

1.5.3. Korollar Jedes  $f \in k[x] \setminus \{0\}$  hat höchstens  $\deg(f)$  Nullstellen in  $k$ .

Beweis: Induktion über  $m := \deg(f)$ . Für  $m=0$  ist die Behauptung klar. Sei nun  $m \geq 1$  und sei die Aussage für Polynome vom Grad höchstens  $m-1$  bereits verifiziert.

Wir betrachten ein Polynom von Grad  $m$ . Im Fall, dass  $f$  keine Nullstellen in  $k$  hat, ist nichts zu zeigen. Wenn  $f$  eine Nullstelle  $a \in k$  hat, dann teilen wir  $f$  mit Rest durch  $x-a$  und erhalten die Darstellung  $f = q \cdot (x-a) + r$  mit  $q \in k[x]$  und  $r \in k$  (denn  $r$  ist ein Polynom vom Grad  $< \deg(x-a) = 1$ ). Wenn wir  $x=a$  einsetzen, erhalten wir  $0 = f(a) = q(a) \cdot (a-a) + r = r$ . Es folgt:  $f = q \cdot (x-a)$  mit  $\deg(q) = \deg(f)-1 = m-1$ . Die Anwendung der Induktionsvoraussetzung für  $q$  ergibt die Behauptung.  $\square$

1.5.4. Korollar. Jedes Ideal  $I \subseteq k[x]$  hat die Form  $I = \langle g \rangle$  mit  $g \in k[x]$ . Das heißt: jedes Ideal in  $k[x]$  kann durch ein Polynom erzeugt werden.

Beweis: Wir nehmen an,  $I \neq \{0\}$ , dann für  $I = \{0\}$  gilt  $I = \langle 0 \rangle$ . Sei  $g$  Polynom aus  $I \setminus \{0\}$  mit dem kleinsten Grad. Wir behaupten  $\langle g \rangle = I$ . Die Inklusion  $\langle g \rangle \subseteq I$  ist klar. Wir zeigen  $I \subseteq \langle g \rangle$ . Sei  $f \in I$  beliebig. Wir teilen  $f$  durch  $g$  mit Rest und erhalten die Darstellung  $f = q \cdot g + r$  mit  $q, r \in k[x]$  und  $\deg(r) < \deg(g)$ . Man hat

$$r = f - q \cdot g \in I \text{ und } \deg(r) < \deg(g).$$

$$\begin{array}{c} \overbrace{\quad}^{\in I} \\ I \end{array} \quad \begin{array}{c} \overbrace{\quad}^{\in I} \\ \underbrace{\quad}_{\in I} \end{array}$$

Aus der Wahl von  $g$  folgt, dass  $r=0$  ist. Also ist  $f = q \cdot g$  für ein  $q \in k[x]$ , das heißt  $f \in \langle g \rangle$ . Wir haben  $I \subseteq \langle g \rangle$  gezeigt.  $\square$

Ein Ideal, das durch ein Polynom erzeugbar ist, nennt man Hauptideal. Ein Ring, in dem alle Ideale

Hauptideale sind, inennt man Hauptidealring.

$\mathbb{Z}$  ist auch ein Hauptidealring, alle Ideale von  $\mathbb{Z}$  haben die Form  $m\mathbb{Z} := \{mz : z \in \mathbb{Z}\}$  mit  $m \in \mathbb{Z}$ .

Eine natürliche Aufgabe: man kriegt  $I = \langle f_1, \dots, f_s \rangle$  und will ein  $g$  mit  $I = \langle g \rangle$  ausrechnen.

1.5.5. Def Ein größter gemeinsamer Teiler von Polynomen  $f, g \in k[x]$  ist ein Polynom  $h \in k[x]$  mit den Eigenschaften:

- (i)  $h$  teilt  $f$  und  $g$
- (ii) jeder  $p \in k[x]$ , dass  $f$  und  $g$  teilt, teilt auch  $h$ .  
Für  $h$  wie oben schreiben wir  $h = \text{ggT}(f, g)$ .

Diese Schreibweise ist eine leichte Vernachlässigung der Bezeichnungen, z.B.  $x^2 = \text{ggT}(x^5 + x^2, x^2)$  aber auch  $2x^2 = \text{ggT}(x^5 + x^2, x^2)$  in  $\mathbb{Q}[x]$ .

