

数学特別講義VII /
代数学特論V

この講義の目的は、代数体の整数環を学ぶことです。

$= \mathbb{Q}$ の有限次拡大体 K $x \in K$ が整であるとは、モノミクな多項式 $f \in \mathbb{Q}[X]$ が存在し、 $f(x) = 0$ 。

§1 整

§1.1 環の整拡大

この講義では、すべての環が単位元をもつ可換環であると仮定する。

- A, B を環とし、 A が B の部分環であるとする。このとき、 B を A の環拡大とよぶ。
- B は自然的に A -代数である。また、 B は A -加群としてもみなすことができる。
- $b \in B$ とする。 b で生成される B の A -部分代数を $A[b]$ で表す。つまり、 $A[b] = \{P(b) \mid P \in A[X]\}$ 。
同様に $b_1, \dots, b_n \in B$ のとき、 $A[b_1, \dots, b_n]$ を帰納法により、 $A[b_1, \dots, b_{n-1}][b_n]$ で定義する。
もし $B = A[b_1, \dots, b_n]$ ($b_1, \dots, b_n \in B$) ならば、 B は有限生成 A -代数であるという。
- B は有限生成 A -加群であるとは、 $B = Ab_1 + \dots + Ab_n$ ($b_1, \dots, b_n \in B$) であることという。
($= \{ \sum_{i=1}^n a_i b_i \mid a_i, b_i \in A \}$)

定義 1.1.1 (整) A, B を環とし、 $A \subset B$ とする。 B の元 b が A 上整であるとは、 A の元 $a_1, a_2, \dots, a_n$ ($n \geq 1$) が存在し、
 $b^n + a_1 b^{n-1} + \dots + a_{n-1} b + a_n = 0$ であることをいう。つまり、 b が A 上のモノミクな多項式の根である。
 B の任意の元が A 上整であるとき、 B が A 上整であるという。

明かに A の任意の元は A 上整である ($a \in A$ が $X - a$ の根である)。

命題 1.1.2 $A \subset B$, $b \in B$ とする。このとき、次の条件が同値である。

- b が A 上整である。
- $A[b]$ が有限生成 A -加群である。
- $A[b] \subset C \subset B$ となる B の部分環 C が存在し、さらに C は有限生成 A -加群である。

証明 (i) $\Rightarrow$ (ii) を示す。 $b^n + a_1 b^{n-1} + \dots + a_{n-1} b + a_n = 0$ とし、 $f = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n$ とおく。

$P \in A[X]$ に対して、 $\deg(R) < n$ となる $Q, R \in A[X]$ が存在し $P = fQ + R$ である。

よって、 $P(b) = R(b)$ となり、ゆえ $A[b]$ が $1, b, \dots, b^{n-1}$ により A -加群として生成される。

(ii) $\Rightarrow$ (iii) $C = A[b]$ とおけばよい。

(iii) $\Rightarrow$ (i) $\{b_1, b_2, \dots, b_m\}$ を A -加群 C の成系とする。

$b b_i = \sum_{j=1}^m a_{ij} b_j$ と書ける ($a_{ij} \in A$)。よって、 $\sum_{j=1}^m (a_{ij} - \delta_{ij} b) b_j = 0$ である。つまり、 $M := (a_{ij})_{1 \leq i, j \leq m}$ とおくと $(bE_m - M) \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = 0$ となる。

$$\Rightarrow (bE_m - M)^* (bE_m - M) \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = 0 \Rightarrow \det(bE_m - M) b_i = 0 \quad (1 \leq i \leq m)$$

余因子行列

$b_1, \dots, b_m$ が C を生成するので、 $1 = a_1 b_1 + \dots + a_m b_m$ とする $a_1, \dots, a_m$ が存在する。

$$\Rightarrow \det(bE_m - M) = \sum_{i=1}^m a_i b_i \det(bE_m - M) = 0$$

$P(t) = \det(tE_m - M)$ はモノミクな多項式である。

□

系 1.1.3 $A \subset B$ とする。 A 上整である B の元全体は B の部分環をなす。

証明 $b, b' \in B$ は A 上整であるとする。

命題 1.1.2 から、 $A[b]$ は有限生成 A -加群である。①

b' は $A[b]$ 上整であるので、 $A[b, b']$ は有限生成 $A[b]$ -加群である。②

① + ② から, $A[b, b']$ は有限生成 A -加群である.

なぜかというと, A_1, A_2, A_3 は環で $A_1 \subset A_2 \subset A_3$ のときに

もし $A_2 = A_1 x_1 + \dots + A_1 x_m$ かつ

$A_3 = A_2 y_1 + \dots + A_2 y_n$ ならば, A_3 が $\{x_i y_j\}_{i,j}$ で生成される.

(*)

$b - b', bb' \in A[b, b']$ から, $b - b', bb'$ は A 上整である.

□

定義 1.14 (整閉包, 整閉) $A \subset B$ のときに,

$\overline{A} = \{b \in B \mid b \text{ は } A \text{ 上整である}\}$ とおき, $\overline{A}$ は B における A の整閉包とよぶ.

$\overline{A} = A$ であるときに, A は B において整閉であるという.

命題 1.1.5 $A \subset B \subset C$ とする. C が B 上整であり, かつ B が A 上整であるときに, C が A 上整である.

証明: $c \in C$ とし, $c^n + b_1 c^{n-1} + \dots + b_{n-1} c + b_n = 0$ ($b_1, \dots, b_n \in B$) とする.
 $R = A[b_1, \dots, b_n]$ とおく. $b_1, \dots, b_n$ が A 上整であるので, 系 1.1.3 の証明の (*) を帰納的に使うことで R は有限生成 A -加群であることが分かる.
 また, c が R 上整であるので, $R[c]$ は有限生成 R -加群である.
 よって, $R[c]$ は有限生成 A -加群である. 命題 1.1.2 (iii) より, c は A 上整である. □

A を整域とし, A の商体を K とおく. K における A の整閉包は, A の正規化という.
 また, A が K において整閉であるとき, A が整閉であるという.

系 1.1.6 ACB とする. A の整閉包 $\bar{A}$ は B において整閉である. つまり, $\bar{\bar{A}} = \bar{A}$.

証明: $A \subset \bar{A} \subset \bar{\bar{A}} \subset B$ である.
 $\bar{A}$ は A 上整であり, かつ $\bar{A}$ は $\bar{A}$ 上整である. よって, $\bar{A}$ は A 上整である.
 以上より, $\bar{\bar{A}} = \bar{A}$ となる. □

補題 1.1.7 A を一意分解環とする. このとき, A は整閉である.

証明: $x = \frac{a}{b}$ を A 上整である K の元とする ($a, b \in A, b \neq 0$). また, a と b は互いに素である
 と仮定してもよい.
 $x^n + a_1 x^{n-1} + \dots + a_n = 0$ ($a_1, \dots, a_n \in A$) と書ける. よって, $a^n + a_1 b a^{n-1} + a_2 b^2 a^{n-2} + \dots + a_n b^n = 0$ となる. (つまり, 公約元をもたない)
 このことから, b が a を割る. a と b 互いに素であるので, b は A の単数でないといけない. よって, $x = ab^{-1} \in A$. □

§1.2 体拡大

L/K を有限次体拡大とする. L の元 x に対し, $T_x: L \rightarrow L, y \mapsto xy$ とおく.
 T_x は K -ベクトル空間 L の K -線型写像とみなす.

$\text{Tr}_{L/K}(x) = \text{Tr}(T_x)$, $N_{L/K}(x) = \det(T_x)$, $f_x(t) = \det(tE - T_x)$ と定義する
 (トレース) (ノルム) (T_x の固有多項式)

性質:

- (i) $\text{Tr}_{L/K}(x+y) = \text{Tr}_{L/K}(x) + \text{Tr}_{L/K}(y)$ ($x, y \in L$), $T_x(ax) = a T_x(x)$ ($a \in K, x \in L$), $\text{Tr}_{L/K}(1) = [L:K]$
- (ii) $N_{L/K}(xy) = N_{L/K}(x) N_{L/K}(y)$ ($x, y \in L$), $N_{L/K}(a) = a^{[L:K]}$ ($a \in K$)
- (iii) $p_x(t)$ を x の $K[t]$ における最小多項式とすると, $f_x(t) = p_x(t)^{[L:K(v)]}$ である.
- (iv) L/K を有限次分離拡大とし, $\bar{K}$ を L の代数閉包と固定する. $\Sigma_{L/K} = \{\sigma: L \rightarrow \bar{K} \mid K \text{ 上の埋め込み}\}$ とおく.
 このとき, $f_x(t) = \prod_{\sigma \in \Sigma_{L/K}} (t - \sigma(x))$, $\text{Tr}_{L/K}(x) = \sum_{\sigma \in \Sigma_{L/K}} \sigma(x)$, $N_{L/K}(x) = \prod_{\sigma \in \Sigma_{L/K}} \sigma(x)$.
- (v) $K \subset L \subset M$ を有限次拡大とすると, $\text{Tr}_{L/K} \circ \text{Tr}_{M/L} = \text{Tr}_{M/K}$, $N_{L/K} \circ N_{M/L} = N_{M/K}$ である.

L/K が分離拡大であるとは, 任意の $x \in L$ に対し, p_x が代数閉包 $\bar{K}$ において相異なる根をもつことをいう.

- ・ 標数が0のとき, 任意の代数拡大は分離拡大である.
- ・ L/K を有限次分離拡大とし, $[L:K] = n$ とおく. このときに, K 上の埋め込み $L \rightarrow \bar{K}$ 全体の集合は n 個のものからなる.
- ・ また, このときに $L = K(\alpha)$ となる $\alpha \in L$ が存在する.

定義 1.2.1 (基底の判別式) L/K を有限次分離拡大とする ($n = [L:K]$ とおく).

K 上の埋め込み $L \rightarrow \bar{K}$ 全体を $\sigma_1, \dots, \sigma_n$ と書く. L/K の基底 $(x_1, \dots, x_n)$ の判別式は, 次のように定義される:

$$d(x_1, \dots, x_n) = \det(\sigma_i x_j)_{1 \leq i, j \leq n}^2$$

例 1.2.2

$L = K(\alpha)$ となる α をとる. このとき, $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ は L/K の基底である. この基底の判別式は

$$d(1, \alpha, \dots, \alpha^{n-1}) = \begin{vmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \dots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \dots & \sigma_2(\alpha)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\alpha) & \sigma_n(\alpha)^2 & \dots & \sigma_n(\alpha)^{n-1} \end{vmatrix}^2$$

$$= \prod_{1 \leq i < j \leq n} (\sigma_j(\alpha) - \sigma_i(\alpha))^2 \quad (\text{特に, } d(1, \alpha, \dots, \alpha^{n-1}) \neq 0 \text{ である})$$

補題 1.2.3 $(x_1, \dots, x_n)$ を L/K の基底とする ($n = [L:K]$).

$d(x_1, \dots, x_n) = \det((\text{Tr}_{L/K}(x_i x_j))_{1 \leq i, j \leq n})$ が成り立つ. さらに, $d(x_1, \dots, x_n) \in K$.

証明: $\text{Tr}_{L/K}(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i x_j)$ ($t = 1, \dots, n$, $\{\sigma_1, \dots, \sigma_n\}$ は埋め込み $L \rightarrow \bar{K}$ 全体と認.)

$$= \sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j) \quad \text{より}$$

$(\text{Tr}_{L/K}(x_i x_j))_{i,j} = (\sigma_i(x_j))_{i,j}^t \times (\sigma_i(x_j))_{i,j}$ である. 補題が従う. $\square$

V を K ベクトル空間とし, $\Psi: V \times V \rightarrow K$ を双線型形式とする.
 Ψ が **非退化** であるとは, 次の条件が成り立つことをいう.

任意の $x \in V$ に対して, $\left[\forall y \in V, \Psi(x, y) = 0 \text{ ならば } x = 0 \text{ である} \right]$

$B = (e_1, \dots, e_n)$ を V の基底とし, M を Ψ の B に関する表現行列とする. このとき,

$$\Psi \text{ が非退化} \iff \det(M) \neq 0$$

命題 1.2.4 任意の L/K の基底 $(x_1, \dots, x_n)$ について, $d(x_1, \dots, x_n) \neq 0$ である.
 また, K ベクトル空間 L 上の双線型形式 $(x, y) \mapsto \text{Tr}_{L/K}(xy)$ は非退化である.

証明: $L = K(\alpha)$ のとき, $d(1, \alpha, \dots, \alpha^{n-1}) \neq 0$ が成り立つ.

例 1.2.2 より, $\det \left(\left(\text{Tr}_{L/K}(\alpha^{i-1} \alpha^{j-1}) \right)_{1 \leq i, j \leq n} \right) \neq 0$.

P を $(x_1, \dots, x_n)$ から $(1, \alpha, \dots, \alpha^{n-1})$ への基底変換の行列とする.

$$\left(\text{Tr}_{L/K}(x_i x_j) \right)_{i,j} = P^t \left(\text{Tr}_{L/K}(\alpha^{i-1} \alpha^{j-1}) \right)_{i,j} P \quad \text{より}$$

命題が従う. □

§1.3. 代数体の判別式

A を整閉整域とする (例えば, 一意分解整域). A の商体を K とおき, L/K を有限次分離拡大とする. また, L における A の整閉包は B で表す.

$$\begin{array}{ccc} B & \subset & L \\ \uparrow & & \uparrow \\ A & \subset & K \end{array}$$

補題 1.3.1

- (i) L は B の商体である.
- (ii) $A = B \cap K$
- (iii) $x \in B$ に対し, $\text{Tr}_{L/K}(x), N_{L/K}(x) \in A$ である.
- (iv) $x \in B^\times \iff N_{L/K}(x) \in A^\times$

証明:

- (i) $x \in L$ とする. x は K 上代数的であるので, $x^n + a_1 x^{n-1} + \dots + a_n = 0$ である ($a_1, \dots, a_n \in K$)
 また, A の元 $a \neq 0$ が存在し, $a a_i \in A$ ($\forall i = 1, \dots, n$) である.
 $(ax)^n + a a_1 (ax)^{n-1} + \dots + a^n a_n = 0$ より ax が A 上整である (つまり, $ax \in B$).
 ゆえに, L の任意の元が $\frac{b}{a}$ ($b \in B, a \in A \setminus \{0\}$) で表すことができる. 特に, L は B の商体である.
- (ii) $A \subset B \cap K$ は明らかである. 逆に, $x \in B \cap K$ とする. x は K の元であり, さらに A 上整である.
 A が整閉であるので, $x \in A$ となる.
- (iii) $x \in B$ とする. K 上の埋め込み $\sigma: L \rightarrow \bar{K}$ に対し, σx は A 上整である. なぜならば,
 $x^n + a_1 x^{n-1} + \dots + a_n = 0$ と書け, ゆえに $(\sigma x)^n + (\sigma a_1)(\sigma x)^{n-1} + \dots + \sigma a_n = 0$ となるからである.
 よって, $\text{Tr}_{L/K}(x) = \sum \sigma x$ と $N_{L/K}(x) = \prod \sigma x$ は K の元であり, さらに A 上整である.
- A が整閉 $\Rightarrow \text{Tr}_{L/K}(x), N_{L/K}(x) \in A$ である.
- (iv) $(\Rightarrow)$: $x \in B^\times$ とする. このとき, $xy = 1$ となる $y \in B$ がある. よって, $N_{L/K}(x) N_{L/K}(y) = N_{L/K}(1) = 1$ となる.
 ゆえに, $N_{L/K}(x) \in A^\times$ である.
- $(\Leftarrow)$: $N_{L/K}(x) \in A^\times$ とする. よって, $N_{L/K}(x) a = 1$ となる $a \in A$ が存在する.
 $L \subset \bar{K}$ を代数閉包を選び, $\sigma_1, \dots, \sigma_n$ は K 上の埋め込み $L \rightarrow \bar{K}$ 全体とする
 (σ_i は包含写像 $L \hookrightarrow \bar{K}$ であるとして仮定して良い). よって,
 $x \sigma_1(x) \dots \sigma_n(x) a = 1$ となる. $y = \sigma_1(x) \dots \sigma_n(x) a$ は L の元であり, さらに A 上整である.
 よって, $y \in B$ となる. このことより, $x \in B^\times$ である. □

補題 1.3.2: $(x_1, \dots, x_n)$ を B の元からなる L/K の基底とする. また, $d = d(x_1, \dots, x_n)$ とおく.
 このとき, $dB \subset Ax_1 + \dots + Ax_n$ である.

