

von $\mathbb{K}$ Polynomdivision $\Rightarrow$

$$f = (x-2)(x+2)(x^3 - 3x + 503) (*)$$

Irreduzibilitätskriterien

Satz (Irreduzibilität und Polynomgrad)

Sei K ein Körper und $f \in K[x] \setminus K$.

(1) Ist $\text{grad}(f) = 1$, dann ist f in $K[x]$ irreduzibel.

(2) Ist $\text{grad}(f) \in \{2, 3\}$, dann gilt:

f ist irreduzibel $\iff f$ hat keine Nullstelle in K

[Für Polynome vom Grad ≥ 4 ist das falsch. Beispiel:

$(x^2+1)^2 \in \mathbb{R}[x]$ hat keine Nullstellen in $\mathbb{R}$, ist aber in $\mathbb{R}[x]$ ein reduzibles Element.]

(3) Ist $\text{grad}(f) \in \{4, 5\}$, hat f keine Nullstellen in K und keinen irreduziblen Teiler vom Grad 2, dann ist f in $K[x]$ irreduzibel.

in R reduzibel ist.

Def Sei R ein faktorieller Ring und $f \in R[x]$.

Man bezeichnet f als primitiv, wenn die Koeffizienten von f keinen gemeinsamen Primteiler haben.

Bsp: i) Normale Polynome sind primitiv.

ii) Das Polynom $f = 2x + 4 \in \mathbb{Z}[x]$ ist nicht primitiv.

Das Polynom f ist reduzibel als Element von $\mathbb{Z}[x]$ (wegen $f = 2 \cdot (x + 2)$), aber irreduzibel in $\mathbb{Q}[x]$.

Satz (Lemma von Gauß)

Sei R ein faktorieller Ring und K sein Quotientenkörper.

Sei $f \in R[x]$. i) Ist f in $R[x]$ irreduzibel, dann auch in $K[x]$.

iii) Ist f in $K[x]$ irreduzibel und primitiv, dann ist f auch in $R[x]$ irreduzibel.

Eisenstein-Kriterium

Sei R ein faktorieller Ring, $p \in R$ ein Primalelement und $f \in R[x]$ ein primitives Polynom, $f = \sum_{k=0}^n a_k x^k$. Gilt

- (i) $p \nmid a_n$ (ii) $p \mid a_k$ für $0 \leq k < n$ (iii) $p^2 \nmid a_0$
dann ist f in $R[x]$ irreduzibel.

Reduktionskriterium

Sei R ein faktorieller Ring, p ein Primalelement und $f \in R[x]$ ein primitives Polynom mit Leitkoeffizient c . Sei $\bar{R} = R/(p)$ und $\bar{f}$ das Bild von f in $\bar{R}[x]$. Ist $c \in (p)$ und $\bar{f}$ in $\bar{R}[x]$ irreduzibel, dann ist f in $R[x]$ irreduzibel.

Abb

kriter

Bsp.

$\bar{f} =$

reduzi

ist irre

H25T

$r_1 + r_2 +$

und r_3

(a) Zer

in

Seien

Achtung. Die Umkehrung des Reduktionskriteriums ist im Allgemeinen falsch.

Bsp.: $f = x^2 + 1 \in \mathbb{Z}[x]$, $p = 2$,

$\bar{f} = x^2 + 1 \in \mathbb{F}_2[x]$ Dann ist $\bar{f}$ reduzibel wg. $x^2 + 1 = (x+1)^2$, aber f ist irreduzibel in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$.

H25T1A3 Seien $a, b, c \in \mathbb{Z} \setminus \{0\}$ mit $r_1 + r_2 + r_3 \in \mathbb{Z}$, wobei $r_1 = \frac{ab}{c}$, $r_2 = \frac{bc}{a}$ und $r_3 = \frac{ac}{b}$ ist.

(a) Zeigen Sie, dass $f = (x-r_1)(x-r_2)(x-r_3)$ in $\mathbb{Z}[x]$ liegt.

Seien $a_0, a_1, a_2, a_3 \in \mathbb{Q}$ die Koeffizienten

R ein
zinitives

ist

iii) $p^2 + a_0$

d.

ein Polynom
von mit Leit-
und $\bar{f}$ das Bild
 $\bar{f}$ in $\bar{R}[x]$ irredu-
zibel.

von

dann

von

$a_2 =$

und

klar:

$r_1 + r_2$

Weiter

$= f^2$

$a_0 = -$

Aus a_0 .

von f , d.h. $f = a_3 x^3 + a_2 x^2 + a_1 x + a_0$,
dann erhält man durch Ausmultiplizieren
von (*) die Gleichungen $a_3 = 1$,

$$a_2 = -(r_1 + r_2 + r_3), \quad a_1 = r_1 r_2 + r_1 r_3 + r_2 r_3$$

$$\text{und } a_0 = -r_1 r_2 r_3.$$

klar: $a_3 \in \mathbb{Z}$. Laut Angabe liegt
 $r_1 + r_2 + r_3$ in $\mathbb{Z}$, also auch a_2 .

$$\begin{aligned} \text{Weiter gilt } a_1 &= \frac{ab}{c} \cdot \frac{bc}{a} + \frac{ab}{c} \cdot \frac{ac}{b} + \frac{bc}{a} \cdot \frac{ac}{b} \\ &= b^2 + a^2 + c^2 \in \mathbb{Z} \quad \text{und} \end{aligned}$$

$$a_0 = -\frac{ab}{c} \cdot \frac{bc}{a} \cdot \frac{ac}{b} = -abc \in \mathbb{Z}.$$

Aus $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ folgt $f \in \mathbb{Z}[x]$.

