Galois対応の証明

$K, L, M, \dots$ は $\mathbb{C}$ の部分体であるとする。

補題1 L/K が有限次Galois拡大ならば $|\mathrm{Gal}(L/K)| = [L:K]$。

証明 単拡大定理より、ある $\theta \in L$ が存在して $L = K(\theta)$。

θ の K 上での最小多項式を $F_\theta(x) \in K[x]$ と書き、$r = [L:K]$ とおく。

このとき、$L = K(\theta) \cong K[x]/(F_\theta(x))$ より、$r = [L:K] = \dim_K L = \deg F_\theta(x)$。

$F_\theta(x)$ は重根を持たないので互いに異なる r 個の根 $\theta_1 = \theta, \theta_2, \dots, \theta_r$ を持つ。
($\theta_1, \dots, \theta_r$ は θ の K 上での共役元と呼ばれる。)

$\sigma \in \mathrm{Gal}(L/K)$ に対して、$0 = \sigma(F_\theta(\theta)) = F_\theta(\sigma(\theta))$ なので $\sigma(\theta) \in \{\theta_1, \dots, \theta_r\}$。

ゆえに写像 $\kappa : \mathrm{Gal}(L/K) \to \{\theta_1, \dots, \theta_r\}$, $\sigma \mapsto \sigma(\theta)$ が定まる。

任意の $i = 1, \dots, r$ について、K 上の体の自己同型 $\sigma_i : L \to L$, $f(\theta) \mapsto f(\theta_i)$ $(f(x) \in K[x])$ が定まり、$\kappa(\sigma) = \sigma(\theta) = \theta_i$ なので、κ は全射であることがわかる。

$\sigma \in \mathrm{Gal}(L/K)$ が $\kappa(\sigma) = \sigma(\theta) = \theta_i$ をみたすとき、任意の $f(x) \in K[x]$ について、
$\sigma(f(\theta)) = f(\sigma(\theta)) = f(\theta_i)$ なので $\sigma = \sigma_i$。ゆえに κ は単射である。

したがって、$|\mathrm{Gal}(L/K)| = |\{\theta_1, \dots, \theta_r\}| = r = [L:K]$。 □

次の補題2の証明は易しい.

補題2 L/K が有限次Galois拡大であるとき,

その任意の中間体 M について, L/M も有限次Galois拡大になる.

証明 $\infty > [L:K] = [L:M][M:K]$ より, $[L:M] < \infty$ なので L/M も有限次拡大になる. ($[M:K] < \infty$ も成立するので M/K も有限次拡大になる.)

L/K がGalois拡大なので, 任意の K 上での体の同型 $\varphi : L \hookrightarrow \mathbb{C}$ について, $\varphi(L) = L$.

$\psi : L \hookrightarrow \mathbb{C}$ を M 上での体の同型とすると, (M の元を固定)
ψ は K 上での同型でも (K の元を固定)
あるので $\psi(L) = L$.

ゆえに, L/M もGalois拡大である. □

以下，L/K は有限次 Galois 拡大であると仮定し，$G=\mathrm{Gal}(L/K)$ とおく．

L/K の中間体 M に対して，G の部分群 G_M を次のように定める：

$$G_M=\mathrm{Gal}(L/M)=\{\sigma\in G\mid \sigma(\beta)=\beta\ (\forall\beta\in M)\}$$

G の部分群 H に対して，L/K の中間体 L^H を次のように定める：

$$L^H=\{\beta\in L\mid \sigma(\beta)=\beta\ (\forall\sigma\in H)\}.$$

G_M と L^H の定義からほぼ自明に以下の補題3，4が得られる．

補題3 (1) $M\subset L^{G_M}$　(2) $H\subset G_{L^H}$

証明 (1) $\beta\in M$ のとき，G_M の定義より $\sigma(\beta)=\beta\ (\forall\sigma\in G_M)$ なので $\beta\in L^{G_M}$．
ゆえに，$M\subset L^{G_M}$．

(2) $\sigma\in H$ のとき，L^H の定義より $\sigma(\beta)=\beta\ (\forall\beta\in L^H)$ なので $\sigma\in G_{L^H}$．
ゆえに $H\subset G_{L^H}$．

