

U1

Situation im univariaten Fall:

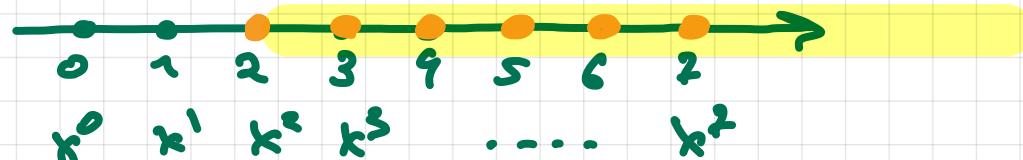
$f \in \langle f_1, \dots, f_s \rangle \Leftrightarrow f \in \langle g \rangle$  mit  $g := \text{ggT}(f_1, \dots, f_s)$

$\Leftrightarrow$  Der Rest der Division von  $f$  durch  $g$  ist 0

Hierbei:

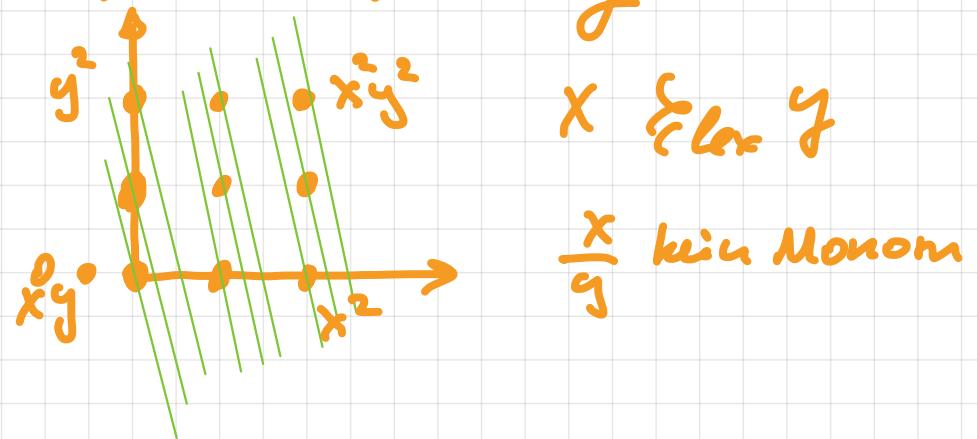
$g$  kann durch den Euklidischen Algorithmus bestimmt werden (verfolgt Polynomdivision)

$g$  ist Nichtnullpolynom vom kleinsten Grad in  $\langle f_1, \dots, f_s \rangle$



Im Multivariaten Fall:

- Eine Polynomdivision benötigt eine Monomordnung



- $\alpha \not\leq \beta \iff x^\alpha$  ist durch  $x^\beta$  teilbar (Division nicht also etwas anders aus)

- Ein Ideal ist i.A. nicht durch ein Polynom erzeugbar (wir müssen durch mehr als ein Polynom teilen können)

2.2.4. Bezeichnung. Wir bezeichnen als  $\text{Rem}(f; G)$

den Rest der Division von  $f \in k[x_1, \dots, x_n]$  durch  $G = (g_1, \dots, g_s)$  mit  $g_1, \dots, g_s \in k[x_1, \dots, x_n] \setminus \{0\}$

## 2.3. Monomiale Ideale und das Lemma von Dickson

Wir verallgemeinern die Bezeichnung  $\langle f_1, \dots, f_s \rangle$  auf unendliche Familien von Polynomen:

2.3.1 Def. Für eine (potenziell unendliche) indexierte Familie  $(f_s)_{s \in S}$  von Polynomen aus  $k[x_1, \dots, x_n]$  wird das Ideal das Ideal definiert, das durch diese Familie erzeugt ist: es ist das Ideal  $\langle f_s : s \in S \rangle$  aller Polynome der Form

$$\sum_{s \in S} h_s f_s \quad \text{mit } h_s \in k[x_1, \dots, x_n] \text{ und mit} \\ h_s \neq 0 \text{ nur für endlich viele } s \in S.$$

Bem. Es ist tatsächlich ein Ideal.

2.3.2. Def. Ist  $A \subseteq \mathbb{Z}_{\geq 0}^n$  (potenzziell endlich),  
 so nennt man das Ideal  $\langle x^\alpha : \alpha \in A \rangle$   
 das monomiale Ideal zu  $A$ .

2.3.3. Def. Auf  $\mathbb{Z}_{\geq 0}^n$  fixieren wir die Teilordnung  $\geq$   
 wie folgt:

$$\alpha = (\alpha_1, \dots, \alpha_n) \geq \beta = (\beta_1, \dots, \beta_n) :\Leftrightarrow \alpha_1 \geq \beta_1, \dots, \alpha_n \geq \beta_n$$

$\alpha \leq \beta$  wird analog definiert.

Bem.  $\alpha \geq \beta \iff x^\alpha$  ist durch  $x^\beta$  teilbar.  
 $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$

2.3.4. Def. Für  $A, B \subseteq \mathbb{Z}_{\geq 0}^n$  nennen wir  
 $A + B := \{ \alpha + \beta : \alpha \in A, \beta \in B \}$

die Minkowski-Summe von  $A$  und  $B$ .

Bew:  $\text{lin}_k :=$  lineare Hülle bzgl. k.

