1 $\mathbb{Q}(\sqrt{-3})$ の整数

1.1 $\mathbb{Q}(\sqrt{-3})$ の整数

$a + b\sqrt{-3}$, a, $b \in \mathbb{Q}$ なる形の複素数の全体を $\mathbb{Q}(\sqrt{-3})$ とおく:

$$\mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}$$

定義より明らかに $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-3})$ である. 複素数の性質より, 任意の a, b, c, $d \in \mathbb{Q}$ に対して,

$$\begin{aligned} a + b\sqrt{-3} = c + d\sqrt{-3} &\iff a + (b\sqrt{3})\sqrt{-1} = c + (d\sqrt{3})\sqrt{-1} \\ &\iff a = c,\ b\sqrt{3} = d\sqrt{3} \\ &\iff a = c,\ b = d \end{aligned}$$

が成り立つ.

[定理 1.1] $\mathbb{Q}(\sqrt{-3})$ は $\mathbb{C}$ の部分体である.

[証明] $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-3})$ より, $\mathbb{Q}(\sqrt{-3})$ は空集合でない.
α, $\beta \in \mathbb{Q}(\sqrt{-3})$ とし,

$$\begin{aligned} \alpha &= a + b\sqrt{-3}, \quad a,\ b \in \mathbb{Q}, \\ \beta &= c + d\sqrt{-3}, \quad c,\ d \in \mathbb{Q} \end{aligned}$$

とおくと,

$$\begin{aligned} \alpha - \beta &= (a + b\sqrt{-3}) + (c + d\sqrt{-3}) \\ &= (a - c) + (b - d)\sqrt{-3} \in \mathbb{Q}(\sqrt{-3}), \\ \alpha\beta &= (a + b\sqrt{-3})(c + d\sqrt{-3}) \\ &= (ac - bd) + (ad + bc)\sqrt{-3} \in \mathbb{Q}(\sqrt{-3}). \end{aligned}$$

したがって, $\mathbb{Q}(\sqrt{-3})$ は $\mathbb{C}$ の部分環である.
$\alpha = a + b\sqrt{-3} \neq 0$ のとき, $a \neq 0$ または $b \neq 0$ だから, $a^2 + 3b^2 \neq 0$. よって,

$$\begin{aligned} \alpha^{-1} = \frac{1}{a + b\sqrt{-3}} &= \frac{a - b\sqrt{-3}}{(a + b\sqrt{-3})(a - b\sqrt{-3})} \\ &= \frac{a}{a^2 + 3b^2} - \frac{b}{a^2 + 3b^2}\sqrt{-3} \in \mathbb{Q}(\sqrt{-3}). \end{aligned}$$

ゆえに, α は $\mathbb{Q}(\sqrt{-3})$ において逆元をもつ. したがって, $\mathbb{Q}(\sqrt{-3})$ は体である. $\square$

以下, この文書の最後まで, $K = \mathbb{Q}(\sqrt{-3})$ とする. さらに, 1 の原始 3 乗根を ζ で表す:

$$\zeta = \frac{-1+\sqrt{-3}}{2}.$$

実際に計算してみれば, 以下のことは直ちに確認できる:

- $\zeta^3 = 1$.
- $\zeta^2 + \zeta + 1 = 0$.
- $\zeta^\sigma = (-1-\sqrt{-3})/2 = \zeta^2$.
- $\zeta + \zeta^\sigma = -1$.
- $\zeta\zeta^\sigma = 1$.

さらに, $\mathbb{Q}(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}\}$ とおくと, $K = \mathbb{Q}(\zeta)$ が成り立つ. 実際, 任意の $a, b \in \mathbb{Q}$ に対して

$$a + b\zeta = a + b \cdot \frac{-1+\sqrt{-3}}{2} = \frac{2a-b}{2} + \frac{b}{2}\cdot\sqrt{-3},$$
$$a + b\sqrt{-3} = a + b + 2b \cdot \frac{-1+\sqrt{-3}}{2} = a + b + 2b\zeta$$

が成り立つことから, $\mathbb{Q}(\zeta) \subseteq K$ と $K \subseteq \mathbb{Q}(\zeta)$ の両方が導かれる.

任意の $a, b, c, d \in \mathbb{Q}$ に対して,

$$\begin{aligned} a + b\zeta = c + d\zeta &\iff \frac{2a-b}{2} + \frac{b}{2}\cdot\sqrt{-3} = \frac{2c-d}{2} + \frac{d}{2}\cdot\sqrt{-3} \\ &\iff 2a - b = 2c - d,\ b = d \\ &\iff a = c,\ b = d \end{aligned}$$

が成り立つ.

K の元 $\alpha = a + b\sqrt{-3}$, $a, b \in \mathbb{Q}$ に対して, α の複素共役のことを K における α の**共役**といい, α^σ で表す: $\alpha^\sigma = x - y\sqrt{-3}$. また, α とその K における共役との積

$$\begin{aligned} \alpha\alpha^\sigma &= (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2 \\ &= |\alpha|^2 \end{aligned}$$

を α の**ノルム**といい, $N_K\alpha$ で表す. 定義より, $N_K\alpha$ は常に負でない有理数であり, $N_K\alpha = 0$ となるのは $\alpha = 0$ のときだけである.

また, K の元を $a + b\zeta$, $a, b \in \mathbb{Q}$ の形で表したときには,

$$\begin{aligned} N(a + b\zeta) &= (a + b\zeta)(a + b\zeta^\sigma) \\ &= a^2 + ab(\zeta + \zeta^\sigma) + b^2\zeta\zeta^\sigma \\ &= a^2 - ab + b^2 \end{aligned}$$

となる.

