
19.07.2025


19.07.2025


19 . 07 . 2025

Algebraisches Kriterium für die Konstruierbarkeit

Satz (26.5)

Sei $\mathcal{P}$ eine beliebige Teilmenge mit $\mathcal{P} \supseteq \{(0,0),(1,0)\}$. Eine Zahl $a \in \mathbb{R}$ liegt genau dann in $(\mathcal{P}_{\text{con}})_{\mathbb{R}}$, wenn eine Körperkette

$$\mathbb{Q}(\mathcal{P}_{\mathbb{R}}) \quad = \quad L_0 \quad \subseteq \quad L_1 \quad \subseteq \quad \ldots \quad \subseteq \quad L_{r-1} \quad \subseteq \quad L_r$$

mit $a \in L_r$ und $[L_{j+1} : L_j] \leq 2$ für $0 \leq j < r$ existiert.

Folgerung (26.6)

Sei $\mathcal{P}$ eine beliebige Teilmenge mit $\mathcal{P} \supseteq \{(0,0),(1,0)\}$. Setzen wir $L = \mathbb{Q}(\mathcal{P}_{\mathbb{R}})$, dann ist $[L(a) : L]$ für jedes $a \in (\mathcal{P}_{\text{con}})_{\mathbb{R}}$ eine Zweierpotenz .

Die Konstruierbarkeit der regelmäßigen n-Ecke

Als regelmäßiges n-Eck bezeichnen wir das Polygon mit den Eckpunkten $P_{n,k} = (\cos(\frac{2k\pi}{n}), \sin(\frac{2k\pi}{n}))$ mit $0 \leq k < n$.

Die Zahlen der Folge $(F_n)_{n \in \mathbb{N}_0}$ gegeben durch $F_n = 2^{2^n} + 1$ sind unter dem Namen Fermat-Zahlen bekannt. Die Primzahlen unter ihnen werden als Fermatsche Primzahlen bezeichnet. Bisher sind nur fünf Fermat-Primzahlen bekannt, nämlich $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$.

Satz (26.11)

Sei $n \in \mathbb{N}$ mit $n \geq 3$. Das regelmäßige n-Eck ist genau dann aus $\mathcal{P} = \{(0,0),(1,0)\}$ mit Zirkel und Lineal konstruierbar, wenn $r, s \in \mathbb{N}_0$ und verschiedene Fermatsche Primzahlen $p_1, ..., p_s$ existieren, so dass die Gleichung $n = 2^r \cdot p_1 \cdot ... \cdot p_s$ erfüllt ist.

Vorbem.: Ist $k \in \mathbb{N}$ und $2^k + 1$ eine Primzahl, dann ist $2^k + 1$ schon eine Fermatsche Primzahl.

Ang. k ist keine Zweierpotenz $\Rightarrow \exists\, a, G \in \mathbb{N}$ mit $G > 1$ ungerade und $aG = 2^k$ $\quad$ G ungerade $\Rightarrow -1$ Nullstelle von $x^G + 1 \Rightarrow \exists\, g \in \mathbb{Z}[x]$ mit $x^G + 1 = (x+1)\,g \Rightarrow 2^{2^k} + 1 = 2^{aG} + 1 = (2^a)^G + 1 = (2^a + 1)\cdot g(2^a) \Rightarrow 2^{2^k} + 1$ ist zerlegbar in zwei Faktoren > 1 $\lightning$ zu $2^k + 1$ prim.

Beweis von Satz 26.11. Sei $n \in \mathbb{N}$, $n \geq 3$

zu zeigen: Das regelmäßige n-Eck ist konstruierbar mit Zirkel und Lineal aus $P = \{(0,0),(1,0)\}$ $\iff$ mit $r, s \in \mathbb{N}_0$, $p_1, \dots, p_s$ verschiedene Fermatsche Primzahlen

$n = 2^r \cdot p_1 \cdots p_s$

Das regelmäßige n-Eck bestehend aus den Punkten $P_{n,k} = \left(\cos\left(\frac{2\pi k}{n}\right), \sin\left(\frac{2\pi k}{n}\right)\right)$ $(0 \leq k < n)$ ist genau dann konstruierbar, wenn $\cos\left(\frac{2\pi}{n}\right)$ konstruierbar ist. „$\Rightarrow$" $P_{n,1} = \left(\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)\right)$ ist konstruierbar $\rightarrow$ $\cos\left(\frac{2\pi}{n}\right)$ ist konstruierbar reelle Zahl