{5}

2.3.5. Lemma. Sei  $A \subseteq \mathbb{Z}_{\geq 0}^n$ . Dann gilt:

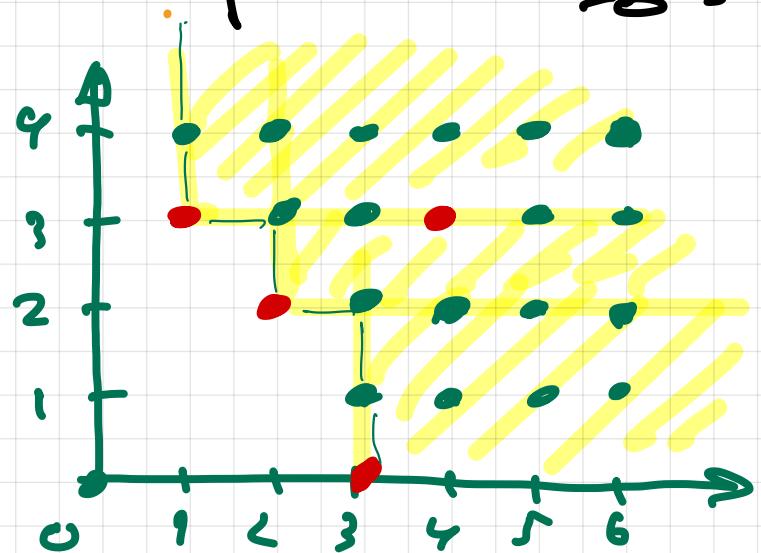
$$\langle x^\alpha : \alpha \in A \rangle = \text{lin}_k \{ x^\beta : \beta \in A + \mathbb{Z}_{\geq 0}^n \}$$

Beweis:

" $\supseteq$ ": Für  $x^\beta$  mit  $\beta \in A + \mathbb{Z}_{\geq 0}^n$

gilt  $x^\beta = x^\alpha + x^\gamma$  mit

$\alpha \in A$  und  $\gamma \in \mathbb{Z}_{\geq 0}^n$ ,



$$\Rightarrow x^\beta = x^\alpha + x^\gamma = \underbrace{x^\alpha}_{\in \langle x^\alpha : \alpha \in A \rangle} \cdot x^\gamma \in \langle x^\alpha : \alpha \in A \rangle$$

$$\Rightarrow \text{lin}_k \{ x^\beta : \beta \in A + \mathbb{Z}_{\geq 0}^n \} \subseteq \langle x^\alpha : \alpha \in A \rangle.$$

" $\subseteq$ ": Wir betrachten ein beliebiges Polynom aus  
 $\langle x^\alpha : \alpha \in A \rangle$ . Das hat die Form  
 $\sum_{\alpha \in A} h_\alpha x^\alpha$  mit  $h_\alpha \in k[x_1, \dots, x_n]$   
und  $h_\alpha \neq 0$  nur für endlich viele  
 $\alpha$ 's.

$h_\alpha$  hat die Form  $h_\alpha = \sum_{\gamma} \underbrace{c_{\alpha, \gamma}}_{k^n} x^\gamma \Rightarrow$

$$h_\alpha x^\alpha = \sum_{\gamma} c_{\alpha, \gamma} x^\gamma \cdot x^\alpha \underset{k}{=} \sum_{\gamma} c_{\alpha, \gamma} x^{\alpha + \gamma}$$

mit  $\alpha + \gamma \in A + \mathbb{Z}_{\geq 0}^n$  für alle  $\gamma \in \mathbb{Z}_{\geq 0}^n$ .

D.h.  $h_\alpha x^\alpha \in \text{link}_k \{x^\beta : \beta \in A + \mathbb{Z}_{\geq 0}^n\}$ .

$$\Rightarrow \sum_{\alpha} h_\alpha x^\alpha \in \text{link}_k \{x^\beta : \beta \in A + \mathbb{Z}_{\geq 0}^n\}.$$



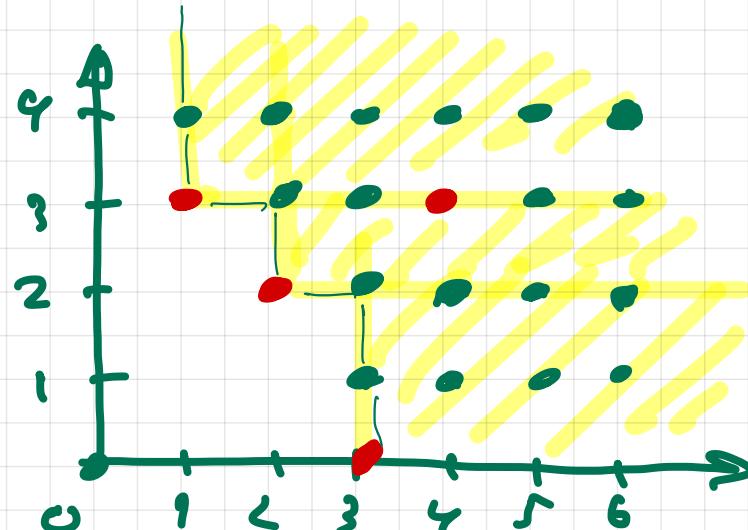
2.3.6. Korollar. Wenn für  $A, B \subseteq \mathbb{Z}_{\geq 0}^n$  die  
Gleichung  $A + \mathbb{Z}_{\geq 0}^n = B + \mathbb{Z}_{\geq 0}^n$  gilt, dann  
gilt  $\langle x^\alpha : \alpha \in A \rangle = \langle x^\beta : \beta \in B \rangle$ .

Beweis: Direkte Konsequenz aus 2.3.5.

### 2.3.7. Beispiele:

$$A = \{(3,0), (2,2), (1,3), (4,3)\}$$

$$\begin{aligned} & \langle x^\alpha : \alpha \in A \rangle = \\ &= \lim_k \{x^\beta : \beta \in \mathbb{Z}_{\geq 0}^n, \\ & \quad \beta \geq (3,0) \text{ oder } \beta \geq (2,2) \text{ oder } \beta \geq (1,3)\} \end{aligned}$$



## 2.3.8 Theorem (Lemma von Dickson)

18

für jedes  $A \subseteq \mathbb{Z}_{\geq 0}^n$  existiert eine endliche Teilmenge  $B$  von  $A$  mit  $\langle x^\alpha : \alpha \in A \rangle = \langle x^\beta : \beta \in B \rangle$ .

