Bsp

Sei $f(x) = X^4 - 2X^3 + X + 1 \in \mathbb{Q}[X]$.

Wir transformieren:

$$g(X) := f(X+2)$$

$$= (X+2)^4 - 2(X+2)^3 + (X+2) + 1$$

$$= X^4 + 4 \cdot 2 \cdot X^3 + 6 \cdot 2^2 \cdot X^2 + 4 \cdot 2^3 \cdot X + 2^4 \cdot 1$$

$$- 2X^3 - 2 \cdot 3 \cdot 2 \cdot X^2 - 2 \cdot 3 \cdot 2^2 \cdot X - 2 \cdot 2^3$$

$$+ X + 2$$

$$+ 1$$

$$= X^4 + \underbrace{6}_{\equiv_3 0} X^3 + \underbrace{12}_{\equiv_3 0} X^2 + \underbrace{9}_{\equiv_3 0} X + \underbrace{3}_{\equiv_3 0}$$

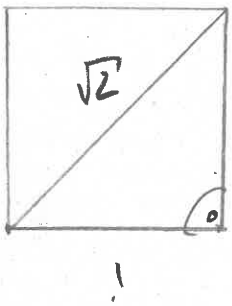
$$\not\equiv_4 0$$

Gemäß Eisenstein bei $p = 3$ ist $g(X) \in \mathbb{Q}[X]$ irreduzibel.

Also ist $f(X)$ irreduzibel.

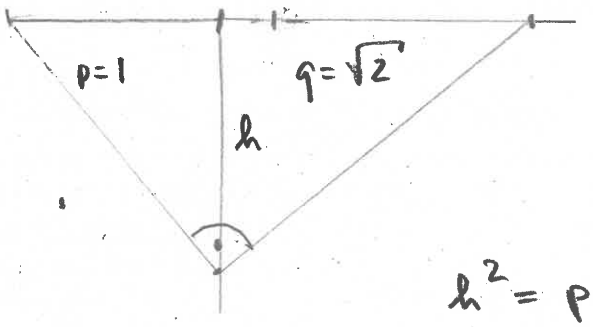
Bsp: $\sqrt[4]{2}$ konstruierbar:

1.



$\rightsquigarrow \sqrt{2}$ konstruierbar

2.



$h^2 = p \cdot q$

$\Rightarrow h = \sqrt[4]{2}$

Bsp

(1) Es gilt $\mathcal{U}(\mathbb{F}_{11}) = \mathbb{F}_{11}^{\times} \simeq C_{10}$

Zyklisch. Wir suchen die Menge aller Erzeuger der Gruppe $\mathcal{U}(\mathbb{F}_{11})$

$$E := \{ x \in \mathcal{U}(\mathbb{F}_{11}) : \langle x \rangle = \mathcal{U}(\mathbb{F}_{11}) \}.$$

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
1	2	4	-3	5	-1	-2	-4	3	-5	1

$\Rightarrow$ 2 ist Erzeuger

$\Rightarrow$ (2^k ist Erzeuger $\Leftrightarrow$ $\operatorname{ggT}(k, 10) = 1$)

$\Rightarrow$ $E = \{ 2^1, 2^3, 2^7, 2^9 \}$

$= \{ 2, -3, -4, -5 \}$

(2) Es ist $X^2+1 \in \mathbb{F}_3[X]$

mangels Nullstelle irreduzibel

$$\Rightarrow \quad \mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1)$$

ist ein Körper mit $3^2 = 9$

Elementen

Mit $\iota := X + (X^2+1)$ wird:

$$\iota^2 = -1$$

$$3 = 0$$

$$\mathbb{F}_9 = \mathbb{F}_3(\iota) = \mathbb{F}_3[\iota]$$

$$= \{a + b\iota : a, b \in \mathbb{F}_3\}$$

Es ist $\mathcal{U}(\mathbb{F}_9) = \mathbb{F}_9^\times \simeq C_8$

zyklisch.

Es gibt i keine Erzeuger der Gruppe $\mathcal{U}(\mathbb{F}_9)$:

$$\langle i \rangle = \{ i^0, i^1, i^2, i^3, i^4, \dots \}$$

$$= \{ 1, i, -1, -i \} < \mathcal{U}(\mathbb{F}_9)$$

Es gibt dagegen $i+1$ ein Erzeuger der Gruppe $\mathcal{U}(\mathbb{F}_9)$:

$$\langle i+1 \rangle = \{ (i+1)^0, (i+1)^1, (i+1)^2, (i+1)^3, (i+1)^4, \dots \}$$

$$= \{ 1, i+1, -i, -i+1, -1, -i-1, i, i-1 \}$$

$$= \mathcal{U}(\mathbb{F}_9)$$