

## 9 分離的代数拡大

### 9.1 多項式の分離性

命題 9.1. 代数拡大  $L/K$  について次は同値。

- (1)  $L/K$  : 分離的。
- (2)  $L/K$  の  $\forall$  部分拡大  $M/K$  は分離的。

*Proof.* 定義 (??) から明らか。 □

命題 9.2.  $f \in K[X] - K$  について以下は同値。

- (1)  $(f, f') = 1$  ( $\Leftrightarrow f$  とその形式微分  $f'$  が互いに素)
- (2)  $f$  の判別式  $\text{disc}(f) \neq 0$  ( $f = \prod_{i=1}^n (X - \alpha_i)$  のとき  $\text{disc}(f) := \prod_{i < j} (\alpha_i - \alpha_j)^2$  と定義する)
- (3)  $K$  のある拡大  $L$  上で  $f$  は相異なる一次式の積になる。
- (4)  $f$  の任意の根は単根 (重解でない)
- (5)  $K[X]/(f)$  は étale/ $K$  ( $\Leftrightarrow K$  上分離的)

*Proof.* (5)  $\Leftrightarrow$  (1)

系 (??) で示した。

(2)  $\Leftrightarrow$  (3)  $\Leftrightarrow$  (4)

明らか。

(1)  $\Rightarrow$  (2) ( $\deg f > 1$  のときを考える) 対偶  $\text{disc}(f) = 0 \Rightarrow (f, f') \neq 1$  を示す。

$\text{disc}(f) = 0$  よりある  $0 \leq i < j \leq n$  があり  $\alpha_i = \alpha_j$  となる。 $i = 1, j = 2$  としても一般性を失わない。これは  $f$  の根なので  $f = (X - \alpha_1)^2 Q(X)$  となる  $Q(X) \in K[X]$  が存在する。よって  $f' = 2(X - \alpha_1)Q(X) + (X - \alpha_1)^2 Q'(X) = (X - \alpha_1)(2Q(X) + (X - \alpha_1)Q'(X))$  となるから  $f, f'$  は共通の  $\alpha_1$  という根を持つので互いに素でないから  $(f, f') \neq 1$  となる。

(2)  $\Rightarrow$  (1) ( $\deg f > 1$  のときを考える) 対偶  $(f, f') \neq 1 \Rightarrow \text{disc}(f) = 0$  を示す。

$(f, f') \neq 1$  よりある  $\alpha$  があってそれを  $f = (X - \alpha)Q_1(X), f' = (X - \alpha)Q_2(X)$  として共通根として持つ。この二つから  $f' = Q_1(X) + (X - \alpha)Q_1'(X) = (X - \alpha)Q_2(X)$  より  $(X - \alpha)(Q_1'(X) - Q_2(X)) = Q_1(X)$  となるから  $f = (X - \alpha)^2(Q_1'(X) - Q_2(X))$  より重根をもつ。したがって根の差の積である  $\text{disc}(f) = 0$  である。

$\deg f = 1$  のときは  $f$  の根は 0 より常に  $\text{disc}(f) = 0$  となるからこの命題には不適。 □

定義 9.3. これらが成り立つとき  $f$  を分離的という。そうでないとき非分離的という。

命題 9.4. 既約多項式  $f \in K[X]$  について次は同値。

- (1)  $f$  は分離的。
- (2)  $f$  は ( $\exists L$  に) 少なくとも一つの単根をもつ。
- (3)  $f' \neq 0$
- (4)  $\text{char}(K) = 0$  か、または  $\text{char}(K) = p > 0$  で  $f \notin K[X^p]$

*Proof.* (1)  $\Rightarrow$  (2) は命題 (9.2) で示した。

(2)  $\Rightarrow$  (3)

$\alpha$  を  $f$  の単根とする。  $f'(\alpha) = 0$  とすると命題 (9.2) の (2)  $\Rightarrow$  (1) の証明より  $f = (X - \alpha)^2 Q(X)$  となるから  $\alpha$  が単根に矛盾するので  $f'(\alpha) \neq 0$  である。よって  $f' \neq 0$

(3)  $\Rightarrow$  (1)

体上の多項式より  $f$  を monic としよ。  $\alpha$  を  $f$  の任意の根とする。  $f$  が既約多項式で monic より  $f$  は最小多項式であるからその次数の最小性と  $f' \neq 0$  より  $f'$  は多項式で  $f'(\alpha) \neq 0$  であるから  $\alpha$  は単根。これが任意の  $f$  の根について成り立つから  $f$  は分離的。