Beweis: Nach Korollar 2.3.6 reicht es eine endliche Teilmenge  $B \subseteq A$  mit  $A + \mathbb{Z}_{\geq 0}^n = B + \mathbb{Z}_{\geq 0}^n$  zu finden.

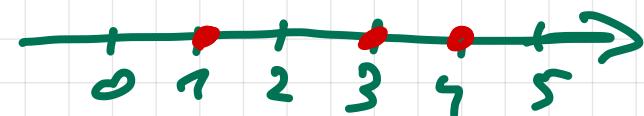
" $\supseteq$ " gilt wegen  $A \supseteq B$ . Es gilt nun  $A + \mathbb{Z}_{\geq 0}^n \subseteq B + \mathbb{Z}_{\geq 0}^n$ .

Dafür reicht es ein  $B$  zu finden, bei dem für jedes  $\alpha \in A$  ein  $\beta \in B$  existiert, für das  $\alpha \geq \beta$  gilt.

(Mit anderen Worten:  $A \subseteq B + \mathbb{Z}_{\geq 0}^n$ )

Die Existenz eines endlichen  $B \subseteq A$  mit  $A \subseteq B + \mathbb{Z}_{\geq 0}^n$  zeigen wir durch Induktion über  $n$ .

$n=1$ :  $A = \emptyset \Rightarrow B = \emptyset$  passt.



$A \neq \emptyset \Rightarrow B = \{\min(A)\}$

ist eine passende Wahl.

Sei  $n \geq 2$  und sei die Behauptung für Teilmenge  
 von  $\mathbb{Z}_{\geq 0}^{n-1}$  bereits verifiziert. Wir betrachten  
 eine beliebige Teilmenge  $A \subseteq \mathbb{Z}_{\geq 0}^n$ . 19

$A = \emptyset \Rightarrow B = \emptyset$  ist eine passende Wahl.

$A \neq \emptyset \Rightarrow$  wir fixieren ein dekoratives  $\gamma = (\gamma_{n-1}, \gamma_n) \in A$

Wir nehmen  $\gamma$  in  $B$  auf.

Für jedes

$$\alpha = (\alpha_1, \dots, \alpha_n) \in A$$

mit  $\alpha \not\equiv \gamma$  gilt

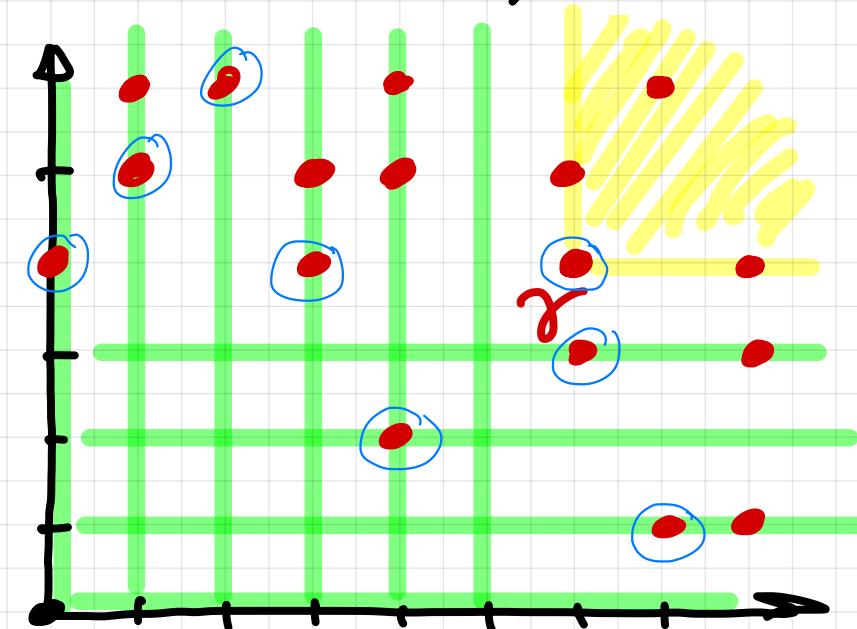
$\alpha_1 \in \{0, \dots, \gamma_1 - 1\}$  oder

$\alpha_2 \in \{0, \dots, \gamma_2 - 1\}$  oder

$\vdots$

$\alpha_n \in \{0, \dots, \gamma_n - 1\}$  (d.h. man hat ein  $i$  mit  $\alpha_i \leq \gamma_i - 1$ )

$\Rightarrow A \subseteq \{\alpha \in \mathbb{Z}_{\geq 0}^n : \alpha \geq \gamma\} \cup \bigcup_{j=1}^n \bigcup_{m=1}^{\gamma_j} A_{j,m}$  mit



$$A_{i,m} := \{ \alpha = (d_1, \dots, d_n) \in A : d_i = m \}$$

10

Bei der Menge  $A_{i,m}$  ist die  $i$ -te Komponente der Elemente von  $A_{i,m}$  fest. Wir können also  $A_{i,m}$  mit einer Teilmenge von  $\mathbb{R}_{\geq 0}^{n-1}$  identifizieren, indem man die  $i$ -te Komponente wegläßt.

Nach der Induktionsvoraussetzung existiert

also ein endliches  $B_{i,m} \subseteq A_{i,m}$  mit:

$$\forall \alpha \in A_{i,m} \exists \beta \in B_{i,m} : \alpha \geq \beta.$$

$\Rightarrow$  Für die Menge  $A$  ist

$$B = \{g\} \cup \bigcup_{i=1}^n \bigcup_{m=1}^{g_i-1} B_{i,m}$$

eine passende Wahl.

