# 第 1 章
# 代数体と整数環

本章では，代数的整数論から，代数体の整数環のイデアルについて基本的な事柄を説明する．これらの事柄は，第 2 章で高さの理論を展開するために用いる．一部は証明を省略しているが，詳しくは [14] などの文献を参照してほしい．

## 1.1 有限次分離拡大のトレースとノルム

$F$ を体，$L$ を $F$ 上の分離的な有限次拡大体とする．$n = [L : F]$ とおく．次節以降への準備として，$L$ の元の $F$ 上のトレースとノルムを定義することから始めよう．

$x \in L$ とする．$x$ の $F$ 上の**トレース** (trace) $\mathrm{Tr}_{L/F}(x)$ と**ノルム** (norm) $\mathrm{Norm}_{L/F}(x)$ を，$x$ をかけることによって得られる $F$ 上の線形写像

$$L \to L, \quad \alpha \mapsto x\alpha \tag{1.1}$$

のトレースと行列式としてそれぞれ定義する．すなわち，$\alpha_1, \ldots, \alpha_n \in L$ を $L$ の $F$ ベクトル空間としての基底とし，$x\alpha_j = \sum_{i=1}^{n} c_{ij}\alpha_i$ $(c_{ij} \in F)$ とおけば，$\mathrm{Tr}_{L/F}(x) = \sum_{i=1}^{n} c_{ii}$，$\mathrm{Norm}_{L/F}(x) = \det(c_{ij})$ である．

トレースとノルムには同値な別の定め方がある．$\Omega$ を $F$ を含む代数閉体とし，

$$\mathrm{Hom}_F(L,\Omega)=\{\sigma \mid \sigma : L \hookrightarrow \Omega \text{ は } \sigma|_F = \mathrm{id}_F \text{ となる体の埋め込み}\} \quad (1.2)$$

とおく．このとき，$\#(\mathrm{Hom}_F(L,\Omega))=[L:F]$ が成り立つ．実際，$L/F$ は分離的な有限次拡大体であるから，$L=F(\theta)$ となる $\theta$ が存在する．$\theta$ の $F$ 上の共役元を $\theta_1,\ldots,\theta_n$ とおけば，$\theta$ を $\theta_i$ にうつす $F$ の元を動かさない体の埋め込み $\sigma_i : L \hookrightarrow \Omega$ が存在し，

$$\mathrm{Hom}_F(L,\Omega)=\{\sigma_1,\ldots,\sigma_n\}$$

となる．このとき，次が成り立つ．

**補題 1.1.** $x \in L$ に対し，

$$\mathrm{Tr}_{L/F}(x)=\sum_{\sigma\in\mathrm{Hom}_F(L,\Omega)}\sigma(x), \quad \mathrm{Norm}_{L/F}(x)=\prod_{\sigma\in\mathrm{Hom}_F(L,\Omega)}\sigma(x)$$

が成り立つ．

**証明:** $F$ に $x$ を添加した体 $F(x)$ を考え，$[F(x):F]=m$, $[L:F(x)]=d$ とおく．このとき，$n=md$ である．$\{1,x,\ldots,x^{m-1}\}$ は $F(x)$ の $F$ 上の基底である．また，$L$ の $F(x)$ 上の基底 $\{\beta_1,\ldots,\beta_d\}$ をとれば，$\{\beta_i x^j\}_{1\le i\le d, 0\le j\le m-1}$ が $L$ の $F$ 上の基底になる．$x$ の $F$ 上の最小多項式を

$$X^m - c_1X^{m-1}+\cdots+(-1)^m c_m \qquad (c_1,\ldots,c_m\in F) \qquad (1.3)$$

とおく．このとき，$x$ をかけることによって得られる $F$ 上の線形写像 $F(x)\to F(x)$, $\alpha\mapsto x\alpha$ の基底 $1,x,\ldots,x^{m-1}$ に関する表現行列 $G$ は，

$$G=\begin{pmatrix} 0 & 0 & \cdots & 0 & (-1)^{m-1}c_m \\ 1 & 0 & \cdots & 0 & (-1)^{m-2}c_{m-1} \\ 0 & 1 & \cdots & 0 & (-1)^{m-3}c_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_1 \end{pmatrix} \in M(m,m;F)$$

となる．よって，$F$ 上の線形写像 (1.1) の基底

$$\beta_1,\ \beta_1x,\ \ldots,\ \beta_1x^{m-1},\ \ldots,\ \beta_d,\ \beta_dx,\ \ldots,\ \beta_dx^{m-1}$$

