# A26: Konstruktionen mit Zirkel und Lineal

Technisches Zeichnen: früher: m.Z.u.L.
heute: CAD

Stichworte: m.Z.u.L. aus $S \subseteq \mathbb{C}$ $\rightsquigarrow$ Körpertheorie

26.2. Vereinbarung: Zeichenebene $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ identifizieren wir mit $\mathbb{C}$

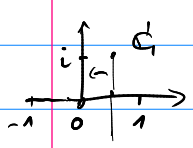
26.3. Def.: Sei $S = \{z_0, z_1, \dots, z_n\} \subseteq \mathbb{C}$, $z_0 = 0$, $z_1 = 1$.
Sei rekursiv:
$S_0 := S$, $S_{i+1} := S_i \cup \{$Menge aller Schnittpunkte von je zwei Objekten aus $M_i\}$,
wo $M_i := \{$Menge aller Geraden durch je zwei Punkte $S_i\}$ "Lineal"
$\cup$ {Menge aller Kreise mit Mittelpunkt in $S_i$ und Radius = Abstand zweier Punkte $S_i$} "Zirkel"

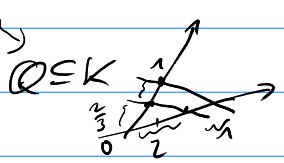
26.4. Def.: $z \in \mathbb{C}$ konstruierbar (m.Z.u.L.) aus $S :\Leftrightarrow z \in \bigcup_{i \in \mathbb{N}_0} S_i$.

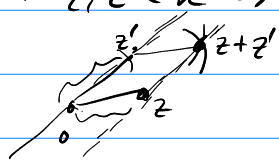
$\mathrm{Kon}(S) := \{z \in \mathbb{C};\ z$ konstr'bar aus $S\} = \bigcup_{i \in \mathbb{N}_0} S_i \subseteq \mathbb{C}$.

26.5. Lemma: $K := \mathrm{Kon}(S)$ ist ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$ mit $\sqrt{-1} = i \in K$, der abg. ist unter (komplex-) Konjugation und Quadratwurzelziehen, d.h. $z \in K \Rightarrow \bar{z}, \sqrt{z} \in K$. ⌜$\sqrt{re^{i\varphi}} := \sqrt{r}\, e^{i\varphi/2}$⌟

Bew.: $0, 1 \in K$ ✓ $\quad * \ i \in K$: ✓ $\quad * \ z, z' \in K \Rightarrow z \pm z'$, $zz' \in K$: (mal in $\mathbb{C}$)




↳ $z = re^{i\varphi}$, $z' = r'e^{i\varphi'}$

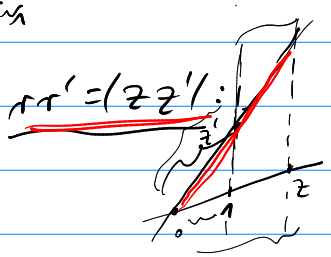
$zz' = rr' e^{i(\varphi+\varphi')}$

$* z \in K^* = K \setminus \{0\} \Rightarrow \frac{1}{z} \in K$

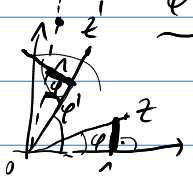
$\frac{1}{z} = |\frac{1}{z}| \cdot e^{-i\varphi}$ für $z = re^{i\varphi}$

$\frac{|zz'|}{|z'|} = \frac{|z|}{1}$

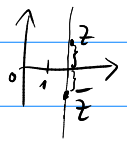
$rr' = |zz'|$:




$\varphi + \varphi'$: ✓



* $z \in K \Rightarrow \bar{z} \in K$: Spiegeln ✓,

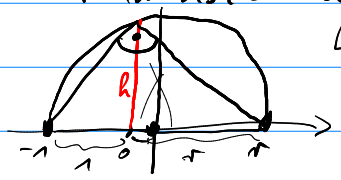



* $z \in K \Rightarrow \sqrt{z} \in K$:

