

§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, $\text{Aut}(L/K)$ をとくに $\text{Gal}(L/K)$ 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) $|\text{Aut}(L/K)| = [L : K]$ 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, $K = L^{\text{Aut}(L/K)}$ 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 $\text{Gal}(L/K)$ の部分群とすると, L/L^H はガロア拡大であり, さらに $\text{Gal}(L/L^H) = H$ 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;

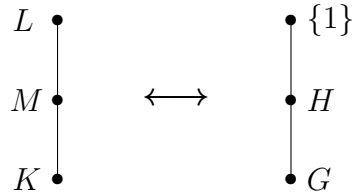
$$\mathcal{M}_{L/K} = \{M \mid M \text{ は } L/K \text{ の中間体}\}, \quad \mathcal{H}_G = \{H \mid H \text{ は } G \text{ の部分群}\}.$$

このとき, 二つの写像

$$\begin{aligned} \mathcal{M}_{L/K} &\longrightarrow \mathcal{H}_G, & M &\mapsto \text{Gal}(L/M) \\ \mathcal{H}_G &\longrightarrow \mathcal{M}_{L/K}, & H &\mapsto L^H \end{aligned}$$

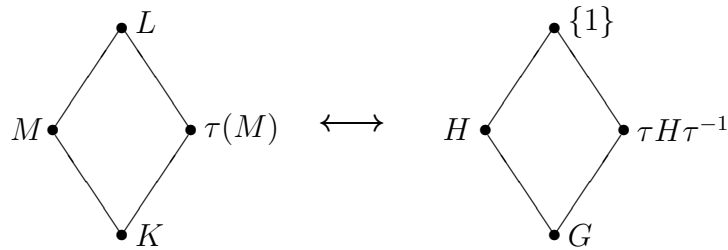
は互いに逆の全単射である.

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, $H = \text{Gal}(L/M)$ (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 $\text{id}_L (= L$ 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.

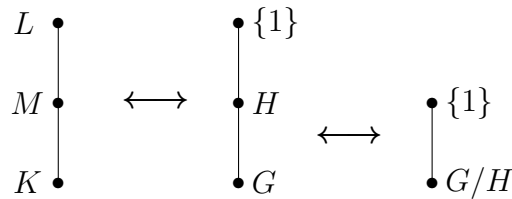


定理 9.8 L/K を有限次ガロア拡大とし, そのガロア群を G とする. M を L/K の中間体, H を M に対応する G の部分群とする.

- (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

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

から自然に同型

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

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.

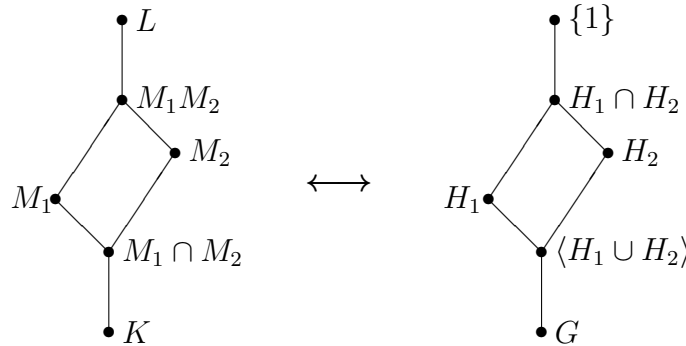
- (1) G が巡回群のとき, L/K を巡回拡大という.
- (2) G がアーベル群のとき, L/K をアーベル拡大という.
- (3) G が可解群のとき, L/K を可解拡大という.

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.

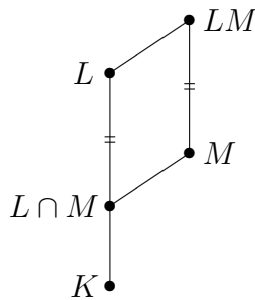
- (1) L/K が巡回拡大ならば, $L/M, M/K$ はともに巡回拡大である.
- (2) L/K がアーベル拡大ならば, $L/M, M/K$ はともにアーベル拡大である.
- (3) L/K が可解拡大, かつ $\text{Gal}(L/M)$ が $\text{Gal}(L/K)$ の正規部分群ならば, $L/M, M/K$ はともに可解拡大である.

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 $M_1 M_2$ 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 $\text{Gal}(L/(L \cap M))$ と自然に同型となる. とくに $\text{Gal}(LM/M)$ は $\text{Gal}(L/K)$ 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) $\text{Gal}(L_1L_2/K)$ は直積 $\text{Gal}(L_1/K) \times \text{Gal}(L_2/K)$ の部分群に同型である.
- (3) 自然な同型

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

が存在する.