1.5.6 Prop. Sei  $f, g \in k[x]$ . Dann gilt:

- (i)  $\text{ggT}(f, g)$  existiert und ist eindeutig bis auf Multiplikation mit einer Konstante aus  $k^\times$  bestimmt.

(ii)  $\langle f, g \rangle = \langle \text{ggT}(f, g) \rangle$ .

Beweis: Es gilt:  $\text{ggT}(f, g) = 0 \Rightarrow f = g = 0$ .

In dem trivialen Fall  $f = g = 0$  gilt (i) sowie (ii).

Wir können also annehmen, dass mindestens eines der Polynome  $f, g$  ungleich 0 ist.

Wir fixieren ein Polynom  $h \in k[x] \setminus \{0\}$  mit dem kleinsten Grad in  $\langle f, g \rangle \setminus \{0\}$ . Aus dem Beweis von Korollar 1.5.4 folgt  $\langle h \rangle = \langle f, g \rangle$ .

Wir behaupten  $h = \text{ggT}(f, g)$ .

Denn wegen

$$\langle f, g \rangle \subseteq \langle h \rangle$$

gilt  $f, g \in \langle h \rangle$

$\Rightarrow h$  teilt  $f$  sowie  $g$ .

$$\rightarrow \langle h \rangle = \{A \cdot h : A \in k[x]\}$$

$$\rightarrow \langle f, g \rangle = \{Cf + Dg : C, D \in k[x]\}$$

$\rightarrow h$  ist Teiler von  $f$  heißt

Wir zeigen, dass es ein  
größter gemeinsamer Teiler  
ist. Sei  $p \in k[x]$  ein

$A \cdot h = f$  gilt nur  
für ein  $A \in k[x]$

beliebiges Polynom, dass  $f$  und  $g$  teilt, d.h.,  
 $C \cdot p = f$  und  $D \cdot p = g$  für gewisse  $C, D \in k[x]$ .

Wegen  $\langle h \rangle \subseteq \langle f, g \rangle$  gilt  $h \in \langle f, g \rangle$   
und somit  $h = A \cdot f + B \cdot g$  für gewisse  
 $A, B \in k[x]$ .  $\Rightarrow$

$$h = A \cdot f + B \cdot g = A \cdot C \cdot p + B \cdot D \cdot p \\ = (A \cdot C + B \cdot D) \cdot p \Rightarrow$$

$p$  teilt  $h$ . D.h. jeder Teiler von  $f$  und  $g$   
teilt  $h$ . D.h.  $h = \text{ggT}(f, g)$ .

Es bleibt die Eindeutigkeit bis auf eine  
Konstante zu zeigen.

Sei  $H$  ein beliebiger größter gem. Teiler von  
 $f$  und  $g$ . Da  $h$  ein Teiler von  $f$  und  $g$  ist  
und  $H$  ein größter gem. Teiler von  $f$  und  $g$   
gilt  $h = q \cdot H$  für ein  $q \in k[x]$ .

Da  $H \in \langle f, g \rangle$  gilt nach der Wahl von  
 $h$  die Ungleichungen  $\deg h \leq \deg H$ .

Aus  $h = q \cdot H$ ,  $\deg h \leq \deg H$ ,  $h \neq 0$

folgt  $q \in k[x] \setminus \{0\}$ .  $\square$

Bemerkung: Es gibt einen Algorithmus, der den  
 $\text{ggT}(f, g)$  ausrechnet.

Ist  $g = 0$ , so gilt  $\text{ggT}(f, 0) = f$

Ist  $g \neq 0$ , so kann man  $f$  durch  $g$  mit  
Rest teilen: man erhält die Darstellung

$$f = q \cdot g + r \quad \text{mit } q, r \in k[x]$$

... - - - - -

$\deg r < \deg g$

$$\begin{aligned} \text{Es gilt: } \text{ggT}(f, g) &= \text{ggT}(q \cdot g + r, g) \\ &= \text{ggT}(g, r) \quad \leftarrow \end{aligned}$$

