

4.3.9 Satz Sei $M \subset \mathbb{C}$, $\{0,1\} \subset M$, $z \in \mathbb{C}$. Äquiv:

- (i) $z \in K(M)$
- (ii) $\exists$ Körper $L_0, \dots, L_n$ mit $K := \mathbb{Q}(M \cup \bar{M}) = L_0 \subset \dots \subset L_n \subset \mathbb{C}$
mit $z \in L_n$ und $[L_i : L_{i-1}] = 2$ für $i=1, \dots, n-1$.
- (iii) $\exists$ Galois-Erweiterung $K \subset L$ mit $z \in L$ und $[L : K] = 2^k$
für ein $k \in \mathbb{N}_0$

Insbes. ist jedes $z \in K(M)$ alg. über $K = \mathbb{Q}(M \cup \bar{M})$ und
 $\exists l \in \mathbb{N}_0 : [K(z) : K] = 2^l$ (da $[K(z) : K] \mid [L : K] = 2^k$).

Beweis (i) $\Rightarrow$ (ii) Es gilt $\bar{K} = \mathbb{Q}(\overline{M \cup \bar{M}}) = \mathbb{Q}(\bar{M} \cup M) = K$.

Falls $i \notin K$, so ist $K \subset K(i)$ Körpererw. von Grad 2, also
O.B.d.A. $i \in K$. Dann $w \in K \leadsto \{\bar{w}, \frac{1}{2}(w+\bar{w}) = \operatorname{Re} w, \frac{1}{2i}(w-\bar{w}) = \operatorname{Im} w, |w|^2 = w \cdot \bar{w}\} \subset K$. Sei z mit einem elem. Schritt aus
 K gewinnbar; wir zeigen: $\exists L \supset K, [L : K] \leq 2, z \in L$.

(Dann folgt die Beh. per Induktion.)

Schnitt Typ(1): $t = p + \lambda(q-p) = r + \lambda'(s-r), \lambda, \lambda' \in \mathbb{R}$

$\leadsto (q-p)\lambda - (s-r)\lambda' = r-p \leadsto \operatorname{Re}(q-p)\lambda - \operatorname{Re}(s-r)\lambda' = \operatorname{Re}(r-p),$
 $\operatorname{Im}(q-p)\lambda - \operatorname{Re}(s-r)\lambda' = \operatorname{Im}(r-p)$. Dies ist ein Syst. mit Koeff
in K mit eindeutig bestimmte Lösung (λ, λ') . Cramer-Regel
 $\leadsto \lambda, \lambda' \in K \leadsto t \in K =: L$.

Schnitt Typ(2): u, v sind von Gestalt $r + \lambda(s-r)$, wobei

$\lambda \in \mathbb{R}$ genügt $|r + \lambda(s-r) - t|^2 = |p-q|^2 \Leftrightarrow$

$$\lambda^2 |s-r|^2 + \lambda(s-r)(\bar{r}-t) + \lambda(\overline{s-r})(r-t) + |r-t|^2 - |p-q|^2 = 0$$

Alle Koeff dieses Pol. von Grad 2 in λ sind in K

$\leadsto L := K(\lambda)$ hat Grad ≤ 2 über K , $L = \bar{L}$ und $u, v \in L$

Schnitt Typ(3) $z \in \{v, w\}$ erfüllt $|z-t|^2 = d^2, |z-u|^2 = d'^2$

d.h. $|z|^2 - 2\operatorname{Re}(tz) + |t|^2 - d^2 = 0$

$$|z|^2 - 2\operatorname{Re}(uz) + |u|^2 - d'^2 = 0$$

(83)

Insbesondere $2 \operatorname{Re}((u-t)z) + |t|^2 - d^2 - |u|^2 + d^2 = 0$

Dies ist eine Geradengleichung für z , erfüllt von u und v , beschreibt also die Gerade g durch u, v .

Die Gleichung können wir $2 \operatorname{Re}(az) + b = 0$ schreiben, mit $a, b \in K$. Dann gilt $\{-\frac{b}{2a}, -\frac{b+i}{2a}\} \in g \cap K$

und wir schließen wie in $\text{Ph}t(2)$.

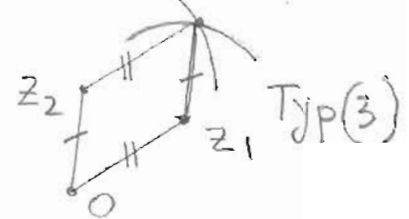
(ii) $\Rightarrow$ (i) Lemma Gilt $0, 1 \in M$, so ist $K(M)$ ein Körper der mit w stets auch $\pm \sqrt{w}$ enthält.

