2次体の整数論

MATHEMATICS.PDF

2011-01-13

目 次

1　代数的整数

複素数 α が**代数的数**であるとは, ある定数でない $\mathbb{Q}$ 係数多項式 $f(X)$ が存在して $f(\alpha)=0$ が成り立つときにいう. 特に, $f(X)$ がモニック (すなわち, 最高次係数が 1) かつ $\mathbb{Z}$ 係数であるときには, α を**代数的整数**という. 代数的数の全体を $\overline{\mathbb{Q}}$, 代数的整数の全体を $\overline{\mathbb{Z}}$ で表す. 定義から明らかに, $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$ が成り立つ.

代数的整数のことも単に整数と呼ぶことがあるため, $\mathbb{Z}$ の元のほうを**有理整数**と呼んで区別する.

a を有理数とすると, a は 1 次多項式 $X-a$ の根である. このことは, a が代数的数であることを意味し, 特に a が有理整数のときには代数的整数であることを示している. よって, $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ および $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$ が成り立つ.

[定理 1.1] $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

[証明] ($\subseteq$)　$\alpha \in \mathbb{Q} \cap \overline{\mathbb{Z}}$ とする. $\alpha \in \mathbb{Q}$ より, α を既約分数として表すことができる:

$$\alpha = \frac{c}{d}, \quad c,\, d \in \mathbb{Z}, \quad d > 0, \quad \gcd(c,d) = 1.$$

また, $\alpha \in \overline{\mathbb{Z}}$ より, ある $a_0,\, a_1,\, \ldots,\, a_{n-1} \in \mathbb{Z}$ が存在して,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

すなわち,

$$\left(\frac{c}{d}\right)^n + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + \cdots + a_1\left(\frac{c}{d}\right) + a_0 = 0.$$

分母を払うと,

$$c^n = -d(a_{n-1}c^{n-1} + \cdots + a_1 c d^{n-2} + a_0 d^{n-1}).$$

これより, $d \mid c^n$. もし仮に $d > 1$ とすれば, d のある素因子 p が存在して $p \mid c^n$, したがって $p \mid c$ となる. これは $\gcd(c,d) = 1$ に反する. ゆえに, $d = 1$. すなわち, $\alpha \in \mathbb{Z}$.

($\supseteq$)　$\mathbb{Z} \subseteq \mathbb{Q}$ かつ $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$ より明らか. □

[定理 1.2] 任意の $\alpha \in \overline{\mathbb{Q}}$ に対して, ある有理整数 $a > 0$ が存在して, $a\alpha \in \overline{\mathbb{Z}}$.

[証明] 仮定より, ある $a_0,\, a_1,\, \ldots,\, a_n \in \mathbb{Q}$ が存在して,

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

が成り立つ. $a_n < 0$ のときには各 a_i を $-a_i$ に置き換えればよいから, $a_n > 0$ と仮定してもよい. a_i の分母の最小公倍数を $l > 0$ とし, $b_i = la_i$ とおくと,

$$b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0, \quad b_i \in \mathbb{Z}, \quad b_n > 0$$

となる. 両辺に b_n^{n-1} を掛けると,

$$b_n^{n-1}(b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0) = 0.$$

よって,

$$(b_n\alpha)^n + b_{n-1}(b_n\alpha)^{n-1} + \cdots + b_1 b_n^{n-2}(b_n\alpha) + b_0 b_n^{n-1} = 0.$$

したがって, $b_n\alpha \in \overline{\mathbb{Z}}$. □

[補題 1.3] $\gamma_1, \gamma_2, \ldots, \gamma_m \in \mathbb{C}$ とし, 少なくとも 1 つは 0 でないとする. また,

$$M = \left\{ \sum_{i=1}^{m} c_i\gamma_i \;\middle|\; c_i \in \mathbb{Z} \right\}$$

とおく. このとき, 任意の $\alpha \in \mathbb{C}$ に対して,

$$\alpha M \subseteq M \Longrightarrow \alpha \in \overline{\mathbb{Z}}$$

が成り立つ.

[証明] $\alpha \in \mathbb{C}$ とし, $\alpha M \subseteq M$ とすると, 各 i に対して,

$$\alpha\gamma_i = \sum_{j=1}^{m} a_{ij}\gamma_j, \quad a_{ij} \in \mathbb{Z}.$$

$A = (a_{ij})$, $\boldsymbol{p} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{bmatrix}$ とおくと, A は $\mathbb{Z}$ 成分の m 次正方行列であり,

$$A\boldsymbol{p} = \alpha\boldsymbol{p}, \quad \boldsymbol{p} \neq \boldsymbol{0}.$$

すなわち, α は A の固有値である. ゆえに, α は A の固有多項式 $\det(xE - A)$ の根であり, その固有多項式は最高次係数が 1 であるような m 次 $\mathbb{Z}$ 係数多項式である. したがって, $\alpha \in \overline{\mathbb{Z}}$. □

[定理 1.4] $\overline{\mathbb{Z}}$ は $\mathbb{C}$ の部分整域である. $\overline{\mathbb{Z}}$ を**代数的整数環**という.

[証明] まず, $\overline{\mathbb{Z}}$ が空集合でないことは明らかである.

$\alpha, \beta \in \overline{\mathbb{Z}}$ を任意にとる. α に対して, ある $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ が存在して,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0. \tag{1}$$

同様に, β に対して, ある $b_0, b_1, \ldots, b_{m-1} \in \mathbb{Z}$ が存在して,

$$\beta^m + b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0 = 0.$$

また, α, β に対して,

$$M = \left\{ \sum_{j=0}^{m-1} \left(\sum_{i=0}^{n-1} c_{ij}\alpha^i \right) \beta^j \;\middle|\; c_{ij} \in \mathbb{Z} \right\}$$

とおく. M は, $\alpha^i\beta^j$ $(0 \leq i \leq n-1, 0 \leq j \leq m-1)$ の $\mathbb{Z}$ 係数の 1 次結合で表されるものの全体である. $\gamma \in M$ を任意にとる. すると,

$$\gamma = \sum_{j=0}^{m-1} \left(\sum_{i=0}^{n-1} c_{ij}\alpha^i \right) \beta^j, \quad c_{ij} \in \mathbb{Z}$$

と表せる. このとき,

$$\begin{aligned} \alpha\gamma &= \sum_{j=0}^{m-1} \left(\sum_{i=0}^{n-1} c_{ij}\alpha^{i+1} \right) \beta^j \\ &= \sum_{j=0}^{m-1} \left(\sum_{i=1}^{n-1} c_{i-1,j}\alpha^i \right) \beta^j + \sum_{j=0}^{m-1} c_{n-1,j}\alpha^n\beta^j. \end{aligned}$$

(1) より $\alpha^n = \sum_{i=0}^{n-1}(-a_i)\alpha^i$ であるから,

$$\begin{aligned} \sum_{j=0}^{m-1} c_{n-1,j}\alpha^n\beta^j &= \sum_{j=0}^{m-1} c_{n-1,j} \left(\sum_{i=0}^{n-1}(-a_i)\alpha^i \right) \beta^j \\ &= \sum_{j=0}^{m-1} \left(\sum_{i=0}^{n-1}(-a_ic_{n-1,j})\alpha^i \right) \beta^j. \end{aligned}$$

ゆえに,

$$\alpha\gamma = \sum_{j=0}^{m-1} \left(\sum_{i=0}^{n-1} c'_{ij}\alpha^i \right) \beta^j, \quad c'_{ij} \in \mathbb{Z}.$$

ただし,

$$c'_{ij} = \begin{cases} -a_0c_{n-1,j}, & i = 0 \text{ のとき} \\ c_{i-1,j} - a_ic_{n-1,j}, & 1 \leq i \leq n-1 \text{ のとき} \end{cases}$$

とおく. したがって, $\alpha M \subseteq M$ が成り立つ. 同様にして, $\beta M \subseteq M$ が成り立つこともいえる. これらから,

$$\begin{aligned} (\alpha - \beta)M \subseteq \alpha M - \beta M \subseteq M - M \subseteq M, \\ (\alpha\beta)M = \alpha(\beta M) \subseteq \alpha M \subseteq M. \end{aligned}$$

$\alpha^1\beta^0 = \alpha \neq 0$ のとき, $\alpha^i\beta^j$ $(0 \leq i \leq n-1, 0 \leq j \leq m-1)$ のうち少なくとも 1 つは 0 でないから, 補題 1.3 より,

$$\alpha - \beta,\ \alpha\beta \in \overline{\mathbb{Z}}. \tag{2}$$

$\alpha^0\beta^1 = \beta \neq 0$ のときも同様である. $\alpha = \beta = 0$ のとき, (2) が成り立つことは明らかである. ゆえに, $\overline{\mathbb{Z}}$ は $\mathbb{C}$ の部分環である.

一般に, 体は整域であり, 整域の部分環は整域である. したがって, $\overline{\mathbb{Z}}$ は整域である. □

[補題 1.5] $\mathbb{Q}\cdot\overline{\mathbb{Z}}\subseteq\overline{\mathbb{Q}}$.

[証明] $r\in\mathbb{Q}$, $\alpha\in\overline{\mathbb{Z}}$ とする. $\alpha\in\overline{\mathbb{Z}}$ より, ある a_0, a_1, …, $a_{n-1}\in\mathbb{Z}$ が存在して,

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0.$$

両辺に r^n を掛けると,

$$r^n(\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0)=0.$$

よって,

$$(r\alpha)^n+a_{n-1}r(r\alpha)^{n-1}+\cdots+a_1r^{n-1}(r\alpha)+a_0r^n=0.$$

したがって, $r\alpha\in\overline{\mathbb{Q}}$. □

[注意 1.1] この時点ではまだ $\overline{\mathbb{Q}}$ が体であること (特に, 積について閉じていること) を証明していないため, $\mathbb{Q}\subseteq\overline{\mathbb{Q}}$ と $\overline{\mathbb{Z}}\subseteq\overline{\mathbb{Q}}$ とから直ちに $\mathbb{Q}\cdot\overline{\mathbb{Z}}\subseteq\overline{\mathbb{Q}}$ とはいかない.

[定理 1.6] $\overline{\mathbb{Q}}$ は $\mathbb{C}$ の部分体である. $\overline{\mathbb{Q}}$ を**代数的数体**という.

[証明] α, $\beta\in\overline{\mathbb{Q}}$ とする. 定理 1.2 より, ある有理整数 $a>0$, $b>0$ が存在して $a\alpha$, $b\beta\in\overline{\mathbb{Z}}$ となる. $\mathbb{Z}\subseteq\overline{\mathbb{Z}}$ および $\overline{\mathbb{Z}}$ が環であること (定理 1.4) から,

$$ab\alpha=b(a\alpha)\in\overline{\mathbb{Z}},$$
$$ab\beta=a(b\beta)\in\overline{\mathbb{Z}}.$$

ゆえに, 再び $\overline{\mathbb{Z}}$ が環であることから,

$$ab(\alpha-\beta)=ab\alpha-ab\beta\in\overline{\mathbb{Z}}.$$

補題 1.5 により,

$$\alpha-\beta=\frac{1}{ab}\cdot ab(\alpha-\beta)\in\overline{\mathbb{Q}}.$$

また, 再び $\overline{\mathbb{Z}}$ が環であることから,

$$ab(\alpha\beta)=(a\alpha)(b\beta)\in\overline{\mathbb{Z}}.$$

再び補題 1.5 により,

$$\alpha\beta=\frac{1}{ab}\cdot ab(\alpha\beta)\in\overline{\mathbb{Q}}.$$

以上より, $\overline{\mathbb{Q}}$ が $\mathbb{C}$ の部分環であることが示された.

$\alpha\in\overline{\mathbb{Q}}$, $\alpha\neq0$ とすると, ある a_0, a_1, …, $a_n\in\mathbb{Q}$ が存在して,

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0,\quad a_n\neq0.$$

$a_0 = 0$ のときは両辺を α で割ればよいから, $a_0 \neq 0$ と仮定してもよい. 両辺に α^{-n} を掛けると,

$$a_n + a_{n-1}\alpha^{-1} + \cdots + a_1(\alpha^{-1})^{n-1} + a_0(\alpha^{-1})^n = 0.$$

ゆえに, $\alpha^{-1} \in \overline{\mathbb{Q}}$. したがって, $\overline{\mathbb{Q}}$ の 0 でないすべての元は $\overline{\mathbb{Q}}$ において逆元をもつ. □

[定理 1.7] $\overline{\mathbb{Q}}$ は $\overline{\mathbb{Z}}$ の商体である.

[証明] 以下のことを証明すればよい.

(i) $\overline{\mathbb{Q}}$ は体である.
(ii) $\overline{\mathbb{Z}}$ は $\overline{\mathbb{Q}}$ の部分整域である.
(iii) 任意の $\alpha \in \overline{\mathbb{Q}}$ に対して, ある $\beta, \gamma \in \overline{\mathbb{Z}}$ が存在して, $\alpha = \beta/\gamma$, $\gamma \neq 0$.

定理 1.6 より, $\overline{\mathbb{Q}}$ は $\mathbb{C}$ の部分体である. よって, (i) が成り立つ.

定理 1.4 より, $\overline{\mathbb{Z}}$ は $\mathbb{C}$ の部分整域である. $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$ であるから, (ii) が成り立つ.

$\alpha \in \overline{\mathbb{Q}}$ とすると, 定理 1.2 より, ある有理整数 $a > 0$ が存在して $a\alpha \in \overline{\mathbb{Z}}$ となる. $\beta = a\alpha$ とおくと, $\alpha = \beta/a$ である. よって, (iii) が成り立つ. □

2 2 次体

$\mathbb{C}$ の部分体 K が**代数体**であるとは, $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$ であり, $\mathbb{Q}$ 上のベクトル空間として有限次元であるときにいう. ここで, スカラー倍は積によって定めるものとする. $[K : \mathbb{Q}] = \dim_{\mathbb{Q}} K$ とおき, これを代数体 K の $\mathbb{Q}$ 上の**次数**という. $[K : \mathbb{Q}] = n$ のとき, K は n 次体であるという. 特に, $[K : \mathbb{Q}] = 2$ のとき, K を **2 次体**という.

有理整数 m に対して,

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$$

とおく. 定義より明らかに $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{m})$ である.

[補題 2.1] m を有理整数とする. このとき, $\sqrt{m}$ が有理数ならば, m は 0 または平方数である.

[証明] $\sqrt{m} \in \mathbb{Q}$ とすると, $\sqrt{m}$ は既約分数として表される:

$$\sqrt{m} = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b > 0, \quad \gcd(a, b) = 1.$$

このとき,

$$b^2 m = a^2.$$

$a^2 \geq 0$, $b^2 \geq 0$ なので, $m \geq 0$ である.

いま, $m \neq 0$ と仮定し, $|a|$, b, m の素因数分解

$$|a| = \prod_{i=1}^{r} p_i^{e_i}, \quad b = \prod_{i=1}^{r} p_i^{f_i}, \quad m = \prod_{i=1}^{r} p_i^{g_i}, \quad e_i,\, f_i,\, g_i \geq 0$$

を考えると, 分解の一意性により,

$$2f_i + g_i = 2e_i \quad (i = 1, 2, \ldots, r).$$

ゆえに, g_1, g_2, …, g_r はすべて偶数でなければならない. したがって, m は平方数である. □

[定理 2.2] m を 0 でも平方数でもない有理整数とする. このとき, 任意の a, b, c, $d \in \mathbb{Q}$ に対して,

$$a + b\sqrt{m} = c + d\sqrt{m} \Longleftrightarrow a = c,\, b = d$$

が成り立つ.

[証明] $a' = a - c$, $b' = b - d$ とおくと,

$$\begin{aligned} a = c,\, b = d &\Longleftrightarrow a - c = b - d = 0 \\ &\Longleftrightarrow a' = b' = 0. \end{aligned}$$

一方,

$$\begin{aligned} a + b\sqrt{m} = c + d\sqrt{m} & \\ &\Longleftrightarrow (a - c) + (b - d)\sqrt{m} = 0 \\ &\Longleftrightarrow a' + b'\sqrt{m} = 0. \end{aligned}$$

さらに,

$$a' = b' = 0 \Longrightarrow a' + b'\sqrt{m} = 0$$

は明らかである. したがって,

$$a' + b'\sqrt{m} = 0 \Longrightarrow a' = b' = 0$$

を示せば十分である.

$a' + b'\sqrt{m} = 0$ とする. もし仮に $b' \neq 0$ とすると,

$$\sqrt{m} = -\frac{a'}{b'} \in \mathbb{Q}.$$

補題 2.1 より, m は 0 または平方数である. これは定理の仮定に反する. ゆえに, $b' = 0$ でなければならない. $a' + b'\sqrt{m} = 0$ より $a' = 0$ もいえる. □

任意の $a, b \in \mathbb{Q}$ に対して,

$$a + b\sqrt{m} \in \mathbb{Q} \Longleftrightarrow b = 0$$

が成り立つ. なぜなら, $(\Rightarrow)$ については, $a, b \in \mathbb{Q}$ とし, $a + b\sqrt{m} \in \mathbb{Q}$ であるとすると, ある $c \in \mathbb{Q}$ が存在して, $a + b\sqrt{m} = c$ となる. 定理 2.2 より, $b = 0$ が得られる. $(\Leftarrow)$ は明らかである.

[補題 2.3] $\mathbb{Q}(\sqrt{m}) \subseteq \overline{\mathbb{Q}}$. ただし, m は有理整数であるとする.

[証明] $\alpha \in \mathbb{Q}(\sqrt{m})$ とすると,

$$\alpha = a + b\sqrt{m}, \quad a, b \in \mathbb{Q}$$

と表せる. 両辺に $-a$ を加えて 2 乗すると,

$$(\alpha - a)^2 = b^2 m.$$

左辺を展開して整理すると,

$$\alpha^2 - 2a\alpha + a^2 - b^2 m = 0.$$

ゆえに, $\alpha \in \overline{\mathbb{Q}}$. したがって, $\mathbb{Q}(\sqrt{m}) \subseteq \overline{\mathbb{Q}}$. □

[定理 2.4] m を 0 でも平方数でもない有理整数とする. このとき, $\mathbb{Q}(\sqrt{m})$ は 2 次体である. 特に, $\mathbb{Q}(\sqrt{m})$ は $\mathbb{Q}$ 上のベクトル空間であり, 1, $\sqrt{m}$ はその $\mathbb{Q}$ 上の基底である.

[証明] $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{m})$ は明らか. 特に, $\mathbb{Q}(\sqrt{m})$ は空集合でない. また, 補題 2.3 より, $\mathbb{Q}(\sqrt{m}) \subseteq \overline{\mathbb{Q}}$.

$\alpha, \beta \in \mathbb{Q}(\sqrt{m})$ とし,

$$\alpha = a + b\sqrt{m}, \quad a, b \in \mathbb{Q},$$
$$\beta = c + d\sqrt{m}, \quad c, d \in \mathbb{Q}$$

とおくと,

$$\alpha - \beta = (a - c) + (b - d)\sqrt{m} \in \mathbb{Q}(\sqrt{m}),$$
$$\alpha\beta = (ac + bdm) + (ad + bc)\sqrt{m} \in \mathbb{Q}(\sqrt{m}).$$

したがって, $\mathbb{Q}(\sqrt{m})$ は $\overline{\mathbb{Q}}$ の部分環である.

$\alpha = a + b\sqrt{m} \neq 0$ のとき, 定理 2.2 より $a - b\sqrt{m} \neq 0$ だから,

$$a^2 - mb^2 = (a + b\sqrt{m})(a - b\sqrt{m}) \neq 0.$$

よって,

$$\begin{aligned}\alpha^{-1} &= \frac{1}{a + b\sqrt{m}} = \frac{a - b\sqrt{m}}{(a + b\sqrt{m})(a - b\sqrt{m})} \\ &= \frac{a}{a^2 - mb^2} - \frac{b}{a^2 - mb^2}\sqrt{m} \in \mathbb{Q}(\sqrt{m}).\end{aligned}$$

ゆえに, α は $\mathbb{Q}(\sqrt{m})$ において逆元をもつ. したがって, $\mathbb{Q}(\sqrt{m})$ は体である.

$\mathbb{Q}(\sqrt{m})$ は $\mathbb{Q}$ を部分体として含むので, $\mathbb{Q}$ 上のベクトル空間をなす. $\mathbb{Q}(\sqrt{m})$ が 1, $\sqrt{m}$ によって $\mathbb{Q}$ 上生成されることは $\mathbb{Q}(\sqrt{m})$ の定義より明らかである. また, 定理 2.2 より, 1, $\sqrt{m}$ は $\mathbb{Q}$ 上 1 次独立である. ゆえに, 1, $\sqrt{m}$ は $\mathbb{Q}(\sqrt{m})$ の $\mathbb{Q}$ 上の基底である. よって, $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{m}) = 2$.

以上より, $\mathbb{Q}(\sqrt{m})$ が 2 次体であることが示された. □

[補題 2.5] 任意の $a \in \mathbb{Q} \setminus \mathbb{Q}^2$ に対して, ある $t \in \mathbb{Q}^\times$, $m \in \mathbb{Z}$ が存在して,

$$a = t^2 m, \quad m \neq 0, 1, \quad m \text{ は平方因子を含まない}$$

となる.

[証明] a を既約分数で表す:

$$a = \frac{b}{c}, \quad b, c \in \mathbb{Z}, \quad c > 0, \quad \gcd(b, c) = 1.$$

さらに,

$$b = b_1^2 b_2, \quad b_2 \text{ は平方因子を含まない},$$
$$c = c_1^2 c_2, \quad c_2 \text{ は平方因子を含まない}$$

とおく. $t = b_1/c_1 c_2$, $m = b_2 c_2$ とおくと, $a = t^2 m$ となる. $a \notin \mathbb{Q}^2$ より, $m \neq 1$. 再び $a \notin \mathbb{Q}^2$ より, $a \neq 0$ だから, $t \neq 0$, $m \neq 0$. また, b_2, c_2 はともに平方因子を含まない有理整数であり, $\gcd(b_2, c_2) = 1$ であるから, m もまた平方因子を含まない有理整数である. □

[定理 2.6] 任意の 2 次体 K に対して, ある有理整数 m が存在して, $K = \mathbb{Q}(\sqrt{m})$ が成り立つ. しかも, m として, 0, 1 と異なり, かつ平方因子を含まないものがとれる.

[証明] K は 2 次体だから, $\mathbb{Q} \subseteq K$. また, $\alpha \in K \setminus \mathbb{Q}$ とすると, $\dim_{\mathbb{Q}} K = 2$ より, 1, α, α^2 は $\mathbb{Q}$ 上 1 次従属である. よって, ある a, b, $c \in \mathbb{Q}$ が存在して,

$$a\alpha^2 + b\alpha + c = 0.$$

もし仮に $a = 0$ とすると, $b\alpha + c = 0$ となり, $b = 0$ ならば $c = 0$ となって α が $\mathbb{Q}$ 上 1 次従属であることに反し, $b \neq 0$ ならば $\alpha = -c/b$ となって $\alpha \notin \mathbb{Q}$ に反する. ゆえに, $a \neq 0$ である. $D = b^2 - 4ac$ とおくと, 2 次方程式の解の公式により,

$$\alpha = \frac{-b \pm \sqrt{D}}{2a}.$$

$\alpha \notin \mathbb{Q}$ より, $D \notin \mathbb{Q}^2$. 補題 2.5 より, ある $t \in \mathbb{Q}^\times$, $m \in \mathbb{Z}$ が存在して,

$$D = t^2 m, \quad m \neq 0, 1, \quad m \text{ は平方因子を含まない}$$

となる. このとき,

$$\alpha = \frac{-b \pm \sqrt{t^2 m}}{2a} = -\frac{b}{2a} \pm \frac{t}{2a}\sqrt{m} \in \mathbb{Q}(\sqrt{m}).$$

したがって, $K = \mathbb{Q} \cup (K \setminus \mathbb{Q}) \subseteq \mathbb{Q}(\sqrt{m})$. 定理 2.6 より, $\mathbb{Q}(\sqrt{m})$ は 2 次体である. よって, K は $\mathbb{Q}(\sqrt{m})$ の $\mathbb{Q}$ 上の部分ベクトル空間であり,

$$\dim_{\mathbb{Q}} K = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{m}) = 2$$

であるから, $K = \mathbb{Q}(\sqrt{m})$. □

[定理 2.7] m, m' はともに 0, 1 と異なり平方因子を含まない有理整数とする. このとき,

$$m \neq m' \Longrightarrow \mathbb{Q}(\sqrt{m}) \cap \mathbb{Q}(\sqrt{m'}) = \mathbb{Q}$$

が成り立つ.

[証明] $m \neq m'$ と仮定する. $\alpha \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{Q}(\sqrt{m'})$ とすると, ある a, b, c, $d \in \mathbb{Q}$ が存在して,

$$\alpha = a + b\sqrt{m} = c + d\sqrt{m'}.$$

もし仮に $b \neq 0$, $d \neq 0$ とすると,

$$\sqrt{m'} = a' + b'\sqrt{m}, \quad a' = \frac{a-c}{d}, \quad b' = \frac{b}{d} \neq 0$$

と表せる. 2 乗すると,

$$m' = (a' + b'\sqrt{m})^2 = (a'^2 + b'^2 m) + 2a'b'\sqrt{m}.$$

定理 2.2 より,

$$m' = a'^2 + b'^2 m, \quad 2a'b' = 0.$$

$b' \neq 0$ だから, 2 番目の式より $a' = 0$. よって, 1 番目の式より $m' = b'^2 m$. 最初に $m \neq m'$ と仮定したから, $b'^2 \neq 1$. これは m' が平方因子を含まないことに反する. ゆえに, $b = 0$ または $d = 0$ でなければならない.

$b = 0$ ならば, $\alpha = a \in \mathbb{Q}$. 一方, $d = 0$ ならば, $\alpha = c \in \mathbb{Q}$. いずれにせよ, $\alpha \in \mathbb{Q}$ となる. ゆえに, $\mathbb{Q}(\sqrt{m}) \cap \mathbb{Q}(\sqrt{m'}) \subseteq \mathbb{Q}$. 逆の包含関係は明らかだから, $\mathbb{Q}(\sqrt{m}) \cap \mathbb{Q}(\sqrt{m'}) = \mathbb{Q}$. □

K を 2 次体とする. $K \subseteq \mathbb{R}$ であるとき, K を**実 2 次体**といい, そうでないとき, K を**虚 2 次体**という. $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ と表すとき, $m > 0$ ならば実 2 次体, $m < 0$ ならば虚 2 次体である.

3　トレースとノルム

$K=\mathbb{Q}(\sqrt{m})$, $m\in\mathbb{Z}$ を 2 次体とする. K の元 $\alpha=a+b\sqrt{m}$, a, $b\in\mathbb{Q}$ に対して,

$$\alpha^{\sigma}=a-b\sqrt{m}$$

を α の**共役**という.

[注意 3.1（複素共役との関係）] $K=\mathbb{Q}(\sqrt{m})$, $m\in\mathbb{Z}$ を 2 次体とし, $\alpha=a+b\sqrt{m}$ を K の元とする.

K が虚 2 次体のとき, すなわち $m<0$ のとき, α の共役 α^{σ} は複素共役に一致する.

K が実 2 次体のとき, すなわち $m>0$ のとき, $b\neq 0$ の場合には, α は無理数で, その共役 α^{σ} は α と異なる. よって, この場合は 2 次体の元の共役と複素共役とが一致しない. $b=0$ の場合には, α は有理数で, その共役は α に一致する. よって, この場合は 2 次体の元の共役と複素共役とが一致する.

[定理 3.1] K を 2 次体とし, $\alpha\in K$ とする.

(i) $(\alpha^{\sigma})^{\sigma}=\alpha$.

(ii) $\alpha^{\sigma}=\alpha\iff\alpha\in\mathbb{Q}$.

(iii) $\alpha=0\iff\alpha^{\sigma}=0\iff\alpha\alpha^{\sigma}=0$.

[証明] $\alpha=a+b\sqrt{m}$, a, $b\in\mathbb{Q}$ とおく.

(i)　$(\alpha^{\sigma})^{\sigma}=(a-b\sqrt{m})^{\sigma}=a-(-b)\sqrt{m}=a+b\sqrt{m}=\alpha$.

(ii)　$\alpha^{\sigma}=\alpha\iff\alpha-\alpha^{\sigma}=0\iff 2b\sqrt{m}=0\iff b=0\iff\alpha\in\mathbb{Q}$.

(iii)　$\alpha=0\iff a+b\sqrt{m}=0\iff a=b=0\iff a-b\sqrt{m}=0\iff\alpha^{\sigma}=0$.

また, $\alpha^{\sigma}=0$ ならば $\alpha\alpha^{\sigma}=0$. 逆に, $\alpha\alpha^{\sigma}=0$ ならば, $\alpha=0$ または $\alpha^{\sigma}=0$. 先に示したように $\alpha=0\iff\alpha^{\sigma}=0$ なので, いずれの場合も $\alpha^{\sigma}=0$. したがって, $\alpha^{\sigma}=0\iff\alpha\alpha^{\sigma}=0$.　□

[定理 3.2] K を 2 次体とし, α, $\beta\in K$ とする.

(i) $\alpha^{\sigma}+\beta^{\sigma}=(\alpha+\beta)^{\sigma}$.

(ii) $-\alpha^{\sigma}=(-\alpha)^{\sigma}$.

(iii) $\alpha^{\sigma}\beta^{\sigma}=(\alpha\beta)^{\sigma}$.

(iv) $(\alpha^{\sigma})^{-1}=(\alpha^{-1})^{\sigma}$. ただし, $\alpha\neq 0$ と仮定する.

[証明] $\alpha=a+b\sqrt{m}$, $\beta=c+d\sqrt{m}$, a, b, c, $d\in\mathbb{Q}$ とおく.

(i)　$\alpha^{\sigma}+\beta^{\sigma}=(a-b\sqrt{m})+(c-d\sqrt{m})=(a+c)-(b+d)\sqrt{m}=((a+c)+(b+d)\sqrt{m})^{\sigma}=(\alpha+\beta)^{\sigma}$.

(ii) $-\alpha^\sigma = -(a-b\sqrt{m}) = (-a)-(-b)\sqrt{m} = ((-a)+(-b)\sqrt{m})^\sigma = \big(-(a+b\sqrt{m})\big)^\sigma = (-\alpha)^\sigma$.

(iii) $\alpha^\sigma\beta^\sigma = (a-b\sqrt{m})(c-d\sqrt{m}) = (ac+bd)-(ad+bc)\sqrt{m} = \big((ac+bd)+(ad+bc)\sqrt{m}\big)^\sigma$
$= (\alpha\beta)^\sigma$.

(iv) $(\alpha^\sigma)^{-1} = \dfrac{1}{a-b\sqrt{m}} = \dfrac{a+b\sqrt{m}}{(a+b\sqrt{m})(a-b\sqrt{m})} = \dfrac{a+b\sqrt{m}}{a^2-b^2m}$. 一方, $(\alpha^{-1})^\sigma = \left(\dfrac{1}{a-b\sqrt{m}}\right)^\sigma$
$= \left(\dfrac{a-b\sqrt{m}}{(a+b\sqrt{m})(a-b\sqrt{m})}\right)^\sigma = \left(\dfrac{a-b\sqrt{m}}{(a+b\sqrt{m})(a-b\sqrt{m})}\right)^\sigma = \left(\dfrac{a-b\sqrt{m}}{a^2-b^2m}\right)^\sigma = \dfrac{a+b\sqrt{m}}{a^2-b^2m}$.

□

2 次体 K の各元の共役により定まる写像

$$\sigma : K \longrightarrow K, \quad \alpha \longmapsto \alpha^\sigma$$

を**共役写像**という. 定理 3.1 より, σ の逆写像は σ 自身である. 特に, σ は全単射である. また, 定理 3.2 より, 共役写像は K から K 自身への (環の) 準同型写像である. したがって, σ は K の自己同型写像である.

$\mathrm{id} : K \longrightarrow K$ を K の恒等写像とし, $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ とおく.

[定理 3.3] K を 2 次体とするとき, $\mathrm{Gal}(K/\mathbb{Q})$ は写像の合成を積として位数 2 の巡回群をなす. $\mathrm{Gal}(K/\mathbb{Q})$ を K の $\mathbb{Q}$ 上の **Galois 群**という.

[証明] σ および id は K の自己同型であり, それらの合成もまた K の自己同型である. したがって, 積が定義できる. また, 写像の合成は結合法則を満たす.

$\sigma \circ \mathrm{id} = \mathrm{id} \circ \sigma = \sigma$ より, $\mathrm{Gal}(K/\mathbb{Q})$ の単位元は id である.

$\sigma \circ \sigma = \mathrm{id}$. すなわち, σ の逆写像は σ 自身である. よって, σ 自身が σ の $\mathrm{Gal}(K/\mathbb{Q})$ における逆元である. id についても同様である.

元の個数は 2 個なので, 群の位数は 2 である. $\sigma \neq \mathrm{id}$ であるから, $\mathrm{Gal}(K/\mathbb{Q})$ は σ によって生成される巡回群である. □

2 次体 $K = \mathbb{Q}(\sqrt{m})$ の元 $\alpha = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$ の**トレース**, **ノルム**を, それぞれ

$$\mathrm{Tr}_K\alpha = \alpha + \alpha^\sigma = 2a,$$
$$N_K\alpha = \alpha\alpha^\sigma = a^2 - b^2m$$

によって定める. 定め方からわかるように, $\mathrm{Tr}_K\alpha$, $N_K\alpha \in \mathbb{Q}$ である. また,

$$X^2 - (\mathrm{Tr}_K\alpha)X + N_K\alpha = (X-\alpha)(X-\alpha^\sigma)$$

であるから, α, α^σ はともに $\mathbb{Q}$ 係数 2 次方程式

$$X^2 - (\mathrm{Tr}_K\alpha)X + N_K\alpha = 0$$

の解である.

K が虚 2 次体のとき, K の元 α の共役 α^σ は複素共役であるから,

$$N_K\alpha = \alpha\alpha^\sigma = |\alpha|^2.$$

よって, 虚 2 次体における 0 でない元のノルムの値は常に正である.

[定理 3.4] K を 2 次体とし, α, $\beta \in K$, $c \in \mathbb{Q}$ とする.

(i) $\mathrm{Tr}_K(\alpha+\beta) = \mathrm{Tr}_K\alpha + \mathrm{Tr}_K\beta$.

(ii) $\mathrm{Tr}_K(c\alpha) = c \cdot \mathrm{Tr}_K\alpha$.

(iii) $\mathrm{Tr}_K c = 2c$.

[証明] (i)　定理 3.2 より $(\alpha+\beta)^\sigma = \alpha^\sigma + \beta^\sigma$ であるから,

$$\begin{aligned}\mathrm{Tr}_K(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^\sigma \\ &= \alpha+\beta+\alpha^\sigma+\beta^\sigma \\ &= (\alpha+\alpha^\sigma)+(\beta+\beta^\sigma) \\ &= \mathrm{Tr}_K\alpha + \mathrm{Tr}_K\beta.\end{aligned}$$

(ii)　定理 3.2 より $(c\alpha)^\sigma = c^\sigma\,\alpha^\sigma = c\alpha^\sigma$ であるから,

$$\mathrm{Tr}_K(c\alpha) = c\alpha + (c\alpha)^\sigma = c\alpha + c\alpha^\sigma = c(\alpha+\alpha^\sigma) = c \cdot \mathrm{Tr}_K\alpha.$$

(iii)　定理 3.1 より $c^\sigma = c$ であるから, $\mathrm{Tr}_K c = c + c^\sigma = c + c = 2c$. □

[定理 3.5] K を 2 次体とし, α, $\beta \in K$, $c \in \mathbb{Q}$ とする.

(i) $N_K(\alpha\beta) = N_K\alpha N_K\beta$.

(ii) $N_K c = c^2$.

(iii) $N_K\alpha = 0 \Longleftrightarrow \alpha = 0$.

(iv) $N_K\alpha^{-1} = (N_K\alpha)^{-1}$. ただし, $\alpha \neq 0$ と仮定する.

[証明] (i)　定理 3.2 より $(\alpha\beta)^\sigma = \alpha^\sigma\beta^\sigma$ であるから,

$$N_K(\alpha\beta) = \alpha\beta(\alpha\beta)^\sigma = \alpha\beta\alpha^\sigma\beta^\sigma = (\alpha\alpha^\sigma)(\beta\beta^\sigma) = N_K\alpha N_K\beta.$$

(ii)　定理 3.1 より $c^\sigma = c$ であるから, $N_K c = cc^\sigma = c^2$.

(iii)　定理 3.1 より, $N_K\alpha \neq 0 \Longleftrightarrow \alpha\alpha^\sigma \neq 0 \Longleftrightarrow \alpha \neq 0$.

(iv)　(iii) より, $\alpha \neq 0$ ならば $N_K\alpha \neq 0$. このとき, (i), (ii) を用いて計算すると,

$$N_K\alpha N_K\alpha^{-1} = N_K(\alpha\alpha^{-1}) = N_K 1 = 1^2 = 1.$$

ゆえに, $N_K\alpha^{-1} = (N_K\alpha)^{-1}$. □

K の各元のトレースにより定まる写像

$$\mathrm{Tr}_K : K \longrightarrow \mathbb{Q}, \quad \alpha \longmapsto \mathrm{Tr}_K\alpha$$

を**トレース写像**という. 定理 3.4 より, トレース写像は $\mathbb{Q}$ 上の線型写像である. また, 各元のノルムにより定まる写像

$$N_K : K^\times \longrightarrow \mathbb{Q}^\times, \quad \alpha \longmapsto N_K\alpha$$

を**ノルム写像**という. ここで, 定理 3.5 より $N_K\alpha = 0 \Longleftrightarrow \alpha = 0$ であるから, ノルム写像は実際に定義できる. 再び定理 3.5 より, ノルム写像は乗法群の準同型写像である.

