10　ノルムとトレース

10.1　ノルムとトレース

定義 10.1. A : 有限次 $K-alg$ とする。$x \in A$ に対して x 倍写像

$$\begin{aligned} T_x : A &\longrightarrow A \\ a &\longmapsto xa \end{aligned}$$

は A が $K-alg$ より $K-$ 線形写像になる。よって $\dim_K(A) = n$ のときある A の基底 $\{e_1, \ldots, e_n\}$ により、 $T_x = (t_{ij})_{i,j=1,\ldots,n}$ とおいたとき行列表示は

$$T_x(e_j) = xe_j = \sum_{i=1}^{n} t_{ij} e_i$$

を満たすような $t_{ij} \in K$ で作られてこれにより行列 $T_x : K^n \longrightarrow K^n$ にできて行列の記法で

$$x(e_1, \cdots, e_n) = (e_1, \cdots, e_n) T_x$$

と書くことができる。

この行列 T_x について x のトレース (trace) $\mathrm{Tr}_{A/K}(x)$ と x のノルム (norm) $\mathrm{N}_{A/K}(x)$ を

$$\begin{aligned} \mathrm{Tr}_{A/K}(x) &:= \mathrm{Tr}(T_x) \\ \mathrm{N}_{A/K}(x) &:= \det(T_x) \end{aligned}$$

とするとこの値は K の元であるから

$$\begin{aligned} \mathrm{Tr}_{A/K} &: A \longrightarrow K \\ \mathrm{N}_{A/K} &: A \longrightarrow K \end{aligned}$$

という写像になっていて $\mathrm{Tr}_{A/K}$ は $K-$ 線形写像、 $\mathrm{N}_{A/K}$ は乗法的 $(\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y))$ である。とくに、定義域を乗法群 $A^\times$ に制限すれば

$$\mathrm{N}_{A/K}|_{A^\times} : A^\times \longrightarrow K$$

は群準同型になる。

例 10.2. $x \in K$ のとき $n := [A : K]$ として、A の基底を $\{e_1, \ldots, e_n\}$ とする。$T_x = (t_{ij})_{i,j=1,\ldots,n}$ とおいたとき行列表示は

$$T_x(e_j) = \sum_{i=1}^{n} t_{ij} e_i$$

とできて $T_x(e_j) = xe_j$ で基底の一次独立性から $t_{jj} = x, t_{ij} = 0$ $(i \neq j)$ となるので

$$T_x = \begin{pmatrix} x & & \\ & \ddots & \\ & & x \end{pmatrix}$$

と書ける。したがって $\mathrm{Tr}_{A/K}(x) = nx, \mathrm{N}_{A/K}(x) = x^n$ となる。

例 10.3. $A := K[X]/(f)$ で $f = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ とする。$x := X + (f) \in A$ についてその x 倍写像 T_x は

$$T_x = \begin{pmatrix} 0 & & & -a_n \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \vdots \\ & & 1 & -a_1 \end{pmatrix}$$

と書けるから $\mathrm{Tr}_{A/K}(x) = -a_1, \mathrm{N}_{A/K}(x) = (-1)^n a_n$ となる。

Proof. $x \in A$ はその定義から f の根になっている。命題 (**??**) の (2) より $\{1, x, \ldots, x^{n-1}\}$ は A の基底になっているのでこの基底を用いて T_x を行列表示にする。$T_x := (t_{ij})_{i,j=1,\ldots,n}$ は x の指数を考えれば

$$T_x(x^j) = \sum_{i=0}^{n-1} t_{i+1j+1} x^i \ (0 \leq j \leq n-1)$$

とできる。$T_x(x^j) = x^{j+1}$ $(0 \leq j \leq n-1)$ より $1 \leq j+1 \leq n-1$ のとき

$$t_{i+1j+1} = \begin{cases} 1 & (j+1 = i) \\ 0 & (j+1 \neq i) \end{cases}$$

$j+1 = n$ のとき $x \cdot x^{n-1} = x^n = X^n + (f) = -a_1X^{n-1} - \cdots - a_n + (f) = -a_1x^{n-1} - \cdots - a_n$ であるので

$$\begin{aligned} T_x(x^{n-1}) = x^n &= -a_1x^{n-1} - a_2x^{n-2} - \cdots - a_n \\ &= \sum_{i=0}^{n-1} t_{i+1n} x^i = t_{nn}x^{n-1} + t_{n-1n}x^{n-2} + \cdots + t_{1n} \end{aligned}$$