„$\Leftarrow$" Für jeden Winkel α ist mit $\cos(\alpha)$ auch $\sin(\alpha) \in \{\pm\sqrt{1-\cos(\alpha)^2}\}$ konstruierbar, und auf Grund der Additionstheoreme von Sinus und

Kosinus $\left(\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)\right.$,

$\left.\sin(\alpha+\beta) = \sin(\alpha)\cos(\beta) + \sin(\beta)\cos(\alpha)\right)$

auch $\cos(k\alpha)$, $\sin(k\alpha)$ $\forall\, k \in \mathbb{Z}$. Mit

$\cos\left(\frac{2\pi}{n}\right)$ sind auch sämtliche Koordinaten

der Punkte $P_{n,k}$ konstruierbar.

außerdem bereits bekannt:

$$\left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\right] = 2 \cdot \left[\mathbb{Q}\left(\cos\left(\tfrac{2\pi}{n}\right)\right) : \mathbb{Q}\right] \quad \forall\, n \geq 3$$

d.h. $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = \frac{1}{2}\varphi(n)$

„$\Longrightarrow$" Ang., das regelmäßige n-Eck ist

konstruierbar, aber n hat nicht diese angegebene Form. Aus der Vor. folgt, dass $\cos\left(\frac{2\pi}{n}\right)$ konstruierbar ist. Notwendiges Krit. $\Rightarrow \frac{1}{2}\varphi(n)$ ist eine Zweierpotenz. Sei $n = 2^r q_1^{e_1} \cdot \ldots \cdot q_s^{e_s}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, $q_1, \ldots, q_s$ ungerade Primzahlen, $e_1, \ldots, e_s \in \mathbb{N}$. $\Rightarrow$

$\varphi(n) = \varphi(2^r) \cdot \varphi(q_1^{e_1}) \cdot \ldots \cdot \varphi(q_s^{e_s})$ Mit $\frac{1}{2}\varphi(n)$ muss auch $\varphi(n)$ eine Zweierpotenz sein. Für $1 \leq j \leq s$ gilt jeweils $\varphi(q_j^{e_j}) = q_j^{e_j - 1}(q_j - 1)$

Ang. $e_j > 1$ für ein j $\Rightarrow$ $\varphi(n)$ wird von der ungeraden Primzahl q_j geteilt $\rightarrow$ $\varphi(n)$ keine Zweierpotenz $\lightning$

also: $e_1 = \dots = e_s = 1$ Ang ein q_j ist keine Fermatsche Primzahl. $\Rightarrow q_j - 1$ ist keine Zweierpotenz. wird also von einer ungeraden Primzahl q geteilt $\Rightarrow q \mid \varphi(n)$ ↯

„$\Leftarrow$" Vor.: $n = 2^r p_1 \cdot \dots \cdot p_s$ mit $r, s \in \mathbb{N}_0$, $p_1, \dots, p_s$ Fermatsche Primzahlen. Es genügt z.Zg., dass $\cos\left(\frac{2\pi}{n}\right)$ eine konstruierbare reelle Zahl ist.

Hinreichend: Es gibt ein Körperturm

$\mathbb{Q} = L_0 \subseteq \dots \subseteq L_t$ mit $\cos\left(\frac{2\pi}{n}\right) \in L_t$

und $[L_j : L_{j-1}] = 2$ für $1 \leq j \leq t$.

$\varphi(n) = \varphi(2^r) \cdot \varphi(p_1) \cdot \dots \cdot \varphi(p_s)$

$\forall n \geq 3$

hinreichend: Es gibt ein Körperturm

p_j Fermatsche Primzahl $\Rightarrow p_j - 1$ ist Zweierpotenz

Für $1 \leq j \leq s$ $\varphi(2^r) = \begin{cases} 1 & \text{für } r \in \{0,1\} \\ 2^{r-1} & \text{für } r \geq 2 \end{cases}$ eben-

falls Zweierpotenz $\Rightarrow \varphi(n)$ ist eine Zweierpotenz

$\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ ist abelsche Gruppe

der Ordnung $\varphi(n)$ Abelsche Gruppen sind auflösbar

$\Rightarrow \exists$ Kette von Untergruppen $U_0 = \mathrm{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})$

$\supseteq \ldots \supseteq U_t$ mit $(U_{j-1} : U_j) = 2$ und $U_t = \{\mathrm{id}\}$

Hauptsatz der Galoistheorie $\Rightarrow$ erhalte eine Körperkette

$L_0 = \mathbb{Q} \subseteq \ldots \subseteq L_t$ mit $[L_j : L_{j-1}] = 2$ und

$L_t = \mathbb{Q}(\zeta_n)$ außerdem $\cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}(\zeta_n)$

wegen $\cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}\zeta + \frac{1}{2}\zeta^{-1}$ $\square$

Quadratische Reste und Nichtreste

Definition (27.1)

Sei p eine Primzahl und $a \in \mathbb{Z}$. Man nennt a einen quadratischen Rest modulo p, wenn eine Zahl $c \in \mathbb{Z}$ mit $a \equiv c^2 \bmod p$ existiert. Andernfalls spricht man von einem quadratischen Nichtrest.