□

2.3.9. Korollar Sei  $\mathcal{E}$  strikte totale Ordnung auf  $\mathbb{Z}_{\geq 0}^n$ ,  
 die für alle  $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$  mit  $\alpha \not\sim \beta$  die Bedingung  
 $\alpha + \gamma \not\sim \beta + \gamma$  erfüllt. Dann sind die folgenden  
 Bedingungen äquivalent:

- (i) Jede nichtleere Teilmenge  $A$  von  $\mathbb{Z}_{\geq 0}^n$  besitzt  
 das kleinste Element bzgl.  $\mathcal{E}$ .
- (ii)  $0$  ist das kleinste Element von  $\mathbb{Z}_{\geq 0}^n$  bzgl.  $\mathcal{E}$ .

Beweis: (i)  $\Rightarrow$  (ii): Wäre das kleinste Element  $\gamma$   
 von  $\mathbb{Z}_{\geq 0}^n$  bzgl.  $\mathcal{E}$  anders als  $0$ , so hätte man  
 $\gamma = \gamma + 0 \not\sim \gamma + \gamma = 2\gamma \Rightarrow$   
 $\gamma \not\sim 2\gamma \Rightarrow$   $\gamma$  war nicht das kleinste Element von  $\mathbb{Z}_{\geq 0}^n$ .

(ii)  $\Rightarrow$  (i): Nach dem Beweis zu 2.3.8 existiert  
 ein additives  $B \subseteq A$  mit  $\forall \alpha \in A \exists \beta \in B: \alpha \geq \beta$ .

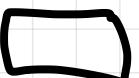
$0 \in \mathbb{B}_{\geq 0}^c$  ist das kleinste Element von  $\mathbb{B}_{\geq 0}^c$  bzgl. 12

E. Wenn  $\alpha \in A$ ,  $\beta \in B$  und  $\alpha \geq \beta$  gilt  
so gilt auch  $\alpha - \beta \notin 0 \Rightarrow$   
 $(\alpha - \beta) + \beta \notin 0 + \beta \Rightarrow \alpha \notin \beta.$

Sei  $\gamma$  das kleinste Element von  $B$  bzgl. E.

für jedes  $\alpha \in A$  gibt es ein  $\beta \in B$  mit  
 $\alpha \geq \beta. \Rightarrow \alpha \notin \beta \Rightarrow \alpha \notin \beta \notin \gamma$   
 $\Rightarrow \alpha \notin \gamma.$

$\Rightarrow \gamma \in B \subseteq A$  ist das kleinste Element  
von  $A$  bzgl. E.



## 2.4. Hilbertscher Basisatz und die Gröbnerbasen.

13

2.4.1 Def. Sei  $I \subseteq k[x_1, \dots, x_n]$  ein Ideal mit  $I \neq \{0\}$ .

Wir definieren

$$LT(I) := \{ LT(f) : f \in I \setminus \{0\} \}$$

und nennen

$$\begin{aligned} \langle LT(I) \rangle &= \langle LT(f) : f \in I \setminus \{0\} \rangle \\ &= \langle LM(f) : f \in I \setminus \{0\} \rangle \end{aligned}$$

das Initial-Ideal von  $I$ .

Bem.  $\langle LT(I) \rangle$  ist ein Monomideal.

Bem. Im Fall  $I = \langle f_1, \dots, f_s \rangle$  gilt in Allgemeines  
 $\langle LT(I) \rangle \neq \langle LT(f_1), \dots, LT(f_s) \rangle$ .

2.4.2. Bsp.  $f_1 = x^3 - 2xy$ ,  $f_2 = x^2y - 2y^2 + x$  (14)

Monom ordering:  $\text{grlex}$

$$\langle \text{LT}(f_1), \text{LT}(f_2) \rangle = \langle x^3, x^2y \rangle$$

$$x^2 = -y f_1 + x f_2$$

$$= -y (\underline{x^3} - \underline{2xy})$$

$$+ x (\underline{x^2y} - \underline{2y^2} + x)$$

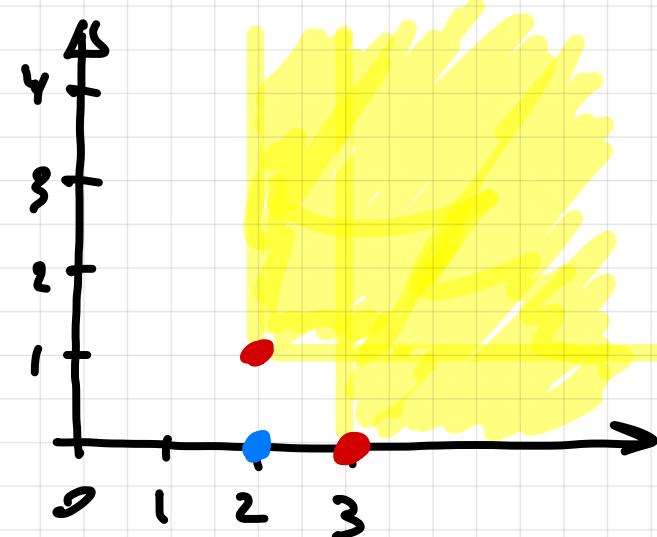
$$\Rightarrow x^2 \in \langle \text{LT}(\mathcal{I}) \rangle \text{ mit } \mathcal{I} = \langle f_1, f_2 \rangle$$

aber  $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$ .

2.4.3. Prop. Für jedes Ideal  $\mathcal{I} \subseteq k[x_1, \dots, x_n]$  mit  $\mathcal{I} \neq \{0\}$

gibt es mindestens viele Polynome  $g_1, \dots, g_s \in \mathcal{I} \setminus \{0\}$

mit  $\langle \text{LT}(\mathcal{I}) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle$ .



