§10. ガロア拡大

定義 10.1 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 10.2 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．

証明 (i)$\Rightarrow$(ii): 仮定 (i) より，とくに L/K は有限次分離拡大，よって定理 8.7 より，ある $\alpha \in L$ を用いて $L = K(\alpha)$ とかける． α は K 上分離的だからその最小多項式 $f(X) \in K[X]$ は分離多項式である． さらに L/K は正規だから $\mathrm{Conj}(\alpha, K) \subset L$，したがって，$f(X)$ の K 上の最小分解体 $K(\mathrm{Conj}(\alpha, K))$ は L に等しい．
(ii)$\Rightarrow$(i): L が K 上の分離多項式 $f(X)$ の K 上の最小分解体であるとする． このとき，定理 9.6 より L/K は正規拡大である． 一方，$f(X)$ の根すべてを $\alpha_i\,(i = 1, \ldots, r)$ とすれば，$L = K(\alpha_1, \ldots, \alpha_r)$ と表されるが，各 α_i は K 上分離的なので，命題 8.12 を繰り返し適用すれば，L/K が分離的であることが導かれる． □

定理 10.3 L/K が有限次ガロア拡大ならば，$|\mathrm{Gal}(L/K)| = [L : K]$ が成り立つ．

証明 L/K は有限次分離拡大なので，原始元定理 (定理 8.7) によって $L = K(\alpha)$ と表され，さらに定理 8.4 より，$|\mathrm{Conj}(\alpha, K)| = [K(\alpha) : K]$ が成り立つ． 一方，$L = K(\alpha)$ は K 上正規でもあるので，定理 9.7 より $|\mathrm{Gal}(K(\alpha)/K)| = |\mathrm{Conj}(\alpha, K)|$，したがって結論の等式を得る． □

定義 10.4 L を体とし，Ω を L の拡大体とする． L から Ω への単射準同型写像の集合 H に対して，

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

を H の（L における）**不変体**という（H の元が準同型写像であることを用いれば，不変体 L^H は L の部分体であることが確かめられる）．

以下，多くの場合，H は代数拡大 L/K の自己同型群 $\mathrm{Aut}(L/K)$ の部分群である． 次の補題は，不変体の定義からすぐに示すことができる．

補題 10.5　L/K を体の拡大とする．

(1) L/K の任意の中間体 M に対して，$M \subset L^{\mathrm{Aut}(L/M)}$ が成り立つ．

(2) $\mathrm{Aut}(L/K)$ の任意の部分群 H に対して，$H \subset \mathrm{Aut}(L/L^H)$ が成り立つ．

定理 10.6　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．

証明　必要性: $M = L^{\mathrm{Aut}(L/K)}$ とおくと，前補題 (1) から $K \subset M$ である．そこで，L/K がガロア，すなわち分離的かつ正規であることを仮定して，$M \subset K$ を導く．そのために $\alpha \in M$ を任意にとる．M の定義から，任意の $\sigma \in \mathrm{Aut}(L/K)$ に対して $\sigma(\alpha) = \alpha$ であるが，L/K は正規なので，定理 9.1 の性質 (iii) を用いれば，$\mathrm{Conj}(\alpha, K) = \{\alpha\}$ が得られる．さらに，α は K 上分離的だから，定理 8.4 より

$$[K(\alpha) : K] = |\mathrm{Conj}(\alpha, K)| = 1, \qquad \therefore\ K(\alpha) = K$$

よって $\alpha \in K$ となるから，$M \subset K$ が導かれた．
十分性: $K = L^{\mathrm{Aut}(L/K)}$ を仮定し，任意の $\alpha \in L$ に対して，

$$(\spadesuit) \qquad |\mathrm{Conj}(\alpha, K)| = [K(\alpha) : K], \qquad \mathrm{Conj}(\alpha, K) \subset L$$

を確かめればよい．なぜなら，前者の等式と定理 8.4 から L/K の分離性が，後者の包含関係と定理 9.1 の性質 (iv) から L/K の正規性が導かれるからである．いま，

$$B_\alpha = \{\, \sigma(\alpha) \mid \sigma \in \mathrm{Aut}(L/K) \,\}$$

とおけば，$B_\alpha \subset L$ であり，系 6.12 より

$$(\heartsuit) \qquad B_\alpha \subset \left\{\, \sigma(\alpha) \mid \sigma \in \mathrm{Aut}(\overline{K}/K) \,\right\} = \mathrm{Conj}(\alpha, K),$$

よって，

$$(\diamondsuit) \qquad |B_\alpha| \le |\mathrm{Conj}(\alpha, K)| \le [K(\alpha) : K]$$

が成り立つ．とくに，B_α は有限集合であり，L 上の多項式

$$f_\alpha(X) = \prod_{\beta \in B_\alpha} (X - \beta)$$

を定義することができる．ここで，任意の $\sigma \in \mathrm{Aut}(L/K)$ に対して

$$f_\alpha^\sigma(X) = \prod_{\beta \in B_\alpha} (X - \sigma(\beta)) = \prod_{\gamma \in \sigma(B_\alpha)} (X - \gamma)$$

