Sei $L\colon K$ eine endliche Körpererweiterung. Setze

$$\mathrm{Gal}(L\colon K) = \{\ \sigma\colon L \to L \mid\ \sigma \text{ ist } K\text{-linearer Körper-Automorphismus von } L\ \},$$

dies ist (bezüglich der Hintereinanderschaltung) eine Gruppe. (Genau dann ist ein Körper-Automorphismus $\sigma\colon L \to L$ $K$-linear, wenn $\sigma(x) = x$ für alle $x \in K$ gilt.)

Ist $L$ ein Körper und $G$ eine Gruppe von Körper-Automorphismen von $L$, so setzen wir

$$\mathrm{Fix}(G) = \{\ \alpha \in L \mid \sigma(\alpha) = \alpha \quad \text{für alle} \quad \sigma \in G\ \},$$

dies ist ein Unterkörper von $L$ und es gilt: *Ist $G$ endlich, so ist* $[L\colon \mathrm{Fix}(G)] = |G|$. (Die Ungleichung $[L\colon \mathrm{Fix}(G)] \geq |G|$ ist eine direkte Folgerung aus dem Dedekind-Lemma; die umgekehrte Ungleichung ist nicht offensichtlich).

Eine endliche Körper-Erweiterung $L\colon K$ ist *galois'sch*, falls $K = \mathrm{Fix}\,\mathrm{Gal}(L\colon K)$ gilt. *Genau dann ist eine endliche Körper-Erweiterung $L\colon K$ galois'sch, wenn $L\colon K$ separabel und normal ist.* (Normalität bedeutet, dass jedes irreduzible Polynom in $K[X]$, das in $L$ eine Nullstelle besitzt, über $L$ in Linearfaktoren zerfällt). Eine endliche separable Körper-Erweiterung ist immer primitiv, sei also $L = K[\alpha]$, sei $f \in K[X]$ das Minimalpolynom von $\alpha$ über $K$; genau dann ist $K[\alpha]\colon K$ normal, wenn $f$ über $K[\alpha]$ in Linearfaktoren zerfällt.)

Beweis, dass eine endliche separable und normale Körper-Erweiterung $L\colon K$ galois'sch ist: Sei $[L\colon K] = n$. Da $L\colon K$ separabel ist, gibt es $\alpha \in L$ mit $L = K[\alpha]$. Seien $\alpha = \alpha_1, \ldots, \alpha_n$ die zu $\alpha$ konjugierten Elemente. Da $L\colon K$ normal ist, gehören diese Elemente zu $L$. Sei $\sigma_i\colon K[\alpha] \to \mathbb{C}$ der zu $\alpha_i$ gehörende Ring-Homomorphismus (mit $\sigma_i(\alpha) = \alpha_i$). Wegen $\alpha_i \in L$ ist das Bild von $\sigma_i$ in $L$ enthalten. Die Abbildung $\sigma_i\colon L \to L$ ist injektiv und $K$-linear, also bijektiv: Jedes $\sigma_i$ ist ein $K$-linearer Körper-Automorphismus von $L$. Es ist demnach $\{\sigma_i \mid 1 \leq i \leq n\}$ eine Teilmenge von $\mathrm{Gal}(L\colon K)$. Das Dedekind-Lemma besagt $|\mathrm{Gal}(L\colon K)| \leq n$, also gilt: $\{\sigma_i \mid 1 \leq i \leq n\} = \mathrm{Gal}(L\colon K)$. Sei $G = \mathrm{Gal}(L\colon K)$. Noch einmal verwenden wir das Dedekind-Lemma, es liefert $[L\colon \mathrm{Fix}(G)] \geq |G|$. Wegen $K \subseteq \mathrm{Fix}(G) \subseteq L$ folgt $K = \mathrm{Fix}(G)$, demnach ist $L\colon K$ galois'sch.

Sei nun $L\colon K$ eine endliche Körper-Erweiterung, die galois'sch ist, mit Galois-Gruppe $G = \mathrm{Gal}(L\colon K)$. Ist $H \subseteq G$ eine Untergruppe, so ist $\mathrm{Fix}(H)$ ein Unterkörper von $L$, der trivialerweise $K$ enthält (also ein "Zwischenkörper" von $L\colon K$) und $L\colon \mathrm{Fix}(H)$ ist galois'sch mit Galois-Gruppe $\mathrm{Gal}(L\colon \mathrm{Fix}(H)) = H$. Wichtig:

(a) *Jeder Zwischenkörper von $L\colon K$ wird auf diese Weise erhalten.* Anders formuliert: *Die Zuordnung*

$$\{\ \text{Untergruppen von } G\ \} \to \{\ \text{Zwischenkörper von } L\colon K\ \}$$
$$H \mapsto \mathrm{Fix}(H)$$

*ist eine Bijektion* (und zwar eine inklusionsumkehrende Bijektion; die umgekehrte Zuordnung ist für $L \supseteq L' \supseteq K$ durch $L' \mapsto \mathrm{Gal}(L\colon L')$ gegeben — trivialerweise ist $\mathrm{Gal}(L\colon L')$ eine Untergruppe von $G$).

(b) *Genau dann ist* $\mathrm{Fix}(H)\colon K$ *galois'sch, wenn $H$ ein Normalteiler in $G$ ist und in diesem Fall ist* $\mathrm{Gal}(\mathrm{Fix}(H)\colon K) = G/H$.