証明: $x \in B$ とする. $a_1, \dots, a_n \in K$ があり, $x = a_1 x_1 + \dots + a_n x_n$ である.
 $1 \leq i \leq n$ に対し,

$$\text{Tr}_{L/K}(x_i x) = \text{Tr}_{L/K}(a_1 x_1 x_i + \dots + a_n x_n x_i) = \sum_{j=1}^n a_j \text{Tr}_{L/K}(x_i x_j) \quad \text{となる.}$$

つまり,

$$\begin{pmatrix} \text{Tr}_{L/K}(x_1 x) \\ \vdots \\ \text{Tr}_{L/K}(x_n x) \end{pmatrix} = \left(\text{Tr}_{L/K}(x_i x_j) \right)_{1 \leq i, j \leq n} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{である.} \quad (*)$$

$M = (\text{Tr}_{L/K}(x_i x_j))_{1 \leq i, j \leq n}$ とおくと, 補題 1.2.3 より, $\det(M) = d$ である.

(*) の両辺に M の余因子行列をかけてあげると, $M^* \begin{pmatrix} \text{Tr}_{L/K}(x x_1) \\ \vdots \\ \text{Tr}_{L/K}(x x_n) \end{pmatrix} = d \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ となる.

$x_1, \dots, x_n \in B$ より, $M \in M_n(A)$ となり, ゆえに $M^* \in M_n(A)$ である.

また, $\text{Tr}_{L/K}(x x_i) \in A$ である. よって, $d x_i \in A$ ($\forall i = 1, \dots, n$) となる.

以上より, $dx = a_1(dx_1) + \dots + a_n(dx_n) \in A$ である. □

命題 1.3.3. A を単項イデアル整域とする. また, $n = [L:K]$ と書く. このとき,
 B は階数 n の自由 A -加群である. つまり, $x_1, \dots, x_n \in B$ があり

$$B = Ax_1 + \dots + Ax_n \quad \text{である.}$$

証明: B を A -加群として考える. 明かに, ねじれなし A -加群である.
 $(x_1, \dots, x_n)$ を L/K の基底とする. また, $zx_1, \dots, zx_n \in B$ となる $z \in B \setminus \{0\}$ が存在する.
 zx_i を x_i に置き換えることにより, $x_1, \dots, x_n \in B$ であると仮定して良い.
 補題 1.3.2 より,

$$dB \subset Ax_1 + \dots + Ax_n \subset B \quad \text{である} \quad (d = d(x_1, \dots, x_n)) \quad (*)$$

A がネーター環 $\Rightarrow dB$ が有限生成 A -加群である.

$\Rightarrow B$ が有限生成 A -加群である.

A が単項イデアル整域であり, さらに B がねじれなし有限生成 A -加群であるので,
 B が自由 A -加群である.

(*) より, $\text{rank}(B) \leq n \leq \text{rank}(B)$ が成り立つことが分かる. よって, $\text{rank}(B) = n$ である. $\square$

注意 1.3.4. A を単項イデアル整域とする。また、 $[L:K] = n$ と書く。

このとき、 $B = Ax_1 + \dots + Ax_n$ となる $x_1, \dots, x_n \in B$ が存在する (命題 1.3.3)。

(i) 上の $(x_1, \dots, x_n)$ が L/K の基底である。

このような基底は A 上整基底とよばれる。

(ii) $\phi \subset B$ を 0 でない B のイデアルとする。 $x \in B \setminus \{0\}$ に対し、
 $xB \subset \phi \subset B$ が成り立つ。 かつ、 ϕ が自由 A -加群であり、さらに ϕ の階数は n となる。

(iii) また、 $\phi \subset L$ が分数イデアルならば、 ϕ は階数 n の自由 A -加群である。
なぜならば、 $I = x\phi$ が B のイデアルであるような $x \in B \setminus \{0\}$ が存在するからである。
(よって、 A -加群として $\phi \cong I$ である)。

定義 1.3.5. (分数イデアル) A を整域とし、 K を A の商体とする。

$J \subset K$ を 0 でない A -部分加群とする。 J が分数イデアルであるとは、
 $x \in A \setminus \{0\}$ が存在し、 $xJ \subset A$ であることをいう。

つまり、分数イデアルとは、 $x^{-1}I$ ($x \in A \setminus \{0\}$, $I \subset A$ イデアル)
のことである。

例えば、 $\frac{1}{3}\mathbb{Z} \subset \mathbb{Q}$ は $\mathbb{Z}$ の分数イデアルである。

命題 1.3.6 $x \in L$ とする。 x の K 上の最小多項式は $p_x(t) \in K[t]$

とおく。このとき、 $x \in B \iff p_x \in A[t]$ 。

証明: ($\Leftarrow$) p_x がモノックな多項式であるので、 x は A 上整である。

($\Rightarrow$) $x \in B$ とする。 $p_x = \prod_{\sigma} (t - \sigma x)$ である。 全ての $\sigma: L \rightarrow \bar{K}$ に対し、

σx は A 上整であるので、 p_x の係数は A 上整である。 $p_x \in K[t]$ であるので

命題が A の整閉性から従う。

□

定義 1.3.7 (代数体) 有理数体 $\mathbb{Q}$ の有限次拡大体 K は **代数体** とよばれる.

このとき, K における $\mathbb{Z}$ の整閉包を $\mathcal{O}_K$ と書く.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

$n = [K: \mathbb{Q}]$ とおくと, $\mathcal{O}_K$ は階数 n の $\mathbb{Z}$ -加群である.

$I \subset K$ を $\mathcal{O}_K$ の分数イデアルとする. 注意 1.3.4 (iii) より, $I = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$ と書ける.

$(x_1, \dots, x_n)$ は一意的に存在するわけではない. しかし, $I = \mathbb{Z}x'_1 + \dots + \mathbb{Z}x'_n$ を別の表現とすると, $\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ $P \in GL_n(\mathbb{Z})$ となる.

よって, $d(x'_1, \dots, x'_n) \stackrel{\substack{\uparrow \\ \text{基底変換}}}{=} \det(P)^2 d(x_1, \dots, x_n) = d(x_1, \dots, x_n)$ となる.

したがって, $d(I) = d(x_1, \dots, x_n)$ とおくと, $d(I)$ は基底 $(x_1, \dots, x_n)$ の選び方に依存しておらず, **矛盾なく定まる**.

定義 1.3.8 (代数体の判別式) K を代数体とする.

$d_K = d(\mathcal{O}_K)$ は K の判別式とよぶ.

§ 2. デデキント環

§ 2.1. 二次体

二次体は $\mathbb{Q}$ の 2 次拡大のことである。例えば, $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$ は二次体である。

K を二次体とする。このとき, 平方因子を持たない $D \in \mathbb{Z} \setminus \{0, 1\}$ が存在し,

$K = \mathbb{Q}(\sqrt{D})$ が成り立つ。さらに, D は一意的に定まる。

定理 2.1.1. $D \neq 0, 1$ を平方因子を持たない有理整数とし, $K = \mathbb{Q}(\sqrt{D})$ とおく。

$$(i) \quad d_K = \begin{cases} D & \text{if } D \equiv 1 \pmod{4} \\ 4D & \text{if } D \equiv 2, 3 \pmod{4} \end{cases}$$

$$(ii) \quad \mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod{4} \\ \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod{4} \end{cases}$$

証明: $\text{Gal}(K/\mathbb{Q}) = \{\text{id}, \sigma\}$ と書く。 $x \in K$ とし, $x = a + b\sqrt{D}$ と書く ($a, b \in \mathbb{Q}$)。

P_x を x の $\mathbb{Q}$ 上の最小多項式とする。 すると,

$$\begin{aligned} P_x(t) &= (t-x)(t-\sigma x) = t^2 - (x+\sigma x)t + x\sigma x \\ &= t^2 - 2a t + (a^2 - Db^2) \end{aligned}$$

命題 1.3.6 より, $x \in \mathcal{O}_K \iff P_x \in \mathbb{Z}[X]$

$$\iff 2a \in \mathbb{Z} \text{ かつ } a^2 - Db^2 \in \mathbb{Z}$$

よって, $4Db^2 \in \mathbb{Z}$ となる。 D が平方因子を持たないのて, $b \in \frac{1}{2}\mathbb{Z}$ である。

また, $a^2 - Db^2 \in \mathbb{Z}$ より 次が成り立つ。

$$(2a)^2 \equiv (2b)^2 D \pmod{4}. \quad (*)$$

$a \in \frac{1}{2}\mathbb{Z}$ に対して, 以下のいずれかが成り立つ.

$$\begin{cases} a \in \mathbb{Z} \text{ ならば } (2a)^2 \equiv 0 \pmod{4} \text{ である.} \\ a \notin \mathbb{Z} \text{ ならば } (2a)^2 \equiv 1 \pmod{4} \text{ である.} \end{cases} \quad (**)$$

● $D \equiv 2, 3 \pmod{4}$ とする.

このとき, 上の (*) と (**) より $a \in \mathbb{Z}$ かつ $b \in \mathbb{Z}$ でないといけない.

$$\text{よって, } \mathcal{O}_K = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \sqrt{D}\mathbb{Z}$$

$$\text{ゆえに, } d_K = \begin{vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{vmatrix}^2 = 4D.$$

● $D \equiv 1 \pmod{4}$ とし, $D = 1 + 4k$ ($k \in \mathbb{Z}$) とする. また, $a = \frac{r}{2}$ と $b = \frac{s}{2}$ ($r, s \in \mathbb{Z}$) と書ける.

$$a^2 - Db^2 \in \mathbb{Z} \iff \frac{r^2}{4} - D\frac{s^2}{4} \in \mathbb{Z}$$

$$\iff \frac{r^2 - s^2}{4} \in \mathbb{Z}$$

$$\iff \frac{(r-s)(r+s)}{4} \in \mathbb{Z}$$

$$\iff r \equiv s \pmod{2}.$$

$$\text{よって, } \mathcal{O}_K = \left\{ \frac{r+s\sqrt{D}}{2} \mid \begin{array}{l} r, s \in \mathbb{Z} \\ r \equiv s \pmod{2} \end{array} \right\} = \mathbb{Z} + \mathbb{Z} \frac{1+\sqrt{D}}{2} = \mathbb{Z} \left[\frac{1+\sqrt{D}}{2} \right]$$

したがって,

$$d_K = \begin{vmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{vmatrix}^2 = D \quad \text{である.}$$

□

例 2.1.2

(a) $D = -1$ のとき, $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, $d_K = -4$ である.

$\mathbb{Z}[\sqrt{-1}]$ はユークリッド環である. 特に, $\mathbb{Z}[\sqrt{-1}]$ は単項イデアル整域である.

実際に, 写像 $\mathbb{Z}[i] \rightarrow \mathbb{N} \cup \{0\}$ ユークリッド関数である
 $z \mapsto |z|^2$

(b) $D = -5$ のとき, $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, $d_K = -20$ である.

$\mathbb{Z}[\sqrt{-5}]$ は一意分解整域でない.

なぜならば, $6 \in \mathbb{Z}[\sqrt{-5}]$ が既約元の積への分解は一意的でないからである.

すなわち, 次のように書ける:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

ここで $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ は既約元である (ただし, 素元でない).

$\mathbb{Z}[\sqrt{-5}]$ は一意分解環でないが, 次の性質をもつ.

$\mathbb{Z}[\sqrt{-5}]$ において, 任意のイデアルが素イデアルの積として一意に書くことができる.

例えば, 元 6 の代わりに, 単項イデアル (6) を考える.

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}) \quad \mathfrak{p}_2 = (3, 1 + \sqrt{-5}) \quad \mathfrak{p}_3 = (3, 1 - \sqrt{-5}) \quad \text{とおく.}$$

$\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ が素イデアルであることは簡単に確認できる.

$$\text{また, } \mathfrak{p}_1^2 = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) = (2)$$

$$\uparrow \quad 2 = 2 + 2\sqrt{-5} - [4 + (-4 + 2\sqrt{-5})]$$

$$\mathfrak{p}_2 \mathfrak{p}_3 = (9, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 6) = (3)$$

$$\uparrow \quad 3 = 9 - 6$$

$$\mathfrak{p}_1 \mathfrak{p}_2 = (6, 2+2\sqrt{5}, 3+3\sqrt{5}) = (1+\sqrt{5})$$

$$\mathfrak{p}_1 \mathfrak{p}_3 = (6, 2-2\sqrt{5}, 3-3\sqrt{5}) = (1-\sqrt{5})$$

よって,

$$\begin{aligned} (6) &= (2) \cdot (3) = (\mathfrak{p}_1^2)(\mathfrak{p}_2 \mathfrak{p}_3) \\ &= (1+\sqrt{5})(1-\sqrt{5}) = (\mathfrak{p}_1 \mathfrak{p}_2)(\mathfrak{p}_1 \mathfrak{p}_3) \quad \text{である.} \end{aligned}$$

つまり, 元 6 を既約元の積として表す表し方は 1 通りでないが,
イデアル (6) は 素イデアルの積として (順番を除いて) 一意的に
分解できる.

