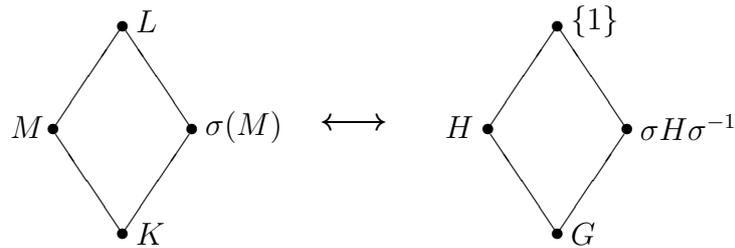


§11. ガロア対応

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. 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 $\sigma(M) \subset \sigma(L) = L$, よって $\sigma(M)$ は L/K の中間体である. また, M と H が対応しているから $M = L^H$, すなわち $\alpha \in L$ に対して

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

したがって,

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

そこで $\rho = \sigma\tau\sigma^{-1}$ と変数変換すれば, $\tau \in H \iff \rho \in \sigma H \sigma^{-1}$ となっているから

$$\beta \in \sigma(M) \iff \rho(\beta) = \beta \quad (\forall \rho \in \sigma H \sigma^{-1}),$$

このことは, 中間体 $\sigma(M)$ が部分群 $\sigma H \sigma^{-1}$ に対応することを示している. \square

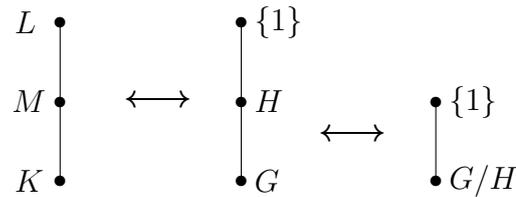
定理 11.2 L/K を有限次ガロア拡大とし, そのガロア群を G とする. M を L/K の中間体, H を M に対応する G の部分群とする. このとき, M/K がガロア拡大であるためには, H が G の正規部分群であることが必要十分である. またこのとき M/K のガロア群は G/H で与えられる. 詳しくは, 制限写像

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

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。□

系 11.3 L/K を有限次ガロア拡大、 M をその任意の中間体とする。

- (1) 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。
- (2) 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。
- (3) L/K が可解拡大ならば、 L/M も可解拡大であり、さらに $\text{Gal}(L/M)$ 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。このことと定理 11.2 から (2) 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 (1) 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。□

定理 11.4 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) $M_1 \cap M_2$ 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。
- (3) 合成体 $M_1 M_2$ に対応する部分群は $H_1 \cap H_2$ 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、

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

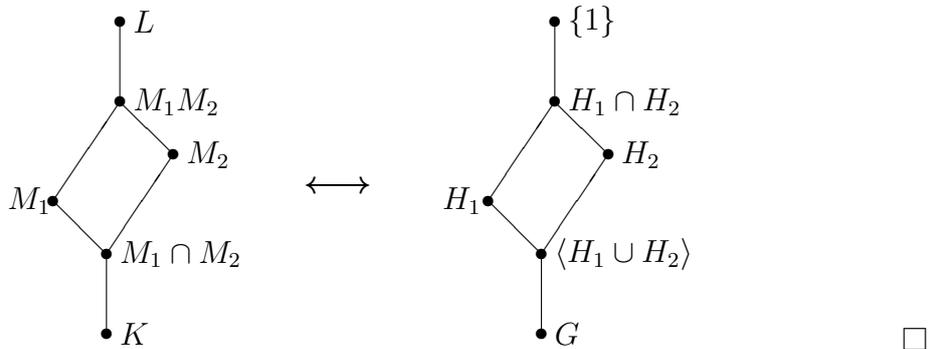
よって $H_2 \subset H_1$ を得る。逆に $H_2 \subset H_1$ を仮定する。 $x \in M_1 = L^{H_1}$ を任意にとると、

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

よって $M_1 \subset M_2$ を得る.

(2) $M_1 \cap M_2$ 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.

(3) $M_1 M_2$ 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.



□

定理 11.5 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) $M_1 M_2$ および $M_1 \cap M_2$ はともに K 上ガロアである.
- (2) $\text{Gal}(M_1 M_2 / K)$ 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

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

が存在する.

証明 (1) は, 定理 8.13 から分離性が, 定理 9.13 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

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

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, $\sigma = \text{id}_{M_1 M_2}$, したがって $\text{Ker } \Gamma = \{\text{id}_{M_1 M_2}\} = \{1\}$, すなわち Γ は単射であり (2) が得られた. 次に, $G = \text{Gal}(M_1 M_2 / K)$ 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 11.2 より, H_1, H_2 は G の正規部分群であり,

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

したがって, 上で定義した単射準同型写像 Γ は

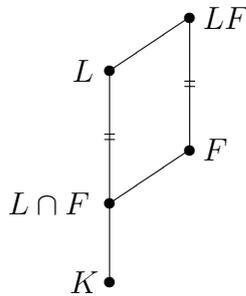
$$\Gamma : G \longrightarrow G / H_1 \times G / H_2$$

と書き換えることができる. 一方, H_1, H_2 の正規性から, $H_1 \cup H_2$ で生成される群は

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

と表すことができる. ここで, 定理 11.4 (3) より, $H_1 \cap H_2$ は $M_1 M_2$ に対応するから単位群, すなわち $H_1 \cap H_2 = \{1\}$ である. 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 $M_1 \cap M_2$ に対応していることが定理 11.4 (2) 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. よってこの場合, Γ は同型写像になり (3) が確かめられた. \square

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, ガロア群は $\text{Gal}(L/(L \cap F))$ と自然に同型となる. 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, $L = K(\alpha)$ とかける. このとき, α は K 上分離的だから F 上もちろん分離的であり, さらに $LF = F(\alpha)$ だから, 命題 8.10 より LF は F 上分離的である. 一方, 定理 9.14 より LF は F 上正規でもあるから, LF/F はガロア拡大である. 次に, 準同型写像

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

を考える. 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, $\text{Ker } \Delta = \{\text{id}_{LF}\} = \{1\}$ を得る. よって Δ は単射である. そこで,

$$\text{Im } \Delta = \text{Gal}(L/L \cap F)$$

を示せば証明は完了する. そのためには, ガロア拡大 L/K において, $\text{Im } \Delta$ に対応する中間体 $L^{\text{Im } \Delta}$ が $L \cap F$ に一致することを確認すればよい. まず, F の元は $\text{Gal}(LF/F)$ で不変だから, $L \cap F$ の元は $\text{Im } \Delta$ で不変, すなわち $L \cap F \subset L^{\text{Im } \Delta}$ が成り立つ. 一方,

$$L^{\text{Im } \Delta} \subset (LF)^{\text{Gal}(LF/F)} = F$$

に注意すれば, $L^{\text{Im } \Delta} \subset L \cap F$ が得られるから, $L^{\text{Im } \Delta} = L \cap F$ が確かめられた. \square