Denn: angenommen  $h$  teilt  $g$  und  $r$ . Dann  
teilt  $h$  auch  $q \cdot g + r$ . Umgekehrt:

wenn  $h \in k[x]$   $q \cdot g + r$  und  $g$  teilt  
dann teilt  $h$  die Polynome  $g$  und

$$r := \underbrace{(q \cdot g + r)}_{\substack{\text{---} \\ \text{---}}} - \underbrace{q \cdot g}_{\substack{\text{---} \\ \text{---}}}$$

Wir haben  $\text{ggT}(f, g)$  durch  $\text{ggT}(g, r)$   
ausgetauscht, wobei  $\deg(r) < \deg(g)$  ist.

Endlich viele Reduktionen wie diese führen  
zum Fall  $\text{ggT}(f, 0) = f$ .

Auf diesen Überlegungen basiert der folgende Algorithmus:

Greatest-Common-Divisor( $f, g$ ):

Annahme:  $f, g \in k[x]$

Ergbnis: Rückgabe von  $\text{ggT}(f, g)$ .

1:  $\triangleright$  Invariante:  $\text{ggT}(f, g)$  bleibt unverändert

2: while  $g \neq 0$ :

3:      $q, r := \text{Univariate-Division}(f, g)$

4:      $f := g$

5:      $g := r$

6:      $\triangleright \deg(g)$  ist gesunken

7: end

8: return  $f$

Dieser Algorithmus heißt der Euklidische Algorithmus.

1.5.7. Korr. Ein größter gemeinsamer Teiler von  $f_1, \dots, f_s \in k[x]$  ist ein Polynom  $h \in k[x]$  mit den Eigenschaften:

- (i)  $h$  teilt die Polynome  $f_1, \dots, f_s$
- (ii) Jedes Polynom, das  $f_1, \dots, f_s$  teilt, teilt auch  $h$ .

Wir schreiben in diesem Fall  $h = \text{ggT}(f_1, \dots, f_s)$ .

1.5.8 Prop. Seien  $f_1, \dots, f_s \in k[x]$  ( $s \geq 2$ ). Dann gilt:

(i)  $\text{ggT}(f_1, \dots, f_s)$  existiert und ist eindeutig bis auf Multiplikation mit einer Konstante aus  $k$  (höchstens).

$$(ii) \langle f_1, \dots, f_s \rangle = \langle \text{ggT}(f_1, \dots, f_s) \rangle$$

(iii) Für  $s \geq 3$  gilt

$$\text{ggT}(f_1, \dots, f_s) = \text{ggT}(f_1, \text{ggT}(f_2, \dots, f_s)).$$

(iv) Es gibt einen Algorithmus zur Berechnung von  $\text{ggT}(f_1, \dots, f_s)$ .

Beweis: (i) und (ii) wird ähnlich wie im Fall  $s=2$  bewiesen (Aufgabe).

Wir zeigen (iii).

Sei  $h = \text{ggT}(f_1, \dots, f_s)$ . Aus (ii) folgt

$$\langle f_1, h \rangle = \langle f_1, f_2, \dots, f_s \rangle$$

Wir wissen aber, dass  $\langle f_1, h \rangle = \langle \text{ggT}(f_1, h) \rangle$  gilt. Aus (ii) folgt also wegen

$$\begin{aligned} \langle f_1, \dots, f_s \rangle &= \langle \text{ggT}(f_1, h) \rangle \\ &\subset \langle \text{ggT}(f_1, \dots, f_s) \rangle \end{aligned}$$

$$\begin{aligned} \Rightarrow \text{ggT}(f_1, \dots, f_s) &= \text{ggT}(f_1, h) \\ &= \text{ggT}(f_1, \text{ggT}(f_2, \dots, f_s)). \end{aligned}$$

(iv): Wir können  $i = s$  und  $g_g := f_s$  setzen und die Polynome  $g_s, \dots, g_1$  rekursiv durch

$$g_{i-1} := \text{ggT}(f_{i-1}, g_i) \text{ für } i > 1.$$

Daraus ergibt sich:  $g_i := \text{ggT}(f_i, \dots, f_s)$  für alle  $i = 1, \dots, s$ . Man kann es durch die Rückwärtsinduktion nach  $i$  mit dem Induktionsbeginn  $i = s$  mit der Verwendung von (iii) zeigen.

