11　正規拡大（準 Galois 拡大）

11.1　共役

定義 11.1. $\Omega := \overline{K}$: K の代数閉包とする。$L/K, M/K(L, M \subset \Omega)$ が K 上共役 (conjugate)とはある $\sigma \in \mathrm{Aut}_K(\Omega)$ があって $\sigma(L) = M$ となること。

$x, y \in \Omega$ が K 上共役 (conjugate)とはある $\sigma \in \mathrm{Aut}_K(\Omega)$ があって $\sigma(x) = y$ となること。

例 11.2. $z, \overline{z} \in \mathbb{C}$ は $\mathbb{R}$ の代数閉包であり、$G = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) := \{\mathrm{Id}_{\mathbb{R}}, \sigma\}, \sigma(z) = \overline{z}$ とする。このとき G の固定体 $\mathbb{R}^G = \mathbb{R}$ となるので $\mathbb{C}/\mathbb{R}$ は Galois である。この σ は複素共役をとる写像であるが $\sigma(z) = \overline{z}$ より一般の共役の定義にも適している。

命題 11.3. K の代数閉包 Ω とし、$x, y \in \Omega$ をとる。このとき次は同値。

(1) x と y は K 上共役。

(2) $K-$ 同型写像 $v : K(x) \longrightarrow K(y)$ で $v(x) = y$ となるものが存在する。

(3) x と y の K 上の最小多項式は同じ。

Proof. (1) $\Rightarrow$ (3)

x の最小多項式を $f \in K[X]$ とする。x と y は共役なのである $\sigma \in \mathrm{Aut}_K(\Omega)$ が存在して $\sigma(x) = y$ となる。σ は $K-$ 自己準同型より K の元を動かさないので f の係数を動かさない。よって $f(y) = f(\sigma(x)) = \sigma(f(x)) = \sigma(0) = 0$ より f は y を根にもつ。y の最小多項式を $g \in K[X]$ とする。$f \neq g$ と仮定すると $\deg(g)$ の最小性から $g|f$ より $f = gh$ となる $h \in K[X], \deg(h) > 0$ が存在する。このとき $f(x) = g(x)h(x) = 0$ となり f より次数の低い g または h が x を根にもつ。これは $\deg(f)$ の最小性に矛盾するから $f = g$ より x と y の最小多項式は一致する。

(3) $\Rightarrow$ (2)

x と y の最小多項式を $f \in K[X]$ とする。このとき命題 (**??**) より $K(x) \cong K[X]/(f) \cong K(y)$ であり、

$$\begin{aligned} K(x) &\longrightarrow K[X]/(f) \longrightarrow K(y) \\ x &\longmapsto X + (f) \longmapsto y \end{aligned}$$

となる同型写像が作れる。したがって $v : K(x) \longrightarrow K(y), x \longmapsto v(y)$ となる $K-$ 同型写像が存在する。

(2) $\Rightarrow$ (1)

Ω は $K(x), K(y)$ の代数閉包でもあるので系 (**??**) から $K-$ 同型 $v : K(x) \longrightarrow K(y)$ を $\tilde{v} : \Omega \longrightarrow \Omega$ に延長できる。これは $K-$ 自己準同型なので $\tilde{v} \in \mathrm{Aut}_K(\Omega)$ で $\tilde{v}(x) = v(x) = y$ より定義から x と y は K 上共役。 □

系 11.4. $x \in K$ の最小多項式 $f \in K[X]$ で $\sigma \in \mathrm{Aut}_K(\Omega)$ とする。このとき

$$g(X) := \prod_{\sigma \in \mathrm{Aut}_K(\Omega)} (X - \sigma(x))$$

は Ω において f を割る。

Proof. 命題 (11.3) の (1) $\Leftrightarrow$ (3) より f は x の共役元を根としてすべて含むので Ω において f が一次因子の積に分解できることより g は f を割る。 □

11.2 正規

定義 11.5. 代数拡大 L/K が正規 (normal)もしくは準 Galois (quasi − galois)であるとは任意の既約多項式 $f \in K[X]$ が根を L 内に一つもてば d は $L[X]$ において一次因子の積に分解することができる。(すべて同じ体の中に根をもつ)

$\Leftrightarrow {}^{\forall}x \in L$ に対してその最小多項式 $f \in K[X]$ は $L[X]$ において一次因子の積に分解できる。

とくに代数閉包 Ω/K は代数閉体の同値条件の命題 (**??**) の (AC1) から正規拡大である。

命題 11.6. 代数拡大 L/K と代数閉包 Ω/K について次は同値。

(1) L/K は正規。

(2) ${}^{\forall}x \in L$ に対してその任意の共役は L に含まれる。

(3) ${}^{\forall}\sigma \in \mathrm{Aut}_K(\Omega), \sigma(L) = L$ となる。

(4) ${}^{\forall}\phi \in \mathrm{Hom}_K(L, \Omega), \phi(L) = L$ となる。

(5) L はある K 上の多項式族 $(f_i)_{i \in I}$ の最小分解体。

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

$x \in L$ の最小多項式 $f \in K[X]$ をとる。L/K が正規で x が L での f の根なので f は $L[X]$ 上で一次因子の積に分解できる。よって f の根はすべて L に含まれている。ここで命題 (11.3) の (1) $\Leftrightarrow$ (3) より x の任意の共役元も最小多項式は f なので f の根であるからそれは L に含まれる。