より $t_{n-kn} = -a_{k+1}$ となる。よって T_x は上記の形になる。

$\mathrm{Tr}_{A/K}(x) = \mathrm{Tr}(T_x) = -a_1$ は明らか。$\mathrm{N}_{A/K}(x) = \det(T_x)$ は n 列をとなりの列と順番に入れ替えていけば入れ替えるごとに -1 倍されて 1 列まで移動させれば行列式の性質より $\det(T_x) = (-1)^{n-1}(-a_n)\det(E_n) = (-1)^n a_n$ となる。 □

Fact 10.4. $L/M/K$ に対し、 Tr, N は推移的。つまり、

$$\begin{aligned} \mathrm{Tr}_{L/K} &= \mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} \\ \mathrm{N}_{L/K} &= \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M} \end{aligned}$$

が成り立つ。

10.2 正則表現

命題 10.5. 体拡大 L/K について x 倍写像を作る対応 T を L の K 上の基底 $\{e_1, \ldots, e_n\}$ によって $T_x \in M_n(K)$ で考えると

$$\begin{aligned} T : L &\longrightarrow M_n(K) \\ x &\longmapsto T_x \end{aligned}$$

は T_x の成分の定まり方より写像であり、単射環準同型になる。この K 上の写像 T を基底 $\{e_1, \ldots, e_n\}$ に関する A/K の正則表現という。

Proof. $T_x, T_y, T_{x+y}, T_{cx}, T_{xy} \in M_n(K)$ $(x, y \in A\ c \in K)$ についてこれはそれぞれ

$$\begin{aligned} x(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_x \\ y(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_y \\ (x+y)(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_{x+y} \\ cx(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_{cx} \\ xy(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_{xy} \end{aligned}$$

を満たしている。それぞれ演算結果が等しくなることを考えれば

$$\begin{aligned} T_{x+y} &= T_x + T_y \\ T_{cx} &= cT_x \\ T_{xy} &= T_x T_y \end{aligned}$$

を満たすので $T : L \longrightarrow M_n(K)$ は環準同型である。

また、 e_j が基底なので $T(x) = T_x = 0 \Leftrightarrow t_i j = 0(^\forall i, j) \Leftrightarrow xe_j = 0(^\forall j) \Leftrightarrow x = 0$ が成り立つから $\ker(T) = \{0\}$ より T は単射。 □

10.3 分離拡大のノルムとトレース

命題 10.6. $L/K : n$ 次分離拡大、 $\Omega : K$ の代数閉包、 $\sigma_i \in \mathrm{Hom}_K(L, \Omega), (1 \leq i \leq n = [L : K] = [L : K]_s($分離拡大より$))$ とする。このとき L の n 個の元 $e_1, \ldots, e_n$ について次は同値。

(1) $e_1, \ldots, e_n$ は L/K の基底。

(2)

$$\det(\sigma_i(e_j)) = \begin{vmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \sigma_2(e_1) & \cdots & \sigma_2(e_n) \\ \vdots & & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_n) \end{vmatrix} \neq 0$$

Proof. (1) $\Rightarrow$ (2)

$\det(\sigma_i(e_j)) = 0$ と仮定すると $X = (\sigma_i(e_j))$ とおいたとき $\vec{x}X = 0$ は非自明解 $(c_1, \ldots, c_n) \in \Omega^n$ をもつ。つまり $\sum_{i=1}^n c_i\sigma_i(e_j) = 0$ $(1 \leq j \leq n)$ となるものが存在している。このとき任意の元 $\alpha \in L$ に対して、基底であることより $\alpha = \sum_{i=1}^n a_i e_i$ となる $a_i \in K$ が存在する。このとき σ_i は K を動かさないので

$$\begin{aligned} \sum_{i=1}^n c_i\sigma_i(\alpha) &= \sum_{i=1}^n c_i\sigma_i\left(\sum_{i=1}^n a_i e_i\right) \\ &= \sum_{i=1}^n c_i \sum_{j=1}^n a_j\sigma_i(e_j) \\ &= \sum_{j=1}^n a_j \sum_{i=1}^n c_i\sigma_i(e_j) \\ &= \sum_{j=1}^n a_j \cdot 0 \\ &= 0 \end{aligned}$$