4 整数環

代数体 K に対して, $\mathfrak{o}_K = K \cap \overline{\mathbb{Z}}$ とおく. $\mathfrak{o}_K$ は, K および $\overline{\mathbb{Z}}$ の部分整域である. $\mathfrak{o}_K$ を K の**整数環**といい, $\mathfrak{o}_K$ の元を K の**整数**という.

[定理 4.1] $\mathbb{Q} \cap \mathfrak{o}_K = \mathbb{Z}$. ただし, K は代数体, $\mathfrak{o}_K$ は K の整数環.

[証明] $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ かつ $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$ より, $\mathbb{Z} \subseteq \mathfrak{o}_K$. さらに,

$$\mathbb{Z} \subseteq \mathbb{Q} \cap \mathfrak{o}_K \subseteq \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$$

より, $\mathbb{Q} \cap \mathfrak{o}_K = \mathbb{Z}$ が得られる. □

[定理 4.2] K を代数体とする. このとき, K は $\mathfrak{o}_K$ の商体である.

[証明] 定理 1.7 と同様にして証明すればよい. $\mathfrak{o}_K$ が K の部分整域であることは $\mathfrak{o}_K$ の定め方から明らかである. $\alpha \in K$ とする. $K \subseteq \overline{\mathbb{Q}}$ であるから, 定理 1.2 より, ある有理整数 $a > 0$ が存在して $a\alpha \in \overline{\mathbb{Z}}$. また, $a \in \mathbb{Z} \subseteq K$ より, $a\alpha \in K$. ゆえに, $a\alpha \in K \cap \overline{\mathbb{Z}} = \mathfrak{o}_K$ となる. $\beta = a\alpha$ とおくと, $\alpha = \beta/a$. □

[定理 4.3] K を 2 次体とする. 任意の $\alpha \in K$ に対して,

$$\alpha \in \mathfrak{o}_K \Longleftrightarrow \mathrm{Tr}_K\alpha,\ N_K\alpha \in \mathbb{Z}$$

が成り立つ.

[証明] ($\Rightarrow$) $\alpha \in \mathfrak{o}_K$ とする. α は代数的整数だから, ある $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ が存在して,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

共役をとると,

$$\begin{aligned}&(\alpha^\sigma)^n + a_{n-1}(\alpha^\sigma)^{n-1} + \cdots + a_1\alpha^\sigma + a_0\\ &\quad = (\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)^\sigma\\ &\quad = 0^\sigma = 0.\end{aligned}$$

したがって, α^σ も代数的整数である. ゆえに,

$$\mathrm{Tr}_K\alpha = \alpha + \alpha^\sigma \in \overline{\mathbb{Z}},$$
$$N_K\alpha = \alpha\alpha^\sigma \in \overline{\mathbb{Z}}.$$

一方で, もともと $\mathrm{Tr}_K\alpha, N_K\alpha \in \mathbb{Q}$ だったから,

$$\mathrm{Tr}_K\alpha,\ N_K\alpha \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$$

となる.

($\Leftarrow$)　$\alpha \in K$ は方程式

$$X^2 - (\mathrm{Tr}_K\alpha)X + N_K\alpha = 0$$

の解である. $\mathrm{Tr}_K\alpha,\ N_K\alpha \in \mathbb{Z}$ とすると, この方程式は $\mathbb{Z}$ 係数である. ゆえに, $\alpha \in \overline{\mathbb{Z}}$. □

[補題 4.4] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする. ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする. また, $\alpha = x + \sqrt{m}$, $x, y \in \mathbb{Q}$ を K の元とする. さらに, $u = 2x$, $v = 2y$ とおく. このとき, 次の 2 つの条件は同値である.

(i) $\alpha \in \mathfrak{o}_K$.

(ii) $u, v \in \mathbb{Z}$ かつ $u^2 - mv^2 \equiv 0 \pmod 4$.

[証明] (i)⇒(ii)　$\alpha \in \mathfrak{o}_K$ とすると, 定理 4.3 より,

$$u = 2x = \mathrm{Tr}_K\alpha \in \mathbb{Z},$$
$$u^2 - mv^2 = 4(x^2 - my^2) = 4 \cdot N_K\alpha \in 4\mathbb{Z}.$$

さらに,

$$mv^2 = u^2 - (u^2 - mv^2) \in \mathbb{Z}.$$

$c = mv^2$ とおく. また, v を既約分数で表す: $v = a/b$, $a, b \in \mathbb{Z}$, $b > 0$, $\gcd(a, b) = 1$. すると,

$$b^2c = ma^2.$$

もし仮に $b > 1$ とすると, ある素数 p が存在して $p \mid b$, したがって $p^2 \mid b^2$. よって, $p^2 \mid ma^2$. ところが, $\gcd(a, b) = 1$ であるから, $p^2 \mid m$. これは m が平方因子を含まないことに反する. ゆえに, $b = 1$. したがって, $v = a \in \mathbb{Z}$.

(ii)⇒(i)　$\mathrm{Tr}_K\alpha = 2x = u \in \mathbb{Z}$. また,

$$4 \cdot N_K\alpha = 4(x^2 - my^2) = u^2 - mv^2 \in 4\mathbb{Z}.$$

ゆえに, $N_K\alpha \in \mathbb{Z}$. したがって, 定理 4.3 より, $\alpha \in \mathfrak{o}_K$. □

[補題 4.5] m, u, $v \in \mathbb{Z}$ とする.

(i) $m \equiv 1 \pmod 4$ のとき,

$$u^2 - mv^2 \equiv 0 \pmod 4 \Longleftrightarrow u \equiv v \pmod 2.$$

(ii) $m \equiv 2, 3 \pmod 4$ のとき,

$$u^2 - mv^2 \equiv 0 \pmod 4 \Longleftrightarrow u \equiv v \equiv 0 \pmod 2.$$

[証明] (i)　$m \equiv 1 \pmod 4$ のとき,

$$\begin{aligned} u^2 - mv^2 \equiv 0 \pmod 4 &\Longleftrightarrow u^2 - v^2 \equiv 0 \pmod 4 \\ &\Longleftrightarrow u^2 \equiv v^2 \pmod 4 \\ &\Longleftrightarrow u \equiv v \pmod 2. \end{aligned}$$

(ii) (⇒)　$u^2 - mv^2 \equiv 0 \pmod 4$ とする.

$m \equiv 2 \pmod 4$ のとき,

$$u^2 \equiv 2v^2 \pmod 4$$

なので,

$$2 \mid u^2 \Longrightarrow 2 \mid u \Longrightarrow 4 \mid u^2 \Longrightarrow 4 \mid 2v^2 \Longrightarrow 2 \mid v^2 \Longrightarrow 2 \mid v.$$

よって, $u \equiv v \equiv 0 \pmod 2$.

$m \equiv 3 \pmod 4$ のとき,

$$u^2 \equiv 3v^2 \pmod 4.$$

もし仮に v が奇数であるとすれば,

$$v \equiv 1 \pmod 2 \Longrightarrow v^2 \equiv 1 \pmod 4 \Longrightarrow u^2 \equiv 3 \pmod 4.$$

一方, 任意の $u \in \mathbb{Z}$ に対して $u^2 \equiv 0, 1 \pmod 4$ であるから, これは矛盾である. ゆえに, v は偶数である. したがって, u も偶数である. すなわち, $u \equiv v \equiv 0 \pmod 2$.

(⇐)　明らかである. □

[定理 4.6] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする．ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする．

(i) $m \equiv 1 \pmod 4$ のとき,

$$\mathfrak{o}_K = \left\{ \frac{u + v\sqrt{m}}{2} \;\middle|\; u, v \in \mathbb{Z},\ u \equiv v \pmod 2 \right\}. \tag{3}$$

(ii) $m \equiv 2, 3 \pmod 4$ のとき,

$$\mathfrak{o}_K = \{x + y\sqrt{m} \mid x, y \in \mathbb{Z}\}. \tag{4}$$

[証明] $\alpha = x + y\sqrt{m}$, $x, y \in \mathbb{Q}$ を K の元とする．また, $u = 2x$, $v = 2y$ とおく．

(i)　$m \equiv 1 \pmod 4$ のとき, 補題 4.4, 補題 4.5 より,

$$\alpha \in \mathfrak{o}_K \Longleftrightarrow u, v \in \mathbb{Z},\ u \equiv v \pmod 2.$$

α を u, v で表すと $\alpha = (u + v\sqrt{m})/2$ なので, 上の同値から直ちに (3) の $\subseteq$ が得られる．逆に, $\alpha = (u + v\sqrt{m})/2$ と条件 $u, v \in \mathbb{Z}$, $u \equiv v \pmod 2$ が先に与えられたとき, $x = u/2$, $y = v/2$ とおくと, $\alpha = x + y\sqrt{m}$ であり, 上の同値より $\alpha \in \mathfrak{o}_K$ が得られる．よって, $\supseteq$ もいえる．

(ii)　$m \equiv 2, 3 \pmod 4$ のとき, 補題 4.4, 補題 4.5 より,

$$\begin{aligned} \alpha \in \mathfrak{o}_K &\Longleftrightarrow u, v \in \mathbb{Z},\ u \equiv v \equiv 0 \pmod 2 \\ &\Longleftrightarrow x, y \in \mathbb{Z}. \end{aligned}$$

よって, (4) が成り立つ．　□

5　整数底

K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする．$\omega_1, \omega_2 \in \mathfrak{o}_K$ が K の**整数底**であるとは, 任意の $\alpha \in \mathfrak{o}_K$ が

$$\alpha = a\omega_1 + b\omega_2, \quad a, b \in \mathbb{Z}$$

と一意的に表されるときにいう．ω_1, ω_2 が K の整数底であることを, 記号で

$$\mathfrak{o}_K = [\omega_1, \omega_2]$$

と表す．

[補題 5.1] K を 2 次体とする．$\omega_1, \omega_2 \in \mathfrak{o}_K$ が K の整数底であるための必要十分条件は, 次の 2 つの条件を満たすことである．

(i) $\mathfrak{o}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

(ii) ω_1, ω_2 は $\mathbb{Z}$ 上 1 次独立である.

[証明] (条件の必要性)　ω_1, $\omega_2 \in \mathfrak{o}_K$ を K の整数底とする. 任意の $\alpha \in \mathfrak{o}_K$ に対して, ある a, $b \in \mathbb{Z}$ が存在して,

$$\alpha = a\omega_1 + b\omega_2 \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

ゆえに, $\mathfrak{o}_K \subseteq \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. 一方, 任意の a, $b \in \mathbb{Z}$ に対して $a\omega_1 + b\omega_2 \in \mathfrak{o}_K$ であるから, 逆の包含関係も成り立つ. したがって, (i) が成り立つ.

$0 = 0 \cdot \omega_1 + 0 \cdot \omega_2$ であるから, 任意の a, $b \in \mathbb{Z}$ に対して,

$$a\omega_1 + b\omega_2 = 0 \Longrightarrow a = b = 0.$$

すなわち, (ii) が成り立つ.

(条件の十分性)　$\alpha \in \mathfrak{o}_K$ とする. (i) より, α は ω_1, ω_2 の $\mathbb{Z}$ 係数の 1 次結合で表される.

a, b, c, $d \in \mathbb{Z}$ とし,

$$\alpha = a\omega_1 + b\omega_2 = c\omega_1 + d\omega_2$$

とすると,

$$(a-c)\omega_1 + (b-d)\omega_2 = 0.$$

(ii) より, $a - c = b - d = 0$. ゆえに, $a = c$, $b = d$. したがって, $\alpha = a\omega_1 + b\omega_2$, a, $b \in \mathbb{Z}$ という表し方は一意的である. □

[定理 5.2] $K = \mathbb{Q}(\sqrt{m})$, $m \neq 0$, 1 は平方因子を含まない有理整数とし,

$$\omega = \begin{cases} \dfrac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4 \text{ のとき}, \\ \sqrt{m}, & m \equiv 2,\ 3 \pmod 4 \text{ のとき} \end{cases}$$

とおくとき, 1, ω は $\mathfrak{o}_K$ の整数底である. これを K の**標準的整数底**という.

[証明] $m \equiv 1 \pmod 4$ のとき, 定理 4.6 より,

$$\mathfrak{o}_K = \left\{ \frac{u+v\sqrt{m}}{2} \;\middle|\; u,\ v \in \mathbb{Z},\ u \equiv v \pmod 2 \right\}.$$

明らかに 1, $\omega \in \mathfrak{o}_K$, したがって $\mathbb{Z} + \mathbb{Z}\omega \subseteq \mathfrak{o}_K$.

$\alpha = (u + v\sqrt{m})/2$, u, $v \in \mathbb{Z}$, $u \equiv v \pmod 2$ を $\mathfrak{o}_K$ の元とすると,

$$\begin{aligned} \alpha &= \frac{u+v\sqrt{m}}{2} \\ &= \frac{(u-v)+v(1+\sqrt{m})}{2} \\ &= \frac{u-v}{2} + v \cdot \frac{1+\sqrt{m}}{2} \\ &= \frac{u-v}{2} + v\omega. \end{aligned}$$

$u \equiv v \pmod 2$ より $(u-v)/2 \in \mathbb{Z}$. よって, $\alpha \in \mathbb{Z} + \mathbb{Z}\omega$. ゆえに, $\mathfrak{o}_K \subseteq \mathbb{Z} + \mathbb{Z}\omega$.

また, 任意の a, $b \in \mathbb{Z}$ に対して,

$$\begin{aligned} a + b\omega &\Longrightarrow a + b \cdot \frac{1+\sqrt{m}}{2} = 0 \\ &\Longrightarrow \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{m} = 0 \\ &\Longrightarrow a + \frac{b}{2} = \frac{b}{2} = 0 \\ &\Longrightarrow a = b = 0. \end{aligned}$$

よって, 1, ω は $\mathbb{Z}$ 上 1 次独立である.

以上の議論と補題 5.1 より, $m \equiv 1 \pmod 4$ のとき, 1, ω は K の整数底である.

$m \equiv 2, 3 \pmod 4$ のとき, 1, ω は $\mathbb{Q}$ 上 1 次独立だから, $\mathbb{Z}$ 上 1 次独立である. また, 定理 4.6 より, $\mathfrak{o}_K$ は 1, ω で $\mathbb{Z}$ 上生成される. 補題 5.1 より, 1, ω は K の整数底である. □

[注意 5.1] 整数底とは, まさに 2 次体 K の整数環 $\mathfrak{o}_K$ における $\mathbb{Z}$ 上の基底のことである.

基底をもつ加法群のことを自由加群という. 代数学の一般論により, 自由加群の基底の元の個数は一定であることが知られている. その個数を自由加群の階数という. 定理 5.2 より $\mathfrak{o}_K$ は元の個数が 2 個の基底を少なくとも 1 つもつから, $\mathfrak{o}_K$ のすべての基底は, その元の個数が必ず 2 個である. すなわち, $\mathfrak{o}_K$ は階数 2 の自由加群である.

[定理 5.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, ω_1, ω_2 を $\mathfrak{o}_K$ の元とする. このとき, ω_1, ω_2 が K の整数底ならば, それらの共役 ω_1^σ, ω_2^σ も K の整数底である.

[証明] $\mathfrak{o}_K = [\omega_1, \omega_2]$ ならば, $\mathfrak{o}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. このとき,

$$\mathbb{Z}\omega_1^\sigma + \mathbb{Z}\omega_2^\sigma = (\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)^\sigma = \mathfrak{o}_K^\sigma = \mathfrak{o}_K.$$

さらに, 任意の x, $y \in \mathbb{Z}$ に対して,

$$\begin{aligned} x\omega_1^\sigma + y\omega_2^\sigma = 0 &\Longrightarrow (x\omega_1 + y\omega_2)^\sigma = 0 \\ &\Longrightarrow x\omega_1 + y\omega_2 = 0 \\ &\Longrightarrow x = y = 0. \end{aligned}$$

ゆえに, ω_1^σ, ω_2^σ は $\mathbb{Z}$ 上 1 次独立である. 補題 5.1 より, ω_1^σ, ω_2^σ は K の整数底である. □

[定理 5.4] ω_1, ω_2 を 2 次体 K の整数底とする. また, p, q, r, $s \in \mathbb{Z}$ とし, $ps - qr = \pm 1$ を満たすとする. このとき,

$$\begin{aligned} \mu_1 &= p\omega_1 + q\omega_2, \\ \mu_2 &= r\omega_1 + s\omega_2 \end{aligned} \tag{5}$$

とおけば, μ_1, μ_2 もまた K の整数底である.

[証明] $\mu_1,\ \mu_2 \in \mathfrak{o}_K$. したがって, $\mathbb{Z}\mu_1 + \mathbb{Z}\mu_2 \subseteq \mathfrak{o}_K$.

(5) を行列で表すと,

$$\begin{bmatrix}\mu_1\\ \mu_2\end{bmatrix} = P\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}, \quad P = \begin{bmatrix}p & q\\ r & s\end{bmatrix}.$$

両辺に P^{-1} を掛けると,

$$\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} = P^{-1}\begin{bmatrix}\mu_1\\ \mu_2\end{bmatrix}, \quad P^{-1} = \frac{1}{ps-qr}\begin{bmatrix}s & -q\\ -r & p\end{bmatrix}.$$

$e = 1/(ps-qr)$ とおくと, $ps - qr = \pm 1$ より $e = \pm 1$ であり,

$$\begin{aligned}\omega_1 &= e(s\mu_1 - q\mu_2),\\ \omega_2 &= e(-r\mu_1 + p\mu_2).\end{aligned}$$

$\alpha \in \mathfrak{o}_K$ を任意にとる. $\omega_1,\ \omega_2$ は K の整数底だから, ある $a,\ b \in \mathbb{Z}$ が存在して,

$$\begin{aligned}\alpha &= a\omega_1 + b\omega_2\\ &= ae(s\mu_1 - q\mu_2) + be(-r\mu_1 + p\mu_2)\\ &= e(as - br)\mu_1 + e(-aq + bp)\mu_2\\ &\in \mathbb{Z}\mu_1 + \mathbb{Z}\mu_2.\end{aligned}$$

ゆえに, $\mathfrak{o}_K \subseteq \mathbb{Z}\mu_1 + \mathbb{Z}\mu_2$.

任意の $a,\ b \in \mathbb{Z}$ に対して,

$$\begin{aligned}a\mu_1 + b\mu_2 = 0 &\Longrightarrow a(p\omega_1 + q\omega_2) + b(r\omega_1 + s\omega_2) = 0\\ &\Longrightarrow (ap + br)\omega_1 + (aq + bs)\omega_2 = 0\\ &\Longrightarrow ap + br = aq + bs = 0.\end{aligned}$$

最後の式を行列で表すと,

$$P\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}.$$

両辺に P^{-1} を掛けると,

$$\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}.$$

すなわち, $a = b = 0$. したがって, $\mu_1,\ \mu_2$ は $\mathbb{Z}$ 上 1 次独立である.

以上の議論と補題 5.1 より, $\mu_1,\ \mu_2$ は K の整数底である. □

[補題 5.5] $\omega_1,\ \omega_2$ を 2 次体 K の整数底, P を $\mathbb{Z}$ 成分の 2 次正方行列とし,

$$\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} = P\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} \tag{6}$$

が成り立つとする. このとき, $P = E$ となる. ただし, E は単位行列である.

[証明] $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ とおくと, (6) より,

$$\omega_1 = p\omega_1 + q\omega_2,$$
$$\omega_2 = r\omega_1 + s\omega_2.$$

$\mathfrak{o}_K$ の元を整数底の $\mathbb{Z}$ 係数の 1 次結合で表す仕方は一意的だから,

$$p = s = 1, \quad q = r = 0.$$

すなわち, $P = E$. □

[補題 5.6] P を $\mathbb{Z}$ 成分の 2 次正方行列とする. このとき, P が $\mathbb{Z}$ 成分の逆行列をもつための必要十分条件は, $\det P = \pm 1$ であることである.

[証明] (条件の必要性) $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ とおく. P が逆行列 P^{-1} をもつとすると,

$$P^{-1} = \frac{1}{\det P} \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}, \quad \det P = ps - qr \neq 0.$$

P^{-1} も $\mathbb{Z}$ 成分ならば, $\det P$ は p, q, r, s をすべて割る. したがって, ある $u \in \mathbb{Z}$ が存在して,

$$\det P = ps - qr = (\det P)^4 u.$$

もし $\det P$ が素因子をもてば, 両辺の素因子の数が一致しないので, $\mathbb{Z}$ における素因子分解の一意性に反する. ゆえに, $\det P$ は素因子をもたない. すなわち, $\det P = \pm 1$.

(条件の十分性) $\det P = \pm 1$ とすると, $P^{-1} = \frac{1}{\det P} \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}$ は P の $\mathbb{Z}$ 成分の逆行列である. □

[定理 5.7] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, ω_1, ω_2, μ_1, $\mu_2 \in \mathfrak{o}_K$, p, q, r, $s \in \mathbb{Z}$ とし,

$$\begin{aligned} \mu_1 &= p\omega_1 + q\omega_2, \\ \mu_2 &= r\omega_1 + s\omega_2 \end{aligned} \tag{7}$$

を満たすとする. このとき, $\mathfrak{o}_K = [\omega_1, \omega_2] = [\mu_1, \mu_2]$ ならば $ps - qr = \pm 1$ が成り立つ.

[証明] (7) を行列で表すと,

$$\begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix} = P \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}, \quad P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}. \tag{8}$$

また, $\omega_1, \omega_2 \in \mathfrak{o}_K = [\mu_1, \mu_2]$ であるから, ある $p', q', r', s' \in \mathbb{Z}$ が存在して,

$$\begin{aligned}\omega_1 &= p'\mu_1 + q'\mu_2,\\ \omega_2 &= r'\mu_1 + s'\mu_2.\end{aligned}$$

これを行列で表すと,

$$\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} = Q\begin{bmatrix}\mu_1\\ \mu_2\end{bmatrix}, \quad Q = \begin{bmatrix}p' & q'\\ r' & s'\end{bmatrix}. \tag{9}$$

(9) に (8) を代入すると,

$$\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} = QP\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}.$$

$\mathfrak{o}_K = [\omega_1, \omega_2]$ であるから, 補題 5.5 より, $QP = E$. すなわち, $P^{-1} = Q$. さらに, 補題 5.6 より, $ps - qr = \det P = \pm 1$. □

2 次体 K の整数底 ω_1, ω_2 が**正規整数底**であるとは, $\omega_2 = \omega_1^\sigma$ が成り立つときにいう.

[定理 5.8] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする. ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする. このとき,

$$K \text{ の正規整数底が存在する} \iff m \equiv 1 \pmod 4$$

が成り立つ. また, $m \equiv 1 \pmod 4$ のとき, $1, \omega = (1+\sqrt{m})/2$ を K の標準的整数底とすると, ω, ω^σ が K の正規整数底である.

[証明] まず, m は平方因子を含まないので, $m \not\equiv 0 \pmod 4$ である.

$m \equiv 1 \pmod 4$ のとき, $\omega = (1+\sqrt{m})/2$ とおくと,

$$\omega^\sigma = \frac{1-\sqrt{m}}{2} = 1 - \frac{1+\sqrt{m}}{2} = 1 - \omega.$$

定理 5.2 より $\mathfrak{o}_K = [1, \omega]$ だから, 任意の $\alpha \in \mathfrak{o}_K$ に対して, ある $a, b \in \mathbb{Z}$ が存在して,

$$\alpha = a + b\omega = (a+b)\omega + a(1-\omega) \in \mathbb{Z}\omega + \mathbb{Z}\omega^\sigma.$$

ゆえに, $\mathfrak{o}_K \subseteq \mathbb{Z}\omega + \mathbb{Z}\omega^\sigma$. 逆の包含関係は明らかである. また, 任意の $a, b \in \mathbb{Z}$ に対して,

$$\begin{aligned}a\omega + b\omega^\sigma = 0 &\Longrightarrow a\omega + b(1-\omega) = 0\\ &\Longrightarrow b + (a-b)\omega = 0\\ &\Longrightarrow b = a - b = 0\\ &\Longrightarrow a = b = 0.\end{aligned}$$

よって, ω, ω^σ は $\mathbb{Z}$ 上 1 次独立である. 補題 5.1 より, $\mathfrak{o}_K = [\omega, \omega^\sigma]$.

$m \not\equiv 1 \pmod 4$ のとき, すなわち $m \equiv 2, 3 \pmod 4$ のとき, $\mathfrak{o}_K = [1, \sqrt{m}]$ である. もし仮に K の正規整数底が存在するとすれば, ある $\alpha \in \mathfrak{o}_K$ が存在して

$$\mathfrak{o}_K = [\alpha, \alpha^\sigma], \quad \alpha = a + b\sqrt{m}, \quad a, b \in \mathbb{Z}$$

と表せる. $\alpha^\sigma = a - b\sqrt{m}$ であるから, 定理 5.7 より,

$$-2ab = \pm 1.$$

これは不可能である. ゆえに, K の正規整数底は存在しない. □

6 判別式

2 次体 K の元 α, β に対して,

$$\begin{vmatrix} \alpha & \beta \\ \alpha^\sigma & \beta^\sigma \end{vmatrix}^2$$

を K における α, β の**判別式**といい, $d_K(\alpha, \beta)$ で表す.

[定理 6.1] K を 2 次体とし, $\alpha, \beta \in K$ とする. このとき,

$$d_K(\alpha, \beta) = \begin{vmatrix} \mathrm{Tr}_K(\alpha^2) & \mathrm{Tr}_K(\alpha\beta) \\ \mathrm{Tr}_K(\alpha\beta) & \mathrm{Tr}_K(\beta^2) \end{vmatrix} \in \mathbb{Q}$$

が成り立つ. 特に, α, β がともに整数環 $\mathfrak{o}_K$ の元ならば $d_K(\alpha, \beta) \in \mathbb{Z}$.

[証明] $A = \begin{bmatrix} \alpha & \beta \\ \alpha^\sigma & \beta^\sigma \end{bmatrix}$ とおくと, ${}^tA = \begin{bmatrix} \alpha & \alpha^\sigma \\ \beta & \beta^\sigma \end{bmatrix}$ であり,

$$\begin{aligned} d_K(\alpha, \beta) &= (\det A)^2 = \det {}^tA \cdot \det A = \det({}^tAA) \\ &= \begin{vmatrix} \alpha^2 + (\alpha^\sigma)^2 & \alpha\beta + \alpha^\sigma\beta^\sigma \\ \alpha\beta + \alpha^\sigma\beta^\sigma & \beta^2 + (\beta^\sigma)^2 \end{vmatrix} \\ &= \begin{vmatrix} \mathrm{Tr}_K(\alpha^2) & \mathrm{Tr}_K(\alpha\beta) \\ \mathrm{Tr}_K(\alpha\beta) & \mathrm{Tr}_K(\beta^2) \end{vmatrix}. \end{aligned}$$

トレースは常に有理数なので, $d_K(\alpha, \beta) \in \mathbb{Q}$. また, 整数環 $\mathfrak{o}_K$ の元のトレースは有理整数なので, $\alpha, \beta \in \mathfrak{o}_K$ ならば $d_K(\alpha, \beta) \in \mathbb{Z}$. □

2 次体 K の元 α に対して,

$$d_K(1, \alpha) = \begin{vmatrix} 1 & \alpha \\ 1 & \alpha^\sigma \end{vmatrix}^2 = (\alpha - \alpha^\sigma)^2$$

を K における α の**判別式**といい, $d_K(\alpha)$ で表す.

[定理 6.2] K を 2 次体とし, $\alpha \in K$ とする.

(i) $d_K(-\alpha) = d_K(\alpha)$.

(ii) $d_K(\alpha^\sigma) = d_K(\alpha)$.

(iii) $d_K(\alpha) = 0 \Longleftrightarrow \alpha \in \mathbb{Q}$.

[証明] (i) $d_K(-\alpha) = \big((-\alpha) - (-\alpha)^\sigma\big)^2 = (-\alpha + \alpha^\sigma)^2 = (\alpha - \alpha^\sigma)^2 = d_K(\alpha)$.

(ii) $d_K(\alpha^\sigma) = \big(\alpha^\sigma - (\alpha^\sigma)^\sigma\big)^2 = (\alpha^\sigma - \alpha)^2 = (\alpha - \alpha^\sigma)^2 = d_K(\alpha)$.

(iii) $d_K(\alpha) = 0 \Longleftrightarrow (\alpha - \alpha^\sigma)^2 = 0 \Longleftrightarrow \alpha - \alpha^\sigma = 0 \Longleftrightarrow \alpha \in \mathbb{Q}$. ここで, 最後の同値において定理 3.1 を用いた. □

[定理 6.3] K を 2 次体とする. このとき, 任意の $\alpha \in K$ に対して,

$$d_K(\alpha) = (\mathrm{Tr}_K \alpha)^2 - 4 \cdot N_K \alpha$$

が成り立つ.

[証明] $d_K(\alpha) = (\alpha - \alpha^\sigma)^2 = (\alpha + \alpha^\sigma)^2 - 4\alpha\alpha^\sigma = (\mathrm{Tr}_K \alpha)^2 - 4 \cdot N_K \alpha$. □

定理 6.3 によれば, $d_K(\alpha)$ は α を解にもつ 2 次方程式

$$X^2 - (\mathrm{Tr}_K \alpha)X + N_K \alpha = 0$$

の判別式に一致することがわかる.

K を 2 次体とし, ω_1, ω_2 を K の整数底とするとき,

$$d_K(\omega_1, \omega_2) = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1^\sigma & \omega_2^\sigma \end{vmatrix}^2$$

を K の**判別式**といい, d_K で表す.

[定理 6.4] d_K の値は K の整数底の選び方によらない.

[証明] $\mathfrak{o}_K = [\omega_1, \omega_2] = [\mu_1, \mu_2]$ とすると, ある p, q, r, $s \in \mathbb{Z}$ が存在して,

$$\mu_1 = p\omega_1 + q\omega_2,$$
$$\mu_2 = r\omega_1 + s\omega_2.$$

定理 5.7 より, $ps - qr = \pm 1$. また, 共役をとると,

$$\mu_1^\sigma = p\omega_1^\sigma + q\omega_2^\sigma,$$
$$\mu_2^\sigma = r\omega_1^\sigma + s\omega_2^\sigma$$

であるから,

$$\begin{vmatrix} \mu_1 & \mu_2 \\ \mu_1^\sigma & \mu_2^\sigma \end{vmatrix} = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1^\sigma & \omega_2^\sigma \end{vmatrix} \begin{vmatrix} p & r \\ q & s \end{vmatrix} = \pm \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1^\sigma & \omega_2^\sigma \end{vmatrix}.$$

したがって, d_K の値は整数底の選び方によらない. □

[定理 6.5] $K = \mathbb{Q}(\sqrt{m})$ とし, $m \neq 0, 1$ を平方因子を含まない有理整数とする. このとき,

$$d_K = \begin{cases} m, & m \equiv 1 \pmod 4 \text{ のとき}, \\ 4m, & m \equiv 2, 3 \pmod 4 \text{ のとき}. \end{cases}$$

特に, $d_K \in \mathbb{Z}$ かつ $d_K \equiv 0, 1 \pmod 4$ である. また, 実 2 次体の判別式は正であり, 虚 2 次体の判別式は負である.

[証明] 標準的整数底を選んで d_K を計算すると, $m \equiv 1 \pmod 4$ のとき,

$$d_K = \begin{vmatrix} 1 & (1+\sqrt{m})/2 \\ 1 & (1-\sqrt{m})/2 \end{vmatrix}^2 = m.$$

$m \equiv 2, 3 \pmod 4$ のとき,

$$d_K = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m.$$

後半の主張は前半より明らかである. □

[定理 6.6] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $1, \omega$ を K の標準的整数底とする. また, $\alpha \in \mathfrak{o}_K$ とし,

$$\alpha = a + b\omega, \quad a, b \in \mathbb{Z}$$

と表すとする. このとき,

$$d_K(\alpha) = b^2 d_K$$

が成り立つ.

[証明] $K = \mathbb{Q}(\sqrt{m})$ とおく. ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする.

$m \equiv 1 \pmod 4$ のとき, $\omega = (1+\sqrt{m})/2$ であるから,

$$\begin{aligned} d_K(\alpha) &= (\alpha - \alpha^\sigma)^2 \\ &= \left(\left(a + b \cdot \frac{1+\sqrt{m}}{2} \right) - \left(a + b \cdot \frac{1-\sqrt{m}}{2} \right) \right)^2 \\ &= b^2 m. \end{aligned}$$

$m \equiv 2, 3 \pmod 4$ のとき, $\omega = \sqrt{m}$ であるから,

$$\begin{aligned} d_K(\alpha) &= (\alpha - \alpha^\sigma)^2 \\ &= \big((a + b\sqrt{m}) - (a - b\sqrt{m})\big)^2 \\ &= 4b^2 m. \end{aligned}$$

定理 6.5 より, $d_K(\alpha) = b^2 d_K$. □

[例 6.1] $1, \omega$ を 2 次体 K の標準的整数底とするとき, $d_K(\omega) = d_K(1, \omega) = d_K$.

7　代数体の単数

K を代数体, $\mathfrak{o}_K$ を K の整数環とする.

$\alpha, \beta \in \mathfrak{o}_K$ に対して, ある $\xi \in \mathfrak{o}_K$ が存在して $\beta = \alpha\xi$ が成り立つとき, α は β を**割る**といい, β は α で**割り切れる**という. このことを記号で $\alpha \mid \beta$ と書く. またこのとき, α を β の**約数**, β を α の**倍数**という.

$\alpha \in \mathfrak{o}_K$ がいくつかの $\beta_1, \beta_2, \ldots, \beta_s \in \mathfrak{o}_K$ の約数であるとき, α をそれらの**公約数**という. また, α がそれらの**最大公約数**であるとは, 2 つの条件

(i) α は $\beta_1, \beta_2, \ldots, \beta_s$ の公約数である.

(ii) $\beta_1, \beta_2, \ldots, \beta_s$ の任意の公約数は α の約数である.

を満たすときにいう. 「約数」を「倍数」に書き換えれば, **公倍数**, **最小公倍数**も同様に定義できる.

[定理 7.1] $\alpha, \beta, \gamma \in \mathfrak{o}_K$ とする.

(i) $\alpha \mid \alpha$.

(ii) $\alpha \mid \beta, \beta \mid \gamma \Longrightarrow \alpha \mid \gamma$.

[証明] (i)　任意の $\alpha \in \mathfrak{o}_K$ に対して, $\alpha = \alpha \cdot 1$. よって, $\alpha \mid \alpha$.

(ii)　$\alpha \mid \beta$ かつ $\beta \mid \gamma$ とする. $\alpha \mid \beta$ より, ある $\xi \in \mathfrak{o}_K$ が存在して,

$$\beta = \alpha\xi.$$

同様に, $\gamma \mid \beta$ より, ある $\xi' \in \mathfrak{o}_K$ が存在して,

$$\gamma = \beta\xi'.$$

2 番目の式を最初の式に代入すると,

$$\gamma = \alpha\xi\xi'.$$

$\xi\xi' \in \mathfrak{o}_K$ であるから, $\alpha \mid \gamma$. □

$\alpha, \beta \in \mathfrak{o}_K$ とする. 一般には,

$$\alpha \mid \beta \quad \text{かつ} \quad \beta \mid \alpha \tag{10}$$

であっても, $\alpha = \beta$ とは限らない. 条件 (10) が成り立つとき, α, β は**同伴**であるという.

[定理 7.2] K を代数体, $\mathfrak{o}_K$ を K の整数環とする. $\mathfrak{o}_K$ の元が同伴であるという関係は, $\mathfrak{o}_K$ における同値関係である.

[証明] (反射)　定理 7.1 より, 任意の $\alpha \in \mathfrak{o}_K$ に対して, $\alpha \mid \alpha$. これより, α は α 自身に同伴である.

(対称)　同伴の定義から明らか.

(推移)　$\alpha, \beta, \gamma \in \mathfrak{o}_K$ とし, α, β が同伴であり, かつ β, γ が同伴であるとする.

α, β が同伴であることから,

$$\alpha \mid \beta \quad \text{かつ} \quad \beta \mid \alpha.$$

また, β, γ が同伴であることから,

$$\beta \mid \gamma \quad \text{かつ} \quad \gamma \mid \beta.$$

ゆえに, 定理 7.1 より,

$$\alpha \mid \gamma \quad \text{かつ} \quad \gamma \mid \alpha.$$

すなわち, α, γ は同伴である. □

$\alpha \in K$ が**単数**であるとは, 2 つの条件

(i) $\alpha \in \mathfrak{o}_K$.

(ii) ある $\alpha' \in \mathfrak{o}_K$ が存在して, $\alpha\alpha' = 1$.

を満たすときにいう.

[定理 7.3] $\alpha, \beta \in \mathfrak{o}_K$ とするとき, 次の 2 つの条件は同値である.

(i) α, β は同伴.

(ii) K の単数 ε が存在して, $\beta = \alpha\varepsilon$.

