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) $\Leftrightarrow$ (5) より「規 $\Leftrightarrow$ 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 $\Leftrightarrow$ 多項式族のすべての多項式が分離的」が言えている。

(2) $\Leftrightarrow$ (4)

有限次拡大のとき系 (??) から「正規 $\Leftrightarrow [L:K]_s = h_L(L)$」が言えている。定義より「分離的 $\Leftrightarrow [L:K] = [L:K]_s$」なので「正規かつ分離的 $\Leftrightarrow [L:K] = [L:K]_s = h_L(L)$」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) $\Leftrightarrow$ (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。

命題 12.3. 分離多項式 $f \in K[X] - K$ にたいしてその最小分解体 L_f を考える。Ω を K の代数閉包で L_f を含むもの、$W := \{x \in \Omega | f \text{ の根 }\}$ とする。f は分離多項式なので $|W| = n := \deg(f)$ となる。このとき $\mathrm{Gal}(L_f/K)$ は W に作用し、根の置換を引き起こす。したがって W の自己同型写像の群、つまり W の置換群を $\mathfrak{S}_W$ とするとき $|W| = n$ から n 次対称群 $\mathfrak{S}_n$ でもあり、

$$\begin{aligned} \mathrm{Gal}(L_f/K) &\longrightarrow \mathfrak{S}_W (= \mathfrak{S}_n) \\ \sigma &\longmapsto \sigma|_W \end{aligned}$$

という単射群準同型が存在する。 ($\mathfrak{S}_W$に $\mathrm{Gal}(L_f/K)$ は埋め込める)

とくに $|\mathrm{Gal}(L_f/K)| = [L_f : K] \le n!$ である。

Proof. $^\forall \sigma \in \mathrm{Gal}(L_f/K) = \mathrm{Aut}_K(L_f)$ は $f(\sigma(x)) = \sigma(f(x)) = 0$ より $\sigma(x) \in W$ だから $\sigma(W) \subset W$ なので

$$\begin{aligned} \sigma|_W : W &\longrightarrow W \\ x &\longmapsto \sigma(x) \end{aligned}$$

となり σ は体の準同型より単射であって $|W| = n$ で有限集合なのでこれは全単射である。したがって $\sigma|_W$ は W 上の全単射写像の群である $\mathfrak{S}_W$ の元となる。$\sigma = \tau \in \mathrm{Gal}(L_f/K)$ のとき、 $\sigma|_W = \tau|_W$ であるので $\mathrm{Gal}(L_f/K) \longrightarrow \mathfrak{S}_W, \sigma \longmapsto \sigma|_W$ は写像になっている。また、 $\sigma|_W = \tau|_W$ のとき、$\mathrm{Aut}_K(L_f)$ の元としての σ, τ は K を動かさないので最小分解体の定義から $L_f = K(W)$ なので W の動かし方で定まるから $\sigma = \tau$ である。したがって制限写像 $\mathrm{Gal}(L_f/K) \longrightarrow \mathfrak{S}_W$ は単射である。

L_f/K は定義 (12.2) から有限次 Galois なので命題 (12.1) の (1) $\Leftrightarrow$ (4) から $[L_f : K] = h_{L_f}(L_f) = |\mathrm{Aut}_K(L_f)| = |\mathrm{Gal}(L_f/K)|$ である。ここで上述のことから $\mathrm{Gal}(L_f/K)$ は $\mathfrak{S}_W = \mathfrak{S}_n$ に埋め込めるから $|\mathrm{Gal}(L_f/K)| = [L_f : K] \le |\mathfrak{S}_n| = n!$ より示された。 □

系 12.4. 一般の n 次多項式 $f \in K[X]$ の最小分解体 L の拡大次数は $n!$ 以下である。

Proof. 命題 (12.3) で f は分離多項式とは限らないので $|W| \le n$ であるから $|\mathfrak{S}_W| \le |\mathfrak{S}_n|$ である。埋め込むことは同様にできるから $\mathrm{Gal}(L_f/K)$ を $\mathrm{Aut}_K(L)$ として $|\mathrm{Aut}_K(L)| \le |\mathfrak{S}_W| \le |\mathfrak{S}_n| = n!$ より成立。 □

命題 12.5. 分離多項式 $f \in K[X] - K$ の根の集合 W とその元 $x, y \in W$ に対して以下は同値。

(1) x と y は K 上共役。

(2) x と y は同じ $\mathrm{Gal}(L_f/K)-$ 軌道上に属する。

(3) x と y は f の同じ既約成分の根。

とくに f が既約であるためには $W \neq \emptyset$ かつ $\mathrm{Gal}(L_f/K)$ が W に推移的に作用することが必要十分である。(群 G が集合 X に推移的に作用するとは $G-$ 軌道 $G(x) := \{\sigma(x) | \sigma \in G\}$ とするとき $G(x) = X$ となること)