に関する表現行列は,

$$\begin{pmatrix} G & O & \cdots & O \\ O & G & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & G \end{pmatrix} \in M(md, md; F)$$

である．これから，$\mathrm{Tr}_{L/F}(x) = dc_1$, $\mathrm{Norm}_{L/F}(x) = c_m^d$ となる．

一方，$x$ の $F$ 上の共役を $x_1, \ldots, x_m$ とすれば，$x_1, \ldots, x_m$ は 式 (1.3) の根全体であり，根と係数の関係から，$\sum_{k=1}^m x_k = c_1$, $\prod_{k=1}^m x_k = c_m$ である．

$\tau \in \mathrm{Hom}_F(F(x), \Omega)$ に対して,

$$\mathrm{Hom}_F(L, \Omega)_\tau = \{\sigma \in \mathrm{Hom}_F(L, \Omega) \mid \sigma|_{F(x)} = \tau\}$$

とおく．このとき，$\#(\mathrm{Hom}_F(L, \Omega)_\tau) = [L : F(x)] = d$ であるので,

$$\begin{aligned} \sum_{\sigma \in \mathrm{Hom}_F(L,\Omega)} \sigma(x) &= d \sum_{\tau \in \mathrm{Hom}_F(F(x),\Omega)} \tau(x) = d \sum_{k=1}^m x_k = dc_1 \\ &= \mathrm{Tr}_{L/F}(x), \\ \prod_{\sigma \in \mathrm{Hom}_F(L,\Omega)} \sigma(x) &= \left( \prod_{\tau \in \mathrm{Hom}_F(F(x),\Omega)} \tau(x) \right)^d = \left( \prod_{k=1}^m x_k \right)^d = c_m^d \\ &= \mathrm{Norm}_{L/F}(x) \end{aligned}$$

となる． □

$A$ と $B$ を，それぞれの商体が，$F$ と $L$ となる整閉整域とする．$A \subseteq B$ かつ $B$ は $A$ 上整であると仮定する．例えば，$B$ が $A$ 加群として有限生成であれば，$B$ は $A$ 上整になる．トレースとノルムの定義と，補題 1.1 を比較することにより，次がわかる．

**補題 1.2.** $x \in B$ ならば，$\mathrm{Tr}_{L/F}(x), \mathrm{Norm}_{L/F}(x) \in A$ である．さらに $x \neq 0$ のとき，$\mathrm{Norm}_{L/F}(x)/x \in B$ である．

**証明:** $\mathrm{Hom}_F(L, \Omega) = \{\sigma_1, \ldots, \sigma_n\}$ とおく．トレースとノルムの定義から,

$\mathrm{Tr}_{L/F}(x), \mathrm{Norm}_{L/F}(x) \in F$ である．仮定から $x$ は $A$ 上整であるから，$\sigma_i(x)$ も $A$ 上整である．よって，補題 1.1 から，$\mathrm{Tr}_{L/F}(x), \mathrm{Norm}_{L/F}(x)$ はいずれも $A$ 上整な元になる．$A$ は $F$ の中で整閉であるから，$\mathrm{Tr}_{L/F}(x), \mathrm{Norm}_{L/F}(x) \in A$ である．

最後の主張を考える．補題 1.1 において，$\sigma_1$ は包含写像と仮定する．このとき，$\mathrm{Norm}_{L/F}(x)/x = \sigma_2(x)\cdots\sigma_n(x)$ である．$\sigma_i(x)$ は $A$ 上整であるので，$\sigma_2(x)\cdots\sigma_n(x)$ も $A$ 上整である．一方 $\mathrm{Norm}_{L/F}(x)/x \in L$ であり，$B$ は整閉整域であるので，$\mathrm{Norm}_{L/F}(x)/x \in B$ を得る． □

$L$ を $F$ 上のベクトル空間とみて，トレースから定まる $F$ 上の対称双線形形式 $(\ ,\ )_{\mathrm{Tr}_{L/F}}$ を，

$$(\ ,\ )_{\mathrm{Tr}_{L/F}} : L \times L \to F, \quad (x, y) \mapsto \mathrm{Tr}_{L/F}(xy) \tag{1.4}$$