となるが c_i は全ては 0 で無いので Dedekind の補題 (**??**) に矛盾する。よって $\det(\sigma_i(e_j)) \neq 0$

(2) $\Rightarrow$ (1)

(2) を満たすような $e_1, \ldots, e_n$ が一次独立であることを示す。$c_1e_1 + \cdots + c_ne_n = 0$ となる $c_i \in K$ をとる。全体に σ_j をかけると $\sum_{i=1}^n c_i\sigma_j(e_i) = 0$ であるから

$$\begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_n) \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

となる。ここで仮定より $\det(\sigma_i(e_j)) \neq 0$ なのでこの連立方程式は自明解のみをもつから $c_1 = \cdots = c_n = 0$ であるので $e_1, \cdots, e_n$ は一次独立。L/K は n 次拡大なので基底の個数は n 個だからこの $e_1, \cdots, e_n$ が基底になる。 □

命題 10.7. L/K : n 次分離拡大、 Ω を K の代数閉包、$\sigma_i : L \longrightarrow \Omega, \alpha \longmapsto \alpha^{\sigma_i}(= \alpha^{(i)}) := \sigma_i(\alpha), \sigma_i \in \mathrm{Hom}_K(L, \Omega)$ としたとき $\alpha \in L$ について

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \alpha^{(i)} = \sum_{i=1}^n \alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^n \alpha^{(i)} = \prod_{i=1}^n \alpha^{\sigma_i}$$

となる。

Proof. L/K の基底を $e_1, \ldots, e_n$ とする。任意の $\alpha \in L$ についてこの基底による正則表現 $T : L \longrightarrow M_n(K), \alpha \longmapsto T_\alpha$ は $\alpha(e_1, \cdots, e_n) = (e_1, \cdots, e_n)T_\alpha$ を満たす。これに σ_i をかけると $\sigma_i(T_\alpha) = T_\alpha$ であり、$\alpha^{(i)}(e_1^{(i)}, \cdots, e_n^{(i)}) = (e_1^{(i)}, \cdots, e_n^{(i)})T_\alpha$ となる。これは

$$T_\alpha^\circ := \begin{pmatrix} \alpha^{(1)} & & \\ & \ddots & \\ & & \alpha^{(n)} \end{pmatrix}$$

と $M := (e_j^{(i)})_{i,j=1,\ldots,n}$ によって $T_\alpha^\circ M = MT_\alpha$ となる。命題 (10.6) の (1) $\Rightarrow$ (2) より $\det(M) \neq 0$ なので正則行列より M^{-1} が存在するから $T_\alpha = M^{-1}T_\alpha^\circ M$ とできる。したがって Tr と det の性質から

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(T_\alpha) = \mathrm{Tr}(M^{-1}T_\alpha^\circ M) = \mathrm{Tr}(T_\alpha^\circ) = \sum_{i=1}^n \alpha^{(i)} = \sum_{i=1}^n \alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha) = \det(T_\alpha) = \det(M^{-1}T_\alpha^\circ M) = \det(T_\alpha^\circ) = \prod_{i=1}^n \alpha^{(i)} = \prod_{i=1}^n \alpha^{\alpha_i}$$

が成り立つ。 □

系 10.8. L/K が有限次分離拡大なら $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ となる $\alpha \in L$ が存在する。

Proof. 任意の $\alpha \in L$ について命題 (10.7) から $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \alpha^{(i)}$ であり、これが 0 に等しいとすると命題 (**??**) に矛盾するからある $\alpha \in L$ で $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ となる。 □

補題 10.9. L/K を標数 $p>0$ の有限次純非分離拡大とする。このとき $\alpha\in L$ について以下が成立する。

$$\mathrm{Tr}_{L/K}(\alpha)=[L:K]\alpha$$
$$\mathrm{N}_{L/K}(\alpha)=\alpha^{[L:K]}$$

