Beweis von Satz 19.7: Wir betrachten zuerst den Fall $L = K(\alpha)$ für ein $\alpha \in L$, und zeigen, dass es höchstens $[K(\alpha):K]$ verschiedene Körperhomom. $\tilde{\varphi}: K(\alpha) \to L'$ mit $\tilde{\varphi}|_K = \varphi$ gibt:

- Sei $f = \sum_{i=0}^{n} a_i X^i$ das Min.-Polynom von α über K.
- Sei $\tilde{\varphi}: K(\alpha) \to L'$ ein Körperhomom.
- Es gilt $[K(\alpha):K] = \operatorname{grad}(f) = n$.
- Für $\hat{f} := \sum_{i=0}^{n} \varphi(a_i) X^i \in L'[X]$ ist $\hat{f}(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(\underbrace{f(\alpha)}_{=0}) = 0$, und somit wird α durch $\tilde{\varphi}$ auf eine Nullstelle von $\hat{f}$ abgebildet. Da nun $\hat{f}$ höchstens n Nullstellen hat, gibt es somit höchstens n Elemente in L', auf die α durch $\tilde{\varphi}$ abgebildet werden kann.
- Andererseits ist $\tilde{\varphi}$ nach Aufgabe 109 (bzw. der Bem. am Ende der Lösung) eindeutig durch das Bild von α bestimmt.

Somit gibt es höchstens $[K(\alpha):K]$ Möglichkeiten für $\tilde{\varphi}$.

Für den allg. Fall verwenden wir Induktion nach $[L:K]$.

- $[L:K] = 1$ ist klar.
- Für $[L:K] > 1$ wählen wir $\alpha \in L$ mit $\operatorname{grad}(\alpha) = r > 1$, wobei $\operatorname{grad}(\alpha) := \operatorname{grad}(f)$ für f Min.-Poly. von α über K.
- Für jeden Körperhom. $\tilde{\varphi}: L \to L'$ mit $\tilde{\varphi}|_K = \varphi$ betrachten wir $\tilde{\varphi}|_{K(\alpha)}$.
- Aus dem obigen Fall erhalten wir höchstens $[K(\alpha):K]$ solche Restriktionen $\tilde{\varphi}|_{K(\alpha)}$. (Ind.-Voraus. / obiger Fall)
- Mit dem Gradsatz $[L:K] = [L:K(\alpha)] \cdot [K(\alpha):K]$ und der Ind.-Voraussetzung erhalten wir dann, dass es höchstens $[L:K]$ versch. Körperhom. $\tilde{\varphi}: L \to L'$ mit $\tilde{\varphi}|_K = \varphi$ gibt.

⊣

Ist die Körpererweiterung $L:K$ endl., normal und separabel (d.h. L ist der Zerfällungskörper eines separablen Polynoms), so erhalten wir eine stärkere Aussage:

Proposition 19.8 Ist L_f der Zerfällungskörper eines separablen Polynoms $f \in K[X]$, so ist

$$|Gal(L:K)| = [L:K].$$

Dies folgt direkt aus

Satz 19.9. Sei L_f der Zerfällungskörper des sep. Polynoms $f \in K[X]$ und sei $\varphi: K \to L'$ ein Körperhom., sodass $\varphi(f)$ über L' in Linearfaktoren zerfällt. Dann gibt es genau $[L:K]$ Körperhom. $\tilde{\varphi}: L \to L'$ mit $\tilde{\varphi}|_K = \varphi$.

Beweis: Wie im Beweis von Satz 19.7; wir verwenden, dass f sep. ist (irred. Faktoren von f haben versch. Nullstellen in L bzw. L') und zeigen den Satz wieder für einfache Körpererweiterungen und mit Induktion nach $[L:K]$. ⊣

Aus dem folgenden Satz wird folgen, dass jede endliche Körpererweiterung $L:K$, wobei $\mathrm{char}(K)=0$, einfach ist.

Satz 19.10. (Satz über primitive Elemente) Eine endliche Körpererweiterung $L:K$ mit $|K| = \infty$ ist einfach genau dann, wenn es nur endlich viele Zwischenkörper M mit $K \subseteq M \subseteq L$ gibt.

Beweis: ($\Leftarrow$) Weil $L:K$ endlich ist, können wir L schreiben als $L = K(\alpha_1, \dots, \alpha_n)$ für $\alpha_i \in L$.

Der Beweis ist mit Induktion über n.