(3)  $\Leftrightarrow$  (4)

$f = \sum_{i=0}^n a_i X^i \in K[X]$  について

$$\begin{aligned} f' &= \sum_{i=0}^n a_i i X^{i-1} = 0 \\ &\Leftrightarrow \begin{cases} a_1 = \cdots = a_n = 0 & (\text{char}(K) = 0) \\ a_i = 0 \ (p \nmid i) & (\text{char}(K) = p > 0) \end{cases} \\ &\Leftrightarrow \begin{cases} f = a_0 & (\text{char}(K) = 0) \\ f = \sum a_{pk} X^{pk} \in K[X^p] & (\text{char}(K) = p > 0) \end{cases} \end{aligned}$$

より、既約多項式は  $f \in K[X] - K$  で否定を考えれば成立。 □

**系 9.5.** 体  $K$  について次は同値。

(1)  $K$  は完全体

(2) 任意の既約多項式  $f \in K[X]$  は分離的

((3)  $\forall L/K$  : 代数拡大は分離的)

*Proof.* (1)  $\Leftrightarrow$  (2) のみ示す。

$\text{char}(K) = 0$  のとき命題 (9.4) の (1)  $\Leftrightarrow$  (4) から  $\forall$  既約多項式  $f \in K[X]$  は分離的。

$\text{char}(K) = p > 0$  のとき

$$K \text{ が完全体} \Leftrightarrow \forall f \in K[X^p] - K \text{ は可約}$$

を示す。これより、既約ならば  $f \notin K[X^p] - K$  が言えて命題 (9.4) の (4)  $\Leftrightarrow$  (1) より既約ならば分離的が言える。

( $\Rightarrow$ )

$f = \sum a_i X^{pi} \in K[X^p] - K$  で  $K^p := \{x^p | x \in K\}$  ( $p$  乗元の集合) とする。  $K$  が完全体なので Frobenius が全射だから  $K = K^p$  なので  $\forall a_i \in K$  に対して  $\exists b_i \in K, a_i = b_i^p \in K^p = K$  である。したがって  $\text{char}(K) = p > 0$  に注意すれば  $f = \sum b_i^p X^{pi} = (\sum b_i X^i)^p$  より  $\sum b_i X^i \in K[X]$  で分解できるから  $f$  は可約。

( $\Leftarrow$ ) 対偶の  $K$  : 非完全  $\Rightarrow \exists f \in K[X^p] - K$  は既約 を示す。

$K$  : 非完全とする。このとき  $K^p \neq K$  から  $\exists a \in K^\times - K^p$  が取れる。ここで  $f = X^p 0a \in K[X]$  は既約になる。

$b$  を  $f$  の根 ( $b^p = a$ ) とし、  $g$  を  $b$  の  $K$  上の最小多項式とする。最小性から  $g \mid f$  で  $\text{char}(K) = p > 0$  より  $f = (X - b)^p$  となるから  $g = (X - b)^d$  ( $d^e = p$ ) と書ける。  $f = g^e$  の形になり、  $p$  が素数から  $d = p$  または  $d = 1$  になる。  $d = 1$  とすると  $g \in K[X]$  より  $b \in K$  であり、  $a = b^p \in K^p$  から  $a \in K^\times - K^p$  に矛盾する。

よって  $d = p$  で  $f = g$  となるから  $f$  は既約。これより既約な  $f \in K[K^p] - K$  が存在するので対偶が示された。  $\square$

## 9.2 元の分離性

**定義 9.6.**  $L/K$  : 拡大としたとき、 $K$  上代数的な元  $x \in L$  が  $K$  上分離的とは体の拡大  $K(x)/K$  が分離的であること。そうでないとき非分離的という。

**命題 9.7.**  $x \in L$  :  $K$  上代数的な元、 $f : x$  の最小多項式とすると、次は同値。

- (1)  $x$  は  $K$  上分離的。
- (2)  $f$  は分離多項式。
- (3)  $x$  は  $f$  の単根。
- (4)  $K[X]/(f)$  は  $K$  上 etale ( $\Leftrightarrow K$  上分離的)

*Proof.*  $x$  が  $K$  上代数的なので命題 (??) から  $K(x) = K[X]/(f)$  となる。

$x$  が  $K$  上分離的るとき定義から  $K(x)/K$  が分離的なので  $K[X]/(f)$  が  $K$  上分離的である。そして命題 (9.2) の (5)  $\Leftrightarrow$  (4) より  $f$  の任意の根は単根より  $x$  は  $f$  の単根であり、 $f$  は分離多項式である。  $\square$