§2.2. 定義

定義 2.2.1. (デデキント環)

A を整域とする. A がデデキント環であるとは以下の3つ条件を満たすことをいう.

- (i) A はネーター環である.
- (ii) A は整閉である.
- (iii) 任意の素イデアル $\mathfrak{p} \neq 0$ は極大イデアルである.

ネーター環の復習

A を環とする. 以下の条件が互いに同値であることが証明できる.

- (i) A の任意のイデアル I が有限生成である(つまり, $I = A\alpha_1 + \dots + A\alpha_n$ と書ける).
- (ii) $I_1 \subset I_2 \subset I_3 \subset \dots$ をイデアルの昇鎖列とする. このとき, $N \geq 1$ があり, $I_N = I_{N+1} = I_{N+2} = \dots$ である.
- (iii) $\{I_j\}_{j \in J}$ ($J \neq \emptyset$) をイデアルの任意の族とする. このとき, この族が包含関係に閉する極大元を持つ. つまり, $j_0 \in J$ が存在し, 「 $\forall j \in J$ に対し, $I_{j_0} \subset I_j \Rightarrow I_{j_0} = I_j$ 」である.

上の条件を満たす環はネーター環とよぶ.

定理 2.2.2 (ヒルベルトの基底定理)

A がネーター環ならば, 多項式環 $A[t_1, \dots, t_n]$ もネーター環である

注意 2.2.3. A をネーター環とし, B を有限生成 A -代数とする.

このとき, B はネーター環である. なぜならば, B が $A[t_1, \dots, t_n]$ (ある $n \geq 1$) の商環として書くことができ, さらにネーター環の商環はネーター環であるからである.

命題 2.2.4: K を代数体とする. $\mathcal{O}_K$ はデデキント環である.

証明: 命題 1.3.3 より, $\mathcal{O}_K$ は有限生成 $\mathbb{Z}$ -加群である. 特に, $\mathcal{O}_K$ は有限生成 $\mathbb{Z}$ -代数であり, ゆえにネーター環である (注意 2.2.3 を参照).
系 1.1.6 より, $\mathcal{O}_K$ は整閉である. 最後に, 0でない任意の素イデアルが極イデアルであることを示す. $\mathfrak{p} \neq 0$ を $\mathcal{O}_K$ の素イデアルとする. まず, $\mathfrak{p} \cap \mathbb{Z} \neq 0$ を証明する.
 $x \in \mathfrak{p} \setminus \{0\}$ をとる. x は $\mathbb{Z}$ 上整であるので, $x^n + a_1 x^{n-1} + \dots + a_n = 0$ と書ける ($a_1, \dots, a_n \in \mathbb{Z}$).
また, $a_n \neq 0$ と仮定して良い. よって, $a_n = -x(x^{n-1} + a_1 x^{n-2} + \dots + a_{n-1}) \in \mathfrak{p} \cap \mathbb{Z}$ となる.
 $\mathfrak{p} \cap \mathbb{Z}$ は $\mathbb{Z}$ の素イデアルなので, $\mathfrak{p} \cap \mathbb{Z} = (p)$ (p : 素数) である. ゆえに,
剰余環 $\mathcal{O}_K/\mathfrak{p}$ は自然的に $\mathbb{F}_p$ -代数の構造をもつ. さらに, $\mathcal{O}_K$ は有限生成 $\mathbb{Z}$ -加群だから, $\mathcal{O}_K/\mathfrak{p}$ は有限生成 $\mathbb{F}_p$ -加群である. 特に, $\mathcal{O}_K/\mathfrak{p}$ は有限集合である.
任意の有限整域は有限体になる. したがって, $\mathcal{O}_K/\mathfrak{p}$ は有限体である.
以上より, $\mathfrak{p}$ は極大イデアルである. □

§2.3. 素イデアル分解

定理 2.3.1. A をデデキント環とする. I を非自明なイデアルとする (つまり, $I \neq 0, A$). このとき, 0 でない素イデアル $p_1, \dots, p_n$ があり,

$$I = p_1 p_2 \cdots p_n$$

が成り立つ. さらに, この分解は順序を除いて一意に定まる.

補題 2.3.2. $I \neq 0$ とする.

$p_1 p_2 \cdots p_n \subset I$ を満たす 0 でない素イデアル $p_1, \dots, p_n$ が存在する.

証明: ネーター環の性質 (iii) を使用する (参照「ネーター環の復習」)

上の条件を満たさないイデアル全体のなす集合を X とする. つまり,

$$I \not\subset X \iff 0 \text{ でない素イデアル } p_1, \dots, p_n \text{ があり, } p_1 \cdots p_n \subset I.$$

X が空集合でないと仮定する. ネーター環なので, X は包含関係に関する極大元 α をもつ.

$\alpha \in X$ より, α は素イデアルでない (素イデアルならば, $p_1 = \alpha$ とおくと $p_1 \subset \alpha$ が成り立つからである).

よって, $x_1, x_2 \in \alpha$ とする $x_1, x_2 \in A \setminus \alpha$ が存在する.

$$\begin{aligned}\alpha_1 &= \alpha + Ax_1 \\ \alpha_2 &= \alpha + Ax_2\end{aligned}$$

とおく. α が X の極大元だから, $\alpha_1, \alpha_2 \notin X$ である. よって, $p_1 \cdots p_n \subset \alpha_1$ が $p_1' \cdots p_n' \subset \alpha_2$

を満たす 0 でない素イデアル $p_1, \dots, p_n, p_1', \dots, p_n'$ がある. しかし, $\alpha_1 \alpha_2 \subset \alpha$ より,

$p_1 \cdots p_n p_1' \cdots p_n' \subset \alpha$ となり, $\alpha \in X$ を矛盾する.

以上より, X は空である. 補題が従う.

□

I を 0 でない A のイデアル とすると,

$$I^{-1} = \{x \in K \mid xI \subset A\}$$

とおく. $a \in I \setminus \{0\}$ ならば, $I^{-1} \subset \{x \in K \mid xa \in A\} = \frac{1}{a}A$ である.

よって, $aI^{-1} \subset A$ となる. したがって, I^{-1} は K の分数イデアルである.

K の 分数イデアル I , J の積 は イデアルの場合と同じように
定義されている. すなわち,

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid n \geq 1, a_i \in I, b_i \in J \right\}$$

と定義する. IJ は 分数イデアル である. なぜならば, $aI \subset A$ かつ $bJ \subset A$
を満たす $a, b \in K$ が あり, ゆえに $abIJ = (aI)(bJ) \subset A$ となるからである.

補題 2.3.3. $I \neq 0$ を イデアル とし, $\mathfrak{p} \neq 0$ を 素イデアル とする.

このとき, $I\mathfrak{p}^{-1} \neq I$ が 成り立つ.

証明:

① まず, $\mathfrak{p}^{-1} \neq A$ であることを示す.

$x \in \mathfrak{p}$ を 0 でない 元 とする. 補題 2.3.2 より, $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset (x) \subset \mathfrak{p}$

となる 0 でない 素イデアル $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$ が 存在する. さらに, n が 最小 である
と仮定して良い.

$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset \mathfrak{p}$ だから $\mathfrak{p}_i \subset \mathfrak{p}$ となる $1 \leq i \leq n$ が ある. 添字を付け直せば
 $i=1$ と仮定して良い. $\mathfrak{p}_1$ が 極大イデアル であるので, $\mathfrak{p} = \mathfrak{p}_1$ となる.

n が 最小 だから, $\mathfrak{p}_2 \cdots \mathfrak{p}_n \not\subset (x)$ である. よって, $y \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ かつ $y \notin (x)$

であるような 元 y が とれる. とくに, $x^{-1}y \notin A$ である. さらに,

$\mathfrak{p}y \subset \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset (x)$ であり, ゆえに $x^{-1}y\mathfrak{p} \subset A$ が 成り立つ.

このことより, $x^{-1}y \in \mathfrak{p}^{-1} \setminus A$ となり, とくに $\mathfrak{p}^{-1} \neq A$ である.

② 次に, $\mathcal{I}\mathcal{P}' \neq \mathcal{I}$ を証明する.

そのために $\mathcal{I}\mathcal{P}' = \mathcal{I}$ が成り立つと仮定する.

A がネーター環だから, $\mathcal{I} = Ax_1 + \dots + Ax_n$ と書ける. ところで, 任意の $x \in \mathcal{P}'$ に対して,

$$x x_i = \sum_{j=1}^n a_{ij} x_j \quad (a_{ij} \in A) \text{ と書ける.}$$

$$M = (a_{ij})_{1 \leq i, j \leq n} \text{ とおくと, } (xE_n - M) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \text{ となる.}$$

よくに, $xE_n - M$ は正則行列でない. ところで, $\det(xE_n - M) = 0$ である.

$\det(xE_n - M)$ は変数 x のモノミオムな多項式なので, x は A 上整である. A が整閉だから $x \in A$

となる. ところで, $\mathcal{P}' \subset A$ であり, ゆえに $\mathcal{P}' = A$ である (明かに $A \subset \mathcal{P}'$ が成り立つからだ).

このことは ① に矛盾する. ところで, $\mathcal{I}\mathcal{P}' \neq \mathcal{I}$ である. □

系 2.3.4. $\mathcal{P} \neq 0$ を素イデアルとする.

$$\mathcal{P}\mathcal{P}' = A \text{ である.}$$

証明: 補題 2.3.3 より $\mathcal{P} \neq \mathcal{P}\mathcal{P}' \subset A$ が成り立つ.

$\mathcal{P}$ が極大イデアルなので $\mathcal{P}\mathcal{P}' = A$ となる

□

補題 2.3.5. $I \neq 0, A$ とする. $I = p_1 p_2 \cdots p_n$ を満たす素イデアル $p_1, \dots, p_n$ が存在する.

証明: 以下の集合を考える.

$$X = \left\{ I \mid \begin{array}{l} I \text{ が非自明なイデアルである} \\ I \text{ が素イデアル分解をもたない} \end{array} \right\}$$

$X \neq \emptyset$ を仮定する. A はネーター環なので, X は極大元 α をもつ.

$\alpha \subset \mathfrak{p}$ となる極大イデアル $\mathfrak{p}$ が存在する. $\alpha \in X$ より, $\alpha \neq \mathfrak{p}$ である.

このとき, $\alpha \subset \alpha \mathfrak{p}' \subset \mathfrak{p} \mathfrak{p}' = A$ である.

補題 2.3.3 より $\alpha \not\subset \alpha \mathfrak{p}'$ が成り立つ. また, α が X の極大元

だから, $\alpha \mathfrak{p}' \notin X$ である. ゆえに, $\alpha \mathfrak{p}' = p_1 p_2 \cdots p_n$ に分解できる

($p_1, p_2, \dots, p_n$ は素イデアルである). したがって, $\alpha = \alpha \mathfrak{p}' \mathfrak{p} = p_1 p_2 \cdots p_n \mathfrak{p}$

となり, $\alpha \in X$ に矛盾する. よって, $X = \emptyset$ であり, 補題が従う. $\square$

補題 2.3.5. $I \neq 0, A$ とする. I の素イデアル分解は一意的である.

つまり, $I = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ ($p_1, \dots, p_n, q_1, \dots, q_m$ は素イデアル) ならば,

$n = m$ であり, かつ順序を除いて $p_1, \dots, p_n$ と $q_1, \dots, q_m$ が一致する.

証明: とくに, $p_1 p_2 \cdots p_n \subset q_1$ が成り立つ.

q_1 が素イデアルなので, $p_i \subset q_1$ を満たす i がある. また, $i=1$ を仮定して

良い. p_1 が極大イデアルだから, $p_1 = q_1$ となる. 両辺に p_1' をかけると,

$p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$ となる. この議論を繰り返すと, 結果がわかる. $\square$

§ 2.4. イデアル 類群

A を デデキント環 とし, A の 商体 を K とおく.

$$J_K = \{ A \text{ の 分数イデアル} \} \quad (\text{注意: } 0 \text{ は 分数イデアルでない と 約束する})$$

とする. J_K は 分数イデアルの積に関して閉じている.

命題 2.4.1

(i) J_K は アベル 群 をなす. 単位元は A であり, 分数イデアル I の逆元は

$$I^{-1} = \{ x \in K \mid xI \subset A \} \quad \text{である. } J_K \text{ は イデアル群 と 呼ばれる.}$$

(ii) 任意の分数イデアル I は 一意的に

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \quad (v_{\mathfrak{p}}(I) \in \mathbb{Z}, \text{ 有限個の } \mathfrak{p} \text{ を除いて } v_{\mathfrak{p}}(I) = 0 \text{ である}). \quad (*)$$

と表すことができる. 注意

証明

(i) I を イデアル とする. 定理 2.3.1 より $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ と書ける ($\mathfrak{p}_1, \dots, \mathfrak{p}_n$: 素イデアル).
 $I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$ とおくと $II^{-1} = A$ となり, ゆえに I が J_K において可逆元である. $I^{-1} = I^{-1}$ を示す.
 $II^{-1} = A$ だから, $I^{-1} \subset I^{-1}$ である. 逆に, $x \in I^{-1}$ とすると, $xI \subset A$ であり,
 $xII^{-1} \subset I^{-1}$ となる. ここで, $II^{-1} = A$ だから $x \in I^{-1}$ が成り立つ.

次に, I を 分数イデアル とする. このとき, $aI \subset A$ となる $a \in A \setminus \{0\}$ がとれる.

aI が A の イデアル なので, J_K において可逆元であり, さらに $(aI)^{-1}(aI) = A$
 $(aI)^{-1} = \{ x \in K \mid xaI \subset A \} = a^{-1}I^{-1}$ により, $a a^{-1} I I^{-1} = I I^{-1} = A$ を得る.

(ii) イデアル の 場合は, 主張が 定理 2.3.1 から従う.

I を 分数イデアル とし, $aI \subset A$ となる $a \in A \setminus \{0\}$ をとる. aI と (a) は 素イデアル分解をもつので
 $aI = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(aI)}, \quad (a) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(a)}$ と書ける.

ゆえに, $I = (a)^{-1}(aI) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(aI) - v_{\mathfrak{p}}(a)}$ となる. よって, $(*)$ のような分解が存在する.

さらに, この分解は 一意的である. □

定義 2.4.2. (イデアル類群)

$(x) = xA \quad (x \in K)$ のような分数イデアルは単項分数イデアルとよぶ.

