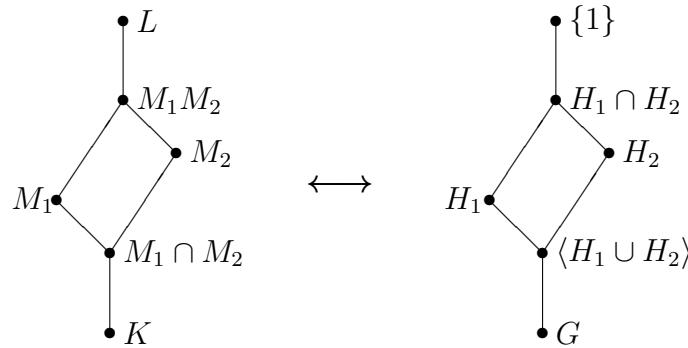


§11. ガロア対応

定理 11.1 L/K を有限次ガロア拡大とし, そのガロア群を G とする. いま, L/K の中間体 M_1, M_2 がそれぞれ G の部分群 H_1, H_2 に対応しているとする.

- (1) $M_1 \subset M_2$ と $H_1 \supset H_2$ は同値である.
- (2) 合成体 M_1M_2 に対応する部分群は $H_1 \cap H_2$ である.
- (3) $M_1 \cap M_2$ に対応する部分群は $H_1 \cup H_2$ で生成される G の部分群である.



証明 (1) まず $M_1 \subset M_2$ を仮定する. $\sigma \in H_2 = \text{Gal}(L/M_2)$ を任意にとると,

$$\sigma(x) = x \quad (\forall x \in M_2) \quad \text{より} \quad \sigma(x) = x \quad (\forall x \in M_1), \quad \therefore \sigma \in \text{Gal}(L/M_1) = H_1$$

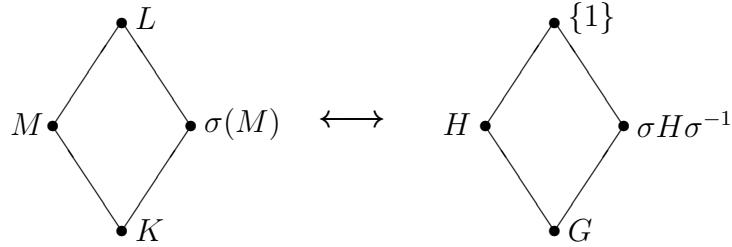
よって $H_2 \subset H_1$ を得る. 逆に $H_2 \subset H_1$ を仮定する. $x \in M_1 = L^{H_1}$ を任意にとると,

$$\sigma(x) = x \quad (\forall \sigma \in H_1) \quad \text{より} \quad \sigma(x) = x \quad (\forall \sigma \in H_2), \quad \therefore x \in L^{H_2} = M_2$$

よって $M_1 \subset M_2$ を得る.

- (2) M_1M_2 は M_1, M_2 を含む最小の体だから, (1) より, 対応する部分群は H_1, H_2 に含まれる最大の部分群 $H_1 \cap H_2$ である.
- (3) $M_1 \cap M_2$ は M_1, M_2 に含まれる最大の体だから, (1) より, 対応する部分群は H_1, H_2 を含む最小の群であり, それは $H_1 \cup H_2$ で生成される G の部分群である. \square

定理 11.2 L/K を有限次ガロア拡大とし, そのガロア群を G とする. M を L/K の中間体, H を M に対応する G の部分群とする. また, $\sigma \in G$ とする. このとき, $\sigma(M)$ は L/K の中間体であり, 対応する G の部分群は $\sigma H \sigma^{-1}$ である.



証明 L/K は正規なので $\sigma(L) = L$, よって $K \subset \sigma(M) \subset L$ となるから $\sigma(M)$ は L/K の中間体である. また, $M = L^H$ より, $\alpha \in L$ に対して

$$\alpha \in M \iff \tau(\alpha) = \alpha \quad (\forall \tau \in H).$$

したがって,

$$\begin{aligned} \beta \in \sigma(M) &\iff \sigma^{-1}(\beta) \in M \iff \tau(\sigma^{-1}(\beta)) = \sigma^{-1}(\beta) \quad (\forall \tau \in H) \\ &\iff (\sigma\tau\sigma^{-1})(\beta) = \beta \quad (\forall \tau \in H) \iff \rho(\beta) = \beta \quad (\forall \rho \in \sigma H \sigma^{-1}) \end{aligned}$$