**系 9.8.**  $x \in L$  が  $\exists g \in K[X]$  の単根ならば  $x$  は  $K$  上分離的。

*Proof.*  $x$  の最小多項式を  $f$  としたとき最小性から  $f \mid g$  より  $f = gh$  となる  $h \in K[X]$  が存在する。このとき  $h$  が  $x$  を根として持っているとする  $f$  の最小性に矛盾するから  $h(x) \neq 0$  である。したがって  $f = gh$  は  $x$  を単根としてもつので命題 (9.7) から  $x$  は  $K$  上分離的。  $\square$

**系 9.9.**  $x \in L$  が  $K$  上分離的ならば  $L/K$  の任意の中間体  $M$  でも分離的。

*Proof.*  $x$  の  $M$  上の最小多項式を  $f_M$  とし、 $K$  上の最小多項式を  $f_K$  とする。このとき  $K[X] \subset M[X]$  から  $M[X]$  上で  $f_M \mid f_K$  となる。 $x$  は  $K$  上分離的なので  $f_K$  の単根であるから系 (9.8) で  $g = f_K \in M[X]$  と見れば  $x$  は  $M$  上分離的である。  $\square$

**命題 9.10.** 拡大  $L/K$  について以下は同値。

- (1)  $L$  は  $K$  上代数的かつ分離的。
- (2)  $L$  の任意の元  $x$  は  $K$  上代数的かつ分離的。
- (3)  $L$  は  $K$  上代数的かつ分離的な元のある部分集合  $S (\subset L)$  によって  $K$  上生成される。 $(L = K(S)$  となる)

*Proof.* (1)  $\Rightarrow$  (2)  $L/K$  が代数的なので  $L$  の任意の元は  $K$  上代数的。分離的であることから、 $L/K$  の任意の有限次部分拡大が分離的である。 $\forall x \in L$  は代数的元なので命題 (??) より  $K(x)/K$  は有限次部分拡大。したがって  $K(x)/K$  が分離的だから定義より  $x$  は分離的。

(2)  $\Rightarrow$  (3) 仮定より  $L$  の任意の元は  $K$  上代数的かつ分離的なので  $S = L$  ととれて、 $K(L) = L$  より成立する。

(3)  $\Rightarrow$  (1) 任意の  $x \in L$  は  $S$  のある有限部分集合  $S'$  によって  $x \in K(S')$  となり、 $K(S')$  は有限次拡大より  $x$  は  $K$  上代数的。よって  $L$  は  $K$  上代数的。 $S' = \{\alpha_1, \dots, \alpha_n\}$  となっている時を考えれば良い。 $L' = K(S') (= K(\alpha_1, \dots, \alpha_n))$  とおくと  $\alpha_i \in L$  は  $K$  上代数的なので命題 (??) から  $L'/K$  は有限次拡大よ

り代数的である。  $K_0 := K, K_n := L'$  として、  $K_{i+1} := K_i(\alpha_{i+1}), 0 \leq i \leq n-1$  と定めると拡大の列

$$K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$$

が作られる。  $\alpha_{i+1}$  は  $K$  上分離的なので系 (9.9) から  $K_n/K_0$  の中間体である  $K_i$  上分離的になる。よって定義から  $K_i(\alpha_i)/K_i = K_{i+1}/K_i$  は分離的であるので  $[K_{i+1} : K_i]_s = [K_{i+1} : K_i]$  となり、  $L'/K$  が有限次より  $[K_{i+1} : K_i]$  も有限だから命題 (??) の (3) を繰り返し用いれば

$$\begin{aligned} [L' : K] &= [K_n : K_0] = \prod_{i=0}^{n-1} [K_{i+1} : K_i] \\ &= \prod_{i=0}^{n-1} [K_{i+1} : K_i]_s = [K_n : K_0]_s = [L' : K]_s \end{aligned}$$

となり  $L'/K$  は分離的である。 □

**系 9.11.** 代数拡大  $L/K$  において次は同値。

- (1)  $L/K$  は分離的。
- (2)  $\forall x \in L$  は  $K$  上の最小多項式の単根。

*Proof.* 命題 (9.10) の (1)  $\Leftrightarrow$  (2) から成立する。 □

**命題 9.12.** (1)  $L/K$  がある集合  $S$  によって  $L = K(S)$  とするとき

$S$  の任意の元が  $K$  上代数的かつ分離的  $\Rightarrow L/K$  は分離的

- (2) 代数拡大  $L_1/K, L_2/K$  ( $\subset {}^3L$ ) に対して  $L_1, L_2$  の合成体を  $L_1L_2$  とすると、

