Ad §6.1: Galoiserweiterungen:

Prop.: Für L/K endlich galoisch ist $|\mathrm{Gal}(L/K)| = [L/K]$.

Bew.: Sei $\bar{L}$ ein algebraischer Abschluss von L. Da L/K separabel ist, gilt nach §5.13 dann $|\mathrm{Hom}_K(L,\bar{L})| = [L/K]$. Da L/K normal ist, gilt für jedes $\varphi \in \mathrm{Hom}_K(L,\bar{L})$ schon $\varphi(L)=L$. Also ist $\mathrm{Hom}_K(L,\bar{L}) = \mathrm{Aut}_K(L)$. qed.

—

Satz: Für jede endliche Gruppe $\Gamma < \mathrm{Aut}(L)$ ist L/L^Γ endlich galoisch mit Galoisgruppe Γ.

Setze $K := L^\Gamma$.

Bew.: (1) Betrachte ein beliebiges $a \in L$. Setze $A := \{\gamma(a) \mid \gamma \in \Gamma\}$, und setze $f(X) := \prod_{a' \in A} (X - a')$. Nach Konstruktion ist $f \in K[X]$.
Wegen $f(a)=0$ ist also a algebraisch über K, und $m_{a,K}$ teilt f. Nach Konstruktion ist f separabel, also auch $m_{a,K}$, also auch a über K. Nach Konstruktion zerfällt f in Linearfaktoren über L. Also enthält L einen Zerfällungskörper von $m_{a,K}$ über K.

(2) Variiere a $\Longrightarrow$ L/K algebraisch, separabel, normal, also galoisch.

(3) Beh.: Für jeden Zwischenkörper $K \subset L' \subset L$ mit L'/K endlich ist $[L'/K] \leq |\Gamma|$.

Beweis: Da L'/K separabel ist, ist $L' = K(a)$ für ein $a \in L'$ nach dem Satz über das primitive Element. Also ist $[L'/K] = [K(a)/K] =$
$= \deg m_{a,K} \overset{(1)}{\leq} \deg(f) = |A| \leq |\Gamma|$. qed.

(4) Beh.: $[L/K] \leq |\Gamma|$.

Beweis: Unter allen L' wie in (3) wähle einen mit $[L'/K]$ maximal. Für alle $b \in L$ ist (1) $\Rightarrow$ b algebraisch über K $\Rightarrow$ $L'(b)/K$ endlich. Wegen der Maximalität folgt $[L'(b)/K] = [L'/K]$, also $L'(b) = L'$, also $b \in L'$. Da b beliebig war, folgt $L = L'$. Aus (3) folgt nun $[L/K] = [L'/K] \leq |\Gamma|$. qed.

(5) Aus $\Gamma < \mathrm{Gal}(L/K)$ folgt nun
$$|\Gamma| \leq |\mathrm{Gal}(L/K)| \overset{\text{P.o.}}{=} [L/K] \overset{(4)}{\leq} |\Gamma|$$
also Gleichheit und $\Gamma = \mathrm{Gal}(L/K)$.

qed

Beispiel: Jede Erweiterung von endlichen Körpern ℓ/k ist endlich galoisch mit zyklischer Galoisgruppe $\langle \mathrm{Frob}_{|k|}|\ell \rangle$.

Beweis: Sei $q := |k|$. Für alle $a \in k$ gilt dann $\mathrm{Frob}_q(a) = a^q = a$, also $k \subset \ell^{\langle \mathrm{Frob}_q|\ell \rangle}$. Aber die Gleichung $a^q = a$ hat höchstens q Lösungen in ℓ, deshalb haben wir sogar $k = \ell^{\langle \mathrm{Frob}_q|\ell \rangle}$. qed.

Beachte: Ist $n := [\ell/k]$, so ist $|\ell| = q^n$ und $\mathrm{Frob}_q|\ell$ hat Ordnung n.

Prop.: Für jede Galoiserweiterung L/K und jeden Zwischenkörper $K \subset K' \subset L$ ist auch L/K' galoisch, und deren Galoisgruppe $\mathrm{Gal}(L/K')$ ist eine Untergruppe von $\mathrm{Gal}(L/K)$.

Beweis:
$$\left.\begin{array}{l} L/K \text{ separabel} \Rightarrow L/K' \text{ separabel} \\ L/K \text{ normal} \Rightarrow L/K' \text{ normal} \end{array}\right\} \Rightarrow L/K' \text{ galoisch.}$$

Klar ist dann $\mathrm{Gal}(L/K') = \mathrm{Aut}_{K'}(L) < \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$. qed.