よって, 中間体 $\sigma(M)$ は部分群 $\sigma H \sigma^{-1}$ に対応する. \square

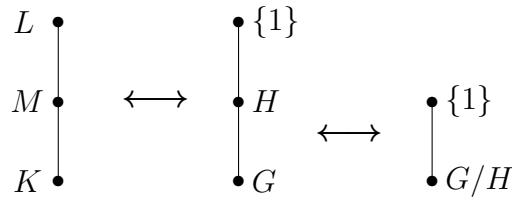
定理 11.3 L/K を有限次ガロア拡大とし, そのガロア群を G とする. M を L/K の中間体, H を M に対応する G の部分群とする. このとき, M/K がガロア拡大であるためには, H が G の正規部分群であることが必要十分である. またこのとき M/K のガロア群は G/H と同型である. 詳しくは, 制限写像

$$G = \text{Gal}(L/K) \longrightarrow \text{Gal}(M/K), \quad \sigma \mapsto \sigma|_M$$

から自然に同型

$$G/H = \text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Gal}(M/K)$$

が引き起こされる.



証明 L/K がガロア拡大なので, とくに M/K は分離的である. したがって, M/K がガロアであるためには, 正規であること, すなわち, 任意の $\sigma \in G$ に対して $\sigma(M) = M$ が成り立つことが必要十分である. 前定理を用いれば,

$$\sigma(M) = M \iff \sigma H \sigma^{-1} = H$$

であるが, 右の等式が任意の $\sigma \in G$ に対して成り立つことは, H が G の正規部分群であることを示している. 後半は, 準同型定理から導かれる. \square

系 11.4 L/K を有限次ガロア拡大, M をその中間体とする.

- (1) L/K がアーベル拡大ならば, $L/M, M/K$ はともにアーベル拡大である.
- (2) L/K が巡回拡大ならば, $L/M, M/K$ はともに巡回拡大である.
- (3) L/K が可解拡大ならば, L/M も可解拡大である. さらに M/K がガロア拡大 (すなわち $\text{Gal}(L/M)$ が $\text{Gal}(L/K)$ の正規部分群) ならば, M/K も可解拡大である.

証明 H を群 G の部分群とする. G がアーベル群ならば, H はアーベル群かつ G の正規部分群であって, 剰余群 G/H もアーベル群である. このことと前定理から (1) が得られる. また, アーベル群を巡回群としても同様のことがいえるから (2) も成り立つ. (3) は, G が可解群のとき H も可解群であり, さらに H が G の正規部分群ならば剰余群 G/H も可解群になることから導かれる. \square

定理 11.5 体の拡大 Ω/K の中間体 M_1, M_2 がともに K 上の有限次ガロア拡大体であるとする.

- (1) M_1M_2 および $M_1 \cap M_2$ はともに K 上ガロアである.
- (2) $\text{Gal}(M_1M_2/K)$ は直積 $\text{Gal}(M_1/K) \times \text{Gal}(M_2/K)$ の部分群に同型である.
- (3) $M_1 \cap M_2 = K$ ならば, 自然な同型

$$\text{Gal}(M_1M_2/K) \cong \text{Gal}(M_1/K) \times \text{Gal}(M_2/K)$$

が存在する.

証明 (1) は, 定理 8.13 から分離性が, 定理 9.14 から正規性が導かれることからわかる. (2) と (3) を示すために, 準同型写像

$$\Gamma : \text{Gal}(M_1M_2/K) \longrightarrow \text{Gal}(M_1/K) \times \text{Gal}(M_2/K), \quad \sigma \mapsto (\sigma|_{M_1}, \sigma|_{M_2})$$

