(1

Ad §6.7: Abelsche Körpererweiterungen:

Satz: Sei L/K endlich, und sei n eine natürliche Zahl mit $\mathrm{char}(K) \nmid n$ und $\mu_n \subset K$. Dann sind äquivalent:

(a) L/K ist eine einfache Radikalerweiterung der Form $L = K(a)$ mit $a^n \in K$.

(b) L/K ist zyklisch der Ordnung ein Teiler von n.

Beweis: (a) $\Rightarrow$ (b) Setze $b := a^n \in K$. Dann ist $X^n - b = \prod_{\zeta \in \mu_n} (X - \zeta a)$. Wegen $\mu_n \subset K$ liegen schon alle ζa in L, also ist L Zerfällungskörper dieses Polynoms. Wegen $\mathrm{char}(K) \nmid n$ ist das Polynom separabel. Also ist L/K galoisch. Betrachte die Abbildung

$$\chi : \mathrm{Gal}(L/K) \to \mu_n, \quad \gamma \mapsto \frac{\gamma(a)}{a}.$$

Für jedes γ ist $\gamma(a) = \zeta a$ für ein $\zeta \in \mu_n$ $\Rightarrow$ wohldefiniert.

Für alle $\gamma, \delta \in \mathrm{Gal}(L/K)$ gilt

$$\chi(\delta\gamma) = \frac{\delta\gamma(a)}{a} = \frac{\delta(\gamma(a))}{\delta(a)} \cdot \frac{\delta(a)}{a} = \delta\left(\frac{\gamma(a)}{a}\right) \cdot \frac{\delta(a)}{a} = \underbrace{\delta(\chi(\gamma))}_{\overset{\shortparallel}{\chi(\gamma)} \text{ wegen } \mu_n \subset K} \cdot \chi(\delta)$$

Also ist χ ein Homomorphismus. Weiter ist

$$\mathrm{Kern}(\chi) = \{\gamma \in \mathrm{Gal}(L/K) \mid \gamma(a) = a\} = \mathrm{Gal}(L/K(a)) = 1.$$

Also ist χ injektiv, somit ist $\mathrm{Gal}(L/K)$ isomorph zu einer Untergruppe der zyklischen Gruppe μ_n, also selbst zyklisch.

(b) $\Rightarrow$ (a) Nach Voraussetzung existiert ein injektiver Homomorphismus $\chi : \mathrm{Gal}(L/K) \hookrightarrow \mu_n$. Fixiere einen. Nach dem Satz über die lineare Unabhängigkeit aus §6.5 sind die Abbildungen $\gamma : L \to L$ für alle $\gamma \in \mathrm{Gal}(L/K)$ L-linear unabhängig. Insbesondere ist daher die Linearkombination

$$\varphi := \sum_{\gamma \in \mathrm{Gal}(L/K)} \chi(\gamma)^{-1} \cdot \gamma \neq 0.$$

Wähle $e \in L$ mit $a := \varphi(e) \neq 0$. Für alle $\delta \in \mathrm{Gal}(L/K)$ gilt dann

$$\delta(a) = \delta\Big(\sum_\gamma \chi(\gamma)^{-1} \gamma(e)\Big) \underset{\mu_n \subset K}{=} \sum_\gamma \chi(\gamma)^{-1} \cdot \delta\gamma(e)$$

$$\Big\| \; \gamma' = \delta\gamma$$

$$\chi(\delta) \cdot a = \chi(\delta) \cdot \sum_{\gamma'} \chi(\gamma')^{-1} \gamma'(e) = \sum_{\gamma'} \chi(\delta^{-1}\gamma')^{-1} \cdot \gamma'(e)$$

Wegen $a \neq 0$ gilt also $\delta(a) = a \iff \chi(\delta) = 1 \overset{\chi \text{ inj.}}{\iff} \delta = 1$

Also ist $Gal(L/K(a)) = \{\delta \in Gal(L/K) \mid \delta(a) = a\} = 1$ und somit $L = K(a)$. Andererseits ist

$$\delta(a^n) = (\delta(a))^n = (\chi(\delta)a)^n = \chi(\delta)^n a^n = a^n$$

und somit $a^n \in K$. Also ist $L = K(a)/K$ eine einfache Radikalerweiterung.

<u>qed</u>.

<u>Bsp.</u>: Für beliebige paarweise verschiedene Primzahlen $p_1, \dots, p_n$ ist $K := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ endlich galoisch über $\mathbb{Q}$ mit $\Gamma := Gal(K/\mathbb{Q}) \cong \mathbb{F}_2^n$. Außerdem ist $K = \mathbb{Q}(\sqrt{p_1} + \dots + \sqrt{p_n})$.

<u>Bew.</u>: Als Zerfällungskörper ist $K/\mathbb{Q}$ galoisch. Betrachte die Abbildung

$$\chi : \Gamma \longrightarrow \{\pm 1\}^n, \quad \sigma \mapsto \left(\frac{\sigma(\sqrt{p_1})}{\sqrt{p_1}}, \dots, \frac{\sigma(\sqrt{p_n})}{\sqrt{p_n}}\right).$$

Wie oben zeigt man, dass χ ein injektiver Homomorphismus ist.

<u>Beh.</u>: Er ist surjektiv.

<u>Bew.</u>: Wenn nicht, ist sein Bild in einem $\mathbb{F}_2$-Unterraum von $\mathbb{F}_2^n$. Also existieren $e_1, \dots, e_n \in \{0,1\}$ nicht alle 0, mit $\forall (\gamma_1, \dots, \gamma_n) \in Bild(\chi)$: $\gamma_1^{e_1} \cdots \gamma_n^{e_n} = 1$. Setze dann $a := \prod_{i=1}^n \sqrt{p_i}^{e_i}$.
Dann gilt $\forall \sigma \in \Gamma$: $\sigma(a) = a$; also $a \in \mathbb{Q}$.
Aber $a^2 = \prod_{i=1}^n p_i^{e_i}$ ist kein Quadrat in $\mathbb{Q}$ $\Longrightarrow$ Widerspruch. qed.

Schließlich ist $\forall \sigma \in \Gamma$: $\sigma(\sqrt{p_1} + \dots + \sqrt{p_n}) = \gamma_1\sqrt{p_1} + \dots + \gamma_n\sqrt{p_n}$
mit $\gamma_i \in \{\pm 1\}$ $\leq \sqrt{p_1} + \dots + \sqrt{p_n}$
mit Gleichheit genau dann, wenn alle $\gamma_i = 1$ sind. Also ist $Stab_\Gamma(\sqrt{p_1} + \dots + \sqrt{p_n}) = 1$ und folglich $K = \mathbb{Q}(\sqrt{p_1} + \dots + \sqrt{p_n})$.

<u>qed</u>.

<u>Folg.</u>: $\sqrt{p_1}, \dots, \sqrt{p_n}$ sind $\mathbb{Q}$-linear unabhängig.