Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil IV: und zurück (GALOISTHEORIE)

A26: Konstruktionen mit Zirkel und Lineal

Stichworte: Konstruierbar m. Z. u. L. aus $S \subseteq \mathbb{C}$, $\mathrm{Kon}(S)$ als Zwischenkörper von $\mathbb{C}|\mathbb{Q}$, Quadratwurzelturm, Unlösbarkeit des Würfelverdopplungsproblems / Winkeldreiteilung / Quadratur des Kreises, Konstruierbarkeit des regelmäßigen n-Ecks, Fermatsche Primzahlen

---

26.1. Einleitung: Wir widmen uns den schon in der Antike diskutierten Probleme nach der möglichen geometrischen Konstruktion bestimmter Punkte der Zeichenebene, welche wir mit $\mathbb{C}$ identifizieren. Die Konstruierbaren Punkte bilden einen Zwischenkörper von $\mathbb{C}|\mathbb{Q}$, dessen Körpergrad eine 2er-Potenz sein muss. Diese Beobachtung beantwortet einige der antiken Fragen.

26.2. Vereinbarung: In diesem Kapitel identifizieren wir die Zeichenebene $\mathbb{R}\times\mathbb{R}$ 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 $M_i\}$,

wobei $M_i := \{$Menge aller Geraden durch je zwei Punkte aus $S_i\}$
$\cup \{$Menge aller Kreise mit Mittelpunkt in S_i und Radius = Abstand zweier Punkte in $S_i\}$.

26.4. Def.: $z \in \mathbb{C}$ $\underbrace{\text{Konstruierbar (m. Z. u. L.)}}_{\text{mit Zirkel und Lineal}}$ aus S $:\Leftrightarrow z \in \bigcup_{i\in\mathbb{N}_0} S_i$.

$$\mathrm{Kon}(S) := \{z \in \mathbb{C};\ z \text{ Konstruierbar aus } S\} = \bigcup_{i\in\mathbb{N}_0} S_i.$$

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

Bew.: $0, 1 \in K$ ✓ $*$ $i \in K$: Errichten die Senkrechte auf der Geraden $(0,1)$ in 0, tragen 1 ab.
$*$ $z, z' \in K \Rightarrow z \pm z', zz' \in K$: ✓, $|zz'|$ mit Strahlensatz $\frac{|zz'|}{|z'|} = \frac{|z|}{1}$ $*$ $z \in K^* \Rightarrow \frac{1}{z} \in K$: ✓
$*$ $z \in K \Rightarrow \bar{z} \in K$: Spiegeln ✓ $*$ $z \in K \Rightarrow \sqrt{z} \in K$: Winkelhalbieren, Höhensatz $(\sqrt{r})$ ✓ $\square$

26.6. **Bem.:** $x+iy \in K \Rightarrow x, y \in K$.

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

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

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

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

$j=0$: s. Lemma 26.5.

$j \rightsquigarrow j+1$: Sei $K_{j+1} = K_j(w)$ mit $w^2 + aw + b = 0$
für $a, b \in K_j \subseteq K = \mathrm{Kon}(S)$ geeignet.

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

"$\Rightarrow$": Zeigen mit 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 $S_0 \cup \bar{S}_0 \cup \{i\}$.

$j \rightsquigarrow j+1$: 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 $S_j \cup \bar{S}_j \cup \{i\}$.

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

$\hookrightarrow cy^2 + dy + e = 0$.

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

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 Elemente 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, $K_0 := \mathbb{Q}(z_0, \dots, \bar{z}_m)$.

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

26.10. Anwendung: Die Würfelverdoppelung (Delisches Problem) ist unmöglich:
$\sqrt[3]{2}$ ist nicht konstruierbar nach 26.9, da T^3-2 irred. nach Eisenstein A15.13,
nach dem $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ keine Potenz von 2 ist.

26.11. Anwendung: Die Winkeldreiteilung ist i.a. nicht möglich,
insb. ist $\frac{\pi}{3}(\hat{=}60°)$ nicht dreiteilbar (m. Z. u. L.).