[証明] (i) $\Rightarrow$ (ii)　$\alpha \mid \beta$ かつ $\beta \mid \alpha$ より, ある $\varepsilon, \varepsilon' \in \mathfrak{o}_K$ が存在して

$$\beta = \alpha\varepsilon, \quad \alpha = \beta\varepsilon'. \tag{11}$$

1 番目の式を 2 番目の式に代入すると,

$$\alpha = \alpha\varepsilon\varepsilon'.$$

両辺に $-\alpha$ を加えると,

$$0 = \alpha(\varepsilon\varepsilon' - 1).$$

$\mathfrak{o}_K$ は整域なので $\alpha = 0$ または $\varepsilon\varepsilon' - 1 = 0$ である. $\alpha \neq 0$ のとき, $\varepsilon\varepsilon' = 1$. ゆえに, ε は K の単数である. $\alpha = 0$ のとき, (11) の 1 番目の式より $\beta = 0$. よって, $\alpha = \beta \cdot 1$.

(ii) $\Rightarrow$ (i)　$\alpha = \beta\varepsilon$ より, $\beta \mid \alpha$. また, ε は単数だから, ある $\varepsilon' \in \mathfrak{o}_K$ が存在して $\varepsilon\varepsilon' = 1$. よって, $\alpha = \beta\varepsilon$ の両辺に ε' を掛けると,

$$\alpha\varepsilon' = \beta\varepsilon\varepsilon' = \beta.$$

ゆえに, $\alpha \mid \beta$. □

[定理 7.4] K を代数体, $\mathfrak{o}_K$ を K の整数環, $\alpha, \beta \in \mathfrak{o}_K$ とする.

(i) α が単数ならば, $-\alpha$ も単数である.

(ii) α が単数ならば, α^{-1} も単数である. ただし, $\alpha \neq 0$ を仮定する.

(iii) α, β が単数ならば, $\alpha\beta$ も単数である.

[証明] (i)　α を単数とする. 定義より, ある $\alpha' \in \mathfrak{o}_K$ が存在して $\alpha\alpha' = 1$. このとき, $-\alpha, -\alpha' \in \mathfrak{o}_K$, $(-\alpha)(-\alpha') = 1$. ゆえに, $-\alpha$ は単数である.

(ii)　α を単数とする. 定義より, ある $\alpha' \in \mathfrak{o}_K$ が存在して $\alpha\alpha' = 1$. α' も単数である. 両辺に α^{-1} を掛けると, $\alpha' = \alpha^{-1}$. ゆえに, α^{-1} は単数である.

(iii)　α, β を単数とする. $\alpha, \beta \in \mathfrak{o}_K$ より $\alpha\beta \in \mathfrak{o}_K$. また, (ii) より α^{-1}, β^{-1} もまた単数であり, $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} \in \mathfrak{o}_K$. ゆえに, 積 $\alpha\beta$ は単数である. □

K における単数の全体を $\mathfrak{o}_K^\times$ と書く.

[定理 7.5] $\mathfrak{o}_K^\times$ は乗法に関して $K^\times$ の部分群になる. ただし, $K^\times = K \setminus \{0\}$ は代数体 K の乗法群であるとする. $\mathfrak{o}_K^\times$ を K の**単数群**という.

[証明] まず, $0 \notin \mathfrak{o}_K^\times$, すなわち, 0 は単数でない. なぜなら, 任意の $\alpha \in \mathfrak{o}_K$ に対して $0 \cdot \alpha = 0 \neq 1$ だからである. よって, $\mathfrak{o}_K^\times \subseteq K \setminus \{0\} = K^\times$.

$1 \in \mathfrak{o}_K^\times$ は明らかなので, $\mathfrak{o}_K^\times$ は空集合でない. また, 定理 7.4 より,

$$\alpha \in \mathfrak{o}_K^\times,\ \alpha \neq 0 \Longrightarrow \alpha^{-1} \in \mathfrak{o}_K^\times,$$
$$\alpha,\ \beta \in \mathfrak{o}_K^\times \Longrightarrow \alpha\beta \in \mathfrak{o}_K^\times.$$

したがって, $\mathfrak{o}_K^\times$ は $K^\times$ の部分群である. □

[定理 7.6] $\mathbb{Q} \cap \mathfrak{o}_K^\times = \{\pm 1\}$. ただし, $\mathfrak{o}_K^\times$ は代数体 K の単数群であるとする.

[証明] $\alpha \in \mathbb{Q} \cap \mathfrak{o}_K^\times$ とする. $\alpha \in \mathbb{Q} \cap \mathfrak{o}_K = \mathbb{Z}$ より,

$$\alpha^{-1} \in \mathbb{Q} \cap \mathfrak{o}_K^\times \subseteq \mathbb{Q} \cap \mathfrak{o}_K = \mathbb{Z}.$$

ゆえに, α は $\mathbb{Q}$ の単数である. すなわち, $\alpha \in \{\pm 1\}$. したがって, $\mathbb{Q} \cap \mathfrak{o}_K^\times \subseteq \{\pm 1\}$. 逆の包含関係は明らかである. □

8　2次体の単数

[定理 8.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\alpha \in \mathfrak{o}_K$ とする. このとき, α が単数ならば, K における α の共役 α^σ も単数である.

[証明] α を単数とすると, ある $\alpha' \in \mathfrak{o}_K$ が存在して $\alpha\alpha' = 1$. このとき, α^σ, $\alpha'^\sigma \in \mathfrak{o}_K$, $\alpha^\sigma\alpha'^\sigma = 1$. ゆえに, α^σ は単数である. □

[定理 8.2] K を 2 次体, $\mathfrak{o}_K$ を整数環, α, $\beta \in \mathfrak{o}_K$ とする. このとき, $\mathfrak{o}_K$ において α が β で割り切れるならば, $\mathbb{Z}$ において $N_K\alpha$ は $N_K\beta$ で割り切れる.

[証明] $\mathfrak{o}_K$ において α が β で割り切れるとすると, ある $\gamma \in \mathfrak{o}_K$ が存在して $\alpha = \beta\gamma$. ノルムをとると,

$$N_K\alpha = N_K(\beta\gamma) = N_K\beta N_K\gamma.$$

α, β, $\gamma \in \mathfrak{o}_K$ より, $N_K\alpha$, $N_K\beta$, $N_K\gamma \in \mathbb{Z}$. ゆえに, $\mathbb{Z}$ において $N_K\alpha$ は $N_K\beta$ で割り切れる. □

[定理 8.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\varepsilon \in K$ とする. このとき, ε が単数であるための必要十分条件は, $\varepsilon \in \mathfrak{o}_K$ かつ $|N_K\varepsilon| = 1$ となることである.

[証明] (条件の必要性)　ε を単数とすると, $\varepsilon \in \mathfrak{o}_K$ であり, ある $\varepsilon' \in \mathfrak{o}_K$ が存在して $\varepsilon\varepsilon' = 1$. 定理 8.2 より, $\mathbb{Z}$ において $1 = N_K1$ は $N_K\varepsilon$ で割り切れる. ゆえに, $N_K\varepsilon = \pm1$.

(条件の十分性)　$\varepsilon \in \mathfrak{o}_K$ かつ $|N_K\varepsilon| = 1$ とすると, $\varepsilon^\sigma \in \mathfrak{o}_K$ かつ $\varepsilon\varepsilon^\sigma = \pm1$. よって, $\varepsilon' = \pm\varepsilon^\sigma$ とおくと, $\varepsilon' \in \mathfrak{o}_K$, $\varepsilon\varepsilon' = 1$. □

[注意 8.1] 整数環の元でなくてもノルムの値が 1 になるものは存在する. 例えば, $K = \mathbb{Q}(\sqrt{-15})$, $\alpha = (1 + \sqrt{-15})/4$ とおくと, $\alpha \notin \mathfrak{o}_K$ かつ $N_K\alpha = 1$.

定理 8.3 より, 2 次体 K の単数群 $\mathfrak{o}_K^\times$ は

$$\mathfrak{o}_K^\times = \{\varepsilon \in \mathfrak{o}_K \mid |N_K\varepsilon| = 1\}$$

と表せる. さらに, K が虚 2 次体のとき, 0 でない元のノルムの値は常に正なので, $|N_K\varepsilon| = 1$ のところは $N_K\varepsilon = 1$ と書き換えられる.

[定理 8.4] K を虚 2 次体とする.

(i) $K = \mathbb{Q}(\sqrt{-1})$ のとき, K のすべての単数は ±1, $\pm\sqrt{-1}$.

(ii) $K=\mathbb{Q}(\sqrt{-3})$ のとき, K のすべての単数は ± 1, $\pm(1-\sqrt{-3})/2$, $\pm(1+\sqrt{-3})/2$.
(iii) それ以外のとき, K の単数は ± 1 のみ.

[証明] ε を K の単数とする. K は虚 2 次体なので, ある平方因子を含まない有理整数 $m>0$ が存在して $K=\mathbb{Q}(\sqrt{-m})$. よって,

$$\varepsilon = a+b\sqrt{-m}, \quad a, b \in \mathbb{Q}$$

と表される. また, 定理 8.3 の後に述べたことから, $N_K\varepsilon = 1$ である.

$b=0$ のとき, $\varepsilon = a \in \mathbb{Q}$. よって,

$$1 = N_K\varepsilon = N_K a = a^2 = \varepsilon^2.$$

ゆえに,

$$\varepsilon = \pm 1. \tag{12}$$

$b\neq 0$ のとき, $t=-\mathrm{Tr}_K\varepsilon$ とおくと, ε は 2 次方程式

$$X^2+tX+1=0$$

の解であるから,

$$\varepsilon = \frac{-t\pm\sqrt{t^2-4}}{2}.$$

$\varepsilon \in \mathfrak{o}_K$ より, $t\in\mathbb{Z}$. また, $\varepsilon = a+b\sqrt{-m}\notin\mathbb{R}$ より上の方程式の判別式 t^2-4 は負なので,

$$(t-2)(t+2) = t^2-4 < 0.$$

よって,

$$-2 < t < 2.$$

$t\in\mathbb{Z}$ であるから, $t=0, \pm 1$. ゆえに,

$$\varepsilon = \pm\sqrt{-1}, \quad \pm(1-\sqrt{-3})/2, \quad \pm(1+\sqrt{-3})/2. \tag{13}$$

したがって, K の単数となりうる $\mathbb{C}$ の元は (12), (13) がすべてである. $K=\mathbb{Q}(\sqrt{-1})$ のとき, K は ± 1, $\pm\sqrt{-1}$ のみを含む. $K=\mathbb{Q}(\sqrt{-3})$ のとき, K は ± 1, $\pm(1-\sqrt{-3})/2$, $\pm(1+\sqrt{-3})/2$ のみを含む. それ以外のとき, K は ± 1 のみを含む. □

[補題 8.5] 任意の $\theta\in\mathbb{R}$ と任意の $n\in\mathbb{Z}$, $n>0$ に対して, ある $x, y\in\mathbb{Z}$ が存在して,

$$|y\theta - x| < \frac{1}{n}, \quad 1\leq y\leq n$$

が成り立つ.

[証明] $y = 0, 1, \ldots, n$ とすると, $n+1$ 個の $y\theta$ が得られる. $x = \lfloor y\theta \rfloor$ とおくと,

$$0 \leq y\theta - x < 1.$$

よって, $y\theta - x$ は次の n 個の区間のいずれかに入る.

$$\left[0, \frac{1}{n}\right), \quad \left[\frac{1}{n}, \frac{2}{n}\right), \quad \ldots, \quad \left[\frac{n-1}{n}, 1\right)$$

$y\theta - x$ は $n+1$ 個あるので, 部屋割り論法により, 少なくとも 2 つは同一の区間に入る. それらを $y_1\theta - x_1$, $y_2\theta - x_2$ とし, $y_2 < y_1$ であるすると,

$$\begin{aligned} &|(y_1 - y_2)\theta - (x_1 - x_2)| \\ &\quad = |(y_1\theta - x_1) - (y_2\theta - x_2)| < \frac{1}{n} \end{aligned}$$

であるから, $x' = x_1 - x_2$, $y' = y_1 - y_2$ とおけば, x', $y' \in \mathbb{Z}$ かつ

$$|y'\theta - x'| < \frac{1}{n}, \quad 1 \leq y' \leq n$$

となる. □

[補題 8.6] K を実 2 次体, $\mathfrak{o}_K$ を K の整数環, d_K を K の判別式とする. このとき, 任意の $n \in \mathbb{Z}$, $n > 0$ に対して, ある $\alpha \in \mathfrak{o}_K$, $\alpha \neq 0$ が存在して,

$$|\alpha| < \frac{1}{n}, \quad |N_K\alpha| < 1 + \sqrt{d_K}$$

が成り立つ.

[証明] $1, \omega$ を K の標準的整数底とする. 補題 8.5 において $\theta = -\omega$ とおくと, ある x, $y \in \mathbb{Z}$ が存在して

$$|y\omega + x| < \frac{1}{n}, \quad 1 \leq y \leq n.$$

$\alpha = x + y\omega$ とおくと, $|\alpha| < 1/n$. また, $y \neq 0$ より, $\alpha \neq 0$.

一方, $\omega - \omega^\sigma = \sqrt{d_K}$ より

$$\begin{aligned} \alpha^\sigma &= x + y\omega^\sigma \\ &= (x + y\omega) - y(\omega - \omega^\sigma) \\ &= \alpha + y\sqrt{d_K} \end{aligned}$$

なので,

$$|\alpha^\sigma| \leq |\alpha| + y\sqrt{d_K} < \frac{1}{n} + n\sqrt{d_K}.$$

したがって, $N_K\alpha = \alpha\alpha^\sigma$ より,

$$\begin{aligned}|N_K\alpha| &= |\alpha||\alpha^\sigma| \\ &< \frac{1}{n}\left(\frac{1}{n} + n\sqrt{d_K}\right) = \frac{1}{n^2} + \sqrt{d_K} \\ &< 1 + \sqrt{d_K}.\end{aligned}$$

□

[定理 8.7] K を実 2 次体とする. このとき, K の単数で ± 1 とは異なるものが存在する.

[証明] K を実 2 次体, $\mathfrak{o}_K$ を K の整数環, d_K を K の判別式とする. 補題 8.6 より, 任意の $n \in \mathbb{Z}$, $n > 0$ に対して, ある $\alpha \in \mathfrak{o}_K$, $\alpha \neq 0$ が存在して,

$$|\alpha| < \frac{1}{n}, \quad |N_K\alpha| < 1 + \sqrt{d_K}. \tag{14}$$

そこで, まず $n_1 = 1$ に対して, (14) を満たす α を α_1 とおく. 次に, $n_2 > 1/|\alpha_1|$ なる n_2 に対して, (14) を満たす α を α_2 とおくと,

$$|\alpha_2| < \frac{1}{n_2} < |\alpha_1|.$$

同様の操作を続けると, $d = \lfloor 1 + \sqrt{d_K} \rfloor + 1$ とおくとき,

$$|\alpha_1| > |\alpha_2| > \cdots > |\alpha_{d^3}| > 0$$

なる $\mathfrak{o}_K$ の元 α_1, α_2, …, α_{d^3} が定まる. 各 α_i のノルムの絶対値は d より小さいので, 有理整数 c で $|N_K\alpha_i| = c$ となる α_i が d^2 個より多く存在するようなものが $1 \leq c < d$ の範囲に存在する.

そこで, $|N_K\alpha_i| = c$ を満たす α_i のすべてを β_1, β_2, …, $\beta_{d'}$ $(d' > d^2)$ とおく. ただし,

$$|\beta_1| > |\beta_2| > \cdots > |\beta_{d'}|$$

が成り立つように番号を振る. $1, \omega$ を K の標準的整数底とし, 各 $i = 1, 2, \ldots, d'$ に対して

$$\beta_i = r_i + s_i\omega, \quad r_i, s_i \in \mathbb{Z}$$

とおく. $c < d$ より $|\mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}| < d^2$ であるから, 部屋割り論法により, ある番号 $i < j$ が存在して

$$r_i \equiv r_j \pmod{c}, \quad s_i \equiv s_j \pmod{c}.$$

$r_i - r_j = cr$, $s_i - s_j = cs$ とおくと,

$$\beta_i - \beta_j = c(r + s\omega).$$

両辺を β_j で割ると,

$$\beta_i\beta_j^{-1} - 1 = c(r + s\omega)\beta_j^{-1}.$$

ゆえに, $\varepsilon = 1 + c(r + s\omega)\beta_j^{-1}$ とおくと,

$$\beta_i\beta_j^{-1} = \varepsilon.$$

$|N_K\beta_i| = |N_K\beta_j|$ なので,

$$\begin{aligned} |N_K\varepsilon| &= |N_K(\beta_i\beta_j^{-1})| = |N_K\beta_i N_K\beta_j^{-1}| \\ &= |N_K\beta_i||N_K\beta_j^{-1}| = |N_K\beta_i||N_K\beta_j|^{-1} \\ &= 1. \end{aligned}$$

また,

$$\beta_j\beta_j^{\sigma} = N_K\beta_j = \pm c$$

より

$$c\beta_j^{-1} = \pm\beta_j^{\sigma} \in \mathfrak{o}_K$$

であるから, $\varepsilon \in \mathfrak{o}_K$. したがって, ε は K の単数である.

$|\beta_i| > |\beta_j|$ より,

$$|\varepsilon| = |\beta_i||\beta_j|^{-1} > 1.$$

ゆえに, $\varepsilon \neq \pm 1$. □

[定理 8.8] K を実 2 次体とする. このとき, $\varepsilon > 1$ を満たす K の単数 ε が存在する. しかも, その中に最小のもの ε_0 が存在する. ε_0 を K の**基本単数**という.

[証明] 定理 8.7 より, K の単数 ε が存在して, $\varepsilon \neq \pm 1$. このとき, 次の 4 通りが考えられる.

(i) $\varepsilon > 1$.
(ii) $0 < \varepsilon < 1$.
(iii) $-1 < \varepsilon < 0$.
(iv) $\varepsilon < -1$.

(i) の場合, すべきことはない. (ii) の場合, ε の代わりに ε^{-1} をとればよい. (iii) の場合, ε の代わりに $-\varepsilon$ をとればよい. (iv) の場合, ε の代わりに $-\varepsilon^{-1}$ をとればよい. 以上より, 定理の前半が証明された.

さて, $\varepsilon > 1$ を K の単数, 1, ω を K の標準的整数底とする. これらの取り方は K にのみ依存することに注意せよ. K の単数は $\mathfrak{o}_K$ の元なので, $a + b\omega$, $a, b \in \mathbb{Z}$ を K の単数とし,

$$1 < a + b\omega \leq \varepsilon \tag{15}$$

とする. $N_K(a + b\omega) = \pm 1$ より,

$$-1 < a + b\omega^{\sigma} < 1. \tag{16}$$

(15), (16) より,

$$0 < b(\omega - \omega^\sigma) < 1 + \varepsilon.$$

d_K を K の判別式とすると, $\omega - \omega^\sigma = \sqrt{d_K} > 0$ より,

$$0 < b < \frac{1+\varepsilon}{\sqrt{d_K}}. \tag{17}$$

また, $\omega > 0$, $\omega^\sigma < 0$ だから, (15), (16) より,

$$\varepsilon\omega^\sigma \leq a\omega^\sigma + b\omega\omega^\sigma \leq \omega^\sigma,$$

$$-\omega < a\omega + b\omega\omega^\sigma < \omega.$$

よって,

$$-(\omega + \omega^\sigma) < a(\omega - \omega^\sigma) < \omega - \varepsilon\omega^\sigma.$$

$\omega - \omega^\sigma = \sqrt{d_K} > 0$ より,

$$-\frac{\omega + \omega^\sigma}{\sqrt{d_K}} < a < \frac{\omega - \varepsilon\omega^\sigma}{\sqrt{d_K}}. \tag{18}$$

$a, b \in \mathbb{Z}$ であるから, (17), (18) より, (15) を満たす単数 $a + b\omega$ は有限個しかない. したがって, その中に最小のものが存在する. それを ε_0 とすれば, ε_0 は 1 より大きい K の単数のうちで最小のものである. □

[定理 8.9] K を実 2 次体, ε_0 を K の基本単数とする. このとき, すべての単数は

$$\pm\varepsilon_0^n, \quad n \in \mathbb{Z}$$

の形で表される. 特に, 実 2 次体の単数は無限にある.

[証明] K の単数 ε を任意にとる.

$\varepsilon > 0$ のとき, $\varepsilon_0 > 1$ より, ある $n \in \mathbb{Z}$ が存在して

$$\varepsilon_0^n \leq \varepsilon < \varepsilon_0^{n+1}.$$

もし仮に $\varepsilon \neq \varepsilon_0^n$ とすると,

$$1 < \varepsilon\varepsilon_0^{-n} < \varepsilon_0.$$

$\varepsilon\varepsilon_0^{-n}$ もまた K の単数であるから, これは ε_0 の最小性に反する. ゆえに, $\varepsilon = \varepsilon_0^n$ でなければならない.

$\varepsilon < 0$ のとき, $-\varepsilon > 0$ なので, ある $n \in \mathbb{Z}$ が存在して $-\varepsilon = \varepsilon_0^n$. よって, $\varepsilon = -\varepsilon_0^n$.

最後の主張は, $\varepsilon_0 > 1$ より

$$1 < \varepsilon_0 < \varepsilon_0^2 < \cdots$$

であることからわかる. □

[定理 8.10] K を実 2 次体, ε_0 を K の基本単数, η を K の単数とする. このとき, すべての単数が

$$\pm\eta^n, \quad n \in \mathbb{Z}$$

の形で表されるための必要十分条件は, $\eta = \pm\varepsilon_0, \pm\varepsilon_0^{-1}$ となることである.

[証明] (条件の必要性)　まず, $\eta > 0$ のときを考える. 仮定より, ある $n_1 \in \mathbb{Z}$ が存在して $\varepsilon_0 = \pm\eta^{n_1}$ となるが, $\varepsilon_0 > 0$ より $\varepsilon_0 = \eta^{n_1}$. また, 定理 8.9 より, ある $n_2 \in \mathbb{Z}$ が存在して $\eta = \pm\varepsilon_0^{n_2}$. これに前式を代入すると, $\varepsilon_0 = \varepsilon_0^{n_1 n_2}$. ゆえに, $n_1 n_2 = 1$. したがって, $n_1 = \pm 1$ となり, $\eta = \varepsilon_0$ または ε_0^{-1}. 同様の議論により, $\eta < 0$ のとき, $\eta = -\varepsilon_0$ または $-\varepsilon_0^{-1}$.

(条件の十分性)　定理 8.9 より明らかである. □

9　代数体のイデアル

K を代数体, $\mathfrak{o}_K$ を K の整数環とする.

K の部分集合 $\mathfrak{a}$ が次の 3 つの条件を満たすとき, $\mathfrak{a}$ を K の**分数イデアル**あるいは単に K の**イデアル**という.

(i) $\mathfrak{a}$ は加法に関して K の部分群である.
(ii) 任意の $x \in \mathfrak{o}_K$, $\alpha \in \mathfrak{a}$ に対して, $x\alpha \in \mathfrak{a}$.
(iii) ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して, 任意の $\alpha \in \mathfrak{a}$ に対して, $c\alpha \in \mathfrak{o}_K$.

条件 (i), (ii) より, K の分数イデアル $\mathfrak{a}$ は $\mathfrak{o}_K$ 加群である.

K の分数イデアル $\mathfrak{a}$ が $\mathfrak{a} \subseteq \mathfrak{o}_K$ を満たすとき, $\mathfrak{a}$ を $\mathfrak{o}_K$ の**イデアル**あるいは K の**整イデアル**という. 一般に, K の部分集合 $\mathfrak{a}$ について, $\mathfrak{a} \subseteq \mathfrak{o}_K$ であることと条件 (iii) において $c = 1$ が取れることとは同値である. したがって, $\mathfrak{o}_K$ のイデアルとは, $\mathfrak{o}_K$ の部分集合 $\mathfrak{a}$ で条件 (i), (ii) を満たすもののことである.

$\mathfrak{a}$ を K の分数イデアルとすると, $\mathfrak{a} \cap \mathfrak{o}_K$ は整数環 $\mathfrak{o}_K$ の部分集合であり, かつ条件 (i), (ii) を満たす. よって, $\mathfrak{a} \cap \mathfrak{o}_K$ は $\mathfrak{o}_K$ のイデアルである. また, $\mathfrak{o}_K$ の任意の元 x に対して, $x\mathfrak{a} = \{x\alpha \mid \alpha \in \mathfrak{a}\}$ は K の分数イデアルである. 条件 (ii) より, $x\mathfrak{a} \subseteq \mathfrak{a}$. 特に, 条件 (iii) より, ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して, $c\mathfrak{a}$ は $\mathfrak{a}$ に含まれる $\mathfrak{o}_K$ のイデアルになる.

[注意 9.1] 代数体 K 自身は, 条件 (i), (ii) を満たすので $\mathfrak{o}_K$ 加群であるが, 条件 (iii) を満たさないので分数イデアルにはならない.

$\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ に対して,

$$\mathfrak{o}_K\alpha_1 + \mathfrak{o}_K\alpha_2 + \cdots + \mathfrak{o}_K\alpha_n = \{x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \mid x_i \in \mathfrak{o}_K\}$$

は K の分数イデアルである. これを α_1, α_2, …, α_n から**生成されるイデアル**といい,

$$(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

という記号で表す. また, α_1, α_2, …, α_n をイデアル $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ の**生成元**という. また, ただ 1 つの元 $\alpha \in K$ から生成されるイデアル

$$(\alpha) = \mathfrak{o}_K \alpha = \{x\alpha \mid x \in \mathfrak{o}_K\}$$

を**単項イデアル**という.

生成元がすべて $\mathfrak{o}_K$ の元であれば, 生成されるイデアルは $\mathfrak{o}_K$ のイデアルになる. 逆に, 生成元の中に $\mathfrak{o}_K$ の元でないものが 1 つでも含まれていれば, 生成されるイデアルは $\mathfrak{o}_K$ に含まれないので, $\mathfrak{o}_K$ のイデアルではない.

0 だけからなる集合 $\{0\}$ は, 0 から生成される $\mathfrak{o}_K$ の単項イデアルである. すなわち, $\{0\} = (0)$. これを**零イデアル**という. 任意の分数イデアルは零イデアルを含む.

また, $\mathfrak{o}_K$ 自身は, 1 から生成される $\mathfrak{o}_K$ の単項イデアルである. すなわち, $\mathfrak{o}_K = (1)$.

[定理 9.1] K を代数体, (α), (β) をそれぞれ α, $\beta \in K$ を生成元とする単項分数イデアルとする. また, $\mathfrak{o}_K^\times$ を K の単数群とする. このとき,

$$(\alpha) = (\beta) \Longleftrightarrow \alpha = \beta\varepsilon \ (\exists \varepsilon \in \mathfrak{o}_K^\times)$$

が成り立つ. 特に,

$$(\alpha) = \mathfrak{o}_K \Longleftrightarrow \alpha \in \mathfrak{o}_K^\times$$

である.

[証明] $(\Rightarrow)$ $(\alpha) = (\beta)$ とする. $\beta \in (\alpha) = \alpha\mathfrak{o}_K$ より, ある $\varepsilon \in \mathfrak{o}_K$ が存在して, $\beta = \alpha\varepsilon$. 一方, $\alpha \in (\beta) = \beta\mathfrak{o}_K$ より, ある $\varepsilon' \in \mathfrak{o}_K$ が存在して, $\alpha = \beta\varepsilon'$. ゆえに, $\alpha = \alpha\varepsilon\varepsilon'$. よって, $\alpha(\varepsilon\varepsilon' - 1) = 0$. これより, $\alpha = 0$ または $\varepsilon\varepsilon' = 1$ となる. $\alpha = 0$ の場合は, $\beta = 0$ となるので, $\alpha = \beta \cdot 1$ である. $\varepsilon\varepsilon' = 1$ の場合は, $\varepsilon \in \mathfrak{o}_K^\times$ である.

$(\Leftarrow)$ $\gamma \in (\alpha) = \alpha\mathfrak{o}_K$ とすると, ある $\gamma' \in \mathfrak{o}_K$ が存在して, $\gamma = \alpha\gamma'$. 一方, $\alpha = \beta\varepsilon$ であるから, $\gamma = \beta\varepsilon\gamma' \in \beta\mathfrak{o}_K = (\beta)$. よって, $(\alpha) \subseteq (\beta)$ である. $\beta = \alpha\varepsilon^{-1}$ を用いれば, 逆の包含関係も同様にして示せる.

後半の主張は, $\mathfrak{o}_K = (1)$ であることから, 前半の主張を $\beta = 1$ の場合に適用することにより得られる:

$$(\alpha) = \mathfrak{o}_K \Longleftrightarrow (\alpha) = (1) \Longleftrightarrow \alpha = \varepsilon \ (\exists \varepsilon \in \mathfrak{o}_K^\times) \Longleftrightarrow \alpha \in \mathfrak{o}_K^\times.$$

□

[定理 9.2] K を代数体とし, $\mathfrak{a}$, $\mathfrak{b}$ を K の分数イデアルとする.

(i) $\mathfrak{a} \cap \mathfrak{b}$ は K の分数イデアルである.

(ii) $\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta \mid \alpha \in \mathfrak{a},\, \beta \in \mathfrak{b}\}$ は K の分数イデアルである. これを $\mathfrak{a}$, $\mathfrak{b}$ の**和**という.

(iii) $\mathfrak{ab} = \{\sum_i \alpha_i\beta_i$ (有限和) $\mid \alpha_i \in \mathfrak{a},\, \beta_i \in \mathfrak{b}\}$ は K の分数イデアルである. これを $\mathfrak{a}$, $\mathfrak{b}$ の**積**という.

[証明] $\mathfrak{a}$, $\mathfrak{b}$ が $\mathfrak{o}_K$ 加群のとき, $\mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$ が $\mathfrak{o}_K$ 加群であることはすぐに確かめられる. 以下, イデアルの定義の条件 (iii) が成り立つことを確かめる.

$\mathfrak{a}$, $\mathfrak{b}$ は K の分数イデアルだから, イデアルの定義の条件 (iii) が成り立つ. すなわち, ある $c_1 \in \mathfrak{o}_K$, $c_1 \neq 0$ が存在して, 任意の $\alpha \in \mathfrak{a}$ に対して, $c_1\alpha \in \mathfrak{o}_K$. 同様に, ある $c_2 \in \mathfrak{o}_K$, $c_2 \neq 0$ が存在して, 任意の $\beta \in \mathfrak{b}$ に対して, $c_2\beta \in \mathfrak{o}_K$.

(i) $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ だから, 任意の $\alpha \in \mathfrak{a} \cap \mathfrak{b}$ に対して, $c_1\alpha \in \mathfrak{o}_K$.

(ii) 任意の $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$ に対して,

$$c_1c_2(\alpha + \beta) = c_2(c_1\alpha) + c_1(c_2\beta) \in \mathfrak{o}_K.$$

ここで, $c_1c_2 \neq 0$ であり, c_1c_2 は α, β には依存しない.

(iii) 任意の $\sum_i \alpha_i\beta_i \in \mathfrak{ab}$ に対して,

$$c_1c_2 \sum_i \alpha_i\beta_i = \sum_i (c_1\alpha_i)(c_2\beta_i) \in \mathfrak{o}_K.$$

ここで, $c_1c_2 \neq 0$ であり, c_1c_2 は $\mathfrak{ab}$ の元には依存しない. □

[例 9.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアル, $\gamma \in K$ とする. このとき,

$$(\gamma)\mathfrak{a} = \gamma\mathfrak{a}$$

が成り立つ. 実際, $\sum_i (\gamma x_i)\alpha_i$, $x_i \in \mathfrak{o}_K$, $\alpha_i \in \mathfrak{a}$ を $\mathfrak{a}$ の任意の元とすると,

$$\sum_i (\gamma x_i)\alpha_i = \gamma \left(\sum_i x_i\alpha_i \right) \in \gamma\mathfrak{a}.$$

ゆえに, $(\gamma)\mathfrak{a} \subseteq \gamma\mathfrak{a}$. 逆に, $\gamma\alpha$, $\alpha \in \mathfrak{a}$ を $\gamma\mathfrak{a}$ の任意の元とすると, 明らかに $\gamma\alpha \in (\gamma)\mathfrak{a}$ である. ゆえに, $\gamma\mathfrak{a} \subseteq (\gamma)\mathfrak{a}$.

[定理 9.3] K を代数体, α_1, α_2, …, α_r, β_1, β_2, …, $\beta_s \in K$ とし,

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_r), \quad \mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_s)$$

とおく.

(i) $\mathfrak{a} + \mathfrak{b} = (\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_s)$.

(ii) $\mathfrak{ab} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_1, \alpha_r\beta_2, \ldots, \alpha_r\beta_s)$.

[証明] (i) $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}_K\alpha_1 + \cdots + \mathfrak{o}_K\alpha_r + \mathfrak{o}_K\beta_1 + \cdots + \mathfrak{o}_K\beta_r$.

(ii) $\mathfrak{c} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_1, \alpha_r\beta_2, \ldots, \alpha_r\beta_s)$ とおく.

$\sum_i \xi_i\eta_i$, $\xi_i \in \mathfrak{a}$, $\eta_i \in \mathfrak{b}$ を $\mathfrak{ab}$ の任意の元とする. 各 ξ_i, η_i は

$$\xi_i = x_1^{(i)}\alpha_1 + x_2^{(i)}\alpha_2 + \cdots x_r^{(i)}\alpha_r, \quad x_j^{(i)} \in \mathfrak{o}_K,$$
$$\eta_i = y_1^{(i)}\beta_1 + y_2^{(i)}\beta_2 + \cdots y_s^{(i)}\beta_s, \quad y_k^{(i)} \in \mathfrak{o}_K$$

と表せるから,

$$\sum_i \xi_i\eta_i = \sum_i \left(\sum_{j,k} x_j^{(i)} y_k^{(i)} \alpha_j\beta_k \right) \in \mathfrak{c}.$$

ゆえに, $\mathfrak{ab} \subseteq \mathfrak{c}$. 逆に,

$$\mathfrak{c} = \sum_{i,j} \mathfrak{o}_K\alpha_i\beta_j \subseteq \mathfrak{ab}.$$

したがって, $\mathfrak{ab} = \mathfrak{c}$. □

K の任意の分数イデアル $\mathfrak{a}$, $\mathfrak{b}$ に対して,

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}, \quad (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{ab}$$

が成り立つことはすぐにわかる. また, $\mathfrak{a}$, $\mathfrak{b}$ がともに $\mathfrak{o}_K$ のイデアルであるとき,

$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$$

が成り立つ.

[注意 9.2] 整数環のイデアルではない分数イデアル $\mathfrak{a}$, $\mathfrak{b}$ に対しては $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ が一般には成立しない. 例えば, $K = \mathbb{Q}$, $\mathfrak{o}_K = \mathbb{Z}$ のとき,

$$\frac{1}{2}\mathbb{Z} \cdot \frac{1}{4}\mathbb{Z} = \frac{1}{8}\mathbb{Z} \supsetneq \frac{1}{4}\mathbb{Z} = \frac{1}{2}\mathbb{Z} \cap \frac{1}{4}\mathbb{Z}$$

となる.

代数体 K の整数環 $\mathfrak{o}_K$ のイデアル $\mathfrak{a}$, $\mathfrak{b}$ が**互いに素**であるとは, $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}_K$ が成り立つときにいう. $\mathfrak{a}$, $\mathfrak{b}$ が互いに素であることを, 記号 $(\mathfrak{a}, \mathfrak{b}) = 1$ で表す. $\mathfrak{a}$, $\mathfrak{b}$ が互いに素になるための必要十分条件は, ある $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$ が存在して $1 = \alpha + \beta$ が成り立つことである.

[定理 9.4] K を代数体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を $\mathfrak{o}_K$ のイデアルとし, $(\mathfrak{a}, \mathfrak{b}) = 1$ であるとする. このとき, $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$ が成り立つ.

[証明] $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ は明らかなので, 逆の包含関係を示す.

$1 \in \mathfrak{o}_K = \mathfrak{a} + \mathfrak{b}$ より,

$$1 = \alpha + \beta, \quad \alpha \in \mathfrak{a},\, \beta \in \mathfrak{b}$$

と表せる. よって, 任意の $\gamma \in \mathfrak{a} \cap \mathfrak{b}$ に対して,

$$\gamma = \gamma(\alpha + \beta) = \alpha\gamma + \gamma\beta \in \mathfrak{ab}.$$

ゆえに, $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$. □

[定理 9.5] K を代数体, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ を K の分数イデアルとする.

(i) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$.

(ii) $\mathfrak{ab} = \mathfrak{ba}$.

(iii) $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$.

(iv) $(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{ab} + \mathfrak{ac}$.

[証明] (i) $\alpha_i + \beta_i$, $\alpha_i \in \mathfrak{a}$, $\beta_i \in \mathfrak{b}$ を $\mathfrak{a} + \mathfrak{b}$ の任意の元とすると,

$$\alpha_i + \beta_i = \beta_i + \alpha_i \in \mathfrak{b} + \mathfrak{a}.$$

ゆえに, $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{b} + \mathfrak{a}$. 逆の包含関係も同様にして示せる.

(ii) $\sum_i \alpha_i\beta_i$, $\alpha_i \in \mathfrak{a}$, $\beta_i \in \mathfrak{b}$ を $\mathfrak{ab}$ の任意の元とすると,

$$\sum_i \alpha_i\beta_i = \sum_i \beta_i\alpha_i \in \mathfrak{ba}.$$

ゆえに, $\mathfrak{ab} \subseteq \mathfrak{ba}$. 逆の包含関係も同様にして示せる.

