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 $\mathrm{disc}(f) \neq 0$ ($f = \prod_{i=1}^{n}(X - \alpha_i)$ のとき $\mathrm{dics}(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$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 etale$/K$ ($\Leftrightarrow K$ 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 $\mathrm{disc}(f) = 0 \Rightarrow (f, f') \neq 1$ を示す。

$\mathrm{dics}(f) = 0$ 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 $f' = 2(X - \alpha_1)Q(X) + (X - \alpha_1)^2 Q'(X) = (X - \alpha_1)(2Q(X) + (X - \alpha_1)^2 Q'(X))$ となるから f, f' は共通の α_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 $(f, f') \neq 1 \Rightarrow \mathrm{disc}(f) = 0$ を示す。

$(f, f') \neq 1$ よりある α 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 $\mathrm{disc}(f) = 0$ である。

$\deg f = 1$ のときは f の根は 0 より常に $\mathrm{disc}(f) = 0$ 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<u>分離的</u>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) $\mathrm{char}(K) = 0$ か、または $\mathrm{char}(K) = p > 0$ で $f \notin K[X^p]$

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

(2) $\Rightarrow$ (3)

α 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 $f=(X-\alpha)^2Q(X)$ となるから α 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 としてよい。α 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 α 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)

$f=\sum_{i=0}^n a_iX^i\in K[X]$ について

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

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

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。

$\mathrm{char}(K)=0$ 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。

$\mathrm{char}(K)=p>0$ 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。

($\Rightarrow$)

$f=\sum a_iX^{pi}\in K[X^p]-K$ 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 $\mathrm{char}(K)=p>0$ に注意すれば $f=\sum b_i^pX^{pi}=(\sum b_iX^i)^p$ より $\sum b_iX^i\in K[X]$ 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 $f=X^p0a\in K[X]$ 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 $\mathrm{char}(K)=p>0$ 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$\underline{K \text{ 上分離的}}$とは体の拡大 $K(x)/K$ が分離的であること。

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き、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 上分離的なとき定義から $K(x)/K$ 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と 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。M を任意の K の有限次部分拡大とする。このとき有限次拡大なので系 (**??**) から $M = K(x_1, \ldots, x_m)$ となる元 $\{x_1, \ldots, x_m\}$ がある。仮定より $x_i \in S$ は分離的

かつ代数的なのでその最小多項式を f_i としたとき、命題 (9.7) から $K(x_i) \cong K[X]/(f)$ は K 上 etale である。したがって系 (**??**) より $K(x_1) \otimes \cdots \otimes K(x_m)$ も K 上 etale である。そして、 M は Rem (**??**) より $K(x_1) \otimes \cdots \otimes K(x_m)$ の商 $K-alg$ の部分代数と同型。したがって M も etale より M は分離的であるので任意の有限次部分拡大が分離的なので L/K は代数的かつ分離的。 □

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

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

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

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

(3) $L/M/K$ で L/K : 代数拡大のとき

$$L/K \text{ が分離的} \Leftrightarrow L/M, M/K \text{ が分離的}$$

(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

$$L/K \text{ が分離的} \Rightarrow L'/K' \text{が分離的}$$

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。$M' := K(a_1, \ldots, a_n)$ とすると $f \in M'[X]$ であり、x の最小多項式のままである。$L' := M'(x)(= K(x, a_1, \ldots, a_n))$ 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。 $\square$