$= \sqrt{r} \cdot e^{i\varphi/2}$ ↺ Winkelhalbieren

$\sqrt{r}$ mit Höhensatz: $h^2 = 1 \cdot r$

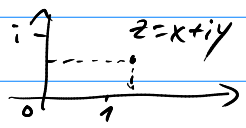
↳ $h = \sqrt{r}$ ✓




□

---

26.6. Bem.: $x+iy \in \mathbb{C} \Rightarrow x, y \in K$ ✓




26.7. Def.: Sei $M \subseteq \mathbb{C}$. Ein Quadratwurzelturm (QWT) für $M$ (über $S = \{0 = z_0, 1 = z_1, z_2, \dots, z_n\}$) ist ein Körperturm $K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_m \ (\subseteq \mathbb{C})$: $K_0 = \mathbb{Q}(z_0, \dots, z_n, \bar{z}_0, \dots, \bar{z}_n)$, $M \subseteq K_m$, $[K_j : K_{j-1}] \leq 2 \ \forall 1 \leq j \leq m$.

26.8. Satz: $z \in \mathbb{C}$ konstruierbar aus $S$ $\Leftrightarrow$ $\exists$ QWT für $\{z\} = M$ über $S$

$\Leftrightarrow$ $\exists$ QWT für $z$ über $S$

Beweis: „$\Leftarrow$": Sei $K_0 = \mathbb{Q}(z_0, \dots, \bar{z}_n) \subseteq K_1 \subseteq \dots \subseteq K_m$ und $z \in K_m$.

VI nach $j$: $K_j \subseteq K = \mathrm{Kon}(S)$.

$j = 0$: s. Lemma 26.5.

$j \to j+1$: Sei $K_{j+1} = K_j(w)$ mit $w^2 + aw + b = 0$

für $a, b \in K_j \subseteq K = \mathrm{Kon}(S)$

$\Rightarrow w = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b} \in \mathrm{Kon}(S)$ nach Lemma 26.5.

„$\Rightarrow$": VI nach $j$: $\exists$ QWT für $S_j \cup \bar{S}_j \cup \{i\}$ über $S$.

$j = 0$: ✓, denn $K_0 \subseteq K_0(i)$ ist QWT für $S_0 \cup \bar{S}_0 \cup \{i\}$.

$j \to j+1$: Sei $w = x+iy \in S_{j+1}$, etwa Schnittpunkt zweier Kreise mit Mittelpunkten $a_1 + ib_1$, $a_2 + ib_2 \in S_j$ und Radien $r_1, r_2$.

Sei $K_0 \subseteq \dots \subseteq K_m$ ein QWT für $S_j \cup \overline{S_j} \cup \{i\}$.

$$\Rightarrow \begin{cases} (x-a_1)^2 + (y-b_1)^2 = r_1^2 \\ \wedge\ (x-a_2)^2 + (y-b_2)^2 = r_2^2 \end{cases} \Rightarrow 2(a_2-a_1)x + 2(b_2-b_1)y = a_2^2 - a_1^2 + r_1^2 - r_2^2 + b_2^2 - b_1^2$$

→ aufl. nach $x$, in Glg. → $cy^2 + dy + e = 0$

$$\Rightarrow [\mathbb{Q}(a_1, a_2, b_1, b_2, r_1^2, r_2^2)(x,y) : \mathbb{Q}(a_1, a_2, b_1, b_2, r_1^2, r_2^2)] \leq 2.$$

Da $a_1, a_2, b_1, b_2, r_1^2, r_2^2 \in K_m$, folgt: $[K_m(w) : K_m] \leq 2$.

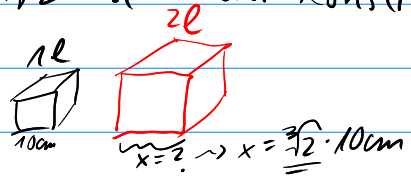
Adjungieren nun sukzessive alle El. aus $S_{j+1} \cup \overline{S_{j+1}}$, erhalten QWT für $S_{j+1} \cup \overline{S_{j+1}} \cup \{i\}$. □

26.9. Kor.: Sei $S = \{0,1\}$ wie oben, $K_0 := \mathbb{Q}(z_0, \dots, \overline{z_m})$

$z \in \mathbb{C}$ konstr'bar aus $S \Rightarrow [K_0(z) : K_0]$ ist Potenz von 2.

26.10. Anwendung: Die Würfelverdopplung (Delisches Problem) ist unmöglich:

↳ $\sqrt[3]{2}$ ist nicht konstruierbar nach 26.9, da $T^3 - 2$ irred. Eisenstein A 15.13 ($p=2$),




nach dem $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ keine Potenz von 2.