Das lässt sich als Algorithmus folgendermaßen umsetzen:

Greatest-Common-Divisor-for-List( $f_1, \dots, f_s$ )

Annahme:  $f_1, \dots, f_s \in k[x]$

Ergebnis: Rückgabe von  $\text{ggT}(f_1, \dots, f_s)$

```

1: i := s
2: g := f_s
3: ▷ Invariante:  $g = \text{ggT}(f_i, \dots, f_s)$ 
4: while i > 1:
5:   g := ggT(f_{i-1}, g)
6:   i := i - 1
7: end
8: return g

```

Ideal Membership Problem war:

gegeben Polynome  $f, f_1, \dots, f_s$ .

Zu entscheiden:  $f \in \langle f_1, \dots, f_s \rangle$  ?

Dieses Problem können wir im univariaten Fall lösen.

1.S.9 Korollar. Es gibt einen Algorithmus, der für gegebene  $f, f_1, \dots, f_s \in k[x]$  feststellt, ob  $f \in \langle f_1, \dots, f_s \rangle$  gilt.

Beweis: Wir berechnen  $g = \text{ggT}(f_1, \dots, f_s)$

Dann gilt:  $\langle a \rangle = \langle 1, \dots, 1 \rangle$

Zum Testen von  $f \in \langle g \rangle$  wird  $f$  durch  $g$  mit Rest dividiert (im Fall  $g = 0$  gilt  $f \in \langle g \rangle$  genau dann, wenn  $f = 0$  ist, wir setzen also  $g \neq 0$  voraus).  
Wir erhalten die Darstellung

$$f = q \cdot g + r \text{ mit } q, r \in k[x]$$

und  $\deg(r) < \deg(g)$ .

Ist  $r = 0$ , so gilt  $f = q \cdot g \in \langle g \rangle$ .

Ist  $r \neq 0$ , so gilt  $f \notin \langle g \rangle$ :  
wäre  $f \in \langle g \rangle$ , so hätte man

$$0 \neq r = f - q \cdot g \in I$$

$\begin{smallmatrix} f \\ q \\ g \end{smallmatrix}$

Aber Nicht-mullelemente des Ideals  $\langle g \rangle$   
haben die Form  $h \cdot g$  mit  $h \in k[x]$  los  
und  $\deg(h \cdot g) \geq \deg(g)$ ,  $\Leftrightarrow$   
 $\Rightarrow \deg(r) < \deg(g)$ ,  $r \neq 0$ .  $\square$

### 1.5. 10. Aufgaben.

- ① Man teile  $x^3 + 2x^2 + x + 1$  durch  $2x + 1$   
mit Rest.
- ② Man bestimme  $\text{ggT}(x^4 - 1, x^6 - 1)$ .
- ③ Zeigen Sie, dass jedes Polynom  
 $f \in \mathbb{C}[x]$  vom Grade  $n \geq 1$  eine  
Darstellung  $f = c(x - r_1) \cdots (x - r_n)$   
mit  $c \in \mathbb{C} \setminus \{0\}$  und  $r_1, \dots, r_n \in \mathbb{C}$  besitzt.
- ④ Aus  $\langle \text{ggT}(f, g) \rangle = \langle f, g \rangle$   $\int_{\text{ggT}(f, g) \in \langle f, g \rangle}$

für  $f, g \in k[x]$  gilt,  
dass  $\text{ggT}(f, g) = Af + Bg$

$$\text{ggT}(f, g) = Af + Bg$$

für  $A, B \in k[x]$

für gewisse  $A, B \in k[x]$  erfüllt ist.

Wie kann man  $A, B$  für gegebene  $f, g$  berechnen?

