27. November 2018

Teilbarkeitslehre

Teilbarkeit

R kommutativer Ring

Definition

$a, b \in R$

$$\begin{aligned} a \mid b \quad &:\Leftrightarrow \quad a \textit{ teilt } b \\ &:\Leftrightarrow \quad \text{es gibt } q \in R : \quad b = qa \end{aligned}$$

Beispiele

- $R = \mathbb{Z}$:
  - $3 \mid 6$
  - $4 \nmid 6$
- $R = \mathit{Rationals}[X]$:
  - $X - 1 \mid X^2 - 1$
  - $X \nmid X^2 - 1$

Teilbarkeit (Forts.)

R kommutativer Ring

Proposition

$\mid$ ist Präordnung auf R

Proposition

- für $a, b, c \in R$: $a \mid b$ und $a \mid c \Rightarrow a \mid b + c$
- für $a \in R$: $a \mid 0$
- für $a, b, c \in R$: $a \mid b \Rightarrow a \mid cb$

Assoziiertheit

R kommutativer Ring

Definition

$a, b \in R$

a assoziiert zu $b :\Leftrightarrow$ es existiert $u \in R^\times$ mit $b = ua$

Beispiele

- $R = \mathbb{Z}$: 3 assoziiert zu -3
- $R = \mathbb{Q}[X]$: $X - 1$ assoziiert zu $2X - 2$

Assoziiertheit (Forts.)

Proposition

Sei R Integritätsbereich, $a, b \in R$.

Dann sind äquivalent:

- a assoziiert zu b
- $a \mid b$ und $b \mid a$

Beispiele

- im Fall $R = \mathbb{Z}$: $|a| = |b|$
- im Fall $R = K[X]$: $a = b = 0$ oder $\text{L.k.}(a)^{-1}a = \text{L.k.}(b)^{-1}b$

Ideale

R kommutativer Ring

Definition

$I \subseteq R$ heißt *Ideal* von R, falls gilt:

- $a + b \in I$ für alle $a, b \in I$
- $ra \in I$ für alle $r \in R$, $a \in I$

Beispiele

- Für $a \in R$ ist $(a) := aR := \{ar \mid r \in R\}$ ein Ideal.
  Ideale dieser Form heißen *Hauptideale*
- Für $a, b \in R$ ist $(a, b) := \{\lambda a + \mu b \mid \lambda, \mu \in R\}$ ein Ideal,
  das kleinste Ideal von R, das a und b enthält.

Ideale (Forts.)

Beispiele

- $R = \mathbb{Z}$: $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$
- $R = \mathbb{Z}$: $(2, 3) = \mathbb{Z}$
- $R = \mathbb{Z}$: $(6, 9) = (3)$
- $R = K[X]$: $XK[X] = \{f \in K[X] \mid X \text{ teilt } f\}$

Bemerkung

Sei R kommutativer Ring und $a, b \in R$

- $a \mid b \Leftrightarrow (b) \subseteq (a)$.
- Ist R Integritätsbereich, dann gilt:
  a assoziiert zu $b \Leftrightarrow (a) = (b)$.

Division mit Rest

Division mit Rest

- $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$

  Dann existieren eindeutige $q, r \in \mathbb{Z}$, $0 \leq r < |b|$ mit

  $$a = qb + r$$

- K Körper, $f \in K[X]$, $g \in K[X] \setminus \{0\}$

  Dann existieren eindeutige $q, r \in K[X]$, $\deg r < \deg g$ mit

  $$f = qg + r$$

Division mit Rest (Forts.)

$f = 2X^3 - 9X^2 + 4X, g = X^2 - 3X - 4 \in \mathbb{Q}[X]$.

Teilbarkeit und Nullstellen von Polynomen

Definition

K Körper, $f \in K[X]$

- *Nullstelle* von f: $a \in K$ mit $f(a) = 0$
- *Linearfaktor* von f: $d \in K[X]$ linear mit $d \mid f$

Proposition

K Körper, $f \in K[X]$, $a \in K$

a ist Nullstelle von $f \Leftrightarrow X - a$ ist Linearfaktor von f

Vielfachheiten von Nullstellen

Definition

K Körper, $f \in K[X] \setminus \{0\}$

$$\mathrm{m}_a(f) = \max\{k \in \mathbb{N}_0 \mid (X-a)^k \text{ teilt } f\}$$

heißt *Vielfachheit* von a als Nullstelle von f.

Beispiel

$$\mathrm{m}_a(2X^2-2) = \begin{cases} & \text{für } a \in \{\qquad\} \\ & \text{für } a \in \mathbb{Q} \setminus \{\qquad\} \end{cases}$$

Bemerkung

K Körper, $f \in K[X] \setminus \{0\}$, $a \in K$

a Nullstelle von $f \Leftrightarrow \mathrm{m}_a(f) \geq 1$

Vielfachheiten von Nullstellen (Forts.)

Sei K ein Körper, $0 \neq f \in K[X]$ und $a_1, \ldots, a_l$ paarweise verschiedene Nullstellen von f der Vielfachheiten $m_1, \ldots, m_l$.

Satz

Es existiert $0 \neq g \in K[X]$ mit $g(a_i) \neq 0$ für alle $1 \leq i \leq l$ und

$$f = (X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_l)^{m_l} g.$$

Folgerung

$\sum_{i=1}^{l} m_i \leq \deg f$.

Die Anzahl der Nullstellen von f, mit Vielfachheiten gezählt, ist kleiner oder gleich $\deg f$.

Vielfachheiten von Nullstellen (Forts.)

Sei K ein Körper, $0 \neq f \in K[X]$.

Folgerung

Äquivalent sind:

- Es existieren paarweise verschiedene Nullstellen $a_1, \ldots, a_l$ von f mit Vielfachheiten $m_1, \ldots, m_l$, so dass gilt: $\sum_{i=1}^{l} m_i = \deg f$,
- Es existieren paarweise verschiedene $a_1, \ldots, a_l \in K$, $c \in K$ und $m_1, \ldots, m_l \in \mathbb{N}$ mit

$$f = c(X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_l)^{m_l}.$$

Vielfachheiten von Nullstellen (Forts.)

Sei K ein Körper, $0 \neq f \in K[X]$.

Definition

Wir sagen: *f zerfällt (vollständig) in Linearfaktoren*, wenn eine der beiden obigen Bedingungen erfüllt ist.

Beispiele

- $X^2 - 1 \in K[X]$ zerfällt in Linearfaktoren
- $X^2 + 1 \in \mathbb{Q}[X]$ zerfällt nicht in Linearfaktoren

Der Fundamentalsatz der Algebra

Definition

Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes $0 \neq f \in K[X]$ in Linearfaktoren zerfällt.

Fundamentalsatz der Algebra

$\mathbb{C}$ ist algebraisch abgeschlossen.

Beispiel

$$\begin{aligned} X^4 - 1 &= (x^2 - 1)(X^2 + 1) \\ &= (X - 1)(X + 1)(X - i)(X + i) \end{aligned}$$

für $i \in \mathbb{C}$ mit $i^2 = -1$.