Erinnerung: 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

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

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

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.)

Beweis für $n = p^k$, p prim, $k \geq 1$.
Sei $\mu_{p^k} = \langle \zeta \rangle$. Dann ist $\zeta^{p^k} = 1$.
$\Rightarrow \mu_{p^{k-1}} = \langle \zeta^p \rangle$

$f(X) := \dfrac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \prod_{i \in (\mathbb{Z}/p^k\mathbb{Z})^\times} (X - \zeta^i) = \sum_{i=0}^{p-1} X^{i \cdot p^{k-1}} \in \mathbb{Z}[X]$ normiert.
$\Rightarrow f(\zeta) = 0$

$$f(Y+1) = \sum_{i=0}^{p-1} (Y+1)^{i \cdot p^{k-1}} = \underbrace{Y^{(p-1)p^{k-1}}} + \dots + \underbrace{p}$$

$$f(Y+1) = \frac{(Y+1)^{p^k} - 1}{(Y+1)^{p^{k-1}} - 1} \equiv \frac{Y^{p^k} + 1 - 1}{Y^{p^{k-1}} + 1 - 1} = Y^{p^k - p^{k-1}} \bmod (p)$$

$\Rightarrow f$ irreduzibel über $\mathbb{Q}$ nach Eisensteinkriterium für p.
$\Rightarrow \zeta$ hat Min.Pol. f über $\mathbb{Q}$
$\Rightarrow [\mathbb{Q}(\mu_{p^k})/\mathbb{Q}] = \deg(f) = |(\mathbb{Z}/p^k\mathbb{Z})^\times|$ zzl.

7.6.5 Satz: Ein regelmässiges n-Eck ist mit Zirkel und Lineal konstruierbar genau dann, wenn $|(\mathbb{Z}/n\mathbb{Z})^\times|$ eine Zweierpotenz ist.

$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\nu_i})$

Bew.: Schreibe $n = \prod_{i=1}^{r} p_i^{\nu_i}$; $\nu_i \geq 1$, p_i prim verschieden.

$\Rightarrow \quad \mu_n = \mu_{p_1^{\nu_1}} \times \dots \times \mu_{p_r^{\nu_r}}$.

n-Eck konstruierbar $\Leftrightarrow$ μ_n konstruierbar $\Leftrightarrow$ $\forall i$: $\mu_{p_i^{\nu_i}}$ konstruierbar. $\Leftrightarrow$ $\exists\, \mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_m$ mit $[K_{i+1}/K_i] = 2$ für alle i und $\mu_{p_i^{\nu_i}} \subset K_m$.

Notwendig: $[\mathbb{Q}(\mu_{p_i^{\nu_i}})/\mathbb{Q}]$ = Potenz von 2. $\Leftrightarrow$ $|(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\times|$ = Potenz von 2.

Hinreichend: Ist $|(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\times|$ eine Potenz von 2, $\Rightarrow$ $\mathrm{Gal}(\mathbb{Q}(\mu_{p_i^{\nu_i}})/\mathbb{Q})$ = 2-Gruppe.
$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_m = \mathbb{Q}(\mu_{p_i^{\nu_i}})$ enthält Kompositionsreihe $\Rightarrow$ $[K_{i+1}/K_i] = 2$. qed.

7.6.6 Bemerkung: Dies ist genau dann der Fall, wenn n ein Produkt einer Zweierpotenz mit paarweise verschiedenen Fermat-Primzahlen, d.h. Primzahlen der Form $2^{2^m}+1$, ist. Die einzigen bisher bekannten Fermat-Primzahlen sind 3, 5, 17, 257, 65537. Für $n = 7, 9, 11, 13, 19$ ist dagegen ein regelmässiges n-Eck nicht konstruierbar.

$\varphi(p^\nu) = (p-1)p^{\nu-1}$ = Potenz von 2

$\Leftrightarrow$ $p = 2$ oder $p > 2$ und $\nu = 1$ und $p-1 = 2^k$. $\Leftrightarrow$ $p = 2^k+1$.

$\forall k = lm$, $l > 1$ ungerade
$\Rightarrow X^m + 1 \mid X^k + 1$.
$\Rightarrow 2^m + 1 \mid 2^k + 1$.

$\sum_{m \geq 1} \frac{2}{\log(2^{2^m}+1)} \sim \sum_{m \geq 1} \frac{2}{2^m \cdot \log 2} \sim \frac{2}{\log 2}$

7.6.7 Satz: *(Kronecker-Weber)* Jede endliche Galoiserweiterung von $\mathbb{Q}$ mit abelscher Galoisgruppe ist einem *Kreisteilungskörper* $\mathbb{Q}(\mu_n)$ enthalten. (ohne Beweis)

7.7 Abelsche Körpererweiterungen

7.7.1 Definition: Eine Galoiserweiterung heisst *abelsch*, bzw. *zyklisch*, bzw. *auflösbar*, wenn ihre Galoisgruppe die entsprechende Eigenschaft hat.