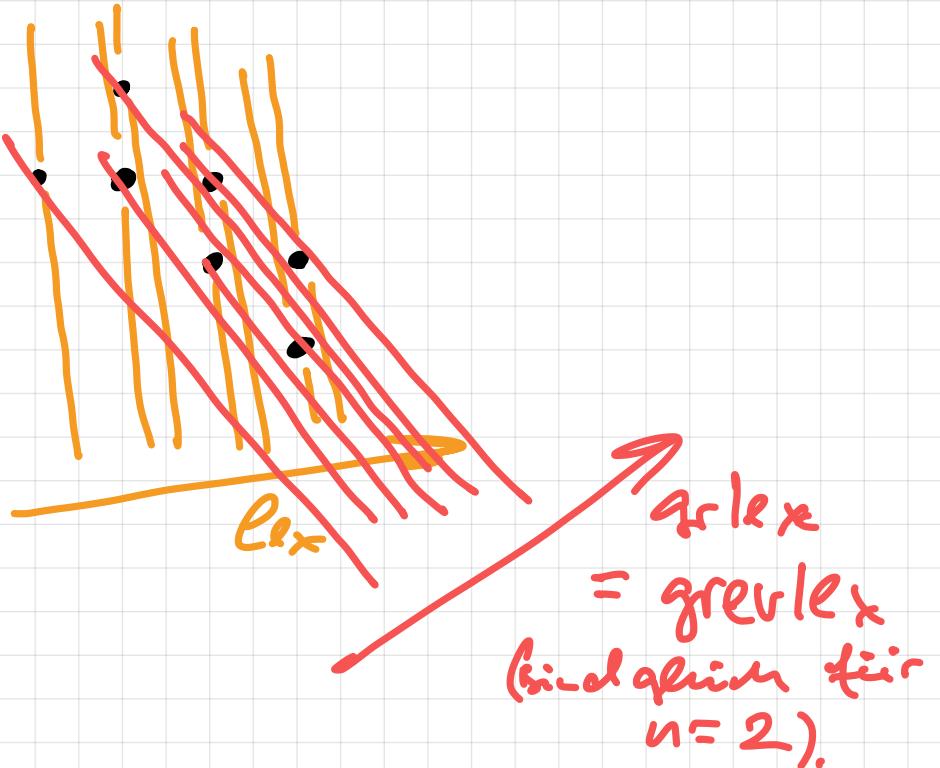
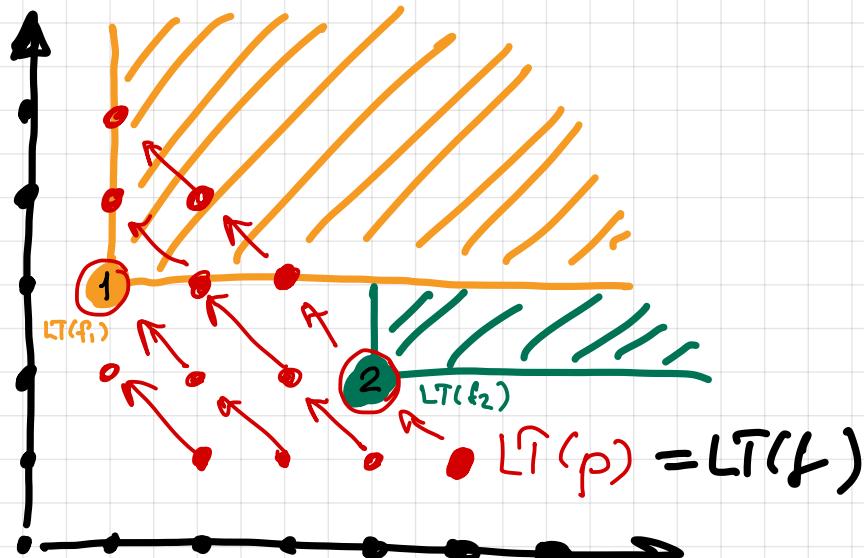
Beweis: eine direkte Folgerung aus den Lemmas von Dickson. VS

## 2.4.4 Theorem (Hilbertscher Basissatz)

Jedes Ideal  $I \subseteq k[x_1, \dots, x_n]$  ist endlich erzeugt, d.h. es existieren endlich viele Polynome  $g_1, \dots, g_s \in I$  mit  $I = \langle g_1, \dots, g_s \rangle$ .

---

Wir holen zwei Punkte aus 2.2. nach.



2.2.2 Theorem. Sei  $\mathcal{E}$  Monomordnung auf  $\mathbb{P}_{\geq 0}^n$  und seien  $f_1, \dots, f_s$   $\in k[x_1, \dots, x_n] \setminus \{0\}$ . Dann existiert für jedes  $f \in k[x_1, \dots, x_n]$  eine Darstellung  $f = a_1 f_1 + \dots + a_s f_s + r$  mit  $a_1, \dots, a_s, r \in k[x_1, \dots, x_n]$ , welche die folgenden Eigenschaften erfüllen:

- kein Term von  $r$  ist durch den Leitterm von  $f_i$  teilbar (für jedes  $i=1, \dots, s$ ).
- $\text{mdeg}(f) < \text{mdeg}(a_i f_i)$  ( $i=1, \dots, s$ ).

Beweis: Diese Darstellung wird durch den Divisionsalgorithmus berechnet. Wir zeigen, dass der Divisionsalgorithmus terminiert und seine Rückgabe die gewünschten Eigenschaften erfüllt. Der Algorithmus terminiert, weil in jeder Iteration der höheren Potenzen des Leitterms von  $p$  des Leitterms bzgl.  $\mathcal{E}$  geschrumpft (entweder durch ein Update eines Quotienten oder durch die Aufnahme des Leiterrms von  $p$  in den Rest). Die Eigenschaft für  $r$  ist erfüllt, weil in den Rest nur die Terme aufgenommen werden, die man nicht  $r$  durch  $\text{LT}(f_1), \dots, \text{LT}(f_s)$  teilen kann.

