

局所数体の整数環の正規底について

九州大・理 円藤 章

1. はじめに. K が有限次代数体 k の有限次拡大体のとき, k と K の整数環をそれぞれ A と B であらわせば, B は当然 A 上の加群とみなされるが, さらに K/k が G をガロア群にもつ正規拡大であれば, B は群環 $A[G]$ 上の加群である. このとき, A -加群 B の底で B のある元の共役からなるものを正規底という. B が正規底をもつことは, B を $A[G]$ -加群とみなしたときに自由加群であることと同じである. このことについて, たとえば次のいくつかの事実が知られている.

$k = \mathbb{Q}$ の場合には

(Hilbert [7]) $K/\mathbb{Q}$ がアーベル拡大で弱分岐であれば, B は正規底をもつ.

(Martinet [11]) p が奇素数で, $K/\mathbb{Q}$ が $2p$ 次の 2 面体群をガロア群にもち弱分岐であれば, B は正規底をもつ.

さらに, 一般に

(Noether [13]-Martinet [11]) $K/\mathbb{K}$ が弱分岐であることと, B が $A[G]$ -加群として射影的であることが同値である。

Leopoldt は B を $A[G]$ -加群とみなすだけでなく, B を群環 $\mathbb{K}[G]$ の部分環 $\mathcal{O} = \{\lambda \in \mathbb{K}[G] \mid \lambda B \subset B\}$ 上の加群として考え, その構造をしらべている。 $\mathcal{O}$ は $\mathbb{K}[G]$ の order であって, $A[G]$ をいくみ, B が正規底をもつときには $\mathcal{O} = A[G]$ である。

(Leopoldt [9]-Jacobinski [8]) $K/\mathbb{K}$ がアーベル拡大である条件をみたせば, B は自由 $\mathcal{O}$ -加群である。その条件は $\mathbb{K} = \mathbb{Q}$ の場合にはみたされている。

(Bergé [1]) p が奇素数で, $K/\mathbb{Q}$ が $2p$ 次の 2 面体群をガロア群にもてば, B は自由 $\mathcal{O}$ -加群である。

さらに, Bertrandias, Ferton [2, 3, 5] は K が $\mathbb{Q}_p$ 上の有限次拡大体 $\mathbb{K}$ の p 次および $2p$ 次正規拡大のときに, 整数環の加群としての構造をしらべている。ここではその方法にしたがって, 次の条件をみたす局所数体の整数環についてのいくつかの結果を述べる。

p を素数とし, g を $p-1$ を割る整数とする。 $\mathbb{K}$ を $\mathbb{Q}_p$ の有限次拡大体とし, $K/\mathbb{K}$ を pg 次正規拡大でそのガロア群 G の中心が単位元 1 のみからなると仮定する。このとき G の生成元 σ, τ を次のようにえらぶことができる。

$$\sigma^p = \tau^g = \tau^{-1} \sigma \tau \sigma^{-\alpha} = 1$$

ここで, α は $\text{mod } p$ で位数 g の整数である。

記号を次のように定める。

A, B : k, K の整数環

v_k, v_K : k, K の付値

e_0, e : k, K の絶対分岐指数 ($e_0 = v_k(p)$, $e = v_K(p)$)

π_0 : A の任意の素元

$\mathcal{O} = \{ \lambda \in k[G] \mid \lambda B \subset B \}$

$\theta \in B$ が k -加群 K の正規底を生成するとき,

$\alpha(\theta) = \{ \lambda \in k[G] \mid \lambda \theta \in B \}$

$\alpha(\theta)$ は $\mathcal{O}$ の左イデアルであって (cf. [4]), $\mathcal{O} \subset \alpha(\theta)$, $\alpha(\theta)\theta = B$,
 $\mathcal{O} = \{ \lambda \in k[G] \mid \lambda \alpha(\theta) \subset \alpha(\theta) \}$ がなりたつ。

補題 1 ([3]). 次の 1), 2), 3) は同値である。

- 1) B は自由 $\mathcal{O}$ -加群である。
- 2) 適当な $\theta \in B$ によって $\alpha(\theta) = \mathcal{O}$ となる。
- 3) すべての $\theta \in B$ について $\alpha(\theta)$ は $\mathcal{O}$ の単項イデアルである。