- (5) Man prüfe, ob  $x^3 + 4x^2 + 3x - 7$   
zum Ideal  $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$   
gehört.
- (6) Berechne die  $\text{ggT}(x^4 + x^2 + 1, x^4 - x^2 - 2x - 1,$   
 $x^3 - 1)$   
und  $\text{ggT}(x^3 + 2x^2 - x - 2, x^3 - 2x^2 - x + 2,$   
 $x^3 - x^2 - 4x + 4)$ .
- (7) Entwickle die einen Algorithmus, der  
entscheidet, ob gegebene  $f_1, \dots, f_s \in k[x]$   
eine gemeinsame Nullstelle in  $C$  haben.  
Der Algorithmus hat Zugriff auf  $+ \cdot$  und  
 $\in C$ .  
Würde ihr Algorithmus immer noch  
funktionieren, wenn man dieser  
Aufgabenstellung  $C$  durch  $R$  austauscht?  
Warum?
- (8) Für  $f = \sum_{j=0}^{\infty} c_j x^j \in k[x]$  definieren wir  
die (formale) Ableitung von  $f$   
als  $f' = \sum_{j=1}^{\infty} j c_j x^{j-1}$ .  
Zeigen Sie, dass  $(f+g)' = f' + g'$   
und  $(fg)' = f'g + fg'$   
für alle  $f, g \in k[x]$  gilt.
- (9) Wir betrachten  $f \in C[x]$  vom Grad

②  $n \geq 1$  in der Darstellung  
 $f = c(x-r_1)^{m_1} \cdot \dots \cdot (x-r_e)^{m_e}$   
 mit  $m_1, \dots, m_e \in \mathbb{Z}_{>0}$ ,  $m_1 + \dots + m_e = n$   
 und  $r_1, \dots, r_e \in \mathbb{C}$  (~~zweiseitig verschieden~~)  
 $c \in \mathbb{C} \setminus \{0\}$ .  
 Wie sehen  $\text{ggT}(f, f')$  und  
 $\frac{f}{\text{ggT}(f, f')}$  aus?

③ Sei  $f \in \mathbb{C}[x]$  mit  $\deg(f) \geq 1$ .

Zerlegen Sie:

$$I(V(f)) = \left\langle \frac{f}{\text{ggT}(f, f')} \right\rangle$$

## KAPITEL 2: GRÖBNERBASEN

Das Lösen der meisten algorithmischen Problemen in kommutativer Algebra basiert auf Gröbnerbasen.

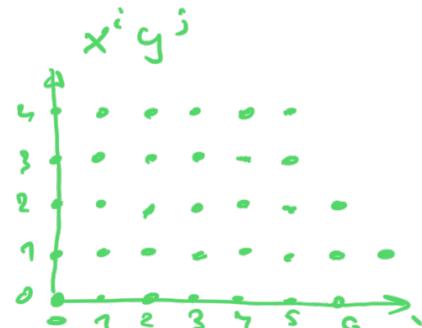
Universeller Fall

$$\begin{matrix} x^0 & x^1 & x^2 & x^3 & x^4 & x^5 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & 2 & 3 & 4 & 5 & \dots \end{matrix}$$

### 2.1. Monomordnungen.

2.1.1 Definition. Eine  
binäre Relation  $\leq$  auf  
einer Menge  $M$  heißt  
(schwache) totale  
Ordnung, wenn für  
alle  $x, y, z \in M$

die folgenden Eigenschaften erfüllt sind:



Antisymmetrie:  $x \not\leq y, y \not\leq x \Rightarrow x = y$   
Transitivität:  $x \not\leq y, y \not\leq z \Rightarrow x \not\leq z$

Totalität: es gilt  $x \leq y$  oder  $y \leq x$

Zur schwachen totalen Ordnung  $\leq$   
kann man die stricke Totale Ordnung  $<$   
introduzieren:

$$x < y \iff x \leq y, x \neq y.$$

Somit hat man zu  $\leq$  auch  $<, \geq, >$ .

Auf der Menge der univariaten Monome  
hat nun die natürliche totale Ordnung

$$x^0 \leq x^1 \leq x^2 \leq x^3 \leq \dots$$

Das Längsmaß der Ordnung

$$0 < 1 < 2 < 3 < \dots$$

auf  $\mathbb{Z}_{\geq 0}$ .

Im multivariaten Fall hat man  
keine eindeutige Wahl.

Man beacht  $\alpha \in \mathbb{Z}_{\geq 0}^n \leftrightarrow x^\alpha$ .

Das heißt Monome zu ordnen ist  
das Etwas wie  $\mathbb{Z}_{\geq 0}^n$  zu ordnen.