## zu Eigenschaft der Quotienten:

Man skript mit  $p = f$ , sodass aus Auskug  
 $\text{ord}_g(p) = \text{ord}_g(f)$  gilt. Da beim Herabsetzen des  
Multiplikativen Grades von  $p$  verringert wird, gilt  $\text{ord}_g(p) \geq \text{ord}_g(f)$   
während der Ausführung.

Die Updates des Quotienten  $q_i$  sind so aufgebaut,  
dass beim Update  $a_{ij} := a_{ij} + T$

$$\begin{aligned}\text{ord}_g(T \cdot f_i) &= \text{ord}_g(p) \text{ gilt. Es folgt} \\ \text{ord}_g(T \cdot f_i) &= \text{ord}_g(p) \geq \text{ord}_g(f) \Rightarrow \\ \text{ord}_g(T \cdot f_i) &\geq \text{ord}_g(f).\end{aligned}$$

Das gilt für jeden Term  $T$ , der man in  $q_i$  einfügt.

$$\Rightarrow \text{ord}_g(a_i \cdot f_i) \geq \text{ord}_g(f). \quad \square$$

2.2.3. Bsp.  $f = xy^2 - x$  durch  $f_1 = xy + 1, f_2 = y^2 - 1$   
teilt das Lex-Ordinary.

Wenn wir  $f$  durch  $(f_1, f_2)$  teilen hat man einen anderen  
Rest als beim teilen von  $f$  durch  $(f_2, f_1)$ .

Im ersten Fall ist der Rest  $\neq 0$ . Im zweiten Fall ist der Rest 0. In allgemeiner spricht die Restausgabe des Polynoms beim Teilen eine willkürige Rolle.

---

Beweis von 2.7.4 (Hilbertscher Basisatz).

Im Fall  $I = \langle 0 \rangle$  ist die Behauptung trivial. Sei  $I \neq \langle 0 \rangle$ .

Nach dem Lemma von Dickson gibt es endlich viele Polynome  $g_1, \dots, g_s \in I \setminus \{0\}$  mit  $\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle$ .

Wir zeigen:  $I = \langle g_1, \dots, g_s \rangle$

" $\geq$ " ist klar wegen  $g_1, \dots, g_s \in I$ . Wir zeigen " $\leq$ ". Sei  $f \in I$  beliebig.

Wir teilen  $f$  durch  $(g_1, \dots, g_s)$ . Auf diese Weise erhalten wir die Darstellung  $f = a_1 g_1 + \dots + a_s g_s + r$  mit

$a_1, \dots, a_s, r \in k[x_1, \dots, x_n]$ , in der kein Term von  $r$  durch  $LT(g_i)$  teilbar ist ( $i = 1, \dots, s$ ). Wir behaupten  $r = 0$ . Andernfalls, man hätte  $r \neq 0$ . Es gilt

$$r = f - (a_1 g_1 + \dots + a_s g_s) \in I.$$

$$\Rightarrow \text{LT}(r) \in \langle \text{LT}(\mathfrak{I}) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle \Rightarrow$$

$\Rightarrow \text{LT}(r)$  ist durch ein  $\text{LT}(g_i)$  mit  $i=1, \dots, s$  filterbar  $\Rightarrow \cancel{\leq}$ .  $\square$

2.4.5. Def. Sei  $\{0\} \neq \mathfrak{I} \subseteq k[x_1, \dots, x_n]$

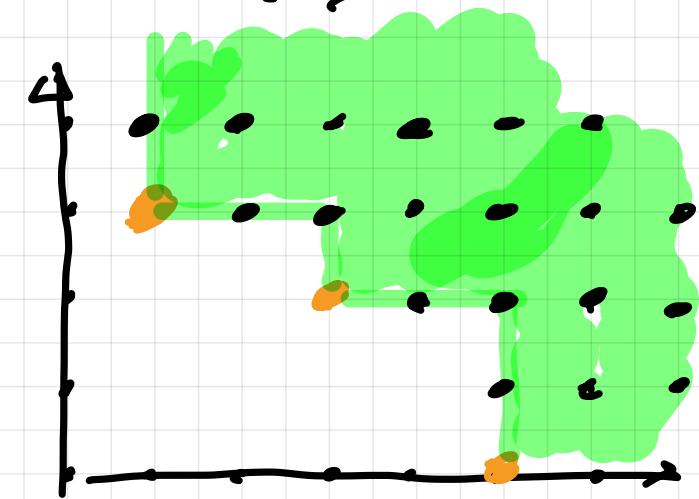
ein ideal. Wir nehmen

$G = (g_1, \dots, g_s)$  eine Gröbnerbasis  
von  $\mathfrak{I}$ , weiter

$$\langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle = \langle \text{LT}(\mathfrak{I}) \rangle \text{ gilt.}$$

2.4.6 Korollar. Sei  $\{0\} \neq \mathfrak{I} \subseteq k[x_1, \dots, x_n]$  ideal. Dann besitzt  
 $\mathfrak{I}$  eine Gröbnerbasis. Jede Gröbnerbasis von  $\mathfrak{I}$  ist eine  
Basis von  $\mathfrak{I}$ .

Beweis: folgt aus unserem Beweis des filterhaften  
Basisatzes.



2.4.7 Theorem (ACC = The Ascending Chain Condition =

20

Kettentheorie - für Ideale) Sei  $(I_j)_{j \in \mathbb{N}}$  eine  
Folge von Idealen in  $k[x_1, \dots, x_n]$  mit der Eigenschaft

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

(Bsp.  $\subseteq$  nicht strikt aufgestiegene geschachtelt). Dann  
existiert ein  $N \in \mathbb{N}$  mit  $I_N = I_{N+1} = I_{N+2} = \dots$

(d.h. die Kette stabilisiert sich).