で定め，**トレース形式** (trace form) とよぶ．さらに，$\alpha_1, \ldots, \alpha_n \in L$ に対して，そのグラム行列 $\left((\alpha_i, \alpha_j)_{\mathrm{Tr}_{L/F}}\right)$ の行列式

$$D(\alpha_1, \ldots, \alpha_n) = \det((\alpha_i, \alpha_j)_{\mathrm{Tr}_{L/F}}) \tag{1.5}$$

を $\alpha_1, \ldots, \alpha_n$ の**判別式** (discriminant) とよぶ．補題 1.1 より，$\mathrm{Hom}_F(L, \Omega) = \{\sigma_1, \ldots, \sigma_n\}$ とおくとき，$\mathrm{Tr}_{L/F}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$ である．よって，$\Delta = (\sigma_i(\alpha_j))$ とおくと，

$$D(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/F}(\alpha_i\alpha_j)) = \det({}^t\Delta \cdot \Delta) = \det(\Delta)^2 \tag{1.6}$$

とも表せる．

**補題 1.3.** トレース形式 $(\ ,\ )_{\mathrm{Tr}_{L/F}}$ は非退化である．したがって，$\alpha_1, \ldots, \alpha_n \in L$ に対して，$\{\alpha_1, \ldots, \alpha_n\}$ が $F$ 上の基底をなすことと，$D(\alpha_1, \ldots, \alpha_n) \neq 0$ であることは同値である．

**証明:** $(\ ,\ )_{\mathrm{Tr}_{L/F}}$ が非退化であるとは，$x \in L$ が任意の $y \in L$ に対して $(x, y)_{\mathrm{Tr}_{L/F}} = 0$ ならば $x = 0$ となることである．非退化性は，$L$ の $F$ 上のある基底に関するグラム行列が正則行列であることと同値である．

$L = F(\theta)$ となる $\theta$ をとって，$L$ の $F$ 上の基底として $\{1, \theta, \ldots, \theta^{n-1}\}$ を

とろう．$\sigma_1(\theta)=\theta_1,\ldots,\sigma_n(\theta)=\theta_n$ とおく．このとき，式 (1.6) から，

$$D(1,\theta,\ldots,\theta^{n-1})=\left(\det(\theta_i^{j-1})\right)^2=\left(\prod_{1\le i<j\le n}(\theta_i-\theta_j)\right)^2\neq 0$$

となる．よって，$(\ ,\ )_{\mathrm{Tr}_{L/F}}$ は非退化である．

$L$ の $F$ 上のある基底に関するグラム行列が正則であることと，$F$ 上の任意の基底に関するグラム行列が正則であることは同値であるから，後半の主張は前半の主張からしたがう． □

## 1.2 代数的整数と判別式

有理数体 $\mathbb{Q}$ の有限次拡大体を**代数体** (algebraic number field) という．本書では，代数体を主に $K$ で表す．

$K$ を代数体とする．$x\in K$ が**代数的整数** (algebraic integer) であるとは，ある正の整数 $m$ と，整数 $a_1,\ldots,a_m$ が存在して，

$$x^m+a_1x^{m-1}+\cdots+a_m=0$$

となることである．$K$ に含まれる代数的整数全体のなす集合を $O_K$ で表し，$K$ の**整数環** (ring of integers) とよぶ．すなわち，代数的整数とは $\mathbb{Z}$ 上整な元のことであり，$O_K$ は $\mathbb{Z}$ の $K$ における整閉包である．

一般に，$B$ が $A$ の拡大環のとき，$B$ の元で $A$ 上整なもの全体 $\widetilde{A}$ は $B$ の部分環をなすから（例えば, [10, 定理 9.1] を参照），$A=\mathbb{Z}$, $B=K$ のときを考えて，$O_K$ は（整数環という言葉の通り）環である．

本節では，前節のトレース形式を用いて，$O_K$ が階数が $n$ の 自由 $\mathbb{Z}$ 加群であることを示そう．

まずトレースとノルムについて，前節で示したことを，$K/\mathbb{Q}$ の場合にまとめておく．まず，$K$ の元 $x$ に対して，トレース $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ とノルム $\mathrm{Norm}_{K/\mathbb{Q}}(x)$ は $\mathbb{Q}$ の元である．記号 $K(\mathbb{C})$ で $K$ の $\mathbb{C}$ **値点**全体を表す．つまり，

$$K(\mathbb{C})=\{\sigma\mid\sigma:K\hookrightarrow\mathbb{C}\text{ は体の埋め込み }\}\tag{1.7}$$