K/k が弱分岐であれば, B は正規底をもつ [13]。以下, K/k は強分岐である ($e = p g e_0$ または $p e_0$) と仮定して, その i 次の分岐群を G_i であらわす: $G_i = \{ s \in G \mid v_K(s(x) - x) \geq i+1, x \in B \}$ 。

整数 t を, $G_t \neq \{1\}$, $G_{t+1} = \{1\}$ で定めて,

$$t = a + bp, \quad 0 \leq a \leq p-1$$

とおくと, $1 \leq t \leq \frac{e}{p-1}$, $(t, g) = 1$ で

$$a=0 \iff t = \frac{e}{p-1}$$

がなりたつ[14]. $\sigma \in G_t$ で, $K/\mathbb{K}$ が完全分岐かどうかによって $\tau \in G_0 - G_1$ または $\tau \in G_0$ である. おのおの場合に, $a=0$ かどうかによって考える.

2. $K/\mathbb{K}$ が完全分岐で $a \neq 0$ の場合. $(t, q)=1$ だから, 1 の原始 q 乗根 $\zeta \in \mathbb{Z}_p$ を $\zeta \equiv \alpha^t \equiv \alpha^{a+q} \pmod{p}$ をみたすようにえらぶ. このとき, τ の位数が q だから K の素元 π を $\tau(\pi^q) = \pi^q$ をみたすようにえらべば, $\tau\sigma\tau = \sigma^\alpha$ であることより

$$\tau(\pi) = \zeta \pi$$

となる. このような K の素元によって, B の元 θ を

$$\theta = \pi^a (1 + \pi^p + \dots + \pi^{(q-1)p})$$

によって定める. 以下, この θ が $K/\mathbb{K}$ の正規底を生成することとをたしかめ, $\mathcal{O}(\theta)$ の構造をしらべることによって補題 1 より B が自由 $\mathcal{O}$ -加群であるための条件を求める.

群環 $\mathbb{Z}_p[G]$ の元 f, g_j を

$$f = \frac{1}{q} (\sigma + \zeta^t \sigma^\alpha + \dots + \zeta^{(q-1)t} \sigma^{\alpha^{q-1}}),$$

$$g_j = \frac{1}{q} (1 + \zeta^{-\frac{a+j}{t}} \tau + \dots + \zeta^{-\frac{(q-1)(a+j)}{t}} \tau^{q-1}), \quad j=0, 1, \dots, q-1$$

によって定める.

補題 2. 1) $g_j f = f g_{j'}$ $j' \equiv j - t \pmod{q}$

$$2) \quad g_j g_{j'} = \begin{cases} g_j & j = j' \\ 0 & j \neq j' \end{cases}$$

$$3) \quad f^p = a_1 f + a_2 f^{g+1} + \dots + a_n f^{p-g} \quad p-1 = ng$$

ここで, $a_i \in p\mathbb{Z}_p$, $p \nmid a_1$ である。

1) と 2) は簡単な計算によってでる。3) は σ を 1 の原始 p 乗根 ω に写すことによって, f を $\mathbb{Q}_p(\omega)$ に写して考えればよい。

さて, θ に g_j を作用させると, $g_j(\theta) = \pi^{a+jp}$ となり, さらに f を作用させて,

$$v_K(f^i g_j(\theta)) = a + it + jp, \quad i=0, 1, \dots, p-1; j=0, 1, \dots, g-1$$

をえる。これらの値は $\text{mod } pg$ ですべて異なるから, θ は $K/\mathbb{K}$ の正規底を生成する。はじめに $\mathcal{O}(\theta)$ の構造をしらべる。 $x \in \mathbb{K}$ について, $x f^i g_j$ が $\mathcal{O}(\theta)$ にふくまれるのは, $v_K(f^i g_j(\theta)) = pg v_K(x) + a + it + jp \geq 0$ のときである。このとき, $x f^i g_j$ が $\mathcal{O}$ にふくまれるためには, $x f^i g_j(B) \subset B$ でなければならない。

定理 1. A -加群 $\mathcal{O}(\theta)$ は

$$\pi_0^{-\nu_{ij}} f^i g_j, \quad i=0, 1, \dots, p-1; j=0, 1, \dots, g-1$$

によって生成される。ただし, $\nu_{ij} = \left[\frac{a+it+jp}{pg} \right]$ である。

$\mathcal{O}(\theta) = \mathcal{O}$ となるのは,

$$a=1, \theta \equiv 0 \pmod{g} \quad \text{または} \quad a=p-1, \theta \equiv -1 \pmod{g}$$