Beweis: Sei  $I := \bigcup_{j=1}^{\infty} I_j$ .  $I$  ist ebenfalls ein Ideal:

$$0 \in I_1 \Rightarrow 0 \in I.$$

$$f, g \in I \Rightarrow f \in I_s, g \in I_t \text{ für gewisse } s, t \in \mathbb{N}$$

$$\Rightarrow f \in I_m, g \in I_m \text{ mit } m = \max\{s, t\}$$

$$\Rightarrow f + g \in I_m$$

$$\Rightarrow f + g \in I.$$

$$h \in k[x_1, \dots, x_n], f \in I \Rightarrow h \in k[x_1, \dots, x_n], f \in I_j \text{ für ein } j \in \mathbb{N}$$

$$\Rightarrow h \cdot f \in I_j \Rightarrow h \cdot f \in I.$$

Nach dem Hilbertschen Basissatz ist  $I$  endlich erzeugt; (2)

es gibt  $f_1, \dots, f_s \in I$  und  $I = \langle f_1, \dots, f_s \rangle$

Für jedes  $i \in \{1, \dots, s\}$  gibt es ein  $N_i \in \mathbb{N}$  mit  $f \in I_{N_i}$ .

Die Behauptung gilt für  $N = \max \{N_1, \dots, N_s\}$ :

alle  $f_1, \dots, f_s \in I_N \Rightarrow I_N = I \Rightarrow$

$$I = I_{N+1} = I_{N+2} = I_{N+3} = \dots$$



2.4.8. Def. Für eine (potentiell unendliche) Menge

$f \subseteq k[x_1, \dots, x_n]$  definieren wir die Varietät  $V$

als  $V(F) = \{a \in k^n : f(a) = 0 \text{ für alle } f \in F\}$ .

2.4.9. Prop. Für jede Teilmenge  $F \subseteq k[x_1, \dots, x_n]$

existiert eine endlich viele Polynome  $f_1, \dots, f_s \in F$

mit  $V(F) = V(f_1, \dots, f_s)$ . Insbesondere ist  $V(F)$  eine affine Varietät.

Beweis: Wir betrachten das (ideal)  $\langle F \rangle$ , das durch alle Polynome aus  $F$  erzeugt ist. Nach dem Hilbertschen Basisatz gibt es endlich viele Polynome  $g_1, \dots, g_m \in \langle F \rangle$  mit  $\langle F \rangle = \langle g_1, \dots, g_m \rangle$ . Man hat  $g_i \in \langle f_i \rangle$  für ein endliches  $f_i \subseteq F$  ( $i = 1, \dots, m$ ).  $\Rightarrow$

$$f_1 \cup \dots \cup f_m$$
 ist eine endliche Menge

Seien  $f_1, \dots, f_s$  Polynome mit  $\{f_1, \dots, f_s\} = F_1 \cup \dots \cup F_m$ .

Es gilt  $V(F) = V(f_1, \dots, f_s)$ :

" $\subseteq$ " gilt wegen  $F \supseteq \{f_1, \dots, f_s\}$ .

" $\supseteq$ ": sei  $a \in V(f_1, \dots, f_s) \Rightarrow f_i(a) = 0, \dots, f_s(a) = 0$ .

$$\Rightarrow (\text{wegen } g_i = \sum_{j=1}^s h_{ij} f_j) \quad g_i(a) = \sum_{j=1}^s h_{ij}(a) \underbrace{f_j(a)}_{=0} = 0$$

$\Rightarrow$  für ein beliebiges  $f \in F$  hat man  $f = \sum_{j=1}^m h_j g_j$

$$\Rightarrow f(a) = \sum_{j=1}^m h_j(g_j(a)) \underbrace{g_j(a)}_{=0} = 0. \Rightarrow a \in V(F) \quad \square$$

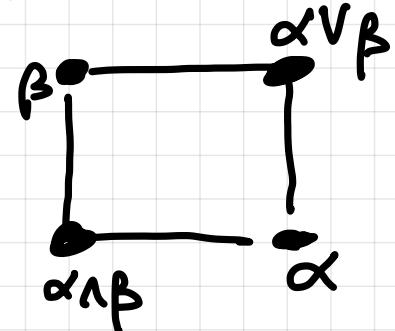
## 2.5. Eigenschaften von Größenbasen. (23)

2.5.1 Definition. Für  $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$

definieren wir:

$$\alpha \vee \beta := (\max\{\alpha_1, \beta_1, \dots, \max\{\alpha_n, \beta_n\}\})$$

$$\alpha \wedge \beta := (\min\{\alpha_1 \beta_1\}, \dots, \min\{\alpha_n \beta_n\})$$



$x^{\alpha \vee \beta}$  ist das kleinste gemeinsame Vielfache von  $x^\alpha$  und  $x^\beta$   
 $x^{\alpha \wedge \beta}$  ist der größte gg. Teiler von  $x^\alpha$  und  $x^\beta$ .

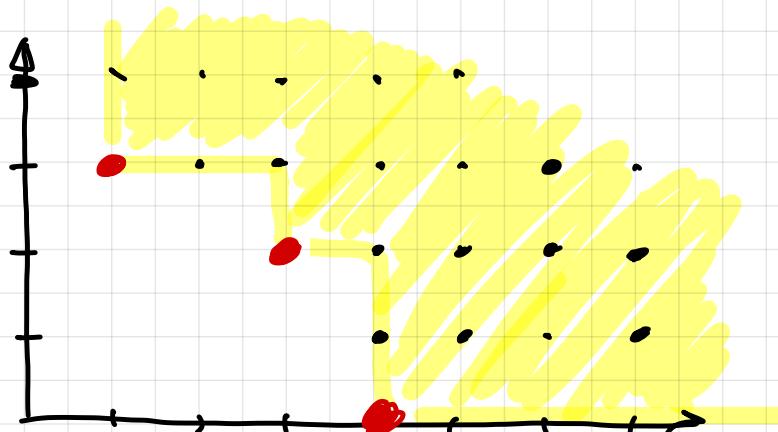
Bzgl. der Teilordnung  $\geq$  auf  $\mathbb{Z}_{\geq 0}^n$  ist  $\alpha \vee \beta$  die kleinste gemeinsame obere Schranke von  $\alpha$  und  $\beta$  und  $\alpha \wedge \beta$  die größte gemeinsame untere Schranke.

