Bem. Aus Satz 18.1 und Kor. 20.2 folgt, dass eine Körpererweiterung $L:K$ genau dann endl., normal und separabel ist, wenn der Körper L der Zerfällungskörper eines separablen Polynoms $f \in K[X]$ ist. Solche Körpererweiterungen heissen **endl. Galoiserweiterungen** oder kurz **galoisch**.

Lemma 20.3 Es sei L ein Körper und $H \leq \mathrm{Aut}(L)$. Dann gilt $[L : L^H] \leq |H|$.

Beweis: Sei $K := L^H$ und $m := |H|$, wobei $H = \{\sigma_1, \dots, \sigma_m\}$.
Wir führen die Annahme $[L:K] > m$ zu einem Widerspruch.

- Ist $[L:K] > m$, so ex. in L Elemente $\alpha_0, \dots, \alpha_m$ die über K lin. unabh. sind. Für jedes der m Elemente $\sigma_i \in H$ betrachten wir die Gleichung
$$\sigma_i(\alpha_0) \cdot X_0 + \dots + \sigma_i(\alpha_m) \cdot X_m = 0$$
in L in den Unbekannten $X_0, \dots, X_m$.
- Wir erhalten m Gleichungen (für jedes $\sigma_i \in H$ eine Gleichung) mit $m+1$ Unbekannten, welche in L eine nicht-triviale Lösung hat.
- Wir wählen die Lösung mit den meisten Nullstellen ($X_0 \neq 0$) und nummerieren die X_i und α_i so, dass $X_0 \neq 0, \dots, X_q \neq 0, X_{q+1} = 0, \dots, X_m = 0$. ($q \geq 1$)
- Ist $\tau \in H$ (also $\tau = \sigma_j$), so ist $\tau(0) = 0$. Für alle $1 \leq i \leq m$ gilt somit
$$\underbrace{\tau\sigma_i}_{=\sigma_{i'} \in H}(\alpha_0) \cdot \tau(X_0) + \dots + \underbrace{\tau\sigma_i}_{=\sigma_{i'} \in H}(\alpha_m) \cdot \tau(X_m) = 0$$
- Die Matrix dieses Gleichungssystems ist bis auf Vertauschung der Zeilen dieselbe wie für das ursprüngliche Gleichungssystems, also ist auch $\tau(X_0), \dots, \tau(X_m)$ eine Lösung des ursprünglichen Systems. [Beachte: Die Spalten werden nicht vertauscht.]

- Weil $x_0 \neq 0$ und $\tau \in \mathrm{Aut}(L)$, ist $\tau(x_0) = 0$. Mit x_i $(0 \leq i \leq m)$ $\tau(x_i)$ $(0 \leq i \leq m)$, sind auch $\tau(x_0) \cdot x_i$ und $x_0 \cdot \tau(x_i)$ $(0 \leq i \leq m)$ Lösungen, und somit auch die Differenz

$$x_i' := \tau(x_0) \cdot x_i - x_0 \cdot \tau(x_i) \quad (0 \leq i \leq m).$$

- Weil $x_0' = \tau(x_0) \cdot x_0 - x_0 \cdot \tau(x_0) = 0$ und weil die Spalten nicht vertauscht werden, muss es sich nach Voraussetzung (max. Anzahl 0'en) um die triviale Lösung handeln. Also gilt $x_0' = \ldots = x_m' = 0$.
- D.h. $\tau(x_0) \cdot x_i = x_0 \cdot \tau(x_i)$ und weil $x_0 \neq 0$, ist

$$x_i \cdot x_0^{-1} = \tau(x_i \cdot x_0^{-1}) \quad \text{für alle } \tau \in H.$$

- Somit gilt: $x_i \cdot x_0^{-1} \in L^H = K$. Für jedes x_i ex. ein $z_i := x_i \cdot x_0^{-1} \in K$ mit $x_i = x_0 \cdot z_i$. $\left[x_0 = x_0 \cdot z_0 \Longrightarrow z_0 \neq 0\right]$
- Für $\sigma = \mathrm{id}$ (id = Identität) erhalten wir

$$\alpha_0 \cdot x_0 + \ldots + \alpha_m x_m = 0 = x_0 \cdot (\alpha_0 z_0 + \ldots + \alpha_m x_m)$$

mit $z_i \in K$. Somit ist, weil $x_0 \neq 0$, $\alpha_0 z_0 + \ldots + \alpha_m x_m = 0$, und weil $z_0 \neq 0$ sind $\alpha_0, \ldots, \alpha_m$ über K lin. abh. $\lightning$ zu $[L:K] > m$

→

Satz 20.4 (Hauptsatz der Galoistheorie)

Die Körpererweiterung $L:K$ sei galoissch (d.h. endl., normal und separabel) mit Galoisgruppe $G = \mathrm{Gal}(L:K)$.

Dann ist die Zuordnung

$$\{H : H \leq G\} \longleftrightarrow \{M : K \subseteq M \subseteq L\}$$

(Untergruppen) (Zwischenkörper)

$$H \longmapsto L^H$$

$$\mathrm{Gal}(L:M) \longleftarrow M$$

eine Bijektion zwischen den Untergruppen von G und den Zwischenkörpern von $L:K$.