Bew.: Für beliebige Winkel α gilt $\cos(3\alpha)=4\cos^3(\alpha)-3\cos(\alpha)$, denn
$l.S.=\cos(\alpha+2\alpha)=\cos(\alpha)\cos(2\alpha)-\sin(\alpha)\sin(2\alpha)=\cos(\alpha)\cdot(2\cos^2(\alpha)-1)-2\underbrace{\sin^2(\alpha)}_{=1-\cos^2(\alpha)}\cos(\alpha)=r.S.$
D.h., dass $\cos(\alpha)$ Wurzel von $4T^3-3T-\cos(3\alpha)$ ist. Sei $\alpha=\frac{\pi}{9}$, also $\cos(\underbrace{3\alpha}_{\pi/3})=\frac{1}{2}$.
Dann ist $4T^3-3T-\frac{1}{2}\in\mathbb{Q}[T]$ irred. $|\mathbb{Q}$,
da sonst auch $2\cdot(4\cdot(\frac{1}{2}T)^3-3\cdot(\frac{1}{2}T)-\frac{1}{2})=\underbrace{T^3-3T-1}_{\text{irred., da: } (T+1)^3-3(T+1)-1=T^3+3T^2-3 \text{ irred. nach Eisenstein}}$ reduzibel wäre.
Da $3\alpha=\frac{\pi}{3}$ konstruierbar, wäre auch $\cos(\alpha)$ konstruierbar,
wenn Winkeldreiteilung möglich wäre.
Aber: $[\mathbb{Q}(\cos(\alpha)):\mathbb{Q}]=3$ keine Potenz von 2, ↯ zu Kor. 26.9. □

26.12. Anwendung: Die Quadratur des Kreises ist unmöglich, d.h. $\sqrt{\pi}$ ist nicht konstruierbar.
Bew.: Sonst wäre $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]$ nach Kor. 26.9 endlich, im ↯ zu Bsp. 18.13 (Lindemann). □

26.13. Anwendung: Reguläres n-Eck konstruierbar $\Leftrightarrow e^{\frac{2\pi i}{n}}\in Kon(S)$.
Klären im folgenden, wann dies der Fall ist.

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

Bew.: „$\Rightarrow$": s. Kor. 26.9 und A22.16.
„$\Leftarrow$": $\mathbb{Q}(\zeta)|\mathbb{Q}$ ist Galoiserw. mit Galoisgruppe G,
$G\cong UG$ von $(\mathbb{Z}/(n))^\times$.
Da $\#G$ Potenz von 2, hat G eine Normalreihe,
deren Faktoren alle zyklisch der Ordnung 2 sind, vgl. A8.11/12.
Der zugehörige Körperturm ist ein QWT für ζ:
$\mathbb{Q}=K_0\subseteq K_1\subseteq\ldots\subseteq K_m=\mathbb{Q}(\zeta)$.
Nach Satz 26.8 ist $\zeta\in Kon(S)$. □

26.15. **Bem.:** Spezialfall $n=p$ prim $\Rightarrow [\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$,

also: $\zeta = e^{\frac{2\pi i}{p}} \in Kon(S) \Leftrightarrow p-1$ Potenz von 2.

26.16. **Def.:** Primzahlen der Form $2^{2^k}+1$ 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.

Polynomdivision: $Y^q+1 = (Y+1)(Y^{q-1}-Y^{q-2}\pm \dots +1)$ □

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

26.19. **Satz (Gauß):** Ein regelmäßiges n-Eck ist m.Z.u.L. genau dann konstruierbar, wenn n von der Gestalt $n = 2^l p_1 p_2 \cdots p_r$ ist mit $l \in \mathbb{N}_0$ und pwv. Fermatschen Primzahlen $p_1, \dots, p_r$.

$\ulcorner \varphi(n) = 2^a \Leftrightarrow 2^k = \prod_{p^e \| n} p^{e-1}(p-1) \Leftrightarrow (\forall p \mid n, p>2\ \exists v_p \geq 1: p-1 = 2^{v_p} \wedge p \| n)$. ⌟

26.20. **Bem.:** Also z.B. 17-Eck konstruierbar, 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 Primzahl p, so dass das zugehörige n-Eck konstruierbar m.Z.u.L. ist.

Fermat hatte daraufhin vermutet, dass alle Zahlen der Form $2^{2^k}+1$ Primzahlen seien. Dies wurde von Euler im Jahr 1732 für $k=5$ widerlegt, indem er die Zerlegung

$$2^{2^5}+1 = 641 \cdot 6\,700\,417$$

fand.

Bislang ist nicht bekannt, ob jenseits des 65537-Ecks noch weitere reguläre p-Ecke (pPZ) existieren, die konstruierbar m.Z.u.L. sind. Aber auch nicht, ob unendlich viele der $2^{2^k}+1$ nicht prim oder wenigstens quadratfrei sind.

Zahlreiche weitere zusammengesetzte Fermatzahlen sind bekannt.

Nach dem Satz von Gauß 26.19 ist das größte reguläre n-Eck mit n ungerade, das nach derzeitigem Wissensstand m.Z.u.L. konstruierbar ist, das mit

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

$\left[F_1 \cdot F_2 \cdot \ldots \cdot F_m = F_{m+1}-2\right.$, denn $F_m := 2^{2^m}+1$ erfüllt $\underbrace{F_{m+1}-2}_{2^{2^{m+1}}-1} = \overbrace{F_m}^{2^{2^m}+1}(\overbrace{F_m-2}^{2^{2^m}-1})$. ⌟

ENDE