補題:有限次拡大 $K \subseteq L$ の有限個の真の中間体 $K \subseteq M_1, \ldots, M_s \subsetneq L$ について $L \neq M_1 \cup \cdots \cup M_s$.

補題：有限次拡大 $K \subseteq L$ について，$\mathrm{Gal}(L/K)$ は有限群.

定理 A：有限次拡大 $K \subseteq L$ について，$|\mathrm{Gal}(L/K)| \leq [L:K]$．等号が成立するとき，相異なる $z_1, \ldots, z_s \in L$ で $\mathrm{Irr}(K; z_1) = (x - z_1) \cdots (x - z_s)$ かつ $L = K(z_1)$ となるものが存在する.

証明：$G = \mathrm{Gal}(L/K)$ とする．補題より元 $z \in L \setminus \bigcup_{e \neq \sigma \in G} L^\sigma$ を取ることができる（ここで $L^\sigma = \{v \in L \mid \sigma(v) = v\} (= L^{\langle \sigma \rangle})$）．取り方から $|G| = |\{\sigma(z) \mid \sigma \in G\}|$．よって $p(x) = \mathrm{Irr}(K; z)$ について, $\deg p(x) \geq |G|$ である．すなわち $[K(z):K] \geq |G|$ を得たので, $[L:K] \geq [K(z):K] \geq |G|$. 等号が成立するとき，$L = K(z)$ で $p(x) = \prod_{\sigma \in G}(x - \sigma(z))$ でなければならない.

定理 B（Artin）：体拡大 $K \subseteq L$ と，有限部分群 $H \subseteq \mathrm{Gal}(L/K)$ について，$[L : L^H] \leq |H|$.

証明：$m > |H|$ のとき任意の $x_1, \ldots, x_m \in L$ は非自明な L^H 線形関係を持つことを示す．$\sigma \in H$ 毎に線形方程式 $\sum_{i=1}^m c_i \sigma(x_i) = 0$ を連立させる（ここで $c_1, \ldots, c_m \in L$）．$\boldsymbol{c} = (c_1, \ldots, c_m)$ が解ならば, 任意の $\tau \in H$ について, $\tau(\boldsymbol{c}) = (\tau(c_1), \ldots, \tau(c_m))$ も解であることを注意する．$m > |H|$ より, 非自明な解が存在する．このうち非ゼロ成分の数が最小の解を 1 つ選んで, $\boldsymbol{c}' = (c'_1, \ldots, c'_m)$ とする．このとき $c'_j = 1$ となる $1 \leq j \leq m$ が存在するとしてよい．取り方から，任意の $\tau \in H$ について，$\boldsymbol{c}' - \tau(\boldsymbol{c}') = \boldsymbol{0}$ でなければならない．よって $c'_1, \ldots, c'_m \in L^H$ が得られた.

系:体拡大 $K \subseteq L$ と, 有限部分群 $H \subseteq \mathrm{Gal}(L/K)$ について, $\mathrm{Gal}(L/L^H) = H$ かつ $|H| = [L : L^H]$.

証明:定理 A と B より $|H| \geq [L : L^H] \geq |\mathrm{Gal}(L/L^H)|$ である．一方で $H \subseteq \mathrm{Gal}(L/L^H)$ である.

定理 C:有限次拡大 $K \subseteq L$ について, 相異なる $z_1, \cdots, z_s \in L$ で $\mathrm{Irr}(K; z_1) = (x - z_1) \ldots (x - z_s)$ かつ $L = K(z_1)$ となるものが存在するとき，$K = L^{\mathrm{Gal}(L/K)}$.

証明：$L \cong K[x]/(\mathrm{Irr}(K; z_1))$ より，$\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_s\}$ である（ここで σ_i は $\sigma_i(z_1) = z_i$ によって定まる）．$v = c_0 + c_1 z_1 + \cdots + c_{s-1} z_1^{s-1} \in L$ を取る（ここで $c_1, \ldots, c_s \in K$）．$\sigma_i(v) = v$ を $i = 1, \ldots, m$ について連立させると,

$$\begin{pmatrix} v \\ v \\ \vdots \\ v \end{pmatrix} = \begin{pmatrix} 1 & z_1 & \ldots & z_1^{s-1} \\ 1 & z_2 & \ldots & z_2^{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_s & \ldots & z_s^{s-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{s-1} \end{pmatrix}$$

を得るが，クラメルの公式より $c_1 = \cdots = c_{s-1} = 0$ である．よって $L^{\mathrm{Gal}(L/K)} \subseteq K$ が示された.

命題：有限次拡大 $K \subseteq L$ について，相異なる $w_1, \ldots, w_t \in L$ で，$(x - w_1) \ldots (x - w_t) \in K[x]$ かつ $L = K(w_1, \ldots, w_t)$ となるものが存在するとき，$|\mathrm{Gal}(L/K)| = [L:K]$.