を考える. いま, $\sigma \in \text{Ker } \Gamma$ ならば, $\sigma|_{M_1} = \text{id}_{M_1}$, $\sigma|_{M_2} = \text{id}_{M_2}$ だから, $\sigma|_{M_1M_2} = \text{id}_{M_1M_2}$, したがって $\text{Ker } \Gamma = \{\text{id}_{M_1M_2}\} = \{1\}$, すなわち Γ は单射であり (2) が得られた. 次に, $G = \text{Gal}(M_1M_2/K)$ とおき, M_1, M_2 に対応する G の部分群を H_1, H_2 とする. M_1, M_2 は K 上ガロアだから, 定理 11.3 より, H_1, H_2 は G の正規部分群で, 自然な同型

$$\text{Gal}(M_1/K) \cong G/H_1, \quad \text{Gal}(M_2/K) \cong G/H_2$$

が得られる. したがって, 上で定義した单射準同型写像 Γ は

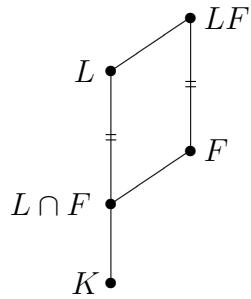
$$\Gamma : G \longrightarrow G/H_1 \times G/H_2$$

と書き換えることができる. ここで, H_1, H_2 の正規性から, $H_1 \cup H_2$ で生成される群は

$$H_1H_2 = \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$$

と一致する。一方、定理 11.1 (2) より、 $H_1 \cap H_2$ は $M_1 M_2$ に対応するから単位群である； $H_1 \cap H_2 = \{1\}$ 。よって、 $H_1 H_2$ は直積群 $H_1 \times H_2$ と同型であり、さらに $M_1 \cap M_2$ に對応していることが定理 11.1 (3) からわかる。そこで、とくに $M_1 \cap M_2 = K$ の場合を考えると、 $G = H_1 H_2 \cong H_1 \times H_2$ であって、 G の位数と $G/H_1 \times G/H_2$ の位数は等しくなる。したがって、 Γ は同型写像であり (3) が確かめられた。□

定理 11.6 L/K が有限次ガロア拡大ならば、 K 上の任意の拡大体 F に対して、 LF/F はガロア拡大であり、そのガロア群は $\text{Gal}(L/(L \cap F))$ と同型である。とくに $\text{Gal}(LF/F)$ は $\text{Gal}(L/K)$ の部分群と同型である。



証明 L/K は分離拡大なので、 L の任意の元は K 上分離的だから、 F 上でも分離的、したがって命題 8.10 等を用いれば、 LF/F は分離拡大である。一方、定理 9.15 より LF は F 上正規であるから、 LF/F はガロア拡大である。定理の後半を示すために、 $M = L \cap F$ とおき、準備として

$$[L : M] = [LF : F]$$

が成り立つことを確かめよう。 L/K は有限次分離拡大だから、原始元定理（定理 8.7）より、 $L = K(\alpha)$ となるような $\alpha \in L$ がとれる。 $f(X)$ を α の K 上の最小多項式、 $g(X)$ を α の F 上の最小多項式とする。 $f(X) \in F[X]$ と考えれば、 $f(X)$ は $g(X)$ で割り切れることがわかるから、 $B \subset \text{Conj}(\alpha, K)$ が存在して、

$$g(X) = \prod_{\beta \in B} (X - \beta)$$

と書くことができる。ここで、 L/K は正規であるから $B \subset \text{Conj}(\alpha, K) \subset L$ 、したがって、 $g(X)$ の係数は $L \cap F = M$ に属する。さらに、 $g(X)$ は F 上既約だから M 上でも既約、よって α の M 上の最小多項式となるから、 $L = M(\alpha)$ 、 $LF = F(\alpha)$ に注意すれば、

$$[L : M] = [M(\alpha) : M] = \deg g = [F(\alpha) : F] = [LF : F]$$

が得られた。さて、準同型写像

$$\Delta : \text{Gal}(LF/F) \longrightarrow \text{Gal}(L/M), \quad \sigma \mapsto \sigma|_L$$

を考える ($M \subset F$ なので定義可能)。いま、 $\sigma \in \text{Ker } \Delta$ とすると $\sigma|_L = \text{id}_L$ だが、もともと σ は F 上の写像なので $\sigma|_F = \text{id}_F$ 、したがって $\sigma = \text{id}_{LF}$ であり、 $\text{Ker } \Delta = \{\text{id}_{LF}\} = \{1\}$ 、よって Δ は单射である。さらに、定理 10.3 と上で示した $[LF : F] = [L : M]$ から、 $\text{Gal}(LF/F)$ と $\text{Gal}(L/M)$ の位数は等しいので、 Δ は同型写像であることが導かれる。□