Bsp für Irreduzibilität via Nullstellen-Test

Man kann den Nullstellentest für die Irreduzibilität von Polynomen auch über die Polynome von Grad 2 oder Grad 3 ausdehnen, wenn man noch weitere mögliche irreduzible Faktoren als mögliche Teiler mit berücksichtigt:

(1) Wir listen einmal alle normierten irreduziblen Polynome in $\mathbb{F}_3[X]$ von Grad 2 auf.

Dazu listen wir alle normierten Polynome von Grad 3 auf, ...

... die konstanten Term $\neq 0$ haben, und streichen wieder die, die in $\mathbb{F}_3$ eine Nullstelle haben:

	Nullstellen
X^2+1	—
$\cancel{X^2-1}$	$1, -1$
$\cancel{X^2+X+1}$	1
X^2+X-1	—
$\cancel{X^2-X+1}$	-1
X^2-X-1	—

$\Rightarrow$ Irreduzible normierte Polynome vom Grad 2 in $\mathbb{F}_3[X]$ sind:

$$X^2+1, \quad X^2+X-1, \quad X^2-X-1$$

(2) Wir wollen überprüfen, ob

$X^4+1 \in \mathbb{F}_3[X]$ irreduzibel

ist.

Nullstelle in $\mathbb{F}_3$ gibt es keine.

Gibt es einen irreduziblen Faktor

von Grad 2 ?

Erster Test:

$$X^4+1 = (X^2+1)\cdot(X^2-1)+2$$

$$\begin{array}{r} X^4+X^2 \\ \hline -X^2+1 \\ -X^2-1 \\ \hline 2 \end{array}$$

$\Rightarrow$ X^2+1 ist kein Teiler.

Zweiter Test:

$$X^4+1 = (X^2+X-1)\cdot(X^2-X-1)$$

$$X^4+X^3-X^2$$

$$\overline{\quad -X^3+X^2+1 \quad}$$

$$-X^3-X^2+X$$

$$\overline{\quad -X^2-X+1 \quad}$$

$\Rightarrow$ X^2+X-1 ist ein Teiler

von X^4+1

$\Rightarrow$ X^4+1 ist <u>nicht</u> irreduzibel

in $\mathbb{F}_3[X]$

(3) Wir wollen überprüfen, ob

$X^4 + X - 1 \in \mathbb{F}_3[X]$

irreduzibel ist.

Nullstelle in $\mathbb{F}_3$ liegt keine vor.

Irreduzibler Faktor von Grad 2?

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

$$\begin{array}{r}
X^4+X^2 \\
\hline
-X^2+X-1 \\
-X^2-1 \\
\hline
X
\end{array}$$

$\Rightarrow$ X^2+1 teilt nicht

- $X^4 + X - 1 = (X^2 + X - 1) \cdot (X^2 - X - 1) + X + 1$

$$\begin{array}{l}
X^4 + X^3 - X^2 \\
\hline
-X^3 + X^2 + X - 1 \\
-X^3 - X^2 + X \\
\hline
-X^2 - 1 \\
-X^2 - X + 1 \\
\hline
X + 1
\end{array}$$

$\Rightarrow X^2 + X - 1$ teilt nicht

Man hätte auch das obige Ergebnis wiederverwenden können. Aber das ist Zufall.

- $X^4 + X - 1 = (X^2 - X - 1) \cdot (X^2 + X - 1) + X + 1$

$$\begin{array}{l}
X^4 - X^3 - X^2 \\
\hline
X^3 + X^2 + X - 1 \\
X^3 - X^2 - X \\
\hline
-X^2 - X - 1 \\
-X^2 + X + 1 \\
\hline
X + 1
\end{array}$$

$\Rightarrow X^2 - X - 1$ teilt nicht

Da nun $X^4 + X - 1$ mangels Nullstelle keinen normierten irreduziblen Teiler von Grad 1 hat und dank Test auch keinen normierten irreduziblen Faktor von Grad 2 hat, ist nun $X^4 + X + 1$ irreduzibel in $\mathbb{F}_3[X]$.

<u>Bsp</u> Für die Irreduzibilität von $X^3 - 2$ in $\mathbb{Q}[X]$ haben wir bislang so argumentiert:

es ist $\sqrt[3]{2} \notin \mathbb{Q}$, also hat ...

$X^3 - 2$ keine Nullstelle in $\mathbb{Q}$. Da es von Grad 3 ist, ist es irreduzibel.

Nun können wir auch Eisenstein anwenden, für $p = 2$:

Es ist

$$X^3 - 2 = X^3 + \underbrace{0}_{\equiv_2 0} X^2 + \underbrace{0}_{\equiv_2 0} X^1 + \underbrace{(-2)}_{\substack{\equiv_2 0, \\ \not\equiv_4 0}} X^0$$

$\overset{\text{Eisenstein}}{\Longrightarrow}$ $X^3 - 2$ ist irreduzibel.

__Bsp__ Es ist $X^4 - 2X + 5$ irreduzibel in $\mathbb{Q}[X]$.

Denn in $\mathbb{F}_3[X]$ wird es zu $X^4 - 2X + 5 = X^4 + X - 1$, und wir wissen nach obigem Beispiel, daß $X^4 + X - 1$ in $\mathbb{F}_3[X]$ irreduzibel ist.

Somit ist auch $X^4 - 2X + 5$ irreduzibel in $\mathbb{Z}[X]$ und also auch in $\mathbb{Q}[X]$.

Bsp Es ist $X^4 + 9X^2 + 6$ irreduzibel in $\mathbb{Q}[X]$.

Dies folgt mit Eisenstein für $p = 3$:

$$X^4 + \underbrace{0}_{\equiv_3 0} \cdot X^3 + \underbrace{9}_{\equiv_3 0} \cdot X^2 + \underbrace{0}_{\equiv_3 0} X^1 + \underbrace{6}_{\substack{\equiv_3 0, \\ \not\equiv_9 0}} \cdot X^0$$

Also ist auch irreduzibel in $\mathbb{Q}[X]$:

$$\begin{aligned}
&(X+1)^4 + 9(X+1)^2 + 6 \\
&= X^4 + 4X^3 + 6X^2 + 4X + 1 \\
&\quad + 9X^2 + 18X + 9 + 6 \\
&= \ldots
\end{aligned}$$

$$\ldots = X^4 + 4X^3 + 15X^2 + 22X + 16$$

Das hätte man mit Eisenstein direkt nicht folgern können.

Aber natürlich kann man umgekehrt dem Polynom

$$X^4 + 4X^3 + 15X^2 + 22X + 16 \quad =: g(X)$$

diese Transformation zu

$$X^4 + 9X^2 + 6 \quad = g(X-1)$$

nicht ansehen, die letzten Endes eine Anwendung von Eisenstein möglich macht.