(iii) $\sum_i \xi_i\gamma_i$, $\xi_i \in \mathfrak{ab}$, $\gamma_i \in \mathfrak{c}$ を $(\mathfrak{ab})\mathfrak{c}$ の任意の元とする. 各 ξ_i は

$$\xi_i = \sum_{j=1}^{r_i} \alpha_j^{(i)}\beta_j^{(i)}, \quad \alpha_j^{(i)} \in \mathfrak{a},\, \beta_j^{(i)} \in \mathfrak{b}$$

のように表せるから,

$$\sum_i \xi_i\gamma_i = \sum_i \left(\sum_{j=1}^{r_i} \alpha_j^{(i)}\beta_j^{(i)} \right) \gamma_i = \sum_i \left(\sum_{j=1}^{r_i} \alpha_j^{(i)}(\beta_j^{(i)}\gamma_i) \right) \in \mathfrak{a}(\mathfrak{bc}).$$

ゆえに, $(\mathfrak{ab})\mathfrak{c} \subseteq \mathfrak{a}(\mathfrak{bc})$. 逆の包含関係も同様にして示せる.

(iv) $\sum_i \xi_i\gamma_i$, $\xi_i \in \mathfrak{a} + \mathfrak{b}$, $\gamma_i \in \mathfrak{c}$ を $(\mathfrak{a} + \mathfrak{b})\mathfrak{c}$ の任意の元とする. 各 ξ_i は

$$\xi_i = \alpha_i + \beta_i, \quad \alpha_i \in \mathfrak{a},\, \beta_i \in \mathfrak{b}$$

と表せるから,

$$\begin{aligned}\sum_i \xi_i\gamma_i &= \sum_i (\alpha_i+\beta_i)\gamma_i \\ &= \sum_i \alpha_i\gamma_i + \sum_i \beta_i\gamma_i \\ &\in \mathfrak{ab}+\mathfrak{ac}.\end{aligned}$$

ゆえに, $(\mathfrak{a}+\mathfrak{b})\mathfrak{c} \subseteq \mathfrak{ab}+\mathfrak{ac}$.

逆に, $\xi+\eta$, $\xi \in \mathfrak{ac}$, $\eta \in \mathfrak{bc}$ を $\mathfrak{ac}+\mathfrak{bc}$ の任意の元とする. ξ, η は

$$\begin{aligned}\xi &= \sum_i \alpha_i\gamma_i, \quad \alpha_i \in \mathfrak{a},\ \gamma_i \in \mathfrak{c}, \\ \eta &= \sum_j \beta_j\gamma'_j, \quad \beta_j \in \mathfrak{b},\ \gamma'_j \in \mathfrak{c}\end{aligned}$$

と表せるから,

$$\begin{aligned}\xi+\eta &= \sum_i \alpha_i\gamma_i + \sum_j \beta_j\gamma'_j \\ &= \sum_i (\alpha_i+0)\gamma_i + \sum_j (0+\beta_j)\gamma'_j \\ &\in (\mathfrak{a}+\mathfrak{b})\mathfrak{c}.\end{aligned}$$

ゆえに, 逆の包含関係もいえる. □

[定理 9.6] K を代数体, $\mathfrak{a}$, $\mathfrak{b}$ を K の分数イデアルとし, $\mathfrak{a} \neq (0)$ とする. このとき,

$$\mathfrak{b}:\mathfrak{a} = \{\gamma \in K \mid \gamma\mathfrak{a} \subseteq \mathfrak{b}\}$$

は K の分数イデアルである. $\mathfrak{b}:\mathfrak{a}$ を $\mathfrak{b}$ の $\mathfrak{a}$ による**商イデアル**という.

[証明] $\mathfrak{c} = \mathfrak{b}:\mathfrak{a}$ とおく.

$$\begin{aligned}\alpha,\ \beta \in \mathfrak{c} &\Longrightarrow \alpha\mathfrak{a} \subseteq \mathfrak{b},\ \beta\mathfrak{a} \subseteq \mathfrak{b} \\ &\Longrightarrow (\alpha-\beta)\mathfrak{a} \subseteq \mathfrak{b} \\ &\Longrightarrow \alpha-\beta \in \mathfrak{c}, \\ \alpha \in \mathfrak{c},\ x \in \mathfrak{o}_K &\Longrightarrow x\alpha\mathfrak{a} \subseteq x\mathfrak{b} \subseteq \mathfrak{b} \\ &\Longrightarrow x\alpha \in \mathfrak{c}.\end{aligned}$$

よって, $\mathfrak{c}$ は $\mathfrak{o}_K$ 加群である.

$\mathfrak{a} \neq (0)$ より, $\mathfrak{a}$ は 0 でない元 α をもつ. $\mathfrak{a}$ は分数イデアルだから, ある $c_1 \in \mathfrak{o}_K$, $c_1 \neq 0$ が存在して, $c_1\alpha \in \mathfrak{o}_K$ となる. またこのとき, $c_1\alpha \in \mathfrak{a}$, $c_1\alpha \neq 0$ である. 一方, $\mathfrak{b}$ は分数イデアルだから, ある $c_2 \in \mathfrak{o}_K$, $c_2 \neq 0$ が存在して, $c_2\mathfrak{b} \subseteq \mathfrak{o}_K$. ゆえに, 任意の $\gamma \in \mathfrak{c}$ に対して,

$$c_2(c_1\alpha)\gamma = c_2\gamma(c_1\alpha) \in c_2\mathfrak{b} \subseteq \mathfrak{o}_K.$$

すなわち, $c = c_2(c_1\alpha)$ とおけば, $c \in \mathfrak{o}_K$, $c \neq 0$ であり, 任意の $\gamma \in \mathfrak{c}$ に対して $c\gamma \in \mathfrak{o}_K$ が成り立つ.
□

K の分数イデアル $\mathfrak{a} \neq (0)$ に対して, $\mathfrak{o}_K$ の $\mathfrak{a}$ による商イデアル

$$\mathfrak{o}_K : \mathfrak{a} = \{\gamma \in K \mid \gamma\mathfrak{a} \subseteq \mathfrak{o}_K\}$$

を $\mathfrak{a}$ の**逆イデアル**といい, $\mathfrak{a}^{-1}$ で表す.

[定理 9.7] K を代数体, $\mathfrak{a}$, $\mathfrak{b}$ を K の (0) でない分数イデアルとする.

(i) $\mathfrak{a}^{-1} \neq (0)$.
(ii) $\mathfrak{a} \subseteq \mathfrak{b} \Longrightarrow \mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$.
(iii) $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{o}_K$.
(iv) $\mathfrak{a}\mathfrak{b} = \mathfrak{o}_K \Longrightarrow \mathfrak{a} = \mathfrak{b}^{-1}$.

[証明] (i) $\mathfrak{a}$ は分数イデアルだから, ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して $c\mathfrak{a} \subseteq \mathfrak{o}_K$. よって, $c \in \mathfrak{a}^{-1}$ であるから, $\mathfrak{a}^{-1} \neq (0)$.

(ii) $\gamma \in \mathfrak{b}^{-1} \Longrightarrow \gamma\mathfrak{b} \subseteq \mathfrak{o}_K \Longrightarrow \gamma\mathfrak{a} \subseteq \mathfrak{o}_K \Longrightarrow \gamma \in \mathfrak{a}^{-1}$.

(iii) $\mathfrak{a}^{-1}\mathfrak{a}$ の元 $\sum_i \alpha_i'\alpha_i$, $\alpha_i \in \mathfrak{a}$, $\alpha_i' \in \mathfrak{a}^{-1}$ を任意にとると, 各 i について $\alpha_i'\alpha_i \in \alpha_i'\mathfrak{a} \subseteq \mathfrak{o}_K$. ゆえに, $\sum_i \alpha_i'\alpha_i \in \mathfrak{o}_K$. したがって, $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{o}_K$.

(iv) 任意の $\alpha \in \mathfrak{a}$ に対して, $\alpha\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} = \mathfrak{o}_K$ より $\alpha \in \mathfrak{b}^{-1}$. ゆえに, $\mathfrak{a} \subseteq \mathfrak{b}^{-1}$. 逆に, $\mathfrak{b}^{-1}\mathfrak{b} \subseteq \mathfrak{o}_K$ より,

$$\mathfrak{b}^{-1} = \mathfrak{o}_K\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1} \subseteq \mathfrak{a}\mathfrak{o}_K = \mathfrak{a}.$$

□

[例 9.2] K を代数体とし, $\alpha \in K$, $\alpha \neq 0$ とする.

$$(\alpha)(\alpha^{-1}) = (\alpha\alpha^{-1}) = (1) = \mathfrak{o}_K$$

であるから, (α) の逆イデアルは (α^{-1}) である.

10 2 次体のイデアル

K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアルとする. $\omega_1, \omega_2 \in K$ が $\mathfrak{a}$ の**基底**であるとは, 任意の $\alpha \in \mathfrak{a}$ が

$$\alpha = a\omega_1 + b\omega_2, \quad a, b \in \mathbb{Z}$$

と一意的に表されるときにいう. ω_1, ω_2 が $\mathfrak{a}$ の基底であることを, 記号で

$$\mathfrak{a} = [\omega_1, \omega_2]$$

と表す.

[補題 10.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアルとする. このとき, $\omega_1, \omega_2 \in K$ が $\mathfrak{a}$ の基底であるための必要十分条件は, 次の 2 つの条件を満たすことである.

(i) $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.
(ii) ω_1, ω_2 は $\mathbb{Z}$ 上 1 次独立である.

[証明] 補題 5.1 と同様にして証明できる. □

イデアルの基底は生成元である. 実際, $\mathfrak{a}$ を 2 次体 K の分数イデアルとし, $\mathfrak{a} = [\omega_1, \omega_2]$ とすると,

$$\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathfrak{o}_K\omega_1 + \mathfrak{o}_K\omega_2 \subseteq \mathfrak{a}$$

より,

$$\mathfrak{a} = \mathfrak{o}_K\omega_1 + \mathfrak{o}_K\omega_2 = (\omega_1, \omega_2).$$

しかし, 逆は必ずしも成立しない. 例えば, 1 は $\mathfrak{o}_K$ の生成元であるが基底ではない.

$\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルであれば, その基底は $\mathfrak{o}_K$ の元である.

$\mathfrak{o}_K$ 自身は $\mathfrak{o}_K$ のイデアルであるが, $\mathfrak{o}_K$ の基底とはまさに K の整数底のことである.

[補題 10.2] 2 次体 K の任意の分数イデアル $\mathfrak{a} \neq (0)$ は, ある 0 でない有理整数を含む.

[証明] $\mathfrak{a}$ を K の (0) でない分数イデアルとする. $\mathfrak{a} \cap \mathfrak{o}_K$ は $\mathfrak{a}$ に含まれる $\mathfrak{o}_K$ のイデアルであり, これが 0 でない有理整数を含むことをいえばよい. したがって, $\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルである場合を証明すれば十分である.

$\mathfrak{a} \neq (0)$ より, $\mathfrak{a}$ は 0 でない元 α をもつ. $\mathfrak{a} \subseteq \mathfrak{o}_K$ より $\alpha \in \mathfrak{o}_K$, したがって $\alpha^\sigma \in \mathfrak{o}_K$ であるから,

$$N_K\alpha = \alpha\alpha^\sigma \in \mathfrak{a}.$$

一方, $\alpha \in \mathfrak{o}_K$, $\alpha \neq 0$ より, $N_K\alpha$ は 0 でない有理整数である. □

[補題 10.3] K を 2 次体, $\mathfrak{a}$ を K の分数イデアル, a_0 を $\mathfrak{a}$ に含まれる最小正の有理整数とする. このとき, 任意の $b \in \mathbb{Z}$ に対して,

$$b \in \mathfrak{a} \Longleftrightarrow b \text{ は } a_0 \text{ の } \mathbb{Z} \text{ における倍数}$$

が成り立つ.

[証明] ($\Rightarrow$)　有理整数における除法の原理より, ある $q, r \in \mathbb{Z}$ が存在して,

$$b = a_0 q + r, \quad 0 \leq r < a_0.$$

$b, a_0 q \in \mathfrak{a}$ より,

$$r = b - a_0 q \in \mathfrak{a}.$$

a_0 の最小性より, $r = 0$. すなわち, b は a_0 の倍数である.

($\Leftarrow$)　b は a_0 の $\mathbb{Z}$ における倍数だから, ある $x \in \mathbb{Z}$ が存在して, $b = a_0 x$. 有理整数はすべて $\mathfrak{o}_K$ の元だから, $b = a_0 x \in \mathfrak{a}$. □

[定理 10.4] K を 2 次体, $\mathfrak{a}$ を K の (0) でない分数イデアルとする. このとき, $\mathfrak{a}$ に含まれる最小正の有理整数 a_0 が存在して, $\mathbb{Z} \cap \mathfrak{a} = a_0\mathbb{Z}$ が成り立つ. したがって特に, $\mathbb{Z} \cap \mathfrak{a}$ は $\mathbb{Z}$ の (0) でないイデアルである.

[証明] 補題 10.2 より, ある $a \in \mathbb{Z}$, $a \neq 0$ が存在して, $a \in \mathfrak{a}$. このとき, $-a \in \mathfrak{a}$ でもある. $\pm a$ の一方は正だから, $\mathfrak{a}$ は正の有理整数を含む. 自然数の整列性により, $\mathfrak{a}$ に含まれる最小正の有理整数 a_0 が存在する.

補題 10.3 より,

$$\begin{aligned} x \in \mathbb{Z} \cap \mathfrak{a} &\iff x \in \mathbb{Z} \text{ かつ } x \in \mathfrak{a} \\ &\iff x \text{ は } a_0 \text{ の } \mathbb{Z} \text{ における倍数} \\ &\iff x \in a_0\mathbb{Z}. \end{aligned}$$

ゆえに, $\mathbb{Z} \cap \mathfrak{a} = a_0\mathbb{Z}$. □

[例 10.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $a \in \mathbb{Z}$, $a > 0$ とする. このとき, $(a) = a\mathfrak{o}_K$ に含まれる最小正の有理整数は a である. 定理 10.4 より, $a\mathfrak{o}_K \cap \mathbb{Z} = a\mathbb{Z}$. したがって, 2 つの有理整数 a, b について, b が $\mathfrak{o}_K$ における a の倍数ならば, b は $\mathbb{Z}$ における a の倍数である.

a が $a\mathfrak{o}_K$ に含まれる最小正の有理整数であることは次のようにして示される. $a\mathfrak{o}_K$ に含まれる正の有理整数 b を任意にとると, ある $x \in \mathfrak{o}_K$ が存在して, $b = ax$. すると, $x = b/a \in \mathbb{Q}$. よって, $x \in \mathbb{Q} \cap \mathfrak{o}_K = \mathbb{Z}$. さらに, $a > 0$, $b > 0$ より $x > 0$. ゆえに, $a \leq ax = b$ となる.

[補題 10.5] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $1, \omega$ を K の標準的整数底, $\mathfrak{a} \neq (0)$ を K の分数イデアルとする. このとき,

$$I_{\mathfrak{a}} = \{c \in \mathbb{Z} \mid b + c\omega \in \mathfrak{a}\,(\exists b \in \mathbb{Z})\}$$

は $\mathbb{Z}$ の (0) でないイデアルである. さらに, c_0 を $I_{\mathfrak{a}}$ の生成元, すなわち $I_{\mathfrak{a}} = c_0\mathbb{Z}$ であるとすれば, 任意の $b, c \in \mathbb{Z}$ に対して,

$$b + c\omega \in \mathfrak{a} \Longrightarrow c_0 \mid b,\ c_0 \mid c$$

が成り立つ. 特に, $\mathfrak{a}$ に含まれるすべての有理整数は c_0 の倍数である.

[証明] $I_\mathfrak{a}$ は $\mathbb{Z}$ の部分集合である. また, $0+0\cdot\omega=0\in\mathfrak{a}$ より $0\in I_\mathfrak{a}$ であるから, $I_\mathfrak{a}$ は空集合でない.

$c, c'\in I_\mathfrak{a}$, $r\in\mathbb{Z}$ を任意にとる. ある $b, b'\in\mathbb{Z}$ が存在して, $b+c\omega$, $b'+c'\omega\in\mathfrak{a}$. このとき,

$$(b-b')+(c-c')\omega=(b+c\omega)-(b'+c'\omega)\in\mathfrak{a},$$
$$(rb)+(rc)\omega=r(b+c\omega)\in\mathfrak{a}.$$

ゆえに, $b-b'$, $rb\in I_\mathfrak{a}$. したがって, $I_\mathfrak{a}$ は $\mathbb{Z}$ のイデアルである. $\mathfrak{a}\neq(0)$ だから, 補題 10.2 より $\mathfrak{a}$ に含まれる有理整数 a が存在する. $\omega\in\mathfrak{o}_K$ より, $a\omega\in\mathfrak{a}$. ゆえに, $a\in I_\mathfrak{a}$. したがって, $I_\mathfrak{a}\neq(0)$.

$\mathbb{Z}$ は単項イデアル整域なので, $I_\mathfrak{a}$ はただ 1 つの元から生成される. c_0 を $I_\mathfrak{a}$ の生成元とする. $I_\mathfrak{a}\neq(0)$ だから, $c_0\neq0$ である.

$b, c\in\mathbb{Z}$ とし, $b+c\omega\in\mathfrak{a}$ とする. $c\in I_\mathfrak{a}=c_0\mathbb{Z}$ だから, $c_0\mid c$ となる.

さて, $K=\mathbb{Q}(\sqrt{m})$ と表す. ただし, $m\neq0, 1$ は平方因子を含まない有理整数である.

$m\equiv1\pmod4$ のとき, $\omega=(1+\sqrt{m})/2$ だから,

$$\mathfrak{a}\ni(b+c\omega)\omega=\frac{1-m}{4}c+(b+c)\omega.$$

よって, $(b+c)\in I_\mathfrak{a}=c_0\mathbb{Z}$. ゆえに, $c_0\mid(b+c)$. 先に $c_0\mid c$ を示したから, $c_0\mid b$.

$m\equiv2, 3\pmod4$ のとき, $\omega=\sqrt{m}$ だから,

$$\mathfrak{a}\ni(b+c\omega)\omega=cm+b\omega.$$

よって, $b\in I_\mathfrak{a}=c_0\mathbb{Z}$. ゆえに, $c_0\mid b$.

特に, $c=0$ の場合を考えれば, $\mathfrak{a}$ に含まれるすべての有理整数が c_0 で割れることがわかる. □

[定理 10.6] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $1, \omega$ を K の標準的整数底, $\mathfrak{a}\neq(0)$ を $\mathfrak{o}_K$ のイデアルとする. さらに, a_0 を $\mathfrak{a}$ に含まれる最小正の有理整数, c_0 を補題 10.5 における $\mathbb{Z}$ のイデアル $I_\mathfrak{a}$ の生成元のうち正であるものとする. このとき, $b+c_0\omega\in\mathfrak{a}$ であるような任意の $b\in\mathbb{Z}$ に対して,

$$\mathfrak{a}=[a_0,\ b+c_0\omega]$$

が成り立つ. また, $b+c_0\omega\in\mathfrak{a}$ であるような $b\in\mathbb{Z}$ は必ず存在する.

$a_0, b+c_0\omega$ を $\mathfrak{a}$ の**標準的基底**という.

[証明] 定理 10.4 より, $\mathfrak{a}$ に含まれる最小正の有理整数 a_0 が存在して, $\mathbb{Z}\cap\mathfrak{a}=a_0\mathbb{Z}$ となる. $I_\mathfrak{a}$ を補題 10.5 における $\mathbb{Z}$ のイデアルとすると, ある正の有理整数 c_0 によって $I_\mathfrak{a}=c_0\mathbb{Z}$ と表せる. また, $I_\mathfrak{a}$ の定義より, ある $b_0\in\mathbb{Z}$ が存在して, $b_0+c_0\omega\in\mathfrak{a}$ となる.

$b \in \mathbb{Z}$, $b + c_0\omega \in \mathfrak{a}$ とすると, $\mathbb{Z}a_0 + \mathbb{Z}(b + c_0\omega) \subseteq \mathfrak{a}$ である.

逆に, $\alpha \in \mathfrak{a}$ とすると, $\mathfrak{a} \subseteq \mathfrak{o}_K = [1, \omega]$ より, $\alpha = u + v\omega$, u, $v \in \mathbb{Z}$ と表せる. $I_\mathfrak{a}$ の定義より $v \in I_\mathfrak{a} = c_0\mathbb{Z}$ だから, ある $y \in \mathbb{Z}$ が存在して, $v = c_0 y$. よって,

$$\alpha - y(b + c_0\omega) = (u + v\omega) - (by + v\omega) = u - by \in \mathbb{Z}.$$

一方, $\alpha - y(b + c_0\omega) \in \mathfrak{a}$ でもあるから,

$$\alpha - y(b + c_0\omega) \in \mathbb{Z} \cap \mathfrak{a} = a_0\mathbb{Z}.$$

したがって, $\mathfrak{a} \subseteq \mathbb{Z}a_0 + \mathbb{Z}(b + c_0\omega)$ もいえる.

$\mathfrak{o}_K = [1, \omega]$, $a_0 \neq 0$, $c_0 \neq 0$ より, 任意の x, $y \in \mathbb{Z}$ に対して,

$$\begin{aligned} & xa_0 + y(b + c_0\omega) = 0 \\ & \quad \Longrightarrow xa_0 + yb = c_0 y = 0 \\ & \quad \Longrightarrow x = y = 0. \end{aligned}$$

よって, a_0, $b + c_0\omega$ は $\mathbb{Z}$ 上 1 次独立である.

したがって, 補題 10.1 より, $\mathfrak{a} = [a_0, b + c_0\omega]$ が成り立つ. □

[定理 10.7] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を $\mathfrak{o}_K$ のイデアルとする. また, a_0, $b_0 + c_0\omega$ を $\mathfrak{a}$ の標準的基底とする. このとき, 任意の $b \in \mathbb{Z}$ に対して,

$$b + c_0\omega \in \mathfrak{a} \Longleftrightarrow b \equiv b_0 \pmod{a_0}$$

が成り立つ.

[証明] ($\Rightarrow$) $b + c_0\omega \in \mathfrak{a}$ であるとする. 除法の原理により, ある q, r, q_0, $r_0 \in \mathbb{Z}$ が存在して,

$$\begin{aligned} b &= a_0 q + r, \qquad 0 \leq r < a_0, \\ b_0 &= a_0 q_0 + r_0, \quad 0 \leq r_0 < a_0. \end{aligned}$$

このとき,

$$\begin{aligned} r - r_0 &= b - b_0 - a_0(q - q_0) \\ &= (b + c_0\omega) - (b_0 + c_0\omega) - a_0(q - q_0) \in \mathfrak{a}. \end{aligned}$$

ゆえに, $|r - r_0| = \pm(r - r_0) \in \mathfrak{a}$ となる. $0 \leq |r - r_0| < a_0$ であるから, a_0 の最小性より, $r = r_0$ となる. したがって, $b \equiv b_0 \pmod{a_0}$.

($\Leftarrow$) $b \equiv b_0 \pmod{a_0}$ とすると, ある $s \in \mathbb{Z}$ が存在して, $b = b_0 + a_0 s$. このとき,

$$b + c_0\omega = a_0 s + (b_0 + c_0\omega) \in \mathfrak{a}.$$

となる. □

[定理 10.8] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, 1, ω を K の標準的整数底, a, b, $c \in \mathbb{Z}$, $a > 0$, $c > 0$ とする. このとき,

$$\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}(b + c\omega)$$

が $\mathfrak{o}_K$ のイデアルならば,

$$\mathbb{Z} \cap \mathfrak{a} = a\mathbb{Z}, \quad I_{\mathfrak{a}} = c\mathbb{Z}$$

であり, a, $b + c\omega$ は $\mathfrak{a}$ の標準的基底である. また,

$$N_K(b + c\omega) \in a\mathbb{Z}$$

が成り立つ.

[証明] $\mathfrak{a}$ を $\mathfrak{o}_K$ のイデアルとする. 任意の $r \in \mathbb{Z} \cap \mathfrak{a}$ に対して, ある s, $t \in \mathbb{Z}$ が存在して,

$$r = sa + t(b + c\omega) = (sa + tb) + ct\omega.$$

$\mathfrak{o}_K = [1, \omega]$ だから,

$$r = sa + tb, \quad ct = 0.$$

$c \neq 0$ より, $t = 0$. よって, $r = sa \in a\mathbb{Z}$. ゆえに, $\mathbb{Z} \cap \mathfrak{a} \subseteq a\mathbb{Z}$. 逆の包含関係は明らかだから, $\mathbb{Z} \cap \mathfrak{a} = a\mathbb{Z}$ となる.

また, $b + c\omega \in \mathfrak{a}$ より $c \in I_{\mathfrak{a}}$ だから, $c\mathbb{Z} \subseteq I_{\mathfrak{a}}$. 逆に, $\alpha \in \mathfrak{a}$ を任意にとると, ある x, $y \in \mathbb{Z}$ が存在して,

$$\alpha = xa + y(b + c\omega) = (xa + yb) + cy\omega.$$

この表し方は α に対して一意的である. ゆえに, $I_{\mathfrak{a}} \subseteq c\mathbb{Z}$. したがって, $I_{\mathfrak{a}} = c\mathbb{Z}$.

定理 10.6 より, a, $b + c\omega$ は $\mathfrak{a}$ の標準的基底である.

さらに, $b + c\omega \in \mathfrak{a}$, $(b + c\omega)^\sigma \in \mathfrak{o}_K$ より,

$$N_K(b + c\omega) = (b + c\omega)(b + c\omega)^\sigma \in \mathbb{Z} \cap \mathfrak{a} = a\mathbb{Z}$$

となる. □

O_K のイデアル $\mathfrak{a}$ が

$$\mathfrak{a} = [a, b + c\omega], \quad a, b, c, \in \mathbb{Z}, \quad a > 0, c > 0$$

と表されているとき, 定理 10.8 より, a, $b + c\omega$ は必ず $\mathfrak{a}$ の標準的基底になる.

[定理 10.9] K を代数体, $\mathfrak{a} \neq (0)$ を K の分数イデアルとする. このとき, ある ω_1, $\omega_2 \in K$ が存在して, $\mathfrak{a} = [\omega_1, \omega_2]$ となる.

[証明] $\mathfrak{a}$ は分数イデアルだから, ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して, $c\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルになる. 定理 10.6 より, ある α_1, $\alpha_2 \in \mathfrak{o}_K$ が存在して, $c\alpha = [\alpha_1, \alpha_2]$ が成り立つ. $\omega_1 = \alpha_1/c$, $\omega_2 = \alpha_2/c$ とおくと, $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ となる. また, 任意の x, $y \in \mathbb{Z}$ に対して,

$$\begin{aligned} x\omega_1 + y\omega_2 = 0 &\Longrightarrow \frac{1}{c}(x\alpha_1 + y\alpha_2) = 0 \\ &\Longrightarrow x\alpha_1 + y\alpha_2 = 0 \\ &\Longrightarrow x = y = 0. \end{aligned}$$

よって, ω_1, ω_2 は $\mathbb{Z}$ 上 1 次独立である. ゆえに, 補題 10.1 より, $\mathfrak{a} = [\omega_1, \omega_2]$. □

[定理 10.10] K を 2 次体, $\mathfrak{a}$ を K の分数イデアルとする. このとき, ある $c \in \mathbb{Z}$, $c > 0$ が存在して, $c\mathfrak{a} \subseteq \mathfrak{o}_K$ となる.

[証明] 定理 10.9 より, $\mathfrak{a}$ は基底 ω_1, $\omega_2 \in K$ をもつ. ω_1, ω_2 は代数的数だから, ある c_1, $c_2 \in \mathbb{Z}$, $c > 0$ が存在して, $c_1\omega_1$, $c_2\omega_2$ は代数的整数となる. このとき, $c = c_1c_2$ とおくと, $c \in \mathbb{Z}$, $c > 0$ かつ

$$\begin{aligned} c\mathfrak{a} &= c_1c_2(\omega_1, \omega_2) \\ &= (c_1c_2\omega_1, c_1c_2\omega_2) \\ &\subseteq K \cap \overline{\mathbb{Z}} = \mathfrak{o}_K. \end{aligned}$$

□

[定理 10.11] K を 2 次体, $\mathfrak{a} \neq (0)$ を K の分数イデアルとし, $\mathfrak{a} = [\omega_1, \omega_2]$ であるとする. このとき, 任意の $\gamma \in K$, $\gamma \neq 0$ に対して, $\gamma\mathfrak{a} = [\gamma\omega_1, \gamma\omega_2]$ となる.

[証明] $\gamma\mathfrak{a} = \gamma(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \mathbb{Z}\gamma\omega_1 + \mathbb{Z}\gamma\omega_2$. また, 任意の x, $y \in \mathbb{Z}$ に対して,

$$\begin{aligned} x\gamma\omega_1 + y\gamma\omega_2 = 0 &\Longrightarrow \gamma(x\omega_1 + y\omega_2) = 0 \\ &\Longrightarrow x\omega_1 + y\omega_2 = 0 \\ &\Longrightarrow x = y = 0. \end{aligned}$$

ゆえに, 補題 10.1 より, $\gamma\mathfrak{a} = [\gamma\omega_1, \gamma\omega_2]$. □

[定理 10.12] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアル, ω_1, ω_2 を $\mathfrak{a}$ の基底とする. また, p, q, r, $s \in \mathbb{Z}$ とし, $ps - qr = \pm 1$ を満たすとする. このとき,

$$\begin{aligned} \mu_1 &= p\omega_1 + q\omega_2, \\ \mu_2 &= r\omega_1 + s\omega_2 \end{aligned}$$

とおけば, μ_1, μ_2 もまた $\mathfrak{a}$ の基底である.

[証明] 定理 5.4 と同様にして証明できる. □

[定理 10.13] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアルとする. $\omega_1, \omega_2, \mu_1, \mu_2 \in K$, $p, q, r, s \in \mathbb{Z}$ とし,

$$\mu_1 = p\omega_1 + q\omega_2,$$
$$\mu_2 = r\omega_1 + s\omega_2$$

を満たすとする. このとき, $\mathfrak{a} = [\omega_1, \omega_2] = [\mu_1, \mu_2]$ ならば $ps - qr = \pm 1$ が成り立つ.

[証明] 定理 5.7 と同様にして証明できる. □

K を 2 次体, $\mathfrak{a} \neq (0)$ を K の分数イデアルとし, ω_1, ω_2 を $\mathfrak{a}$ の基底とするとき,

$$d(\mathfrak{a}) = d_K(\omega_1, \omega_2) = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1^\sigma & \omega_2^\sigma \end{vmatrix}^2$$

を $\mathfrak{a}$ の**判別式**という.

$\mathfrak{o}_K$ のイデアルとしての基底とはまさに K の整数底のことなので, $d(\mathfrak{o}_K)$ と K の判別式 d_K とは同一のものである.

[定理 10.14] $d(\mathfrak{a})$ の値は $\mathfrak{a}$ の基底の選び方によらない.

[証明] 定理 6.4 と同様にして証明できる. □

11 イデアルのノルム

[定理 11.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアルとする. このとき,

$$\mathfrak{a}^\sigma = \{\alpha^\sigma \mid \alpha \in \mathfrak{a}\}$$

もまた K の分数イデアルである. $\mathfrak{a}^\sigma$ を $\mathfrak{a}$ の**共役イデアル**という.

$\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルならば, $\mathfrak{a}^\sigma$ も $\mathfrak{o}_K$ のイデアルである.

[証明] $0 = 0^\sigma \in \mathfrak{a}^\sigma$ より, $\mathfrak{a}^\sigma$ は空集合でない.

$\alpha, \beta \in \mathfrak{a}$, $x \in \mathfrak{o}_K$ を任意にとる. $\alpha - \beta \in \mathfrak{a}$ より,

$$\alpha^\sigma - \beta^\sigma = (\alpha - \beta)^\sigma \in \mathfrak{a}^\sigma.$$

また, $x^\sigma \in \mathfrak{o}_K$ より $x^\sigma \alpha \in \mathfrak{a}$ だから,

$$x\alpha^\sigma = (x^\sigma \alpha) \in \mathfrak{a}^\sigma.$$

さらに, $\mathfrak{a}$ は分数イデアルだから, ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して, 任意の $\alpha \in \mathfrak{a}$ に対して $c\alpha \in \mathfrak{o}_K$ となる. よって, 任意の $\alpha \in \mathfrak{a}$ に対して,

$$c^\sigma \alpha^\sigma = (c\alpha)^\sigma \in \mathfrak{o}_K, \quad c^\sigma \in \mathfrak{o}_K.$$

ここで, c^σ は α に依存しない. ゆえに, $\mathfrak{a}^\sigma$ は K の分数イデアルである.

$\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルならば, $\mathfrak{a} \subseteq \mathfrak{o}_K$ より, 任意の $\alpha \in \mathfrak{a}$ に対して, $\alpha^\sigma \in \mathfrak{o}_K$ となる. したがって, $\mathfrak{a}^\sigma \subseteq \mathfrak{o}_K$. □

[定理 11.2] K を 2 次体とし, $\mathfrak{a}$, $\mathfrak{b}$ を K の分数イデアルとする.

(i) $(\mathfrak{a}+\mathfrak{b})^\sigma = \mathfrak{a}^\sigma + \mathfrak{b}^\sigma$.

(ii) $(\mathfrak{ab})^\sigma = \mathfrak{a}^\sigma \mathfrak{b}^\sigma$.

[証明] (i) 任意の $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$ に対して

$$(\alpha+\beta)^\sigma = \alpha^\sigma + \beta^\sigma$$

が成り立つことから明らか.

(ii) 任意の有限和 $\sum_i \alpha_i\beta_i$, $\alpha_i \in \mathfrak{a}$, $\beta_i \in \mathfrak{b}$ に対して

$$\left(\sum_i \alpha_i\beta_i\right)^\sigma = \sum_i \alpha_i^\sigma \beta_i^\sigma$$

が成り立つことから明らか. □

[定理 11.3] K を 2 次体とし, $\alpha_1, \alpha_2, \ldots, \alpha_s \in K$ とする. このとき,

$$(\alpha_1, \alpha_2, \ldots, \alpha_s)^\sigma = (\alpha_1^\sigma, \alpha_2^\sigma, \ldots, \alpha_s^\sigma)$$

が成り立つ.

[証明] 任意の $x_1, x_2, \ldots, x_s \in \mathfrak{o}_K$ に対して,

$$\left(\sum_{i=1}^s x_i\alpha_i\right)^\sigma = \sum_{i=1}^s x_i^\sigma \alpha_i^\sigma = \sum_{i=1}^s x_i\alpha_i^\sigma.$$

これより, 求める等式が成り立つことは明らかである. □

[定理 11.4] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を K の分数イデアル, $\mathfrak{a}^\sigma$ を $\mathfrak{a}$ の共役イデアルとする. このとき, ある $u \in \mathbb{Q}$, $u > 0$ がただ 1 つ存在して,

$$\mathfrak{a}\mathfrak{a}^\sigma = (u)$$

が成り立つ. $\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルならば, $u \in \mathbb{Z}$ である.

[証明] 定理 10.10 より, ある $v \in \mathbb{Z}$, $v > 0$ が存在して, $v\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルになる. α, β を $v\mathfrak{a}$ の基底とすれば,

$$v\mathfrak{a} = (\alpha,\, \beta), \quad \alpha,\, \beta \in \mathfrak{o}_K.$$

定理 11.3 より,

$$v\mathfrak{a}^\sigma = (v\mathfrak{a})^\sigma = (\alpha^\sigma,\, \beta^\sigma).$$

よって,

$$v^2\mathfrak{a}\mathfrak{a}^\sigma = (\alpha\alpha^\sigma,\, \alpha\beta^\sigma,\, \alpha^\sigma\beta,\, \beta\beta^\sigma).$$

$a = \alpha\alpha^\sigma$, $b = \alpha\beta^\sigma + \alpha^\sigma\beta$, $c = \beta\beta^\sigma$ とおくと, a, b, $c \in \mathbb{Z}$ である. $g = \gcd(a,\, b,\, c)$ とおくと, $g > 0$ であり,

$$g = ax + by + cz, \quad x,\, y,\, z \in \mathbb{Z}$$

と表せる. よって, $g \in v^2\mathfrak{a}\mathfrak{a}^\sigma$ となり, $(g) \subseteq v^2\mathfrak{a}\mathfrak{a}^\sigma$ がいえる. 逆に,

$$\alpha\alpha^\sigma = a = g \cdot \frac{a}{g} \in (g),$$
$$\beta\beta^\sigma = a = g \cdot \frac{b}{g} \in (g).$$

さらに,

$$\mathrm{Tr}_K \frac{\alpha\beta^\sigma}{g} = \frac{\alpha\beta^\sigma}{g} + \frac{\alpha^\sigma\beta}{g} = \frac{b}{g} \in \mathbb{Z},$$
$$N_K \frac{\alpha\beta^\sigma}{g} = \frac{\alpha\beta^\sigma}{g} \cdot \frac{\alpha^\sigma\beta}{g} = \frac{ac}{g^2} \in \mathbb{Z}.$$

よって, $\alpha\beta^\sigma/g$, $\alpha^\sigma\beta/g \in \mathfrak{o}_K$. ゆえに,

$$\alpha\beta^\sigma = g \cdot \frac{\alpha\beta^\sigma}{g} \in (g),$$
$$\alpha^\sigma\beta = g \cdot \frac{\alpha^\sigma\beta}{g} \in (g).$$

したがって, $v^2\mathfrak{a}\mathfrak{a}^\sigma \subseteq (g)$ もいえる.