- Der Fall $n=1$ ist klar.
- Ist $M = K(\alpha_1, \dots, \alpha_{n-1})$, dann ist $K \subseteq M \subseteq L$ ein Zwischenkörper und mit Induktionsvoraussetzung ist $M = K(\beta)$ für ein β.
- Dann ist $L = K(\alpha_n, \beta) = K(\alpha_1, \dots, \alpha_n)$.
- Für jedes $a \in K$ definieren wir $M_a := K(\alpha_n + a\beta)$. Dann ist $K \subseteq M_a \subseteq L$ ein Zwischenkörper.
- Weil es nach Voraussetzung nur endl. viele Zwischenkörper gibt aber K unendlich ist, finden wir $a, b \in K$ mit $a \neq b$ und $M_a = M_b$.
- Somit gilt
$$\beta = \frac{(\alpha_n + b\beta) - (\alpha_n + a\beta)}{b-a} \in M_b.$$
- Weiter haben wir $\alpha_n = \underbrace{(\alpha_n + b\beta)}_{\in M_b} - \underbrace{b\beta}_{\in M_b} \in M_b$ und somit ist $L = K(\alpha_n, \beta) = M_b = K(\alpha_n + b\beta)$, also ist $L:K$ einfach.

($\Rightarrow$): Sei nun $L = K(\alpha)$ für ein $\alpha \in L$ und sei M ein Zwischenkörper, also $K \subseteq M \subseteq L$.

- Dann ist $L = M(\alpha)$. Sei f das Min. Poly. von α über K und g das Min.-Poly. von α über M. Dann gilt $g \mid f$.
- Sei $g = a_0 + a_1 X + \dots + X^r$ und sei $M_0 := K(a_0, \dots, a_{r-1}) \subseteq M$. Dann ist $g \in M_0[X]$ für $\tilde{g}$ das Min.-Poly. von α über M_0 gilt $\tilde{g} \mid g$.
- Somit haben wir $[K:M] = \operatorname{grad}(g) \geq \operatorname{grad}(\tilde{g}) = [K:M_0]$
$$= [K:M] \cdot [M:M_0] \Rightarrow [M:M_0] = 1.$$
- Also gilt $M = M_0$ und M ist durch g (mit $g \mid f$) bestimmt, und weil f nur endl. viele normierte Teiler hat, ex. nur endl. viele Zw.-Körper. [im Zerfällungskörper von f]

20. Der Hauptsatz der Galoistheorie

Lemma 20.1 Sei L_f der Zerfällungskörper des separablen Polynoms $f \in K[X]$ und sei $G = \mathrm{Gal}(L_f : K)$. Dann ist $L_f^G = K$.

Beweis: Mit Prop. 19.8 gilt $|\mathrm{Gal}(L_f : K)| = [L_f : K] =: n$.

Sei $K' := L_f^G$, also

$$K' = \{ a \in L_f : \forall \sigma \in G \ (\sigma(a) = a) \}.$$

- Dann ist $K \subseteq K' \subseteq L_f$ und somit $[L_f : K'] =: m \leq n$.
- L_f ist der Zerfällungskörper von $f \in K'[X]$ und mit Prop. 19.8 gilt $[L_f : K'] = m = |\mathrm{Gal}(L_f : K')|$.
- Mit Satz 19.1 ist $G \leq \mathrm{Gal}(L_f : K') = \mathrm{Gal}(L_f : L_f^G)$.
- Somit ist $G = \mathrm{Gal}(L_f : K) = \mathrm{Gal}(L_f : K')$, d.h. $m = n$ und aus $\underbrace{[L_f : K]}_{=n} = \underbrace{[L_f : K']}_{=n} \cdot \underbrace{[K' : K]}_{\Rightarrow = 1}$ folgt $K' = K$.

⊣

Bem. Unter der Voraussetzung von Lemma 20.1 ist der Fixkörper zur Galoisgruppe $\mathrm{Gal}(L_f : K)$ der Körper K.

Korollar 20.2 Ist L_f der Zerfällungskörper eines sep. Polynoms $f \in K[X]$, dann ist die Körpererweiterung $L_f : K$ separabel.

Beachte: Die Körpererweiterung $L_f : K$ ist normal (Satz 18.1).

Beweis: Sei $\alpha \in L_f$ beliebig. Zu zeigen: α ist separabel. Seien $\alpha_1, \ldots, \alpha_r$ die in L_f zu α konj. Elemente, wobei wir jede Nullstelle nur einmal aufführen, und sei $g := (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_r)$.

- Da nun jedes $\sigma \in \mathrm{Gal}(L_f : K) =: G$ die Nullstellen $\alpha_1, \ldots, \alpha_r$ permutiert, ist $\sigma(g) = g$, d.h. die Koeffizienten von g liegen in L^G; mit Lemma 20.1 also in K und somit ist $g \in K[X]$ separabel.

⊣