単項分数イデアル全体のなす集合を P_K とおくと, P_K は J_K の部分群をなす.

イデアル類群とは, 商群 $\mathcal{C}_K = J_K / P_K$ のことをいう.

注意 2.4.3

(i) 命題 2.4.1 より, J_K は自由群である.

つまり, $J_K \simeq \mathbb{Z}^{(X)}$ $X = \{x \neq 0 \mid x \text{ 素イデアル} \}$ である.

(ii) A が単項イデアル整域 $\Leftrightarrow P_K = J_K \Leftrightarrow \mathcal{C}_K = 0$.

§3. ミンコフスキー理論

§3.1. ミンコフスキー空間

K を代数体とし, $n = [K: \mathbb{Q}]$ とする.
埋め込み $\tau: K \hookrightarrow \mathbb{C}$ はちょうど n 個存在する.

$$K_{\mathbb{C}} = \prod_{\substack{\tau \\ (\tau: K \hookrightarrow \mathbb{C})}} \mathbb{C} \quad \text{とおく.}$$

自然な写像 $j: K \rightarrow K_{\mathbb{C}}$ が得られる.
 $x \mapsto (\tau(x))_{\tau}$

$K_{\mathbb{C}}$ のヘルミット内積は $\langle x, y \rangle = \sum_{\tau} x_{\tau} \overline{y_{\tau}}$ で定義される.

$$\begin{aligned} \text{Tr}: K_{\mathbb{C}} &\longrightarrow \mathbb{C} \\ (x_{\tau})_{\tau} &\longmapsto \sum_{\tau} x_{\tau} \end{aligned}$$

とおくと, $\text{Tr}(j(x)) = \sum_{\tau} \tau(x) = \text{Tr}_{K/\mathbb{Q}}(x) \quad (x \in K)$ が成り立つ.

ガロワ群 $\text{Gal}(\mathbb{C}/\mathbb{R})$ が $\{\tau: K \hookrightarrow \mathbb{C} \text{ 埋め込み}\}$ に作用する.

$\tau: K \hookrightarrow \mathbb{C}$ が与えられているとき, $\bar{\tau}$ を $\bar{\tau}(x) = \overline{\tau(x)}$ で定める.

また, $z = (z_{\tau})_{\tau} \in K_{\mathbb{C}}$ に対して, $F(z) = (\bar{z}_{\bar{\tau}})_{\tau}$ とおくと, 写像

$$F: K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}}$$

が得られる.

$\langle Fx, Fy \rangle = \sum_{\tau} \bar{x}_{\bar{\tau}} y_{\tau} = \overline{\langle x, y \rangle}$ が成り立つことを注意せよ.

$K_{\mathbb{R}} \subset K_{\mathbb{C}}$ を次のように定義する.

$$K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \mid F(z) = z\}$$

と置く. すなわち, $K_{\mathbb{R}}$ は $z_{\tau} = \bar{z}_{\bar{\tau}}$ となる $z = (z_{\tau})_{\tau}$ からなる部分集合.

明かに, $K_{\mathbb{R}}$ は $\mathbb{R}$ ベクトル空間である.

$x \in K$ に対して, $z = (x)_{\tau}$ とおくと, $F(z) = (\bar{x}_{\bar{\tau}})_{\tau} = (x)_{\tau} = z$ により, $z \in K_{\mathbb{R}}$ である.

したがって, j は写像 $j: K \longrightarrow K_{\mathbb{R}}$ を誘導する.

$x, y \in K_{\mathbb{R}}$ に対して, $\langle x, y \rangle = \langle Fx, Fy \rangle = \overline{\langle x, y \rangle}$ が成り立つので, $\langle x, y \rangle \in \mathbb{R}$ となる.

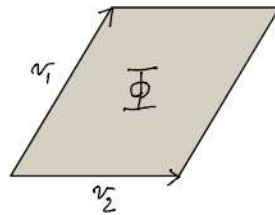
よって, 内積 $K_{\mathbb{R}} \times K_{\mathbb{R}} \longrightarrow \mathbb{R}$ が得られる.
 $(x, y) \longmapsto \langle x, y \rangle$

$K_{\mathbb{R}}$ は n 次元ユークリッド空間であり, ミンコフスキー空間と大抵等しい.

$v_1, \dots, v_n \in K_{\mathbb{R}}$ を線型独立なベクトルとする。このとき、集合

$$\Phi = \Phi(v_1, \dots, v_n) = \{x_1 v_1 + \dots + x_n v_n \mid 0 \leq x_i < 1\}$$

は 平行四辺形 という



$(e_1, \dots, e_n)$ を正規直交基底とする。また、 $A = (a_{ij})_{1 \leq i, j \leq n}$ を $(e_1, \dots, e_n)$ から $(v_1, \dots, v_n)$ への基底の変換行列とする。このとき、 Φ の体積は

$$\text{vol}(\Phi) = |\det(A)|$$

である。

定義 3.1.1. (格子) V を n 次元 $\mathbb{R}$ ベクトル空間とする. V の格子とは

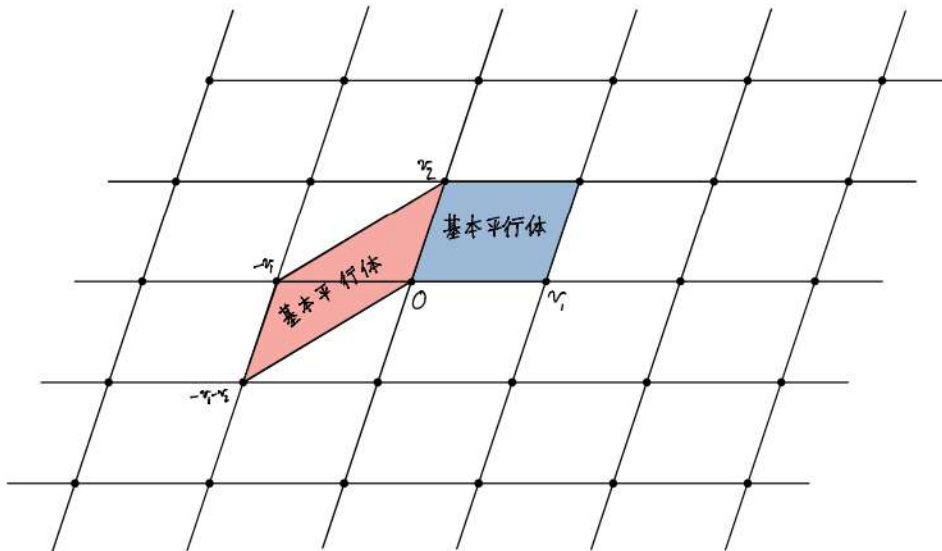
$$\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m \quad (v_1, \dots, v_m \text{ 線型独立})$$

という形の部分群のことをいう. さらに, $m=n$ のとき, Γ は完全格子であるという.

$\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m$ ($v_1, \dots, v_m$ 線型独立) のとき, $v_1, \dots, v_m$ は Γ の基底とよぶ. このとき, $(v_1, \dots, v_m)$ で定まる平行四辺形

$$\Phi(v_1, \dots, v_m) = \left\{ \sum_{i=1}^m \lambda_i v_i \mid 0 \leq \lambda_i < 1 \right\}$$

は Γ の基本平行体という.



$\mathbb{Z}v_1 + \mathbb{Z}v_2 = \mathbb{Z}v_2 + \mathbb{Z}(-v_1 - v_2)$ などが成り立つから,
格子の基底と基本平行体は一意的に存在するわけではない.

Γ を $\mathbb{K}_{\mathbb{R}}$ の完全格子とする. Γ の体積 $\text{vol}(\Gamma)$ は次のように定義される. $(v_1, \dots, v_n)$ を Γ の基底とする (つまり, $\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$).
このとき,

$$\text{vol}(\Gamma) = \text{vol}(\Phi(v_1, \dots, v_n))$$

ここで定義する $\text{vol}(\Gamma)$ が 基底 $(v_1, \dots, v_n)$ の選び方に依存しないことを注意する。

実際に, $\Gamma = \mathbb{Z}v'_1 + \dots + \mathbb{Z}v'_n$ ならば, $P \in GL_n(\mathbb{Z})$ を用いて $\begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = P \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ となる.

$|\det(P)| = 1$ より, $\text{vol}(\Phi(v'_1, \dots, v'_n)) = \text{vol}(\Phi(v_1, \dots, v_n))$ である.

補題 3.1.2 Γ を完全格子とし, $\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ とする.

このとき, $\text{vol}(\Gamma) = \left| \det((\langle v_i, v_j \rangle)_{1 \leq i, j \leq n}) \right|^{1/2}$ である.

証明: $(e_1, \dots, e_n)$ を $K_{\mathbb{R}}$ の正規直交基底とする.

$A = (a_{ij})_{i,j}$ を $e_1, \dots, e_n$ から $v_1, \dots, v_n$ への基底の変換行列とする.

つまり, $v_i = \sum_{k=1}^n a_{ik} e_k$ ($a_{ik} \in \mathbb{R}$) である. このとき,

$$\begin{aligned} (\langle v_i, v_j \rangle)_{1 \leq i, j \leq n} &= \left(\sum_{k, l} a_{ik} a_{jl} \langle e_k, e_l \rangle \right)_{1 \leq i, j \leq n} \\ &= \left(\sum_{k=1}^n a_{ik} a_{jk} \right)_{1 \leq i, j \leq n} = A^t A \quad \text{である.} \end{aligned}$$

よって, $B = (\langle v_i, v_j \rangle)_{i,j}$ とおくと $\det(B) = \det(A)^2$. ゆえに,

$\text{vol}(\Gamma) = |\det(A)| = \det(B)^{1/2}$ である.

補題 3.1.3 σ を $\mathcal{Q}_K$ のイデアルとする. このとき,

$$d(\sigma) = [\mathcal{Q}_K : \sigma]^2 d_K \quad \text{である} \quad (\text{ここから, } [\mathcal{Q}_K : \sigma] = |\mathcal{Q}_K / \sigma| \text{ である}).$$

証明:

$M \subset \mathbb{Z}^n$ が階数 n の部分群ならば, $M = \mathbb{Z}d_1e_1 \oplus \mathbb{Z}d_2e_2 \oplus \dots \oplus \mathbb{Z}d_ne_n$ となる

$\mathbb{Z}^n$ の基底 $(e_1, \dots, e_n)$, 整数 $d_1, \dots, d_n \in \mathbb{Z}$ が存在する. よって, $\mathbb{Z}_M^n \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_n}$

となり, ゆえに $|\mathbb{Z}_M^n| = d_1 d_2 \dots d_n$ である.

σ も $\mathcal{O}_K$ も階数 $n = [K:\mathbb{Q}]$ の自由 $\mathbb{Z}$ 加群である (注意 1.3.4. (ii)). したがって,

$e_1, \dots, e_n \in \mathcal{O}_K$, $d_1, \dots, d_n \in \mathbb{Z}$ が存在し, $\mathcal{O}_K = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n$ から $\sigma = \mathbb{Z}d_1e_1 \oplus \dots \oplus \mathbb{Z}d_ne_n$ である.

よって, $\sigma_1, \dots, \sigma_n$ を埋め込み $K \hookrightarrow \mathbb{C}$ とすると,

$$\begin{aligned} d(\sigma) &= d(d_1e_1, \dots, d_ne_n) = \det \left((\sigma_i(d_je_j))_{1 \leq i, j \leq n} \right)^2 \\ &= (d_1 \dots d_n)^2 \det \left((\sigma_i(e_j))_{1 \leq i, j \leq n} \right) = [\mathcal{O}_K: \sigma]^2 d(\mathcal{O}_K). \quad \square \end{aligned}$$

写像 $j: K \rightarrow K_{\mathbb{R}}$ を考える. $x_1, \dots, x_n \in K$ が K の基底ならば,
 $x \mapsto (\sigma(x))_{\mathbb{C}}$

$jx_1, \dots, jx_n$ は $\mathbb{R}$ ベクトル空間 $K_{\mathbb{R}}$ の基底になることを説明する.

埋め込み $K \hookrightarrow \mathbb{C}$ を $e_1, \dots, e_n$ と書くと

$$\begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \sigma_2(x_2) & \dots & \sigma_2(x_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(x_1) & \sigma_n(x_2) & \dots & \sigma_n(x_n) \end{vmatrix} = d(x_1, \dots, x_n) \neq 0$$

← 命題 1.2.4

よって, $jx_1, \dots, jx_n$ は $\mathbb{C}$ ベクトル空間 $K_{\mathbb{C}}$ の基底をなす. $\mathbb{C}$ 上線型独立だから,

とくに $\mathbb{R}$ 上線型独立である. $\dim_{\mathbb{R}}(K_{\mathbb{R}}) = n$ より, $jx_1, \dots, jx_n$ は $K_{\mathbb{R}}$ の基底をなす.

このことから,

$$j(\mathbb{Z}x_1 + \dots + \mathbb{Z}x_n) = \mathbb{Z}jx_1 + \dots + \mathbb{Z}jx_n$$

は $K_{\mathbb{R}}$ の完全格子である. とくに, σ を $\mathcal{O}_K$ のイデアルとすると $j(\sigma)$ は $K_{\mathbb{R}}$ の完全格子である.

命題 3.1.4 σ を 0 でない $\mathcal{O}_K$ のイデアルとし, $\Gamma = j(\sigma)$ とおく. このとき,

$$\text{vol}(\Gamma) = \sqrt{|d_K|} \cdot [\mathcal{O}_K : \sigma] \quad (\text{ここで } [\mathcal{O}_K : \sigma] = |\mathcal{O}_K / \sigma| \text{ である}).$$

証明: $n = [K : \mathbb{Q}]$ ($K/\mathbb{Q}$ の次数) とする.

注意 1.3.4 (ii) より $\sigma = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$ となる $\alpha_1, \dots, \alpha_n$ が存在する.

そこで, $\Gamma = \mathbb{Z}j\alpha_1 + \dots + \mathbb{Z}j\alpha_n$ である. $\{\tau_1, \dots, \tau_n\}$ を埋め込み $K \hookrightarrow \mathbb{C}$ 全体の集合とする.

σ の判別式は $d(\sigma) = \det((\tau_i(\alpha_k))_{1 \leq i, k \leq n})^2 = [\mathcal{O}_K : \sigma]^2 d_K$ である.