$L_1L_2/K$  が分離的  $\Leftrightarrow L_1/K, L_2/K$  がともに分離的

- (3)  $L/M/K$  で  $L/K$  : 代数拡大のとき

$L/K$  が分離的  $\Leftrightarrow L/M, M/K$  が分離的

- (4)  $L/K, K'/K$  とその合成体  $L' := LK' = K'(L)$  について  $L/K$  が代数的であるとき

$L/K$  が分離的  $\Rightarrow L'/K'$  が分離的

*Proof.* (1)

$S$  の元は代数的かつ分離的で  $L$  は  $K$  上  $S$  で生成されるから命題 (9.10) の (3)  $\Leftrightarrow$  (1) から成立。

(2)

( $\Rightarrow$ ) 定義より  $L_1, L_2 \subset L_1L_2$  から明らか。

( $\Leftarrow$ ) (4) で  $L = L_1, K' = L_2, L' = L_1L_2$  とおけば  $L_1/K$  が分離的より  $L_1L_2/L_2$  が分離的になる。(3) から  $L_1L_2/L_2, L_2/K$  が分離的より  $L_1L_2/K$  が分離的より示された。

(3)

( $\Rightarrow$ )  $L/K$  が分離的より、  $\forall x \in L$  は  $K$  上分離的。したがって  $\forall x \in M \subset L$  も  $K$  上分離的であるから  $M$  は  $K$  上分離的。また、系 (9.9) より  $\forall x \in L$  は  $M$  上分離的でもあるので  $L$  は  $M$  上分離的。

( $\Leftarrow$ ) まず、命題 (??) より、  $L/M, M/K$  は代数拡大。  $\forall x \in L$  をとると  $M$  上代数的かつ分離的より最小多項式  $f = \sum_{i=0}^n a_i X^i \in M[X]$  があり、これは分離多項式である。  $M' := K(a_1, \dots, a_n)$  とすると  $f \in M'[X]$

であり、 $x$  の最小多項式のままである。 $L' := M'(x) (= K(x, a_1, \dots, a_n))$  とすると、命題 (??) と  $f \in M'[X]$  から、 $L' = M'[X]/(f)$  は有限次拡大で、 $x$  は最小多項式  $f$  の単根だから命題 (9.7) より、 $L'$  は  $M'$  上分離的。また、 $M'/K$  は  $M/K$  が分離的より定義から分離的。よって  $L'/M, M'/K$  が有限次拡大かつ分離的であることから系 (??) の (3) から  $[L' : K] = [L' : M'][M' : K] = [L' : M']_s [M' : K]_s = [L' : K]_s$  となるので  $L'/K$  も分離的。したがって  $x \in L'$  は  $K$  上分離的であるから元の任意性より  $L$  は  $K$  上分離的。

(4)

$L/K$  が代数的より、 $\forall x \in L$  は  $K$  上代数的であるが、 $K \subset K'$  より  $K'$  上代数的でもある。また、 $x$  の  $K$  上の最小多項式を  $f$  とすると  $f \in K[X] \subset K'[X]$  で、 $L/K$  が分離的から  $x$  は  $f$  の単根なので系 (9.8) より  $x$  は  $K'$  上分離的。したがって  $L$  は  $K'$  上分離的かつ代数的な元の集合なので命題 (9.10) の (3)  $\Leftrightarrow$  (1) から  $L' = K'(L)$  は  $K'$  上代数的かつ分離的。  $\square$

### 9.3 原始元

**定義 9.13.**  $L/K$  : 拡大で、 $x \in L$  が  $L/K$  の原始元 (primitive element)とは  $L = K[x] (= K[X]/(f) = K(x))$  となること。ただし  $f$  は  $x$  の  $K$  上の最小多項式である。定理 (??) から  $L/K$  が原始元を持つためには有限次拡大であることが必要である。

**定理 9.14.**  $L/K$  について次は同値。

- (1)  $L/K$  は原始元をもつ
  - (2)  $L/K$  は中間体を有限個しか持たない。
- さらに、 $L/K$  が有限次分離拡大ならこれらが成立する。

