数理解析研究所講究録
第230巻 1975年 59-69

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しられている。

$k=\mathbb{Q}$ 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/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 $k[G]$ の部分環 $\mathcal{O}=\{\lambda\in k[G] \mid \lambda B\subset B\}$ 上の加群として考え，その構造をしらべている。$\mathcal{O}$ は $k[G]$ の order であって，$A[G]$ をふくみ，B が正規底をもつときには $\mathcal{O}=A[G]$ である。

(Leopoldt [9]-Jacobinski [8]) K/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 $k=\mathbb{Q}$ 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 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。k を $\mathbb{Q}_p$ の有限次拡大体とし，K/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 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

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

$\theta \in B$ が k-加群 K の正規底を生成するとき，

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

$\mathfrak{A}(\theta)$ は $\mathfrak{O}$ の左イデアルであって (cf. [4]), $\mathfrak{O} \subset \mathfrak{A}(\theta)$, $\mathfrak{A}(\theta)\theta = B$, $\mathfrak{O} = \{\lambda \in k[G] \mid \lambda\mathfrak{A}(\theta) \subset \mathfrak{A}(\theta)\}$ 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 $\mathfrak{O}$-加群である。

2) 適当な $\theta \in B$ によって $\mathfrak{A}(\theta) = \mathfrak{O}$ となる。

3) すべての $\theta \in B$ にたいして $\mathfrak{A}(\theta)$ は $\mathfrak{O}$ 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 ($e = pge_0$ または pe_0) と仮定して，そのとき次の分岐群を 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，

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

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

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

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

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

$$\theta=\pi^a(1+\pi^p+\cdots+\pi^{(g-1)p})$$

によって定める。以下，この θ が K/k の正規底を生成することをたしかめ，$\mathcal{O}(\theta)$ 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

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

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

によって定める。

補題2. 1) $g_jf=fg_{j'}\qquad j'\equiv j-t\pmod g$

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

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

ここで, $a_i \in p\mathbb{Z}_p$, $p \| a_1$ 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,

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

をえる。これらの値は mod pg ですべて異なるから, θはK/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。$x \in k$にたいして, $xf^i g_j$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, $xf^i g_j$が$\mathcal{O}$にふくまれるためには, $xf^i g_j(B) \subset B$ でなければならない。

定理 1. A-加群 $\mathcal{O}(\theta)$ は

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

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

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

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

のときである。

定理の後半については, $b \equiv 0 \pmod g$ 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 $v_K(f^i g_{g-1}(\pi^{a-1})) = a-1+it < pg + ibp = pg\nu_{i,g-1}$ 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, $B=\mathcal{O}(\theta)\theta$ 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。 $b\not\equiv 0 \pmod g$ 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。$\lambda\in k[G]$ が $\mathcal{O}$ にふくまれるのは, $\lambda\pi_0^{-\nu_{ij}} f^i g_j$ がすべて $\mathcal{O}(\theta)$ にふくまれるときである。とくに $xf^i g_j$, $x\in k$, にたいしては, $j-i't\equiv j' \pmod g$ のとき $xf^i g_j\,\pi_0^{-\nu_{i'j'}} f^{i'} g_{j'} = x\pi_0^{-\nu_{i'j'}} f^{i+i'} g_{j'}$ であるから, $i+i'\leqq p-1$ のときには $v_k(x)\leqq \nu_{i+i',j'}-\nu_{i'j'}$ 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 $f, f^2, \cdots, f^{p-1}$ の一次和としてあらわしておく。そこで, 整数 c_1 を

$$a+c_1\equiv 1 \pmod g,\quad 0\leqq c_1\leqq g-1$$

によって定める。 $t<\frac{e}{p-1}-c_1$ のときには $e_0\geqq \nu_{p-1,g-1}$ である。このとき, $v_k(x)\geqq -\nu_{ij}$, $i+i'>p-1$ ならば $x\pi_0^{-\nu_{i'j'}} f^{i+i'} g_{j'}\in\mathcal{O}(\theta)$ 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