$A = (\tau_k(\alpha_i))_{1 \leq i, k \leq n}$ とおくとき,

$$(\langle j\alpha_i, j\alpha_k \rangle)_{1 \leq i, k \leq n} = \left(\sum_{r=1}^n \tau_r(\alpha_i) \overline{\tau_r(\alpha_k)} \right)_{1 \leq i, k \leq n} = A \cdot {}^t \bar{A} \quad \text{となる}$$

$$\text{よって, } \text{vol}(\Gamma) = \det((\langle j\alpha_i, j\alpha_k \rangle)_{1 \leq i, k \leq n})^{1/2}$$

$$= |\det A|$$

$$= \sqrt{|d_K|} [\mathcal{O}_K : \sigma] \quad \text{となる}$$

□

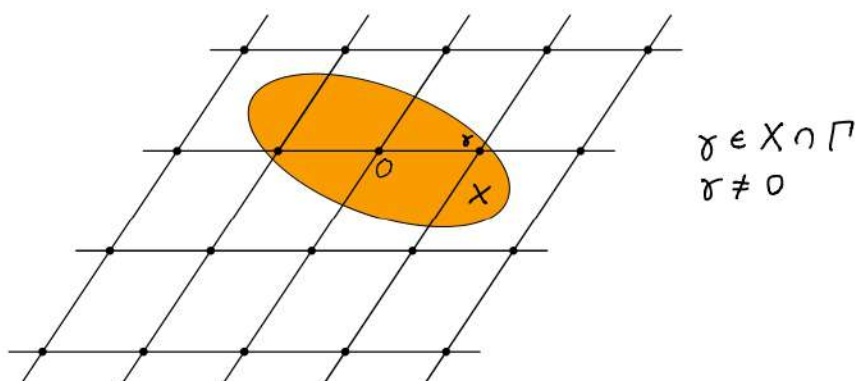
§3.2. ミンコフスキーの格子点定理

定理 3.2.1. Γ を $K_{\mathbb{R}}$ (あるいは, 一般のユークリッド空間) の完全格子とす.

また, $X \subset K_{\mathbb{R}}$ を次の条件を満たす部分集合とす

- (i) $x \in X$ ならば $-x \in X$ である
- (ii) X は $\square$ である (つまり, $x, y \in X, 0 \leq t < 1$ のとき $tx + (1-t)y \in X$).
- (iii) $\text{vol}(X) > 2^n \text{vol}(\Gamma)$ である.

このとき, X においては, 0 でない $\gamma \in \Gamma$ が存在する.



証明: $\gamma \in \Gamma$ について, 集合 $\frac{1}{2}X + \gamma = \{\frac{1}{2}x + \gamma \mid x \in X\}$ を考える.

$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$ となる互いに異なる $\gamma_1, \gamma_2 \in \Gamma$ が存在することを示せばよい.

なぜならは, $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$ ($x_1, x_2 \in X$) と書ける. ゆえに, $\gamma = \gamma_1 - \gamma_2$ とおくと,

$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}(x_2 - x_1)$ である. $\frac{1}{2}(x_2 - x_1)$ は x_2 と $-x_1$ の中点だから, 仮定 (i) と (ii) より $\gamma \in X$ である.

$(\frac{1}{2}X + \gamma)_{\gamma \in \Gamma}$ がいずれも互いに共通部分をもたないとする.

Φ を Γ の基本平行体とする. $\Phi \supset \bigsqcup_{\gamma \in \Gamma} \Phi \cap (\frac{1}{2}X + \gamma)$ より,

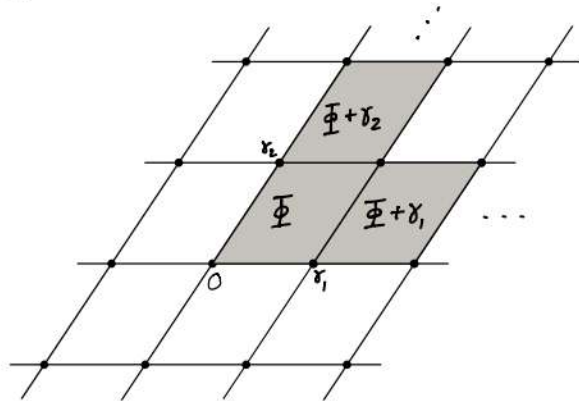
$$\text{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \text{vol}(\Phi \cap (\frac{1}{2}X + \gamma)).$$

全ての $v \in K_{\mathbb{R}}$, $Y \subset K_{\mathbb{R}}$ に対して, $\text{vol}(Y) = \text{vol}(Y+v)$ より

$$\text{vol}(\Phi \cap (\tfrac{1}{2}X + \gamma)) = \text{vol}((\Phi - \gamma) \cap \tfrac{1}{2}X) \text{ である.}$$

よって, $\text{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \text{vol}((\Phi - \gamma) \cap \tfrac{1}{2}X)$ となる.

また, $\bigsqcup_{\gamma \in \Gamma} (\Phi - \gamma) = K_{\mathbb{R}}$ が成り立つ.



よって, $\tfrac{1}{2}X = \bigsqcup_{\gamma \in \Gamma} ((\Phi - \gamma) \cap \tfrac{1}{2}X)$ であり, ゆえに

$$\text{vol}(\tfrac{1}{2}X) = \sum_{\gamma \in \Gamma} \text{vol}((\Phi - \gamma) \cap \tfrac{1}{2}X) \text{ である}$$

以上より, $\text{vol}(\Phi) \geq \text{vol}(\tfrac{1}{2}X) = \tfrac{1}{2^n} \text{vol}(X)$ となり,

仮定 (iii) に矛盾する. 定理が従う.

□

K を代数体とし, $n = [K:\mathbb{Q}]$ とおく.

埋め込み $\tau: K \hookrightarrow \mathbb{C}$ が実埋め込みであるとは, $\tau(K)$ が $\mathbb{R}$ に含まれることをいう.

τ は実埋め込みでないとき, 虚埋め込みであるという. 明らかに,

$$\tau \text{ が実埋め込みである} \iff \tau = \bar{\tau}$$

実埋め込みの個数は r とおくことにする.

虚埋め込みの個数は常に偶数である. なぜならば, 虚埋め込みは複素共役のペア $\sigma_1, \bar{\sigma}_1, \sigma_2, \bar{\sigma}_2, \dots, \sigma_s, \bar{\sigma}_s$ になっているからである.

複素共役のペアの個数は s とおくことにする. つまり, 虚埋め込みの個数は $2s$ である. よって,

$$n = r + 2s$$

例 3.2.2 $\alpha = \sqrt[3]{2}$ とおき, $K = \mathbb{Q}(\alpha)$ とする.

$[K:\mathbb{Q}] = 3$ より, ちょうど3つの埋め込み $K \hookrightarrow \mathbb{C}$ が存在する.

$\tau: K \hookrightarrow \mathbb{C}$ を埋め込みとすると, $\tau(\alpha)$ は $X^3 - 2$ の根である.

$$X^3 - 2 = (X - \alpha)(X - \alpha j)(X - \alpha j^2) \quad (j = e^{\frac{2\pi i}{3}})$$

τ_1, τ_2, τ_3 をそれぞれ $\tau_1(\alpha) = \alpha, \tau_2(\alpha) = \alpha j, \tau_3(\alpha) = \alpha j^2$ で定まる埋め込みとする. $\bar{\tau}_1 = \tau_1, \bar{\tau}_2 = \tau_3, \bar{\tau}_3 = \tau_2$ である. よって, $r = 1, s = 1$ である.

定理 3.2.3. $\mathcal{O}$ を 0 でない $\mathbb{Q}_K$ のイデアルとする. また, $(c_\tau)_\tau$ ($c_\tau > 0$) を実数の族とする ($\tau = \bar{\tau}$ し, τ は埋め込み $K \hookrightarrow \mathbb{C}$ 全体の集合を走る).

$(c_\tau)_\tau$ は以下の条件を満たすとする.

$$(i) \quad c_\tau = c_{\bar{\tau}} \quad (\tau: K \hookrightarrow \mathbb{C})$$

$$(ii) \quad \prod_{\tau} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} [\mathbb{Q}_K: \mathbb{Q}]$$

このとき,

$$|\tau(a)| < c_\tau \quad (\forall \tau: K \hookrightarrow \mathbb{C})$$

を満たす $a \in \mathcal{O} \setminus \{0\}$ が存在する.

証明の準備

$\rho_1, \dots, \rho_n$ を K の実埋め込みとする. また, $\sigma_1, \dots, \sigma_s$ を互いに複素共役でない K の虚埋め込みとする.

$z = (z_\tau)_\tau \in K_{\mathbb{R}}$ に対し, $x = (x_\tau)_\tau$ を次のように定める.

- τ が実埋め込みならば, $x_\tau = z_\tau$ と定める.
- $\tau = \sigma_i$ ($1 \leq i \leq s$) ならば, $x_\tau = \operatorname{Re}(z_\tau)$ と定める.
- $\tau = \bar{\sigma}_i$ ($1 \leq i \leq s$) ならば, $x_\tau = \operatorname{Im}(z_\tau)$ と定める.

$f(z) = (x_\tau)_\tau$ とおくことで写像

$$f: K_{\mathbb{R}} \longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^n$$

が得られる. 明かに, $\ker(f) = 0$ だから, f は $\mathbb{R}$ ベクトル空間の同型である.

補題 3.2.4 埋め込み τ に対して, a_τ を

$$a_\tau = \begin{cases} 1 & \text{if } \tau \text{ が実埋め込みである} \\ 2 & \text{if } \tau \text{ が虚埋め込みである} \end{cases} \quad \text{で定義する.}$$

また, $x = (x_\tau)_\tau, y = (y_\tau)_\tau \in \prod_{\tau} \mathbb{R}$ に対し $\langle x, y \rangle' = \sum_{\tau} a_\tau x_\tau y_\tau$ とおくことで

$\prod_{\tau} \mathbb{R}$ に内積が得られる. このとき, 同型 $f: K_{\mathbb{R}} \rightarrow \prod_{\tau} \mathbb{R}$ は $K_{\mathbb{R}}$ の内積 $\langle, \rangle$ を内積 $\langle, \rangle'$ に移す. つまり, $z_1, z_2 \in K_{\mathbb{R}}$ に対して, $\langle z_1, z_2 \rangle = \langle f(z_1), f(z_2) \rangle'$ が成り立つ.

証明:

$z = (z_\tau)_\tau, z' = (z'_\tau)_\tau \in K_{\mathbb{R}}$ とし, $z_\tau = a_\tau + ib_\tau, z'_\tau = a'_\tau + ib'_\tau$ と書く ($a_\tau, b_\tau, a'_\tau, b'_\tau \in \mathbb{R}$)

$\tau = \sigma_i$ のとき,

$$\begin{aligned}
 z_z \bar{z}'_z + z_{\bar{z}} \bar{z}'_{\bar{z}} &= \bar{z}_z \bar{z}'_z + \bar{z}_{\bar{z}} z'_z = (a_z + i b_z)(a'_z - i b'_z) + (a_z - i b_z)(a'_z + i b'_z) \\
 &= 2(a_z a'_z + b_z b'_z) \\
 &= 2(x_z x'_z + x_{\bar{z}} x'_{\bar{z}})
 \end{aligned}$$

$$\text{よ, } \mathcal{L} \quad \langle z, z' \rangle = \sum_z z_z \bar{z}'_z = \sum_{z \text{ 実}} x_z x'_z + 2 \sum_{z \text{ 虚}} x_z x'_z \quad z' \text{ あり.}$$

$$= \langle f(z), f(z') \rangle' \quad \square$$

$(v_1, \dots, v_n)$ を $K_{\mathbb{R}}$ の正規直交基底とする. 補題 3.2.4. より, $(f(v_1), \dots, f(v_n))$

は内積 $\langle, \rangle'$ に関する正規直交基底である.

$(e^z)_z$ を $\prod_z \mathbb{R}$ の標準基底とする. すなわち, $e^z = (\delta_{z,z'})_{z'}$, $\delta_{zz'} = \begin{cases} 0 & \text{if } z \neq z' \\ 1 & \text{if } z = z' \end{cases}$.

このとき, $\left(\frac{1}{\sqrt{a_z}} e^z\right)_z$ は内積 $\langle, \rangle'$ に関して正規直交基底である.

$$\begin{array}{ccc} \sum_{i=1}^n \lambda_i v_i & K_{\mathbb{R}} & \xrightarrow[\sim]{f} \prod_z \mathbb{R} \\ \uparrow & \uparrow \lambda & \downarrow \cong \\ (\lambda_1, \dots, \lambda_n) & \mathbb{R}^n & \xrightarrow[A]{} \mathbb{R}^n \end{array}$$

行列

集合 $Y \subset \mathbb{R}^n$ に対し, $\text{vol}_{\mathbb{R}^n}(A(Y)) = |\det A| \text{vol}_{\mathbb{R}^n}(Y)$ である.

また, $\det A = \prod_z \frac{1}{\sqrt{a_z}} = \sqrt{\frac{1}{2^{2s}}} = 2^{-s}$ である.

よって, 集合 $X \subset K_{\mathbb{R}}$ に対し,

$$\text{vol}_{\mathbb{R}^n}(f(X)) = 2^{-s} \text{vol}_{K_{\mathbb{R}}}(X)$$

が成り立つ.

定理 3.2.3 の証明

$$X = \left\{ (z_z)_z \in K_{\mathbb{R}} \mid |z_z| < c_z \right\}$$

と定めると, X は $[x \in X \Rightarrow -x \in X]$ を満たし, さらに凸集合である.

$\Gamma = j(\alpha)$ とおく. Γ は $K_{\mathbb{R}}$ の完全格子である. 定理 3.2.1 より,

$\text{vol}(X) > 2^n \text{vol}(\Gamma)$ を示せば良い.

同型 $f: K_{\mathbb{R}} \xrightarrow{\sim} \prod_z \mathbb{R}$ による X の像を考える.

$$f(X) = \left\{ (x_z)_z \in \prod_z \mathbb{R} \mid \begin{array}{ll} -c_z < x_z < c_z & \text{if } z \text{ が実埋め込み} \\ x_z^2 + x_{\bar{z}}^2 < c_z^2 & \text{if } z = \sigma_i \text{ (15155)} \end{array} \right\}$$

よって,

$$\begin{aligned} \text{vol}(X) &= 2^s \text{vol}(f(X)) \\ &= 2^s \cdot \left(2^r \prod_{z \neq \bar{z}} c_z \right) \cdot \left(\prod_{i=1}^s \pi c_{\sigma_i}^2 \right) \\ &= 2^{r+s} \pi^s \left(\prod_z c_z \right) \\ &> 2^{r+s} \pi^s \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} [Q_K: \sigma] \\ &= 2^n \text{vol}(\Gamma) \end{aligned}$$

定理から従う.

□

§3.3. 絶対ノルム

命題 3.3.1 σ を 0 でない Q_K のイデアルとする.