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

原始元を  $x \in L$  とし、その最小多項式を  $f \in K[X]$  とする。 $f$  を  $L$  上で割り切ることができる monic 多項式  $g \in L[X]$  に対して、その係数で生成される  $K$  上の体を  $E_g$  とする。この  $\deg(f) = n$  のとき、 $L$  で  $f$  は高々  $n$  個の既約多項式の積に表すことができる。この既約多項式の積の組み合わせが  $g$  になりうるので  $g$  の個数は高々  $2^n$  個であるのでこのような体  $E_g$  は有限個である。 $L$  の中間体が全て  $E_g$  でかければ有限個だけであることがわかるのでそれを示す。

$M$  をある中間体とすると  $K \subset M, L = K[x]$  より  $M[x] = L$  となる。ここで  $x$  の  $M$  上の最小多項式を  $f_M$  とすると  $[L : M] = \deg(f_M)$  である。 $K[X] \subset M[X]$  より  $f_M | f$  であるので  $f_M$  は  $M$  上、したがって  $L$  上で  $f$  を割り切る。 $f_M \in M[X]$  より  $f_M$  の係数はすべて  $M$  に含まれているから  $E_{f_M} \subset M$  である。また、 $E_{f_M}[x] = L$  より、 $f_M \in E_{f_M}[X], f_M(x) = 0$  から  $[L : E_{f_M}] \leq \deg(f_M) = [L : M]$  となるので  $M \subset E_{f_M}$  である。したがって  $M = E_{f_M}$  となり  $E_g$  の形で書けるから中間体は高々  $2^n$  個の有限個しか持たない。

(2)  $\Rightarrow$  (1)

まず原始元の最小多項式の存在性のため、 $L/K$  が代数拡大であることを背理法により示す。 $L/K$  が超越元  $x$  を持つと仮定する。このとき命題 (??) の (3)  $\Leftrightarrow$  (1) の否定から  $1, x, x^2, \dots$  は一次独立である。したがってその部分集合  $1, x^2, (x^2)^2, \dots$  も一次独立より  $x^2$  も  $K$  上超越元である。ここで  $K(x) = K(x^2)$  と仮定すると、 $x = f(x^2)/g(x^2)$  となる  $f(X), g(X) (\neq 0) \in K[X]$  が存在するから、 $x$  が  $Xg(X^2) - f(X^2) \in K[X]$  の根になる。 $Xg(X^2)$  は奇数次、 $f(X^2)$  は偶数次より  $Xg(X^2) - f(X^2)$  となるからこれは  $x$  を根にもつ 0 でない  $K$  上多項式になるため  $x$  の超越性に矛盾する。よって  $K(x) \neq K(x^2)$  であるから  $K(x^2) \subsetneq K(x)$  で

ある。これを繰り返せば

$$K \subset \cdots \subsetneq K(x^3) \subsetneq K(x^2) \subsetneq K(x) \subset L$$

となり無限個の中間体が存在してしまうのでこれは仮定に矛盾するから  $L/K$  は超越元を持たないから代数拡大である。

さらに、 $L/K$  は有限生成であることを背理法により示す。有限生成でないとすると  $\alpha_i \in L$  より

$$K \subsetneq K(\alpha_1) \subsetneq K(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq K(\alpha_1, \dots, \alpha_n) \subsetneq \cdots \subset L$$

として無限個の中間体が存在してしまうので仮定に矛盾するから  $L/K$  は有限生成。以上より  $L/K$  は有限次元代数拡大である。

単拡大であることを示す。

・  $K$  が有限体のとき

系 (??) からある素数  $p$  と正整数  $f = [K : F_p]$  があり、 $q = p^f$  として、 $K \cong F_q$  (位数  $q = p^f$  の有限体) となる。 $L/K$  は有限次拡大より拡大次数を  $e$  とすると、 $L \cong F_{q^e}$  とできる。 $F_{q^e}$  の乗法群  $F_{q^e}^\times$  は位数  $q^e - 1$  の巡回群になるので  $F_{q^e}^\times$  は位数  $q^e - 1$  の元  $\zeta \in F_{q^e}^\times$  を持つ。したがって  $F_{q^e}^\times = \{1, \zeta, \dots, \zeta^{q^e-2}\}$  から、 $F_{q^e} = \{0, 1, \zeta, \dots, \zeta^{q^e-2}\}$  となる。よって  $F_{q^e} \subset F_q(\zeta) \subset F_{q^e}$  から  $L = F_{q^e} = F_q(\zeta) = K(\zeta)$  より原始元  $\zeta$  が存在する。

