12 Galois 拡大再論

12.1 Galois 拡大

命題 12.1. 代数拡大 L/K について次は同値

(1) L/K は Galois

(2) L/K は正規かつ分離的

(2)′ $^\forall x \in L$ に対し、その最小多項式は分離的かつ $L[X]$ において一次因子の積に分解される。

(3) L/K はある分離多項式族 $(f_i)_{i\in I}$ の最小分解体

さらに、 L/K が有限次なら次も同値

(4) $[L:K] = h_L(L)(:= |\mathrm{Aut}_K(L)|)$

Proof. Ω を K の代数閉包とする。

(2) $\Leftrightarrow$ (2)′ は正規の定義 (**??**) と系 (**??**) と多項式の分離性の定義 (**??**) から明らか。

(1) $\Rightarrow$ (2)

$^\forall x \in L$ とその最小多項式 $f \in K[X]$ をとる。また、 $Y_x := \{\sigma(x) | \sigma \in \mathrm{Aut}_K(L)\}$ と定めるとこれは x の Ω における共役元の集合の部分集合になり、$\sigma \in \mathrm{Aut}_K(L)$ から $Y \subset L$ である。命題 (**??**) の (1) $\Leftrightarrow$ (3) から x の共役元はすべて f の根なので高々 $\deg(f)$ 個しかないので Y_x は有限集合。$g := \prod_{y\in Y_x}(X-y), n := \deg(g)$ とする。y はすべて異なるから単根なので g は分離的である。また、 y は x の共役元より f の根でもあるから g のすべての根は f の根より $g|f$ となる。

$y \in Y_x \subset L$ よりその元から作られる基本対称式は L に含まれるので $g = \sum_{i=1}^n a_i X^i, a_i \in L$ と書ける。$\sigma g = \sum_{i=1}^n \sigma(a_i)X^i$ とすると係数だけに σ をかけているから $(\sigma g)(X) = \prod_{y\in Y_x}(X - \sigma(y))$ となる。ここで $y \in Y_x$ より $y = \tau(x), \tau \in \mathrm{Aut}_K(L)$ となるものが存在する。$\mathrm{Aut}_K(L)$ は自己同型写像であるから $\sigma\circ\tau \in \mathrm{Aut}_K(L)$ より $\sigma(y) = \sigma\circ\tau(x)) \in Y_x$ となる。ここで Y_x は有限集合であることと σ は体の準同型より単射なのでそれぞれの y は σ によりそれぞれ異なる Y_x の元に行く。したがって $(\sigma g)(X) = \prod_{y\in Y_x}(X-y) = g(X)$ となるから a_i は $^\forall\sigma \in \mathrm{Aut}_K(L)$ によって動かされない。L/K が Galois より $L^{\mathrm{Aut}_K(L)} = K$ より $a_i \in K$ であるから $g \in K[X]$ である。

$g, f \in K[X]$ で $g|f$ より f の最小性から $f = g$ なので任意の $x \in L$ の最小多項式は $f = \prod_{y\in Y_x}(X-y)$ と $L[X]$ 上で一次因子の積に分解されるので L/K は正規。また、 $g(=f)$ は分離的でもあったので任意の最小多項式が分離的より系 (**??**) より L/K は分離的であるので L/K は正規かつ分離的。

(2) $\Rightarrow$ (1)

$L = K$ のとき $L^{\mathrm{Aut}_K(L)} = K^{\mathrm{Aut}_K(K)} = K$ で成立。$L \neq K$ のとき $L \supsetneq K$ であるから $^\forall x \in L - K$ をとる。これがある $\sigma \in \mathrm{Aut}_K(L)$ で $\sigma(x) \neq x$ となればよい。

x の最小多項式を $f \in K[X]$ とすると $x \in L - K$ より $\deg(f) > 1$ であり、仮定から L/K が分離的より系 (**??**) から f が単根を持つので定義より分離的だから $f(y) = 0$ で $y \neq x$ であるような元 $y \in \Omega$ が存在する。y の K 上の最小多項式も f なので命題 (**??**) の (2) $\Leftrightarrow$ (3) から $\sigma(x) = y$ となるような $\sigma \in \mathrm{Aut}_K(\Omega)$ が存在する。仮定から L/K は正規なので命題 (**??**) の (1) $\Leftrightarrow$ (3) から $\sigma(L) = L$ より $\sigma|_L \in \mathrm{Aut}_K(L)$ となる。この σ により $\sigma(x) = y \neq x$ なので x は固定されないから固定されるのは K の元のみなので $L^{\mathrm{Aut}_K(L)} = K$ となり定義より L/K は Galois である。

(2) $\Leftrightarrow$ (3)

命題 (**??**) の (1) ⇔ (5) より「規 ⇔ ある多項式族 $(f_i)_{i\in I}$ の最小分解体」が言えている。その多項式族は $^\forall x \in L$ の最小多項式の族であったので系 (**??**) より「分離的 ⇔ 多項式族のすべての多項式が分離的」が言えている。

(2) ⇔ (4)

有限次拡大のとき系 (**??**) から「正規 ⇔ $[L:K]_s = h_L(L)$」が言えている。定義より「分離的 ⇔ $[L:K] = [L:K]_s$」なので「正規かつ分離的 ⇔ $[L:K] = [L:K]_s = h_L(L)$」となり示された。 □

12.2 多項式の Galois 群

定義 12.2. K : 体、 $f \in K[X] - K$: 分離多項式、 L_f : f の K 上の最小分解体とするときその根をすべて添加しているので命題 (**??**) から L_f/K は有限次だから命題 (12.1) の (1) ⇔ (3) から L_f/K は有限次 Galois 拡大である。このとき $\mathrm{Gal}(L_f/K)$ をf の K 上の Galois 群という。