[定理 1.2] $\alpha, \beta \in K$ とする．このとき,

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

が成り立つ.

[証明] $N_K(\alpha\beta) = \alpha\beta(\alpha\beta)^\sigma = \alpha\beta\alpha^\sigma\beta^\sigma = \alpha\alpha^\sigma\beta\beta^\sigma = N_K\alpha N_K\beta.$ $\square$

$a + b\zeta$, $a, b \in \mathbb{Z}$ なる形の複素数を K の**整数**という．これに対して, 従来の整数, すなわち $\mathbb{Z}$ の元のことを**有理整数**と呼ぶことにする.

K の整数の全体を $\mathbb{Z}[\zeta]$ で表す:

$$\mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}.$$

定義から明らかに, $\mathbb{Z} \subseteq \mathbb{Z}[\zeta]$ である．また, 任意の $a, b \in \mathbb{Z}$ に対して $N(a + b\zeta) = a^2 - ab + b^2 \in \mathbb{Z}$ であるから, K の整数のノルムは常に有理整数になる.

$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ とおくと, 任意の $a, b \in \mathbb{Z}$ に対して $a + b\sqrt{-3} = a - b + 2b\zeta$ が成り立つから $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\zeta]$ であることはいえるが, $\zeta \notin \mathbb{Z}[\sqrt{-3}]$ なので $\mathbb{Z}[\sqrt{-3}] \neq \mathbb{Z}[\zeta]$ である.

[定理 1.3] $\mathbb{Z}[\zeta]$ は K の部分整域である. $\mathbb{Z}[\zeta]$ を K の**整数環**という.

[証明] $R = \mathbb{Z}[\zeta]$ とおく． $R \subseteq K$ である． $\mathbb{Z} \subseteq R$ より, R は空集合でない． また, 任意の $a, b, c, d \in \mathbb{Z}$ に対して,

$$(a + b\zeta) - (c + d\zeta) = (a - c) + (b - d)\zeta \in R.$$

また, $\zeta^2 + \zeta + 1 = 0$ を用いれば,

$$\begin{aligned}(a + b\zeta)(c + d\zeta) &= ac + (ad + bc)\zeta + bd\zeta^2 \\ &= (ac - bd) + (ad + bc - bd)\zeta \in R.\end{aligned}$$

ゆえに, R は K の部分環である．さらに, K は体, したがって整域であるから, その部分環である R も整域である. $\square$

[定理 1.4] α, β を K の整数とし, $\beta \neq 0$ とする．このとき, ある K の整数 κ, ρ が存在して,

$$\alpha = \beta\kappa + \rho, \quad N_K\rho < N_K\beta$$

が成り立つ.

[証明] 任意の実数 t に対して, $\lfloor t \rfloor$ を t 以下の有理整数のうちで最大のものとし,

$$n(t) = \begin{cases} \lfloor t \rfloor, & t \leq (2\lfloor t \rfloor + 1)/2 \text{ のとき} \\ \lfloor t \rfloor + 1, & t > (2\lfloor t \rfloor + 1)/2 \text{ のとき} \end{cases}$$

とおくと,

$$|t - n(t)| \leq \frac{1}{2}$$

が成り立つ[1)].

$z = x + y\zeta$ を K の任意の元とし, $\kappa = n(x) + n(y)\zeta$ とおく. このとき, κ は K の整数であり,

$$\begin{aligned} N_K(z - \kappa) &= (x - n(x))^2 - (x - n(x))(y - n(y)) + (y - n(y))^2 \\ &= |x - n(x)|^2 + |x - n(x)||y - n(y)| + |y - n(y)|^2 \\ &\leq \frac{3}{4}. \end{aligned}$$

$z = \alpha/\beta$ とおくと,

$$N_K\left(\frac{\alpha}{\beta} - \kappa\right) \leq \frac{3}{4}.$$

両辺に $N_K(\beta)$ を掛けると,

$$N_K\beta \cdot N_K\left(\frac{\alpha}{\beta} - \kappa\right) \leq \frac{3}{4} N_K\beta.$$

定理 1.2 を用いて左辺を計算すれば,

$$N_K\beta \cdot N_K\left(\frac{\alpha}{\beta} - \kappa\right) = N_K\left(\beta \cdot \left(\frac{\alpha}{\beta} - \kappa\right)\right) = N_K(\alpha - \kappa\beta).$$

ゆえに,

$$N_K(\alpha - \kappa\beta) \leq \frac{3}{4} N_K\beta < N_K\beta.$$

$\rho = \alpha - \beta\kappa$ とおけば, 求める結果が得られる. □

1.2 単数

K の整数 ε が**単数**であるとは, ある K の整数 ε' が存在して $\varepsilon\varepsilon' = 1$ が成り立つときにいう. 単数の全体を $\mathbb{Z}[\zeta]^\times$ で表す.

[定理 1.5] K の整数で単数となるものは, ± 1, $\pm\zeta$, $\pm(1 + \zeta)$ の 6 つである:

$$\mathbb{Z}[\zeta]^\times = \{\pm 1, \pm\zeta, \pm(1 + \zeta)\}.$$

$\mathbb{Z}[\zeta]^\times$ は $-\zeta$ を生成元とする位数 6 の巡回群になる. $\mathbb{Z}[\zeta]^\times$ を**単数群**という.

---

1) $n(t)$ は t の両側に隣接する 2 つの整数のうち t に近いほうを意味する.