・  $K$  が無限体のとき

$\forall \alpha \in L$  について有限次拡大より  $[K(\alpha) : K] \leq [L : K] \leq \infty$  なので  $\{[K(\alpha) : K] | \alpha \in L\}$  は正整数の有界集合。したがってある  $\alpha_0 \in L$  が存在して、 $\forall \alpha \in L$  で  $[K(\alpha) : K] \leq [K(\alpha_0) : K]$  となる。ここで任意に  $\beta \in L$  を一つ定める。 $\forall c \in K$  について  $M_c := K(c\alpha_0 + \beta)$  とする。これは  $L/K$  の中間体より有限個しかないが  $K$  が無限体より、 $c$  は無限個とれるのである異なる  $c_1, c_2 \in K$  で  $M := M_{c_1} = M_{c_2}$  となる。このとき  $c_1, c_2 \in K \subset M$  から  $c_1 - c_2 \in M, c_1 - c_2 \neq 0$  より  $(c_1 - c_2)^{-1} \in M$  が存在する。また、 $(c_1\alpha_0 + \beta) - (c_2\alpha_0 + \beta) = (c_1 - c_2)\alpha_0 \in M$  なので  $(c_1 - c_2)^{-1}$  をかけても  $M$  に含まれているので  $\alpha_0 \in M$  となる。そして  $c_1\alpha_0 \in M$  にもなるので  $\beta = (c_1\alpha_0 + \beta) - c_1\alpha_0 \in M$  である。これより、 $K(\alpha_0) \subset M = K(c_1\alpha_0 + \beta)$  で  $[K(\alpha_0) : K] \leq [K(c_1\alpha_0 + \beta) : K]$  となるが  $\alpha_0$  の定義から  $[K(\alpha_0) : K] = [K(c_1\alpha_0 + \beta) : K]$  で  $K(\alpha_0) = K(c_1\alpha_0 + \beta) = M$  である。そして任意にとった  $\beta \in L$  が  $M = K(\alpha_0)$  に含まれるので  $L = K(\alpha_0)$  となるから  $L/K$  は原始元  $\alpha_0$  をもつ。□

**例 9.15.**  $L := F_p(X, Y), K := F_p(X^p, Y^p)$  とする。この中間体として  $K(f_i), f_i := X + g_i Y, g_i \in F_p(X, Y)$  をとると、 $g_i \neq g_j \Rightarrow K(f_i) \neq K(f_j)$  となり、 $g_i$  のとり方は無限個あるので  $L/K$  の中間体は無限個あるから  $L/K$  に原始元は存在しない。

**例 9.16.**  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$  は  $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$  ともできるので原始元が存在するから中間体は有限個。

## 9.4 分離閉体、分離閉包

**定義 9.17.**  $L/K$  : 拡大に対して  $K$  の  $L$  の中での 相対的分離 (代数) 閉包 (relative separable (algebraic) closure)  $L_s$  とは

$$L_s := \{x \in L | x \text{ は } K \text{ 上分離的}\}$$

となるもの。これは命題 (9.10) の (2)  $\Leftrightarrow$  (1) より  $K$  上代数的かつ分離的な拡大で  $L$  に含まれる代数的かつ分離的な拡大のうち最大のもの。