以上より, $v^2\mathfrak{a}\mathfrak{a}^\sigma = (g)$ が成り立つ. $u = g/v^2$ とおくと, $u \in \mathbb{Q}$, $u > 0$, $\mathfrak{a}\mathfrak{a}^\sigma = (u)$ となる.

$\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルであるときは, 上の議論を $v = 1$ の場合に行えばよいから, $u = g \in \mathbb{Z}$ となる.

u, $u' \in \mathbb{Q}$, $u > 0$, $u' > 0$ とし,

$$\mathfrak{a}\mathfrak{a}^\sigma = (u) = (u')$$

であるとすると, ある $\varepsilon \in \mathfrak{o}_K$ が存在して, $u = u'\varepsilon$ となる. ところが, $\varepsilon \in \mathbb{Q} \cap \mathfrak{o}_K^\times = \{\pm 1\}$ であるから $\varepsilon = \pm 1$ であり, $u > 0$, $u' > 0$ より $\varepsilon = 1$. したがって, $u = u'$. □

2 次体 K の分数イデアル $\mathfrak{a} \neq (0)$ に対して, 定理 11.4 における u を $\mathfrak{a}$ の**ノルム**といい, $N\mathfrak{a}$ で表す. $N\mathfrak{a}$ は常に正の有理数である. $\mathfrak{a}$ が整数環 $\mathfrak{o}_K$ のイデアルならば, $N\mathfrak{a}$ は有理整数である.

[定理 11.5] K を 2 次体, $\alpha \in K$, $\alpha \neq 0$ とする. このとき, 単項分数イデアル $(\alpha) = \alpha\mathfrak{o}_K$ について,

$$N(\alpha) = |N_K\alpha|$$

が成り立つ.

[証明] イデアルのノルムの定義と定理 11.3 より,

$$(N(\alpha)) = (\alpha)(\alpha)^\sigma = (\alpha)(\alpha^\sigma) = (\alpha\alpha^\sigma) = (N_K\alpha).$$

ゆえに, ある $\varepsilon \in \mathfrak{o}_K^\times$ が存在して,

$$N(\alpha) = N_K\alpha \cdot \varepsilon.$$

$N(\alpha)$, $N_K\alpha \in \mathbb{Q}$ より, $\varepsilon \in \mathbb{Q} \cap \mathfrak{o}_K^\times = \{\pm 1\}$. イデアルのノルムは常に正だから,

$$N(\alpha) = |N(\alpha)| = |N_K\alpha||\varepsilon| = |N_K\alpha|.$$

□

[例 11.1] K を 2 次体, $a \in \mathbb{Q}$ とするとき, $N_K a = a^2$ より, $N(a) = |N_K a| = a^2$.

[定理 11.6] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を K の (0) でない分数イデアルとする. このとき,

$$N(\mathfrak{ab}) = N\mathfrak{a}N\mathfrak{b}$$

が成り立つ.

[証明] イデアルのノルムの定義と定理 11.2 より,

$$\begin{aligned}(N(\mathfrak{ab})) &= (\mathfrak{ab})(\mathfrak{ab})^\sigma = \mathfrak{ab}\mathfrak{a}^\sigma\mathfrak{b}^\sigma \\ &= \mathfrak{a}\mathfrak{a}^\sigma\mathfrak{b}\mathfrak{b}^\sigma = (N\mathfrak{a})(N\mathfrak{b}) \\ &= (N\mathfrak{a}N\mathfrak{b}).\end{aligned}$$

よって, ある $\varepsilon \in \mathfrak{o}_K^\times$ が存在して,

$$N(\mathfrak{ab}) = N\mathfrak{a}N\mathfrak{b} \cdot \varepsilon.$$

$N(\mathfrak{ab})$, $N\mathfrak{a}$, $N\mathfrak{b} \in \mathbb{Z}$ であるから, $\varepsilon \in \mathbb{Q} \cap \mathfrak{o}_K^\times = \{\pm 1\}$. また, $N(\mathfrak{ab})$, $N\mathfrak{a}$, $N\mathfrak{b}$ はすべて正であるから, $\varepsilon = 1$. したがって, 求める等式が得られる. □

[定理 11.7] K を 2 次体, $\mathfrak{a} \neq (0)$ を K の分数イデアル, $\gamma \neq 0$ を K の元とする. このとき,

$$N(\gamma\mathfrak{a}) = N_K\gamma \cdot N\mathfrak{a}$$

が成り立つ.

[証明] 定理 11.2, 定理 11.3 を用いて計算すると,

$$\begin{aligned} N(\gamma\mathfrak{a}) &= (\gamma\mathfrak{a})(\gamma\mathfrak{a})^\sigma = (\gamma)\mathfrak{a}((\gamma)\mathfrak{a})^\sigma = (\gamma)\mathfrak{a}(\gamma)^\sigma\mathfrak{a}^\sigma \\ &= (\gamma)\mathfrak{a}(\gamma^\sigma)\mathfrak{a}^\sigma = (\gamma)(\gamma^\sigma)\mathfrak{a}\mathfrak{a}^\sigma = (\gamma\gamma^\sigma)\mathfrak{a}\mathfrak{a}^\sigma = \gamma\gamma^\sigma\mathfrak{a}\mathfrak{a}^\sigma \\ &= N_K\gamma \cdot N\mathfrak{a}. \end{aligned}$$

□

[定理 11.8] K を 2 次体, $\mathfrak{a} \neq (0)$ を K の分数イデアル, $\mathfrak{a}^\sigma$ を $\mathfrak{a}$ の共役イデアル, $\mathfrak{a}^{-1}$ を $\mathfrak{a}$ の逆イデアル, $N\mathfrak{a}$ を $\mathfrak{a}$ のノルムとする. このとき,

$$\mathfrak{b} = \frac{1}{N\mathfrak{a}}\mathfrak{a}^\sigma$$

とおくと, $\mathfrak{a}\mathfrak{b} = \mathfrak{o}_K$, $\mathfrak{a}^{-1} = \mathfrak{b}$ が成り立つ.

[証明] イデアルのノルムの定義より,

$$\mathfrak{a}\mathfrak{a}^\sigma = (N\mathfrak{a}).$$

両辺に $1/N\mathfrak{a}$ を掛けることにより, $\mathfrak{a}\mathfrak{b} = \mathfrak{o}_K$ が得られる. さらに, 定理 9.7 より, $\mathfrak{a}^{-1} = \mathfrak{b}$. □

[定理 11.9] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を K の分数イデアル, $\mathfrak{a}^{-1}$ を $\mathfrak{a}$ の逆イデアルとする. このとき,

$$N\mathfrak{a}^{-1} = (N\mathfrak{a})^{-1}$$

が成り立つ.

[証明] 定理 11.8 より $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}_K$ であるから,

$$N\mathfrak{a}N\mathfrak{a}^{-1} = N(\mathfrak{a}\mathfrak{a}^{-1}) = N\mathfrak{o}_K = 1.$$

これより, 求める等式が得られる. □

［定理 11.10］ K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を $\mathfrak{o}_K$ のイデアル, a_0, $b + c_0\omega$ を $\mathfrak{a}$ の標準的基底とする. このとき, 加法群として

$$\mathfrak{o}_K/\mathfrak{a} \cong \mathbb{Z}/a_0\mathbb{Z} \oplus \mathbb{Z}/c_0\mathbb{Z}.$$

したがって,

$$[\mathfrak{o}_K : \mathfrak{a}] = a_0c_0$$

が成り立つ. 特に, 剰余環 $\mathfrak{o}_K/\mathfrak{a}$ の元の個数は有限である.

［証明］ 定理 15.5 より $b \in c_0\mathbb{Z}$ なので, $b = c_0b'$, $\omega' = b' + \omega$ とおくと,

$$\mathfrak{a} = \mathbb{Z}a_0 + \mathbb{Z}c_0\omega'$$

となる. 一方, $\mathfrak{o}_K = [1, \omega']$ なので, 写像

$$f : \mathfrak{o}_K \longrightarrow \mathbb{Z}/a_0\mathbb{Z} \oplus \mathbb{Z}/c_0\mathbb{Z}, \quad u + v\omega' \longmapsto (u + a_0\mathbb{Z},\, v + c_0\mathbb{Z})$$

が定まる. ただし, u, $v \in \mathbb{Z}$ とする.

任意の u_1, u_2, v_1, $v_2 \in \mathbb{Z}$ に対して,

$$\begin{aligned}
&f\big((u_1 + v_1\omega') + (u_2 + v_2\omega')\big) \\
&\quad = f\big((u_1 + u_2) + (v_1 + v_2)\omega'\big) \\
&\quad = \big((u_1 + u_2) + a_0\mathbb{Z},\, (v_1 + v_2) + c_0\mathbb{Z}\big) \\
&\quad = \big((u_1 + a_0\mathbb{Z}) + (u_2 + a_0\mathbb{Z}),\, (v_1 + c_0\mathbb{Z}) + (v_2 + c_0\mathbb{Z})\big) \\
&\quad = (u_1 + a_0\mathbb{Z},\, v_1 + c_0\mathbb{Z}) + (u_2 + a_0\mathbb{Z},\, v_2 + c_0\mathbb{Z}) \\
&\quad = f(u_1 + v_1\omega') + f(u_2 + v_2\omega').
\end{aligned}$$

よって, f は加法群の準同型写像である.

任意の $\boldsymbol{x} \in \mathbb{Z}/a_0\mathbb{Z} \oplus \mathbb{Z}/c_0\mathbb{Z}$ に対して, ある u, $v \in \mathbb{Z}$ が存在して, $\boldsymbol{x} = (u + a_0\mathbb{Z},\, v + a_0\mathbb{Z})$. このとき, $u + v\omega' \in \mathfrak{o}_K$ かつ $f(u + v\omega') = \boldsymbol{x}$. よって, f は全射である.

u, $v \in \mathbb{Z}$ とすると,

$$\begin{aligned}
u + v\omega' \in \operatorname{Ker} f &\Longleftrightarrow (u + a_0\mathbb{Z},\, v + c_0\mathbb{Z}) = \mathbf{0} \\
&\Longleftrightarrow u \in a_0\mathbb{Z},\, v \in c_0\mathbb{Z}.
\end{aligned}$$

$u = a_0u'$, $v = c_0v'$, u', $v' \in \mathbb{Z}$ であるとすると,

$$u + v\omega' = u'a_0 + v'(b + c_0\omega) \in \mathbb{Z}a_0 + \mathbb{Z}(b + c_0\omega) = \mathfrak{a}.$$

逆に,

$$u + v\omega' \in \mathfrak{a} = \mathbb{Z}a_0 + \mathbb{Z}c_0\omega'$$

であるとすると, $\mathfrak{o}_K$ の元を基底 1, ω' の $\mathbb{Z}$ 係数の 1 次結合で表す仕方は一意的だから, $u \in a_0\mathbb{Z}$, $v \in c_0\mathbb{Z}$ が得られる. したがって, $\mathrm{Ker}\, f = \mathfrak{a}$.

準同型定理により, 同型

$$\mathfrak{o}_K/\mathfrak{a} \cong \mathbb{Z}/a_0\mathbb{Z} \times \mathbb{Z}/c_0\mathbb{Z}, \quad (u + v\omega') + \mathfrak{a} \longmapsto (u + a_0\mathbb{Z},\, v + c_0\mathbb{Z})$$

が得られる. ゆえに, $[\mathfrak{o}_K : \mathfrak{a}] = a_0c_0$. □

[定理 11.11] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を $\mathfrak{o}_K$ のイデアル, $\mathfrak{a}^\sigma$ を $\mathfrak{a}$ の共役イデアルとする. このとき,

$$N\mathfrak{a} = [\mathfrak{o}_K : \mathfrak{a}]$$

が成り立つ.

[証明] a_0, $b + c_0\omega$ を $\mathfrak{a}$ の標準的基底とする. 定理 15.5 より, a_0, $b \in c_0\mathbb{Z}$ であり,

$$a_0 = c_0a_0', \quad b = c_0b', \quad \omega' = b' + \omega$$

とおくと,

$$\mathfrak{a} = c_0\mathfrak{a}_\circ, \quad \mathfrak{a}_0 = [a_0', \omega']$$

となる. a_0', ω' は $\mathfrak{a}_0$ の標準的基底であるから, $\mathbb{Z} \cap \mathfrak{a}_0 = a_0'\mathbb{Z}$ が成り立つ.

$$N_K\omega' = \omega'\omega'^\sigma \in \mathbb{Z} \cap \mathfrak{a}_0 = a_0'\mathbb{Z}$$

より, ある $q \in \mathbb{Z}$ が存在して, $N_K\omega' = \omega'\omega'^\sigma = a_0'q$ となる.

さて, イデアルの基底は生成元なので,

$$\mathfrak{a} = (a_0,\, b + c_0\omega).$$

定理 11.3 より,

$$\mathfrak{a}^\sigma = (a_0,\, b + c_0\omega^\sigma).$$

これらの積を計算すると,

$$\begin{aligned}
\mathfrak{a}\mathfrak{a}^\sigma &= (a_0,\, b + c_0\omega)(a_0,\, b + c_0\omega^\sigma) \\
&= c_0^2(a_0',\, \omega')(a_0',\, \omega'^\sigma) \\
&= c_0^2(a_0'^2,\, a_0'\omega',\, a_0'\omega'^\sigma,\, \omega'\omega'^\sigma) \\
&= a_0'c_0^2(a_0',\, \omega',\, \omega'^\sigma,\, q).
\end{aligned}$$

定理 11.10 より $a_0'c_0^2 = a_0c_0 = [\mathfrak{o}_K : \mathfrak{a}]$ であるから,

$$\begin{aligned}
\mathfrak{a}\mathfrak{a}^\sigma &= a_0c_0(a_0',\, \omega',\, \omega'^\sigma,\, q) \\
&= [\mathfrak{o}_K : \mathfrak{a}] \cdot (a_0',\, \omega',\, \omega'^\sigma,\, q).
\end{aligned}$$

定理 11.4 より, ある $u \in \mathbb{Z}$, $u > 0$ が存在して,

$$(u) = [\mathfrak{o}_K : \mathfrak{a}] \cdot (a'_0,\, \omega',\, \omega'^{\sigma},\, q).$$

u は, 右辺の元になるので, $[\mathfrak{o}_K : \mathfrak{a}]$ の倍数である. ここで, u, $[\mathfrak{o}_K : \mathfrak{a}]$ はともに有理整数なので, u が $\mathfrak{o}_K$ における $[\mathfrak{o}_K : \mathfrak{a}]$ の倍数であれば, $\mathbb{Z}$ においても倍数であることに注意せよ. $u = [\mathfrak{o}_K : \mathfrak{a}] \cdot u'$, $u' \in \mathbb{Z}$ とおくと, $u' > 0$ であり,

$$(u') = (a'_0,\, \omega',\, \omega'^{\sigma},\, q).$$

$\omega' \in (u')$ であり, $\mathfrak{o}_K = [1, \omega]$ だから, ある x, $y \in \mathbb{Z}$ が存在して,

$$b' + \omega = \omega' = u'(x + y\omega) = (b' + u'x) + u'y\omega.$$

よって, $u'y = 1$ となり, $u' = \pm 1$ が得られる. $u' > 0$ だったから, $u' = 1$. ゆえに, $u = [\mathfrak{o}_K : \mathfrak{a}]$ となる. □

[例 11.2] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を $\mathfrak{o}_K$ のイデアルとする. このとき, 定理 11.11 より,

$$N\mathfrak{a} = 1 \Longleftrightarrow [\mathfrak{o}_K : \mathfrak{a}] = 1 \Longleftrightarrow \mathfrak{a} = \mathfrak{o}_K$$

が成り立つ.

一般の分数イデアルの場合には, イデアルのノルムの値が 1 であっても $\mathfrak{o}_K$ に一致するとは限らない. 例えば, $K = \mathbb{Q}(\sqrt{-15})$, $\alpha = (1 + \sqrt{-15})/4$ とおくと, 定理 11.5 より,

$$N(\alpha) = |N_K \alpha| = 1.$$

しかし, $\alpha \notin \mathfrak{o}_K$ なので, $(\alpha) \neq \mathfrak{o}_K$.

[定理 11.12] K を代数体, 1, ω を K の標準的整数底, $\mathfrak{a} \neq (0)$ を K の分数イデアルとする. このとき, 任意の u_1, u_2, v_1, $v_2 \in \mathbb{Q}$ に対して,

$$\mathfrak{a} = [u_1 + v_1\omega,\, u_2 + v_2\omega] \Longrightarrow N\mathfrak{a} = |u_1v_2 - v_1u_2|$$

が成り立つ.

[証明] cu_1, cu_2, cv_1, $cv_2 \in \mathbb{Z}$ となる $c \in \mathbb{Z}$, $c > 0$ をとると,

$$c\mathfrak{a} = [cu_1 + cv_1\omega,\, cu_2 + cv_2\omega], \quad cu_1 + cv_1\omega,\, cu_2 + cv_2\omega \in \mathfrak{o}_K$$

となるから, $c\mathfrak{a}$ は K の整数環 $\mathfrak{o}_K$ のイデアルである. a_0, $b + c_0\omega$ を $c\mathfrak{a}$ の標準的基底とすると,

$$cu_1 + cv_1\omega = pa_0 + q(b + c_0\omega), \quad p,\, q \in \mathbb{Z},$$
$$cu_2 + cv_2\omega = ra_0 + s(b + c_0\omega), \quad r,\, s \in \mathbb{Z}$$

と表せるから,

$$\begin{bmatrix} cu_1 & cv_1 \\ cu_2 & cv_2 \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix} = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a_0 & 0 \\ b & c_0 \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix}.$$

補題 5.5 より,

$$\begin{bmatrix} cu_1 & cv_1 \\ cu_2 & cv_2 \end{bmatrix} = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a_0 & 0 \\ b & c_0 \end{bmatrix}.$$

一方, 定理 10.13 より,

$$\begin{vmatrix} p & q \\ r & s \end{vmatrix} = ps - qr = \pm 1.$$

ゆえに, 定理 11.10 より,

$$\begin{aligned} c^2(u_1v_2 - v_1u_2) = \begin{vmatrix} cu_1 & cv_1 \\ cu_2 & cv_2 \end{vmatrix} &= \begin{vmatrix} p & q \\ r & s \end{vmatrix} \begin{vmatrix} a_0 & 0 \\ b & c_0 \end{vmatrix} \\ &= \pm a_0c_0 = \pm N(c\mathfrak{a}). \end{aligned}$$

一方, 定理 11.7 より,

$$N(c\mathfrak{a}) = N_K c \cdot N\mathfrak{a} = c^2 N\mathfrak{a}.$$

ゆえに, $N\mathfrak{a} = |u_1v_2 - v_1u_2|$ が得られる. □

[定理 11.13] K を 2 次体, $\mathfrak{a} \neq (0)$ を K の分数イデアルとする. このとき,

$$d(\mathfrak{a}) = d_K \cdot (N\mathfrak{a})^2$$

が成り立つ.

[証明] まず, $\mathfrak{a}$ が K の整数環 $\mathfrak{o}_K$ のイデアルである場合を証明する.

1, ω を K の標準的整数底, α, β を $\mathfrak{a}$ の基底とするとき,

$$\alpha = u_1 + v_1\omega, \quad u_1, v_1 \in \mathbb{Z},$$
$$\beta = u_2 + v_2\omega, \quad u_2, v_2 \in \mathbb{Z}$$

と表せる. 定理 11.12 より, $N\mathfrak{a} = |u_1v_2 - v_1u_2|$. また,

$$\alpha^\sigma = u_1 + v_1\omega^\sigma, \quad \beta^\sigma = u_2 + v_2\omega^\sigma$$

であるから,

$$\begin{vmatrix} \alpha & \beta \\ \alpha^\sigma & \beta^\sigma \end{vmatrix} = \begin{vmatrix} 1 & \omega \\ 1 & \omega^\sigma \end{vmatrix} \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}.$$

したがって,

$$\begin{aligned} d(\mathfrak{a}) &= d_K(\alpha,\, \beta) = d_K(1,\, \omega) \cdot (u_1 v_2 - v_1 u_2)^2 \\ &= d_K \cdot (N\mathfrak{a})^2 \end{aligned}$$

となる.

次に, $\mathfrak{a}$ が K の分数イデアルであるとき, ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して, $c\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルになる. よって,

$$d(c\mathfrak{a}) = d_K \cdot (N(c\mathfrak{a}))^2.$$

α, β を $\mathfrak{a}$ の基底とすると, $c\alpha$, $c\beta$ は $c\mathfrak{a}$ の基底である. よって,

$$\begin{aligned} d(c\mathfrak{a}) &= \begin{vmatrix} c\alpha & c\beta \\ c^\sigma \alpha^\sigma & c^\sigma \beta^\sigma \end{vmatrix}^2 = (cc^\sigma)^2 \begin{vmatrix} \alpha & \beta \\ \alpha^\sigma & \beta^\sigma \end{vmatrix}^2 \\ &= (N_K c)^2 d(\mathfrak{a}). \end{aligned}$$

また, 定理 11.7 より, $N(c\mathfrak{a}) = N_K c \cdot N\mathfrak{a}$. ゆえに,

$$\begin{aligned} (N_K c)^2 d(\mathfrak{a}) &= d_K \cdot (N_K c \cdot N\mathfrak{a})^2 \\ &= (N_K c)^2 \cdot d_K \cdot (N\mathfrak{a})^2. \end{aligned}$$

$c \neq 0$ より $N_K c \neq 0$ であるから, 分数イデアルの場合にも求める等式が得られる. □

12 イデアルの整除

K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする.

$\mathfrak{o}_K$ のイデアル $\mathfrak{a}$, $\mathfrak{b}$ に対して, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{t}$ が存在して $\mathfrak{b} = \mathfrak{a}\mathfrak{t}$ が成り立つとき, $\mathfrak{a}$ は $\mathfrak{b}$ を**割る**といい, $\mathfrak{b}$ は $\mathfrak{a}$ で**割り切れる**という. このことを記号で $\mathfrak{a} \mid \mathfrak{b}$ と書く. またこのとき, $\mathfrak{a}$ を $\mathfrak{b}$ の**約イデアル**, $\mathfrak{b}$ を $\mathfrak{a}$ の**倍イデアル**という.

$\mathfrak{o}_K$ のイデアル $\mathfrak{a}$ がいくつかの $\mathfrak{o}_K$ のイデアル $\mathfrak{b}_1$, $\mathfrak{b}_2$, …, $\mathfrak{b}_s$ の約イデアルであるとき, $\mathfrak{a}$ をそれらの**公約イデアル**という. また, $\mathfrak{a}$ がそれらの**最大公約イデアル**であるとは, 2 つの条件

(i) $\mathfrak{a}$ は $\mathfrak{b}_1$, $\mathfrak{b}_2$, …, $\mathfrak{b}_s$ の公約イデアルである.

(ii) $\mathfrak{b}_1$, $\mathfrak{b}_2$, …, $\mathfrak{b}_s$ の任意の公約イデアルは $\mathfrak{a}$ の約イデアルである.

を満たすときにいう. 「約イデアル」を「倍イデアル」に書き換えれば, **公倍イデアル**, **最小公倍イデアル**も同様に定義できる.

[定理 12.1] K を 2 次体, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ を K の分数イデアルとし, $\mathfrak{a} \neq (0)$ とする. このとき,

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} \Longrightarrow \mathfrak{b} = \mathfrak{c}$$

が成り立つ.

[証明] $\mathfrak{a} \neq (0)$ を K の分数イデアルとする. 定理 11.4 より, ある $u \in \mathbb{Q}$ が存在して,

$$\mathfrak{a}\mathfrak{a}^{\sigma} = (u), \quad u > 0.$$

これと $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ より,

$$u\mathfrak{b} = (u)\mathfrak{b} = \mathfrak{a}^{\sigma}\mathfrak{a}\mathfrak{b} = \mathfrak{a}^{\sigma}\mathfrak{a}\mathfrak{c} = (u)\mathfrak{c} = u\mathfrak{c}.$$

$u \neq 0$ より, $\mathfrak{b} = \mathfrak{c}$ となる. 実際,

$$\begin{aligned} \beta \in \mathfrak{b} &\Longrightarrow u\beta \in u\mathfrak{b} = u\mathfrak{c} \\ &\Longrightarrow u\beta = u\gamma \ (\exists \gamma \in \mathfrak{c}) \\ &\Longrightarrow \beta = \gamma \in \mathfrak{c} \end{aligned}$$

より, $\mathfrak{b} \subseteq \mathfrak{c}$. 逆の包含関係も同様にして示せる. □

[定理 12.2] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を K の分数イデアルとする. このとき, 次の 2 つの条件は同値である.

(i) ある $\mathfrak{o}_K$ のイデアル $\mathfrak{t}$ が存在して, $\mathfrak{b} = \mathfrak{a}\mathfrak{t}$.
(ii) $\mathfrak{b} \subseteq \mathfrak{a}$.

[証明] (i)⇒(ii)　$\mathfrak{t}$ を $\mathfrak{o}_K$ のイデアルで $\mathfrak{b} = \mathfrak{a}\mathfrak{t}$ を満たすものとすると,

$$\mathfrak{b} = \mathfrak{a}\mathfrak{t} \subseteq \mathfrak{a}\mathfrak{o}_K = \mathfrak{a}.$$

(ii)⇒(i)　$\mathfrak{b} \subseteq \mathfrak{a}$ とする. $\mathfrak{a} = (0)$ のとき, $\mathfrak{b} = (0)$ だから, $\mathfrak{t} = (0)$ とすれば $\mathfrak{b} = \mathfrak{a}\mathfrak{t}$ となる.
$\mathfrak{a} \neq (0)$ のとき, 定理 11.4 より, ある $a \in \mathbb{Q}$, $a > 0$ が存在して,

$$\mathfrak{b}\mathfrak{a}^{\sigma} \subseteq \mathfrak{a}\mathfrak{a}^{\sigma} = (a).$$

ところで, 定理 10.9 より, $\mathfrak{b}\mathfrak{a}^{\sigma}$ は基底 ω_1, ω_2 をもつ. 基底は生成元になる. すなわち, $\mathfrak{b}\mathfrak{a}^{\sigma} = (\omega_1, \omega_2)$ が成り立つ. $\omega_1, \omega_2 \in (a) = a\mathfrak{o}_K$ なので, ある $\omega_1', \omega_2' \in \mathfrak{o}_K$ が存在して, $\omega_1 = a\omega_1'$, $\omega_2 = a\omega_2'$. よって, $\mathfrak{t} = (\omega_1', \omega_2')$ とおくと, $\mathfrak{t}$ は $\mathfrak{o}_K$ のイデアルである. さらに,

$$\mathfrak{b}\mathfrak{a}^{\sigma} = (a)\mathfrak{t} = \mathfrak{a}\mathfrak{a}^{\sigma}\mathfrak{t} = \mathfrak{a}\mathfrak{t}\mathfrak{a}^{\sigma}.$$

ゆえに, 定理 12.1 より, $\mathfrak{b} = \mathfrak{a}\mathfrak{t}$. □

[定理 12.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を K の分数イデアルとする.

(i) $\mathfrak{a} + \mathfrak{b}$ は $\mathfrak{a}$, $\mathfrak{b}$ を両方含む分数イデアルのうちで最小のものである.
(ii) $\mathfrak{a} \cap \mathfrak{b}$ は $\mathfrak{a}$, $\mathfrak{b}$ の両方に含まれる分数イデアルのうちで最大のものである.

また, $\mathfrak{a}$, $\mathfrak{b}$ が $\mathfrak{o}_K$ のイデアルであるとき, $\mathfrak{a}$, $\mathfrak{b}$ の最大公約イデアル, 最小公倍イデアルは, それぞれ $\mathfrak{a}$, $\mathfrak{b}$ に対してただ 1 つである. 一方,

(i) $\mathfrak{a}+\mathfrak{b}$ は $\mathfrak{a}$, $\mathfrak{b}$ の最大公約イデアルである.

(ii) $\mathfrak{a}\cap\mathfrak{b}$ は $\mathfrak{a}$, $\mathfrak{b}$ の最小公倍イデアルである.

イデアルが 3 つ以上の場合にも同様のことが成り立つ.

[証明] 2 つのイデアルの場合についてのみ証明する. 3 つ以上の場合についても同様である.

(前半の (i)) 任意の $\alpha\in\mathfrak{a}$ に対して, $\alpha+0\in\mathfrak{a}+\mathfrak{b}$. ゆえに, $\mathfrak{a}\subseteq\mathfrak{a}+\mathfrak{b}$. 同様に, $\mathfrak{b}\subseteq\mathfrak{a}+\mathfrak{b}$.

K の分数イデアルで $\mathfrak{a}$, $\mathfrak{b}$ の両方を含むものを任意にとると, 任意の $\alpha\in\mathfrak{a}$, $\beta\in\mathfrak{b}$ に対して, $\alpha+\beta\in\mathfrak{c}$. よって, $\mathfrak{a}+\mathfrak{b}\subseteq\mathfrak{c}$.

(前半の (ii)) $\mathfrak{a}\cap\mathfrak{b}$ は集合として $\mathfrak{a}$, $\mathfrak{b}$ の両方に含まれる最大のものである. そして, $\mathfrak{a}\cap\mathfrak{b}$ 自身が K の分数イデアルである.

定理 12.2 より, 最大公約イデアルが 2 つあれば, 互いにもう一方を含むので, 両者は一致する. 最小公倍イデアルについても同様である.

(後半の (i)) $\mathfrak{a}$, $\mathfrak{b}$ が $\mathfrak{o}_K$ のイデアルならば, $\mathfrak{a}+\mathfrak{b}$ も $\mathfrak{o}_K$ のイデアルである. よって, 前半の (i) と定理 12.2 より, $\mathfrak{a}+\mathfrak{b}$ は $\mathfrak{a}$, $\mathfrak{b}$ の最大公約イデアルである.

(後半の (ii)) $\mathfrak{a}$, $\mathfrak{b}$ が $\mathfrak{o}_K$ のイデアルならば, $\mathfrak{a}\cap\mathfrak{b}$ も $\mathfrak{o}_K$ のイデアルである. よって, 前半の (ii) と定理 12.2 より, $\mathfrak{a}\cap\mathfrak{b}$ は $\mathfrak{a}$, $\mathfrak{b}$ の最小公倍イデアルである. □

[定理 12.4] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を $\mathfrak{o}_K$ の (0) でないイデアルとする. このとき,

$$\mathfrak{a}\subseteq\mathfrak{b},\ N\mathfrak{a}=N\mathfrak{b}\Longrightarrow\mathfrak{a}=\mathfrak{b}$$

が成り立つ.

[証明] $\mathfrak{a}\subseteq\mathfrak{b}$ だから, 定理 12.2 より, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{c}$ が存在して,

$$\mathfrak{a}=\mathfrak{b}\mathfrak{c}.$$

両辺のノルムをとると,

$$N\mathfrak{a}=N\mathfrak{b}N\mathfrak{c}.$$

$N\mathfrak{a}=N\mathfrak{b}$ より, $N\mathfrak{c}=1$ が得られる. $\mathfrak{c}$ は $\mathfrak{o}_K$ のイデアルだから, $\mathfrak{c}=\mathfrak{o}_K$. したがって, $\mathfrak{a}=\mathfrak{b}$. □

[定理 12.5] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ を $\mathfrak{o}_K$ のイデアルとする. このとき, 次の 2 つの条件は同値である.

(i) $(\mathfrak{a},\mathfrak{c})=1$ かつ $(\mathfrak{b},\mathfrak{c})=1$.

(ii) $(\mathfrak{ab},\, \mathfrak{c}) = 1$.

[証明] (i)⇒(ii)　$(\mathfrak{a},\, \mathfrak{c}) = 1$, すなわち $\mathfrak{a} + \mathfrak{c} = \mathfrak{o}_K$ より,

$$1 = \alpha + \gamma, \quad \alpha \in \mathfrak{a}, \quad \gamma \in \mathfrak{c}$$

と表せる. 同様に, $(\mathfrak{b},\, \mathfrak{c}) = 1$ より,

$$1 = \beta + \gamma', \quad \beta \in \mathfrak{b}, \quad \gamma' \in \mathfrak{c}$$

と表せる. ゆえに,

$$\begin{aligned} 1 = 1 \cdot 1 &= (\alpha + \gamma)(\beta + \gamma') \\ &= \alpha\beta + (\alpha\gamma' + \beta\gamma + \gamma\gamma') \\ &\in \mathfrak{ab} + \mathfrak{c}. \end{aligned}$$

したがって, $(\mathfrak{ab},\, \mathfrak{c}) = 1$.

(ii)⇒(i)　$\mathfrak{ab} \subseteq \mathfrak{a}$ なので,

$$\mathfrak{o}_K = \mathfrak{ab} + \mathfrak{c} \subseteq \mathfrak{a} + \mathfrak{c}.$$

逆の包含関係は明らかだから, $\mathfrak{a} + \mathfrak{c} = \mathfrak{o}_K$. したがって, $(\mathfrak{a},\, \mathfrak{c}) = 1$ となる. $(\mathfrak{b},\, \mathfrak{c}) = 1$ も同様にして示せる. □

[定理 12.6] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ を $\mathfrak{o}_K$ のイデアルとする. このとき,

$$\mathfrak{a} \mid \mathfrak{bc},\, (\mathfrak{a},\, \mathfrak{b}) = 1 \Longrightarrow \mathfrak{a} \mid \mathfrak{c}$$

が成り立つ.

[証明] $\mathfrak{a} \mid \mathfrak{bc}$, $(\mathfrak{a},\, \mathfrak{b}) = 1$ であるとする. 前者の条件と定理 12.2 より, $\mathfrak{bc} \subseteq \mathfrak{a}$. また, 後者の条件, すなわち $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}_K$ より,

$$1 = \alpha + \beta, \quad \alpha \in \mathfrak{a}, \quad \beta \in \mathfrak{b}$$

と表せる. ゆえに, 任意の $\gamma \in \mathfrak{c}$ に対して,

$$\gamma = \gamma(\alpha + \beta) = \gamma\alpha + \beta\gamma \in \mathfrak{a} + \mathfrak{bc} \subseteq \mathfrak{a}.$$

したがって, $\mathfrak{c} \subseteq \mathfrak{a}$. 定理 12.2 より, $\mathfrak{a} \mid \mathfrak{c}$. □

[定理 12.7] K を 2 次体, $\mathfrak{o}_K$ を K の整数環とし,

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

を $\mathfrak{o}_K$ のイデアルの無限列とする. このとき, ある番号 i_0 が存在して,

$$\mathfrak{a}_{i_0} = \mathfrak{a}_{i_0+1} = \cdots$$

となる.

[証明] $\mathfrak{a} = \bigcup_{j=1}^{\infty} \mathfrak{a}_j$ とおくと, $\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルになる. 実際, $\alpha, \beta \in \mathfrak{a}$, $x \in \mathfrak{o}_K$ を任意にとると, ある番号 j_1, j_2 が存在して, $\alpha \in \mathfrak{a}_{j_1}$, $\beta \in \mathfrak{a}_{j_2}$ である. このとき, $\alpha \in \mathfrak{a}_{j_1} \subseteq \mathfrak{o}_K$. また, $x\alpha \in \mathfrak{a}_{j_1} \subseteq \mathfrak{a}$. さらに, $j_0 = \max\{j_1, j_2\}$ とすると, $\alpha \subseteq \mathfrak{a}_{j_1} \subseteq \mathfrak{a}_{j_0}$, $\beta \in \mathfrak{a}_{j_2} \subseteq \mathfrak{a}_{j_0}$ だから, $\alpha - \beta \in \mathfrak{a}_{j_0} \subseteq \mathfrak{a}$. ゆえに, $\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルである.

ω_1, ω_2 を $\mathfrak{a}$ の基底とする. ある番号 i_1, i_2 が存在して, $\omega_1 \in \mathfrak{a}_{i_1}$, $\omega_2 \in \mathfrak{a}_{i_2}$ となる. $i_0 = \max\{i_1, i_2\}$ とすると, $\omega_1, \omega_2 \in \mathfrak{a}_{i_0}$. ゆえに, $\mathfrak{a} = (\omega_1, \omega_2) \subseteq \mathfrak{a}_{i_0}$. 逆の包含関係は明らかだから, $\mathfrak{a} = \mathfrak{a}_{i_0}$. したがって, 任意の番号 $i \geq i_0$ に対して,

$$\mathfrak{a} = \mathfrak{a}_{i_0} \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}$$

より, $\mathfrak{a}_i = \mathfrak{a}_{i_0} = \mathfrak{a}$. □

[注意 12.1] 定理 12.7 は, 分数イデアルの無限列に対しては一般には成り立たない. 例えば,

$$\left(\frac{1}{2}\right) \subsetneq \left(\frac{1}{2^2}\right) \subsetneq \left(\frac{1}{2^3}\right) \subsetneq \cdots$$

である.

