

Sei  $L/K$  endlich galoissch mit Galoisgruppe  $\Gamma$ , 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  $L^{\Gamma'} = K(b_0, \dots, b_m)$ .

Beweis: Setze  $K' := K(b_0, \dots, b_m) \subseteq L^{\Gamma'}$  und  $f \in K'[X]$

$$\text{und } f(a) = 0 \Rightarrow \left. \begin{aligned} [L/K'] &\leq \deg(f) = |\Gamma'| = [L/L^{\Gamma'}] \\ &\quad \underbrace{\quad}_{\text{''}} \\ &= [L/L^{\Gamma'}] \cdot [L^{\Gamma'}/K'] \end{aligned} \right\} \Rightarrow [L^{\Gamma'}/K'] = 1$$

ged.

Weiter ist der folgende Satz nützlich:

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

...

↑  
bzgl. Addition + · im Bild

Beweis: Wenn nicht, sei  $\sum_{i=1}^n a_i \sigma_i = 0$  eine kürzeste nichttriviale Relation mit  $\sigma_i \in \text{Gal}(L/K)$  verschiedene,

$a_i \in L^x$  und  $n \geq 1 \Rightarrow n \geq 2$

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

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

Da  $n \geq 2$  und  $\sigma_1 \neq \sigma_2$  ist, existiert  $b \in L^x$ :  $\Rightarrow \sum_{i=2}^n a_i \left( \frac{\sigma_i(b)}{\sigma_1(b)} - 1 \right) \cdot \sigma_i = 0$ .

$\sigma_1(b) \neq \sigma_2(b)$

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

$\Rightarrow \sigma_i(b) = \sigma_1(b)$   
 $\Rightarrow$  Widerspruch!

qed

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

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

$\swarrow$   $K$ -linear.

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

Bem: ObdR  $\Gamma = \Gamma'$  da  $\begin{pmatrix} L \\ \Gamma \\ L^{\Gamma'} \end{pmatrix}$  Galois mit Gruppe  $\Gamma'$ .

$\Rightarrow \varphi: L \rightarrow K$   $K$ -linear.  $\Rightarrow$  linear.

Wäre  $\varphi = 0$ , dann wäre  $\sum_{\gamma \in \Gamma} \gamma = 0 \Rightarrow$  Widerspruch. 7.5.4.

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

qed.

## 7.6 Kreisteilungskörper

$$u = p^k, p = \text{char}(K) > 0 \\ \Rightarrow \mu_n = \{1\}$$

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

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

Bsp.:  $K \subset \mathbb{C} = \bar{K}$   
 $\mu_n = \langle e^{\frac{2\pi i}{n}} \rangle$

$$\mu_n := \mu_n(\bar{K}) := \{ \zeta \in \bar{K} \mid \zeta^n = 1 \} = \text{Ker}(\bar{K}^\times \rightarrow \bar{K}^\times, \gamma \mapsto \gamma^n)$$

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

Beweis:  $\frac{d}{dx}(x^n - 1) = n \cdot x^{n-1}$  liefert zu  $x^n - 1$   $\Rightarrow x^n - 1$  separabel  $\Rightarrow |\mu_n(\bar{K})| = n$ .

$\Rightarrow \mu_n$  abelsche Gruppe der Ordnung  $n$ . Sei  $\mu_n \cong \mathbb{Z}_{e_1} \times \dots \times \mathbb{Z}_{e_r}$  mit  $e_1 | e_2 | \dots | e_r$ ;  $e_i \in \mathbb{Z}^{\geq 2}$   
 $\Rightarrow \mu_n$  hat Exponent  $e_r \Rightarrow \forall \zeta \in \mu_n: \zeta^{e_r} = 1 \Rightarrow \zeta$  Nullstelle von  $x^{e_r} - 1 \Rightarrow |n| \leq e_r \Rightarrow n \leq e_r$   
 $e_1 \cdot \dots \cdot e_r = n \Rightarrow n = e_r$

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

$$\forall \gamma \in \text{Gal}(K(\mu_n)/K) \forall \zeta \in \mu_n: \gamma(\zeta) = \zeta^{e(\gamma)}$$

$\mu_n \cong \mathbb{Z}_{e_r}$   
 $\mathbb{Z}_{e_r}^{\times}$

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

Beweis:  $K(\mu_n) = \mathbb{Z}$ -Erweiterung des sep. Polynom  $x^n - 1$  über  $K \Rightarrow K(\mu_n)/K$  endlich galoissch.

Wähle  $\zeta \in \mu_n$  Erzeugendes.  $\forall \sigma \in \Gamma: \sigma(\zeta) = \zeta^{e(\sigma)}$  für ein eindeutiges  $e(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ .

$$\forall \sigma, \tau \in \Gamma: \sigma(\tau(\zeta)) = \sigma(\zeta^{e(\tau)}) = \sigma(\zeta)^{e(\tau)} = (\zeta^{e(\sigma)})^{e(\tau)} = \zeta^{e(\sigma) \cdot e(\tau)}$$

$$(\sigma\tau)(\zeta) = \zeta^{e(\sigma\tau)} \Rightarrow e(\sigma\tau) = e(\sigma) \cdot e(\tau)$$

Insbesondere  $\sigma = \sigma^{-1} \Rightarrow 1 = e(\sigma^{-1}) \cdot e(\sigma) \Rightarrow e(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$

Für jedes  $\zeta \in \mu_n \exists m \in \mathbb{Z} : \zeta = \zeta^m \Rightarrow \zeta(\zeta) = \zeta(\zeta^m) = \zeta^{e(\zeta) \cdot m} = \zeta^{e(\zeta)}$

Jedes  $\zeta \in \mu$  ist eine  $n$ -te  $\zeta \mid \mu_n$  e. i. z. d. Schicht.

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

$\text{Gal}(k(\mu_n)/k)$  erzeugt in  $\sigma : x \mapsto x^q$   
 $\Rightarrow \forall \zeta \in \mu_n : \zeta^{e(\zeta)} = \sigma(\zeta) = \zeta^q$

Analyse:  $\# \tau(u, q) = ?$   
 $q = 2 \Rightarrow \bar{2} \in (\mathbb{Z}/17\mathbb{Z})^\times = \mathbb{F}_{17}^\times$   
 $\bar{2}^4 = \bar{16} = -1$   
 $[\mathbb{F}_2(\mu_{17})/\mathbb{F}_2] = 8 \Rightarrow \bar{2}$  hat Ordnung 8

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

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

$$2^8 - 1 = 256 - 1 = 255$$

$$= 5 \cdot 51$$

$$= 5 \cdot 3 \cdot 17$$