とくに $[L:K]>1$ のとき $\mathrm{Tr}_{L/K}(\alpha)=0$ である。

Proof. 標数 $p>0$ の体の有限次拡大なので $[L:K]=p^e,[L:K(\alpha)]=p^f,[K(\alpha):K]=p^g,f+g=e$ とする。$\mathrm{char}(K)=p>0$ の純非分離拡大なので $K=L_s$ から、補題 (**??**) より α の最小多項式 $f(X)\in K[X]$ が存在して命題 (**??**) より次数は $p^g=[K(\alpha):K]$ なので $f=X^{p^g}-\alpha^{p^g}=(X-\alpha)^{p^g}$ とかける。Tr と N の推移律から

$$\mathrm{Tr}_{L/K}(\alpha)=\mathrm{Tr}_{K(\alpha)/K}(\mathrm{Tr}_{L/K(\alpha)}(\alpha))$$
$$\mathrm{N}_{L/K}(\alpha)=\mathrm{N}_{K(\alpha)/K}(\mathrm{N}_{L/K(\alpha)}(\alpha))$$

である。$\alpha\in K(\alpha)$ より例 (10.2) から $\mathrm{Tr}_{L/K(\alpha)}(\alpha)=[L:K(\alpha)](\alpha),\mathrm{N}_{L/K(\alpha)}(\alpha)=\alpha^{[L:K(\alpha)]}$ であることと Tr が準同型で N が乗法的であることより

$$\mathrm{Tr}_{L/K}(\alpha)=\mathrm{Tr}_{K(\alpha)/K}([L:K(\alpha)]\alpha)=[L:K(\alpha)]\mathrm{Tr}_{K(\alpha)/K}(\alpha)=p^f\mathrm{Tr}_{K(\alpha)/K}(\alpha)$$
$$\mathrm{N}_{L/K}(\alpha)=\mathrm{N}_{K(\alpha)/K}(\alpha^{[L:K(\alpha)]})=(\mathrm{N}_{K(\alpha)/K}(\alpha))^{[L:K(\alpha)]}=\mathrm{N}_{K(\alpha)/K}(\alpha)^{p^f}$$

となる。また、$K(\alpha)=K[X]/(f)$ より例 (10.3) から $f=X^n+a_1X^{n-1}+\cdots+a_n$ のとき $\mathrm{Tr}_{K(\alpha)/K}(\alpha)=-a_1,\mathrm{N}_{K(\alpha)/K}(\alpha)=(-1)^na_n$ である。二項定理より $f=(X-\alpha)^{p^g}=X^{p^g}-p^gX^{n-1}\alpha+\cdots+(-\alpha)^{p^g}$ なので $a_1=-p^g\alpha,a_n=(-\alpha)^{p^g}$ であるのでこれを代入すれば

$$\mathrm{Tr}_{L/K}(\alpha)=p^f\cdot-(-p^g\alpha)=p^{f+g}\alpha=p^e\alpha=[L:K]\alpha$$
$$\mathrm{N}_{L/K}(\alpha)=((-1)^{p^g}(-\alpha)^{p^g})^{p^f}=((-1)^{2p^g}\alpha^{p^g})^{p^f}=\alpha^{p^e}=\alpha^{[L:K]}$$

となり、示された。$[L:K]=p^e$ より $[L:K]>1$ では p の冪なので $\mathrm{char}(K)=p>0$ より $\mathrm{Tr}_{L/K}(\alpha)=0$ である。 □

補題 10.10. 有限次拡大 L/K に対して、K の代数閉包を Ω とし $\sigma_i\in\mathrm{Hom}_K(L,\Omega),1\le i\le s:=[L:K]_s$ とする。このとき $^\forall\alpha\in L$ に対して

$$\mathrm{Tr}_{L/K}(\alpha)=[L:K]_i\sum_{i=1}^{s}\alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha)=\left(\prod_{i=1}^{s}\alpha^{\sigma_i}\right)^{[L:K]_i}$$

となる。(命題 (10.7) では有限次分離拡大であったがより一般に有限次拡大で述べている)