Definition des Legendre-Symbols

Definition (27.2)

Sei p eine ungerade Primzahl und $a \in Z$. Das Legendre-Symbol modulo p ist definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest modulo } p \text{ und } p \nmid a \\ 0 & \text{falls } p \mid a \\ -1 & \text{falls } a \text{ quadratischer Nichtrest modulo } p. \end{cases}$$

Beweis von Lemma 27.2

geg: $a, b \in \mathbb{Z}$, p Primzahl, $p > 2$

zeige: $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right)$ falls $a \equiv b \bmod p$

1. Fall: $\left(\frac{a}{p}\right) = 1 \Rightarrow p \nmid a$. $\exists c \in \mathbb{Z}$ mit $c^2 \equiv a \bmod p$

$\Rightarrow c^2 \equiv b \bmod p$, $a \not\equiv 0 \bmod p$, $b \equiv a \bmod p \Rightarrow b \not\equiv 0 \bmod p \Rightarrow p \nmid b$ ausgesamt: $\left(\frac{b}{p}\right) = 1$

2. Fall: $\left(\frac{a}{p}\right) = 0$ 3. Fall: $\left(\frac{a}{p}\right) = -1$ analog

zeige: $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ $\forall a, b \in \mathbb{Z}$

2. Fall: $\left(\frac{a}{p}\right) = 0$ 3. Fall $\left(\frac{a}{p}\right) = -1$ analog

unmittelbar klar, falls $p \mid a$ oder $p \mid b$

Seien also $p \nmid a$ und $p \nmid b$ voraus.

1. Fall: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1 \Rightarrow \exists c, d \in \mathbb{Z}$ mit $a \equiv c^2 \bmod p$, $b \equiv d^2 \bmod p \Rightarrow ab \equiv c^2 d^2 \equiv (cd)^2 \bmod p \Rightarrow ab$ ist quadratischer Rest modulo $p \overset{p \nmid ab}{\Rightarrow} \left(\frac{ab}{p}\right) = 1 = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

2. Fall: $\left(\frac{a}{p}\right) = 1, \left(\frac{b}{p}\right) = -1$ Ang. $\left(\frac{ab}{p}\right) = 1 \Rightarrow \exists c \in \mathbb{Z}$ mit $ab \equiv c^2 \bmod p$ $\left(\frac{a}{p}\right) = 1 \Rightarrow \exists d \in \mathbb{Z}$ mit $a \equiv d^2 \bmod p$

$\Rightarrow d^2 b \equiv c^2 \bmod p$ $p \nmid a \Rightarrow p \nmid d \Rightarrow d + p\mathbb{Z}$ ist invertierbar in $\mathbb{F}_p \Rightarrow \exists u \in \mathbb{Z}$ mit $ud \equiv 1 \bmod p \Rightarrow (ud)^2 b \equiv (uc)^2 \bmod p \Rightarrow b \equiv (uc)^2 \bmod p \Rightarrow \left(\frac{b}{p}\right) \in \{0, 1\}$ ↯ also: $\left(\frac{ab}{p}\right) = -1$

3. Fall: $\left(\frac{a}{p}\right) = -1$, $\left(\frac{b}{p}\right) = 1$ analog zum 2. Fall

4. Fall: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$ z.zg.: $\left(\frac{ab}{p}\right) = 1$

Sei $c \in \mathbb{Z}$ eine Primitivwurzel modulo p
(d.h. $\mathbb{F}_p^\times = \langle c + p\mathbb{Z} \rangle$) $p \nmid a, b \Rightarrow$
$a + p\mathbb{Z}, b + p\mathbb{Z} \in \mathbb{F}_p^\times \Rightarrow \exists k, l \in \mathbb{Z}$
mit $a \equiv c^k \bmod p$, $b \equiv c^l \bmod p$
Sowohl k als auch l sind ungerade, dann:
Ang. $k = 2k'$ für ein $k' \in \mathbb{Z}$. $\Rightarrow a \equiv c^{2k'}$
$\equiv (c^{k'})^2 \bmod p \Rightarrow$ a quadratischer Rest modulo

mit $a = c^k \bmod p$, $b = c^l \bmod p$

$p \nmid a$ $\Rightarrow \left(\frac{a}{p}\right) = -1$. Also gilt $k = 2k' + 1$ für ein $k' \in \mathbb{Z}$. Zeige genauso, dass ein $l' \in \mathbb{Z}$ mit $l = 2l' + 1$ existiert $\rightarrow ab \equiv c^k \cdot c^l \equiv$