2.1.2. Definition. Eine Monomordnung auf  
 $\mathbb{Z}_{\geq 0}^n$  ist eine Relation  $\leq$  auf  $\mathbb{Z}_{\geq 0}^n$   
mit den folgenden Eigenschaften:

(i)  $\leq$  ist eine strikte totale Ordnung

(ii) Für alle  $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$  mit  $\alpha \leq \beta$   
und jeder  $\gamma \in \mathbb{Z}_{\geq 0}^n$  gilt:

$$\alpha + \gamma \leq \beta + \gamma.$$

(iii) Jede nichtleere Teilmenge  $A$  von  $\mathbb{Z}_{\geq 0}^n$   
besitzt ein Element  $\beta \in A$ , das in  $A$   
bzgl. der ordnung  $\leq$  am kleinsten ist

d.h.  $\alpha \succ \beta$  für alle  $\alpha \in A \setminus \{\beta\}$ ,

### 2.1.3. Definition. Eine strikt absteigende Kette

einer total geordneten Menge  $M$   
ist eine (endliche oder unendliche)

Folge der Elemente aus  $M$  mit  
 $a_0 \succ a_1 \succ a_2 \succ a_3 \succ \dots$ .

### 2.1.4. Lemma. Sei $M$ eine total geordnete Menge.

Dann sind die folgenden Bedingungen äquivalent:

- (i) jede strikt absteigende Kette in  $M$  ist endlich.
- (ii) jede nicht leere Teilmenge  $A$  von  $M$  besitzt das kleinste Element bzgl. der Ordnung von  $M$ .

Beweis: Wir zeigen Kontraposition:

nicht (i)  $\Leftrightarrow$  nicht (ii).

Angenommen, es gibt eine Menge  $\emptyset \neq A \subseteq M$ , die kein kleinstes enthält. Wir wählen  $a_0 \in A$  beliebig. Da  $a_0$  kein kleinstes Element von  $A$  ist, gibt es  $a_1 \in A$  mit  $a_0 \succ a_1$ . Da  $a_1$  kein kleinstes Element von  $A$  ist, gibt es  $a_2 \in A$  mit  $a_1 \succ a_2$  usw. So konstruieren wir

$a_0 \succ a_1 \succ a_2 \succ \dots$

mit  $a_i \in A$  für alle  $i \in \mathbb{Z}_{\geq 0}$ .

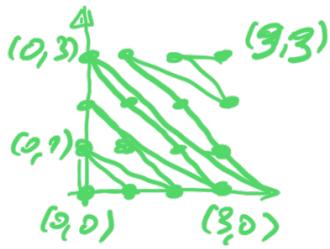
Umgekehrt: sei  $a_0 \succ a_1 \succ a_2 \succ \dots$

mit  $a_i \in M$  für alle  $i \in \mathbb{Z}_{\geq 0}$   
eine unendliche strikt absteigende  
Kette. Dann hat die Menge

$A = \{a_i : i \in \mathbb{Z}_{\geq 0}\}$  kein kleinstes

Element: Für jedes  $a_i$  ist  $a_{i+1}$   
noch kleiner

□.



00	0	1	2	3
21	A	B	C	D
12	A	A	00	00
33	A	B	01	01
	C	C	02	02
	A	D	03	03
	B	A	10	10
	B	C	11	11
	B	D	12	12
			13	13

### 2.1.5 Definition (Lex-, Grlex- und Grelex-Ordnungen).

Auf  $\mathbb{Z}_{\geq 0}^n$  führen wir die folgenden drei  
Ordnungen ein:

$\alpha \not\sim_{\text{lex}} \beta \iff \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$   
für ein  $i \in \{1, \dots, n\}$

$$\begin{aligned} & (\alpha, b, f, a, h, r, e, n) \not\sim_{\text{lex}} \\ & (\alpha, b, P, e, h, r, e, n) \\ & a=0, b=1, d=2, e=3, \dots \end{aligned}$$

$\alpha \not\sim_{\text{grlex}} \beta \iff |\alpha| > |\beta| \text{ oder}$   
 $|\alpha| = |\beta| \text{ und } \alpha \not\sim_{\text{lex}} \beta.$