Proof. 定義より $[L:K]_i=[L:L_s],s=[L:K]_s=|\mathrm{Hom}_K(L,\Omega)|$ である。命題 (**??**) から $s=[L:K]_s=[L_s:K]$ となっていてその証明から $\mathrm{Hom}_K(L_s,\Omega)$ と $\mathrm{Hom}_K(L,\Omega)$ の間の定義域を制限する写像が全単射であるから $\sigma_i\in\mathrm{Hom}_K(L,\Omega)$ に対して $\sigma_i|_{L_s}\in\mathrm{Hom}_K(L_s,\Omega)$ が全部で s 個ある。このとき $^\forall\alpha\in L$ に対して L/L_s は定義から純非分離拡大なので命題 (10.9) から

$$\mathrm{Tr}_{L/L_s}(\alpha)=[L:L_s]\alpha=[L:K]_i\alpha$$
$$\mathrm{N}_{L/L_s}(\alpha)=\alpha^{[L:L_s]}=\alpha^{[L:K]_i}$$

となる。$\mathrm{Tr}_{L/L_s}, \mathrm{N}_{L/L_s}$ はともに $L \longrightarrow L_s$ の写像なので $[L:K]_i\alpha, \alpha^{[L:K]_i} \in L_s$ である。

命題 (10.7) から $\mathrm{Tr}_{L_s/K}, \mathrm{N}_{L_s/K}$ について $\sigma_i|_{L_s} : L_s \longrightarrow \Omega, 1 \leq i \leq s$ より

$$\mathrm{Tr}_{L_s/K}(\beta) = \sum_{i=1}^{s} \beta^{\sigma_i|_{L_s}} = \sum_{i=1}^{s} \beta^{\sigma_i}$$
$$\mathrm{N}_{L_s/K}(\gamma) = \prod_{i=1}^{s} \gamma^{\sigma_i|_{L_s}} = \prod_{i=1}^{s} \gamma^{\sigma_i}$$

となる。$\beta := [L:K]_i\alpha, \gamma := \alpha^{[L:K]_i}$ とすれば推移律より

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L_s/K}(\mathrm{Tr}_{L/L_s}(\alpha)) = \mathrm{Tr}_{L_s/K}(\beta) = \sum_{i=1}^{s} \beta^{\sigma} = \sum_{i=1}^{s} [L:K]_i \alpha^{\sigma_i} = [L:K]_i \sum_{i=1}^{s} \alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{L_s/K}(\mathrm{N}_{L/L_s}(\alpha)) = \mathrm{N}_{L_s/K}(\gamma) = \prod_{i=1}^{s} \gamma^{\sigma_i} = \prod_{i=1}^{s} \left(\alpha^{[L:K]_i}\right)^{\sigma_i} = \left(\prod_{i=1}^{s} \alpha^{\sigma_i}\right)^{[L:K]_i}$$

となり成立する。 □

系 10.11. L/K を有限次非分離拡大で $[L:K] > 1$ とすれば任意の $\alpha \in L$ について $\mathrm{Tr}_{L/K}(\alpha) = 0$ となる。

(補題 (10.9) は純非分離拡大のみだったが一般の非分離拡大で成り立つことを述べている)

Proof. $\mathrm{char}(K) = 0$ は分離拡大なので $\mathrm{char}(K) = p > 0$ とする。このとき $[L:K] > 1$ から $[L:K] = p^e$ $(e \in \mathbb{Z}^+)$ であるから $[L:K]_i = [L:L_s] = p^f$ $(f \in \mathbb{Z}^+)$ となる。補題 (10.10) より任意の $\alpha \in L$ で $\mathrm{Tr}_{L/K}(\alpha) = [L:K]_i \sum_{i=1}^{s} \alpha^{\sigma_i} = p^f \sum_{i=1}^{s} \alpha^{\sigma_i}$ となる。これは $\mathrm{char}(K) = p > 0$ より 0 になるので示された。 □

命題 10.12. 有限次拡大 L/K について以下は同値

(1) L/K は分離拡大。

(2) $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ となる $\alpha \in L$ が存在する。

Proof. (1) ⇒ (2)

系 (10.8) で示した。

(2) ⇒ (1)

$[L:K] > 1$ のとき系 (10.11) の対偶をとればよい。$[L:K] = 1$ のとき L_s は $K \subset L_s \subset L$ であり、$L = K$ から $L_s = L$ なので $L/K = L_s/K$ は分離拡大。

□