２次体の整数環について　（平成２６年）

定義　$O_K = \{ \alpha \in K \mid T(\alpha) \in Z,\ N(\alpha) \in Z \}$　を２次体 K の整数環という.
O_K の元を整数という.

（注）$T(\alpha)$ ：α のトレース, $N(\alpha)$ ：α のノルム

補助定理　$\alpha \in K,\ \alpha^2 \in O_K$ なら　$\alpha \in O_K$

証明　$\alpha^2 \in O_K$ だから, $N(\alpha^2),\ T(\alpha^2) \in Z$

$N(\alpha)^2 = N(\alpha^2)$ だから, $N(\alpha) \in Z$

$T(\alpha)^2 = T(\alpha^2) + 2N(\alpha)$ より, $T(\alpha) \in Z$

$\therefore\ \alpha \in O_K$

系　m ：平方因子を含まない有理整数

$\alpha^2 m \in O_K$, なら $\alpha \in O_K$

定理　$K = Q(\sqrt{m})$ ：２次体, m ：平方因子を含まない有理整数

$$O_k = \begin{cases} \left[1,\ \sqrt{m}\ \right] & m \equiv 2,\ 3\ (\ mod\ 4\ ) \\ \left[1,\ \dfrac{1 + \sqrt{m}}{2}\right] & m \equiv 1\ (mod\ 4\ ) \end{cases}$$

証明１　$\alpha = a + b\sqrt{m} \qquad a,\ b \in Q$

$T(\alpha) = 2a,\quad N(\alpha) = a^2 - b^2 m$

$\alpha \in O_K \Rightarrow 2a \in Z,\ a^2 - b^2 m \in Z$

$\Rightarrow 4a^2 - 4b^2 m \in Z$

$\Rightarrow (2b)^2 m \in Z$

m は平方因子を含まないから, 系より

$2b \in Z$

$\therefore\ 2a,\ 2b \in Z$

$2a = u,\quad 2b = v$ とおくと

$u,\ v \in Z,\ u^2 - m v^2 \equiv 0\ (\ mod\ 4\ ),$

$u \equiv v\ (\ mod\ 2\ )$

$\therefore\ a,\ b \in Z$

(1) $u \equiv v \equiv 1 \pmod 2$ のとき $m \equiv 1 \pmod 4$

$$\alpha = a + b\sqrt{m} = \frac{u + v\sqrt{m}}{2}$$

$$= \frac{u - v}{2} + v\,\frac{1 + \sqrt{m}}{2} \in \left[1,\ \frac{1 + \sqrt{m}}{2}\right]$$

(2) $m \equiv 2, 3 \pmod 4$ のとき $u \equiv v \equiv 0 \pmod 2$

$$\therefore\ a,\ b \in \mathrm{Z}$$

よって $\alpha = \left[1,\ \sqrt{m}\right]$

証明２

(1) $m \equiv 2, 3 \pmod 4$ のとき

$\mathrm{Z}[\omega] = \mathrm{Z}\left[\sqrt{m}\right] = \left\{a + b\sqrt{m}\right\}$ $(a, b \in \mathrm{Z})$

$\mathrm{T}(a + b\sqrt{m}) = 2a \in \mathrm{Z}$

$\mathrm{N}(a + b\sqrt{m}) = a^2 - b^2 m \in \mathrm{Z}$

$\therefore\ \mathrm{Z}[\omega] \subset \mathrm{O_K}$ ……①

逆に $\alpha \in \mathrm{O_K}$ とする

$\alpha = a + b\sqrt{m}$ $(a, b \in \mathrm{Q})$

$\mathrm{T}(\alpha) = 2a \in \mathrm{Z}$

$\mathrm{N}(\alpha) = a^2 - m b^2 \in \mathrm{Z}$

$\therefore\ (2a)^2 - m(2b)^2 \in \mathrm{Z}$

$m(2b)^2 \in \mathrm{Z}$ $\therefore\ 2b \in \mathrm{Z}$

$\therefore\ 2a,\ 2b \in \mathrm{Z}$

$a,\ b \in \mathrm{Z}$

$\because\ 2a = u,\ 2n = v$ とおくと

$$a^2 - mb^2 = \frac{u^2 - mv^2}{4} \in \mathrm{Z}$$

$u^2 - mv^2 \equiv 0 \pmod 4$ また $m \not\equiv 0 \pmod 2$

$\therefore\ u \equiv v \equiv 0 \pmod 2$

u, v : 偶数 $\therefore\ a,\ b \in \mathrm{Z}$

$\therefore\ \mathrm{Z}[\omega] \supset \mathrm{O_K}$ ……②

①②より

$\mathrm{Z}[\omega] = \mathrm{O_K}$

(2)　$m \equiv 1 \pmod 4$ のとき

$$\mathrm{Z}[\omega] = \left\{ k + \frac{1+\sqrt{m}}{2} l \right\} \quad (k,\ l \in \mathrm{Z})$$

$$= \left\{ \frac{(2k+l) + \sqrt{m}\, l}{2} \right\}$$

$$\mathrm{T}\left(k + \frac{1+\sqrt{m}}{2} l \right) = 2k + l \in \mathrm{Z}$$

$$\mathrm{N}\left(k + \frac{1+\sqrt{m}}{2} l \right) = \left(\frac{2k+l}{2} \right)^2 - m \left(\frac{l}{2} \right)^2$$

$$= \frac{(2k+l)^2 - m\, l^2}{4} \in \mathrm{Z}$$

$\because\ m \equiv 1 \pmod 4$ だから

$$(2k+l)^2 - m\, l^2 \equiv (2k+l)^2 - l^2 \equiv 0 \pmod 4$$

$\therefore\ \mathrm{Z}[\omega] \subset \mathrm{O_K}$ ……③

逆に　$\alpha \in \mathrm{O_K}$ をとると,

$$\alpha = a + b\sqrt{m} \quad (a,\ b \in \mathrm{Q})$$

$\mathrm{T}(\alpha) = 2a \in \mathrm{Z}$

$\mathrm{N}(\alpha) = a^2 - m\, b^2 \in \mathrm{Z}$

$\therefore\ m\, b^2 \in \mathrm{Z}$

$\therefore\ b \in \mathrm{Z}$

$m \equiv 1 \pmod 4$ より,

$$u^2 - m\, v^2 \equiv u^2 - v^2 \pmod 4$$

$\therefore\ u \equiv v \pmod 2$

$\therefore\ a \in \mathrm{Z}$

$\therefore\ \mathrm{Z}[\omega] \supset \mathrm{O_K}$ ……④

③④　より,

$$\mathrm{Z}[\omega] = \mathrm{O_K}$$

引用文献

1.　数論序説　　小野　孝　著　　裳華房　　１９８８

2.　素数と２次体の整数論　　青木　昇　著　　共立出版　　２０１３