Ist dies gezeigt, dann: $\{0, 1\} \cup M \cup \overline{M} \subset K(M) \xrightarrow{\text{Lemma}} K \subset K(M)$

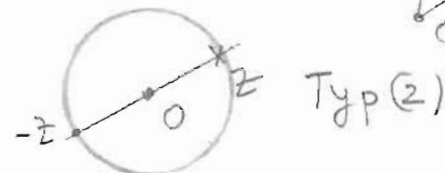
Lemma $L_1 \subset K(M) \rightsquigarrow \dots \rightsquigarrow L_n \subset K(M) \rightsquigarrow z \in K(M)$.

Beweis des Lemmas:

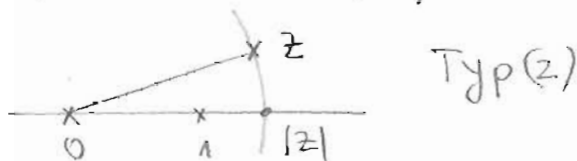
• $z_1, z_2 \in K(M) \rightsquigarrow z_1 + z_2 \in K(M)$ da



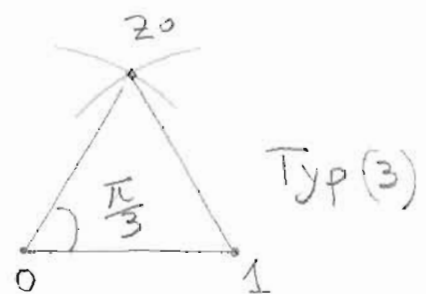
• $z \in K(M) \rightsquigarrow -z \in K(M)$



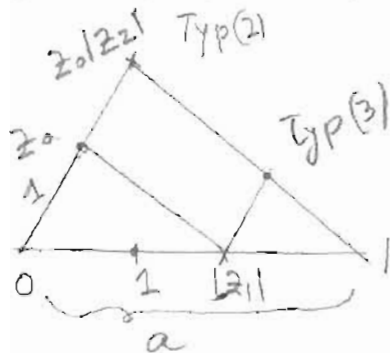
• $z \in K(M) \rightsquigarrow |z| \in K(M)$



• $z_0 = e^{\pi i/3} \in K(M)$



• $z_1, z_2 \in K(M) \rightsquigarrow |z_1 z_2| \in K(M)$



Strahlensatz:

$$\frac{a - |z_1|}{a} = \frac{|z_2| - 1}{|z_2|}$$

$$\rightsquigarrow 1 - \frac{|z_1|}{a} = 1 - \frac{1}{|z_2|}$$

$$\rightsquigarrow a = |z_1 z_2|$$

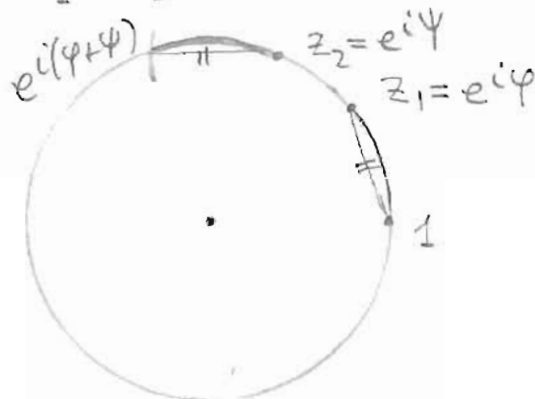
(84)

$$\bullet z \in K(M) \setminus \{0\} \leadsto |z|^{-1} \in K(M)$$

$$\bullet z \in K(M) \leadsto z^{-1} \in K(M)$$

$$\text{da } \bar{z} \in K(M), z = |z|^{-1} \cdot \bar{z} \quad (\text{Typ}(2))$$

$$\bullet z_1, z_2 \in K(M) \leadsto z_1 z_2 \in K(M). \quad \text{O.B.d.A. } |z_1| = |z_2| = 1$$



Also ist $K(M)$ ein Körper.

