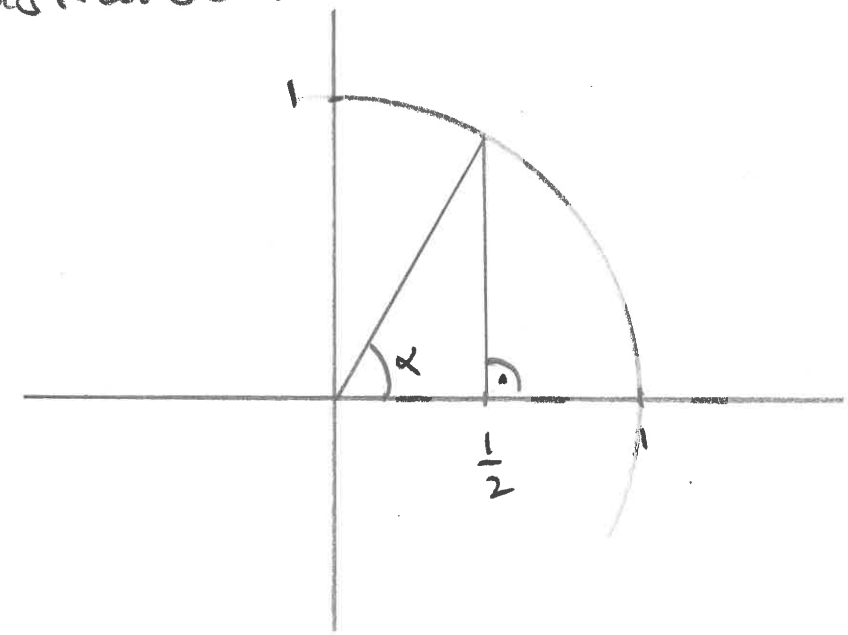
Bsp zu "unmögliche Konstruktionen mit Zirkel und Lineal".

Im allgemeinen kann man zu vorgegebenem Winkel α nicht $\frac{\alpha}{3}$ konstruieren.

Wir können zwar $\alpha = 60° = \frac{\pi}{3}$ konstruieren:



Wir können aber <u>nicht</u> $\frac{\alpha}{3} = 20° = \frac{\pi}{9}$ konstruieren.

Annahme, doch.

Dann könnten wir auch $\cos\left(\frac{\alpha}{3}\right)$

konstruieren.

Allgemein gilt für $x \in \mathbb{R}$:

$$\cos(x)^3 \overset{\text{Analysis}}{=} \left(\frac{1}{2}\left(e^{ix} + e^{-ix}\right)\right)^3$$

$$= \frac{1}{8}\left(e^{3ix} + 3e^{ix} + 3e^{-ix} + e^{-3ix}\right)$$

$$= \frac{1}{4}\cos(3x) + \frac{3}{4}\cos(x)$$

Speziell gilt

$$\cos\left(\frac{\alpha}{3}\right)^3 = \frac{1}{4}\cos(\alpha) + \frac{3}{4}\cos\left(\frac{\alpha}{3}\right).$$

Also

$$\cos\left(\frac{\alpha}{3}\right)^3 - \frac{3}{4}\cos\left(\frac{\alpha}{3}\right) - \frac{1}{8} = 0$$

Also ist $\cos\left(\frac{\alpha}{3}\right)$ eine Nullstelle

von

$$X^3 - \frac{3}{4}X - \frac{1}{8}$$

Behauptung:

Es ist $X^3 - \frac{3}{4}X - \frac{1}{8} \in \mathbb{Q}[X]$

irreduzibel,

Gzz: $\left(\frac{1}{2}X\right)^3 - \frac{3}{4}\cdot\frac{1}{2}X - \frac{1}{8}\cdot \in \mathbb{Q}[X]$

irreduzibel!

Gzz: $X^3 - 3X - 1 \in \mathbb{Q}[X]$

irreduzibel!

Aber modulo 2 ist

$X^3 - 3X - 1 = X^3 + X + 1 \in \mathbb{F}_2[X]$

irreduzibel. Dies zeigt die ...

... Behauptung, vgl. Bem 199.

Sei $c := \cos\left(\frac{\alpha}{3}\right)$.

Es ist $\mu_{c,\mathbb{Q}}(X) = X^3 - \frac{3}{4}X - \frac{1}{8}$

$\in \mathbb{Q}[X]$,

vgl. Bemerkung 184.

Also ist $[\mathbb{Q}(c) : \mathbb{Q}] = 3$,

Da aber nach Annahme c mit Zirkel und Lineal konstruierbar ist, gibt es eine Körpererweiterung $L|\mathbb{Q}$ mit $c \in L$ und mit $[L : \mathbb{Q}] = 2^n$ für ein $n \in \mathbb{Z}_{\geq 0}$; vgl. Bemerkung 204.