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} [Q_K: \sigma]$$

を満たす $a \in \sigma \setminus \{0\}$ が存在する.

証明: 小さい $\varepsilon > 0$ をとる.

$$c_z = c_{\bar{z}} \quad \text{かつ} \quad \prod_z c_z = \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} [Q_K: \sigma] + \varepsilon$$

を満たす正の実数 $(c_z)_z$ がとれる. 定理 3.2.3 より

$$|z(a)| < c_z \quad (z: K \hookrightarrow \mathbb{C})$$

となる $a \in \sigma \setminus \{0\}$ が存在する. よって,

$$|N_{K/\mathbb{Q}}(a)| = \prod_z |z(a)| < \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} [Q_K: \sigma] + \varepsilon$$

$N_{K/\mathbb{Q}}(a) \in \mathbb{Z}$ なのだから, $|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} [Q_K: \sigma]$ となる $a \in \sigma \setminus \{0\}$ が

存在する.

□

実は、より強力な結果が証明できる:

定理 3.3.2 α を 0 でない $\mathcal{O}_K$ のイデアルとする. このとき,

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^S \sqrt{|d_K|} [\mathcal{O}_K : \alpha]$$

を満たす $\alpha \in \alpha \setminus \{0\}$ が存在する.

定義 3.3.3 $\alpha \neq 0$ を $\mathcal{O}_K$ のイデアルとする. α の絶対ノルム $N(\alpha)$ は

$$N(\alpha) = [\mathcal{O}_K : \alpha] \quad \text{で定める.}$$

補題 3.3.4

(i) α を 0 でない $\mathcal{O}_K$ の元とする. このとき, $N(\alpha \mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$ である.

(ii) $\alpha \neq 0$ をイデアルとし, $\alpha = \mathfrak{p}_1^{k_1} \mathfrak{p}_2^{k_2} \cdots \mathfrak{p}_r^{k_r}$ を α の素イデアル分解とする. このとき,

$$N(\alpha) = N(\mathfrak{p}_1)^{k_1} N(\mathfrak{p}_2)^{k_2} \cdots N(\mathfrak{p}_r)^{k_r} \quad \text{である.}$$

証明:

(i) $\mathcal{O}_K = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$ となる $x_1, \dots, x_n \in \mathcal{O}_K$ がとれる.

よって, $\alpha \mathcal{O}_K = \mathbb{Z}\alpha x_1 \oplus \cdots \oplus \mathbb{Z}\alpha x_n$ である.

補題 3.1.3. より, $d(\alpha \mathcal{O}_K) = [\mathcal{O}_K : \alpha \mathcal{O}_K]^2 d_K$ である.

一方,

$$d(\alpha \mathcal{O}_K) = d(\alpha x_1, \dots, \alpha x_n) = \begin{vmatrix} \tau_1(\alpha x_1) & \cdots & \tau_1(\alpha x_n) \\ \tau_2(\alpha x_1) & \cdots & \tau_2(\alpha x_n) \\ \vdots & & \vdots \\ \tau_n(\alpha x_1) & \cdots & \tau_n(\alpha x_n) \end{vmatrix}^2$$

($\tau_1, \dots, \tau_n$ は埋め込み $K \hookrightarrow \mathbb{C}$ である)

$$= \left(\prod_{i=1}^n \varepsilon_i(\alpha) \right)^2 d_K = N_{K/\mathbb{Q}}(\alpha)^2 d_K$$

よって, $N(\alpha \mathcal{O}_K) = [\mathcal{O}_K : \alpha \mathcal{O}_K] = |N_{K/\mathbb{Q}}(\alpha)|$ となる.

(ii) $\mathfrak{p}_1^{k_1}, \dots, \mathfrak{p}_r^{k_r}$ は互いに素であるので $\mathcal{O}_K/\alpha \simeq \mathcal{O}_K/\mathfrak{p}_1^{k_1} \times \dots \times \mathcal{O}_K/\mathfrak{p}_r^{k_r}$ である.

ゆえに, $N(\alpha) = N(\mathfrak{p}_1^{k_1}) \dots N(\mathfrak{p}_r^{k_r})$ である. よって, 素イデアル $\mathfrak{p}$ に対して $N(\mathfrak{p}^k) = N(\mathfrak{p})^k$

を示せば良い. 降鎖列

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \dots \supset \mathfrak{p}^k$$

を考える. 各 $0 \leq i \leq k-1$ に対して, 群同型 $\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^i/\mathfrak{p}^{i+1}$ を次のように定める.

素イデアル分解の一意性より, $\mathfrak{p}^{i+1} \subsetneq \mathfrak{p}^i$ である. よって, $x \in \mathfrak{p}^i$ から $x \notin \mathfrak{p}^{i+1}$ を満たす

x がとれる. $J = (x) + \mathfrak{p}^{i+1}$ とおくと, $\mathfrak{p}^{i+1} \subsetneq J \subset \mathfrak{p}^i$ である. よって, $\mathfrak{p} \not\subset J \subset \mathfrak{p}^i \subset \mathcal{O}_K$

となり, ゆえに $J/\mathfrak{p}^{i+1} = \mathcal{O}_K/\mathfrak{p}$ となる. したがって, $J = \mathfrak{p}^i$ である. 写像

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\varphi} & \mathfrak{p}^i/\mathfrak{p}^{i+1} \\ a & \longmapsto & ax + \mathfrak{p}^{i+1} \end{array} \quad \text{を考える.}$$

$\mathfrak{p}^i = (x) + \mathfrak{p}^{i+1}$ より, φ は全射である. また, $\mathfrak{p} \subset \text{Ker}(\varphi) \subset \mathcal{O}_K$ であるので,

$\mathfrak{p} = \text{Ker}(\varphi)$ が成り立つ. よって, 群同型 $\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^i/\mathfrak{p}^{i+1}$ が得られる.

最後に, $[\mathcal{O}_K : \mathfrak{p}^k] = [\mathcal{O}_K : \mathfrak{p}] \cdot \underbrace{[\mathfrak{p} : \mathfrak{p}^2]}_{= [\mathcal{O}_K : \mathfrak{p}]} \cdot \dots \cdot \underbrace{[\mathfrak{p}^{k-1} : \mathfrak{p}^k]}_{= [\mathcal{O}_K : \mathfrak{p}]} = [\mathcal{O}_K : \mathfrak{p}]^k$ である. □

補題 3.3.4 (ii) より

$$N(\alpha\mathfrak{a}) = N^p(\alpha) N(\mathfrak{a}) \quad (\alpha, \mathfrak{a} \neq 0 \text{ は } \mathcal{O}_K \text{ のイデアル})$$

一般に, 分数イデアル $\mathfrak{I} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ ($k_1, \dots, k_r \in \mathbb{Z}$) について,

$N(\mathfrak{I}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{k_i}$ と定めると 準同型 $N: J_K \rightarrow \mathbb{Q}_{>0}$ が得られる.

補題 3.3.5. $\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアルとする. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ となる素数 p が存在する.
また, $N(\mathfrak{p}) = p^f$ となる $f \geq 1$ が存在する.

証明: 命題 2.2.4 の証明より, $\mathfrak{p} \neq 0$ のとき, $\mathfrak{p} \cap \mathbb{Z} = (p)$ (p 素数) である.
よって, 単準同型 $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$ があり, $\mathcal{O}_K/\mathfrak{p}$ は有限次元 $\mathbb{F}_p$ ベクトル空間になる.
ゆえに $N^p(\mathfrak{p}) = p^f$ (ある $f \geq 1$) が成り立つ. $\square$

§ 3.4. 類数の有限性

K のイデアル群は $\mathcal{I}_K = J_K/P_K$ で定義される. 分数イデアル α について,
 α の P_K による剰余類は α のイデアル類とよび, $[\alpha]$ と書くことにする.

定理 3.4.1. $\alpha \neq 0$ を $\mathcal{O}_K$ のイデアルとする. α のイデアル類においては,

$$N^p(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \quad \text{強いバースン: } N^p(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

を満たすイデアル $\mathfrak{a}$ が存在する.

証明: $\alpha\alpha^{-1} \subset \mathcal{O}_K$ となる $\alpha \in \mathcal{O}_K \setminus \{0\}$ をとり, $\mathfrak{J} = \alpha\alpha^{-1}$ とおく.

命題 3.3.1 (または定理 3.3.2.) より,

$$|N_{K/\mathbb{Q}}(y)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathfrak{J}) \quad (\text{または } \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} N(\mathfrak{J}))$$

となる $y \in \mathfrak{J} \setminus \{0\}$ が存在する. よって,

$$N(J^{-1}(y)) = N(J)^{-1} |N_{K/\mathbb{Q}}(y)| \leq \left(\frac{2}{\pi}\right)^S \sqrt{d_K} \quad \left(\text{または } \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^S \sqrt{d_K}\right)$$

$b = J^{-1}(y)$ とおくと, $b = \sigma(\alpha^{-1}y)$ であるので, $[\sigma] = [b]$ となる.

また, $y \in J$ より, $b \in J^{-1}J = \mathcal{O}_K$ が成り立つ.

□

定理 3.4.2. $\mathcal{C}_K$ は有限群である.

証明:

$$S = \left\{ \sigma \mid \sigma : \mathcal{O}_K \text{ のイデアル かつ } N(\sigma) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^S \sqrt{d_K} \right\} \text{ とする.}$$

写像 $S \longrightarrow \mathcal{C}_K$ は 全射 である. なぜならは,
 $\sigma \longmapsto [\sigma]$

① イデアル $\mathfrak{b}$ に対して, 定理 3.4.1. より $[\sigma] = [\mathfrak{b}]$ となる $\mathfrak{b} \in S$ が存在する.

② また, 分数イデアル σ に対して, $[\sigma] = [x\sigma]$ ($x \in \mathcal{O}_K, x \neq 0$) より,

$[\sigma] = [J]$ となるイデアル J が存在. ① より $[\sigma] = [\mathfrak{b}]$ となる $\mathfrak{b} \in S$ が存在.

よって, S が有限集合であることを示せば良い. $M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^S \sqrt{d_K}$ とする.

$\sigma \in S$ とし, $\sigma = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ ($k_1, \dots, k_r \geq 1$) とすると, $N(\sigma) = N(\mathfrak{p}_1)^{k_1} \cdots N(\mathfrak{p}_r)^{k_r}$ である.

よって, 「 $N(\mathfrak{p}) \leq M$ となる素イデアル $\mathfrak{p} \neq 0$ は高々有限個しか存在しない」(*) を示せば良い.

補題 3.3.5 より, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ とすると, $N(\mathfrak{p}) = p^f$ ($f \geq 1$) が成り立つ.

これより, $N(\mathfrak{p}) \leq M$ のとき, 素数 $p \leq M$ があり, $\mathfrak{p} \in \mathfrak{p}$ である.

とくに, $\mathfrak{p} \mathcal{O}_K \subset \mathfrak{p}$ となる (つまり, $\mathfrak{p} \mid \mathfrak{p} \mathcal{O}_K$ である).

$\mathcal{O}_K$ はデデキント環なので, $\mathfrak{p} \mid \mathfrak{p} \mathcal{O}_K$ を満たす素イデアル $\mathfrak{p}$ は有限個しか存在しない.

よって, 集合 $\{\mathfrak{p} \text{ 素イデアル} \mid \mathfrak{p} \mid \mathfrak{p} \mathcal{O}_K, p \text{ は素数}, p \leq M\}$ は有限である.

主張 (*) が従う.

□

例 3.4.3 $K = \mathbb{Q}(\sqrt{-5})$ とする. $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ である.

例 2.1.2 (ii) より, $\mathcal{O}_K$ は単項イデアル整域でない ($\Leftrightarrow \mathcal{O}_K \neq \{0\}$).

$r = 0, s = 1$ であり, $d_K = -4 \times 5 = -20$ である. よって,

$$\left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} = \frac{4\sqrt{5}}{\pi} \approx 2.84$$

よって,

$S = \{ \alpha \mid N(\alpha) \leq 2 \} \longrightarrow \mathcal{O}_K$ は全射である.
 $\alpha \longmapsto [\alpha]$

$p_1 = (2, 1+\sqrt{-5}), p_2 = (3, 1+\sqrt{-5}), p_3 = (3, 1-\sqrt{-5})$ とおく.

$$\begin{aligned} p_1^2 &= (2) \\ p_2 p_3 &= (3) \end{aligned}$$

ゆえに, $N(p_1)^2 = N((2)) = |N_{K/\mathbb{Q}}(2)| = 2^2$ であり, $N(p_1) = 2$ となる.

よって, $S = \{ \mathcal{O}_K, p_1 \}$ である. よって, $|\mathcal{O}_K| \leq 2$ である. $\mathcal{O}_K \neq \{0\}$ より,

$$\mathcal{O}_K = \{ [1], [p_1] \} \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{となる.}$$

$[p_2]$ と $[p_3]$ を考える.

$N(p_2) N(p_3) = 3^2$ であり, $N(p_2) = N(p_3) = 3$ となる.

$a, b \in \mathbb{Z}$ に対して, $N_{K/\mathbb{Q}}(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$ である.

よって, $N_{K/\mathbb{Q}}(1 + \sqrt{-5}) = 6$ である.

また, $p_1 p_2 = (6, 3+3\sqrt{-5}, 2+2\sqrt{-5}, -4+2\sqrt{-5})$ となる.

$$(3+3\sqrt{-5}) - (2+2\sqrt{-5}) = 1+\sqrt{-5}$$

よって, $(1+\sqrt{-5}) \in \phi_1\phi_2$ である. $N((1+\sqrt{-5})) = 6 = N(\phi_1\phi_2)$ より,

$$\phi_1\phi_2 = (1+\sqrt{-5})$$

ゆえに, (2) $\phi_2 = (1+\sqrt{-5})\phi_1$ であり, $[\phi_2] = [\phi_1]$ となる.

同様に,

$$\phi_1\phi_3 = (1-\sqrt{-5})$$

よって, $[\phi_3] = [\phi_1]$ が成り立つ.

§4. テイリクシの単数定理

$\mathbb{Q}_K$ の単数群を $\mathbb{Q}_K^\times$ と書く. $x \in K$ を 1 の n 乗根とする. $x^n - 1 = 0$ となる $n \geq 1$ があるから, x は $\mathbb{Z}$ 上 整である. また, $x \in \mathbb{Q}_K^\times$ となる. K に属する 1 の n 乗根の集合を $\mu(K)$ と書く. $\mu(K)$ は $\mathbb{Q}_K^\times$ の部分群をなす.