13 素イデアル

K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする. $\mathfrak{o}_K$ のイデアル $\mathfrak{p}$ が**極大イデアル**であるとは, $\mathfrak{p} \neq \mathfrak{o}_K$ であって, $\mathfrak{o}_K$ の任意のイデアル $\mathfrak{a}$ に対して

$$\mathfrak{a} \mid \mathfrak{p} \Longrightarrow 「\mathfrak{a} = \mathfrak{p} \text{ または } \mathfrak{a} = \mathfrak{o}_K」 \tag{19}$$

が成り立つときにいう. 条件 (19) は, 定理 12.2 より,

$$\mathfrak{p} \subseteq \mathfrak{a} \Longrightarrow 「\mathfrak{a} = \mathfrak{p} \text{ または } \mathfrak{a} = \mathfrak{o}_K」$$

と同値である.

[補題 13.1] R を可換環, $\mathfrak{a}$ を R のイデアルとする. $\mathfrak{a}$ を含む R のイデアルと, $R/\mathfrak{a}$ のイデアルとは 1 対 1 に対応し, その対応は包含関係を変えない.

[証明] $\mathfrak{a}$ を含む R のイデアル全体の集合を Ω とし, $R/\mathfrak{a}$ のイデアル全体の集合を Ω' とする. また, $\pi : R \longrightarrow R/\mathfrak{a}$ を自然な全射準同型とする.

任意の $\mathfrak{b} \in \Omega$ に対して, π は全射だから, $\pi(\mathfrak{b}) \in \Omega'$. また, 任意の $\mathfrak{b}' \in \Omega'$ に対して, $\pi^{-1}(\mathfrak{b}') \in \Omega$ となる. よって, 2 つの写像

$$\Omega \longrightarrow \Omega', \quad \mathfrak{b} \longmapsto \pi(\mathfrak{b}),$$
$$\Omega' \longrightarrow \Omega, \quad \mathfrak{b}' \longmapsto \pi^{-1}(\mathfrak{b})$$

が定まる. π は全射だから, $\pi(\pi^{-1}(\mathfrak{b}')) = \mathfrak{b}'$. 一方, $\mathfrak{a} = \mathrm{Ker}\,\pi$ かつ $\mathfrak{a} \subseteq \mathfrak{b}$ だから, $\pi^{-1}(\pi(\mathfrak{b})) = \mathfrak{b}$. したがって, 上の 2 つの写像は互いに他の逆写像であり, Ω と Ω' とは 1 対 1 に対応する. この対応が包含関係を変えないことは, 写像の定め方から明らかである. □

[補題 13.2] R を可換環とする. このとき,

$$R \text{ は体} \Longleftrightarrow R \text{ のイデアルは } (0) \text{ と } R \text{ のみ}$$

が成り立つ.

[証明] ($\Rightarrow$) $\mathfrak{a}$ を R のイデアルとし, $\mathfrak{a} \neq (0)$ であるとすると, $x \in \mathfrak{a}$ で $x \neq 0$ なるものが存在する. R は体なので, ある $y \in R$ が存在して, $1 = xy$. 一方, $\mathfrak{a}$ は R のイデアルなので, $xy \in \mathfrak{a}$. ゆえに, $1 \in \mathfrak{a}$. よって, $R = (1) \subseteq \mathfrak{a}$. 逆の包含関係は明らかだから, $R = \mathfrak{a}$ となる.

($\Leftarrow$) $x \in R$, $x \neq 0$ とする. 仮定より $(x) = R$ となり, $1 \in (x)$ となる. よって, ある $y \in R$ が存在して $xy = 1$. したがって, R の 0 でないすべての元は逆元をもつ. ゆえに, R は体である. □

[定理 13.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{p}$ を $\mathfrak{o}_K$ のイデアルとする. このとき, 次の 2 つの条件は同値である.

(i) $\mathfrak{p}$ は極大イデアル.

(ii) 剰余環 $\mathfrak{o}_K/\mathfrak{p}$ は体.

[証明] 定理 12.2 より,

$$\mathfrak{p} \text{ は極大イデアル}$$
$$\Longleftrightarrow \mathfrak{p} \text{ を含む } \mathfrak{o}_K \text{ のイデアルは } \mathfrak{p} \text{ と } \mathfrak{o}_K \text{ のみ.}$$

補題 13.1 より,

$$\begin{aligned}&\mathfrak{p} \text{ を含む } \mathfrak{o}_K \text{ のイデアルは } \mathfrak{p} \text{ と } \mathfrak{o}_K \text{ のみ}\\ &\quad\Longleftrightarrow \mathfrak{o}_K/\mathfrak{p} \text{ のイデアルは零イデアルと } \mathfrak{o}_K/\mathfrak{p} \text{ のみ.}\end{aligned}$$

補題 13.2 より,

$$\begin{aligned}&\mathfrak{o}_K/\mathfrak{p} \text{ のイデアルは零イデアルと } \mathfrak{o}_K/\mathfrak{p} \text{ のみ}\\ &\quad\Longleftrightarrow \mathfrak{o}_K/\mathfrak{p} \text{ は体.}\end{aligned}$$

ゆえに, (i), (ii) は同値である. □

[定理 13.4] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を $\mathfrak{o}_K$ のイデアルとし, $\mathfrak{a} \neq \mathfrak{o}_K$ とする. このとき, $\mathfrak{a}$ を含む極大イデアルが存在する.

[証明] 背理法で証明する. $\mathfrak{a}$ を含む極大イデアルは存在しないと仮定する.

$\mathfrak{a}_1 = \mathfrak{a}$ とおく. 定理 11.10 より $[\mathfrak{o}_K : \mathfrak{a}_1]$ は有限である. これを l とおく.

背理法の仮定より $\mathfrak{a}_1$ 自身は極大イデアルではないので, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{a}_2$ が存在して,

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{o}_K.$$

同様に, $\mathfrak{a}_2$ も極大イデアルではないので, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{a}_3$ が存在して,

$$\mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \mathfrak{o}_K.$$

こうして, $\mathfrak{o}_K$ のイデアルの列

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_l \subsetneq \mathfrak{o}_K$$

ができる. ところが,

$$[\mathfrak{a}_2 : \mathfrak{a}_1] \geq 2, \quad \ldots, \quad [\mathfrak{a}_l : \mathfrak{a}_{l-1}] \geq 2, \quad [\mathfrak{o}_K : \mathfrak{a}_l] \geq 2$$

であるから,

$$l = [\mathfrak{o}_K : \mathfrak{a}_1] = [\mathfrak{o}_K : \mathfrak{a}_l][\mathfrak{a}_l : \mathfrak{a}_{l-1}] \cdots [\mathfrak{a}_2 : \mathfrak{a}_1] \geq 2^{l+1}.$$

これは不可能である. □

2 次体 K の整数環 $\mathfrak{o}_K$ のイデアル $\mathfrak{p}$ が**素イデアル**であるとは, $\mathfrak{p} \neq \mathfrak{o}_K$ であって, $\mathfrak{o}_K$ の任意のイデアル $\mathfrak{a}$, $\mathfrak{b}$ に対して

$$\mathfrak{p} \mid \mathfrak{ab} \Longrightarrow 「\mathfrak{p} \mid \mathfrak{a} \text{ または } \mathfrak{p} \mid \mathfrak{b}」 \tag{20}$$

が成り立つときにいう. 条件 (20) は, 定理 12.2 より,

$$\mathfrak{ab} \subseteq \mathfrak{p} \Longrightarrow 「\mathfrak{a} \subseteq \mathfrak{p} \text{ または } \mathfrak{b} \subseteq \mathfrak{p}」$$

と同値である.

[定理 13.5] K を 2 次体, $\mathfrak{o}_K$ を整数環, $\mathfrak{p}$ を $\mathfrak{o}_K$ のイデアルとし, $\mathfrak{p} \neq \mathfrak{o}_K$ とする. このとき, 次の 3 つの条件は同値である.

(i) $\mathfrak{p}$ は素イデアル.

(ii) 任意の x, $y \in \mathfrak{o}_K$ に対して,

$$\alpha\beta \in \mathfrak{p} \Longrightarrow 「\alpha \in \mathfrak{p} \text{ または } \beta \in \mathfrak{p}」$$

が成り立つ.

(iii) $\mathfrak{o}_K/\mathfrak{p}$ は整域.

[証明] (i)⇒(ii)　$\mathfrak{p}$ が素イデアルであるとすれば,

$$\begin{aligned} \alpha\beta \in \mathfrak{p} &\Longrightarrow (\alpha)(\beta) = (\alpha\beta) \subseteq \mathfrak{p} \\ &\Longrightarrow (\alpha) \subseteq \mathfrak{p} \text{ または } (\beta) \subseteq \mathfrak{p} \\ &\Longrightarrow \alpha \in \mathfrak{p} \text{ または } \beta \in \mathfrak{p}. \end{aligned}$$

(ii)⇒(i)　$\mathfrak{ab} \subseteq \mathfrak{p}$, $\mathfrak{a} \not\subseteq \mathfrak{p}$, $\mathfrak{b} \not\subseteq \mathfrak{p}$ と仮定すると, $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$ が存在して, $\alpha\beta \in \mathfrak{p}$, $\alpha \notin \mathfrak{p}$, $\beta \notin \mathfrak{p}$. ところが, 仮定より $\alpha \in \mathfrak{p}$ または $\beta \in \mathfrak{p}$ となって矛盾が生じる. ゆえに, $\mathfrak{ab} \subseteq \mathfrak{p}$ ならば, $\mathfrak{a} \subseteq \mathfrak{p}$ または $\mathfrak{b} \subseteq \mathfrak{p}$ が成り立つ.

(ii)⇔(iii)　$\pi : \mathfrak{o}_K \to \mathfrak{o}_K/\mathfrak{p}$ を自然な全射準同型とすると, $\mathfrak{o}_K/\mathfrak{p} = \pi(\mathfrak{o}_K)$, $\mathfrak{p} = \operatorname{Ker}\pi$ であるから,

$$\begin{aligned} \text{(ii)} &\Longleftrightarrow \alpha\beta \in \operatorname{Ker}\pi \text{ ならば, } \alpha \in \operatorname{Ker}\pi \text{ または } \beta \in \operatorname{Ker}\pi \ (\forall\alpha,\ \beta \in \mathfrak{o}_K) \\ &\Longleftrightarrow \pi(\alpha)\pi(\beta) = \pi(0) \text{ ならば, } \pi(\alpha) = \pi(0) \text{ または } \pi(\beta) = \pi(0) \ (\forall\alpha,\ \beta \in \mathfrak{o}_K) \\ &\Longleftrightarrow \text{(iii)}. \end{aligned}$$

□

[補題 13.6] 有限個の元からなる整域は体である.

[証明] R を有限個の元からなる整域とし, $a \in R$, $a \neq 0$ を任意にとる. 写像

$$f_a : R \longrightarrow R, \quad x \longmapsto ax$$

を考えると, 任意の x, $x' \in R$ に対して, R は整域かつ $a \neq 0$ より,

$$\begin{aligned} f(x) = f(x') &\Longrightarrow ax = ax' \Longrightarrow a(x - x') = 0 \\ &\Longrightarrow x - x' = 0 \Longrightarrow x = x'. \end{aligned}$$

よって, f_a は単射であり, $|R| = |f_a(R)|$. ところが, $f_a(R) \subseteq R$ かつ R は有限集合だから, $f_a(R) = R$ でなければならない. ゆえに, $1 \in R$ に対して, ある $a' \in R$ が存在して, $f_a(a') = 1$ となる. すなわち, $aa' = 1$. したがって, 0 以外の元はすべて逆元をもつから, R は体である. □

[定理 13.7] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を $\mathfrak{o}_K$ のイデアルとし, $\mathfrak{a} \neq (0)$ であるとする. このとき, 次の 2 つの条件は同値である.

(i) $\mathfrak{a}$ は素イデアル.

(ii) $\mathfrak{a}$ は極大イデアル.

[証明] 定理 11.10, 定理 13.3, 定理 13.5, 補題 13.6 より得られる. □

14 素イデアル分解

以下に述べる定理 14.1, 定理 14.2 は, いわゆる**イデアル論の基本定理**と呼ばれるものである.

[定理 14.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を $\mathfrak{o}_K$ のイデアルとし, $\mathfrak{a} \neq (0)$, $\mathfrak{o}_K$ であるとする. このとき, $\mathfrak{a}$ は素イデアルの積で表される.

[証明] $\mathfrak{a}_1 = \mathfrak{a}$ とおく. 定理 13.4 より, $\mathfrak{a}_1$ はある極大イデアル $\mathfrak{p}_1$ に含まれる. 定理 10.2 より, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{a}_2$ が存在して, $\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{a}_2$ となる. $\mathfrak{p} \neq \mathfrak{o}_K$ より, $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. さらに, $\mathfrak{a}_1$ が極大イデアルでなければ, $\mathfrak{a}_2 \subsetneq \mathfrak{o}_K$.

以上の議論をまとめると, $\mathfrak{a}_1$ が極大イデアルでないと仮定すれば, ある極大イデアル $\mathfrak{p}_1$ と $\mathfrak{o}_K$ のイデアル $\mathfrak{a}_2$ が存在して,

$$\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{a}_2, \quad \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{o}_K.$$

同様に, $\mathfrak{a}_2$ が極大イデアルでないと仮定すれば, ある極大イデアル $\mathfrak{p}_2$ と $\mathfrak{o}_K$ のイデアル $\mathfrak{a}_3$ が存在して,

$$\mathfrak{a}_2 = \mathfrak{p}_2\mathfrak{a}_3, \quad \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \mathfrak{o}_K.$$

これを続けると,

$$\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{a}_2, \quad \mathfrak{a}_2 = \mathfrak{p}_2\mathfrak{a}_3, \quad \dots, \quad \mathfrak{a}_{l-1} = \mathfrak{p}_{l-1}\mathfrak{a}_l$$

と, $\mathfrak{o}_K$ のイデアルの列

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_l \subsetneq \mathfrak{o}_K, \quad l = [\mathfrak{o}_K : \mathfrak{a}_1]$$

が得られる. ここで, 定理 11.10 より $[\mathfrak{o}_K : \mathfrak{a}_1]$ は有限である. ところが,

$$[\mathfrak{a}_2 : \mathfrak{a}_1] \geq 2, \quad \dots, \quad [\mathfrak{a}_l : \mathfrak{a}_{l-1}] \geq 2, \quad [\mathfrak{o}_K : \mathfrak{a}_l] \geq 2$$

であるから,

$$l = [\mathfrak{o}_K : \mathfrak{a}_1] = [\mathfrak{o}_K : \mathfrak{a}_l][\mathfrak{a}_l : \mathfrak{a}_{l-1}] \cdots [\mathfrak{a}_2 : \mathfrak{a}_1] \geq 2^{l+1}.$$

これは不可能である. ゆえに, $\mathfrak{a}_1$, $\mathfrak{a}_2$, ..., $\mathfrak{a}_l$ のうちのどれかは極大イデアルである. $\mathfrak{a}_i$ が極大イデアルであるような番号 i を r とおき, $\mathfrak{p}_r = \mathfrak{a}_r$ とおけば, 極大イデアルの積への分解

$$\mathfrak{a} = \mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

が得られる. 定理 13.7 より, 各 $\mathfrak{p}_i$ は素イデアルである. □

[定理 14.2] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を $\mathfrak{o}_K$ のイデアルとし, $\mathfrak{a} \neq (0)$, $\mathfrak{o}_K$ であるとする. このとき, $\mathfrak{a}$ の素イデアルの積による表し方は順序を除いて一意的である.

[証明] $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s$ のように素イデアルの積として 2 通りに表されたとき, $r = s$ かつ適当に番号を付け替えることにより $\mathfrak{p}_i = \mathfrak{q}_i$ $(i = 1, 2, \ldots, r)$ となることを, r に関する数学的帰納法により証明する.

$r = 1$ のとき,

$$\mathfrak{a} = \mathfrak{p}_1 = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s.$$

もし仮に $s \geq 2$ とすると, $\mathfrak{q}_1 \subsetneq \mathfrak{o}_K$, $\mathfrak{q}_2\cdots\mathfrak{q}_s \subseteq \mathfrak{q}_2 \subsetneq \mathfrak{o}_K$ より,

$$\mathfrak{p}_1 = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s \subsetneq \mathfrak{q}_1\mathfrak{o}_K = \mathfrak{q}_1 \subsetneq \mathfrak{o}_K.$$

これは $\mathfrak{p}_1$ が極大イデアルであることに反する. よって, $s = 1$ となり, $\mathfrak{p}_1 = \mathfrak{q}_1$ となる.

$r > 1$ のとき, $r - 1$ のときは素イデアルによる表し方の一意性が成り立つとする.

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s$$

とすれば, $\mathfrak{q}_1 \mid \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ である. $\mathfrak{q}_1$ は素イデアルであるから, いずれかの $\mathfrak{p}_i$ を割るが, $\mathfrak{q}_1 \mid \mathfrak{p}_1$ であるとしても一般性を失わない. 定理 13.7 より $\mathfrak{p}_1$ は極大イデアルだから, $\mathfrak{p}_1 = \mathfrak{q}_1$ となる. 定理 12.1 より,

$$\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_2\cdots\mathfrak{q}_s.$$

帰納法の仮定から, $r = s$ かつ番号を適当に付け替えれば $\mathfrak{p}_i = \mathfrak{q}_i$ $(i = 2, 3, \ldots, r)$ となる. よって, r のときも素イデアルによる表し方の一意性が成り立つ. □

[定理 14.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を K の (0) でない分数イデアルとする. また, $\mathfrak{a}^{-1}$, $\mathfrak{b}^{-1}$ をそれぞれ $\mathfrak{a}$, $\mathfrak{b}$ の逆イデアルとする.

(i) $(\mathfrak{ab})^{-1} = \mathfrak{b}^{-1}\mathfrak{a}^{-1}$.

(ii) $(\mathfrak{a}^e)^{-1} = (\mathfrak{a}^{-1})^e$. ただし, $e > 0$ は有理整数.

[証明] (i) 定理 11.8 より,

$$\mathfrak{ab}(\mathfrak{ab})^{-1} = \mathfrak{o}_K.$$

両辺に $\mathfrak{b}^{-1}\mathfrak{a}^{-1}$ を掛けると,

$$\mathfrak{b}^{-1}\mathfrak{a}^{-1}\mathfrak{ab}(\mathfrak{ab})^{-1} = \mathfrak{b}^{-1}\mathfrak{a}^{-1}.$$

一方, 定理 11.8 より,

$$\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{b}^{-1}\mathfrak{b} = \mathfrak{o}_K.$$

ゆえに, 求める等式が得られる.

(ii)　(i) より, $(\mathfrak{a}^2)^{-1} = (\mathfrak{a}^{-1})^2$ が成り立つ. $e > 2$ の場合は数学的帰納法により示せる.　□

イデアル $\mathfrak{a}$ と有理整数 $e > 0$ に対して, $\mathfrak{a}^{-e} = (\mathfrak{a}^{-1})^e$ と定義する.

[定理 14.4] 2 次体 K の分数イデアル $\mathfrak{a} \neq (0)$, $\mathfrak{o}_K$ は, 相異なる $\mathfrak{o}_K$ の素イデアルの冪積で順序を除いて一意的に表される:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}\mathfrak{p}_{r+1}^{e_{r+1}}\mathfrak{p}_{r+2}^{e_{r+2}}\cdots\mathfrak{p}_{r+s}^{e_{r+s}},$$

ただし, e_1, ..., e_r は正, e_{r+1}, ..., e_{r+s} は負であるとし, $i \neq j$ ならば $\mathfrak{p}_i \neq \mathfrak{p}_j$ とする.

[証明] (表されること)　$\mathfrak{a} \neq (0)$ を分数イデアルとする. ある $c \in \mathfrak{o}_K$, $c \neq 0$ が存在して,

$$(c)\mathfrak{a} = c\mathfrak{a} \subseteq \mathfrak{o}_K.$$

$(c)\mathfrak{a}$ に対して定理 14.1 を適用すると,

$$(c)\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r.$$

一方, $(\lambda) \subseteq \mathfrak{o}_K$ だから, 定理 14.1 により,

$$(c) = \mathfrak{p}_{r+1}\mathfrak{p}_{r+2}\cdots\mathfrak{p}_{r+s}.$$

ゆえに,

$$\mathfrak{p}_{r+1}\mathfrak{p}_{r+2}\cdots\mathfrak{p}_{r+s}\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r.$$

両辺に $\mathfrak{p}_{r+s}^{-1}\cdots\mathfrak{p}_{r+2}^{-1}\mathfrak{p}_{r+1}^{-1}$ を掛けると, 定理 11.8 より $\mathfrak{p}_i^{-1}\mathfrak{p}_i = \mathfrak{o}_K$ であるから,

$$\mathfrak{a} = \mathfrak{p}_{r+s}^{-1}\cdots\mathfrak{p}_{r+2}^{-1}\mathfrak{p}_{r+1}^{-1}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$$

となる. ここからさらに $\mathfrak{p}_i^{-1}\mathfrak{p}_i = \mathfrak{o}_K$ によって素イデアルとその逆イデアルを消去していけば, 定理で述べたような形で表される.

(表し方の一意性)　$\mathfrak{a}$ が 2 通りに表されたとする:

$$\begin{aligned}\mathfrak{a} &= \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}\mathfrak{p}_{r+1}^{e_{r+1}}\mathfrak{p}_{r+2}^{e_{r+2}}\cdots\mathfrak{p}_{r+s}^{e_{r+s}} \\ &= \mathfrak{q}_1^{f_1}\mathfrak{q}_2^{f_2}\cdots\mathfrak{q}_{r'}^{f_{r'}}\mathfrak{q}_{r+1}^{f_{r'+1}}\mathfrak{q}_{r'+2}^{f_{r'+2}}\cdots\mathfrak{q}_{r'+s'}^{f_{r'+s'}}\end{aligned}$$

ただし, e_1, ..., e_r, f_1, ..., $f_{r'}$ は正, e_{r+1}, ..., e_{r+s}, $f_{r'+1}$, ..., $f_{r'+s'}$ は負であるとし, $i \neq j$ ならば $\mathfrak{p}_i \neq \mathfrak{p}_j$, $\mathfrak{q}_i \neq \mathfrak{q}_j$ とする. 定理 11.8 を用いると,

$$\begin{aligned}&\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}\mathfrak{q}_{r+1}^{-f_{r'+1}}\mathfrak{q}_{r'+2}^{-f_{r'+2}}\cdots\mathfrak{q}_{r'+s'}^{-f_{r'+s'}} \\ &\quad = \mathfrak{q}_1^{f_1}\mathfrak{q}_2^{f_2}\cdots\mathfrak{q}_{r'}^{f_{r'}}\mathfrak{p}_{r+1}^{-e_{r+1}}\mathfrak{p}_{r+2}^{-e_{r+2}}\cdots\mathfrak{p}_{r+s}^{-e_{r+s}}.\end{aligned}$$

$\mathfrak{p}_i$ 同士は互いに異なり, $\mathfrak{q}_i$ 同士も互いに異なるから, 定理 14.2 より, 番号を適当に付け替えれば

$$\mathfrak{p}_i = \mathfrak{q}_i, \quad e_i = f_i, \quad r = r', \quad s = s' \quad (i = 1, 2, \ldots, r+s)$$

となる. □

K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする. K の分数イデアル $\mathfrak{a} \neq (0)$, $\mathfrak{o}_K$ は, 定理 14.4 より, 相異なる $\mathfrak{o}_K$ の素イデアル $\mathfrak{p}_\mathrm{i}$ の積に分解する:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}, \quad e_i \in \mathbb{Z}.$$

この表示を $\mathfrak{a}$ の**素イデアル分解**といい, 各々の素イデアル $\mathfrak{p}_i$ を $\mathfrak{a}$ の**素イデアル因子**という. 分解の一意性により, 各 e_i は $\mathfrak{a}$ と $\mathfrak{p}_\mathrm{i}$ に対して一意的に定まる. そこで, $\mathfrak{o}_K$ の素イデアル $\mathfrak{p}$ に対して,

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}) = \begin{cases} e_i, & \mathfrak{p} = \mathfrak{p}_i \text{ のとき} \\ 0, & \mathfrak{p} \nmid \mathfrak{a} \text{ のとき} \end{cases}$$

と定める. また, $\mathfrak{a} = \mathfrak{o}_K$ または $\mathfrak{a} = (0)$ のときは, それぞれ $\mathrm{ord}_\mathfrak{p}(\mathfrak{o}_K) = 0$, $\mathrm{ord}_\mathfrak{p}((0)) = \infty$ と定める. $\mathrm{ord}_\mathfrak{p}(\mathfrak{a})$ を $\mathfrak{a}$ の $\mathfrak{p}$ **指数**という.

$\mathfrak{a}$, $\mathfrak{b}$ を 2 次体 K の分数イデアルとする.

すべての素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}) = \mathrm{ord}_\mathfrak{p}(\mathfrak{b})$$

が成り立つことは, $\mathfrak{a} = \mathfrak{b}$ であるための必要十分条件である.

すべての素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}) \leq \mathrm{ord}_\mathfrak{p}(\mathfrak{b})$$

が成り立つことは, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{t}$ が存在して $\mathfrak{b} = \mathfrak{a}\mathfrak{t}$ となるための必要十分条件である. このことは, 定理 12.2 より, $\mathfrak{b} \subseteq \mathfrak{a}$ と同値である.

特に, すべての素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}) \geq 0$$

が成り立つことは, $\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルであるための必要十分条件である. なぜなら, $\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルであることは $\mathfrak{a} \subseteq \mathfrak{o}_K$ と同値であり, すべての素イデアル $\mathfrak{p}$ に対して $\mathrm{ord}_\mathfrak{p}(\mathfrak{o}_K) = 0$ だからである.

$\mathfrak{a}$, $\mathfrak{b}$ の積 $\mathfrak{a}\mathfrak{b}$ について, すべての素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = \mathrm{ord}_\mathfrak{p}(\mathfrak{a}) + \mathrm{ord}_\mathfrak{p}(\mathfrak{b})$$

が成り立つ. また, 和 $\mathfrak{a}+\mathfrak{b}$ と共通部分 $\mathfrak{a}\cap\mathfrak{b}$ について, 定理 12.3 より, すべての素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}+\mathfrak{b}) = \min\{\mathrm{ord}_\mathfrak{p}(\mathfrak{a}), \mathrm{ord}_\mathfrak{p}(\mathfrak{b})\}$$
$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}\cap\mathfrak{b}) = \max\{\mathrm{ord}_\mathfrak{p}(\mathfrak{a}), \mathrm{ord}_\mathfrak{p}(\mathfrak{b})\}$$

が成り立つ. なお, $\mathfrak{a}$, $\mathfrak{b}$ が $\mathfrak{o}_K$ のイデアルであるとき, $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}\cap\mathfrak{b}$ はそれぞれ $\mathfrak{a}$, $\mathfrak{b}$ の最大公約イデアル, 最小公倍イデアルである.

$\mathfrak{a}$, $\mathfrak{b}$ が $\mathfrak{o}_K$ のイデアルであるとき, $(\mathfrak{a},\,\mathfrak{b})=1$ であること, すなわち $\mathfrak{a}+\mathfrak{b}=\mathfrak{o}_K$ が成り立つための必要十分条件は, すべての素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b})=0$$

が成り立つことである. これは, $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})\geq 0$, $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\geq 0$ より, 任意の素イデアル $\mathfrak{p}$ に対して

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})=0 \quad \text{または} \quad \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})=0$$

が成り立つことと同値である. それは, $\mathfrak{a}$ と $\mathfrak{b}$ が共通の素イデアル因子を持たないことを意味する.

[定理 14.5] K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする. K の任意の分数イデアル $\mathfrak{a}\neq(0)$ に対して, $\mathfrak{o}_K$ のイデアル $\mathfrak{b}$, $\mathfrak{c}$ が一意的に存在して,

$$\mathfrak{a}=\mathfrak{b}\mathfrak{c}^{-1},\quad (\mathfrak{b},\,\mathfrak{c})=1$$

が成り立つ.

[証明] $\mathfrak{a}=\mathfrak{o}_K$ のときは, $\mathfrak{b}=\mathfrak{c}=\mathfrak{o}_K$ とすればよい. $\mathfrak{a}\neq\mathfrak{o}_K$ のときは, 定理 14.4 の素イデアルの積による表示において

$$\mathfrak{b}=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$
$$\mathfrak{c}=\mathfrak{p}_{r+s}^{-e_{r+s}}\cdots\mathfrak{p}_{r+2}^{-e_{r+2}}\mathfrak{p}_{r+1}^{-e_{r+1}}$$

とおけばよい. $(\mathfrak{b},\,\mathfrak{c})=1$ であることは, $\mathfrak{p}_1$, $\mathfrak{p}_2$, …, $\mathfrak{p}_{r+s}$ が相異なる素イデアルであることによる. $\mathfrak{b}$, $\mathfrak{c}$ の一意性は, $\mathfrak{a}$ を素イデアルの積で表示する仕方の一意性からわかる. □

K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{p}$ を $\mathfrak{o}_K$ の素イデアルとする. 各 $\alpha\in K$ に対して, α の $\mathfrak{p}$ **指数** $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ を, 単項イデアル (α) の $\mathfrak{p}$ 指数 $\mathrm{ord}_{\mathfrak{p}}((\alpha))$ によって定義する. そうすると, 写像

$$\mathrm{ord}_{\mathfrak{p}}:K\longrightarrow\mathbb{R}\cup\{\infty\},\quad \alpha\longmapsto\mathrm{ord}_{\mathfrak{p}}(\alpha)$$

が定まる. これを $\mathfrak{p}$ **進付値**という.

[定理 14.6] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{p}$ を $\mathfrak{o}_K$ の素イデアル, α, $\beta\in K$ とする.

(i) $\mathrm{ord}_{\mathfrak{p}}(\alpha\beta)=\mathrm{ord}_{\mathfrak{p}}(\alpha)+\mathrm{ord}_{\mathfrak{p}}(\beta)$.

(ii) $\mathrm{ord}_{\mathfrak{p}}(\alpha+\beta)\geq\min\{\mathrm{ord}_{\mathfrak{p}}(\alpha),\mathrm{ord}_{\mathfrak{p}}(\beta)\}$. さらに, $\mathrm{ord}_{\mathfrak{p}}(\alpha)\neq\mathrm{ord}_{\mathfrak{p}}(\beta)$ ならば等号が成り立つ.

[証明] (i)　$\mathrm{ord}_{\mathfrak{p}}((\alpha\beta)) = \mathrm{ord}_{\mathfrak{p}}((\alpha)(\beta)) = \mathrm{ord}_{\mathfrak{p}}((\alpha)) + \mathrm{ord}_{\mathfrak{p}}((\beta))$ よりわかる.

(ii)　$\alpha+\beta \in (\alpha)+(\beta)$ より, $(\alpha+\beta) \subseteq (\alpha)+(\beta)$. よって, $(\alpha)+(\beta) \mid (\alpha+\beta)$. これより, 求める不等式が得られる.

さらに, $\mathrm{ord}_{\mathfrak{p}}(\alpha) < \mathrm{ord}_{\mathfrak{p}}(\beta)$ ならば,

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(\alpha+\beta) &\geq \min\{\mathrm{ord}_{\mathfrak{p}}(\alpha), \mathrm{ord}_{\mathfrak{p}}(\beta)\} \\ &= \mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}\big((\alpha+\beta)-\beta\big) \\ &\geq \min\{\mathrm{ord}_{\mathfrak{p}}(\alpha+\beta), \mathrm{ord}_{\mathfrak{p}}(\beta)\}.\end{aligned}$$

最後の式がもし仮に $\mathrm{ord}_{\mathfrak{p}}(\beta)$ に等しいとすると, $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq \mathrm{ord}_{\mathfrak{p}}(\beta)$ となり矛盾が生じる. よって, 最後の式は $\mathrm{ord}_{\mathfrak{p}}(\alpha+\beta)$ でなければならない. ゆえに, $\mathrm{ord}_{\mathfrak{p}}(\alpha+\beta) = \mathrm{ord}_{\mathfrak{p}}(\alpha)$ となる. 同様に, $\mathrm{ord}_{\mathfrak{p}}(\beta) < \mathrm{ord}_{\mathfrak{p}}(\alpha)$ ならば, $\mathrm{ord}_{\mathfrak{p}}(\alpha+\beta) = \mathrm{ord}_{\mathfrak{p}}(\beta)$ となる. □

[定理 14.7] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b}$ を $\mathfrak{o}_K$ の (0) でないイデアルとし, $\mathfrak{b} \subseteq \mathfrak{a}$ であるとする. このとき, ある $\mu \in \mathfrak{a}$ が存在して,

$$\mathfrak{b} + (\mu) = \mathfrak{a}$$

が成り立つ.

[証明] まず, $\mathfrak{b}$ の素イデアル分解を

$$\mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{f_i}, \quad f_i \geq 1$$

とする. $\mathfrak{b} \subseteq \mathfrak{a}$ より $\mathfrak{a} \mid \mathfrak{b}$. よって, $\mathfrak{a}$ を

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}, \quad 0 \leq e_i \leq f_i$$

と表すことができる. $\mathfrak{m} = \mathfrak{a}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i+1}$ とおく. さらに, 各 i について $\mathfrak{m}_i = \mathfrak{m}\mathfrak{p}_i^{-1}$ とおく. $\mathfrak{m}_i$ は $\mathfrak{o}_K$ のイデアルである. また, $\mathfrak{m}_i \mid \mathfrak{m}$ かつ $\mathfrak{m}_i \neq \mathfrak{m}$ であるから, $\mathfrak{m} \subsetneq \mathfrak{m}_i$. よって, 各 i に対して, $\mu_i \in \mathfrak{m}_i$ で $\mu_i \notin \mathfrak{m}$ となるものが存在する. $(\mu_i) \subseteq \mathfrak{m}_i$ より $\mathfrak{m}_i \mid (\mu_i)$ であるから,

$$\mathrm{ord}_{\mathfrak{p}_j}(\mu_i) \begin{cases} \geq e_i, & j = i \text{ のとき} \\ \geq e_j + 1, & j \neq i \text{ のとき} \end{cases}$$

である. 一方, もし仮に $\mathrm{ord}_{\mathfrak{p}_i}(\mu_i) \geq e_i + 1$ とすると, $\mathfrak{m} \mid (\mu_i)$ となって $\mu_i \notin \mathfrak{m}$ に反するから, $\mathrm{ord}_{\mu_i}(\beta_i) \leq e_i$. したがって,

$$\mathrm{ord}_{\mathfrak{p}_j}(\mu_i) \begin{cases} = e_i, & j = i \text{ のとき} \\ > e_j, & j \neq i \text{ のとき} \end{cases}$$

が成り立つ. $\mu = \sum_{i=1}^{r} \mu_i$ とおく. 各 i について, $\mathfrak{m}_i$ の定め方より $\mathfrak{a} \mid \mathfrak{m}_i$, よって $\mathfrak{m}_i \subseteq \mathfrak{a}$ であるから, $\mu_i \in \mathfrak{a}$. ゆえに, $\mu \in \mathfrak{a}$. また,

$$\mathrm{ord}_{\mathfrak{p}_1}(\mu_2 + \cdots + \mu_r) \geq \min\{\mathrm{ord}_{\mathfrak{p}_1}(\mu_2), \ldots, \mathrm{ord}_{\mathfrak{p}_1}(\mu_r)\} > e_1$$

であるから, 定理 14.6 より, $\mathrm{ord}_{\mathfrak{p}_1}(\mu) = \mathrm{ord}_{\mathfrak{p}_1}(\mu_1) = e_1$ となる. $i = 2, 3, \ldots, r$ の場合も同様なので,

$$\mathrm{ord}_{\mathfrak{p}_i}(\mu) = \mathrm{ord}_{\mathfrak{p}_i}(\mu_i) = e_i, \quad (i = 1, 2, \ldots, r)$$

がいえる. ゆえに,

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{b} + (\mu)) &= \min\{\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{b}), \mathrm{ord}_{\mathfrak{p}_i}(\mu)\} \\ &= \min\{f_i, e_i\} = e_i. \end{aligned}$$

一方, $\mathfrak{p} \neq \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ なる素イデアル $\mathfrak{p}$ に対しては, $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0$ であり, $\mu \in \mathfrak{o}_K$ より $\mathrm{ord}_{\mathfrak{p}_i}(\mu) \geq 0$ であるから,

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b} + (\mu)) &= \min\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}), \mathrm{ord}_{\mathfrak{p}}(\mu)\} \\ &= \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0. \end{aligned}$$

以上より, $\mathfrak{o}_K$ のすべての素イデアル $\mathfrak{p}$ に対して,

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b} + (\mu)) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$$

が示された. したがって, $\mathfrak{b} + (\mu) = \mathfrak{a}$ となる. □

[定理 14.8] K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする. このとき,

$$\mathfrak{o}_K \text{ が素元分解整域} \Longrightarrow \mathfrak{o}_K \text{ が単項イデアル整域}$$

が成り立つ.

[証明] (0) と $\mathfrak{o}_K$ はもともと単項イデアルであり, それ以外の $\mathfrak{o}_K$ の任意のイデアルは素イデアルの積に表されるから, 任意の (0) でない素イデアルが単項イデアルであることを示せば十分である.