(2) $\Rightarrow$ (1)

${}^{\forall}x \in L$ について L/K が代数拡大より最小多項式 $f \in K[X]$ がある。f の他の根 $a_i \in \Omega/K, 1 \leq i \leq n := \deg(f)$ も f を最小多項式として持っているから命題 (11.3) の (1) $\Leftrightarrow$ (3) より a_i は x の共役元である。したがって $a_i \in L$ であるから f は $L[X]$ で $f = \prod_{i=1}^{n}(X - a_i)$ と一次因子の積に分解できるので L/K は正規拡大。

(1) $\Rightarrow$ (5)

${}^{\forall}x \in L$ の K 上の最小多項式の族 $(f_i)_{i \in I}$ をとり、この最小分解体を M とする。このとき $M[X]$ では f_i はすべて一次因子の積に分解できるから $M \subset L$ であり、 $x \in M$ でもあるので $M = L$ より L は $(f_i)_{i \in I}$ の最小分解体である。

(5) $\Rightarrow$ (3)

L が $(f_i)_{i \in I}$ の最小分解体であるとする。f_i の根を $\alpha_{ij} \in \Omega/K, 1 \leq j \leq n := \deg(f_i)$ とする。この根の集合を R_i とおくとき最小分解体の定義から $L = K(\cup_{i \in I} R_i)$ とかける。${}^{\forall}\sigma \in \mathrm{Aut}_K(\Omega)$ をとったときこれは K を動かさない。また、 α_{ij} の最小多項式はすべて f_i なのでそれぞれ共役であり体の準同型から単射なので $\sigma(R_i) = R_i$ となる。したがって $\sigma(L) = \sigma(K(\cup_{i \in I} R_i)) = K(\cup_{i \in I} R_i) = L$ より成立。

(3) $\Rightarrow$ (2)

${}^{\forall}x \in L$ に対してその共役は任意の $\sigma \in \mathrm{Aut}_K(\Omega)$ による $\sigma(x)$ であるが仮定より $\sigma(L) = L$ より $\sigma(x) \in L$ となる。したがって任意の元のすべての共役は L に含まれるので成立。

(4) $\Rightarrow$ (3)

${}^{\forall}\sigma \in \mathrm{Aut}_K(\Omega)$ をとる。このとき $\sigma|_L \in \mathrm{Hom}_K(L, \Omega)$ なので仮定より $\sigma|_L(L) = L$ で $\sigma|_L(L) = \sigma(L)$ より成立。

(3) $\Rightarrow$ (4)

$\phi \in \mathrm{Hom}_K(L,\Omega)$ にたいして $L, \phi(L)$ は K の代数拡大なので定理 (**??**) から代数閉包 Ω に埋め込めるので Ω はこれらの代数閉包でもある。ϕ は体の準同型より単射なので $\phi : L \longrightarrow \phi(L)$ は全単射となっているから $L \cong \phi(L)$ になっていて系 (**??**) よりこれを延長する $\sigma : \Omega \longrightarrow \Omega$ が存在する。したがって仮定より $\sigma(L) = L$ であり、 $\sigma|_L = \phi$ なので $\phi(L) = \sigma|_L(L) = \sigma(L) = L$ より成立。 □

系 11.7. L/K : 有限次拡大のとき

$$L/K : \text{正規} \Leftrightarrow [L:K]_s = h_L(L)(:= |\mathrm{Hom}_K(L,L)|)$$

が成り立つ。

Proof. 系 (**??**) より $[L:K]_s \leq [L:K]$ より L/K が有限次拡大なので $[L:K]_s$ も有限。$L \subset \Omega$ から一般に $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\Omega)$ である。体の準同型は単射なので $\mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$ とも書ける

($\Rightarrow$)

命題 (11.6) の (1) $\Leftrightarrow$ (4) から ${}^\forall\sigma \in \mathrm{Hom}_K(L,\Omega)$ をとると $\sigma(L) = L$ となっているので $\sigma \in \mathrm{Aut}_K(L)$ である。よって $\mathrm{Hom}_K(L,\Omega) \subset \mathrm{Aut}_K(L)$ であるので、一般に $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\Omega)$ が成り立つことを考えれば $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,\Omega)$ だから $h_L(L) = [L:K]_s$ である。

($\Leftarrow$)

$h_L(L) = [L:K]_s$ が有限で成り立っていて $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\Omega)$ より $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,\Omega)$ である。${}^\forall\sigma \in \mathrm{Hom}_K(L,\Omega)$ をとると $\sigma \in \mathrm{Aut}_K(L)$ なので $\sigma(L) = L$ を満たすから命題 (11.6) の (1) $\Leftrightarrow$ (4) から L/K は正規。 □