§4.1. 準備

写像 $j: K \rightarrow K_{\mathbb{R}}$ を考える. $(K_{\mathbb{R}} = \{(z_i)_i \mid z_i = \bar{z}_i\} \subset K_{\mathbb{C}} = \prod_i \mathbb{C})$
 $x \mapsto (x)_i$

$K_{\mathbb{R}}^\times = \{(z_i)_i \in K_{\mathbb{R}} \mid \forall i, z_i \neq 0\}$ とすると, 写像 $j: K^\times \rightarrow K_{\mathbb{R}}^\times$ が得られる.

写像 $\ell: K_{\mathbb{R}}^\times \rightarrow \prod_i \mathbb{R}$ を次のように定める

$$\begin{aligned} \ell: K_{\mathbb{R}}^\times &\longrightarrow \prod_i \mathbb{R} \\ (z_i)_i &\longmapsto (\log |z_i|)_i \end{aligned}$$

明かに, ℓ の像は部分空間

$$[\prod_i \mathbb{R}]^+ = \{(a_i)_i \in \prod_i \mathbb{R} \mid a_{\bar{i}} = a_i\}$$

に含まれる. ところで, 写像 $\ell: K_{\mathbb{R}}^\times \rightarrow [\prod_i \mathbb{R}]^+$ が得られる. 以下の図式を構成する.

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & [\prod_i \mathbb{R}]^+ \\ N_{K/\mathbb{Q}} \downarrow & & \downarrow N & & \downarrow \text{Tr} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{\log |\cdot|} & \mathbb{R} \end{array}$$

ここで, 写像 N, Tr はそれぞれ

$$\begin{aligned} N: K_{\mathbb{R}}^\times &\longrightarrow \mathbb{R}^\times \\ (z_i)_i &\longmapsto \prod_i z_i \end{aligned}$$

$$\begin{aligned} \text{Tr}: [\prod_i \mathbb{R}]^+ &\longrightarrow \mathbb{R} \\ (a_i)_i &\longmapsto \sum_i a_i \end{aligned}$$

で定義される.

補題 1.3.1 (iv) より, $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(x) = \pm 1\}$ である.

次の集合を考察する.

(*)

$$\begin{aligned} S &= \{z \in K_{\mathbb{R}}^\times \mid N(z) = \pm 1\} \\ H &= \{a \in [\mathbb{H}_{\mathbb{R}}]^+ \mid \text{Tr}(a) = 0\} \end{aligned}$$

(*) より, $x \in \mathcal{O}_K^\times$ ならば $j(x) \in S \subset K_{\mathbb{R}}^\times$ である. したがって,
群準型 $\mathcal{O}_K^\times \xrightarrow{j} S \xrightarrow{\lambda} H$ が得られる. 合成写像 $\lambda \circ j$ を λ と書く.

$$\mathcal{O}_K^\times \xrightarrow{\lambda} H, \quad x \mapsto (\log |z(x)|)_z$$

また,

$$\Gamma = \lambda(\mathcal{O}_K^\times) \quad \text{と定める.}$$

Γ は $\mathbb{R}$ ベクトル空間 H の部分群である (後ほど, Γ が H の格子であることを示す)

補題 4.1.1. 準同型写像 $\lambda: \mathcal{O}_K^\times \longrightarrow \Gamma$ について,
 $\text{Ker}(\lambda) = \mu(K)$ が成り立つ.

証明: 明らかに,

$$\text{Ker}(\lambda) = \{x \in \mathcal{O}_K^\times \mid |z(x)| = 1, \quad z: K \hookrightarrow \mathbb{C}^\times\} \quad \text{である.}$$

$x \in \mu(K)$ とする. $x^n = 1$ ($n \geq 1$) より, $|z(x)| = 1$ となり, $x \in \text{Ker}(\lambda)$ である.

$j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ は完全格子である. よって, 任意の $K_{\mathbb{R}}$ の有界集合 Y に対して,

$Y \cap j(\mathcal{O}_K)$ は有限である.

$$j(\text{Ker}(\lambda)) \subset \{(z_\tau)_\tau \in K_K \mid |z_\tau| = 1, \tau: K \hookrightarrow \mathbb{C}\}$$

より, $j(\text{Ker}(\lambda))$ は格子 $j(Q_K)$ の有界部分集合である. したがって,

$j(\text{Ker}(\lambda))$ は有限である. j は単射なので, $\text{Ker}(\lambda)$ は有限群である.

N を位数とすると, 各 $x \in \text{Ker}(\lambda)$ に対して $x^N = 1$ が成り立つ (ラグランジュの定理).

以上より, $\text{Ker}(\lambda) = \mu(K)$ である. $\square$

補題 4.12. $a \in \mathbb{Z}$ とし, 集合 $E_a = \{x \in Q_K \mid N_{K/\mathbb{Q}}(x) = a\}$ を考える.

$x, y \in E_a$ に対して, 「 $x \sim y \iff y = ux, y \in Q_K$ 」で同値関係 $\sim$ を定義する.

E_a においては有限個の同値類しか存在しない.

証明: $a \neq 0$ と仮定して良い. また, $a \geq 1$ に対して, 集合

$E'_a = \{x \in Q_K \mid |N_{K/\mathbb{Q}}(x)| = a\} = E_a \cup E_{-a}$ は有限個の同値類

しかもたないことを示せば良い.

$x, y \in E'_a$ とし, $x \equiv y \pmod{aQ_K}$ とする.

このとき, $y = x + az$ ($z \in Q_K$) と書ける. よって,

$$\begin{aligned} \frac{y}{x} &= 1 + \frac{az}{x} = 1 \pm \left(\frac{N_{K/\mathbb{Q}}(z)}{x} \right) z \\ &= 1 \pm \left(\prod_{\tau \neq id} \tau(z) \right) z \end{aligned}$$

とくに $\frac{y}{x} \in Q_K$ である. 同様に $\frac{z}{y} \in Q_K$ である. ゆえに $\frac{x}{y} \in Q_K^\times$ となる.

つまり $x \sim y$ が成り立つ. これより, Q_K/aQ_K の1つの剰余類においては,

同値関係 $\sim$ に関する同値類が高々1つしか存在しない. Q_K/aQ_K は有限集合より,

$$|E'_a/\sim| \leq [Q_K : aQ_K] \quad \text{となり, 主張が従う.}$$

$\square$

次, 「部分群 $\Gamma \subset H$ は完全格子である」 という結果を証明する. まず,
その証明に必要な定理を説明する.

定理 4.1.3. V を有限次元 $\mathbb{R}$ ベクトル空間とし, $M \subset V$ を部分群とする.

次の条件は互いに同値である.

- (i) M は格子である (つまり $M = \mathbb{Z}x_1 \oplus \dots \oplus \mathbb{Z}x_m$, $x_1, \dots, x_m$ は線型独立である)
- (ii) 0 の近傍 W が存在して, $W \cap M = \{0\}$ である.
- (iii) X を V の有界集合とする. このとき, $X \cap M$ は有限集合である.

証明:

(i) $\Rightarrow$ (ii) は簡単である.

(ii) $\Rightarrow$ (iii) : V 上のノルム $\|\cdot\|$ をとる. 仮定より, $\varepsilon > 0$ が存在し,
 $\{x \in M \mid \|x\| \leq \varepsilon\} = \{0\}$ である. よって, 全ての $x, y \in M$ に対して,
 $\|x - y\| > \varepsilon$ が成り立つ. X は有界なから, $X \subset B_1 \cup \dots \cup B_N$ (B_i : 半径 $\frac{\varepsilon}{2}$ の球体)
といえる. $|M \cap X \cap B_i| \leq 1$ より, $M \cap X$ は有限である.

(iii) $\Rightarrow$ (i) : V_0 を Γ で生成される部分ベクトル空間とし, m を V_0 の次元とする.

V_0 の基底 $(v_1, \dots, v_m)$ をなすベクトル $v_1, \dots, v_m \in \Gamma$ がとれる.

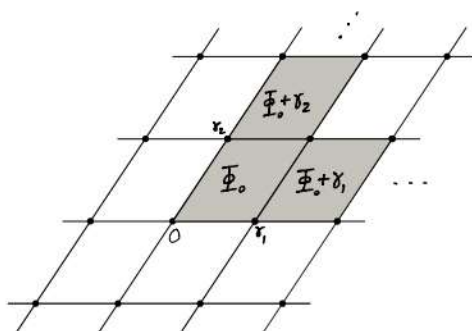
$$\Gamma_0 = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m$$

とする. 指数 $[\Gamma: \Gamma_0]$ は有限であることを証明する.

$$\Phi_0 = \{d_1v_1 + \dots + d_mv_m \mid 0 \leq d_i < 1\}$$

と定める. Φ_0 は Γ_0 の基本平行体だから, $V_0 = \bigsqcup_{\gamma \in \Gamma_0} \gamma + \Phi_0$ が成り立つ.

(*)



$\Gamma = \{\gamma_i\}_{i \in \mathbb{I}}$ と書く. $\Gamma \subset V_0$ であるので, (*) より 任意の $\gamma_i \in \Gamma$ に対して, $\gamma_i = \gamma_{0,i} + \nu_i$ ($\gamma_{0,i} \in \Gamma_0$, $\nu_i \in \Phi_0 \cap \Gamma$) と書ける.

仮定より, Φ_0 に属する Γ の元の個数は有限である. よって,

$\{\nu_i\}_{i \in \mathbb{I}} = \{\nu_1, \dots, \nu_q\}$ と書け, $[\Gamma: \Gamma_0]$ は有限である. $q = [\Gamma: \Gamma_0]$ とおくと,

$$\Gamma \subset \frac{1}{q} \Gamma_0 = \mathbb{Z} \frac{\nu_1}{q} \oplus \dots \oplus \mathbb{Z} \frac{\nu_m}{q}$$

となる. 自由アーベル群の部分群は自由であるので, (i) が従う. □

補題 4.1.4: V を有限次元 $\mathbb{R}$ ベクトル空間とし, $\Gamma \subset V$ を V の格子とする.

このとき,

$$\Gamma \text{ が完全格子である} \iff \begin{array}{l} \text{有界部分集合 } M \subset V \text{ が存在し,} \\ V = \bigcup_{\gamma \in \Gamma} M + \gamma \text{ である.} \end{array}$$

証明: ($\Rightarrow$) M として Γ の基本平行体とすれば良い.

($\Leftarrow$) V_0 を Γ で生成された部分ベクトル空間とする. $v \in V$ として, $n \geq 1$ とする.

$nv = m_n + \gamma_n$ となる $m_n \in M$, $\gamma_n \in \Gamma$ がある. よって, $v = \frac{m_n}{n} + \frac{\gamma_n}{n}$ である. M は有界だから, $\frac{m_n}{n} \rightarrow 0$ となる. したがって, $v = \lim_{n \rightarrow \infty} \frac{\gamma_n}{n} \in V_0$. 以上より, $V = V_0$ となり, Γ は完全格子である. □

§4.2. 単数定理

命題 4.2.1

- (i) H は $r+s-1$ 次元 $\mathbb{R}$ ベクトル空間である。
 (ii) $\Gamma \subset H$ は H の完全格子である。

証明: (i) $[\prod_{\mathbb{Z}} \mathbb{R}]^+ = \{(a_z)_z \mid a_z = a_{\bar{z}}\}$ は $r+s$ 次元ベクトル空間である。

ゆえに, $H = \{a \in [\prod_{\mathbb{Z}} \mathbb{R}]^+ \mid \text{Tr}(a) = 0\}$ の次元は $r+s-1$ となる。

(ii) Γ は格子であることを示す。定理 4.1.3. より,

「実数 $c > 0$ に対して, $\Gamma_c = \{(a_z)_z \in \Gamma \mid |a_z| \leq c\}$ は有限である」
 を示せば良い。 $\Gamma = \ell(j(\mathcal{O}_K^{\times}))$ であるので,

$$\Gamma_c = \ell\left(\{(x_z)_z \in j(\mathcal{O}_K^{\times}) \mid |\log |x_z|| \leq c\}\right)$$

また, $|\log |x_z|| \leq c \iff e^{-c} \leq |x_z| \leq e^c$ である。 $j(\mathcal{O}_K)$ は $K_{\mathbb{R}}$ の格子だから, $|x_z| \leq e^c$ ($\forall z$) を満たす $(x_z)_z \in j(\mathcal{O}_K)$ の個数は有限である。 よって, Γ_c は有限である。

Γ は H の完全格子であることを示す。

$$c_z = c_{\bar{z}} \quad \text{かつ} \quad \prod_z c_z > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

を満たす実数 $c_z > 0$ (z : 埋め込み) がとれる。 $C = \prod_z c_z$ とおく。 また,

$$X = \{(z_z)_z \in K_{\mathbb{R}} \mid |z_z| < c_z\} \quad \text{とおく。}$$

$y = (y_z)_z \in S$ とし, 集合 $Xy = \{xy \mid x \in X\}$ を考える。 $c'_z = c_z |y_z|$ とおくと

$$Xy = \{(z_z)_z \in K_{\mathbb{R}} \mid |z_z| < c'_z\} \quad \text{が成り立つ。}$$

$$c'_z = c_z \quad \text{かつ} \quad \prod_z c'_z = \prod_z c_z \underbrace{\prod_z |y_z|}_{=1} = \prod_z c_z > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \quad \text{である。}$$

定理 3.2.3 より, $j(Q_K) \cap Xy \neq \{0\}$ である. つまり, $|z(a)| < c'_z \quad (\forall z)$
 を満たす $a \in Q_K \ (a \neq 0)$ が存在. (**)

補題 4.1.2. の同値関係 $\sim$ を考える. 補題 4.1.2. より, $a \in \mathbb{Z}$ に対して,

$E_a = \{x \in Q_K \mid N_{K/\mathbb{Q}}(x) = a\}$ においては, 有限個の同値類しか存在しない.

よって, 集合 $E_{\leq c} = \{x \in Q_K \mid |N_{K/\mathbb{Q}}(x)| \leq c\}$ においても有限個の同値類しかない.

$x_1, \dots, x_N$ を $E_{\leq c}$ の同値類の完全代表系とする. $1 \leq i \leq N$ について, $y_i = j(x_i)^{-1}$ とおき,

$$T = S \cap \left(\bigcup_{i=1}^N Xy_i \right) \subset K_R \quad \text{と定める.}$$

X は有界だから, T も有界である.

$$S = \bigcup_{v \in Q_K^\times} T j(v) \quad \text{が成り立つことを示す.}$$

$y \in S$ とすると $y^{-1} \in S$ である. 集合 Xy^{-1} を考える. (**) より,

$j(Q_K) \cap Xy^{-1} \neq \{0\}$ であり, ゆえに $|z(a)| < c'_z = c_z |y_z|^{-1}$ を満たす
 $a \in Q_K \setminus \{0\}$ が存在する.

$$|N_{K/\mathbb{Q}}(a)| = \prod_z |z(a)| < \prod_z c'_z = \prod_z c_z = c \quad \text{であるので,}$$

$j(a) = (z(a))_z \in E_{\leq c}$ となる. よって, ある $x_i \ (1 \leq i \leq N)$ があって,
 $a \sim x_i$ である. つまり, $x_i = a \cdot v \ (v \in Q_K^\times)$ と書ける.

$$y = (y j(v)^{-1}) j(v) \quad \text{と書く.}$$

また, $y j(v)^{-1} = y j(a) j(x_i)^{-1} = y j(a) y_i$ である.