[証明] まず,

$$1 \cdot 1 = (-1) \cdot (-1) = -(1+\zeta)\zeta = -\zeta(1+\zeta) = 1$$

より, ± 1, $\pm\zeta$, $\pm(1+\zeta)$ は単数である.

$\varepsilon = a + b\zeta$ を単数とすれば, ある K の整数 ε' が存在して,

$$\varepsilon\varepsilon' = 1.$$

両辺のノルムをとると,

$$N_K\varepsilon N_K\varepsilon' = 1.$$

よって, $N_K\varepsilon = a^2 - ab + b^2$ は $\mathbb{Z}$ における 1 の約数である. ノルムの値は正なので,

$$a^2 - ab + b^2 = 1.$$

両辺を 4 倍して変形すると,

$$(2a-b)^2 + 3b^2 = 4.$$

この方程式を満たす a, b の組を求めればよいが, $3b^2 \leq 4$ より $b^2 = 0$ または 1. よって, $b = 0, \pm 1$ である. $b = 0$ のときは, $(2a)^2 = 4$ より $a = \pm 1$ を得る. $b = 1$ のときは, $(2a-1)^2 = 1$ より $a = 0, 1$ を得る. $b = -1$ のときは, $(2a+1)^2 = 1$ より $a = -1, 0$ を得る. ゆえに, すべての解は

$$(a, b) = (\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1)$$

の 6 つである. よって, $\varepsilon = \pm 1, \pm\zeta, \pm(1+\zeta)$ を得る.

$\mathbb{Z}[\zeta]^\times$ が $-\zeta$ から生成される巡回群であることは,

$$(-\zeta)^2 = \zeta^2 = -(1+\zeta), \quad (-\zeta)^3 = -1,$$
$$(-\zeta)^4 = -\zeta, \quad (-\zeta)^5 = -\zeta^2 = 1+\zeta, \quad (-\zeta)^6 = 1$$

よりわかる. □

α, β を 0 でない K の整数とするとき, α が β に**同伴**であるとは, ある単数 ε が存在して $\alpha = \beta\varepsilon$ が成り立つときにいう. このことを記号で $\alpha \sim \beta$ と書く. 2 つの K の整数が同伴であるという関係は $\mathbb{Z}[\zeta]$ における同値関係である. 単数は $\pm 1, \pm\zeta, \pm(1+\zeta)$ の 6 つなので, α に同伴なものは

$$\pm\alpha, \quad \pm\alpha\zeta, \quad \pm\alpha(1+\zeta)$$

の 6 つである.

[定理 1.6] ε を K の整数とする. このとき, 次の 3 つの条件は同値である.

(i) ε は単数である.

(ii) ε は 1 に同伴である.

(iii) $N_K\varepsilon = 1$.

［証明］ (i)⇒(ii) ε を単数とすると, ある K の整数 ε' が存在して, $\varepsilon\varepsilon' = 1$. このとき, ε' もまた単数である. したがって, ε は 1 に同伴である.

(ii)⇒(iii) ε が 1 に同伴であるとすると, ある単数 ε' が存在して, $\varepsilon\varepsilon' = 1$. ノルムをとり, 定理 1.2 を用いて計算すると,

$$N_K\varepsilon N_K\varepsilon' = N_K(\varepsilon\varepsilon') = N_K 1 = 1.$$

$N_K\varepsilon$, $N_K\varepsilon'$ はともに正の有理整数だから, $N_K\varepsilon = 1$ となる.

(iii)⇒(i) $N_K\varepsilon = 1$ とすると, ノルムの定義より $\varepsilon\varepsilon^\sigma = 1$ であり, ε^σ は K の整数だから, ε は単数である. □

1.3 $\mathbb{Q}(\sqrt{-3})$ の整数の整除

2 つの K の整数 α, β に対して, ある K の整数 ξ 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.

α がいくつかの $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{Z}[\zeta]$ 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.

2 つ以上の K の整数に対して, それらの最大公約数と同伴なものも最大公約数であり, また, 任意の 2 つの最大公約数は同伴になる. 最小公倍数についても同様である.

［定理 1.7］ α, β, κ, ρ を K の整数とし,

$$\alpha = \beta\kappa + \rho$$

が成り立っているとする. このとき, α, β の最大公約数と β, ρ の最大公約数とは同伴である.

［証明］ α, β の最大公約数を δ とおき, β, ρ の最大公約数を δ' とおく. $\alpha = \beta\kappa + \rho$ より, δ' は α を割る. δ' は β も割るから, α, β の公約数である. ゆえに, δ' は δ を割る. 同様に, $\rho = \alpha - \beta\kappa$ より, δ が δ' を割ることもいえる. ゆえに, $\delta' \mid \delta$ かつ $\delta \mid \delta'$. したがって, $\delta' \sim \delta$. □

［定理 1.8］ α, β を K の整数とする. まず,

$$\alpha = \beta\kappa_0 + \rho_1, \quad N_K\rho_1 < N_K\beta$$

なる κ_0, ρ_1 を求める．$N_K\rho_1 \neq 0$ ならば,

$$\beta = \rho_1\kappa_1 + \rho_2, \quad N_K\rho_2 < N_K\rho_1$$

なる κ_1, ρ_2 を求める．$N_K\rho_2 \neq 0$ ならば,

$$\rho_1 = \rho_2\kappa_2 + \rho_3, \quad N_K\rho_3 < N_K\rho_2$$

なる κ_2, ρ_3 を求める．以下同様の操作を行うと, ある番号 $n \geq 0$ が存在して, $\rho_{n+1} = 0$ かつ ρ_n は α, β の最大公約数である．

