有理数体上の4元数環の基底と極大整数環

伊吹山 知 義 (東大理)

有理数体上与えられた偶数個の素点が分岐する4元数環，およびその1つの極大整数環の基底を具体的に求めてみた．本質的には新しい内容を含むものではないが，このようにはっきりと述べてある文献も知らないので，何かの参考になればと思い，書きとめておくことにした．結果は次の通り．

定理．∞ が分岐しないとき，相異なる偶数個の正の素数 $p_1, \cdots, p_r$ を指定するとき，$m=p_1\cdots p_r$ とおく．

$q\equiv 5 \bmod 8$ かつ $p_i\neq 2$ なる $p_i|m$ に対して

$$\left(\frac{q}{p_i}\right)=-1$$

となるような正の素数 q をとり，

$$D=\boldsymbol{Q}+\boldsymbol{Q}\alpha+\boldsymbol{Q}\beta+\boldsymbol{Q}\alpha\beta$$

$$\alpha^2=m,\quad \beta^2=q,\quad \alpha\beta=-\beta\alpha$$

とおくとこれはちょうど $p_1, \cdots, p_r$ のみが分岐する4元数環になっている．

$a^2\equiv m \bmod q$ なる整数 a をとるとき，

$$\mathfrak{O}=\boldsymbol{Z}+\boldsymbol{Z}\frac{1+\beta}{2}+\boldsymbol{Z}\frac{\alpha(1+\beta)}{2}+\boldsymbol{Z}\frac{(a+\alpha)\beta}{q}$$

が D の1つの極大整数環を与える．

以上で q の存在は Dirichlet の素数定理．また a の存在は，q のとり方より $(m/q)=1$ が容易(後述)．

∞ が分岐するとき，相異なる奇数個の正の素数 $p_1, \cdots, p_r$ を指定し，$m=p_1\cdots p_r$ とおく．あとは上記の ∞ が分岐しない場合の条件のうちで，すべて $m\to -m$，$q\to -q$ とおけばよい．すなわち，q は，

$$-q\equiv 5 \bmod 8,\ p_i\neq 2 \text{ に対して } (-q/p_i)=-1$$

を満足する正の素数

$$D=\boldsymbol{Q}+\boldsymbol{Q}\alpha+\boldsymbol{Q}\beta+\boldsymbol{Q}\alpha\beta$$

$$\alpha^2=-m,\quad \beta^2=-q,\quad \alpha\beta=-\beta\alpha$$

$a^2\equiv -m \bmod q$ で

$$\mathfrak{O}=\boldsymbol{Z}+\boldsymbol{Z}\frac{1+\beta}{2}+\boldsymbol{Z}\frac{\alpha(1+\beta)}{2}+\boldsymbol{Z}\frac{(a+\alpha)\beta}{q}.$$

注意 1. Hasse の定理より，$\boldsymbol{Q}$ 上の 4 元数環は，$M_2(\boldsymbol{Q})$ を除いて，上に与えたもの以外に存在しない．また類数 1 の 4 元数環，特に不定符号 4 元数環では極大整数環は内部自己同型を除いて，上のもので一意的に決まる．

注意 2. $\mathfrak{D} \supset \boldsymbol{Z}+\boldsymbol{Z}\alpha+\boldsymbol{Z}\beta+\boldsymbol{Z}\alpha\beta$

注意 3. 特殊な場合には，より簡単な基底のとり方がある．例えば

$p \equiv 3 \bmod 4$(素数)および ∞ の 2 点が分岐するとき

$$D=\boldsymbol{Q}+\boldsymbol{Q}\alpha+\boldsymbol{Q}\beta+\boldsymbol{Q}\alpha\beta$$

$$\alpha^2=-p,\quad \beta^2=-1,\quad \alpha\beta=-\beta\alpha$$

$$\mathfrak{D}=\boldsymbol{Z}+\boldsymbol{Z}\beta+\boldsymbol{Z}\frac{1+\alpha}{2}+\boldsymbol{Z}\frac{\beta(1+\alpha)}{2}$$

2 および ∞ が分岐するとき

$$D=\boldsymbol{Q}+\boldsymbol{Q}\alpha+\boldsymbol{Q}\beta+\boldsymbol{Q}\alpha\beta$$

$$\alpha^2=\beta^2=-1,\quad \alpha\beta=-\beta\alpha$$

$$\mathfrak{D}=\boldsymbol{Z}+\boldsymbol{Z}\alpha+\boldsymbol{Z}\beta+\boldsymbol{Z}\frac{1+\alpha+\beta+\alpha\beta}{2}$$

ととることができる．

証明．以下，不定符号 4 元数環の場合のみ証明する．(定符号でも全く同様)

1. D が指定された分岐を持つこと．

Hilbert 記号を使えば簡単に検証できるが，ここでは直接証明する．$\xi=x+y\alpha+z\beta+w\alpha\beta \in D$ に対して，(被約ノルム)$=n(\xi)=x^2-my^2-qz^2+mqw^2$ とおく．$D_p=D\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{Q}_p \ni \xi_p$ に対して，

$$D_p \text{ が division} \Longleftrightarrow n(\xi_p)\neq 0 \text{ for } \forall \xi_p \neq 0$$