**定義 9.18.** 体  $\Omega$  が分離閉体 (separably closed) とはその分離的代数拡大は  $\Omega$  のみであること。

**定義 9.19.**  $\Omega$  が体  $K$  の分離閉包 (separable closure) とは  $K$  の代数拡大で分離閉体であること。 $K$  上分離閉な拡大ともいう。

**命題 9.20.**  $\Omega : K$  上代数閉な拡大とすると

- (1)  $\Omega_s$  は  $K$  の分離閉包。
- (2)  $K$  の分離閉包は  $K$  上の同型を除き一意

*Proof.* (1)  $L$  を  $\Omega_s$  の分離的代数拡大とする。 $\Omega_s$  は  $K$  上代数的な元の集合でもあるので  $\Omega$  が  $K$  上の代数閉包より拡大  $\Omega/\Omega_s$  がつくれる。 $L/\Omega_s$  は代数拡大で  $\Omega$  は代数閉体なので命題 (??) から  $\Omega_s$ –準同型  $u : L \rightarrow \Omega$  が存在し、 $\Omega$  の中に  $L$  を  $u(L)$  として埋め込める。このとき  $\Omega$  の中で  $u(L)/\Omega_s, \Omega_s/K$  はともに分離的なので命題 (9.12) の (3) より  $u(L)/K$  は分離的で  $u$  は  $\Omega_s$ –準同型から  $K$ –準同型でもあるので構造を保存するから  $u(L)/K$  は代数拡大。したがって  $u(L)/K$  は代数的かつ分離的な拡大であり  $\Omega_s \subset u(L)$  なので相対的分離閉包の最大性から  $\Omega_s = u(L)$  となる。これより  $u$  の終域を制限して  $\Omega_s$ –準同型  $u : L \rightarrow \Omega_s$  とできる。これは体の準同型から単射であり、 $u(L) = \Omega_s$  より全射なので同型なので  $L \cong \Omega_s$  となる。そして、 $L$  は  $\Omega_s$  の拡大なので  $\Omega_s \subset L$  から  $L = \Omega_s$  となる。 $\Omega_s$  の任意の分離的代数拡大は  $\Omega_s$  だけであることが示されたので  $\Omega_s$  は分離閉体である。相対的分離閉包の定義から  $K$  の代数拡大でもあるので  $K$  の分離閉包である。

(2)  $E$  を  $K$  の分離閉包とする。 $E$  は  $K$  の代数拡大より  $\Omega$  が  $K$  の代数閉包より定理 (??) から  $K$ –準同型  $v : E \rightarrow \Omega$  が存在して  $E$  を  $\Omega$  に  $v(E)$  として埋め込める。 $v$  は構造を保存するから  $v(E)$  は  $K$  の分離閉包なので分離的代数拡大になっているから  $\Omega_s$  の最大性より  $v(E) \subset \Omega_s$  であり、 $v(E)$  は  $\Omega_s/K$  の中間体となっている。 $\Omega_s/K$  が分離的より命題 (9.12) の (3) から  $\Omega_s/v(E)$  は分離的。 $v(E)$  が  $K$  の分離閉包より分離閉体だから  $v(E)$  の分離拡大はそれ自身だけなので  $v(E) = \Omega_s$  である。 $E \subset \Omega_s$  は一般に言っていないので  $E = \Omega_s$  とはならない。これより、 $v$  の終域を制限した  $K$ –準同型  $v : E \rightarrow \Omega_s$  は同型写像になるので任意の  $K$  の分離閉包は  $\Omega_s$  と同型になるから同型を除いて一意に定まる。□

**系 9.21.**  $L/K$  : 分離的代数拡大、 $E/K$  : 分離閉な拡大としたときある  $K$ –準同型  $\phi : L \rightarrow E$  が存在する。(任意の分離的代数拡大は分離閉体  $E$  に埋め込める)

定理 (??) の代数閉体のときと同じである。

*Proof.*  $\Omega$  を  $E$  の代数閉包とすると  $K$  の  $\Omega$  の中での相対的分離閉包  $\Omega_s$  は  $K$  上分離的な元の集合なので  $\Omega_s \subset E$  である。 $\Omega$  は  $K$  上代数閉でもあるので命題 (9.20) の (1) より  $\Omega_s$  は  $K$  の分離閉包となるから (2) と  $\Omega_s \subset E$  から同型より更に、 $\Omega_s = E$  となる。また、 $\Omega$  は  $K$  の代数閉包であるから  $L/K$  が代数拡大より定理 (??) から  $K$ –準同型  $v : L \rightarrow \Omega$  が存在する。 $v$  は構造を保存するから  $v(L)$  は  $K$  上分離的かつ代数的であるから、 $v(L) \subset \Omega_s = E$  である。したがって  $K$ –準同型  $v : L \rightarrow E$  が存在する。□

## 9.5 非分離次数

**定義 9.22.**  $L/K$  とその  $K$  の  $L$  の中での相対的分離閉包  $L_s$  について  $[L : K]_i := [L : L_s]$  を  $L/K$  の非分離次数 (inseparable degree) という。

**補題 9.23.** 有限次拡大  $L/K$  とその相対的分離閉包  $L_s$  について  $x \in L - L_s$  の  $L_s$  上の最小多項式  $f \in L_s[X]$

はある素数  $p$  と正整数  $e$  と  $y \in L_s$  で  $f = X^{p^e} - y$  と書ける。

*Proof.*  $L/K$  が有限次拡大より代数拡大である。  $\text{char}(K) = 0$  のとき  $K$  は完全体より系 (9.5) の (1)  $\Leftrightarrow$  (3) からその任意の代数拡大  $L/K$  は分離的なので  $L = L_s$  となる。したがって  $L - L_s = \emptyset$  より補題は成立する。