［証明］ もし仮に, 任意の番号 $i \geq 1$ に対して $N_K\rho_i \neq 0$ であるとすると, 定理 1.4 を繰り返し用いて,

$$N_K\beta > N_K\rho_1 > N_K\rho_2 > \cdots > N_K\rho_l > 0, \quad l = N_K\beta$$

なる減少列が作れる．ところが, 各 i に対して $N_K\rho_i \leq N_K\beta - i$ であるから, $N_K\rho_l \leq N_K\beta - l = 0$ となって $N_K\rho_l > 0$ と矛盾する．よって, ある番号 $n \geq 0$ が存在して, $N_K\rho_{n+1} = 0$ となる．このとき, $\rho_{n+1} = 0$ であるから, $\rho_{n-1} = \rho_n\kappa_n$ となり, ρ_n は ρ_{n-1}, ρ_n の最大公約数である．

いま, 2 つの K の整数 ξ, η の最大公約数を (ξ, η) で表すことにすれば, 定理 1.7 より,

$$(\alpha, \beta) \sim (\beta, \rho_1) \sim (\rho_1, \rho_2) \sim \cdots \sim (\rho_{n-1}, \rho_n) \sim \rho_n.$$

ゆえに, ρ_n は α, β の最大公約数である． □

［定理 1.9］ α, β を 0 でない K の整数とし, α, β の最小公倍数を λ, 最大公約数を δ とする．このとき, $\alpha\beta$ は $\lambda\delta$ に同伴である．

［証明］ λ は α, β の公倍数であるから, ある α_1, β_1 が存在して,

$$\lambda = \alpha\beta' = \beta\alpha'. \tag{1}$$

一方, $\alpha\beta$ は α, β の倍数であるから, それらの最小公倍数である λ の倍数である．よって, ある K の整数 δ' が存在して,

$$\alpha\beta = \lambda\delta'. \tag{2}$$

(1) を (2) に代入すると,

$$\alpha\beta = \alpha\beta'\delta' = \beta\alpha'\delta'.$$

これより,

$$\alpha = \alpha'\delta', \quad \beta = \beta'\delta' \tag{3}$$

を得る．よって, δ' は α, β の公約数であるから, それらの最大公約数である δ の約数である．すなわち, ある K の整数 ε が存在して,

$$\delta = \delta'\varepsilon. \tag{4}$$

δ' は α, β を割るから, ある α'', β'' が存在して,

$$\alpha = \delta'\varepsilon\alpha'', \quad \beta = \delta'\varepsilon\beta''.$$

これを (3) に代入すると,

$$\delta'\varepsilon\alpha'' = \delta'\alpha', \quad \delta'\varepsilon\beta'' = \delta'\beta'.$$

もし仮に $\delta' = 0$ ならば, (2) より $\alpha\beta = 0$ となって α, β がともに 0 でないことに反する．したがって, $\delta' \neq 0$ であるから,

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

ゆえに, ε は α', β' の公約数である．これを (1) に代入すると,

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

各辺に ε^{-1} を掛けると,

$$\lambda\varepsilon^{-1} = \alpha\beta'' = \beta\alpha''.$$

よって, $\lambda\varepsilon^{-1}$ は α, β の公倍数であり, したがって λ の倍数である．すなわち, ある K の整数 ε' が存在して, $\lambda\varepsilon^{-1} = \lambda\varepsilon'$. ゆえに, $\varepsilon^{-1} = \varepsilon'$. これより $\varepsilon\varepsilon' = 1$ となるから, ε は単数である．また, (2), (4) より,

$$\alpha\beta\varepsilon = \lambda\delta$$

が得られる．すなわち, $\alpha\beta$ は $\lambda\delta$ に同伴である． □

2 つ以上の K の整数が**互いに素**であるとは, 単数以外の公約数が存在しないときにいう．互いに素であることは, 最大公約数が単数であることと同値である．

［定理 1.10］ α, β, γ を K の整数とする．α, β は互いに素であり, ともに 0 でないとする．このとき,

$$\alpha \mid \beta\gamma \Longrightarrow \alpha \mid \gamma$$

が成り立つ．

［証明］ α, β は互いに素だから, それらの最大公約数は単数である．よって, 定理 1.9 より, α, β の最小公倍数は $\alpha\beta$ に同伴である．また, $\alpha \mid \beta\gamma$ より, $\beta\gamma$ は α, β の公倍数である．ゆえに, $\beta\gamma$ は $\alpha\beta$ の倍数となる．すなわち, ある K の整数 ξ が存在して,

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

$\beta \neq 0$ であるから, 両辺を β で割ると, $\gamma = \alpha\xi$. すなわち, $\alpha \mid \gamma$. □

1.4　既約元分解とその一意性

π を 0 でも単数でもない K の整数とする．π が**既約元**であるとは, 任意の K の整数 α, β に対して,

$$\pi = \alpha\beta \Longrightarrow \alpha \text{ または } \beta \text{ が単数}$$

が成り立つときにいう．また, π が**素元**であるとは, 任意の K の整数 α, β に対して,

$$\pi \mid \alpha\beta \Longrightarrow \pi \mid \alpha \text{ または } \pi \mid \beta$$

が成り立つときにいう．

［定理 1.11］　(i) 既約元と同伴な K の整数は既約元である．

(ii) 素元と同伴な K の整数は素元である．

［証明］ (i)　π を既約元, ε と単数とする．α, β を K の整数とし, $\pi\varepsilon = \alpha\beta$ とすると, $\pi = \alpha\beta\varepsilon^{-1}$ より, α または $\beta\varepsilon^{-1}$ は単数である．$\beta\varepsilon^{-1}$ が単数のときは, ある K の整数 ε' が存在して $\beta\varepsilon^{-1}\varepsilon' = 1$ となるから, β は単数である．ゆえに, α または β は単数である．したがって, $\pi\varepsilon$ もまた既約元である．