だが，$\mathrm{Aut}(L/K)$ が群であることに注意すれば，$\sigma(B_\alpha) = B_\alpha$，よって $f_\alpha^\sigma(X) = f_\alpha(X)$ であることがわかる．すなわち $f_\alpha(X)$ の係数は $L^{\mathrm{Aut}(L/K)} = K$ に属する; $f_\alpha(X) \in K[X]$．さらに $f_\alpha(\alpha) = 0$ であるから，補題 3.5 より

$$[K(\alpha) : K] \le \deg f_\alpha(X) = |B_\alpha|\,.$$

よって，$(\heartsuit)$ の包含関係と $(\diamondsuit)$ の不等号はすべて等号に置き換えられ，

$$\mathrm{Conj}(\alpha, K) = B_\alpha \subset L, \qquad |\mathrm{Conj}(\alpha, K)| = [K(\alpha) : K],$$

すなわち $(\spadesuit)$ が確かめられた．　□

系 10.7 L/K をガロア拡大としそのガロア群を G とする．M を L/K の中間体とすると，L/M はガロア拡大でそのガロア群 $\mathrm{Gal}(L/M)$ は G の部分群であり，さらに $L^{\mathrm{Gal}(L/M)} = M$ が成り立つ．

証明 L/K の分離性から L/M が分離的であること（定理 8.11），また，L/K の正規性から L/M が正規拡大であること（定理 9.13）がわかるから，L/M はガロア拡大である．後半は前定理から導かれる． □

定理 10.8 L/K を有限次ガロア拡大としそのガロア群を G とする．H を $\mathrm{Gal}(L/K)$ の部分群とすると，L^H は L/K の中間体，したがって 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．

証明 $M = L^H$ とおく．L/M がガロア拡大であることは，系 10.7 で示されている．補題 10.5 (2) より $H \subset \mathrm{Gal}(L/M)$ であり，このことと定理 10.3 を用いて

$$|H| \leq |\mathrm{Gal}(L/M)| = |\mathrm{Aut}(L/M)| = [L:M].$$

一方，原始元定理 (定理 8.7) より $L = M(\alpha)$ をみたす $\alpha \in L$ がとれる．そこで，L 上の多項式

$$g_\alpha(X) = \prod_{\sigma \in H} (X - \sigma(\alpha))$$

を考えると，H が群であることから，任意の $\sigma \in H$ に対して $g_\alpha^\sigma(X) = g_\alpha(X)$ であり，$g_\alpha(X)$ の係数は $L^H = M$ に属することがわかる; $g_\alpha(X) \in M[X]$．さらに $g_\alpha(\alpha) = 0$ なので

$$[L:M] \leq \deg g_\alpha(X) = |H|\,.$$

したがって，上の不等式と合わせて $|H| = |\mathrm{Gal}(L/M)|$ であり，よって $H = \mathrm{Gal}(L/M)$ を得る． □

定理 10.9 (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．

証明　写像に名前を付けて，$\Phi : \mathcal{M}_{L/K} \to \mathcal{H}_G$ および $\Psi : \mathcal{H}_G \longrightarrow \mathcal{M}_{L/K}$ とする．このとき，任意の $M \in \mathcal{M}_{L/K}$，$H \in \mathcal{H}_G$ に対して

$$\Psi(\Phi(M)) = M, \qquad \Phi(\Psi(H)) = H$$

を示せばよいが，これらはそれぞれ

$$L^{\mathrm{Gal}(L/M)} = M, \qquad \mathrm{Gal}(L/L^H) = H$$

のことであり，系 10.7，定理 10.8 ですでに示されている．□

定義 10.10　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;

$$G = \mathrm{Gal}(L/K).$$

L/K の中間体 M と G の部分群 H の間に，

$$H = \mathrm{Gal}(L/M)$$

あるいは，これと同値な

$$M = L^H$$

の関係があるとき，M と 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，単位群を簡単に $\{1\}$ と略記することにする．

$$\begin{tikzcd} L \arrow[d, dash] & & \{1\} \arrow[d, dash] \\ M \arrow[d, dash] & \longleftrightarrow & H \arrow[d, dash] \\ K & & G \end{tikzcd}$$

定義 10.11　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．
(4) G がシン群のとき，L/K を**シン拡大**という（ジョークです！ごめん）．

例 10.12　(1)　素数次ガロア拡大は巡回拡大である．なぜなら，素数位数の有限群は巡回群だから．

(2)　次数 5 以下のガロア拡大はアーベル拡大である．なぜなら，位数が 5 以下の有限群はすべてアーベル群だから．

(3)　次数 60 未満のガロア拡大は可解拡大である．なぜなら，位数が 60 未満の有限群はすべて可解群だから．