Koeffizienten

14

$$x^2 - 5/2x + 5/3$$

ist die Irreduzibilität
 $\mathbb{Q}[x]$. Da auch
 äquivalent zur
 $12x^2 - 5x + 2$ in $\mathbb{Q}[x]$
 ist primitiv, wegen
 ist die Irred von g
 Irreduzibilität von g

(b) Zeigen Sie: $r_1, r_2, r_3 \in \mathbb{Z}$

Allgemein gilt: Ist $f \in \mathbb{Z}[x]$, $f =$

$$\sum_{k=0}^n a_k x^k \text{ mit } a_n \neq 0, \text{ und ist } \alpha \in \mathbb{Q}$$

eine Nullstelle von f , $\alpha = \frac{p}{q}$ mit p, q

$\in \mathbb{Z}$, $\text{ggT}(p, q) = 1$, dann folgt $p \mid a_0$

und $q \mid a_n$. Ist f normiert, d.h. $a_n = 1$,

dann folgt insbesondere $\alpha \in \mathbb{Z}$

Das Polynom f aus der Aufgabenstellung
 ist normiert und liegt nach Teil (a) in
 $\mathbb{Z}[x]$. Jede rationale Nullstelle von f ist also
 ganzzahlig. Da $r_1, r_2, r_3 \in \mathbb{Q}$ die Nullstellen
 von f sind, folgt $r_1, r_2, r_3 \in \mathbb{Z}$. $\square$

und
einfaches
 g in $\mathbb{F}_5[x]$,

$$\bar{g}(2) \\ \bar{g}(3) \\ -4 \neq 0.$$

$$\bar{g} = -3 \neq 0$$

Wegen $\deg(\bar{g}) = 1$
reduzibel ist.

somit irreduzibel



H2ST3 A1 Übung: F13T3 A4

Zeigen Sie, dass $f = 5x^3 - 10x^2 - \frac{5}{2}x + \frac{5}{3}$
in $\mathbb{Q}[x]$ irreduzibel ist.

Da 5 in $\mathbb{Q}$ eine Einheit ist, ist die Irreduzibilität von f äquivalent zur Irreduzibilität von $\frac{1}{5}f = x^3 - 2x^2 - \frac{1}{2}x + \frac{1}{3}$ in $\mathbb{Q}[x]$. Da auch 6 in $\mathbb{Q}$ eine Einheit ist, ist dies äquivalent zur Irreduzibilität von $6 \cdot \frac{1}{5}f = 6x^3 - 12x^2 - 3x + 2$ in $\mathbb{Q}[x]$. Das Polynom $g = \frac{6}{5}f \in \mathbb{Z}[x]$ ist primitiv, wegen $\text{ggT}(6, -12, -3, 2) = 1$. Somit ist die Irred von g in $\mathbb{Q}[x]$ äquivalent zur Irreduzibilität von g in $\mathbb{Z}[x]$.

(b) Zu

Allgemein

$$\sum_{k=0}^n a_k$$

eine n
 $\in \mathbb{Z}$,

und q
dann f

Das Pol

ist norm

$\mathbb{Z}[x]$.

ganzzah

von f in

Polynoms

(ii) $\mathbb{R}$

$\mathbb{Z}[x]$

05, 5115

nach dem Eisen-
kriterium auch in $\mathbb{Q}[x]$

f in $\mathbb{R}$ eine
Nullstelle, dass f

$$\sqrt{5} = 1+1+1+1$$

Das Polynom $g \in \mathbb{Z}[x]$ ist primitiv, und
der Leitkoeffizient 6 ist kein Vielfaches
von $p=5$. Sei $\bar{g}$ das Bild von g in $\mathbb{F}_5[x]$,
d.h. $\bar{g} = x^3 - \bar{2}x^2 - \bar{3}x + \bar{2}$.

$$\begin{aligned}\bar{g}(0) &= \bar{2} \neq \bar{0}, \quad \bar{g}(1) = -\bar{2} \neq \bar{0}, \quad \bar{g}(2) \\ &= \bar{8} - \bar{8} - \bar{6} + \bar{2} = -\bar{4} \neq \bar{0}, \quad \bar{g}(3) \\ &= \bar{g}(-\bar{2}) = -\bar{8} - \bar{4} + \bar{6} + \bar{2} = -\bar{4} \neq \bar{0}, \\ \bar{g}(4) &= \bar{g}(-1) = -\bar{1} - \bar{2} + \bar{3} + \bar{2} = -\bar{3} \neq \bar{0}\end{aligned}$$

$\Rightarrow \bar{g}$ hat in $\mathbb{F}_5$ keine Nullstellen. Wegen $\deg(\bar{g}) = 3$ folgt daraus, dass $\bar{g}$ in $\mathbb{F}_5[x]$ irreduzibel ist.

