Sei L/K endlich galoissch mit Galoisgruppe Γ, und sei $\Gamma' < \Gamma$ eine Untergruppe.

7.5.2 Allgemeine Konstruktion: Nach dem Satz vom primitiven Element ist $L = K(a)$ für ein geeignetes $a \in L$. Betrachte das Hilfspolynom

$$F(X) := \sum_{i=0}^{m} b_i X^i := \prod_{\gamma \in \Gamma'} (X - \gamma(a)) \in L[X].$$

schon in $L^{\Gamma'}[X]$
$\Rightarrow$ alle $b_i \in L^{\Gamma'}$.

7.5.3 Satz: Dann gilt $L^{\Gamma'} = K(b_0, \ldots, b_m)$.

Beweis: Sei $K' := K(b_0, \ldots, b_m) \subseteq L^{\Gamma'}$ und $F \in K'[X]$

und $F(a) = 0 \Rightarrow [L : K'] \leq \deg(F) = |\Gamma'| = [L : L^{\Gamma'}]$

$[L : L^{\Gamma'}] \cdot [L^{\Gamma'} : K']$

$\Rightarrow [L^{\Gamma'} : K'] = 1$

$\Rightarrow L^{\Gamma'} = K'$

qed.

Weiter ist der folgende Satz nützlich:

7.5.4 Satz: Die Menge $\Gamma = \mathrm{Gal}(L/K)$, betrachtet als Teilmenge des L-Vektorraums aller Abbildungen $L \to L$, ist L-linear unabhängig.

Beweis: Wenn nicht, so $\sum_{i=1}^{n} a_i \sigma_i = 0$ eine kürzeste nichttriviale Relation mit $\sigma_i \in \mathrm{Gal}(L/K)$ verschieden, $a_i \in L^\times$ und $n \geq 1$. $\Rightarrow n \geq 2$

Für jedes $b \in L^\times$ gilt $\forall x \in L$: $\sum_{i=1}^{n} a_i \sigma_i(b) \cdot \sigma_i(x) = \left(\sum_{i=1}^{n} a_i \sigma_i\right)(bx) = 0$.

$\Rightarrow \sum_{i=1}^{n} a_i \cdot \sigma_i(b) \cdot \sigma_i = 0 \Rightarrow \sum_{i=1}^{n} a_i \cdot \frac{\sigma_i(b)}{\sigma_1(b)} \cdot \sigma_i = 0$.

Da $n \geq 2$ und $\sigma_1 \neq \sigma_2$ ist, existiert $b \in L^\times$: $\sigma_1(b) \neq \sigma_2(b)$

$\Rightarrow \sum_{i=2}^{n} a_i \left(\frac{\sigma_i(b)}{\sigma_1(b)} - 1\right) \cdot \sigma_i = 0$.

Minimalität von $n \Rightarrow \forall i: \frac{\sigma_i(b)}{\sigma_1(b)} - 1 = 0$.

$\Rightarrow \sigma_i(b) = \sigma_1(b)$.

↯ Widerspruch!

qed.

7.5.5 Folge: Für jede Untergruppe $\Gamma' < \mathrm{Gal}(L/K)$ haben wir eine surjektive Abbildung

$$\varphi: \quad L \to L^{\Gamma'},\ x \mapsto \sum_{\gamma \in \Gamma'} \gamma(x).$$

K-linear.

Auch damit kann man also explizite Elemente von $L^{\Gamma'}$ konstruieren.

Beweis: OBdA $\Gamma = \Gamma'$. da L / $L^{\Gamma'}$) galois ist Gruppe Γ'.

$\Rightarrow \varphi : L \to K$ K-linear. $\Rightarrow$ trivial.

Wäre $\varphi = 0$, dann wäre $\sum_{\gamma \in \Gamma} \gamma = 0$ $\Rightarrow$ Widerspruch. z.U.k.

Also $\varphi \neq 0$ $\Rightarrow$ surjektiv.

qed.

7.6 Kreisteilungskörper

Sei n eine natürliche Zahl mit $\mathrm{char}(K) \nmid n$, und sei $\overline{K}$ ein algebraischer Abschluss von K.

7.6.1 Proposition: Die Gruppe der *n-ten Einheitswurzeln*

$$\mu_n := \mu_n(\overline{K}) := \{\zeta \in \overline{K} \mid \zeta^n = 1\}$$

ist eine zyklische Untergruppe der Ordnung n von $\overline{K}^\times$.

7.6.2 Proposition: Die Körpererweiterung $K(\mu_n)/K$ ist endlich galoissch, und es existiert ein eindeutiger Homomorphismus $e\colon \mathrm{Gal}(K(\mu_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ mit der Eigenschaft

$$\forall \gamma \in \mathrm{Gal}(K(\mu_n)/K)\ \forall \zeta \in \mu_n\colon \gamma(\zeta) = \zeta^{e(\gamma)}.$$

Dieser Homomorphismus ist injektiv. Insbesondere ist $\mathrm{Gal}(K(\mu_n)/K)$ abelsch.

7.6.3 Beispiel: Ist k ein endlicher Körper der Kardinalität q, so entspricht $\mathrm{Gal}(k(\mu_n)/k)$ der von der Restklasse $q + n\mathbb{Z}$ erzeugten Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. Zum Beispiel ist $\mathrm{Gal}(\mathbb{F}_2(\mu_{17})/\mathbb{F}_2)$ zyklisch der Ordnung 8.

7.6.4 Satz: Es ist $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$.

(Beweis im allgemeinen Fall: Siehe z.B. Jantzen, Schwermer: Algebra, Kap. 6, §2.)