Beweis: Sei $K \subseteq M \subseteq L$. Da $L:K$ endl., normal, separabel, ist auch (unter anderem mit Bem. zu Kor. 20.2) $L:M$ endl., normal und separabel. [Bem. $M:K$ ist ebenfalls separabel, aber nicht notwendigerweise normal.]

- $H \longmapsto L^H \longmapsto \mathrm{Gal}(L:L^H) \leq G$

  L^H ist Zw.-Körper mit Satz 19.1

  $H \leq \mathrm{Gal}(L:L^H)$ mit Satz 19.1 $\Rightarrow |H| \leq |\mathrm{Gal}(L:L^H)| \leq [L:L^H] \leq |H|$

  (Prop. 19.6, Lem. 20.3)

  $\Rightarrow H = \mathrm{Gal}(L:L^H)$

- $M \longmapsto \underbrace{\mathrm{Gal}(L:M)}_{\leq G \text{ mit Satz 19.2}} \longmapsto L^H = M$ mit Lem. 20.1

⊣

Das folgende Korollar ist eine Folgerung aus Satz 19.10 (über primitive Elemente).

Korollar 20.5 Ist $L:K$ eine endl. separable Körpererweiterung. Dann ist $L:K$ einfach (d.h. es ex. $\alpha \in L$ mit $L = K(\alpha)$).

Beweis: Ist $L:K$ endl. und separabel, dann ist $L = K(\alpha_1, \dots, \alpha_n)$ für $\alpha_i \in L$. Sei N der Zerfällungskörper von $\prod_{i=1}^{n} f_i$ über K, wobei f_i das Min.-Poly. von α_i über K ist.

- Dann ist $N:K$ galoisch (also endl., normal und separabel).
- Mit dem Hauptsatz der Galoistheorie 20.4 entspricht jeder Zwischenkörper $K \subseteq M \subseteq N$ in bijektiver Weise einer Untergruppe von $\mathrm{Gal}(N:K)$.
- Weil $[N:K]$ endlich ist, ist auch $|\mathrm{Gal}(N:K)|$ endlich und somit kann es nur endl. viele Zwischenkörper $K \subseteq M \subseteq N$ (bzw. Untergruppen $H \leq \mathrm{Gal}(N:K)$) geben. Insbesondere gibt es nur endl. viele Zwischenkörper $K \subseteq M \subseteq L \subseteq N$ und mit Satz 19.10 ist $L = K(\alpha)$.

⊣

Im Folgenden sei $L:K$ galoissch (d.h. endl., normal und separabel).

Korollar 20.6 Ist M ein Zwischenkörper, d.h. $K \subseteq M \subseteq L$,
so ist $[M:K] = [\mathrm{Gal}(L:K) : \mathrm{Gal}(L:M)]$
($M:K$: nicht notwendig galoisch; $L:K$: galoisch; $L:M$: galoisch)

Beweis: Sei M ein Zwischenkörper und sei
$$H := \mathrm{Gal}(L:M) \leq \mathrm{Gal}(L:K) =: G.$$
- Es gilt $|G| = [L:K]$ und $|H| = [L:M]$ (mit Satz 18.1)
- Aus $[L:K] = [L:M] \cdot [M:K]$ folgt:
$$[M:K] = \frac{[L:K]}{[L:M]} = \frac{|G|}{|H|} = [G:H]$$
⊣

Korollar 20.6 Jeder aufsteigenden Folge von Zwischenkörpern
$$K \subseteq M_1 \subseteq \ldots \subseteq M_n \subseteq L$$
entspricht eine absteigende Folge von Untergruppen von $\mathrm{Gal}(L:K)$:
$$\mathrm{Gal}(L:K) \geq \mathrm{Gal}(L:M_1) \geq \ldots \geq \mathrm{Gal}(L:M_n) \geq \mathrm{Gal}(L:L)$$
$$G \geq H_1 \geq \ldots \geq H_n \geq \{e\}$$
bzw. $\{\mathrm{id}\}$ mit $\mathrm{id} \in \mathrm{Aut}(L)$

Beweis:
- Die Körpererweiterungen $L:M_i$ sind endl., normal und separabel, also galoissch.
- M_{i+1} ist ein Zwischenkörper der Körpererweiterung $L:M_i$, d.h. $M_i \subseteq M_{i+1} \subseteq L$.
- Somit ist $\mathrm{Gal}(L:M_{i+1}) = H_{i+1} \leq H_i = \mathrm{Gal}(L:M_i)$.

⊣

Ein einfaches Beispiel: Sei $L = K(\alpha)$ mit $[K(\alpha):K] = 2$.
Dann ist $\alpha^2 \in K$ und L ist der Zerfällungskörper von $X^2 - \alpha^2$ über K. Weiter ist $|\mathrm{Gal}(L:K)| = [L:K] = 2$, d.h. $G := \mathrm{Gal}(L:K) \cong C_2$ und für $H \leq G$ gilt $H = \{e\}$ oder $H = G$. Somit hat $L:K$ keine nicht-trivialen Zwischenkörper.