Somit ist $L \mid \mathbb{Q}(c) \mid \mathbb{Q}$,

und also

$$2^n = [L : \mathbb{Q}]$$

$$\overset{\text{L193}}{=} [L : \mathbb{Q}(c)] \cdot [\mathbb{Q}(c) : \mathbb{Q}]$$

$$= \underbrace{[L : \mathbb{Q}(c)]}_{\in \mathbb{Z}_{\geq 1}} \cdot 3$$

Wir haben einen Widerspruch.

Bsp zu Einheitengruppen von Körpern.

Es ist $U(\mathbb{F}_{13}) = \mathbb{F}_{13}^{\times}$

eine zyklische Gruppe: $U(\mathbb{F}_{13}) \simeq C_{12}$.

Vgl. Korollar 207.

Konkret z.B.:

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8 = -5$

$2^4 = -10 = 3$

$2^5 = 6$

$2^6 = 12 = -1$

$2^7 = -2$

$2^8 = -4$

$2^9 = 5$

$2^{10} = -3$

$2^{11} = -6$

$\Rightarrow \quad U(\mathbb{F}_{13}) = \langle 2 \rangle$

Aber z.B. $3 = 2^4$.

Also $\langle 3 \rangle = \{ 2^0, 2^4, 2^8 \}$

$= \{ 1, 3, -4 \}$

$\Rightarrow \quad U(\mathbb{F}_{13}) > \langle 3 \rangle$.

Bsp zu Einheitengruppen von Körpern.

Es war $\mathbb{F}_8 = \mathbb{F}_2(\beta)$

$= \{ a_0 + a_1\beta + a_2\beta^2 : a_0, a_1, a_2 \in \mathbb{F}_2 \}$

mit $\beta^3 = \beta + 1$, $2\beta = 0$;

vgl. Scan 16.06.20 – 8.

Es ist $U(\mathbb{F}_8) = \mathbb{F}_8^\times$

eine zyklische Gruppe:

$U(\mathbb{F}_8) \simeq C_7$. Vgl. Korollar 207.

Konkret z.B.: – – –

$\beta^0 = 1$ $\qquad$ $\beta^4 = \beta^2 + \beta$

$\beta^1 = \beta$ $\qquad$ $\beta^5 = \beta^2 + \beta + 1$

$\beta^2 = \beta^2$ $\qquad$ $\beta^6 = \beta^2 + 1$

$\beta^3 = \beta + 1$

Also $\mathcal{U}(\mathbb{F}_8) = \langle \beta \rangle$.

Aber auch:

$$\mathcal{U}(\mathbb{F}_8) = \langle \beta^2 + \beta \rangle .$$

Denn: $\beta^2 + \beta = \beta^4$

$$\Rightarrow \quad (\beta^2 + \beta)^2 = (\beta^4)^2 = \beta$$

$4 \cdot 2 \equiv_7 1$

$$\Rightarrow \quad \beta \in \langle \beta^2 + \beta \rangle \leq \mathcal{U}(\mathbb{F}_8)$$

$$\Rightarrow \mathcal{U}(\mathbb{F}_8) \overset{\text{1.0.}}{=} \langle \beta \rangle \leq \langle \beta^2 + \beta \rangle \leq \mathcal{U}(\mathbb{F}_8)$$

$\Rightarrow \ldots$

... $U(\mathbb{F}_8) = \langle \beta^2 + \beta \rangle$

Natürlich kann man dies auch durch Auflisten aller Potenzen von $\beta^2 + \beta$ bestätigen.

Bsp zu mehrfachen Faktor.

Es ist ja etwas seltsam, nun in $\mathbb{F}_2[X]$ Ableitungen wie $(X^2)' = 0$, $(X^4)' = 0$, ... zu haben.

Aber diese helfen dennoch, mehrfache Faktoren zu erkennen.

Z.B. ist $(X^4 + X^2 + 1)' = 0$

in $\mathbb{F}_2[X]$.

Also ist

$$ggT\left(X^4+X^2+1,\ (X^4+X^2+1)'\right)$$

$$= ggT\left(X^4+X^2+1,\ 0\right)$$

$$= X^4+X^2+1 \neq 1$$

Also hat X^4+X^2+1 einen irreduziblen Faktor mit Exponent ≥ 2.

Tatsächlich ist wegen Frobenius einfach

$$X^4+X^2+1 = (X^2+X+1)^2$$

in $\mathbb{F}_2[X]$.