§9. ガロア拡大

定義 9.1 分離拡大かつ正規拡大である体の拡大を**ガロア拡大**という．L/K がガロア拡大のとき，$\mathrm{Aut}(L/K)$ をとくに $\mathrm{Gal}(L/K)$ と表し，L/K の**ガロア群**，または L の K 上のガロア群という．

定理 9.2 有限次拡大 L/K に対して，次は同値である．

(i) L/K はガロアである．
(ii) L は K 上のある分離多項式の K 上の最小分解体である．
(iii) $|\mathrm{Aut}(L/K)| = [L : K]$ が成り立つ．

定義 9.3 L を体とする．L からある体への単射準同型写像の集合 A に対して，

$$L^A = \{\, x \in L \mid \text{任意の } \sigma \in A \text{ に対して } \sigma(x) = x \,\}$$

を A の**不変体**という．

定理 9.4 代数拡大 L/K がガロアであるためには，$K = L^{\mathrm{Aut}(L/K)}$ であることが必要十分である．

定理 9.5 L/K を有限次ガロア拡大とし，H を $\mathrm{Gal}(L/K)$ の部分群とすると，L/L^H はガロア拡大であり，さらに $\mathrm{Gal}(L/L^H) = H$ が成り立つ．

定理 9.6 (ガロア理論の基本定理) 有限次ガロア拡大 L/K に対して，そのガロア群を G とする．$\mathcal{M}_{L/K}$ を L/K の中間体全体の集合，$\mathcal{H}_G$ を G の部分群全体の集合とする;

$$\mathcal{M}_{L/K} = \{\, M \mid M \text{ は } L/K \text{ の中間体} \,\}, \qquad \mathcal{H}_G = \{\, H \mid H \text{ は } G \text{ の部分群} \,\}.$$

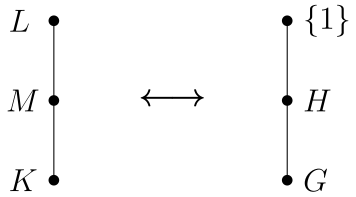
このとき，二つの写像

$$\mathcal{M}_{L/K} \longrightarrow \mathcal{H}_G, \qquad M \mapsto \mathrm{Gal}(L/M)$$

$$\mathcal{H}_G \longrightarrow \mathcal{M}_{L/K}, \qquad H \mapsto L^H$$

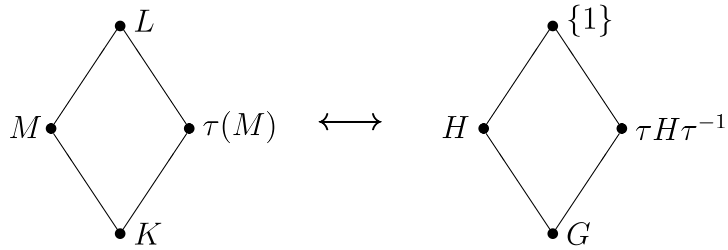
は互いに逆の全単射である．

定義 9.7　有限次ガロア拡大 L/K に対してそのガロア群を G とする．L/K の中間体 M と G の部分群 H の間に，$H = \mathrm{Gal}(L/M)$（すなわち $M = L^H$）の関係があるとき，M, H は互いに対応するという．この対応を**ガロア対応**という．とくに K は G に対応し，L は id_L ($= L$ 上の恒等写像) だけを元にもつ群（単位群）に対応する．今後，この単位群を簡単に $\{1\}$ と略記することにする．

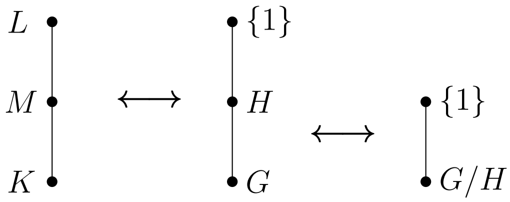


定理 9.8　L/K を有限次ガロア拡大とし，そのガロア群を G とする．M を L/K の中間体，H を M に対応する G の部分群とする．

(1) $\tau \in G$ に対して，$\tau(M)$ は L/K の中間体であり，対応する G の部分群は $\tau H \tau^{-1}$ である．



(2) 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条件である．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

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

から自然に同型

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

が引き起こされる．

定義 9.9 L/K をガロア拡大，そのガロア群を G とする．

(1) G が巡回群のとき，L/K を**巡回拡大**という．

(2) G がアーベル群のとき，L/K を**アーベル拡大**という．

(3) G が可解群のとき，L/K を**可解拡大**という．

系 9.10 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．

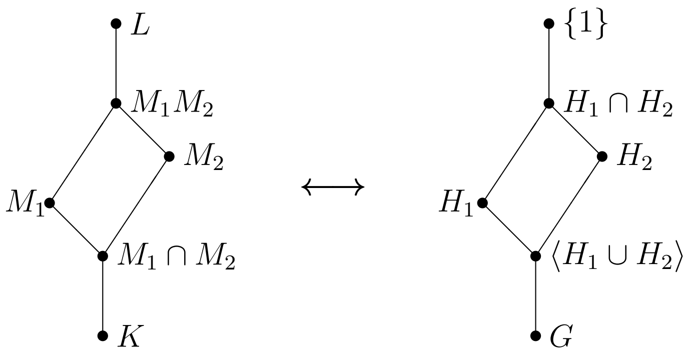
(3) L/K が可解拡大，かつ $\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群ならば，L/M, M/K はともに可解拡大である．

定理 9.11 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．

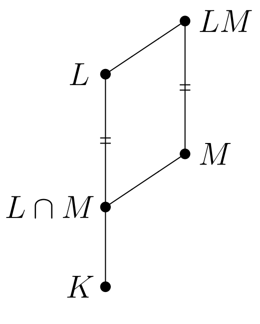
(1) $M_1 \subset M_2$ と $H_1 \supset H_2$ は同値である．

(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_1M_2 に対応する部分群は $H_1 \cap H_2$ である．



定理 9.12 L/K が有限次ガロア拡大ならば，K 上の任意の拡大体 M に対して，LM/M はガロア拡大であり，ガロア群は $\mathrm{Gal}(L/(L\cap M))$ と自然に同型となる． とくに $\mathrm{Gal}(LM/M)$ は $\mathrm{Gal}(L/K)$ の部分群と同型である．



定理 9.13 L_1, L_2 がともに K 上の有限次ガロア拡大体であるとする.

(1) L_1L_2 および $L_1 \cap L_2$ はともに K 上ガロアである.

(2) $\mathrm{Gal}(L_1L_2/K)$ は直積 $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ の部分群に同型である.

(3) 自然な同型

$$\mathrm{Gal}(L_1L_2/(L_1 \cap L_2)) \cong \mathrm{Gal}(L_1/(L_1 \cap L_2)) \times \mathrm{Gal}(L_2/(L_1 \cap L_2))$$

が存在する.