7.7.2 Definition: Eine Erweiterung der Form $L = K(a)/K$ mit $\underset{}{\overset{b}{\overset{\shortparallel}{a^n}}} \in K$ heisst eine *einfache Radikalerweiterung.*

$\Rightarrow a = \text{"}\sqrt[n]{b}\text{"}$

7.7.3 Satz: *(Kummer-Theorie)* Sei L/K endlich und 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 vom Grad 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 $\mu_n \subset K$ sind alle $\zeta a \in L$

$\Rightarrow L = K(a)$ Zerfällungskörper von $X^n - b$. Wegen $\frac{d}{dX}(X^n - b) = n \cdot X^{n-1}$ mit $n \neq 0$ in K $\Rightarrow$ teilerfremd zu $X^n - b$.

OBdA $b \neq 0$.

$\Rightarrow$ separabel.

$\Rightarrow L/K$ galoisch.

Betrachte $\boxed{\chi : \mathrm{Gal}(L/K) \longrightarrow \mu_n,\ \gamma \mapsto \frac{\gamma(a)}{a}}$ wohldefiniert weil $\gamma(a) \in \mu_n \cdot a$.

$\forall \sigma, \gamma \in \mathrm{Gal}(L/K)$: $\frac{\sigma\gamma(a)}{a} = \frac{\sigma\left(\frac{\gamma(a)}{a} \cdot a\right)}{a} = \underbrace{\sigma\left(\frac{\gamma(a)}{a}\right)}_{\frac{\gamma(a)}{a}} \cdot \frac{\sigma(a)}{a} = \frac{\sigma(a)}{a} \cdot \frac{\gamma(a)}{a} \Rightarrow \chi$ Homom.

$\gamma \in \mathrm{Ker}(\chi) \Longleftrightarrow \frac{\gamma(a)}{a} = 1 \Longleftrightarrow \gamma(a) = a \Longleftrightarrow \gamma = \mathrm{id}$. Also ist χ injektiv.

$\Rightarrow \mathrm{Gal}(L/K) \hookrightarrow \mu_n =$ zyklisch der Ordnung n $\Rightarrow$ (b).

(b) $\Rightarrow$ (a)

$\left.\begin{array}{l} \mu_n \text{ zyklisch der Ordnung } n \\ \mathrm{Gal}(L/K) \text{ zyklisch der Ordnung Teiler von } n \end{array}\right\} \Rightarrow \exists$ inj. Homom. $\chi : \mathrm{Gal}(L/K) \hookrightarrow \mu_n$.

Suche: $a \in L^\times$ mit $\forall \gamma \in \mathrm{Gal}(L/K)$: $\chi(\gamma) = \frac{\gamma(a)}{a} \iff \gamma(a) = \chi(\gamma)\cdot a$.

Erinn.: Die $\gamma \in \mathrm{Gal}(L/K)$ sind lin. unabh. als Elemente von $\mathrm{Abb}(L, L)$.

$\Rightarrow \varphi := \sum_{\gamma} \chi(\gamma)^{-1} \cdot \gamma \neq 0$. Also existiert $c \in L$ mit $a := \varphi(c) \neq 0$.

$$\Rightarrow \forall \sigma \in \mathrm{Gal}(L/K): \underline{\sigma(a)} = \sigma\Big(\sum_{\gamma} \underbrace{\chi(\gamma)^{-1}}_{\in \mu_n} \gamma(c)\Big) = \sum_{\gamma} \chi(\gamma)^{-1} \cdot \sigma\gamma(c) =$$

$\tau = \sigma\gamma$

$\gamma = \sigma^{-1}\tau$

$$= \sum_{\tau \in \mathrm{Gal}(L/K)} \chi(\sigma^{-1}\tau)^{-1} \cdot \tau(c) = \sum_{\tau} \chi(\sigma)\cdot\chi(\tau^{-1})\,\tau(c)$$

$$= \chi(\sigma)\cdot \sum_{\tau} \chi(\tau)^{-1}\tau(c) = \underline{\chi(\sigma)\cdot a}.$$

$\Rightarrow \sigma(a^n) = \chi(\sigma)^n \cdot a^n = a^n \Rightarrow a^n \in K$.