26.11. Anwendung: Die Winkeldreiteilung ist i.a. nicht möglich, [sogar fast nie mögl.!]

insb. ist $\frac{\pi}{3}$ ($\hat{=} 60°$) nicht dreiteilbar (m.z.u.L.).

Bew.: Für bel. Winkel $\alpha$ gilt $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$.

$$\text{l.S.} = \cos(3\alpha) = \cos(2\alpha + \alpha) = \cos(\alpha)\cos(2\alpha) - \sin(\alpha)\sin(2\alpha) = \dots = \text{r.S.}$$

$$\begin{cases} \cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha) = 2\cos^2(\alpha) - 1 \\ \sin(2\alpha) = 2\sin(\alpha)\cos(\alpha) \end{cases} \quad (\sin^2(\alpha) = 1 - \cos^2(\alpha))$$

D.h. $\cos(\alpha)$ ist Wurzel von $4T^3 - 3T - \cos(3\alpha)$.

Sei $\alpha = \frac{\pi}{9}$, also $\cos(3\alpha) = \cos(\frac{\pi}{3}) = \frac{1}{2}$.

Dann ist $4T^3 - 3T - \frac{1}{2} \in \mathbb{Q}[T]$ irred. / $\mathbb{Q}$,

da sonst auch $2 \cdot (4(\frac{1}{2}T)^3 - 3 \cdot (\frac{1}{2}T) - \frac{1}{2}) = T^3 - 3T - 1$ reduzibel wäre

irred.: $(T+1)^3 - 3(T+1) - 1 = T^3 + 3T^3 - 3$ ✓

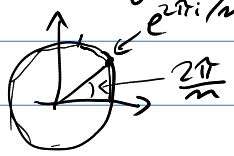
Da $3\alpha = \frac{2\pi}{3}$ Konstr'bar, wäre auch $\cos(\alpha)$ Konstr'bar, wenn Winkeldreiteilung i.a. möglich wäre.
Aber: $[\mathbb{Q}(\cos(\alpha)):\mathbb{Q}] = 3$ Keine 2er-Potenz, $\lightning$ zu Kor. 26.9. $\square$

26.12. Anwendung: Die Quadratur des Kreises ist unmöglich, d.h. $\sqrt{\pi}$ ist nicht Konstr'bar.

Bew.: Sonst wäre $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]$ nach Kor. 26.9 endlich, im $\lightning$ zu Bsp. 18.13. (Lindemann). $\square$

[$\pi$ transzendent, d.h. $\pi$ ist nicht algebraisch!]

26.13. Anwendung: Regelmäßige $n$-Eck Konstr'bar $\Leftrightarrow e^{2\pi i/n} \in Kon(S)$.

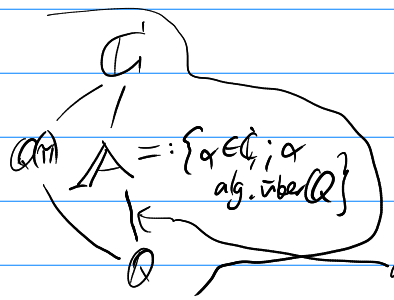



26.14. Lemma: $\zeta = e^{2\pi i/n} \in Kon(S) \Leftrightarrow [\mathbb{Q}(\zeta):\mathbb{Q}]$ Potenz von 2 [A22.16]

$[Gal(\mathbb{Q}(\zeta)|\mathbb{Q}) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ Bem.: Grad $= \varphi(n)$]

Bew.: „$\Rightarrow$": Kor. 26.9, A22.16

„$\Leftarrow$": $\mathbb{Q}(\zeta)|\mathbb{Q}$ ist galois, Galoisgruppe $G \cong UG_n(\mathbb{Z}/n\mathbb{Z})^\times$.
Da $\#G$ Potenz von 2, hat $G$ eine Normalreihe, deren Faktoren alle zykl. der Ordnung 2, vgl. A8.11(1,2).
Der zugeh. Körperturm (laut HS) ist ein QWT für $\zeta$:
$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = \mathbb{Q}(\zeta)$
Satz 26.8 $\Rightarrow \zeta \in Kon(S)$. $\square$



26.15. Bem.: Spezialfall $n = p$ prim $\Rightarrow [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$,
also $\zeta = e^{2\pi i/p} \in \mathrm{Kon}(S) \Leftrightarrow p-1$ Potenz von 2.
$S = \{0, 1\}$
$\hookrightarrow p = 2^m + 1$