□

補題4 対応 $M \mapsto G_M$ と $H \mapsto L^H$ は包含関係を逆転させる．すなわち，

(1) L/K の中間体 $M' \supset M$ に対して，$G_{M'} \subset G_M$．

(2) G の部分群 $H' \subset H$ に対して，$L^{H'} \supset L^H$．

証明 (1) $\sigma \in G_{M'}$ (すなわち，$\sigma(\beta') = \beta' \ (\forall \beta' \in M')$) のとき，任意の $\beta \in M$ について，$M' \supset M$ より $\beta \in M'$ でもあるので $\sigma(\beta) = \beta$ となるなので，$\sigma \in G_M$．
ゆえに，$G_{M'} \subset G_M$．

(2) $\beta \in L^H$ (すなわち，$\sigma(\beta) = \beta \ (\forall \sigma \in H)$) のとき，任意の $\sigma' \in H'$ について，$H' \subset H$ より $\sigma' \in H$ でもあるので $\sigma'(\beta) = \beta$ となるので，$\beta \in L^{H'}$．
ゆえに，$L^{H'} \supset L^H$．

□

補題5 L/Kの中間体 $M' \supset M$ について $G_{M'} = G_M$ ならば $M' = M$.

証明 L/Kの中間体 $M' \supsetneq M$ について $G_{M'} \subsetneq G_M$ となることを示せばよい.

補題2より, L/Mも有限次Galois拡大になる.

単拡大定理より, ある$\theta \in M'$が存在して, $M' = M(\theta)$となる.

θのM上での最小多項式を$F(x) \in M[x]$と書く. $F(x)$は重根を持たない.

$M' \supsetneq M$より, $2 \leqq [M' : M] = \deg F(x)$なので,

$F(x)$はθと異なる根θ'を持つ(θと異なるM上でのθの共役元θ'が存在).

L/MはGalois拡大なので$\theta' \in L$.

M上での体の同型 $\varphi : M' = M(\theta) \hookrightarrow L$, $f(\theta) \mapsto f(\theta')$ $(f(x) \in M[x])$ が得られる.

$M' \hookrightarrow L$, $\beta' \mapsto \beta'$ とは異なる

$\varphi : M' \hookrightarrow L$, $f(\theta) \mapsto f(\theta')$ を作れた.

つづく

単拡大定理より，ある $\eta \in L$ が存在して，$L = M'(\eta) = M(\theta, \eta)$.

η の $M' = M(\theta)$ 上での最小多項式を $G(x) = \sum_i a_i x^i$ $(a_i \in M' = M(\theta))$ と書き，

$H(x) = \sum_i \varphi(a_i) x^i \in M(\theta')[x]$ とおき，$H(x)$ の根の1つを $\tilde{\eta}$ と書く：

$$\begin{cases} L = M'(\eta) \cong M'[x]/(G(x)), & f(\eta) \leftrightarrow \overline{f(x)} \quad (f(x) \in M'[x]), \\ M(\theta')(\tilde{\eta}) \cong M(\theta')[x]/(H(x)), & g(\tilde{\eta}) \leftrightarrow \overline{g(x)} \quad (g(x) \in \varphi(M')[x]) \\ M'[x] \cong M(\theta)[x], & \sum_i a_i x^i \leftrightarrow \sum_i \varphi(a_i) x^i \quad (a_i \in M'), \quad G(x) \leftrightarrow H(x) \end{cases}$$

（$M(\theta)$ は M' と書き換え）

M 上の体の同型 $\psi : L = M'(\eta) \hookrightarrow \mathbb{C}$, $\sum_i a_i \eta^i \mapsto \sum_i \varphi(a_i) \tilde{\eta}^i$ $(a_i \in M')$ が得られる：

$$L = M'(\eta) \cong M'[x]/(G(x)) \cong M(\theta')[x]/(H(x)) \cong M(\theta')(\tilde{\eta}) \subset \mathbb{C}.$$
$$\sum_i a_i \eta^i \leftrightarrow \overline{\sum_i a_i x^i} \longleftrightarrow \overline{\sum_i \varphi(a_i) x^i} \longleftrightarrow \sum_i \varphi(a_i) \tilde{\eta}^i$$

問題6-1 解答例 ① と同様の構成

L/M は Galois 拡大なので $\psi(L) = L$ となり，

$\sigma \in \mathrm{Gal}(L/M) = G_M$ を $\sigma(\gamma) = \psi(\gamma)$ $(\gamma \in L)$ と作れる.