のときである。

定理の後半については, $\theta \equiv 0 \pmod{g}$ のときに $a \neq 1$ ならば, $ia < p < (i+1)a$ であるような $i < p-1$ について $v_K(f^i g_{g-1}(\pi^{a-1})) = a-1+it < pg + i\theta p = pg \nu_{i, g-1}$ となり $\pi_0^{-\nu_{i, g-1}} f^i g_{g-1} \notin \mathcal{O}$ である。

逆に $a=1$ ならば, $B=\alpha(\theta)\theta$ であることと補題 2 をつかって $\pi_0^{-\nu_{ij}} f^i g_j(B) \subset B$ がえられる。 $\theta \neq 0 \pmod{\mathfrak{g}}$ のときも同じようにすればよい。

次に $\mathcal{O}$ の構造をしらべる。 $\lambda \in k[\theta]$ が $\mathcal{O}$ にふくまれるのは, $\lambda \pi_0^{-\nu_{ij}} f^i g_j$ がすべて $\alpha(\theta)$ にふくまれるときである。 とくに $x f^i g_j$, $x \in k$, については, $j+i't \equiv j' \pmod{\mathfrak{g}}$ のとき $x f^i g_j \pi_0^{-\nu_{ij'}} f^{i'} g_{j'} = x \pi_0^{-\nu_{i+i', j+j'}} f^{i+i'} g_{j+j'}$ であるから, $i+i' \leq p-1$ のときには $\nu_k(x) \leq \nu_{i+i', j+j'} - \nu_{i', j'}$ であればよい。 $i+i' > p-1$ のときには補題 2 をつかって $f^{i+i'}$ を $f, f^2, \dots, f^{p-1}$ の $-$ 次和としてあらわしておく。 そこで, 整数 c_1 を

$$a + c_1 \equiv 1 \pmod{\mathfrak{g}}, \quad 0 \leq c_1 \leq \mathfrak{g}-1$$

によって定める。 $t < \frac{e}{p-1} - c_1$ のときには $e_0 \geq \nu_{p-1, \mathfrak{g}-1}$ である。 このとき, $\nu_k(x) \geq -\nu_{ij}$, $i+i' > p-1$ ならば $x \pi_0^{-\nu_{ij'}} f^{i+i'} g_{j+j'} \in \alpha(\theta)$ であることがわかる。 これらのことより次の結果をえる。

定理 2. $t < \frac{e}{p-1} - c_1$ ならば, A -加群 $\mathcal{O}$ は

$$\pi_0^{-\mu_{ij}} f^i g_j, \quad i=0, 1, \dots, p-1; \quad j=0, 1, \dots, \mathfrak{g}-1$$

によって生成される。 ただし, $\mu_{ij} = \min_{\substack{0 \leq i' \leq p-1-i \\ j' \equiv j-i't \pmod{\mathfrak{g}}}} \{\nu_{i+i', j+j'} - \nu_{i', j'}\}$ である。

$\alpha(\theta)$ が $\mathcal{O}$ の単項イデアルであるための条件を求めるために整数 c_2 を

$$a + c_2 \equiv 1 \pmod{\mathfrak{g}}, \quad 1 \leq c_2 \leq \mathfrak{g}$$

によって定める。 $t < \frac{e}{p-1} - c_2$ ならば $e_0 > \nu_{p-1, g-1}$ である。 $\mathcal{O}\lambda$ は $\{\pi_0^{-\mu_{ij}} f^i g_j \lambda\}$ によって生成されているから、 $\lambda = \sum_{i,j} a_{ij} f^i g_j$, $a_{ij} \in k$, とおいて補題2をつかって $\pi_0^{-\mu_{ij}} f^i g_j \lambda$ の各項をしらべる。 $\alpha(\theta) = \mathcal{O}\lambda$ ならば、まず g_j の項を比較することにより $v_k(a_{0j}) = 0$ でなければならぬことがわかり、各項を逐次比較していくと次の結果をえる。

定理3. $t < \frac{e}{p-1} - c_2$ ならば、 $\alpha(\theta) = \mathcal{O}\lambda$ とあらわされるのは $\alpha(\theta) = \mathcal{O}$ のときにかぎる。