$\mathfrak{p} \neq (0)$ を $\mathfrak{o}_K$ の素イデアルとする. $\alpha \in \mathfrak{p}$, $\alpha \neq 0$ をとれば, $\mathfrak{p} \neq \mathfrak{o}_K$ より α は単元でない. よって, 仮定より α は

$$\alpha = \prod_{i=1}^{r} p_i^{e_i}, \quad e_i \geq 1$$

のように素元 p_i の積に表される. $\mathfrak{p}$ は素イデアルだから,

$$\prod_{i=1}^{r} p_i^{e_i} \in \mathfrak{p} \Longrightarrow \text{ある } i \text{ が存在して } p_i \in \mathfrak{p}.$$

ゆえに,

$$(p_i) \subseteq \mathfrak{p}_i \subsetneq \mathfrak{o}_K.$$

一方, p_i は素元だから (p_i) は素イデアルになる．$\mathfrak{o}_K$ において素イデアルは極大イデアルだから, $(p_i) = \mathfrak{p}$. したがって, $\mathfrak{p}$ は単項イデアルである． □

[注意 14.1] 定理 14.8 は, 一般に, イデアル論の基本定理が成り立つ整域, いわゆる Dedekind 整域において成り立つ. 一方, 定理 14.8 の逆, すなわち単項イデアル整域ならば素元分解整域であることは, イデアル論の基本定理を仮定しなくても成り立つ.

15 原始イデアル

K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする．$\mathfrak{o}_K$ のイデアル $\mathfrak{a}_0$ が**原始イデアル**であるとは, $\mathfrak{a}_0$ に含まれるすべての元の公約数で有理整数であるものが ± 1 のみであるときにいう.

[補題 15.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, ω_1, ω_2 を K の整数底, a, b, $c \in \mathbb{Z}$ とする．このとき, c が $\mathfrak{o}_K$ における $a\omega_1 + b\omega_2$ の約数ならば, c は $\mathbb{Z}$ における a, b の公約数である.

[証明] 仮定より, ある $x \in \mathfrak{o}_K$ が存在して, $a\omega_1 + b\omega_2 = cx$ となる．ω_1, ω_2 は整数底だから, ある a', $b' \in \mathbb{Z}$ が存在して, $x = a'\omega_1 + b'\omega_2$. ゆえに,

$$a\omega_1 + b\omega_2 = c(a'\omega_1 + b'\omega_2) = ca'\omega_1 + cb'\omega_2.$$

整数底の $\mathbb{Z}$ 係数の 1 次結合で表す仕方は一意的だから,

$$a = ca', \quad b = cb'.$$

すなわち, c は a, b の公約数である． □

[定理 15.2] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, 1, ω を K の標準的整数底, $\mathfrak{a}$ を $\mathfrak{o}_K$ のイデアルとする．このとき, ある $b \in \mathbb{Z}$ が存在して $b + \omega \in \mathfrak{a}$ ならば, $\mathfrak{a}$ は原始イデアルである.

[証明] $d \in \mathbb{Z}$ を $\mathfrak{a}$ のすべての元の公約数とすると, d は $\mathfrak{o}_K$ における $b + \omega$ の約数である．補題 15.1 より, d は $\mathbb{Z}$ において 1 を割る．ゆえに, $d = \pm 1$. したがって, $\mathfrak{a}$ は原始イデアルである． □

[補題 15.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, 1, ω を K の標準的整数底とする．また, ω_1, $\omega_2 \in K$ とし,

$$\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

とおく. このとき, $\omega\omega_1,\ \omega\omega_2 \in \mathfrak{a}$ ならば,

$$\mathfrak{a} = \mathfrak{o}_K\omega_1 + \mathfrak{o}_K\omega_2$$

が成り立つ. したがって, $\mathfrak{a}$ は $\omega_1,\ \omega_2$ から生成される K の分数イデアルである. 特に, $\omega_1,\ \omega_2 \in \mathfrak{o}_K$ であれば, $\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルである.

[証明] $\alpha \in \mathfrak{o}_K\omega_1 + \mathfrak{o}_K\omega_2$ とすると,

$$\alpha = x\omega_1 + y\omega_2, \quad x,\ y \in \mathfrak{o}_K$$

と表される. $\mathfrak{o}_K = [1,\ \omega]$ より,

$$\begin{aligned} x &= x_1 + x_2\omega, \quad x_1,\ x_2 \in \mathbb{Z}, \\ y &= y_1 + y_2\omega, \quad y_1,\ y_2 \in \mathbb{Z} \end{aligned}$$

と表される. よって,

$$\begin{aligned} \alpha &= (x_1 + x_2\omega)\omega_1 + (y_1 + y_2\omega)\omega_2 \\ &= x_1\omega_1 + x_2\omega\omega_1 + y_1\omega_2 + y_2\omega\omega_2. \end{aligned}$$

$\omega\omega_1,\ \omega\omega_2 \in \mathfrak{a}$ より,

$$\begin{aligned} \omega\omega_1 &= u_1\omega_1 + u_2\omega_2, \quad u_1,\ u_2 \in \mathbb{Z}, \\ \omega\omega_2 &= v_1\omega_1 + v_2\omega_2, \quad v_1,\ v_2 \in \mathbb{Z} \end{aligned}$$

と表される. ゆえに,

$$\begin{aligned} \alpha &= x_1\omega_1 + x_2(u_1\omega_1 + u_2\omega_2) \\ &\qquad + y_1\omega_2 + y_2(v_1\omega_1 + v_2\omega_2) \\ &= (x_1 + x_2u_1 + y_2v_1)\omega_1 \\ &\qquad + (x_2u_2 + y_1 + y_2v_2)\omega_2 \\ &\in \mathfrak{a}. \end{aligned}$$

したがって, $\mathfrak{o}_K\omega_1 + \mathfrak{o}_K\omega_2 \subseteq \mathfrak{a}$. 逆の包含関係は明らかである. □

[定理 15.4] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $1,\ \omega$ を K の標準的整数底, $a,\ b \in \mathbb{Z},\ a > 0$ とする. このとき,

$$N_K(b + \omega) \in a\mathbb{Z}$$

ならば,

$$\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}(b + \omega)$$

は $\mathfrak{o}_K$ の原始イデアルであり, $a,\ b + \omega$ は $\mathfrak{a}$ の標準的基底である.

[証明] $\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルであることをいうためには $\mathfrak{a} = \mathfrak{o}_K a + \mathfrak{o}_K(b+\omega)$ となることをいえばよいが, 補題 15.3 より, $a\omega$, $(b+\omega)\omega \in \mathfrak{a}$ をいえば十分である.

まず,

$$a\omega = -ba + a(b+\omega) \in \mathfrak{a}.$$

次に, $\omega^2 - (\mathrm{Tr}_K\omega)\omega + N_K\omega = 0$ より, $v = \mathrm{Tr}_K\omega = \omega + \omega^\sigma$, $-u = N_K\omega = \omega\omega^\sigma$ とおくと,

$$\omega^2 = u + v\omega, \quad u,\, v \in \mathbb{Z}.$$

$N_K(b+\omega) \in a\mathbb{Z}$ より, ある $s \in \mathbb{Z}$ が存在して,

$$\begin{aligned} sa = N_K(b+\omega) &= (b+\omega)(b+\omega)^\sigma \\ &= b^2 + vb - u. \end{aligned}$$

ゆえに,

$$\begin{aligned} (b+\omega)\omega &= b\omega + (u+v\omega) \\ &= -(b^2+vb-u) + (b+v)(b+\omega) \\ &= -sa + (b+v)(b+\omega) \in \mathfrak{a}. \end{aligned}$$

以上より, $\mathfrak{a}$ が $\mathfrak{o}_K$ のイデアルであることが証明された.

$b+\omega \in \mathfrak{a}$ であるから, 定理 15.2 より, $\mathfrak{a}$ は原始イデアルである.

定理 10.8 より, a, $b+\omega$ は $\mathfrak{a}$ の標準的基底である. □

[定理 15.5] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を $\mathfrak{o}_K$ のイデアル, a_0, $b + c_0\omega$ を $\mathfrak{a}$ の標準的基底とする. このとき, c_0 は $\mathbb{Z}$ における a_0, b の公約数である. したがって,

$$\mathfrak{a}_0 = \mathbb{Z}a_0' + \mathbb{Z}(b'+\omega), \quad a_0 = c_0a_0', \quad b = c_0b'$$

とおけば, $\mathfrak{a} = c_0\mathfrak{a}_0$ となる. $\mathfrak{a}_0$ は原始イデアルであり, a_0', $b'+\omega$ は $\mathfrak{a}_0$ の標準的基底である.

[証明] 補題 10.5 より, c_0 は $\mathbb{Z}$ における a_0, b の約数である. よって, $\mathfrak{a} = c_0\mathfrak{a}_0$ となる. このとき, $\mathfrak{a}_0 = c_0^{-1}\mathfrak{a}$ なので, $\mathfrak{a}_0$ は K の分数イデアルである. $\mathfrak{a}_0 \subseteq \mathfrak{o}_K$ より, $\mathfrak{a}_0$ は $\mathfrak{o}_K$ のイデアルである. $b'+\omega \in \mathfrak{a}_0$ であるから, 定理 15.2 より, $\mathfrak{a}_0$ は原始イデアルである. 定理 10.8 より, a_0', $b'+\omega$ は $\mathfrak{a}_0$ の標準的基底である. □

[例 15.1] $\mathfrak{o}_K$ を 2 次体 K の整数環, 1, ω を K の標準的整数底とする. $\mathfrak{o}_K$ については, $a_0 = c_0 = 1$ となる. したがって, 任意の $b \in \mathbb{Z}$ に対して, 1, $b+\omega$ は $\mathfrak{o}_K$ の標準的基底である. また, $\mathfrak{o}_K$ は原始イデアルである.

K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$ を $\mathfrak{o}_K$ の原始イデアルとする. このとき, 原始イデアルの定義より, 定理 15.5 において $c_0 = 1$ となり,

$$\mathfrak{a} = [a,\, b+\omega], \quad a,\, b \in \mathbb{Z}, \quad a > 0$$

と表される. ここで, 定理 10.8, 定理 15.2 より, 一般の $\mathfrak{o}_K$ のイデアル $\mathfrak{a}$ がこの形で表されれば, $\mathfrak{a}$ は原始イデアルであり, a, $b+\omega$ は必ず $\mathfrak{a}$ の標準的基底であることに注意しておく. 定理 11.10, 定理 11.11 より,

$$N\mathfrak{a} = a$$

が成り立つ.

[定理 15.6] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} = [a,\, b+\omega]$ を $\mathfrak{o}_K$ の原始イデアルとする. $i = 1, 2$ に対して,

$$\mathfrak{a}_i = \mathbb{Z}a_i + \mathbb{Z}(b+\omega), \quad a_i \in \mathbb{Z}$$

とおく. このとき, $a = a_1 a_2$ ならば, $\mathfrak{a}_1$, $\mathfrak{a}_2$ も原始イデアルで $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ が成り立つ.

[証明] 定理 10.8 より

$$N(b+\omega) \in a\mathbb{Z} \subseteq a_i\mathbb{Z}$$

だから, 定理 15.4 より $\mathfrak{a}_i$ は原始イデアルであり, a_i, $b+\omega$ は $\mathfrak{a}_i$ の標準的基底である. よって,

$$\begin{aligned}
\mathfrak{a}_1\mathfrak{a}_2 &= (a_1,\, b+\omega)(a_2,\, b+\omega) \\
&= (a_1a_2,\, a_1(b+\omega),\, a_2(b+\omega),\, (b+\omega)^2) \\
&= (a,\, a_1(b+\omega),\, a_2(b+\omega),\, (b+\omega)^2) \\
&\subseteq (a,\, b+\omega) = \mathfrak{a}.
\end{aligned}$$

一方,

$$N\mathfrak{a} = a = a_1a_2 = N\mathfrak{a}_1 N\mathfrak{a}_2.$$

定理 12.4 より, $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$. □

16 素数の 2 次体での分解

K を 2 次体, $\mathfrak{o}_K$ を K の整数環, p を素数とする. イデアル論の基本定理により, 単項イデアル $(p) = p\mathfrak{o}_K$ は素イデアルの積に順序を除いて一意的に分解される:

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}, \quad e_i \geq 1, \quad g \geq 1.$$

これを p の K での**素イデアル分解**という. 両辺のノルムをとると,

$$p^2 = N\mathfrak{p}_1^{e_1} N\mathfrak{p}_2^{e_2} \cdots N\mathfrak{p}_g^{e_g}.$$

$i = 1, 2, \ldots, g$ に対して, $N\mathfrak{p}_i = [\mathfrak{o}_K : \mathfrak{p}_i] \in \mathbb{Z}$ なので, $\mathbb{Z}$ における素因数分解の一意性により,

$$N\mathfrak{p}_i = p^{f_i}$$

の形になる. $\mathfrak{p}_i \subsetneq \mathfrak{o}_K$ より $N\mathfrak{p}_i > 1$ なので, $f_i \geq 1$ である. よって,

$$2 = e_1 f_1 + e_2 f_2 + \cdots + e_g f_g, \quad e_i \geq 1, \quad f_i \geq 1, \quad g \geq 1$$

が成り立つ. したがって, 次の 3 つの場合が可能である:

(D1) $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$.
(D2) $g = 1$, $e_1 = 1$, $f_1 = 2$.
(D3) $g = 1$, $e_1 = 2$, $f_1 = 1$.

それぞれの場合に, p の K での素イデアル分解は次のようになる:

(D1) $(p) = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $N\mathfrak{p}_1 = N\mathfrak{p}_2 = p$.
(D2) $(p) = \mathfrak{p}_1$, $N\mathfrak{p}_1 = p^2$.
(D3) $(p) = \mathfrak{p}_1^2$, $N\mathfrak{p}_1 = p$.

(D1) の場合, p は $K/\mathbb{Q}$ で**完全分解する**という. (D2) の場合, p は $K/\mathbb{Q}$ で**惰性する**という. (D3) の場合, p は $K/\mathbb{Q}$ で**完全分岐する**という. また, すべての i について $e_i = 1$ のとき, すなわち, いまの場合でいえば完全分解か惰性のどちらかであるとき, p は $K/\mathbb{Q}$ で**不分岐**であるという.

e_i を $\mathfrak{p}_i$ の $K/\mathbb{Q}$ における**分岐指数**といい, f_i を $\mathfrak{p}_i$ の $K/\mathbb{Q}$ における**相対次数**という. また, $f_i = 1, 2$ のそれぞれの場合に応じて, $\mathfrak{p}_i$ を **1 次の素イデアル**, **2 次の素イデアル**という.

[定理 16.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{p} \neq (0)$ を $\mathfrak{o}_K$ の素イデアル, p を $\mathfrak{p}$ に含まれる最小正の有理整数とする.

(i) p は素数である.
(ii) $\mathfrak{p}$ に含まれる素数は p のみである.
(iii) $N\mathfrak{p} = p$ または p^2. もっと詳しくいうと,

$$N\mathfrak{p} = \begin{cases} p, & \mathfrak{p} \neq (p) \text{ のとき} \\ p^2, & \mathfrak{p} = (p) \text{ のとき} \end{cases}$$

が成り立つ.

[証明] 定理 10.4 より, $\mathfrak{p}$ に含まれる最小正の有理整数 p が存在して, $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ となる.

(i) もし仮に p が素数でなければ, ある $a, b \in \mathbb{Z}$ が存在して,

$$p = ab, \quad 1 < a < p, \quad 1 < b < p.$$

ところが, $\mathfrak{p}$ は素イデアルであるから,

$$ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \text{ または } b \in \mathfrak{p}.$$

これは p の最小性に反する. ゆえに, p は素数でなければならない.

(ii)　$\mathfrak{p}$ に含まれるすべての有理素数は, $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ の元, したがって p の倍数である. よって, p 以外の素数は $\mathfrak{p}$ に含まれない.

(iii)　$p \in \mathfrak{p}$ より, $(p) \subseteq \mathfrak{p}$. ゆえに, $\mathfrak{p} \mid (p)$. すなわち, ある $\mathfrak{o}_K$ のイデアル $\mathfrak{a}$ が存在して,

$$(p) = \mathfrak{p}\mathfrak{a}.$$

よって,

$$N\mathfrak{p}N\mathfrak{a} = N(p) = |N_K p| = p^2.$$

$\mathfrak{p} = (p)$ のとき, $N\mathfrak{p} = N(p) = p^2$.

$\mathfrak{p} \neq (p)$ のとき, $\mathfrak{a} \subsetneq \mathfrak{o}_K$ であるから,

$$N\mathfrak{a} = [\mathfrak{o}_K : \mathfrak{a}] > 1.$$

$\mathfrak{p}$ は素イデアルなので, 定義より $\mathfrak{p} \subsetneq \mathfrak{o}_K$. よって,

$$N\mathfrak{p} = [\mathfrak{o}_K : \mathfrak{p}] > 1.$$

ゆえに, $N\mathfrak{p} = p$ となる. □

定理 16.1 によれば, 任意の素イデアル $\mathfrak{p}$ に対して, ある素数 p がただ 1 つ存在して, $\mathfrak{p} \mid (p)$. したがって, $\mathfrak{p}$ は, p の素イデアル分解にのみ現れ, p 以外の素数の素イデアル分解には現れない.

さて, K を 2 次体, $\mathfrak{o}_K$ を K の整数環, p を素数, $\mathfrak{p}$ を p の K での素イデアル分解に現れる素イデアルとする. このとき, $\mathfrak{o}_K/\mathfrak{p}$ は整域である. 元の個数が有限なので, $\mathfrak{o}_K/\mathfrak{p}$ は体になるのであった. 環の準同型写像

$$\varphi_{\mathfrak{p}} : \mathbb{Z} \longrightarrow \mathfrak{o}_K/\mathfrak{p}, \quad x \longmapsto x + \mathfrak{p}$$

を考えると, $\operatorname{Ker}\varphi_{\mathfrak{p}} = p\mathbb{Z}$ となる. 実際,

$$\begin{aligned} x \in \operatorname{Ker}\varphi_{\mathfrak{p}} &\Longleftrightarrow x \in \mathbb{Z},\ \varphi_{\mathfrak{p}}(x) = \mathfrak{p} \\ &\Longleftrightarrow x \in \mathbb{Z},\ x + \mathfrak{p} = \mathfrak{p} \\ &\Longleftrightarrow x \in \mathbb{Z},\ x \in \mathfrak{p} \\ &\Longleftrightarrow x \in \mathfrak{p} \cap \mathbb{Z}. \end{aligned}$$

定理 16.1 より p は $\mathfrak{p}$ に含まれる最小の有理整数なので, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. ゆえに, $\operatorname{Ker}\varphi_{\mathfrak{p}} = p\mathbb{Z}$ となる. したがって, 準同型定理により, 体から体の中への単射準同型

$$\mathbb{Z}/p\mathbb{Z} \cong \mathfrak{o}_K/\mathfrak{p}, \quad x + p\mathbb{Z} \longmapsto x + \mathfrak{p}$$

が得られる．これによって, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を $\mathfrak{o}_K/\mathfrak{p}$ の部分体とみなすことができ, $\mathfrak{o}_K/\mathfrak{p}$ は $\mathbb{F}_p$ 上のベクトル空間になる．

[定理 16.2] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, p を素数とする．また, $\mathfrak{p}$ を単項イデアル $(p) = p\mathfrak{o}_K$ の素イデアル因子, f を $\mathfrak{p}$ の $K/\mathbb{Q}$ における相対次数とする．このとき, 体の拡大次数 $[\mathfrak{o}_K/\mathfrak{p} : \mathbb{F}_p]$ は f に一致する．

[証明] $\mathfrak{o}_K/\mathfrak{p}$ は $\mathbb{F}_p$ の拡大体なので, $\mathbb{F}_p$ 上のベクトル空間になる．$d = \dim_{\mathbb{F}_p} \mathfrak{o}_K/\mathfrak{p}$ とおくと, 体の拡大次数の意味から $[\mathfrak{o}_K/\mathfrak{p} : \mathbb{F}_p] = d$ である．また, ベクトル空間としての同型

$$\mathfrak{o}_K/\mathfrak{p} \cong \overbrace{\mathbb{F}_p \oplus \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p}^{d},$$

が成り立つ．$|\mathbb{F}_p| = p$ であるから,

$$|\mathfrak{o}_K/\mathfrak{p}| = p^d.$$

一方,

$$|\mathfrak{o}_K/\mathfrak{p}| = [\mathfrak{o}_K : \mathfrak{p}] = N_K\mathfrak{p} = p^f.$$

ゆえに, $f = d = [\mathfrak{o}_K/\mathfrak{p} : \mathbb{F}_p]$ となる． □

[定理 16.3] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a} \neq (0)$ を $\mathfrak{o}_K$ のイデアルとする．このとき, $\mathfrak{a}$ のノルム $N\mathfrak{a}$ が素数ならば, $\mathfrak{a}$ は素イデアルである．

[証明] もし仮に $\mathfrak{a}$ が素イデアルでないとすると, イデアル論の基本定理より,

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r, \quad r \geq 2$$

のように素イデアル分解できる．両辺のノルムをとると,

$$N\mathfrak{a} = N\mathfrak{p}_1 N\mathfrak{p}_2 \cdots N\mathfrak{p}_r.$$

ところが, 各 i について, $\mathfrak{p} \subsetneq \mathfrak{o}_K$ だから,

$$N\mathfrak{p} = [\mathfrak{o}_K : \mathfrak{p}] > 1.$$

これは $N\mathfrak{a}$ が素数であることに反する．したがって, $\mathfrak{a}$ は素イデアルである． □

[定理 16.4] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{p}$ を $\mathfrak{o}_K$ の素イデアルとする．このとき, $\mathfrak{p}$ の共役イデアル $\mathfrak{p}^\sigma$ もまた $\mathfrak{o}_K$ の素イデアルである．

[証明] $\mathfrak{p}^\sigma \subseteq \mathfrak{o}_K$ は明らかであるが, もし仮に $\mathfrak{p}^\sigma = \mathfrak{o}_K$ とすれば,

$$\mathfrak{p} = (\mathfrak{p}^\sigma)^\sigma = \mathfrak{o}_K^\sigma = \mathfrak{o}_K$$

となり矛盾が生じる. よって, $\mathfrak{p}^\sigma \neq \mathfrak{o}_K$. また, 任意の $x, y \in \mathfrak{o}_K$ に対して,

$$\begin{aligned} xy \in \mathfrak{p}^\sigma &\Longrightarrow x^\sigma y^\sigma = (xy)^\sigma \in (\mathfrak{p}^\sigma)^\sigma = \mathfrak{p} \\ &\Longrightarrow x^\sigma \in \mathfrak{p} \text{ または } y^\sigma \in \mathfrak{p} \\ &\Longrightarrow x = (x^\sigma)^\sigma \in \mathfrak{p}^\sigma \text{ または } y = (y^\sigma)^\sigma \in \mathfrak{p}^\sigma. \end{aligned}$$

ゆえに, $\mathfrak{p}^\sigma$ は $\mathfrak{o}_K$ の素イデアルである. □

(D1) の場合, $N\mathfrak{p}_1 = p$ より $(p) = (N\mathfrak{p}_1) = \mathfrak{p}_1\mathfrak{p}_1^\sigma$. 定理 16.4 より $\mathfrak{p}_1^\sigma$ もまた素イデアルだから, 分解の一意性により, $\mathfrak{p}_2 = \mathfrak{p}_1^\sigma$ となる. 同様に, $(p) = \mathfrak{p}_2\mathfrak{p}_2^\sigma$ から $\mathfrak{p}_1 = \mathfrak{p}_2^\sigma$ が得られる.

(D2) の場合, $\mathfrak{p}_1^\sigma = (p^\sigma) = (p) = \mathfrak{p}_1$ である.

(D3) の場合, $N\mathfrak{p}_1 = p$ より $(p) = (N\mathfrak{p}_1) = \mathfrak{p}_1\mathfrak{p}_1^\sigma$. 定理 16.4 より $\mathfrak{p}_1^\sigma$ もまた素イデアルだから, 分解の一意性により, $\mathfrak{p}_1 = \mathfrak{p}_1^\sigma$ となる.

以上の議論より, (D1), (D2), (D3) のそれぞれについて, p の K での素イデアル分解を共役イデアルによって表すと次のようになる:

(D1) $(p) = \mathfrak{p}\mathfrak{p}^\sigma$, $\mathfrak{p} \neq \mathfrak{p}^\sigma$, $N\mathfrak{p} = N\mathfrak{p}^\sigma = p$.
(D2) $(p) = \mathfrak{p} = \mathfrak{p}^\sigma$, $N\mathfrak{p} = p^2$.
(D3) $(p) = \mathfrak{p}^2 = \mathfrak{p}\mathfrak{p}^\sigma$, $\mathfrak{p} = \mathfrak{p}^\sigma$, $N\mathfrak{p} = p$.

[補題 16.5] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{p}$ を $\mathfrak{o}_K$ の素イデアル, $p \in \mathfrak{p}$ を素数とする.

(i) $N\mathfrak{p} = p$ のとき, ある $b \in \mathbb{Z}$ が存在して, p, $b + \omega$ は $\mathfrak{p}$ の標準的基底である.
(ii) $N\mathfrak{p} = p^2$ のとき, ある $b \in \mathbb{Z}$ が存在して, p, $b + p\omega$ は $\mathfrak{p}$ の標準的基底である.

[証明] a_0, $b_0 + c_0\omega$ を $\mathfrak{p}$ の標準的基底とする. 定理 16.1 より, p は $\mathfrak{p}$ に含まれる最小正の有理整数である. よって, $a_0 = p$. また, c_0 は $\mathbb{Z}$ において a_0 を割るから, $c_0 = 1$ または p である. $N\mathfrak{p} = a_0c_0$ より, $N\mathfrak{p} = p$ のとき $c_0 = 1$ となり, $N\mathfrak{p} = p^2$ のとき $c_0 = p$ となる. □

[補題 16.6] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする. ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする. $\mathfrak{o}_K$ を K の整数環, $1, \omega$ を K の標準的整数底, $b \in \mathbb{Q}$ とする.

$m \equiv 1 \pmod 4$ のとき,

$$\begin{aligned} N_K(b + \omega) &= b^2 + b + \frac{1 - m}{4} \\ &= \frac{1}{4}\big((2b + 1)^2 - m\big). \end{aligned}$$

$m \equiv 2, 3 \pmod 4$ のとき,

$$N_K(b+\omega) = b^2 - m.$$

[証明] $b \in \mathbb{Q}$ より $b^\sigma = b$ だから,

$$\begin{aligned} N_K(b+\omega) &= (b+\omega)(b+\omega)^\sigma \\ &= (b+\omega)(b+\omega^\sigma) \\ &= b^2 + (\omega+\omega^\sigma)b + \omega\omega^\sigma. \end{aligned}$$

$m \equiv 1 \pmod 4$ のとき,

$$\begin{aligned} \omega + \omega^\sigma &= \frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} = 1, \\ \omega\omega^\sigma &= \frac{1+\sqrt{m}}{2} \cdot \frac{1-\sqrt{m}}{2} = \frac{1-m}{4} \end{aligned}$$

より,

$$\begin{aligned} N_K(b+\omega) &= b^2 + b + \frac{1-m}{4} \\ &= \frac{1}{4}(4b^2 + 4b + 1 - m) \\ &= \frac{1}{4}\big((2b+1)^2 - m\big). \end{aligned}$$

$m \equiv 2, 3 \pmod 4$ のとき,

$$\begin{aligned} \omega + \omega^\sigma &= \sqrt{m} - \sqrt{m} = 0, \\ \omega\omega^\sigma &= \sqrt{m} \cdot (-\sqrt{m}) = -m \end{aligned}$$

より,

$$N_K(b+\omega) = b^2 - m.$$

□

[補題 16.7] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする. ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする. p を素数とし, $K/\mathbb{Q}$ において $(p) = \mathfrak{p}\mathfrak{p}^\sigma$ と素イデアル分解するものとする.

(i) $m \equiv 1 \pmod 4$ のとき, 合同方程式 $(2X+1)^2 \equiv m \pmod{4p}$ は有理整数解をもつ.

(ii) $m \equiv 2, 3 \pmod 4$ のとき, 合同方程式 $X^2 \equiv m \pmod p$ は有理整数解をもつ.

[証明] $(p) = \mathfrak{p}\mathfrak{p}^\sigma$ より, $N_K\mathfrak{p} = p$ である. 補題 16.5 より, ある $b \in \mathbb{Z}$ が存在して, p, $b+\omega$ は $\mathfrak{p}$ の標準的基底になる. 特に $\mathfrak{p} = \mathbb{Z}p + \mathbb{Z}(b+\omega)$ だから, 定理 10.8 より, $N_K(b+\omega) \in p\mathbb{Z}$.

$m \equiv 1 \pmod 4$ のとき, 補題 16.6 より,

$$4N_K(b+\omega) = (2b+1)^2 - m.$$

ゆえに,

$$(2b+1)^2 - m \in 4p\mathbb{Z}.$$

すなわち,

$$(2b+1)^2 \equiv m \pmod{4p}.$$

$m \equiv 2, 3 \pmod 4$ のとき, 補題 16.6 より,

$$N_K(b+\omega) = b^2 - m.$$

ゆえに,

$$b^2 \equiv m \pmod p.$$

□

[定理 16.8] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする. ただし, $m \neq 0, 1$ は平方因子を含まない有理整数とする. $\mathfrak{o}_K$ を K の整数環, p を奇素数とする.

(i) $p \nmid m$ のとき.

(a) $\left(\dfrac{m}{p}\right) = 1$ のとき, p は $K/\mathbb{Q}$ で完全分解する:

$$(p) = \mathfrak{p}\mathfrak{p}^\sigma, \quad \mathfrak{p} \neq \mathfrak{p}^\sigma, \quad N\mathfrak{p} = p.$$

(b) $\left(\dfrac{m}{p}\right) = -1$ のとき, p は $K/\mathbb{Q}$ で惰性する:

$$(p) = \mathfrak{p}, \quad N\mathfrak{p} = p^2.$$

(ii) $p \mid m$ のとき, p は $K/\mathbb{Q}$ で完全分岐する:

$$(p) = \mathfrak{p}^2, \quad N\mathfrak{p} = p.$$

[証明] (i) (a) $m \equiv 1 \pmod 4$ のとき. 仮定より, $a^2 \equiv m \pmod p$ かつ $\gcd(a, p) = 1$ なる $a \in \mathbb{Z}$ が存在する.

$$b = \begin{cases} a, & a \text{ が奇数のとき} \\ a+p, & a \text{ が偶数のとき} \end{cases}$$

とおくと, $b^2 \equiv m \pmod p$ かつ $\gcd(b, p) = 1$ である. p は奇素数なので, b は奇数である. そこで,

$$\mathfrak{p} = \mathbb{Z}p + \mathbb{Z}(b' + \omega), \quad b = 2b' + 1, \quad b' \in \mathbb{Z}$$

とおく. 補題 16.6 より,

$$N_K(b'+\omega) = \frac{(2b'+1)^2 - m}{4} = \frac{b^2 - m}{4}.$$

b は奇数だから $b^2 \equiv 1 \equiv m \pmod 4$ であり, $\gcd(4,\, p) = 1$ より $b^2 \equiv m \pmod{4p}$ が成り立つ. ゆえに,

$$N_K(b'+\omega) \in p\mathbb{Z}.$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, p, $b'+\omega$ は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p} = p$ なので,

$$(p) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^\sigma.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである. さらに, 定理 16.4 より, $\mathfrak{p}^\sigma$ も素イデアルである.

$$\mathfrak{p} = (p,\, b'+\omega), \quad \mathfrak{p}^\sigma = (p,\, b'+\omega^\sigma), \quad \omega + \omega^\sigma = 1$$

より,

$$\begin{aligned}
\mathfrak{p} + \mathfrak{p}^\sigma &= (p,\, b'+\omega,\, b'+\omega^\sigma) \\
&= (p,\, (b'+\omega) + (b'+\omega^\sigma),\, b'+\omega^\sigma) \\
&= (p,\, 2b'+1,\, b'+\omega^\sigma) \\
&= (p,\, b,\, b'+\omega^\sigma).
\end{aligned}$$

$\gcd(b,\, p) = 1$ より, ある x, $y \in \mathbb{Z}$ が存在して,

$$1 = bx + py \in (p,\, b,\, b'+\omega^\sigma) = \mathfrak{p} + \mathfrak{p}^\sigma.$$

ゆえに, $\mathfrak{p} + \mathfrak{p}^\sigma = \mathfrak{o}_K$. もし仮に $\mathfrak{p} = \mathfrak{p}^\sigma$ ならば $\mathfrak{p} + \mathfrak{p}^\sigma = \mathfrak{p} \neq \mathfrak{o}_K$ となり矛盾が生じる. したがって, $\mathfrak{p} \neq \mathfrak{p}^\sigma$ であり, p は $K/\mathbb{Q}$ で完全分解する.

$m \equiv 2,\, 3 \pmod 4$ のとき. 仮定より, $b^2 \equiv m \pmod p$ かつ $\gcd(b,\, p) = 1$ なる $b \in \mathbb{Z}$ が存在する.

$$\mathfrak{p} = \mathbb{Z}p + \mathbb{Z}(b+\omega)$$

とおく. 補題 16.6 と b の定め方より,

$$N_K(b+\omega) = b^2 - m \in p\mathbb{Z}.$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, p, $b+\omega$ は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p} = p$ なので,

$$(p) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^\sigma.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである. さらに, 定理 16.4 より, $\mathfrak{p}^\sigma$ も素イデアルである.

$$\mathfrak{p} = (p,\, b+\omega), \quad \mathfrak{p}^\sigma = (p,\, b+\omega^\sigma), \quad \omega + \omega^\sigma = 0$$

より,

$$\begin{aligned}\mathfrak{p}+\mathfrak{p}^{\sigma} &= (p,\, b+\omega,\, b+\omega^{\sigma})\\ &= (p,\, (b+\omega)+(b+\omega^{\sigma}),\, b+\omega^{\sigma})\\ &= (p,\, 2b,\, b+\omega^{\sigma}).\end{aligned}$$

$\gcd(2b,\, p)=1$ より, ある $x,\, y\in\mathbb{Z}$ が存在して,

$$1 = 2bx+py \in (p,\, 2b,\, b+\omega^{\sigma}) = \mathfrak{p}+\mathfrak{p}^{\sigma}.$$

ゆえに, $\mathfrak{p}+\mathfrak{p}^{\sigma}=\mathfrak{o}_K$. したがって, $\mathfrak{p}\neq\mathfrak{p}^{\sigma}$ であり, p は $K/\mathbb{Q}$ で完全分解する.

(i) (b)　仮定より合同方程式 $X^2\equiv m \pmod p$ は有理整数解をもたないので, 補題 16.7 より p は $K/\mathbb{Q}$ で完全分解も完全分岐もしない. したがって, 惰性する.

(ii)　$m\equiv 1 \pmod 4$ のとき. $b=(m-1)/2$ とおき,

$$\mathfrak{p} = \mathbb{Z}p+\mathbb{Z}(b+\omega)$$

とおく. 補題 16.6 と b の定め方より,

$$\begin{aligned}N_K(b+\omega) &= \frac{(2b+1)^2-m}{4} = \frac{m^2-m}{4}\\ &= \frac{m(m-1)}{4}\in p\mathbb{Z}.\end{aligned}$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, $p,\, b+\omega$ は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p}=p$ なので,

$$(p) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^{\sigma}.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである.

$$\begin{aligned}\mathfrak{p}^{\sigma} &= (p,\, b+\omega^{\sigma}) = \left(p,\, \frac{m-\sqrt{m}}{2}\right)\\ &= \left(p,\, \frac{\sqrt{m}-m}{2}\right) = \left(p,\, \frac{\sqrt{m}-m}{2}+m\right)\\ &= \left(p,\, \frac{m+\sqrt{m}}{2}\right) = (p,\, b+\omega)\\ &= \mathfrak{p}\end{aligned}$$

より, $(p)=\mathfrak{p}^2$. したがって, p は $K/\mathbb{Q}$ で完全分岐する.

$m\equiv 2,\, 3 \pmod 4$ のとき.

$$\mathfrak{p} = \mathbb{Z}p+\mathbb{Z}\omega$$

とおく. $\omega=\sqrt{m}$ より,

$$N_K\omega = -m\in p\mathbb{Z}.$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, p, ω は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p} = p$ なので,

$$(p) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^\sigma.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである.

$$\begin{aligned}\mathfrak{p}^\sigma &= (p,\, \omega^\sigma) = (p,\, -\sqrt{m}) \\ &= (p,\, \sqrt{m}) = (p,\, \omega) \\ &= \mathfrak{p}\end{aligned}$$

より, $(p) = \mathfrak{p}^2$. したがって, p は $K/\mathbb{Q}$ で完全分岐する. □

[定理 16.9] $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする. ただし, $m \neq 0,\, 1$ は平方因子を含まない有理整数とする. $\mathfrak{o}_K$ を K の整数環とする.

