Polynomring $K[X]$, $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i$

$$f+g = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) X^i$$

$$f \cdot g = \sum_{i=0}^{n+m} c_i X^i, \quad c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

$\deg(f+g) \leq \max\{\deg f, \deg g\}$ Gleichheit, falls $\deg f \neq \deg g$

$\deg f \cdot g = \deg f + \deg g$

$K[X]$ Integritätsbereich, $K[X]^\times = K^\times$.

R komm. Ring, $a, b, c \in R$

- $a \mid b$ $:\Leftrightarrow$ es ex. $q \in R$: $b = qa$

  a teilt b b ist Vielfaches von a

- $a \mid b$ u. $a \mid c$ $\Rightarrow$ $a \mid b+c$
- $a \mid 0$
- $a \mid b$ $\Rightarrow$ $a \mid bc$
- a assoziiert zu b $:\Leftrightarrow$ es ex. $u \in R^\times$: $b = ua$

R Integritätsbereich, $a, b \in R$

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

R komm. Ring

$I \subseteq R$ heißt Ideal, falls:

- $0 \in I$
- $a+b \in I$ für alle $a, b \in I$
- $ar \in I$ für alle $a \in I, r \in R$

Beispiele: $(a) = aR = \{ar \mid r \in R\} = \{x \in R \mid a \mid x\}$

Menge aller Vielfachen von a

$(a,b) = \{\lambda a + \mu b \mid \lambda, \mu \in R\}$

- Division

Division mit Rest in $R = \mathbb{Z}$ oder $R = K[X]$

$a, b \in R$, $b \neq 0$

$\Rightarrow$ es ex. eind. best. $q, r \in R$ mit

$$a = qb + r \qquad \text{und} \qquad r = 0$$

oder $r \neq 0$ und $0 \le r < |b|$ $(R = \mathbb{Z})$, $\deg r < \deg b$ $(R = K[X])$

- $f \in K[X]$, $a \in K$
  - a Nullstelle von f $:\Leftrightarrow$ $f(a) = 0$
  - a " " f $\Leftrightarrow$ $X - a \mid f$
  - $m_a(f) := \max\{k \in \mathbb{N}_0 \mid (X-a)^k \mid f\}$

    Vielfachheit von a als Nullstelle von f

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 $m_1, \ldots, m_l$.

Ist $f = 0$, dann ist jedes $a \in K$ Nullstelle von f.

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 $a_1, \dots, a_l$ von f mit Vielfachheiten $m_1, \dots, m_l$, so dass gilt: $\sum_{i=1}^{l} m_i = \deg f$,
- Es existieren paarweise verschiedene $a_1, \dots, a_l \in K$, $c \in K$ und $m_1, \dots, m_l \in \mathbb{N}$ 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 $X^2 - 1 = (X-1)(X+1)$
- $X^2 + 1 \in \mathbb{Q}[X]$ 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 $i^2 = -1$.

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 $a \in R$ Vielfachenmengen von a.
- $(a, b) = \{\lambda a + \mu b \mid a, b \in R\}$.

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*.

<u>Beweis des Satzes</u>: <u>1. Fall</u>: $I = \{0\}$ ✓ $I = (0)$.

<u>2 Fall</u>: $I \neq \{0\}$. Wähle $a \in I$ mit

$$\left.\begin{array}{ll} |a| \text{ minimal} & (R = \mathbb{Z}) \\ \deg a \quad \text{"} & (R = K[X]) \end{array}\right\} \text{ unter allen Elementen aus } I \setminus \{0\}$$

<u>Beh</u>: $I = (a)$

<u>Bew</u>: „$\supseteq$" $(a) \subseteq I$ da I Ideal

„$\subseteq$" Sei $x \in I$ Zu zeigen: $x \in (a)$, d.h. $a \mid x$

Es ex. $q, r \in R$: $x = qa + r$ und

$$\left.\begin{array}{l} 0 \leq r < |a| \\ \deg r < \deg a \end{array}\right\} \begin{array}{l} R = \mathbb{Z} \\ R = K[X] \end{array}$$

$r = x - qa \in I$ (da $x \in I$, $qa \in I$ wegen $a \in I$)

$\Rightarrow r = 0$ wegen der Minimalität von a. ∎

ggT und kgV (Forts.)

Erinnerung

X geordnete Menge, $x \in X$

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

= größten Element

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. $\mid$ 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. $\mid$ ein Maximum.
Dieses ist von der Gestalt $\lambda f + \mu g$ für geeignete $\lambda, \mu \in K[X]$.