Nach dem Reduktionsskizem ist g somit irreduzibel
in $\mathbb{Z}[x]$ und damit f in $\mathbb{Q}[x]$. $\square$

H25

Zeige
in $\mathbb{Q}$

Da 5
z.B. (ist
von $\frac{1}{5}$
6 in $\mathbb{Q}$
Irreduz
Das Pol
ggT(6,
in $\mathbb{Q}[x]$
in $\mathbb{Z}[x]$

Nullstelle
dass

F21T3A1 (c) (i) - (c) (iv)

Untersuchen Sie die Irreduzibilität des Polynoms

$$f = x^{2021} + 105x^3 + 15x + 45$$

Körper

über folgenden Körpern: (i) $\mathbb{Q}$ (ii) $\mathbb{R}$

besitzt

(iii) $\mathbb{F}_2$ (iv) $K = \mathbb{Q}(t)/(f(t))$

eine Null-

zu (i) Weil f als normiertes Polynom in $\mathbb{Z}[x]$

K mit

primälv ist und wegen $5 \nmid 1$, $5 \nmid 105$, $5 \nmid 15$,

von $K[t]/(f(t))$

$5 \nmid 45$ und $5^2 \nmid 45$ ($45 = 3^2 \cdot 5$) ist f nach dem Eisen-

unter dem angeg.

stein Kriterium in $\mathbb{Z}[x]$ irreduzibel, und damit auch in $\mathbb{Q}[x]$.

> 1). $\square$

zu (ii) Als Polynom ungeraden Grades hat f in $\mathbb{R}$ eine Nullstelle. Wegen $\deg(f) > 1$ folgt daraus, dass f in $\mathbb{R}$ reduzibel ist.

zu (iii) Es gilt $f(\overline{1}) = \overline{1} + \overline{105} \cdot \overline{1} + \overline{15} \cdot \overline{1} + \overline{45} = \overline{1} + \overline{1} + \overline{1} + \overline{1}$.

$= \bar{4} = \bar{0} \Rightarrow f$ hat in $\mathbb{F}_2$ eine Nullstelle.
 Wegen $\text{grad}(f) > 1$ folgt daraus, dass
 f in $\mathbb{F}_2[x]$ reduzibel ist.

zu (iv) Allgemein gilt: Ist K ein Körper
 und $f \in K[x]$ irreduzibel, dann besitzt
 f in Faktorisierung $K[t]/(f(t))$ eine Null-
 stelle, nämlich $t + (f(t))$, wobei K mit
 dem Teilkörper $\{a + f(t) \mid a \in K\}$ von $K[t]/(f(t))$
 identifiziert wird. Somit ist f über dem angeg.
 Körper reduzibel (wegen $\text{grad}(f) > 1$). $\square$

F2173

Untersuch

$$f = x^{202}$$

über $\mathbb{F}_2$

(iii) $\mathbb{F}_2$

zu (i) Wei

prüfen

5145 m

steinkates

zu (ii) Als f

Nullstelle

in $\mathbb{R}$ red

zu (iii) Es g

Übung: F20T3AS
F13T1A2

H12T3AS Zerlegen Sie das

Polynom $f = x^5 - 7x^3 + 503x^2 + 12x - 2012$
in $\mathbb{Q}[x]$ in irreduzible Faktoren.
(503 ist eine Primzahl)

Positives Einsetzen der Teiler des konstanten Terms -2012 liefert die Nullstellen ± 2 .
 $\Rightarrow (x-2)(x+2) = x^2 - 4$ ist Teiler
von f . Polynomdivision $\Rightarrow$

$$f = (x-2)(x+2)(x^3 - 3x + 503) (*)$$

= 4
wegen
 f in
zu (iv)
und f
 f in
stelle,
den Teil
identifiz
Körper

Sei $g = x^3 - 3x + 503$. Weil g ganzzahlig und normiert ist, liegt jede rationale Nullstelle von g in $\mathbb{Z}$ und ist Teiler von 503. Weil 503 Primzahl ist, sind $\pm 1, \pm 503$ die einzigen Teiler, aber:

$$g(1) = 501 \neq 0, \quad g(-1) = 505 \neq 0$$

$$g(503) = 503^3 - 3 \cdot 503 + 503 >$$

$$100^3 - 2 \cdot 503 = 10^6 - 1006 > 0$$

$$g(-503) = (-503)^3 + 3 \cdot 503 + 503$$

$< -10^6 + 2012 < 0$. Da g in $\mathbb{Q}$ keine Nullstelle hat und vom Grad 3 ist, ist g in $\mathbb{Q}[x]$ irreduzibel. Also ist (*) bereits eine Zerlegung in irred. Faktoren