$a \equiv 1 \pmod{g}$ のときには、 $c_1 = 0$, $c_2 = g$ で c_1 と c_2 は異なる。それ以外のときには $c_1 = c_2$ である。そこで、 $a \equiv 1 \pmod{g}$ で $\frac{e}{p-1} - g \leq t < \frac{e}{p-1}$ のときに $\frac{a}{pg}$ を連分數に展開して[]の方法によってもう少しくわしくしらべると、次のことがわかる。

定理5. $g=2$ のとき $\frac{e}{p-1} - 2 \leq t < \frac{e}{p-1}$ ならば、次のおのおの場合に適当な單數 $u \in A$ をえらぶと、 $\alpha(\theta) = \mathcal{O}(g_0 + (u + \pi_0^{-\nu_{i_0,1}} f^{i_0}) g_1)$ となる。

$$1) \quad a | 2p-1, \quad a \equiv 1 \pmod{4}, \quad i_0 = \frac{2p-1-a}{2a}$$

$$2) \quad p \equiv 1 \pmod{3}, \quad a=3, \quad i_0 = \frac{p-1}{3}$$

$$3) \quad p=5, \quad a=3, \quad i_0=2$$

実際、いずれの場合にも $\nu_{i_0} = \mu_{i_0}$, $i=0, 1, \dots, p-1$, であって、 $j=1$ については $\pi_0^{-\mu_{i_1}} f^{i_1} g_1 (u + \pi_0^{-\nu_{i_0,1}} f^{i_0}) g_1 = \sum_{i=0}^{p-1} \xi_{i,i'} \pi_0^{-\nu_{i',1}} f^{i'} g_1$, $\xi_{i,i'} \in A$, とおくとき

$$(\xi_{i,j}) \equiv \begin{pmatrix} u & & & \\ & u & & \\ & & \ddots & \\ & & & 0 \cdots 0 \\ & & & & u \end{pmatrix} + \begin{pmatrix} 0 \cdots 0 & 0 & \cdots 0 \\ & 0 & \ddots & \\ & & \ddots & 0 \\ & & & 0 & \cdots 0 \\ * & & & & 1 \\ 0 & \cdots & 0 & \# \end{pmatrix} \pmod{\pi_0}$$

となる。*, ..., # は A の適当な単数をあらわす。 u を適当にえらぶとこの行列が A 上の正則行列となるから、上がでる。

3. $K/\mathbb{K}$ が完全分岐で $a=0$ の場合. このときは $t = \frac{e}{p-1}$ で, G の部分群 $\langle \sigma \rangle$ に対応する $K/\mathbb{K}$ の中間体が 1 の p 乗根をいくむ[10]. このことから K の素元 π を $\sigma(\pi^p) = \pi^p$ および $\tau(\pi^q) = \pi^q$ をみたすようにえらべることがわかる. このような K の素元 π によって, B の元 θ を

$$\theta = 1 + \pi + \cdots + \pi^{p^q-1}$$

によって定める. $\tau(\pi) = \zeta\pi$ となる 1 の原始 q 乗根 $\zeta \in \mathbb{Z}_p$ にたいして, $\zeta \equiv \alpha^s \pmod{q}$ をみたす整数 s をえらんで, $a \neq 0$ のときと同じように $\mathbb{Z}_p G$ の元 f, g_j を

$$f = \frac{1}{q} (\sigma + \zeta^s \sigma^\alpha + \cdots + \zeta^{(q-1)s} \sigma^{\alpha^{q-1}}),$$

$$g_j = \frac{1}{q} (1 + \zeta^{-j} \tau + \cdots + \zeta^{-(q-1)j} \tau^{q-1}), \quad j = 0, 1, \dots, q-1$$

によって定める. この場合にも θ に f と g_j を作用させると, $\{f^i g_j(\theta)\}$ が $K/\mathbb{K}$ の底であることがわかり, したがって θ が正規底を生成する. $v_K(f^i g_0(\theta)) = it + q$, $v_K(f^i g_j(\theta)) = it + j$, $j \neq 0$, である. そして, すべての $x \in B$ にたいして $v_K(f^i g_j(x)) \geq it$ である.