(i) $m \equiv 1 \pmod 8$ のとき, 2 は $K/\mathbb{Q}$ で完全分解する:

$$(2) = \mathfrak{p}\mathfrak{p}^\sigma, \quad \mathfrak{p} \neq \mathfrak{p}^\sigma, \quad N\mathfrak{p} = 2.$$

(ii) $m \equiv 5 \pmod 8$ のとき, 2 は $K/\mathbb{Q}$ で惰性する:

$$(2) = \mathfrak{p}, \quad N\mathfrak{p} = 4.$$

(iii) $m \equiv 2,\, 3 \pmod 4$ のとき, 2 は $K/\mathbb{Q}$ で完全分岐する:

$$(2) = \mathfrak{p}^2, \quad N\mathfrak{p} = 2.$$

[証明] $m \equiv 1 \pmod 8$ のとき.

$$\mathfrak{p} = \mathbb{Z} \cdot 2 + \mathbb{Z}\omega$$

とおく. $\omega = (1 + \sqrt{m})/2$ より,

$$N_K\omega = \frac{1 - m}{4} \in 2\mathbb{Z}.$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, 2, ω は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p} = 2$ なので,

$$(2) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^\sigma.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである. さらに, 定理 16.4 より, $\mathfrak{p}^\sigma$ も素イデアルである.

$$\mathfrak{p} = (2,\, \omega), \quad \mathfrak{p}^\sigma = (2,\, \omega^\sigma), \quad \omega + \omega^\sigma = 1$$

より,

$$\begin{aligned}\mathfrak{p} + \mathfrak{p}^\sigma &= (2,\, \omega,\, \omega^\sigma) = (2,\, \omega + \omega^\sigma,\, \omega^\sigma) \\ &= (2,\, 1,\, \omega^\sigma) = \mathfrak{o}_K.\end{aligned}$$

もし仮に $\mathfrak{p} = \mathfrak{p}^\sigma$ ならば $\mathfrak{p} + \mathfrak{p}^\sigma = \mathfrak{p} \neq \mathfrak{o}_K$ となり矛盾が生じる. したがって, $\mathfrak{p} \neq \mathfrak{p}^\sigma$ であり, 2 は $K/\mathbb{Q}$ で完全分解する.

$m \equiv 5 \pmod 8$ のとき. 合同方程式 $(2X+1)^2 \equiv 5 \pmod 8$ は有理整数解をもたないので, 補題 16.7 より, 2 は $K/\mathbb{Q}$ で完全分解も完全分岐もしない. したがって, 惰性する.

$m \equiv 2 \pmod 4$ のとき.

$$\mathfrak{p} = \mathbb{Z} \cdot 2 + \mathbb{Z}\omega$$

とおく. $\omega = \sqrt{m}$ より,

$$N_K\omega = -m \in 2\mathbb{Z}.$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, 2, ω は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p} = 2$ なので,

$$(2) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^\sigma.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである.

$$\begin{aligned}\mathfrak{p}^\sigma &= (2,\, \omega^\sigma) = (2,\, -\sqrt{m}) \\ &= (2,\, \sqrt{m}) = (2,\, \omega) \\ &= \mathfrak{p}\end{aligned}$$

より, $(2) = \mathfrak{p}^2$. したがって, 2 は $K/\mathbb{Q}$ で完全分岐する.

$m \equiv 3 \pmod 4$ のとき.

$$\mathfrak{p} = \mathbb{Z} \cdot 2 + \mathbb{Z}(1+\omega)$$

とおく. $\omega = \sqrt{m}$ より,

$$N_K(1+\omega) = (1+\sqrt{m})(1-\sqrt{m}) = 1 - m \in 2\mathbb{Z}.$$

定理 15.4 より, $\mathfrak{p}$ は $\mathfrak{o}_K$ のイデアルであり, 2, ω は $\mathfrak{p}$ の標準的基底である. $N\mathfrak{p} = 2$ なので,

$$(2) = (N\mathfrak{p}) = \mathfrak{p}\mathfrak{p}^\sigma.$$

また, 定理 16.3 より, $\mathfrak{p}$ は素イデアルである.

$$\begin{aligned}\mathfrak{p}^\sigma &= (2,\, 1+\omega^\sigma) = (2,\, 1-\sqrt{m}) \\ &= (2,\, \sqrt{m}-1) = (2,\, (\sqrt{m}-1)+2) \\ &= (2,\, 1+\sqrt{m}) = (2,\, 1+\omega) \\ &= \mathfrak{p}\end{aligned}$$

より, $(2) = \mathfrak{p}^2$. したがって, 2 は $K/\mathbb{Q}$ で完全分岐する. □

K を 2 次体とし, d_K を K の判別式とする. p が奇素数のとき,

$$\chi_{d_K}(p) = \begin{cases} \left(\dfrac{d_K}{p}\right), & p \nmid d_K \text{ のとき} \\ 0, & p \mid d_K \text{ のとき} \end{cases}$$

と定める. ただし, $\left(\frac{*}{*}\right)$ は Legendre 記号である. また, $p = 2$ のとき,

$$\chi_{d_K}(2) = \begin{cases} 1, & m \equiv 1 \pmod 8 \text{ のとき} \\ -1, & m \equiv 5 \pmod 8 \text{ のとき} \\ 0, & m \equiv 2, 3 \pmod 4 \text{ のとき} \end{cases}$$

と定める. $\chi_{d_K}(p)$ を **Kronecker 記号**という. $p = 2$ の場合も含めて, $\chi_{d_K}(p)$ は記号 $\left(\dfrac{d_K}{p}\right)$ で表されることがある. これも Kronecker 記号と呼ばれる.

Kronecker 記号を用いると, 定理 16.8, 定理 16.9 は次のように統一的に述べられる.

[定理 16.10] K を 2 次体, d_K を K の判別式, p を素数とする.

(i) $\chi_{d_K}(p) = 1$ のとき, p は $K/\mathbb{Q}$ で完全分解する.

(ii) $\chi_{d_K}(p) = -1$ のとき, p は $K/\mathbb{Q}$ で惰性する.

(iii) $\chi_{d_K}(p) = 0$ のとき, p は $K/\mathbb{Q}$ で完全分岐する.

[証明] 平方因子を含まない有理整数 $m \neq 0, 1$ によって $K = \mathbb{Q}(\sqrt{m})$ と表す.

p が奇素数かつ $p \nmid m$ のとき, Legendre 記号の性質より

$$\left(\frac{4m}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{m}{p}\right)$$

であるから,

$$\chi_{d_K}(p) = \left(\frac{d_K}{p}\right) = \left(\frac{m}{p}\right)$$

となる. よって, (i), (ii) が得られる.

残りの場合は, Kronecker 記号の定義から明らかである. □

d_K は, $m \equiv 1 \pmod 4$ のときは m であり, $m \equiv 2, 3 \pmod 4$ のときは $4m$ である. したがって, 任意の素数 p に対して,

$$\chi_{d_K}(p) = 0 \Longleftrightarrow p \mid d_K$$

が成り立つ. このことと定理 16.10 から, 次のいわゆる**判別定理**が得られる.

[定理 16.11] K を 2 次体, d_K を K の判別式, p を素数とする. このとき,

$$p \text{ が } K/\mathbb{Q} \text{ で完全分岐する} \Longleftrightarrow p \mid d_K$$

が成り立つ.

17　イデアル類群

K を 2 次体, $\mathfrak{o}_K$ を K の整数環とする.

$\mathfrak{o}_K$ の (0) でないイデアルの全体を $\mathcal{I}_K$ で表す. $\mathcal{I}_K$ における 2 項関係 $\sim$ を, $\mathfrak{a}$, $\mathfrak{b}$ に対して

$$\mathfrak{a} \sim \mathfrak{b} \Longleftrightarrow \text{ある } \gamma \in K,\ \gamma \neq 0 \text{ が存在して, } \mathfrak{a} = \gamma\mathfrak{b}$$

によって定める. $\mathfrak{a} \sim \mathfrak{b}$ が成り立つとき, $\mathfrak{a}$ と $\mathfrak{b}$ は**対等**であるという.

[定理 17.1] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{I}_K$ とする. このとき, 次の 2 つの条件は同値である.

(i) $\mathfrak{a}$ と $\mathfrak{b}$ は対等.

(ii) ある α, $\beta \in \mathfrak{o}_K$, $\alpha \neq 0$, $\beta \neq 0$ が存在して, $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

[証明] (i)⇒(ii)　$\mathfrak{a}$ と $\mathfrak{b}$ が対等であるとすると, ある $\gamma \in K$, $\gamma \neq 0$ が存在して, $\mathfrak{a} = \gamma\mathfrak{b}$. 一方, $\gamma \in \overline{\mathbb{Q}}$ だから, ある有理整数 $a > 0$ が存在して, $a\gamma \in \overline{\mathbb{Z}} \cap K = \mathfrak{o}_K$. このとき, $a\mathfrak{a} = a\gamma\mathfrak{b}$. そこで, $\alpha = a$, $\beta = a\gamma$ とおくと, $\alpha\mathfrak{a} = \beta\mathfrak{b}$, α, $\beta \in \mathfrak{o}_K$, $\alpha \neq 0$, さらに $\gamma \neq 0$ より $\beta \neq 0$.

(ii)⇒(i)　$\alpha \neq 0$ より, $\alpha\mathfrak{a} = \beta\mathfrak{b}$ の両辺に α^{-1} を掛けると, $\mathfrak{a} = \alpha^{-1}\beta\mathfrak{b}$. そこで, $\gamma = \alpha^{-1}\beta$ とおくと, $\mathfrak{a} = \gamma\mathfrak{b}$ となり, $\beta \neq 0$ より $\gamma \neq 0$. □

[定理 17.2] 対等であるという関係 $\sim$ は $\mathcal{I}_K$ における同値関係である.

[証明] $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \in \mathcal{I}_K$ とする.

(反射)　$\mathfrak{a} = 1 \cdot \mathfrak{a}$ より, $\mathfrak{a} \sim \mathfrak{a}$.

(対称)　$\mathfrak{a} \sim \mathfrak{b}$ とすると, ある $\gamma \in K$, $\gamma \neq 0$ が存在して, $\mathfrak{a} = \gamma\mathfrak{b}$. よって,

$$\gamma^{-1}\mathfrak{a} = \gamma^{-1}\gamma\mathfrak{b} = \mathfrak{b}.$$

ゆえに, $\mathfrak{b} \sim \mathfrak{a}$.

(推移)　$\mathfrak{a} \sim \mathfrak{b}$ かつ $\mathfrak{b} \sim \mathfrak{c}$ とする. $\mathfrak{a} \sim \mathfrak{b}$ より, ある $\gamma \in K$, $\gamma \neq 0$ が存在して, $\mathfrak{a} = \gamma\mathfrak{b}$. 同様に, $\mathfrak{b} \sim \mathfrak{c}$ より, ある $\gamma' \in K$, $\gamma' \neq 0$ が存在して, $\mathfrak{b} = \gamma'\mathfrak{c}$. ゆえに,

$$\mathfrak{a} = \gamma\mathfrak{b} = \gamma\gamma'\mathfrak{c}, \quad \gamma\gamma' \neq 0.$$

したがって, $\mathfrak{a} \sim \mathfrak{c}$. □

$\mathcal{I}_K$ の $\sim$ による商集合 $\mathcal{I}_K/\sim$ を $\mathcal{C}_K$ で表す. また, $\mathcal{C}_K$ に属する各同値類を**イデアル類**という. $\mathfrak{a} \in \mathcal{I}_K$ を代表元とするイデアル類を $[\mathfrak{a}]$ で表す:

$$[\mathfrak{a}] = \{\mathfrak{b} \in \mathcal{I}_K \mid \mathfrak{b} \sim \mathfrak{a}\}.$$

$\mathfrak{o}_K$ の (0) でない元から生成される単項イデアルの全体を $\mathcal{P}_K$ とおく.

[定理 17.3] $\mathcal{P}_K$ は 1 つのイデアル類になる. ただし, K を 2 次体とする.

[証明] 任意の単項イデアル $(\alpha) = \alpha\mathfrak{o}_K \neq (0)$ は明らかに $\mathfrak{o}_K$ と対等である. よって, $\mathcal{P}_K \subseteq [\mathfrak{o}_K]$.
また, $\mathfrak{a} \in \mathcal{I}_K$, $\mathfrak{a} \sim \mathfrak{o}_K$ とすると, ある $\gamma \in K$, $\gamma \neq 0$ が存在して,

$$\mathfrak{a} = \gamma\mathfrak{o}_K = (\gamma).$$

$\mathfrak{a} \subseteq \mathfrak{o}_K$ より,

$$\gamma \in (\gamma) \subseteq \mathfrak{o}_K.$$

ゆえに, $\mathfrak{a} \in \mathcal{P}_K$. したがって, $[\mathfrak{o}_K] \subseteq \mathcal{P}_K$. □

[定理 17.4] $\mathcal{C}_K$ は Abel 群になる. $\mathcal{C}_K$ を**イデアル類群**という.

[証明] まず, イデアル類の積を, 各 $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{I}_K$ に対して,

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{ab}]$$

によって定義する.

積が well-defined であること, すなわち, 代表元 $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{I}_K$ の選び方によらないことは次のようにして示される: $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{b}$, $\mathfrak{b}' \in \mathcal{I}_K$ とし, $\mathfrak{a} \sim \mathfrak{a}'$, $\mathfrak{b} \sim \mathfrak{b}'$ とする. $\mathfrak{a} \sim \mathfrak{a}'$ より, ある $\gamma_1 \in K$, $\gamma_1 \neq 0$ が存在して, $\mathfrak{a} = \gamma_1\mathfrak{a}'$. 同様に, $\mathfrak{b} \sim \mathfrak{b}'$ より, ある $\gamma_2 \in K$, $\gamma_2 \neq 0$ が存在して, $\mathfrak{b} = \gamma_2\mathfrak{b}'$. ゆえに, $\mathfrak{ab} = \gamma_1\gamma_2\mathfrak{a}'\mathfrak{b}'$, $\gamma_1\gamma_2 \neq 0$. したがって, $\mathfrak{ab} \sim \mathfrak{a}'\mathfrak{b}'$.

任意の $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \in \mathcal{I}_K$ に対して, $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ より,

$$\begin{aligned}([\mathfrak{a}][\mathfrak{b}])[\mathfrak{c}] &= ([\mathfrak{ab}])[\mathfrak{c}] = [(\mathfrak{ab})\mathfrak{c}] \\ &= [\mathfrak{a}(\mathfrak{bc})] = [\mathfrak{a}][\mathfrak{bc}] \\ &= [\mathfrak{a}]([\mathfrak{b}][\mathfrak{c}]).\end{aligned}$$

よって, 積は結合法則を満たす. また, $\mathfrak{ab} = \mathfrak{ba}$ より,

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{ab}] = [\mathfrak{ba}] = [\mathfrak{b}][\mathfrak{a}].$$

よって, 積は可換である.

単位元は $[\mathfrak{o}_K]$ である. 実際, 任意の $\mathfrak{a} \in \mathcal{I}_K$ より,

$$[\mathfrak{a}][\mathfrak{o}_K] = [\mathfrak{a}\mathfrak{o}_K] = [\mathfrak{a}].$$

任意の $\mathfrak{a} \in \mathcal{I}_K$ に対して, $\mathfrak{a}\mathfrak{a}^\sigma = (N\mathfrak{a})$ より,

$$[\mathfrak{a}][\mathfrak{a}^\sigma] = [\mathfrak{a}\mathfrak{a}^\sigma] = [(N\mathfrak{a})] = [\mathfrak{o}_K].$$

したがって, $[\mathfrak{a}]$ の逆元は存在し, それは $[\mathfrak{a}^\sigma]$ である.

以上より, $\mathcal{C}_K$ が Abel 群になることが証明された. □

2 次体 K の (0) でない分数イデアルの全体を $\mathcal{I}_K^*$ で表す. また, K の (0) でない単項分数イデアルの全体を $\mathcal{P}_K^*$ で表す.

[定理 17.5] K を 2 次体とする.

(i) $\mathcal{I}_K^*$ は Abel 群になる.
(ii) $\mathcal{P}_K^*$ は $\mathcal{I}_K^*$ の部分群になる.

[証明] (i) $\mathcal{I}_K^*$ の積をイデアルの積で定義する. そうすると, 結合法則, 交換法則が成り立つことは明らかである. 単位元は K の整数環 $\mathfrak{o}_K$ である. 定理 11.8 より, 各 $\mathfrak{a} \in \mathcal{I}_K^*$ に対して, その逆元は逆イデアル $\mathfrak{a}^{-1}$ である.

(ii) $\mathfrak{o}_K \in \mathcal{P}_K^*$ より, $\mathcal{P}_K^*$ は空集合でない. さらに, 任意の $(\alpha), (\beta) \in \mathcal{P}_K^*$ に対して,

$$(\alpha)(\beta)^{-1} = (\alpha)(\beta^{-1}) = (\alpha\beta^{-1}) \in \mathcal{P}_K^*.$$

ゆえに, $\mathcal{P}_K^*$ は $\mathcal{I}_K^*$ の部分群である. □

$\mathcal{I}_K^*$ の $\mathcal{P}_K^*$ による剰余群 $\mathcal{I}_K^*/\mathcal{P}_K^*$ を $\mathcal{C}_K^*$ で表す.

[定理 17.6] $\mathcal{P}_K^* \cap \mathcal{I}_K = \mathcal{P}_K$. ただし, K を 2 次体とする.

[証明] $\mathfrak{a} \in \mathcal{P}_K^* \cap \mathcal{I}_K$ とする. $\mathfrak{a} \in \mathcal{P}_K^*$ より, ある $\alpha \in K$, $\alpha \neq 0$ が存在して, $\mathfrak{a} = (\alpha)$ となる. 一方, $\mathfrak{a} \in \mathcal{I}_K$ より, $\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルなので, $(\alpha) \subseteq \mathfrak{o}_K$ である. $\alpha \in (\alpha)$ より, $\alpha \in \mathfrak{o}_K$. したがって, $\mathfrak{a} = (\alpha) \in \mathcal{P}_K$ となり, $\mathcal{P}_K^* \cap \mathcal{I}_K \subseteq \mathcal{P}_K$. 逆の包含関係は明らか. □

[定理 17.7] K を 2 次体とする. このとき, $\mathcal{C}_K^*$ は $\mathcal{C}_K$ に同型である. 特に, $|\mathcal{C}_K^*| = |\mathcal{C}_K|$ が成り立つ. $\mathcal{C}_K^*$ のこともまた**イデアル類群**という.

[証明] 写像

$$f : \mathcal{I}_K \longrightarrow \mathcal{I}_K^*/\mathcal{P}_K^*, \quad \mathfrak{a} \longmapsto \mathfrak{a}\mathcal{P}_K^*$$

を考える. $\mathfrak{a}, \mathfrak{a}' \in \mathcal{I}_K^*$ に対して,

$$f(\mathfrak{a}\mathfrak{a}') = \mathfrak{a}\mathfrak{a}'\mathcal{P}_K^* = (\mathfrak{a}\mathcal{P}_K^*)(\mathfrak{a}'\mathcal{P}_K^*) = f(\mathfrak{a})f(\mathfrak{a}')$$

より, f は準同型写像である. また, 任意の分数イデアル $\mathfrak{b}$ に対して, ある $c \in O_K$, $c \neq 0$ が存在して, $c\mathfrak{b} \in \mathcal{I}_K$ となる. このとき,

$$f(c\mathfrak{b}) = c\mathfrak{b}\mathcal{P}_K^* = \mathfrak{b}\mathcal{P}_K^*.$$

ゆえに, f は全射である. さらに,

$$\begin{aligned}\mathfrak{a} \in \operatorname{Ker} f &\iff \mathfrak{a} \in \mathcal{I}_K,\ f(\mathfrak{a}) = \mathcal{P}_K^* \\ &\iff \mathfrak{a} \in \mathcal{I}_K,\ \mathfrak{a}\mathcal{P}_K^* = \mathcal{P}_K^* \\ &\iff \mathfrak{a} \in \mathcal{I}_K,\ \mathfrak{a} \in \mathcal{P}_K^* \\ &\iff \mathfrak{a} \in \mathcal{P}_K^* \cap \mathcal{I}_K.\end{aligned}$$

定理 17.6 より $\mathcal{P}_K^* \cap \mathcal{I}_K = \mathcal{P}_K$ だから, $\operatorname{Ker} f = \mathcal{P}_K$. 準同型定理より,

$$\mathcal{I}_K/\mathcal{P}_K \cong \mathcal{I}_K^*/\mathcal{P}_K^*, \quad [\mathfrak{a}] \longmapsto \mathfrak{a}\mathcal{P}_K^*$$

が得られる. □

[定理 17.8] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, $\mathfrak{a}$, $\mathfrak{m} \in \mathcal{I}_K$ とする. このとき, ある $\mathfrak{b} \in \mathcal{I}_K$ が存在して, $\mathfrak{a}\mathfrak{b} \sim \mathfrak{o}_K$ かつ $(\mathfrak{b}, \mathfrak{m}) = 1$ が成り立つ.

[証明] $\mathfrak{c} = \mathfrak{a}\mathfrak{m}$ とすると, $\mathfrak{c} \subseteq \mathfrak{a}$ である. 定理 14.7 より, ある $\mu \in \mathfrak{a}$ が存在して, $\mathfrak{a} = \mathfrak{c} + (\mu)$ となる. $(\mu) \subseteq \mathfrak{a}$ から, ある $\mathfrak{b} \in \mathcal{I}_K$ が存在して, $(\mu) = \mathfrak{a}\mathfrak{b}$. したがって, $\mathfrak{a}\mathfrak{b} \sim \mathfrak{o}_K$. さらに,

$$\mathfrak{a} = \mathfrak{c} + (\mu) = \mathfrak{a}\mathfrak{m} + \mathfrak{a}\mathfrak{b} = \mathfrak{a}(\mathfrak{m} + \mathfrak{b}).$$

$\mathfrak{a} \neq (0)$ より, $\mathfrak{o}_K = \mathfrak{m} + \mathfrak{b}$ となる. すなわち, $(\mathfrak{b}, \mathfrak{m}) = 1$. □

[定理 17.9] K を 2 次体, $C > 0$ を実数とする. このとき, $\mathfrak{a} \in \mathcal{I}_K$ で $N\mathfrak{a} \leq C$ を満たすものは有限個しかない.

[証明] まず, $N\mathfrak{a} = 1$ であるような $\mathfrak{o}_K$ のイデアルは $\mathfrak{o}_K$ のみである.
$\mathfrak{a} \neq \mathfrak{o}_K$ とする. イデアル論の基本定理により,

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

と素イデアルの積で表される. ノルムをとると,

$$N\mathfrak{a} = N\mathfrak{p}_1 N\mathfrak{p}_2 \cdots N\mathfrak{p}_r.$$

$N\mathfrak{a} \leq C$ より,

$$N\mathfrak{p}_1 N\mathfrak{p}_2 \cdots N\mathfrak{p}_r \leq C.$$

よって, 各 i について $N\mathfrak{p}_i \leq C$. 一方, $N\mathfrak{p}_i = [\mathfrak{o}_K : \mathfrak{p}] \geq 2$ であるから,

$$2^r \leq N\mathfrak{p}_1 N\mathfrak{p}_2 \cdots N\mathfrak{p}_r \leq C.$$

よって, $r \leq \log_2 C$ となる. ゆえに, $\mathfrak{a}$ は $\lfloor \log_2 C \rfloor$ 個以下の素イデアルの積である. したがって, $N\mathfrak{p} \leq C$ となる素イデアル $\mathfrak{p}$ が有限個しかなことを示せばよい.

$\mathfrak{p}$ を $N\mathfrak{p} \leq C$ なる素イデアルとする. 定理 16.1 より, ある素数 p が存在して, $N\mathfrak{p} = p$ または p^2. いずれにせよ, $p \leq C$ である. さらに, $\mathfrak{p} \mid (p)$. すなわち, $\mathfrak{p}$ は p の K における素イデアル分解に現れる. C 以下の素数は高々C 個であり, 素数の K における素イデアル分解に現れる素イデアルは高々2 個で, しかも 1 つの素イデアルが 2 つ以上の異なる素数の素イデアル分解に現われることはないから, $\mathfrak{p}$ の個数は $2C$ 個以下である.

以上より, $\mathfrak{a}$ の個数は $(2C)^{\lfloor \log_2 C \rfloor} + 1$ を超えない. したがって, 有限個である. □

[定理 17.10] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, d_K を K の判別式とする. このとき, K のイデアル類群 $\mathcal{C}_K$ に属する任意のイデアル類は, その代表元として $N\mathfrak{a} \leq M_K$ を満たす原始イデアル $\mathfrak{a} \in \mathcal{I}_K$ を選べる. ただし,

$$M'_K = \begin{cases} \sqrt{d_K}/2, & K \text{ が実 2 次体のとき} \\ \sqrt{-d_K/3}, & K \text{ が虚 2 次体のとき} \end{cases}$$

とおく.

[証明] イデアル類を任意にとり, その類に属するイデアルのうちノルムが最小のものを $\mathfrak{a}$ とする. 定理 15.5 より, ある有理整数 $c_0 > 0$ と原始イデアル $\mathfrak{a}_0$ が存在して,

$$\mathfrak{a} = c_0 \mathfrak{a}_0.$$

両辺のノルムをとると, 定理 11.7 より,

$$N\mathfrak{a} = c_0^2 \cdot N\mathfrak{a}_0.$$

よって, $N\mathfrak{a}_0 \leq N\mathfrak{a}$. ところが, $\mathfrak{a} \sim \mathfrak{a}_0$ であるから, $N\mathfrak{a}$ の最小性より $N\mathfrak{a} = N\mathfrak{a}_0$ でなければならない. ゆえに, $c_0 = 1$. したがって, $\mathfrak{a} = \mathfrak{a}_0$ となり, $\mathfrak{a}$ は原始イデアルである. その標準的基底は a, $r + \omega$ なる形であり, $N\mathfrak{a} = a$ である. 定理 10.7 より,

$$-\frac{a}{2} \leq r < \frac{a}{2} \tag{21}$$

としてよい. 定理 10.8 より $N_K(r + \omega) \in a\mathbb{Z}$ であるから,

$$N_K(r + \omega) = ac, \quad c \in \mathbb{Z} \tag{22}$$

とおく. $(r + \omega) \subseteq \mathfrak{a}$ だから, $\mathfrak{a} \mid (r + \omega)$. すなわち, ある $\mathfrak{b} \in \mathcal{I}_K$ が存在して,

$$(r + \omega) = \mathfrak{a}\mathfrak{b}.$$

ノルムをとると,

$$N(r + \omega) = N\mathfrak{a} N\mathfrak{b}.$$

また,

$$N(r+\omega) = |N_K(r+\omega)| = |ac| = a|c|.$$

ゆえに,

$$N\mathfrak{a}N\mathfrak{b} = a|c|.$$

これより, $N\mathfrak{b} = |c|$ が得られる. よって,

$$\mathfrak{b}\mathfrak{b}^\sigma = (N\mathfrak{b}) = (c).$$

ゆえに,

$$(r+\omega)\mathfrak{b}^\sigma = \mathfrak{a}\mathfrak{b}\mathfrak{b}^\sigma = \mathfrak{a}(c) = c\mathfrak{a}.$$

したがって, $\mathfrak{a} \sim \mathfrak{b}^\sigma$ である. $N\mathfrak{a}$ の最小性より,

$$N\mathfrak{a} \leq N\mathfrak{b}^\sigma = N\mathfrak{b}.$$

すなわち, $a \leq |c|$. 一方,

$$b = \mathrm{Tr}_K(r+\omega) = (r+\omega) + (r+\omega^\sigma) \tag{23}$$

とおくと, 平方因子を含まない有理整数 $m \neq 0, 1$ によって $K = \mathbb{Q}(\sqrt{m})$ と表せば, $m \equiv 1 \pmod 4$ のときは $\omega + \omega^\sigma = 1$ より $b = 2r+1$ となり, $m \equiv 3 \pmod 4$ のときは $\omega + \omega^\sigma = 0$ より $b = 2r$ となる. よって, いずれの場合も, (21) より $|b| \leq a$. したがって,

$$|b| \leq a \leq |c|. \tag{24}$$

さて, $r+\omega$ は 2 次方程式

$$X^2 - (\mathrm{Tr}_K(r+\omega))X + N_K(r+\omega) = 0$$

の解だから, 式 (22), 式 (23), 定理 6.3, 定理 6.6 より,

$$\begin{aligned} b^2 - 4ac &= \mathrm{Tr}_K(r+\omega)^2 - 4 \cdot N_K(r+\omega) \\ &= d_K(r+\omega) = d_K. \end{aligned}$$

K が実 2 次体のとき, すなわち $m > 0$ のとき, $d_K > 0$ であるから, (24) より

$$4ac < d_K + 4ac = b^2 \leq a|c|.$$

よって, $4c < |c|$. もし仮に $c \geq 0$ とすると, $4c < c$ となって矛盾が生じる. ゆえに, $c < 0$. したがって,

$$d_K = b^2 - 4ac = b^2 + 4a|c| \geq 4a^2$$

となり,

$$N\mathfrak{a} = a \leq \frac{\sqrt{d_K}}{2} = M'_K$$

が成り立つ.

K が虚 2 次体のとき, すなわち $m<0$ のとき, $d_K=b^2-4ac<0$ である. $a>0$, $b^2\geq 0$ より, $c>0$ となる. (24) より,

$$4a^2\leq 4ac=b^2-d_K\leq a^2-d_K.$$

よって,

$$3a^2\leq -d_K.$$

ゆえに,

$$N\mathfrak{a}=a\leq\sqrt{\frac{-d_K}{3}}=M'_K$$

が成り立つ. □

[注意 17.1] 定理 17.10 の M'_K は, Minkowski の定数と呼ばれているものと少し異なる. n 次代数体 K に対して,

$$M_K=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$$

を **Minkowski の定数**という. ただし, $2r_2$ は虚の共役体の個数, d_K は K の判別式である. K が実 2 次体のときは, $r_2=0$ なので,

$$M_K=\frac{2!}{2^2}\sqrt{d_K}=\frac{\sqrt{d_K}}{2}$$

となり, M'_K と一致する. 一方, K が虚 2 次体のときは, $r_2=1$ なので,

$$M_K=\frac{2!}{2^2}\cdot\frac{4}{\pi}\cdot\sqrt{-d_K}=\frac{2\sqrt{-d_K}}{\pi}$$

となる. $2/\pi=0.6366\cdots$, $1/\sqrt{3}=0.5773\cdots$ だから, $M'_K<M_K$ である.

[例 17.1] $\mathfrak{o}_K$ を 2 次体 K の整数環とする. 単項イデアルの類 $\mathcal{P}_K$ に属するイデアルでノルムが最小のものは $\mathfrak{o}_K$ である. $\mathfrak{o}_K$ は K の標準的整数底 $1,\omega$ を基底とする原始イデアルである.

[定理 17.11] 2 次体 K のイデアル類群 $\mathcal{C}_K$ は有限 Abel 群である. $\mathcal{C}_K$ に属するイデアル類の個数, すなわち $|\mathcal{C}_K|$ を K の**類数**といい, h_K で表す.

[証明] Abel 群であることは定理 17.4 においてすでに示した.

ノルムが M'_K 以下のイデアルからなる I_K の部分集合を Ω とする. Ω に属する任意のイデアルは, 必ずいずれかのイデアル類に属し, 2 つ以上の異なるイデアル類には属さない. このことは, Ω から $\mathcal{C}_K$ への写像が定まることを意味する. 定理 17.9 より, ノルムが M'_K 以下のイデアルは有限個しかない. すなわち, Ω は有限集合である. 定理 17.10 より, 任意のイデアル類はノルムが M'_K 以下のイデアルを代表元として選べる. このことは, Ω から $\mathcal{C}_K$ への全射が存在することを意味する. ゆえに, $\mathcal{C}_K$ もまた有限集合である. □

[定理 17.12] K を 2 次体, h_K を K の類数とする. このとき, 任意の K の分数イデアル $\mathfrak{a}$ に対して, $\mathfrak{a}^{h_K}$ は単項イデアルである.

[証明] $\mathfrak{a}$ を K の分数イデアルとする. $\mathfrak{a}=(0)$ のときは明らかなので, $\mathfrak{a}\neq(0)$ のときを考える.

一般に, 有限群 G の元の位数は, G の位数の約数である. 定理 17.7, 定理 17.11 より, イデアル類群 $\mathcal{C}_K^*$ は有限群であり, h_K は $\mathcal{C}_K^*$ の位数である. ゆえに, 任意の $\mathfrak{a}\in\mathcal{I}_K^*$ に対して,

$$\mathfrak{a}^{h_K}\mathcal{P}_K^* = (\mathfrak{a}\mathcal{P}_K^*)^{h_K} = \mathcal{P}_K^*.$$

よって, $\mathfrak{a}^{h_K}\in\mathcal{P}_K^*$. すなわち, $\mathfrak{a}^{h_K}$ は単項イデアルである. □

[定理 17.13] K を 2 次体, $\mathfrak{o}_K$ を K の整数環, h_K を K の類数とする. このとき, 次の 3 つの条件は同値である.

(i) $h_K=1$.
(ii) 任意の K の分数イデアル $\mathfrak{a}$ は単項イデアル.
(iii) $\mathfrak{o}_K$ は単項イデアル整域.

[証明] h_K の定義と定理 17.7 より,

$$\begin{aligned} h_K=1 &\iff |\mathcal{C}_K|=1 \iff \mathcal{I}_K=\mathcal{P}_K \\ &\iff |\mathcal{C}_K^*|=1 \iff \mathcal{I}_K^*=\mathcal{P}_K^*. \end{aligned}$$

したがって, (i), (ii), (iii) は同値である.

以下, 参考までに, (iii) から $|\mathcal{C}_K^*|=1$ を直接的に導く証明を述べる.

$\mathfrak{a}\in\mathcal{I}_K^*$ とする. 分数イデアルの定義より, ある $c\in\mathfrak{o}_K$, $c\neq0$ が存在して, $c\mathfrak{a}$ は $\mathfrak{o}_K$ のイデアルになる. 仮定より, $c\mathfrak{a}$ は単項イデアルである. $c\mathfrak{a}=(\alpha)$, $\alpha\in\mathfrak{o}_K$, $\alpha\neq0$ とおけば, $\mathfrak{a}=(c^{-1}\alpha)$ となる. よって, $\mathfrak{a}\in\mathcal{P}_K^*$. ゆえに, $\mathcal{I}_K^*\subseteq\mathcal{P}_K^*$ となり, 逆の包含関係は明らかだから, $\mathcal{I}_K^*=\mathcal{P}_K^*$. したがって, $h_K=1$. □

2 次体 K の類数 h_K を, 定理 17.10 に基づいて計算する手順は以下のとおりである.

1. イデアル $\mathfrak{a}\in\mathcal{I}_K$ で $N\mathfrak{a}\leq M_K'$ を満たすものをすべて求める.
2. 1. で求めたイデアルが互いに対等かどうかを調べる.
3. 対等でないものの個数が h_K である.

ここで, 手順 1. は, $p\leq M_K'$ なる素数 p の K での素イデアル分解に現れる素イデアルを求めることに帰着する. なぜなら, $\mathfrak{a}\in\mathcal{I}_K$ で $2\leq N\mathfrak{a}\leq M_K'$ を満たすものは, そのような素イデアルの積として表されるからである (定理 17.9 の証明). そのうち, p が $K/\mathbb{Q}$ で惰性して (p) が $\mathfrak{o}_K$ の素イデアルである場合は $(p)\in\mathcal{P}_K$ が最初から分かっている. したがって, $K/\mathbb{Q}$ で惰性しない素数 p の素イデアル分解を考えれば十分である.

[例 17.2] $K=\mathbb{Q}(\sqrt{m})$, $m=5$ とする. $m\equiv 1 \pmod 4$ より, $d_K=5$. このとき,

$$M'_K=\frac{\sqrt{5}}{2}=1.1180\cdots<2.$$

$\mathcal{I}_K$ に属するイデアルでノルムが 1 以下のものは $\mathfrak{o}_K$ のみであるから, $\mathbb{Q}(\sqrt{5})$ の類数は 1 である.

[例 17.3] $K=\mathbb{Q}(\sqrt{m})$, $m=-5$ とする. $m\equiv 3 \pmod 4$ より, $d_K=4\cdot(-5)=-20$. このとき,

$$M'_K=\sqrt{\frac{20}{3}}=2.5819\cdots<3.$$

1, ω を K の標準的整数底とすると, $\omega=\sqrt{-5}$.

2 の K での分解について考える. $m\equiv 3 \pmod 4$ より, 2 は $K/\mathbb{Q}$ で完全分岐する.

$$\mathfrak{p}=\mathbb{Z}\cdot 2+\mathbb{Z}(1+\omega)$$

とおくと, $\mathfrak{p}$ は素イデアルであり,

$$(2)=\mathfrak{p}^2,\quad N\mathfrak{p}=2$$

が成り立つ.

もし仮に $\mathfrak{p}$ が単項イデアルならば,

$$\mathfrak{p}=(a+b\omega),\quad a,\,b\in\mathbb{Z}$$

と表せる. すると,

$$2=N\mathfrak{p}=|N_K(a+b\omega)|=a^2+5b^2.$$

ところが, この方程式の解になる有理整数の組 $(a,\,b)$ は存在しない. 実際, そのような $(a,\,b)$ が存在すれば, $a^2\equiv 2 \pmod 5$ が成り立たなければならないが, 2 は $\bmod 5$ で平方非剰余なので, 不可能である. よって, $\mathfrak{p}$ は単項イデアルではない. すなわち, $\mathfrak{p}\not\sim\mathfrak{o}_K$.

$\mathcal{I}_K$ に属するイデアルでノルムが 2 以下のものは $\mathfrak{o}_K$, $\mathfrak{p}$ のみであるから, $\mathbb{Q}(\sqrt{-5})$ の類数は 2 である.

参考文献

[1] 小野孝: 数論序説, 裳華房, 1987.

[2] 河田敬義: 数論—古典数論から類体論へ, 岩波書店, 1992.

[3] 木田雅成: 数理・情報系のための整数論講義, サイエンス社, 2007.

[4] 高木貞治: 初等整数論講義 第 2 版, 岩波書店, 1971.

[5] 武隈良一: 2 次体の整数論, 槙書店, 1966.

[6] 藤崎源二郎: 代数的整数論入門 (上), 裳華房, 1975.

[7] 山本芳彦: 数論入門, 岩波書店, 2003.

索 引