ示す. α を $\mathfrak{o}_{K_1 K_2}(S)/\mathfrak{o}_{K_2}(S)$ の normal basis の生成元とする. $u := R(\alpha)$ とおくと, G_1 は可換だから, Proposition 5.2 より, $u \in \mathfrak{o}_{K_1 K_2}(S)[G_1]^\times$. $(n_1, n_2) = 1$ より, $n_1 a_1 + n_2 a_2 = 1$ をみたす $a_i \in \mathbb{Z}$ がとれる. $v := u^{a_2}$ とおくと, G_1 は可換だから, (5.1) より, $v^s = v \cdot s^{a_2} \ (\forall s \in G_1)$. $Nv :=$

$\prod_{t \in G_2} v^t$ (v のノルム) とすると, $(Nv)^t = Nv$ ($\forall t \in G_2$). よって, $Nv \in \mathfrak{o}_{K_1}(S)[G_1]$.
同様に, $(Nv)^{-1} \in \mathfrak{o}_{K_1}(S)[G_1]$. したがって, $Nv \in \mathfrak{o}_{K_1}(S)[G_1]^\times$. $\forall s \in G_1$ に対して,

$$\begin{aligned} (Nv)^s &= \prod_{t \in G_2} v^{st} = \prod_{t \in G_2} v^{ts} = \prod_{t \in G_2} (v^s)^t = \prod_{t \in G_2} (v \cdot s^{a_2})^t \\ &= \prod_{t \in G_2} (v^t \cdot s^{a_2}) = Nv \cdot s^{a_2 n_2} = Nv \cdot s. \end{aligned}$$

よって, (5.1) より, $\exists \beta \in \mathfrak{o}_{K_1}(S)$ s. t. $Nv = R_{G_1}(\beta)$. $R_{G_1}(\beta) \in \mathfrak{o}_{K_1}(S)[G_1]^\times$ だから Proposition 5.2 より, $\mathfrak{o}_{K_1}(S)/\mathfrak{o}_k(S)$ は不分岐かつ β は normal basis の生成元となる. $\square$

Remark 5.2. 分岐拡大については例えば [Ka1, Lemma 3] を参照せよ.

参考文献

I. $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ の NORMAL BASIS に関する論文

- [B1] J. Brinkhuis, *Embedding problems and Galois modules*, doctoral dissertation, University of Leiden, 1981.
- [B2] ———, *Normal integral bases and embedding problems*, Math. Ann. **264** (1983), 537–543.
- [B3] ———, *Galois modules and embedding problems*, J. Reine Angew. Math. **346** (1984), 141–165.
- [B4] ———, *Normal integral bases and complex conjugation*, J. Reine Angew. Math. **375** (1987), 157–166.
- [B5] ———, *Galois module structure as the obstruction to a local-global principle*, J. Algebra **145** (1992), 454–462.
- [B6] ———, *Unramified abelian extensions of CM-fields and their Galois module structure*, Bull. London Math. Soc. **24** (1992), 236–242.
- [B7] ———, *On the Galois module structure over CM-fields*, Manuscripta Math. **75** (1992), 333–347.
- [B8] ———, *Normal integral bases and the Spiegelungssatz of Scholz*, Acta Arithmetica **LXIX** (1995), no. 1, 1–9.
- [Ch] L. N. Childs, *The group of unramified kummer extensions of prime degree*, Proc. London Math. Soc. **35** (1977), no. 3, 407–422.
- [Co1] J. Cougnard, *Quelques extensions modérément ramifiées sans base normale*, J. London Math. Soc. **31** (1985), 200–204.
- [Co2] ———, *Bases normales relatives dans certaines extensions cyclotomiques*, J. Number Theory **23** (1986), 336–346.
- [FN] V. Fleckinger and T. Nguyen Quang Do, *Bases normales, unités et conjecture faible de Leopoldt*, Manuscripta Math. **71** (1991), 183–195.
- [Fr1] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. Reine Angew. Math. **286/287** (1976), 380–440.