証明：$K_i = K(w_1, \ldots, w_i)$ について，K 環準同型 $K_i \to L$ は $[K_i : K]$ 個あることを示す．K 環準同型 $g : K_{i-1} \to L$ について，$g'|_{K_{i-1}} = g$ なる K 環準同型 $g : K_i \to L$ は丁度 $[K_i : K_{i-1}]$ 個ある（このことは，$K_i \cong K_{i-1}[x]/(\mathrm{Irr}(K_{i-1}; w_i))$ と，$\mathrm{Irr}(K_{i-1}; w_i)$ が L において異なる一次式に分解することから従い，定理 C の証明の最初の議論と同様である）.

系（ガロア拡大の特徴付け）：有限次拡大 $K \subseteq L$ について，次は同値である．

(P) 相異なる $w_1, \dots, w_t \in L$ で，$(x-w_1)\dots(x-w_t) \in K[x]$ かつ $L = K(w_1, \dots, w_t)$ となるものが存在する．
(Q) $|\mathrm{Gal}(L/K)| = [L:K]$.
(R) ある部分群 $H \subseteq \mathrm{Gal}(L/K)$ が存在して，$K = L^H$（注：このとき系より $H = \mathrm{Gal}(L/K)$）．

証明：(P) のとき，命題と定理 A より L/K は定理 C の仮定を満たす．よって $H = \mathrm{Gal}(L/K)$ として (R) が従う．(R) のとき，系より (Q) が従う．(Q) のとき，定理 A より (P) が従う．

系（ガロア理論の基本定理）：有限次拡大 $K \subseteq L$ がガロア拡大ならば，対応

$$\{M \mid K \subseteq M \subseteq L : \text{中間体}\} \to \{H \mid H \subseteq \mathrm{Gal}(L/K) : \text{部分群}\}, \quad M \mapsto \mathrm{Gal}(L/M)$$

は全単射で、逆写像は $H \mapsto L^H$ によって与えられる．

証明：中間体 M について，(P) より L/M はガロア拡大である．よって (R) より $L^{\mathrm{Gal}(L/M)} = M$．部分群 H について，$\mathrm{Gal}(L/L^H) = H$ は，定理 A,B の直後の系であった．

系（ガロア理論の基本定理の続き）：上の全単射で，以下は同値．

(X) M/K がガロア拡大
(Y) $\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群

このとき制限 $\sigma \mapsto \sigma|_M$ は，群同型 $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$ を誘導する．

証明：中間体 M と $\tau \in \mathrm{Gal}(L/K)$ について，$\mathrm{Gal}(L/\tau(M)) = \tau\,\mathrm{Gal}(L/M)\tau^{-1}$ を導くことは易しい．(X) ならば (P)（を M に適用することに）より $\tau(M) = M$ が分かるので (Y) である．(Y) ならば，$\mathrm{Gal}(L/\tau(M)) = \mathrm{Gal}(L/M)$ より $\tau(M) = M$ である．よって制限は準同型 $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ を誘導し，単射 $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \hookrightarrow \mathrm{Gal}(M/K)$ が得られる．左辺の個数は (Q) と連鎖律より $[M:K]$ であるから，定理 A と (P) より (X) である．

例：$K = \mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ はガロア拡大．実際 $\mathrm{Irr}(\mathbb{Q}; \sqrt{2}+\sqrt{3}) = x^4 - 10x^2 + 1$ の解は

$$\alpha_1 = \sqrt{2}+\sqrt{3}, \quad \alpha_2 = \sqrt{2}-\sqrt{3} = -\frac{1}{\alpha_1}, \quad \alpha_3 = -\sqrt{2}+\sqrt{3} = \frac{1}{\alpha_1}, \quad \alpha_4 = -\sqrt{2}-\sqrt{3} = -\alpha_1.$$

よって $G = \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ であり（ここで σ_i は $\sigma(\alpha_1) = \alpha_i$ で決まる），$|G| = 4$ なので $G \cong C_4$ または $G \cong C_2 \times C_2$ である．$\forall i, \sigma_i^2 = \mathrm{id}$ から後者と分かる．ガロア対応は

$$\{e\} \leftrightarrow K(= \mathbb{Q}(\sqrt{2}, \sqrt{3})), \{\sigma_1, \sigma_2\} \leftrightarrow \mathbb{Q}(\sqrt{2}), \{\sigma_1, \sigma_3\} \leftrightarrow \mathbb{Q}(\sqrt{3}), \{\sigma_1, \sigma_4\} \leftrightarrow \mathbb{Q}(\sqrt{6}), G \leftrightarrow \mathbb{Q}.$$

例：$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ はガロア拡大ではないが，$K = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ はガロア拡大である（ここで ω は 1 の原始 3 乗根）．$G = \mathrm{Gal}(K/\mathbb{Q}) \cong C_6$ または $G \cong \mathfrak{S}_3$ だが，ガロア拡大でない中間体の存在から後者と分かる．中間体は $K, \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}$．ここで $\mathbb{Q}(\sqrt{-3})$ は $\mathfrak{S}_3$ の正規部分群に対応し，$\mathbb{Q}(\sqrt[3]{2}\omega^i)$ は $\mathfrak{S}_3$ の互換で生成される位数 2 の部分群の対応する（$i = 0, 1, 2$）．