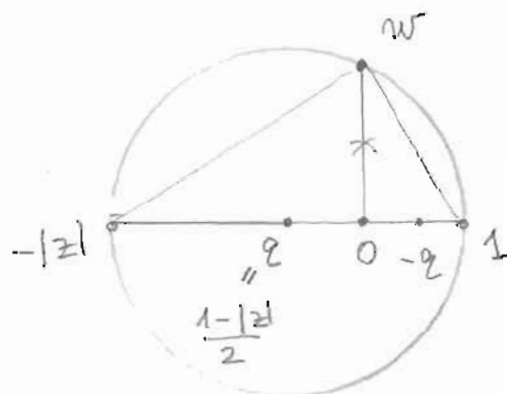
$$\bullet z \in K(M) \leadsto \pm \sqrt{z} \in K(M). \quad \text{Ist } z = |z| e^{i\varphi}, \text{ so}$$

$$\pm \sqrt{z} = \pm \sqrt{|z|} e^{i\varphi/2}. \quad \text{Winkelhalbierung ist mit Zirkel und Lineal}$$

machbar. Bleibt $\sqrt{|z|}$:

Höhensatz:

$$|w|^2 = |z| \cdot 1 \leadsto |w| = \sqrt{|z|}.$$



(ii) $\Rightarrow$ (iii) $K \subset L_n$ ist endliche Körpererw. und auch separabel
 (da $\text{char } K = 0 \leadsto \exists \alpha \in \bar{K} : L_n = K(\alpha)$). Sei $f \in K[x]$ das
 Minimalpolynom zu α (separabel) und $L(\supset L_n)$ ein Zerfällungskörper
 zu $\alpha \leadsto K \subset L$ galois, $L = K(\underbrace{\alpha = \alpha_1, \dots, \alpha_k}_{\text{Nst von } f})$

f irreduzibel $\leadsto \text{Gal}(L/K)$ op. transitiv auf $\{\alpha_1, \dots, \alpha_k\}$

Seien $\sigma_2, \dots, \sigma_k \in \text{Gal}(L/K)$ mit $\sigma_j(\alpha) = \alpha_j$.

Seien $\beta_1, \dots, \beta_n$ mit $\beta_i \in L_i \setminus L_{i-1}$, d.h. β_i von $\text{Grnd } L_i / L_{i-1}$

$$\Rightarrow K(\alpha_j) = K(\sigma_j(\beta_1), \dots, \sigma_j(\beta_n)) \text{ für alle } j$$

$$\Rightarrow L = K(\alpha_1, \dots, \alpha_k) = K(\underbrace{\beta_1, \dots, \beta_n}_{\gamma_1, \dots, \gamma_n}, \underbrace{\sigma_2(\beta_1), \dots, \sigma_2(\beta_n)}_{\gamma_{n+1}, \dots})$$

$$[K(\gamma_1, \dots, \gamma_\ell) : K(\gamma_1, \dots, \gamma_{\ell-1})] \leq 2 \leadsto [L : K] \text{ Zweierpotenz}$$

$$(iii) \Rightarrow (ii) \text{ ord Gal}(L/K) = 2^k \leadsto 2\text{-Gruppe} \xrightarrow{1.7.6} \text{auflösbar}$$

$$\leadsto \exists \text{ Normalreihe } \{e\} = N_0 \triangleleft \dots \triangleleft N_k = \text{Gal}(L/K) = \text{Gal}(L/K)$$

$$\text{mit } [N_i : N_{i-1}] = 2. \text{ Setze } L_i = [N_i] \leadsto K = L_0 \subset \dots \subset L_k = L$$

$$\text{mit } [L : L_i] = \text{ord } N_{k-i} = 2^{k-i} \leadsto [L_i : L_{i-1}] = 2. \quad \square$$

4.3.10 Korollar Sei $M = \{0, 1\}$, also $K = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$

(i) Würfeldoppelung nicht möglich: $\sqrt[3]{2}$ nicht mit Zirkel und Lineal konstruierbar

(ii) Quadratur des Kreises ist unmöglich

(iii) Ein regelmäßiges n -Eck ist genau dann mit Zuz konstruierbar, wenn $\varphi(n) = 2^l$

Beweis (i) $\sqrt[3]{2}$ ist nicht mit Zuz konstruierbar, da $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^l$

(ii) Wissen, dass π nicht algebraisch (Satz von Lindemann)
Wäre $\sqrt{\pi}$ algebraisch $\leadsto \pi \in \mathbb{Q}(\sqrt{\pi})$ algebraisch.

(iii) Sei $\zeta_n = e^{2\pi i/n}$ primitive n -te EHW. Dann gilt

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n), \text{ also } \varphi(n) = 2^l \text{ nach 4.3.9}$$

Umgekehrt, $\mathbb{Q}(\zeta_n)$ ist galois über $\mathbb{Q}$, also ζ_n ist konstruierbar nach 4.3.9(iii). $\square$

Bsp $\varphi(7) = 6, \varphi(9) = 6, \varphi(11) = 10 \leadsto 7\text{-}, 9\text{-}, 11\text{-Eck}$
nicht konstruierbar

$\varphi(5) = 4, \varphi(15) = 8, \varphi(17) = 16 \leadsto 5\text{-}, 15\text{-}, 17\text{-Eck}$
konstruierbar. $\square$