(ii)　π を素元, ε と単数とする．α, β を K の整数とし, $\pi\varepsilon \mid \alpha\beta$ とすると, ある K の整数 ξ が存在して, $\alpha\beta = \pi\varepsilon\xi$. 両辺に $(\varepsilon^{-1})^2$ を掛けると,

$$(\alpha\varepsilon^{-1})(\beta\varepsilon^{-1}) = \pi\varepsilon^{-1}\xi.$$

よって, $\pi \mid (\alpha\varepsilon^{-1})(\beta\varepsilon^{-1})$. ゆえに, $\pi \mid \alpha\varepsilon^{-1}$ または $\pi \mid \beta\varepsilon^{-1}$. これより, $\pi\varepsilon \mid \alpha$ または $\pi\varepsilon \mid \beta$ が得られる．したがって, $\pi\varepsilon$ もまた素元である．　□

［定理 1.12］ π を K の整数とし, π^σ を π の共役とする．

(i) π が既約元ならば π^σ も既約元である．

(ii) π が素元ならば π^σ も素元である．

［証明］ (i)　π を既約元とする．α, β を K の整数とし, $\pi^\sigma = \alpha\beta$ とする．

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

であるから, α^σ または β^σ は単数である．よって, α または β も単数である．したがって, π^σ は既約元である．

(ii)　π を素元とする．α, β を K の整数とし, $\pi^\sigma \mid \alpha\beta$ とする．このとき, ある K の整数 ξ が存在して, $\alpha\beta = \pi^\sigma\xi$. ゆえに,

$$\alpha^\sigma\beta^\sigma = (\alpha\beta)^\sigma = (\pi^\sigma\xi) = \pi\xi^\sigma.$$

π は素元だから, $\pi \mid \alpha^\sigma$ または $\pi \mid \beta^\sigma$ となる. $\pi \mid \alpha^\sigma$ のとき, ある K の整数 ξ' が存在して, $\alpha^\sigma = \pi\xi'$. よって,

$$\alpha = (\alpha^\sigma)^\sigma = (\pi\xi')^\sigma = \pi^\sigma \xi'^\sigma.$$

ゆえに, $\pi^\sigma \mid \alpha$. 同様に, $\pi \mid \beta^\sigma$ のとき, $\pi^\sigma \mid \beta$ となる. ゆえに, $\pi^\sigma \mid \alpha$ または $\pi^\sigma \mid \beta$. したがって, π は素元である. □

[定理 1.13] π を K の整数とする. このとき, 次の 2 つの条件は同値である.

(i) π は既約元である.

(ii) π は素元である.

[証明] (i)⇒(ii)　π を既約元, α, β を K の整数とし, $\pi \mid \alpha\beta$ とする. δ を π, α の最大公約数とすると, δ は π の約数だから, δ は単数であるか, または π に同伴である. δ が単数であるとき, α と π は互いに素だから, 定理 1.10 より, β が π で割り切れる. 一方, δ が π に同伴であるとき, α は δ で割り切れるから, π でも割り切れる. ゆえに, $\pi \mid \alpha$ または $\pi \mid \beta$ である. したがって, π は素元である.

(ii)⇒(i)　π を素元, α, β を K の整数とし, $\pi = \alpha\beta$ とする. $\pi \mid \alpha\beta$ であるから, $\pi \mid \alpha$ または $\pi \mid \beta$ が成り立つ. $\pi \mid \alpha$ のとき, ある K の整数 ξ が存在して $\alpha = \pi\xi$ となるから,

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

$\pi \neq 0$ より, $1 = \xi\beta$. ゆえに, β は単数である. 同様に, $\pi \mid \beta$ のとき, α が単数であることが導かれる. ゆえに, α または β は単数である. したがって, π は既約元である. □

[定理 1.14] α を K の整数とする. このとき, $N_K\alpha$ が素数ならば α は既約元である.

[証明] 対偶を示す. α が既約元でないとすると, ある K の整数 β, γ が存在して,

$$\alpha = \beta\gamma, \quad \beta, \gamma \text{ は単数でない}.$$

ノルムをとると, 定理 1.2, 定理 1.6 より,

$$N_K\alpha = N_K\beta N_K\gamma, \quad N_K\beta > 1, \quad N_K\gamma > 1.$$

ゆえに,

$$1 < N_K\beta < N_K\alpha, \quad 1 < N_K\gamma < N_K\alpha.$$

したがって, $N_K\alpha$ は素数でない. □

[定理 1.15] α を 0 でも単数でもない K の整数とする．このとき, α は既約元の積で表される．

[証明] ノルムの定義より, $N_K\alpha$ は正の有理整数であり,

$$N_K\alpha = 0 \Longleftrightarrow \alpha = 0.$$

また, 定理 1.6 より,

$$N_K\alpha = 1 \Longleftrightarrow \alpha \text{ は単数}.$$

したがって, すべての有理整数 $n \geq 2$ に対して, n に関する命題

(P_n)　$N_K\alpha = n$ なる K の整数 α は既約元の積で表される．

が成り立つことを示せばよい．n に関する数学的帰納法により証明する．

$n = 2$ のとき, 2 は素数だから, 定理 1.14 より, $N_K\alpha = 2$ を満たす α は既約元である．

$n > 2$ のとき, $2 \leq k \leq n-1$ なるすべての有理整数 k に対しては命題 (P_k) が成り立つと仮定する．α を $N_K\alpha = n$ なる K の整数とする．α が既約元でないとすると, ある K の整数 β, γ が存在して,

