ggT und kgV

Erinnerung

R kommutativer Ring, $I \subseteq R$ Ideal in R, falls

- $I \neq \emptyset$;
- $a + b \in I$ für alle $a, b \in I$;
- $ar \in I$ für alle $a \in I$, $r \in R$.

Beispiele

- Hauptideale: $(a) = aR$ für $a \in R$
- $(a, b) = \{\lambda a + \mu b \mid a, b \in R\}$.

ggT und kgV (Forts.)

Sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K.

Satz
Ist I ein Ideal in R, dann exisitiert $a \in R$ mit $I = (a)$, d.h. I ist ein Hauptideal.

Definition
Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*.

ggT und kgV (Forts.)

Erinnerung

X geordnete Menge, $x \in X$
x heißt Maximum von X, falls $y \leq x$ für alle $y \in X$.

Erinnerung

Die Teilbarkeitsrelation ist eine Ordnung auf $\mathbb{N}$ sowie auf $\{f \in K[X] \setminus \{0\} \mid f \text{ normiert}\}$.

ggT und kgV (Forts.)

Folgerung

- Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Betrachte

$$D := \{d \in \mathbb{N} \mid d \text{ teilt } a \text{ und } d \text{ teilt } b\}.$$

Dann besitzt D bzgl. $|$ ein Maximum.
Dieses ist von der Gestalt $\lambda a + \mu b$ für geeignete $\lambda, \mu \in \mathbb{Z}$.

- Seien $f, g \in K[X]$, $g \neq 0$. Betrachte

$$D := \{d \in K[X] \mid d \text{ teilt } f, d \text{ teilt } g \text{ und } d \text{ normiert}\}.$$

Dann besitzt D bzgl. $|$ ein Maximum.
Dieses ist von der Gestalt $\lambda f + \mu g$ für geeignete $\lambda, \mu \in K[X]$.

ggT und kgV (Forts.)

Definition

Sei $R = \mathbb{Z}$ oder $R = K[X]$ und seien $a, b \in R$.

$$\mathrm{ggT}(a, b) := \max D$$

mit D wie in der Folgerung, falls $b \neq 0$, und

$$\mathrm{ggT}(a, 0) := |a|,$$

falls $b = 0$.

$\mathrm{ggT}(a, b)$ heißt der *größte gemeinsame Teiler* von a und b.

Notation

Ist $R = K[X]$ und $a \neq 0$, dann bezeichnet $|a|$ das eindeutig bestimmte normierte Polynom in der Assoziiertenklasse von a (und $|a| = 0$ für $a = 0$).

ggT und kgV (Forts.)

Bemerkung

Sei $R = \mathbb{Z}$ oder $R = K[X]$ und seien $a, b \in R$, $b \neq 0$ und

$$d \in \begin{cases} \mathbb{N}, & \text{falls } R = \mathbb{Z} \\ K[X] \setminus \{0\} \text{ normiert}, & \text{falls} R = K[X] \end{cases}$$

Dann sind äquivalent:

- $d = \mathrm{ggT}(a, b)$
- (i) $d \mid a$ und $d \mid b$;

  (ii) ist $d' \in R$ mit $d' \mid a$ und $d' \mid b$, dann ist $d' \mid d$.

ggT und kgV (Forts.)

Lemma von Bézout

Sei $R = \mathbb{Z}$ oder $R = K[X]$ und seien $a, b \in R$.

Dann existieren $\lambda, \mu \in R$ mit

$$\mathrm{ggT}(a, b) = \lambda a + \mu b.$$

ggT und kgV (Forts.)

Erinnerung: Sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K.

Satz

Ist I ein Ideal in R, dann exisitiert $a \in R$ mit $I = (a)$.

ggT und kgV (Forts.)

Folgerung

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

$$V := \{v \in \mathbb{N} \mid a \text{ teilt } v \text{ und } b \text{ teilt } v\}.$$

  Dann besitzt V bzgl. $|$ ein Miminimum.

- Seien $f, g \in K[X] \setminus \{0\}$. Betrachte

$$V := \{v \in K[X] \setminus \{0\} \mid f \text{ teilt } v, g \text{ teilt } v \text{ und } v \text{ normiert}\}.$$

  Dann besitzt V bzgl. $|$ ein Minimum.

ggT und kgV (Forts.)

Definition

Sei $R = \mathbb{Z}$ oder $R = K[X]$ und seien $a, b \in R$.

$$\mathrm{kgV}(a, b) := \min V$$

mit V wie in der Folgerung, falls $a, b \neq 0$, und

$$\mathrm{kgV}(a, b) := 0,$$

falls $a = 0$ oder $b = 0$.

$\mathrm{kgV}(a, b)$ heißt das *kleinste gemeinsame Vielfache* von a und b.

ggT und kgV (Forts.)

Bemerkung

Sei $R = \mathbb{Z}$ oder $R = K[X]$ und seien $a, b \in R$, $a, b \neq 0$ und

$$v \in \begin{cases} \mathbb{N}, & \text{falls } R = \mathbb{Z} \\ K[X] \text{ normiert}, & \text{falls } R = K[X] \end{cases}$$

Dann sind äquivalent:

- $v = \mathrm{kgV}(a, b)$
- (i) $a \mid v$ und $b \mid v$;

  (ii) ist $v' \in R$ mit $a \mid v'$ und $b \mid v'$, dann ist $v \mid v'$.

Euklidischer Algorithmus

Sei $R = \mathbb{Z}$ oder $R = K[X]$

Erinnerung

Lemma von Bézout: Für $a, b \in R$ gibt es $\lambda, \mu \in R$ mit

$$\mathrm{ggT}(a, b) = \lambda a + \mu b.$$

Ziel

Berechne $\mathrm{ggT}(a, b)$, λ, μ algorithmisch.

Lemma

Es seien $a, b \in R$.

- $\mathrm{ggT}(a, 0) = |a|$.
- Sind $q, r \in R$ mit $a = qb + r$, dann ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Euklidischer Algorithmus (Forts.)

Beispiel

In $\mathbb{Z}$: ggT$(168, 91)$

Euklidischer Algorithmus (Forts.)

Beispiel

In $\mathbb{Q}[X]$: $\mathrm{ggT}(2X^3 - 9X^2 + 4X, X^2 - 3X - 4)$.

Euklidischer Algorithmus (Forts.)

Es sei $R = \mathbb{Z}$ oder $R = K[X]$.

Erweiterter euklidischer Algorithmus

Es seien $a, b \in R$ mit $b \neq 0$.
Die folgende Prozedur liefert $d, \lambda, \mu \in R$ mit
$d = \mathrm{ggT}(a, b) = \lambda a + \mu b$.

EUKLID(a, b)
1 Bestimme q, r mit $a = qb + r$ und $\nu(r) < \nu(b)$.
2 **if** $r = 0$
3 **then return** $(|b|, 0, |b|/b)$
4 **else** $(d, \lambda, \mu) \leftarrow$ EUKLID(b, r)
5 **return** $(d, \mu, \lambda - q\mu)$