$\theta \in M' = M(\theta)$ について，$\sigma(\theta) = \varphi(\theta) = \theta' \neq \theta$ なので $\sigma \notin G_{M'}$.

補題4(1)より $G_{M'} \subset G_M$ となり，$\sigma \in G_M \setminus G_{M'}$ なので $G_{M'} \subsetneq G_M$. □

定理 (Galois対応) $M \mapsto G_M$ と $H \mapsto L^H$ は互いに相手の逆写像である.

証明

1 $G_{LH} = H$ を示そう. 補題3(2)より $G_{LH} \supset H$ なので $G_{LH} \subset H$ を示せばよい.

そのためには, $|G_{LH}| \leqq |H|$ を示せば十分である.

単拡大定理より, ある $\theta \in L$ が存在して, $L = L^H(\theta)$ となる.

$f(x) = \prod_{\tau \in H} (x - \tau(\theta)) = \sum_i c_i x^i$ $(c_i \in L)$ とおく.

このとき, $\sigma \in H$ について, $\sum_i \sigma(c_i) x^i = \prod_{\tau \in H} (x - \sigma\tau(\theta)) \overset{\rho \in \sigma\tau}{=} \prod_{\rho \in H} (x - \rho(\theta)) = f(x)$

なので $\sigma(c_i) = c_i$ となるので, $c_i \in L^H$, $f(x) \in L^H[x]$ である.

$f(\theta) = 0$ なので,

$|H| = \deg f(x) \geqq \deg(\theta$ の L^H 上での最小多項式$) = [L^H(\theta) : L^H] = [L : L^H]$

補題1より, $[L : L^H] = |\mathrm{Gal}(L/L^H)| = |G_{LH}|$.

ゆえに, $|H| \geqq |G_{LH}|$. したがって, $G_{LH} \subset H$ $(\therefore G_{LH} = H)$.

[2] $L^{G_M} = M$ を示そう.

補題3(1)より, $L^{G_M} \supset M$.

[1]の結果を $H = G_M$ に適用すると $G_{L^{G_M}} = G_M$.

補題5を $M' = L^{G_M}$ に適用すると, $L^{G_M} = M$ が得られる. □

以上によって, $\mathbb{C}$ の部分体の場合のGalois対応が証明された.

注意 (1) 標数0の一般的な場合は $\mathbb{C}$ をKを含む代数閉包におきかえれば同様の方法でGalois対応が証明される.

(2) 標数 $p > 0$ の場合にも, 最小多項式が重根を持たずにすむための適切な定式化(分離性の仮定)をすれば本質的に同じ方法でGalois対応を証明可能である □

追記 2021-11-17

Galois対応の [2] は以下のようにすれば容易に示せました。(めんどうな補題5の証明は必要ない。)

易しい [2] の別証 $L^{G_M} = M$ を示そう。

ほぼ自明の補題3 (1) より, $L^{G_M} \supset M$.

ゆえに, $L^{G_M} = M$ を示すためには $[L^{G_M} : K] = [M : K]$ を示せば十分である。

(K 上の有限次元ベクトル空間 V とその部分空間 W について, $V = W \Leftrightarrow \dim_K V = \dim_K W$.
これを $V = L^{G_M}$, $W = M$ に適用した。)

補題2より, L/L^{G_M} も L/M も Galois 拡大であり,
補題1より, $[L : L^{G_M}] = |G_{L^{G_M}}|$, $[L : M] = |G_M|$.

(注意 $G_M = \mathrm{Gal}(L/M)$)

[1] の結果を $H = G_M$ に適用すると $G_{L^{G_M}} = G_M$ なので $[L : L^{G_M}] = [L : M]$.

これと, $[L : L^{G_M}][L^{G_M} : K] = [L : K] = [L : M][M : K]$ より, $[L^{G_M} : K] = [M : K]$.

したがって, $L^{G_M} = M$. □

ムダにめんどうな証明を紹介して申しわけありませんでした。