$|y_z z(a)| < c_z \quad (\forall z)$ より, $y j(a) \in X$ である.

よって, $y j(v)^{-1} \in S \cap Xy_i$ となる.

しにかつて, $S = \bigcup_{v \in \mathcal{O}_K^\times} T_{j(v)}$ が成り立つ.

写像 $\ell: K_{\mathbb{R}}^\times \longrightarrow [\prod_{\mathbb{R}}]^\times$ を考える. 明かに $\ell(S) = H$ である.

$$(z_z)_z \longmapsto (\log |z_z|)_z$$

ゆえに,

$$H = \ell(S) = \bigcup_{v \in \mathcal{O}_K^\times} \ell(T) + \overset{\lambda(v)}{\ell(j(v))} = \bigcup_{\gamma \in \Gamma} \ell(T) + \gamma \quad \text{となる.}$$

$M = \ell(T)$ とおく. M が H の有界集合であることを示す.

T は有界であるので, $D > 0$ が存在し, 任意の $x \in T$ に対して $|x_z| \leq D$ ($\forall z$) である.

$\prod_z x_z = 1$ より, $|x_z| \geq \frac{1}{D^{n-1}}$ といえる.

よって, $-(n-1) \log D \leq \log |x_z| \leq \log D$ が成り立ち, $M = \ell(T)$ は有界である.

最後に $H = \bigcup_{\gamma \in \Gamma} M + \gamma$ より Γ は完全格子である (補題 4.1.4. 参照).

□

補題 4.2.2 A, A' をアーベル群とし, $f: A \rightarrow A'$ を全準同型とする.

また, A' が自由アーベル群であるとする. このとき, $A = B \oplus \text{Ker}(f)$ となる部分群 $B \subset A$ が存在する. さらに, f の B への制限は群同型 $B \xrightarrow{f} A'$ である.

証明: $\{x'_i\}_{i \in I}$ を A' の基底とする. また, $f(x_i) = x'_i$ ($i \in I$) となる A の元 x_i をとる. 準同型

$$g: A' \longrightarrow A \quad \sum_{i \in I} k_i x'_i \mapsto \sum_{i \in I} k_i x_i$$

を考える. $f \circ g(\sum k_i x'_i) = \sum k_i x'_i$ であり, ゆえに $f \circ g = \text{id}_{A'}$ である.

$B = \text{Im}(g) = \langle \{x_i \mid i \in I\} \rangle$ とおく.

$x \in B \cap \text{Ker}(f)$ とし, $x = g(y)$ ($y \in A'$) とすると, $0 = f(x) = f(g(y)) = y$

となる. よって $x = 0$ となる. したがって, $B \cap \text{Ker}(f) = 0$ である.

また, $x \in A$ とする. $x = g(f(x)) + (x - g(f(x)))$ と書ける.

$b = g(f(x))$, $c = x - g(f(x))$ とおく.

$f(c) = f(x) - f(g(f(x))) = f(x) - f(x) = 0$ より, $c \in \text{Ker}(f)$

よって, $x = b + c \in B + \text{Ker}(f)$ である. したがって, $A = B + \text{Ker}(f)$ である.

以上より, $A = B \oplus \text{Ker}(f)$ が成り立つ.

f の B への制限が群同型 $B \rightarrow A'$ であることは簡単に確認できる.

□

定理 4.2.3 K を代数体とする. このとき,

$$G_K^x \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$$

証明: 準同型 $\mathcal{O}_K^X \xrightarrow{\lambda} \Gamma$ は全射であり, $\ker(\lambda) = \mu(K)$ が成り立つ
 (補題 4.1.1 参照). 補題 4.2.2 より,

$$\mathcal{O}_K^X \simeq \mu(K) \times \Gamma \quad \text{である.}$$

命題 4.2.1 より, Γ は H の完全格子である.

$$H = \left\{ (a_z)_z \in \left[\prod_z \mathbb{R} \right]^+ \mid \sum_z a_z = 0 \right\}$$

の次元は $\dim(H) = \dim \left[\prod_z \mathbb{R} \right]^+ - 1 = r+s-1$ である.

よって, Γ の階数は $r+s-1$ であり, $\Gamma \simeq \mathbb{Z}^{r+s-1}$ となる.

以上より, $\mathcal{O}_K^X \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$ である.

□

定理 4.2.3 より, 単数 $\varepsilon_1, \dots, \varepsilon_t$ ($t=r+s-1$) を用いて,

$$\mathcal{O}_K^X = \left\{ \zeta \varepsilon_1^{k_1} \cdots \varepsilon_t^{k_t} \mid \zeta \in \mu(K), k_1, \dots, k_t \in \mathbb{Z} \right\} \quad \text{と書ける.}$$

このような単数 $\varepsilon_1, \dots, \varepsilon_t$ は **基本単数** という.

§4.3. 二次体

K を二次体とし, $K = \mathbb{Q}(\sqrt{D})$ (D は平方因数をもたない, $D \neq 0, 1$) とする.

• $D < 0$ のとき, 定理 4.2.3 を使う必要もなく, $\mathcal{O}_K^X$ は有限であることが分る.

なぜならば, $x = a + b\sqrt{D} \in \mathcal{O}_K$ ($a, b \in \mathbb{Q}$) とすると,

$$N_{K/\mathbb{Q}}(x) = a^2 - Db^2 \text{ である (よって, } N_{K/\mathbb{Q}}(x) \geq 0 \text{)}. \quad \text{よって,}$$

$$\mathcal{O}_K^X = \{ x \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(x) = 1 \}$$

$a^2 - Db^2 = 1$ ならば, $a \leq 1, b \leq 1$ が成り立つ.

定理 2.1.1 より, $2a, 2b \in \mathbb{Z}$ である. よって, $\mathcal{O}_K^X$ は有限である.

定理 4.2.3 より,

$$\mathcal{O}_K^{\times} = \mu(K)$$

が成り立つ.

($r=0, s=1$ である)

- $D > 1$ とする. このとき, $r=2, s=0$ である.

ゆえに, $\mathcal{O}_K^{\times} \simeq \mu(K) \times \mathbb{Z}$ である. $K \subset \mathbb{R}$ より, $\mu(K) = \{\pm 1\}$ である.

したがって,

$$\mathcal{O}_K^{\times} \simeq \{\pm 1\} \times \mathbb{Z}$$

である.

このことから, $u \in \mathcal{O}_K^{\times}$ を基本単数とすると, 全ての基本単数は $\{u, -u, u^{-1}, -u^{-1}\}$ である.

よって, $u > 1$ を満たす基本単数は一意に存在する.

注意 4.3.1 u を基本単数とし, $u > 1$ とする. $u = a + b\sqrt{D}$ ($a, b \in \mathbb{Q}$) と書くと,

$$\{u, u^{-1}, -u, -u^{-1}\} = \{\pm a \pm b\sqrt{D}\}$$

である.

u はこの集合の最大元であるので, $a, b \in \mathbb{Q}_{>0}$ である. (*)

また,

$$\{x \in \mathcal{O}_K^{\times} \mid x > 1\} = \{u^k \mid k \geq 1\}$$

$$\{x \in \mathcal{O}_K^{\times} \mid 0 < x < 1\} = \{u^k \mid k < 0\}$$

である

$\nu > 1$ であるような基本単数を求めるアルゴリズム

- $D = 2, 3 \pmod{4}$ の場合

このとき, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ である.

集合

$$F = \left\{ b \in \mathbb{Z}_{\geq 1} \mid Db^2 + 1 \text{ または } Db^2 - 1 \text{ が平方数である} \right\}$$

を考えると, b_1 を F の最小元とする. このとき, $a_1^2 - Db_1^2 \in \{\pm 1\}$ となる $a_1 \in \mathbb{Z}_{\geq 1}$ は一意に存在する ($Db^2 + 1$ と $Db^2 - 1$ は高々一つが平方数であるから).

$\nu = a_1 + b_1\sqrt{D}$ は $\nu > 1$ を満たす基本単数である.

証明: $N_{K/\mathbb{Q}}(\nu) = a_1^2 - Db_1^2 = \pm 1$ より, $\nu \in \mathcal{O}_K^\times$ である.

ν' を $\nu' > 1$ を満たす基本単数とする. $\nu' = \nu$ を示す.

$\nu' = a'_1 + b'_1\sqrt{D}$ ($a'_1, b'_1 \in \mathbb{Z}$) と書く. 列 $\{\nu'^k\}_{k \geq 1}$ を考える.

$(\nu')^k = a'_k + b'_k\sqrt{D}$ ($a'_k, b'_k \in \mathbb{Z}$) と書ける.

$$\begin{aligned} \nu'^{k+1} &= (a'_k + b'_k\sqrt{D})(a'_1 + b'_1\sqrt{D}) \\ &= a'_k a'_1 + b'_1 b'_k D + (a'_1 b'_k + b'_1 a'_k)\sqrt{D} \end{aligned}$$

より, $a'_{k+1} = a'_k a'_1 + b'_1 b'_k D$ かつ $b'_{k+1} = a'_1 b'_k + b'_1 a'_k$ である.

注意 4.3.1 の (*) より $a'_1, b'_1 \geq 1$ である. よって, $a'_k \geq 1, b'_k \geq 1$ となる.

また, $(b'_k)_{k \geq 1}$ は単調増加列である. (**)

$\nu = a_1 + b_1\sqrt{D}$ ($a_1 \geq 1, b_1 \geq 1$) より, $\nu > 1$ が成り立つ.

よって, $\nu = (\nu')^m$ となる $m \geq 1$ が存在する (注意 4.3.1 参照)

任意の $k \geq 1$ に対し, $b_k \in F$ である. (**) より, $m = 1$ である.

よって, $\nu = \nu'$ である.

□

- $D \equiv 1 \pmod{4}$ とする.

$$\text{このとき, } \mathcal{O}_K = \mathbb{Z}\left[\frac{\sqrt{D}+1}{2}\right] = \left\{ \frac{1}{2}(a+b\sqrt{D}) \mid a, b \in \mathbb{Z}, a \equiv b \pmod{2} \right\}$$

$\frac{1}{2}(a+b\sqrt{D}) \in \mathcal{O}_K^*$ とすると, $a^2 - Db^2 = \pm 4$ である. 集合

$$F = \left\{ b \in \mathbb{Z}_{>0} \mid Db^2 + 4 \text{ または } Db^2 - 4 \text{ が平方である} \right\}$$

を考え, b_1 を F の最小元とする.

$a_1^2 - Db_1^2 = \pm 4$ を満たす 最小の $a_1 \geq 1$ をとる ($D=5$ のとき,

$$1^2 - 5 \cdot 1^2 = -4 \text{ かつ } 3^2 - 5 \cdot 1^2 = 4 \text{ より, } (a_1, b_1) = (1, 1) \text{ と } (a_1, b_1) = (3, 1)$$

両方ともこの条件を満たす. このとき, $a_1 = 1$ とする).

$$u = \frac{1}{2}(a_1 + b_1\sqrt{D}) \text{ は } u > 1 \text{ を満たす基本単数である.}$$

証明: $u' = \frac{1}{2}(a'_1 + b'_1\sqrt{D})$ ($a'_1, b'_1 \geq 1$) を $u' > 1$ となる基本単数とする.

$$(u')^k = \frac{1}{2}(a'_k + b'_k\sqrt{D}) \text{ と書く. すると,}$$

$$\begin{aligned} (u')^{k+1} &= \frac{1}{2}(a'_k + b'_k\sqrt{D}) \cdot \frac{1}{2}(a'_1 + b'_1\sqrt{D}) \\ &= \frac{1}{4}(a'_k a'_1 + Db'_k b'_1 + (a'_k b'_1 + b'_k a'_1)\sqrt{D}) \\ &= \frac{1}{2}(a'_{k+1} + b'_{k+1}\sqrt{D}) \end{aligned}$$

ゆえに, $a'_{k+1} = \frac{1}{2}(a'_k a'_1 + Db'_k b'_1)$ かつ $b'_{k+1} = \frac{1}{2}(a'_k b'_1 + b'_k a'_1)$ となる.

$a'_1 \geq 2$ のとき, $(b'_k)_{k \geq 1}$ は単調増加列であり, 上と同様に $u = u'$ となる.

$a'_1 = 1$ とする. $a_1^2 - Db_1^2 = \pm 4$ より, $Db_1^2 \in \{-3, 5\}$ である. $D > 0$ より,

$Db_1^2 = 5$ となり, $D=5, b'_1=1$ が成り立つ.

$$\text{よって, } a'_{k+1} = \frac{1}{2}(a'_k + 5b'_k) \text{ かつ } b'_{k+1} = \frac{1}{2}(a'_k + b'_k) \text{ である.}$$

よって, $5b'_k > a'_k \geq b'_k$ であり, $a'_{k+1} > a'_k$ である. したがって, $u' = u$ となる.

例 4.3.2

(i) $D=2$ とする.

$D \equiv 2 \pmod{4}$ であるので, 集合

$$\{b \geq 1 \mid Db^2 + 1 \text{ または } Db^2 - 1 \text{ が平方数である}\}$$

を考える.

$$\begin{aligned} 2 \cdot 1^2 + 1 &= 3 && \text{平方数でない.} \\ 2 \cdot 1^2 - 1 &= 1 = 1^2 && \text{である.} \end{aligned}$$

よって, $u = 1 + \sqrt{2}$ は $\mathbb{Z}[\sqrt{2}]$ の基本単数である.

つまり, $\mathbb{Z}[\sqrt{2}]^\times = \{\pm (1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$ である.

(ii) $D=6$ とする. $D \equiv 2 \pmod{4}$ である.

$$6 \cdot 1^2 + 1 = 7, \quad 6 \cdot 1^2 - 1 = 5 \quad \text{は平方数でない.}$$

$$6 \cdot 2^2 + 1 = 25 = 5^2$$

よって, $u = 5 + 2\sqrt{6}$ は $\mathbb{Z}[\sqrt{6}]$ の基本単数である.