$$\alpha = \beta\gamma, \quad \beta, \gamma \text{ は単数でない}.$$

ノルムをとると, 定理 1.2, 定理 1.6 より,

$$N_K\alpha = N_K\beta N_K\gamma, \quad N_K\beta > 1, \quad N_K\gamma > 1.$$

ゆえに,

$$2 \leq N_K\beta < N_K\alpha, \quad 2 \leq N_K\gamma < N_K\alpha.$$

帰納法の仮定より, β, γ はともに既約元の積で表される．ゆえに, α も既約元の積で表される．したがって, n のときも命題 (P_n) は正しい．　□

[定理 1.16] K の整数 α を既約元の積で表す仕方は同伴を除き一意的である．

[証明] 証明すべきことは, K の整数 α が既約元の積で

$$\alpha \sim \pi_1\pi_2\cdots\pi_r \sim \pi_1'\pi_2'\cdots\pi_s'$$

と 2 通りに表されたとき, $r = s$ かつ適当に番号を付け替えれば $\pi_i \sim \pi_i'$ $(i = 1, 2, \ldots, r)$ となることである．ここで, $\sim$ は同伴であることを表す．

r に関する数学的帰納法により証明する．

$r = 1$ のとき．

$$\alpha \sim \pi_1 \sim \pi_1'\pi_2'\cdots\pi_s'.$$

とすると, ある単数 ε が存在して,

$$\pi_1 = \pi'_1\pi'_2 \cdots \pi'_s\varepsilon.$$

もし仮に $s \geq 2$ とすると, π_1 は既約元なので, π'_1 または $\pi'_2 \cdots \pi'_s\varepsilon$ が単数である. π'_1 は既約元であり, したがって単数でないから, $\pi'_2 \cdots \pi'_s\varepsilon$ が単数である. 定理 1.2, 定理 1.6 より,

$$\begin{aligned} N_K\pi'_2 \cdots N_K\pi'_s &= N_K\pi'_2 \cdots N_K\pi'_s N_K\varepsilon \\ &= N'_K(\pi'_2 \cdots \pi'_s\varepsilon) = 1. \end{aligned}$$

ところが, $\pi'_2, \ldots, \pi'_s$ は単数でないから, $N_K\pi'_2 \cdots N_K\pi'_s$ は 1 より大きい. これは矛盾である. したがって, $s = 1$ となり, $\pi_1 = \pi'_1\varepsilon$ となる.

$r > 1$ のとき. $r - 1$ に対しては既約元の積による表し方の一意性が成り立つと仮定する.

$$\alpha \sim \pi_1\pi_2 \cdots \pi_r \sim \pi'_1\pi'_2 \cdots \pi'_s$$

とすると, ある単数 ε が存在して,

$$\pi_1\pi_2 \cdots \pi_r = \pi'_1\pi'_2 \cdots \pi'_s\varepsilon.$$

このとき, $\pi'_1 \mid \pi_1\pi_2 \cdots \pi_r$ である. 定理 1.13 より π'_1 は素元であるから, いずれかの π_i を割るが, 番号を適当に付け替えて $\pi'_1 \mid \pi_1$ としてもよい. すなわち, ある K の整数 ε_1 が存在して $\pi_1 = \pi'_1\varepsilon_1$ となる. π_1 は既約元だから, ε_1 が単数になる. よって,

$$\pi_2 \cdots \pi_r = \pi'_2 \cdots \pi'_s\varepsilon\varepsilon_1$$

かつ $\varepsilon\varepsilon_1$ は単数である. すなわち,

$$\pi_2 \cdots \pi_r \sim \pi'_2 \cdots \pi'_s.$$

帰納法の仮定より, $r = s$ となり, 番号を適当に付け替えることで $\pi_i \sim \pi'_i$ $(i = 2, \ldots, r)$ となる. したがって, r のときも既約元の積による表し方の一意性が成り立つ. □

1.5 イデアル

$\mathbb{Z}[\zeta]$ の空でない部分集合 $\mathfrak{a}$ が, 次の 2 つの条件

(i) 任意の $\alpha, \beta \in \mathfrak{a}$ に対して, $\alpha - \beta \in \mathfrak{a}$.

(ii) 任意の $\gamma \in \mathbb{Z}[\zeta]$, $\alpha \in \mathfrak{a}$ に対して, $\gamma\alpha \in \mathfrak{a}$.

を満たすとき, $\mathfrak{a}$ を $\mathbb{Z}[\zeta]$ の**イデアル**という.

K の整数 $\alpha_1, \alpha_2, \ldots, \alpha_r$ に対して,

$$\{x_1\alpha_1 + x_2\alpha_2 + \cdots + x_r\alpha_r \mid x_i \in \mathbb{Z}[\zeta]\}$$

は $\mathbb{Z}[\zeta]$ のイデアルである．これを $\alpha_1, \alpha_2, \ldots, \alpha_r$ から**生成されるイデアル**といい,

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

という記号で表す．また, $\alpha_1, \alpha_2, \ldots, \alpha_r$ をイデアル $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ の**生成元**という．また, ただ 1 つの元 $\alpha \in \mathbb{Z}[\zeta]$ から生成されるイデアル

$$(\alpha) = \{x\alpha \mid x \in \mathbb{Z}[\zeta]\}$$

を**単項イデアル**という．

α, β を K の整数とする．このとき,

$$\begin{aligned}(\alpha) = (\beta) &\Longleftrightarrow \beta \in (\alpha) \text{ かつ } \alpha \in (\beta) \\ &\Longleftrightarrow \alpha \mid \beta \text{ かつ } \beta \mid \alpha \\ &\Longleftrightarrow \alpha \sim \beta\end{aligned}$$