$c^{2k'+1} c^{2l'+1} = c^{2(k'+l')+2} \equiv \left(c^{k'+l'+1}\right)^2 \bmod p$

$\rightarrow ab$ ist quadr. Rest modulo $p \overset{p \nmid ab}{\Longrightarrow} \left(\frac{ab}{p}\right) = 1$

□

Elementare Rechenregeln für das Legendre-Symbol

Lemma (27.3)

Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$. Dann gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{und} \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ falls } a \equiv b \bmod p.$$

Das Eulersche Kriterium

Satz (27.4)

Sei p eine ungerade Primzahl. Dann gilt $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$.

Ergänzungssätze zum Quadratischen Reziprozitätsgesetz

Satz (27.5)

Für jede ungerade Primzahl p gilt

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}$$

und

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{falls } p \equiv 1, 7 \bmod 8 \\ -1 & \text{falls } p \equiv 3, 5 \bmod 8 \end{cases}$$

Das Quadratische Reziprozitätsgesetz

Satz (27.6)

Für zwei beliebige voneinander verschiedene ungerade Primzahlen p, q gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} =$$

$$\begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Anwendungsbeispiel:

Ist 83 ein quadratischer Rest modulo 101?

Berechne das Legendre-Symbol $\left(\frac{83}{101}\right)$.

$$\left(\frac{83}{101}\right) \overset{\text{83, 101 sind Primzahlen}}{\underset{101 \equiv 1 \bmod 4}{=}} \left(\frac{101}{83}\right) = \left(\frac{18}{83}\right)$$

↑ QRG $\Rightarrow \left(\frac{83}{101}\right)\cdot\left(\frac{101}{83}\right) = 1$

$$= \left(\frac{2}{83}\right)\cdot\left(\frac{3}{83}\right)\cdot\underbrace{\left(\frac{3}{83}\right)}_{\in \{\pm 1\}} = \left(\frac{2}{83}\right) = -1$$

↑ $83 \equiv 3 \bmod 8$

Ergebnis: 83 ist kein quadratischer Rest modulo 101

weitere Anwendung:

Für welche ungeraden Primzahlen p besitzt das Polynom $x^2 - 5x + 7$ eine Nullstelle in $\mathbb{F}_p$?

Sei $\alpha \in \mathbb{F}_p$. Dann gilt die Äquivalenz

$$\alpha^2 - \bar{5}\alpha + \bar{7} = \bar{0} \iff \alpha^2 - \bar{5}\alpha = -\bar{7} \Rightarrow$$

$$\alpha^2 - \bar{5}\alpha + (\bar{5}\bar{2}^{-1})^2 = (\bar{5}\cdot\bar{2}^{-1})^2 - \bar{7} \Rightarrow$$

$$(\alpha - \bar{5}\bar{2}^{-1})^2 = (\bar{5}\cdot\bar{2}^{-1})^2 - \bar{7}$$

also: Das Polynom hat genau dann eine Nullstelle, wenn $(\bar{5}\bar{2}^{-1})^2 - \bar{7}$ ein Quadrat in $\mathbb{F}_p$ ist. äquivalent: $\bar{5}^2 - \bar{4}\cdot\bar{7}$ ist Quadrat in $\mathbb{F}_p$

$\Leftrightarrow$ -3 ist Quadrat in $\mathbb{F}_p$

Für $p \neq 3$ ist das wiederum zu $\left(\frac{-3}{p}\right) = 1$.

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \begin{cases} \left(\frac{p}{3}\right) & \text{falls } p \equiv 1 \bmod 4 \\ -\left(\frac{p}{3}\right) & \text{falls } p \equiv 3 \bmod 4 \end{cases}$$

(QRG)

$$= \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 3 \\ -1 & \text{falls } p \equiv 2 \bmod 3 \end{cases}$$

Ergebnis: Für alle Primzahlen $p \geq 5$ hat $x^2 - 5x + 7$ genau dann eine Nullstelle in $\mathbb{F}_p$, wenn $p \equiv 1 \bmod 3$ ist.