$\text{char}(K) = p > 0$  のときのみを考える。  $f$  の根  $x$  は  $K$  上分離的な元の集合の  $L_s$  に含まれないので非分離的な元である。したがって  $f$  は非分離的なので命題 (9.4) の (1)  $\Leftrightarrow$  (4) から  $\text{char}(K) = p > 0$  で考えていることに注意すれば  $f \in L_s[X^p]$  である。よって  $f = g_1(X^p), g_1 \in L_s[X]$  となる  $g_1$  が存在する。もし  $g_1$  が非分離的であるとまた  $f$  と同様に  $g_1 \in L_s[X^p]$  となるから  $g_1 = g_2(X^p), g_2 \in L_s[X]$  となる  $g_2$  が存在し、  $f = g_2(X^{p^2})$  となる。これを  $g_n$  と  $g_{n+1}$  に帰納的に繰り返せば  $f, g_i$  が有限次よりあるところで分離的な多項式になり止まるのでこれを  $g_e = g$  とおくと  $f = g(X^{p^e}), g \in L_s[X], e \in \mathbb{Z}$  と書ける。  $f \in L_s[X^p]$  より  $\deg(f) = p^{e'}$  とおけるので  $p^e \cdot \deg(g) = \deg(f) = p^{e'}$  が成り立つ。

$f$  は  $x$  を根として持つので  $f(x) = g(x^{p^e}) = 0$  より  $g$  の根でもある。この  $g$  の根を  $y$  とすると  $y$  は  $L_s$  上分離的で  $y = x^{p^e} \in L$  である。  $L_s$  上分離的な元なので定義より  $L_s(y)/L_s$  が分離的となるが  $L_s$  は命題 (9.20) の (1) より分離閉体なので  $L_s(y) = L_s$  とならなくてはならない。したがって  $y \in L_s$  である。ここで  $h(X) = X^{p^e} - y$  とすると  $h(X) \in L_s[X]$  であり、  $\text{char}(K) = p > 0$  より  $(X - x)^{p^e} = X^{p^e} - x^{p^e} = X^{p^e} - y = h(X)$  から  $h(X)$  は  $x$  を根にもつ  $L_s$  上の多項式となる。

このとき  $\deg(g) > 1$  と仮定すると  $p^e \cdot \deg(g) = p^{e'}$  の等式より  $p^{e'-e} = \deg(g) > 1$  から  $e' > e$  となるから  $\deg(h) = p^e < p^{e'} = \deg(f)$  となる。しかしこれは  $f$  の最小性に矛盾するから  $\deg(g) = 1$  である。したがって  $g(X) = X - y$  より  $f(X) = g(X^{p^e}) = X^{p^e} - y$  となるので  $x \in L - L_s$  の最小多項式は  $x^{p^e} = y$  となる  $y \in L_s$  によって  $X^{p^e} - y$  とかける。

□

**命題 9.24.** 有限次拡大  $L/K$  について

$$[L : K]_s = [L_s : K]$$

がなりたつ。

*Proof.*  $\Omega$  を  $K$  の代数閉包とする。  $L_s/K$  は命題 (9.10) の (2)  $\Leftrightarrow$  (1) より分離的なので  $[L_s : K]_s = [L_s : K] = |\text{Hom}_K(L_s, \Omega)|$  となる。そして、  $[L : K]_s = |\text{Hom}_K(L, \Omega)|$  であるから定義域を制限する写像  $\text{Hom}_K(L_s, \Omega) \rightarrow \text{Hom}_K(L, \Omega)$  が全単射であることを示せば  $[L : K]_s = [L_s : K]$  となることが示される。

・全射性

$\forall \phi \in \text{Hom}_K(L_s, \Omega)$  の  $L$  への拡張を  $\tilde{\phi} \in \text{Hom}_K(L, \Omega)$  とする。補題 (9.23) から  $x \in L - L_s$  の  $L_s$  上の最小多項式がある素数  $p$  と  $n \in \mathbb{Z}$  と  $a \in L_s$  で  $X^{p^n} - a$  の形になる。よって  $\tilde{\phi}(x)^{p^n} = \tilde{\phi}(x^{p^n}) = \tilde{\phi}(a) = \phi(a)$  より  $\tilde{\phi}(x) = \phi(a)^{1/p^n}$  と定まる。この  $\tilde{\phi}$  をとればいいので全射

・単射性

$\phi \in \text{Hom}_K(L_s, \Omega)$  の  $\tilde{\phi} \in \text{Hom}_K(L, \Omega)$  への延長は  $\tilde{\phi}(x) = \phi(a)^{1/p^n}$  より  $\phi$  に依るので一意的なので単射。

□