26.16. Def.: Primzahlen der Form $2^{2^a} + 1$ heißen Fermatsche Primzahlen.

26.17. Bem.: $m \geq 1$ mit $2^m + 1$ prim $\Rightarrow m$ Potenz von 2, d.h. $m = 2^k$ für ein $k \in \mathbb{N}_0$.
Bew.: Sei $m = vq$ zusammengesetzt mit $v, q \in \mathbb{N}$, $q > 1$ ungerade.
Dann: $2^m + 1 = (2^v + 1) \cdot \sum_{i=0}^{q-1} (-1)^i 2^{iv}$ nicht prim
↑ Polydiv.: $y^q + 1 = (y+1) \cdot (y^{q-1} - y^{q-2} \pm \ldots + 1)$

$\lceil \frac{y^q+1}{y+1} \overset{\uparrow}{=} \frac{1-(-y)^q}{1-(-y)} \overset{\uparrow}{=} (-y)^{q-1} + (-y)^{q-2} + \ldots + 1 \rfloor$ da $2 \nmid q$
$2 \nmid q$, geom. Σ

□

26.18. Kor.: Sei $p$ prim. Dann $\zeta = e^{2\pi i/p} \in \mathrm{Kon}(S) \Leftrightarrow p$ Fermatsche Primzahl.

26.19. Satz (Gauß): Ein regelmäßiges $n$-Eck ist m.Z.u.L. konstruierbar, genau dann wenn $n$ von der Gestalt $n = 2^\ell p_1 p_2 \cdots p_r$ ist mit $\ell \in \mathbb{N}_0$, und pvv. Fermatschen Primzahlen $p_1, \ldots, p_r$.
$\lceil$ 26.14. $\rightsquigarrow [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ ist 2-er-Potenz.
$\varphi(n) = 2^a \Leftrightarrow 2^a =$
PFZ: $n = \prod_{p^{v_p} \| n} p^{v_p} \rightarrow \varphi(n) = \prod_{p^{v_p} \| n} \varphi(p^{v_p}) = \prod_{p^{v_p} \| n} p^{v_p - 1}(p-1)$
$\leftarrow p^{v_p} \| n$, $p^{v_p+1} \nmid n$

$\Leftrightarrow \forall\, p \mid n, p > 2\ \exists\, v_p \geq 1 : p - 1 = 2^{v_p}$
$\wedge\ p \| n$ ⌋

$= 2^{2^2} + 1$

26.20. Bem.: Also z.B. 17-Eck konstruierbar m.Z.u.L.
Aber 7-Eck oder 9-Eck nicht!

26.21. Bem.: Für $p = 3 = 2^{2^0}+1$, $p = 5 = 2^{2^1}+1$, $p = 17 = 2^{2^2}+1$, $p = 257 = 2^{2^3}+1$,
$p = 65537 = 2^{2^4}+1$ ergibt $n = 2^{2^k}+1$ eine PZ $p$, sr dass das zugeh. $p$-Eck Konstr'bar m. Z.-u.L. ist.
Fermat vermutete, dass alle $2^{2^n}+1$ prim.
Euler 1732 für $n=5$ widerlegt, er fand $2^{2^5}+1 = 641 \cdot 6700417$.
Offen bis heute: gibt es weitere Fermat-PZen!?
unendl. viele zus. gesetzt?
unendl. viele quadratfrei? ($n = \prod_{p \mid n} p$ quadratfrei)
Zahlreiche weitere zusammengesetzte Fermatzahlen sind bekannt.

S. v. Gauß 26.19 ist das größte reguläre $n$-Eck, $2^k n$, ist nach derzeitigem Wissenstand m. Z.-u.L. Konstr'bar, das mit

$$n = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 = 2^{32} - 1 = 4\,294\,967\,295.$$

$$\rightarrow \left[ F_1 \cdot F_2 \cdot \ldots \cdot F_m \doteq F_{m+1} - 2 \right]$$

$$F_{m+1} - 2 = 2^{2^m \cdot 2} - 1 = \left(2^{2^m}\right)^2 - 1$$

$$= \left(2^{2^m}+1\right)\left(2^{2^m}-1\right) = F_m \, (F_m - 2)$$

ENDE