Proof. Ω を K の代数閉包とする。

(1) $\Leftrightarrow$ (2)

f が分離的なので L_f/K は有限次 Galois 拡大であるから正規なので $\sigma \in \mathrm{Aut}_K(\Omega), \sigma(L_f) = L_f$ を満たすから $\sigma|_{L_f} \in \mathrm{Aut}_K(L_f) = \mathrm{Gal}(L_f/K)$ となる。また、 $\sigma \in \mathrm{Gal}(L_f/K)$ は系 (**??**) より $\tilde{\sigma} \in \mathrm{Aut}_K(\Omega)$ に拡張できる。これより

$$\begin{aligned} x \text{ と } y \text{ が } K \text{ 上共役} &\Leftrightarrow {}^{\exists}\sigma \in \mathrm{Aut}_K(\Omega), x = \sigma(y) \\ &\Leftrightarrow y \in \{\sigma(x) | \sigma \in \mathrm{Gal}(L_f/K)\} \\ &\Leftrightarrow y \text{ は } x \text{ の } \mathrm{Gal}(L_f/K) - \text{軌道に含まれる} \end{aligned}$$

となる。

(1) $\Leftrightarrow$ (3)

命題 (**??**) の (1) $\Leftrightarrow$ (3) より x と y が K 上共役 $\Leftrightarrow$ x と y の K 上の最小多項式は同じなのでその最小多項式を $g \in K[X] - K$ とすれば g は f の既約成分であるので示された。

もし $\mathrm{Gal}(L_f/K)$ が $W(\neq \emptyset)$ に推移的に作用するとすると、ある f の根 x に対してその $\mathrm{Gal}(L_f/K)-$ 軌道は W に一致するので任意の f の根は (2) $\Leftrightarrow$ (3) から f の同じ既約成分の根になる。したがって f の根はすべて f の既約成分の根になるから f は既約。f が既約であるとき (2) $\Leftrightarrow$ (3) からすべての根はある f の根 x と同じ $\mathrm{Gal}(L_f/K)-$ 軌道上に属するから $W \subset \mathrm{Gal}(L_f/K)-$ 軌道である。また、 x の軌道はすべて f の根になるから $W \supset \mathrm{Gal}(L_f/K)-$ 軌道より $W = \mathrm{Gal}(L_f/K)-$ 軌道となり推移的である。 □

例 12.6. K : 体、 $L := K(T_1, \ldots, T_n)$: n 変数の有理関数体とする。$G := \mathfrak{S}_n$ として T_i の添字の置換とする。つまり、 $\sigma \in G$ と $f = f(T_1, \ldots, T_n) \in L$ に対して、$\sigma f := f(T_{\sigma(1)}, \ldots, T_{\sigma(n)})$ と作用させることとする。このとき、 G の元は T_i を写し、 K の元は動かさないので L の体の自己同型とみなせるので $G \subset \mathrm{Aut}_{体}(L)$ となる。

$M := L^G$ とおくとこれは $T_1, \ldots, T_n$ の対称有理式の集合になる。このとき L/M が Galois となって、$G = \mathrm{Gal}(L/M)$ を満たす。とくに $[L : M] = n!$ となる。

Proof. $s_i := (T_1, \ldots, T_n$の i 次基本対称式$)$ とすると $s_i \in L$ である。つまり、 $s_1 = T_1 + \cdots + T_n, s_2 = T_1T_2 + T_1T_3 + \cdots + T_{n-1}T_n, \cdots, s_n = T_1 \cdots T_n$ となっている。$M_0 := K(s_1, \ldots, s_n)$ とおくと基本対称式は文字を置換しても同じままなので M_0 は G で固定される。よって $M_0 \subset M$ である。

ここで $T_1, \ldots, T_n$ は解と係数の関係から $X^n - s_1X^{n-1} + \cdots + (-1)^n s_n \in M_0[X]$ の根になる。$T_1, \ldots, T_n$ はそれぞれ異なるから命題 (**??**) からこの多項式は分離的である。L はこの多項式の最小分解体なので定義 (12.2) から L/M_0 は有限次 Galois 拡大になる。命題 (12.3) から $[L : M_0] \leq n!$ である。また、 L/M は Artin の定理 (**??**) から Galois 拡大で $G = \mathfrak{S}_n = \mathrm{Aut}_M(L)$ であり、Rem (**??**) から $[L : M] = |\mathrm{Aut}_M(L)| = |\mathfrak{S}_n| = n!$ となる。よって $M_0 \subset M$ と $[L : M_0] \leq n! = [L : M]$ より $M_0 = M$ となる。以上より M は $T_1, \ldots, T_n$ の対称有理式の集合になり、$G = \mathfrak{S}_n = \mathrm{Gal}(L/M)$ で、 $[L : M] = n!$ となる。 □