が成り立つ．

0 だけからなる集合 $\{0\}$ は, 0 から生成される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．任意のイデアルは零イデアルを含む．

また, $\mathbb{Z}[\zeta]$ 自身は, 1 から生成される単項イデアルである．すなわち, $\mathbb{Z}[\zeta] = (1)$．

［定理 1.17］ $\mathbb{Z}[\zeta]$ のすべてのイデアルは単項イデアルである．

［証明］ 零イデアル (0) は単項イデアルだから, それ以外の $\mathbb{Z}[\zeta]$ のイデアルが単項イデアルであることを示せばよい．

$\mathfrak{a} \neq (0)$ を $\mathbb{Z}[\zeta]$ のイデアルとすると, $\{N_K\gamma \mid \gamma \in \mathfrak{a}, \gamma \neq 0\}$ は正の有理整数からなる空でない集合である．自然数の整列性により, この集合には最小元が存在する．そこで, $\mathfrak{a}$ の 0 でない元でノルムの値が最小であるようなものを β とする．定理 1.4 より, 任意の $\alpha \in \mathfrak{a}$ に対して, ある $\kappa, \rho \in \mathbb{Z}[\zeta]$ が存在して,

$$\alpha = \beta\kappa + \rho, \quad N_K\rho < N_K\beta$$

が成り立つ．もし仮に $\rho \neq 0$ とすれば,

$$\rho = \alpha - \beta\kappa \in \mathfrak{a}$$

となり, β の最小性に反する．ゆえに, $\rho = 0$．したがって, $\alpha = \beta\kappa \in (\beta)$ となり, $\mathfrak{a} \subseteq (\beta)$ がいえる．逆の包含関係は明らかだから, $\mathfrak{a} = (\beta)$ であり, $\mathfrak{a}$ は単項イデアルである． □

［定理 1.18］ $\alpha_1, \alpha_2, \ldots, \alpha_r$ を K の整数とし, それらの最大公約数を δ とする．このとき,

$$(\alpha_1, \alpha_2, \ldots, \alpha_r) = (\delta)$$

が成り立つ．

[証明] 定理 1.17 より, $\mathbb{Z}[\zeta]$ のすべてのイデアルは単項イデアルだから, ある K の整数 β が存在して,

$$(\alpha_1,\, \alpha_2,\, \ldots,\, \alpha_r) = (\beta).$$

このとき, $\beta \in (\alpha_1,\, \alpha_2,\, \ldots,\, \alpha_r)$ であるから, ある K の整数 $\xi_1,\, \xi_2,\, \ldots,\, \xi_r$ が存在して,

$$\beta = \alpha_1\xi_1 + \alpha_2\xi_2 + \cdots + \alpha_r\xi_r.$$

よって, δ は β を割る. 逆に, 各 i について $\alpha_i \in (\beta)$ であるから, β は $\alpha_1,\, \alpha_2,\, \ldots,\, \alpha_r$ の公約数である. よって, β は δ の約数である. ゆえに, δ は β に同伴である. したがって, $(\delta) = (\beta)$ となる. □

1.6 素数の $\mathbb{Q}(\sqrt{-3})$ での分解

p を素数とする. $\mathbb{Z}[\zeta]$ において,

$$p \sim \pi_1^{e_1}\pi_2^{e_2}\cdots\pi_g^{e_g}$$

と互いに同伴でない既約元の冪積で表すことができる. ノルムをとると,

$$p^2 = (N_K\pi_1)^{e_1}(N_K\pi_2)^{e_2}\cdots(N_K\pi_g)^{e_g}.$$

各 $N_K\pi_i$ は正の有理整数なので, $N_K\pi = p^{f_i}$ の形であり,

$$2 = e_1f_1 + e_2f_2 + \cdots + e_gf_g$$

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) $g = 1,\, e_1 = 2,\, f_1 = 1.$

それぞれの場合に応じて,

(D1) $p \sim \pi_1\pi_2,\, \pi_1 \not\sim \pi_2,\, N_K\pi_1 = N_K\pi_2 = p.$

(D2) $p \sim \pi_1,\, N_K\pi_1 = p^2.$

(D3) $p \sim \pi_1^2,\, N_K\pi_1 = p.$

(D1), (D2), (D3) のとき, それぞれ p は $K/\mathbb{Q}$ で**完全分解する**, **惰性する**, **完全分岐する**という.

[定理 1.19] π を素元とする[2]. π の倍数であるような有理整数の中で最小のものを p とする. このとき, p は素数である.

[2] K の整数においては, 既約元であることと素元であることとは同値である (定理 1.13).

［証明］ π は単数でないから, $p \neq 1$. もし仮に p が合成数であるとすれば, ある正の有理整数 a, b が存在して,

$$p = ab, \quad 1 < a < p, \quad 1 < b < p.$$

一方, $\pi \mid p = ab$ であるから, $\pi \mid a$ または $\pi \mid b$. これは p の最小性に反する. したがって, p は素数である. $\square$

［定理 1.20］ p を素数とする. このとき,

$$p \text{ は } K/\mathbb{Q} \text{ で完全分岐する} \iff p = 2$$

が成り立つ.