- [FK] T. Fukuda and K. Komatsu, *Normal bases and λ -invariants of number fields*, Proc. Japan Acad. **67A** (1991), 243–245.
- [GS] E. J. Gómez Ayala and R. Schertz, *Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Number Theory **44** (1993), 41–46.
- [Go] E. J. Gómez Ayala, *Bases normales d'entier dans les extensions de Kummer de degré premier*, J. de Théorie des Nombres de Bordeaux **6** (1994), 95–116.
- [Gr] M. -N. Gras, *Bases d'entiers dans les extensions cycliques de degré 4 de $\mathbb{Q}$* , Sémin. de Théorie des Nombres, Bordeaux, 1982–1983.
- [Gr1] C. Greither, *Cyclic Galois extensions and normal bases*, Trans. Amer. Math. Soc. **326** (1991), 307–343.
- [Ic1] H. Ichimura, *On p -adic L -functions and normal bases of rings of integers*, J. Reine Angew. Math. **462** (1995), 169–184.
- [Ic2] ———, *On a normal integral basis problem over cyclotomic $\mathbb{Z}_p$ -extensions*, to appear in J. Math. Soc. Japan.
- [Ka1] F. Kawamoto, *On normal integral bases*, Tokyo J. Math. **7** (1984), 221–231.
- [Ka2] ———, *Remark on “On Normal Integral bases”*, Tokyo J. Math. **8** (1985), 275.
- [Ka3] ———, *On normal integral bases of local fields*, J. Algebra **98** (1986), 197–199.
- [Ka4] ———, *Normal integral bases and divisor polynomials*, doctoral dissertation, Gakushuin University, 1986.
- [Ka5] ———, *A note on ideal bases*, Tokyo J. Math. **11** (1988), 303–309.
- [Ka6] ———, *On normal bases of some ring extensions in number fields I*, to appear in Tokyo J. Math.
- [KK] F. Kawamoto and K. Komatsu, *Normal bases and $\mathbb{Z}_p$ -extensions*, J. Algebra **163** (1994), 335–347.
- [KM1] I. Kersten and J. Michaliček, *$\mathbb{Z}_p$ -extensions of complex multiplication fields*, J. Number Theory **32** (1989), 131–150.
- [KM2] ———, *On vandiver's conjecture and $\mathbb{Z}_p$ -extensions of $\mathbb{Q}(\zeta_{p^n})$* , J. Number Theory **32** (1989), 371–386.
- [Ko1] K. Komatsu, *Modular construction of normal basis*, J. Math. Soc. Japan **46** (1994), 235–243.
- [Ko2] ———, *Normal basis and Greenberg's conjecture*, Math. Ann. **300** (1994), 157–163.
- [M1] R. Massy, *Bases normales d'entiers relatives quadratiques*, J. Number Theory **38** (1991), 216–239.
- [M2] ———, *Formules de construction de bases normales d'entiers relatives*, C. R. Acad. Sci. Paris, Sér. I, **313** (1991), 477–482.
- [Mc] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134.
- [Oka] T. Okada, *Normal bases of class fields over Gauss' number field*, J. London Math. Soc. **22** (1980), no. 2, 221–225.
- [Oku] K. Okutsu, *Construction of integral basis I–IV*, Proc. Japan Acad., **58A** (1982), pp. 47–49, 87–89, 117–119, 167–169.
- [So] B. Sodaigui, *Structure galoisienne relative des anneaux d'entiers*, J. Number Theory **28** (1988), 189–204.
- [T1] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*,

Invent. Math. **63** (1981), 41–79.

- [T2] ———, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math., **121** (1985), 519–535.
- [T3] ———, *The Galois module structure of certain arithmetic principal homogeneous spaces*, J. Algebra **153** (1992), 203–214.

II. 関数体へのアナロジー

- [C1] R. J. Chapman, *Carlitz modules and normal integral bases*, J. London Math. Soc. **44** (1991), no. 2, 250–260.
- [C2] ———, *Kummer theory and Galois module structure in global function fields*, Math. Z. **208** (1991), no. 3, 375–388.
- [C3] ———, *Classgroups of sheaves of locally free modules over global function fields*, Ohio State Univ. Math. Res. Inst. Publ. **2** (1992), 403–411.

III. 成書と参考図書

- [CT] Ph. Cassou-Noguès and M. J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics 66, Birkhäuser, Boston Basel Stuttgart, 1987.
- [CR] C. W. Curtis and I. Reiner, *Methods of representation theory*, vol. I, II, Wiley-Interscience, New York, 1981, 1987.
- [Fr2] A. Fröhlich, *Galois module structure of algebraic integers*, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1983.
- [Fr3] ———, *Classgroups and hermitian modules*, Progress in Mathematics 48, Birkhäuser, Boston Basel Stuttgart, 1984.
- [Gr2] C. Greither, *Cyclic Galois extensions of commutative rings*, Lecture Notes in Math. 1534, Springer-Verlag, 1992.
- [Iw] K. Iwasawa, *Local class field theory*, Oxford University Press, 1986.
- [L] R. Long, *Algebraic number theory*, Marcel Dekker, New York, 1977.
- [R] I. Reiner, *Maximal orders*, Academic Press, London, 1975.
- [Se] J. P. Serre, 有限群の線型表現, 岩波書店, 1974.
- [Sn1] V. P. Snaith, *Explicit Brauer induction*, Cambridge Studies in Advanced Math., Cambridge University Press, 1994.
- [Sn2] ———, *Galois module structure*, Fields Institute Monographs 2, American Mathematical Society, 1994.
- [T4] M. J. Taylor, *Classgroups of group rings*, London Mathematical Society Lecture Note Series 91, Cambridge University Press, 1984.
- [T5] ———, *Hopf orders and Galois module structure*, in “Group rings and class groups”, DMV Seminar 18, Birkhauser Verlag, Basel, 1992.