<u>Beweis der Folgerung</u> (für $R = \mathbb{Z}$):

Betrachte $(a,b) = \{ \lambda a + \mu b \mid \lambda, \mu \in \mathbb{Z} \}$ Ideal in $\mathbb{Z}$

Sei $d \in \mathbb{Z}$ mit $(d) = (a,b)$ (Satz) OBdA: $d \in \mathbb{N}$

$$\left.\begin{array}{l} (a) \subseteq (a,b) = (d) \Longrightarrow d \mid a \\ (b) \subseteq (a,b) = (d) \Longrightarrow d \mid b \end{array}\right\} \Longrightarrow d \in D$$

$d = \lambda a + \mu b$ für geeignete $\lambda, \mu \in \mathbb{Z}$

<u>Beh.</u>: $d = \operatorname{Max} D$.

<u>Bew.</u>: Sei $d' \in D$. Zu zeigen: $d' \mid d$

$d' \mid a$ und $d' \mid b \Longrightarrow d' \mid \underbrace{\lambda a + \mu b}_{d}$. $\blacksquare$

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:

- $d = \text{ggT}(a, b)$
- (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

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

<u>Def</u>:

a, b teilerfremd $:\Longleftrightarrow$ $\mathrm{ggT}(a,b) = 1$

<u>Bézout</u>:

a, b teilerfremd $\Rightarrow \exists\, \lambda, \mu \in R: \; 1 = \lambda a + \mu b.$

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 existiert $a \in R$ 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. $\mid$ 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. $\mid$ ein Minimum.

Beweis: Analog zum Beweis für D.
Ersetze (a, b) durch das Ideal $(a) \cap (b)$.

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 $v \mid v'$.

Es gilt: $\cancel{\mathrm{ggT}(a,b) = |ab|}$ $\mathrm{kgV}(a,b) = \dfrac{|ab|}{\mathrm{ggT}(a,b)}$

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.

Ohne Primfaktor-zerlegung.

Lemma

Es seien $a, b \in R$.

(a) ▶ $\mathrm{ggT}(a, 0) = |a|$.

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

<u>Beweis von (b)</u>: $b = 0$ $\quad \mathrm{ggT}(\cancel{a}\, r, 0) = |r| = \mathrm{ggT}(0, r)$.

$b \neq 0$ $\quad$ Für $d \in \mathbb{Z}$ gilt: $d \mid qb + r$ und $d \mid b \iff$

$d \mid r$ und $d \mid b$.

Euklidischer Algorithmus (Forts.)

Beispiel

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

$$168 = 1 \cdot 91 + 77$$
$$91 = 1 \cdot 77 + 14$$
$$77 = 5 \cdot 14 + 7$$
$$\cancel{14 = 2 \cdot 14 + 0}$$
$$14 = 2 \cdot 7 + 0$$

Rückwärts Einsetzen:

$$\begin{aligned} 7 &= 77 - 5 \cdot 14 \\ &= 77 - 5 \cdot (91 - 1 \cdot 77) \\ &= -5 \cdot 91 + 6 \cdot 77 \\ &= -5 \cdot 91 + 6 \cdot (168 - 91) \\ &= 6 \cdot 168 - 11 \cdot 91 \end{aligned}$$

$$\Rightarrow \mathrm{ggT}(168, 91) = \mathrm{ggT}(91, 77) = \mathrm{ggT}(77, 14) = \mathrm{ggT}(14, 7)$$
$$= \mathrm{ggT}(7, 0) = 7.$$

Euklidischer Algorithmus (Forts.)

Beispiel

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

$$\underbrace{2X^3 - 9X^2 + 4X}_{a} = \underbrace{(2X-3)}_{q} \cdot \underbrace{(X^2-3X-4)}_{b} + \underbrace{(3X-12)}_{r}$$

$$\begin{array}{l} X^2-3X-4 : (3X-12)\left(\frac{1}{3}X + \frac{1}{3}\right) \\ \underline{-(X^2-4X)} \\ \qquad X-4 \\ \qquad \underline{-(X-4)} \\ \qquad\quad 0 \end{array}$$

$$X^2-3X-4 = \frac{1}{3}(X+1)(3X-12)$$

$$\Rightarrow \mathrm{ggT}(a,b) = X-4$$

Rückwärts Einsetzen:

$$X - 4 = \frac{1}{3}(3X - 12) = \frac{1}{3}(a - (2X-3)b) = \frac{1}{3}a - \frac{1}{3}(2X-3)b.$$

Euklidischer Algorithmus (Forts.)

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

Erweiterter euklidischer Algorithmus

Ausgabe (d, λ, μ)

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

$$\nu(r) = \begin{cases} |r| & R = \mathbb{Z} \\ \deg r & R = K[X] \end{cases}$$

$\textsc{Euklid}(a, b)$

Bestimme q, r mit $a = qb + r$ und $\nu(r) < \nu(b)$.
if $r = 0$
  then return $(|b|, 0, |b|/b)$
  else $(d, \lambda, \mu) \leftarrow \textsc{Euklid}(b, r)$
    return $(d, \mu, \lambda - q\mu)$