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

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

$\mathcal{O}(\theta)$ 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

$$a+c_2\equiv 1 \pmod g,\quad 1\leqq c_2\leqq g$$

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。$\mathfrak{O}\lambda$ 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。$\mathfrak{A}(\theta)=\mathfrak{O}\lambda$ ならば，まず g_j の項を比較することにより $v_k(a_{0j})=0$ でなければならないことがわかり，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，$\mathfrak{A}(\theta)=\mathfrak{O}\lambda$ とあらわされるのは $\mathfrak{A}(\theta)=\mathfrak{O}$ 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 $\frac{e}{p-1}-g\leqq t<\frac{e}{p-1}$ のときに $\frac{a}{pg}$ を連分数に展開して[ ]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 $\frac{e}{p-1}-2\leqq t<\frac{e}{p-1}$ ならば，次のおのおのの場合に適当な単数 $u\in A$ をえらぶと，$\mathfrak{A}(\theta)=\mathfrak{O}(g_0+(u+\pi_0^{-\nu_{i_0 1}}f^{i_0})g_1)$ となる。

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

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

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

実際，いずれの場合にも $\nu_{i0}=\mu_{i0}$, $i=0,1,\cdots,p-1$, であって，$j=1$ にたいしては $\pi_0^{-\mu_{i1}}f^i g_1(u+\pi_0^{-\nu_{i_0 1}}f^{i_0})g_1=\sum_{i'=0}^{p-1}\xi_{ii'}\pi_0^{-\nu_{i'1}}f^{i'}g_1$, $\xi_{ii'}\in A$, とおくとき

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

となる。 $*, \cdots, *$ 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/k が完全分岐で $\alpha=0$ の場合。 このときは $t=\frac{e}{p-1}$ で，Gの部分群 (σ) に対応する K/k の中間体が1の p 乗根をふくむ[10]。このことからKの素元 π を $\sigma(\pi^p)=\pi^p$ および $\tau(\pi^g)=\pi^g$ 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

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

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

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

$$g_j=\frac{1}{g}(1+\zeta^{-j}\tau+\cdots+\zeta^{-(g-1)j}\tau^{g-1}), \qquad j=0,1,\cdots,g-1$$

によって定める。この場合にもθにfと g_j を作用させてみると，$\{f^i g_j(\theta)\}$ が K/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。 $v_K(f^i g_0(\theta))=it+g$，$v_K(f^i g_j(\theta))=it+j$，$j\neq 0$，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

$$\pi_0^{-\nu_i} f^i g_j, \qquad i=0,1,\cdots,p-1\ ;\ j=0,1,\cdots,g-1$$

によって生成され，$\mathfrak{O}$に一致する。ただし，$\nu_i=\left[\frac{ib}{g}\right]$である。

以上のことをまとめると，K/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/kが完全分岐するとき，次の場合にはBは自由$\mathfrak{O}$-加群である。

1) $a=0$

2) $a=1$, $b\equiv 0 \pmod g$ または $a=p-1$, $b\equiv -1 \pmod g$

3) $g=2$, $a \mid 2p-1$, $a\equiv 1 \pmod 4$, $\frac{e}{p-1}-2\leqq t<\frac{e}{p-1}$

4) $p\equiv 1 \pmod 3$, $g=2$, $a=3$, $\frac{e}{p-1}-2\leqq t<\frac{e}{p-1}$

5) $p=5$, $g=2$, $a=3$, $\frac{e}{4}-2\leqq t<\frac{e}{4}$

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

4. K/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. $\frac{t}{p}=a_0+\frac{1}{a_1}+\cdots+\frac{1}{a_r}$, $a_0=b$, $a_r>1$ と連分数に展開したとき，$0\leqq r\leqq 2$ または $3\leqq r\leqq 4$, $\frac{e}{p-1}-1\leqq t<\frac{e}{p-1}$ のときBは自由$\mathfrak{O}$-加群である。逆にBが自由$\mathfrak{O}$-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 $r=1,2$, $\frac{e}{p-1}-1\leqq t<\frac{e}{p-1}$ のときには $r=3,4$ である。

文 献

[1] BERGÉ, 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 diedrale de degré 2p d'un corps local. C. R. Acad. Sci.(A) 274(1972) 1529-1532.

[6] FERTON, M.-J. Sur le ideaux 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'ordere 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.