［証明］ p が完全分岐するとすれば, ある既約元 π が存在して,

$$p \sim \pi^2, \quad p = N_K \pi = \pi\pi^\sigma.$$

既約元の積による表し方の一意性から, $\pi \sim \pi^\sigma$. また, 単元は ± 1, $\pm\zeta$, $\pm(1+\zeta)$ の 6 つであるから,

$$\pi = \pm\pi^\sigma,\ \pm\pi^\sigma\zeta,\ \pm\pi^\sigma\zeta^2.$$

ここで, $1 + \zeta = -\zeta^2$ を用いた. $\pi = x + y\zeta$, $x, y \in \mathbb{Z}$ とおくと,

$$x + y\zeta = \pm(x + y\zeta^\sigma),\ \pm(x + y\zeta^\sigma)\zeta,\ \pm(x + y\zeta^\sigma)\zeta^2.$$

右辺を計算すると,

$$\begin{aligned}
x + y\zeta^\sigma &= x + y\zeta^2 = x - y(1+\zeta) \\
&= (x - y) - y\zeta, \\
(x + y\zeta^\sigma)\zeta &= (x + y\zeta^2)\zeta = y + x\zeta, \\
(x + y\zeta^\sigma)\zeta^2 &= (x + y\zeta^2)\zeta^2 = x\zeta^2 + y\zeta \\
&= -(1+\zeta)x + y\zeta \\
&= -\left(x + (x - y)\zeta\right).
\end{aligned}$$

ゆえに,

$$x + y\zeta = \pm((x - y) - y\zeta),\ \pm(y + x\zeta),\ \mp\left(x + (x - y)\zeta\right).$$

右辺のそれぞれに対して, 関係式

$$\begin{cases} x = x - y \\ y = -y, \end{cases} \begin{cases} x = y - x \\ y = y, \end{cases} \begin{cases} x = y \\ y = x, \end{cases} \begin{cases} x = -y \\ y = -x, \end{cases} \begin{cases} x = -x \\ y = y - x \end{cases} \begin{cases} x = x \\ y = x - y, \end{cases}$$

が得られる．これらを使って変数を減らすと，

$$\pi = x,\, y,\, x(1+\zeta),\, x(1-\zeta),\, x(1+2\zeta),\, x(2+\zeta).$$

$N_K(1+\zeta)=1$, $N_K(1-\zeta)=N_K(1+2\zeta)=N_K(2+\zeta)=3$ であるから，

$$p = N_K\pi = x^2,\, y^2,\, 3x^2.$$

したがって, $p=3$ でなければならない．

逆に，

$$\begin{aligned} N_K(1-\zeta) &= (1-\zeta)(1-\zeta^\sigma) \\ &= (1-\zeta)(1-\zeta^2) = 3 \\ &= -\zeta^2(1-\zeta)^2 \\ &\sim (1-\zeta)^2. \end{aligned}$$

まとめると，

$$3 \sim (1-\zeta)^2, \quad N_K(1-\zeta) = 3.$$

定理 1.14 より, $1-\zeta$ は既約元である．したがって, 3 は $K/\mathbb{Q}$ で完全分岐する． □

【定理 1.21】 p を 3 ではない素数とする．

(i) p は $K/\mathbb{Q}$ で完全分解する $\Longleftrightarrow p \equiv 1 \pmod 3$.

(ii) p は $K/\mathbb{Q}$ で惰性する $\Longleftrightarrow p \equiv 2 \pmod 3$.

【証明】 p は 3 ではないので, $p \equiv 1$ または $2 \pmod 3$．また, 定理 1.20 より, p は $K/\mathbb{Q}$ で完全分解するか惰性するかしかない．よって, (i) を証明すれば十分である．

p が完全分解するとすれば, $N\pi = p$ となる．$\pi = x + y\zeta$, $x, y \in \mathbb{Z}$ とおくと，

$$x^2 - xy + y^2 = p.$$

両辺を 4 倍して変形すると，

$$(2x-y)^2 + 3y^2 = 4p.$$

よって，

$$(2x-y)^2 \equiv p \pmod 3.$$

したがって, p は 3 を法として平方剰余である．ゆえに, $p \equiv 1 \pmod 3$.

逆に, $p \equiv 1 \pmod 3$ とすると, p は 3 を法とする平方剰余である．平方剰余の相互法則と第 1 補充法則により, -3 は p を法とする平方剰余である．ゆえに, ある有理整数 x が存在して，

$$(x-\sqrt{-3})(x+\sqrt{-3}) = x^2+3 \in p\mathbb{Z} \subseteq p\mathbb{Z}[\zeta].$$

もし仮に p が $K/\mathbb{Q}$ で惰性するならば, p は $\mathbb{Z}[\zeta]$ の既約元, したがって素元であるから, $p \mid x+\sqrt{-3}$ または $p \mid x-\sqrt{-3}$ となる. $p \mid x+\sqrt{-3}$ のとき, ある K の整数 $x'+y'\zeta$, x', $y' \in \mathbb{Z}$ が存在して,

$$x+1+2\zeta = x+\sqrt{-3} = p(x'+y'\zeta) = px'+py'\zeta.$$

これより $py'=2$ となり, $p=2$ を得るが, これは $p \equiv 1 \pmod 3$ に反する. $p \mid x-\sqrt{-3} = x-1-2\zeta$ のときも, 同様にして矛盾が導かれる. ゆえに, p は $K/\mathbb{Q}$ で惰性しない. したがって, p は $K/\mathbb{Q}$ で完全分解する. □

参考文献

[1] A. ヴェイユ (片山孝次訳): 初学者のための整数論, 現代数学社, 1995

[2] 高木貞治: 初等整数論講義 第 2 版, 岩波書店, 1971.