χ injektiv, also $\sigma = \mathrm{id} \iff \chi(\sigma) = 1 \iff \sigma(a) = a. \iff \sigma \in \mathrm{Gal}(L/K(a))$

Also ist $L = K(a)$

qed

7.7.4 Beispiel: Im Fall char$(K) \neq 2, 3$ ist jede zyklische Erweiterung vom Grad 3 von K enthalten in $K(\sqrt{-3}, \sqrt[3]{b})$ für ein $b \in \cancel{K}$ und eine geeignete Wahl der Wurzeln.
$K(\sqrt{-3})$

ζ primitive 3te Einheitswurzel $\iff \zeta = \frac{-1 \pm \sqrt{-3}}{2}$.

7.7.5 Bemerkung: Da jede endliche abelsche Gruppe ein direktes Produkt von zyklischen Gruppen ist, hat jede abelsche Körpererweiterung L/K die Form $L_1 \cdots L_m$ für zyklische Erweiterungen L_i/K. Diese L_i kann man mittels Kummer-Theorie beschreiben.

7.7.6 Beispiel: Für beliebige paarweise verschiedene Primzahlen $p_1, \ldots, p_n$ ist der Körper

$$K := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) \subset \mathbb{R}.$$

endlich galoissch über $\mathbb{Q}$ mit Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}^n$. Ausserdem gilt

$\sigma(\sqrt{p_1} + \ldots + \sqrt{p_n}) = \pm\sqrt{p_1} \pm \ldots \pm \sqrt{p_n}$

$\sqrt{p_i}$ hat Min.Pol. $X^2 - p_i$ über $\mathbb{Q}$.

$$K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + \ldots + \sqrt{p_n}).$$

Bem.: Betrachte $\chi: \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \{\pm 1\}^n$, $\sigma \mapsto \left(\frac{\sigma(\sqrt{p_1})}{\sqrt{p_1}}, \ldots, \frac{\sigma(\sqrt{p_n})}{\sqrt{p_n}}\right)$.

injektiver Homo. Bild Untergruppe von $\{\pm 1\}^n$.

Wenn Bild $\neq \{\pm 1\}^n$, dann existieren $e_1, \ldots, e_n \in \{0, 1\}$ nicht alle 0 mit $\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})$:

$\prod_{i=1}^n \left(\frac{\sigma(\sqrt{p_i})}{\sqrt{p_i}}\right)^{e_i} = 1$. Setze $d := \prod_{i=1}^n p_i^{e_i} \Rightarrow \forall \sigma: \frac{\sigma(\sqrt{d})}{\sqrt{d}} = 1 \Rightarrow \sqrt{d} \in \mathbb{Q}$. $\rightsquigarrow$ Widerspruch!

qed

7.8 Auflösbare Körpererweiterungen

7.8.1 Lemma: Betrachte eine Körpererweiterung L'/K der Form $L' = LK'$ für Zwischenkörper L und K'. Ist L/K galoissch, so ist auch L'/K' galoissch und es gibt einen natürlichen injektiven Homomorphismus

$$\mathrm{Gal}(L'/K') \hookrightarrow \mathrm{Gal}(L/K),\ \gamma \mapsto \gamma|L.$$

$$\begin{tikzcd}[column sep=small] & L'=LK' \arrow[d, dash] \\ L \arrow[ur, dash] \arrow[d, dash, "\text{gal.}"'] & K' \\ K \arrow[ur, dash] & \end{tikzcd}$$

$m_{a,K}$

Beweis: $L' = K'(L)$. Jedes $a \in L$ ist separabel über K und sein MinPol über K zerfällt über L in Linearfaktoren. MinPol. von a über K' ist $m_{a,K'} \mid m_{a,K}$.
$\Rightarrow m_{a,K'}$ separabel und zerfällt über L' in Linearfaktoren $\Rightarrow L'/K'$ galoissch.
L/K normal $\Rightarrow \forall \gamma \in \mathrm{Gal}(L'/K'): \gamma(L) = L. \Rightarrow \gamma|L \in \mathrm{Gal}(L/K)$.
Homo. ✓ $\quad \gamma|K' = id.$
$\gamma \in \mathrm{Ker} \iff \gamma|L = id. \iff \gamma = id.$ Also injektiv. Qed

7.8.2 Definition: (a) Ein Körperturm $K_m/\ldots/K_0$, bei dem jedes K_i/K_{i-1} eine einfache Radikalerweiterung ist, heisst ein *Radikalturm*.

(b) Ein Polynom $f \in K[X]$ heisst *auflösbar durch Radikale*, wenn es einen Radikalturm $K_m/\ldots/K_0 = K$ gibt, so dass f über K_m in Linearfaktoren zerfällt.

Letzteres bedeutet, dass jede Nullstelle von f in einem algebraischen Abschluss von K durch eine explizite Formel in Termen der vier Grundrechenarten und Wurzeln beliebiger Ordnung, ausgehend von Elementen von K, darstellbar ist.