(0)　もちろん ∞ は分岐しない．

(1)　一般に

$p\neq 2$ なら $\boldsymbol{Q}_p(\sqrt{q})/\boldsymbol{Q}_p$ が不分岐 2 次拡大

$$\Longleftrightarrow (q/p)=-1,\quad (q,p)=1$$

$p=2$ なら $\boldsymbol{Q}_p(\sqrt{q})/\boldsymbol{Q}_p$ が不分岐 2 次拡大

$$\Longleftrightarrow q\equiv 5 \bmod 8.$$

よって上の q および $p|m$ に対して，$\boldsymbol{Q}_p(\sqrt{q})/\boldsymbol{Q}_p$ は不分岐 2 次拡大，m は $\boldsymbol{Q}_p$ の素元だから，これらできまる $\boldsymbol{Q}_p$ 上の巡回多元環 D_p は division である．

$$\therefore\quad p|m \text{ なら，} D_p \text{ は division}$$

(2)　$p\nmid m$ に対して，$n(\xi_p)=0$，$\xi_p\neq 0$ なる解，$\xi_p\in D_p$ があることをいう．

$p\nmid m$，$p\neq 2$，q で $(q/p)=1$ のとき，$x^2-q=0$ なる $x\in \boldsymbol{Q}_p$ がある．

$p\nmid m$ で $p=2$ または $p\neq q$ かつ $(q/p)=-1$ なら，m が $\boldsymbol{Q}_p$ の単数，$\boldsymbol{Q}_p(\sqrt{q})/\boldsymbol{Q}_p$ は不分岐 2 次拡大より，局所類体論によって，$x^2-qy^2=m$ なる解 $x,y\in\boldsymbol{Q}_p$ がある．よって $p\nmid m$，$p\neq q$ のときは p は分岐しない．$p=q$ の時，Hasse の和定理によって分岐しないことは以上よりあきらかだが直接証明する．

$(m/q)=1$ なら，$x^2-m=0$ なる $x\in\boldsymbol{Q}_p$ があるので分岐しない．よってこれを示す．

$p_i|m$，$p_i\neq 2$ の時

$$\left(\frac{p_i}{q}\right)\left(\frac{q}{p_i}\right)=(-1)^{\frac{p_i-1}{2}\cdot\frac{q-1}{2}}=1$$

$$\therefore\quad \left(\frac{p_i}{q}\right)=-1$$

$p_i=2$ の時

$$\left(\frac{2}{q}\right)=(-1)^{\frac{q^2-1}{8}}=-1$$

よって

$$\left(\frac{m}{q}\right)=\left(\frac{p_1}{q}\right)\cdots\cdots\left(\frac{p_r}{q}\right)=(-1)^r=1.$$

よって D はちょうど指定された分岐をもつ $\boldsymbol{Q}$ 上の 4 元数環である．またこれで $a^2\equiv m \bmod q$ なる a の存在もいえた．

2. $\mathfrak{D}$ が D の 1 つの極大整数環を与えること．

$\mathfrak{D}\ni 1$，また $\boldsymbol{Z}$ 上有限生成かつ D の $\boldsymbol{Q}$ 上の基底を含む．よって $\mathfrak{D}$ が整数環であることをいうには，部分環であることをいえばよい．また極大整数環の判別式は，一般論より，$m^2\boldsymbol{Z}$ になるから，

$$\mathfrak{D} \text{ が極大} \Longleftrightarrow \mathfrak{D} \text{ の判別式}=m^2\boldsymbol{Z}.$$

これらを

$$\mathfrak{D}=\boldsymbol{Z}+\boldsymbol{Z}\frac{1+\beta}{2}+\boldsymbol{Z}\frac{\alpha(1+\beta)}{2}+\boldsymbol{Z}\frac{(a+\alpha)\beta}{q}$$

について確かめればよい．

	ω_1	ω_2	ω_3	ω_4
ω_2^2	$\frac{q-1}{4}$	1	0	0
$\omega_2\omega_3$	$\frac{-a(1-q)}{4}$	$\frac{a(1-q)}{2}$	$\frac{1-q}{2}$	$\frac{q(q-1)}{4}$
$\omega_2\omega_4$	a	$-a$	-1	$\frac{q+1}{2}$
$\omega_3\omega_2$	$\frac{a(1-q)}{4}$	$\frac{a(q-1)}{2}$	$\frac{q+1}{2}$	$\frac{q(1-q)}{4}$
ω_3^2	$\frac{m(1-q)}{4}$	0	0	0
$\omega_3\omega_4$	$-m+\frac{(1-q)(a^2-m)}{2q}$	$a^2-\frac{a^2-m}{q}$	a	$\frac{a(1-q)}{2}$
$\omega_4\omega_2$	0	a	1	$\frac{1-q}{2}$
$\omega_4\omega_3$	$\frac{(q-1)(a^2-m)}{2q}$	$\frac{a^2-m}{q}-a^2$	$-a$	$\frac{a(1-q)}{2}$
ω_4^2	$\frac{a^2-m}{q}$	0	0	0

$$\omega_1=1,\ \ \omega_2=\frac{1+\beta}{2},\ \ \omega_3=\frac{\alpha(1+\beta)}{2},\ \ \omega_4=\frac{(a+\alpha)\beta}{q}$$

とおく．念のため前頁に表をかかげておく．表の右側は左の数を ω_i の 1 次結合で表わした時の係数を示す．

前表によって，$a^2\equiv m \bmod q$，$q\equiv 5 \bmod 8$ に注意すれば，これらの係数がすべて整数であることより，$\mathfrak{O}$ は部分環であることがわかる．また，$\mathrm{tr}\,(\omega_1)=2$, $\mathrm{tr}\,(\omega_2)=1$, $\mathrm{tr}\,(\omega_3)=\mathrm{tr}\,(\omega_4)=0$ に注意して，

$$(\mathfrak{O}\text{ の判別式})=\begin{vmatrix} 2 & 1 & & 0 \\ 1 & \dfrac{q+1}{2} & 0 & a \\ 0 & 0 & \dfrac{m(1-q)}{2} & -m \\ 0 & a & -m & \dfrac{2(a^2-m)}{q} \end{vmatrix}=-m^2$$

よって $\mathfrak{O}$ は極大整数環である．(証明おわり)

(1972 年 1 月 24 日提出)