定理 6. A -加群 $\mathcal{O}(\theta)$ は

$$\pi_0^{-\nu_i} f^i g_j, \quad i=0, 1, \dots, p-1; j=0, 1, \dots, q-1$$

によって生成され、 $\mathcal{O}$ に一致する。ただし、 $\nu_i = [\frac{iq}{p}]$ である。

以上のことをまとめると、 $K/\mathbb{K}$ が完全分岐する場合は補題1より次のようになる。

定理7. $K/\mathbb{K}$ が完全分岐するとき、次の場合には B は自由 $\mathcal{O}$ -加群である。

- 1) $a=0$
- 2) $a=1, q \equiv 0 \pmod{p}$ または $a=p-1, q \equiv -1 \pmod{p}$
- 3) $q=2, a|2p-1, a \equiv 1 \pmod{4}, \frac{e}{p-1} - 2 \leq t < \frac{e}{p-1}$
- 4) $p \equiv 1 \pmod{3}, q=2, a=3, \frac{e}{p-1} - 2 \leq t < \frac{e}{p-1}$
- 5) $p=5, q=2, a=3, \frac{e}{4} - 2 \leq t < \frac{e}{4}$

逆に $t < \frac{e}{p-1} - c_2$ のとき、 B が自由 $\mathcal{O}$ -加群ならば2)がなりたつ。

4. $K/\mathbb{K}$ が完全分岐でない場合。この場合は $e = pe_0$ で、

[2,5]と同じ結果になる。

定理8. $\frac{t}{p} = a_0 + \frac{1}{a_1} + \dots + \frac{1}{a_r}$, $a_0 = b, a_r > 1$ と連分数に展開したとき、 $0 \leq r \leq 2$ または $3 \leq r \leq 4, \frac{e}{p-1} - 1 \leq t < \frac{e}{p-1}$ のとき B は自由 $\mathcal{O}$ -加群である。逆に B が自由 $\mathcal{O}$ -加群ならば、 $t = \frac{e}{p-1}$ のときには $r=0$, $t < \frac{e}{p-1} - 1$ のときには $r=1, 2, \frac{e}{p-1} - 1 \leq t < \frac{e}{p-1}$ のときには $r=3, 4$ である。

文 献

- [1] BERGE, A.-M. Sur l'arithmétique d'une extension diédrale.
Ann. Inst. Fourier 22-2(1972) 31-59.
- [2] BERTRANDIAS, F., BERTRANDIAS, J.-P. et FERTON, M.-J. Sur
l'anneau des entiers d'une extension cyclique de degré premier
d'un corps local. C. R. Acad. Sci.(A) 274(1972) 1388-1391.
- [3] BERTRANDIAS, F. et FERTON, M.-J. Sur l'anneau des entiers
d'une extension cyclique de degré premier d'un corps local.
C. R. Acad. Sci.(A) 274(1972) 1330-1333.
- [4] DEURING, M. Algebren.
- [5] FERTON, M.-J. Sur l'anneau des entiers d'une extension
diédrale de degré $2p$ d'un corps local. C. R. Acad. Sci.(A)
274(1972) 1529-1532.
- [6] FERTON, M.-J. Sur le idéaux d'une extension cyclique de degré
premier d'un corps local. C. R. Acad. Sci.(A) 276(1973)
1483-1486.
- [7] HILBERT, D. Die Theorie der algebraischen Zahlkörper. Jahber.
Deut. Math.-Ver. 4(1897) 175-546.
- [8] JACOBINSKI, H. Über die Hauptordnung eines Körpers als
Gruppenmodule. J. Reine Angew. Math. 213(1964) 151-164.
- [9] LEOPOLDT, H.-W. Über die Hauptordnung der ganzen Elemente eines
abelschen Zahlkörpers. J. Reine Angew. Math. 201(1959) 119-149.
- [10] MACKENZIE, R. and WHAPLES, G. Artin-Schreier equation in
characteristic zero. Amer. J. Math. 78(1956) 473-485.
- [11] MARTINET, J. Sur l'arithmétique des extensions galoisiennes
à groupe de Galois diédral d'ordre $2p$. Ann. Inst. Fourier
19(1971) 123- 126.

- [12] MARTINET, J. Anneau des entiers d'une extensions galoisienne
consdéré comme module sur l'algèbre du groupe de Galois.
Bull. Soc. Math. France Mém. 25(1971) 123-126.
- [13] NOETHER, E. Normalbasis bei Körpern ohne höhere Verzweigung.
J. Reine Angew. Math. 167(1932) 147- 152.
- [14] SERRE, J.-P. Corps locaux.