Galois 対応の証明

K, L, M, … は $\mathbb{C}$ の部分体であるとする。 ← 標数0でも同様

資料07-3

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

証明 単拡大定理より、ある $\theta \in L$ が存在して $L = K(\theta)$。 ← 単拡大定理は空気のごとく使われる。

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、$r = [L:K] = \dim_K L = \deg F_\theta(x)$。

$Gal(L/K) \to \{\theta_1, \dots, \theta_r\}$, $\sigma \mapsto \sigma(\theta)$ が全単射を示す。

$F_\theta(x)$ 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。) L/K は Galois 拡大なので $L = K(\theta_i)$。

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

$L = K(\theta) \cong K[x]/(F_\theta(x)) \cong K(\theta_i) = L$

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、$\kappa(\sigma_i) = \sigma_i(\theta) = \theta_i$ なので、κ は全射であることがわかる。

$\sigma \in Gal(L/K)$ 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、$|Gal(L/K)| = |\{\theta_1, \dots, \theta_r\}| = r = [L:K]$。 □

次の補題2の証明は自明に近い.

補題2 L/K が有限次Galois拡大であるとき,

注意 M/K はGalois拡大になるとは限らない.

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, $\varphi(L) = L$.

M の元を固定　　K の元を固定

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

ゆえに, L/M もGalois拡大である. □

例 $L = \mathbb{Q}(\sqrt[3]{3}, \omega)$, $\omega = \frac{-1+\sqrt{-3}}{2}$, $K = \mathbb{Q}$ とすると, L/K は3次のGalois拡大になる.
($\because$ L = (x^3-3 の K 上で最小分解体) = ($\mathbb{Q}$ に x^3-3 の根をすべて付け加えてできる体))
$M = \mathbb{Q}(\sqrt[3]{3})$ のとき, L/M はGalois拡大だが, $M/K = \mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ はGalois拡大ではない.

以下，L/K は有限次 Galois 拡大であると仮定し，$G = Gal(L/K)$ 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：

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

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) $H \subset G_{L^H}$

← 後で (1), (2) で $=$ が成立することを示すが，$\subset$ は自明になる．

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，$L^{H'} \supset L^H$．

□

定理 (Galois対応) K, L が $\mathbb{C}$ の部分体で L/K が有限次Galois拡大のとき,

(本当は $\mathbb{C}$ の部分体という仮定は不要)

$$\{L/K\text{の中間体}\} \longleftrightarrow \{\mathrm{Gal}(L/K)\text{の部分群}\}$$
$$M \longmapsto G_M$$
$$L^H \longleftarrow H$$

は互いに相手の逆写像である.

証明 1 $G_{L^H} = H$ を示そう.

補題3(2)より $G_{L^H} \supset H$ なので $|G_{L^H}| \leqq |H|$ 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.

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

次の例を思い出そう,

$$\left.\begin{aligned} &(x-(\sqrt{2}+\sqrt{3}))\\ &\times(x-(-\sqrt{2}+\sqrt{3}))\\ &\times(x-(\sqrt{2}-\sqrt{3}))\\ &\times(x-(-\sqrt{2}-\sqrt{3})) \end{aligned}\right\} \in \mathbb{Q}[x]$$

$\rho = \sigma\tau$ とおく.

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

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

補題2より, L/L^H も有限次Galois拡大であり, 補題1より, $[L : L^H] = |\mathrm{Gal}(L/L^H)| = |G_{L^H}|$.

ゆえに, $|H| \geqq |G_{L^H}|$. したがって, $G_{L^H} = H$.

(注) この 1 の部分だけが非自明!

2 $L^{G_M} = M$ を示そう. ほぼ自明な補題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, $L^{G_M} = M$. □

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 □

(1 を使えばやさしい)