2.5.2 Definition. Seien  $f, g \in k[x_1, \dots, x_n]^{> 0}$  mit

$\alpha = \text{mdeg}(f)$  und  $\beta = \text{mdeg}(g)$ . Wir definieren das S-Polygon von  $f$  und  $g$  als

$$S(f, g) = \frac{x^{\alpha \vee \beta}}{\text{LT}(f)} f - \frac{x^{\alpha \vee \beta}}{\text{LT}(g)} g$$

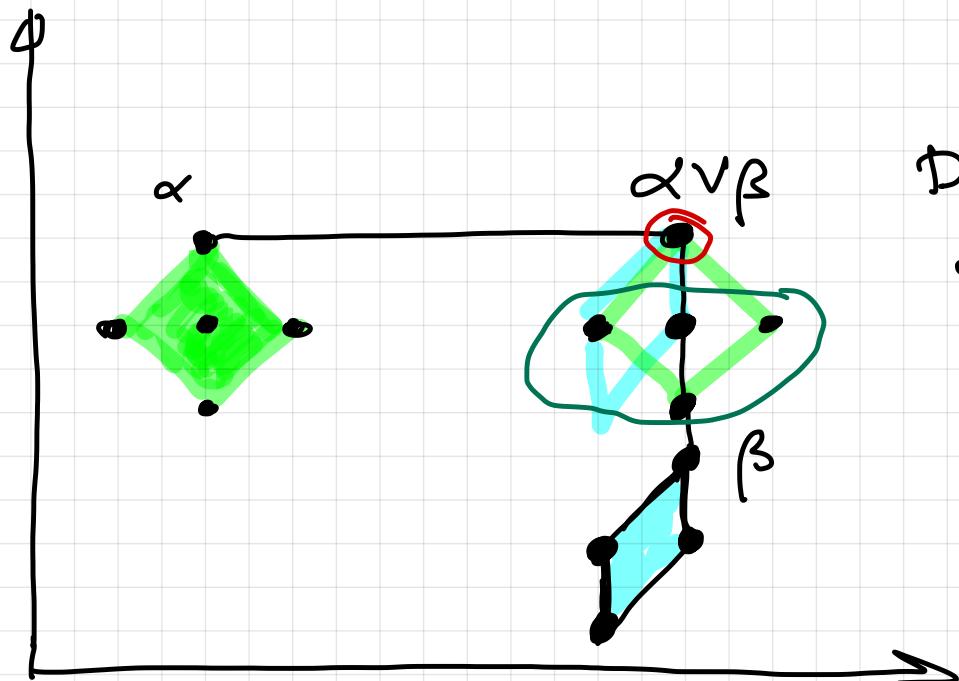
(24)



$$LT(f) = L(f) \cdot x^\alpha$$

$$LT(g) = L(g) \cdot x^\beta$$

$$S(f, g) = \underbrace{\frac{x^{\alpha + \beta}}{LT(f)} f}_{mdeg_{LC} = \alpha + \beta} - \underbrace{\frac{x^{\alpha + \beta}}{LT(g)} g}_{mdeg_{LC} = \alpha + \beta}$$



Die Leitterme der beiden Polynome sind  $x^{\alpha + \beta}$ . Diese Terme kompensieren sich.

2.5.3. Bemerkung.

- $S(f, g)$  hängt nicht von  $\text{LC}(f)$  und  $\text{LC}(g)$  ab. Oder mit anderen Worten gilt  $S(cf, d \cdot g) = S(f, g)$  für  $c, d \in k \setminus \{0\}$ .
- Es gilt  $S(x^\gamma f, x^\gamma g) = x^\gamma S(f, g)$  für  $\gamma \in \mathbb{Z}_{\geq 0}^n$ .
- $\text{mdeg}(S(f, g)) \preceq \text{mdeg}(f) \vee \text{mdeg}(g)$

$\vee = \text{wedge}$

2.5.4. Lemma Sei  $\delta \in \mathbb{Z}_{\geq 0}^n$ . Seien  $f_1, \dots, f_s \in k[x_1, \dots, x_n] \setminus \{0\}$  und  $c_1, \dots, c_s \in k$  so genügt, dass  $\text{mdeg}(f_i) = \delta$  für alle  $i \in \{1, \dots, s\}$  gilt und für  $f = c_1 f_1 + \dots + c_s f_s$  die Bedingung  $\text{mdeg}(f) \geq \delta$  erfüllt ist. Dann ist

$$f \in \text{link}_K \{ S(f_i, f_j) : 1 \leq i, j \leq s \}.$$

Beweis: ObdA keiner  $\text{LC}(f_i) = \gamma$  für alle  $i \in \{1, \dots, s\}$  angenommen werden:

$$f = \sum_{i=1}^s c_i f_i = \sum_{i=1}^s c_i \underbrace{\text{LC}(f_i)}_{\text{neut } c_i} \cdot \underbrace{\frac{f_i}{\text{LC}(f_i)}}_{\text{neut } f_i}.$$

Diese Ähnlichkeit hat keine Auswirkung auf  $S$ -Polynome  $S(f_i, f_j)$ .

$$\Rightarrow S(f_i, f_j) = \frac{x^{\delta_{ij}}}{x^{\delta}} \cdot f_i - \frac{x^{\delta_{ji}}}{x^{\delta}} \cdot f_j = f_i - f_j. \quad \text{L26}$$

$$\text{mdeg } f = \text{mdeg } (\sum_{i=1}^s c_i f_i) \rightarrow \delta \quad \left\{ \begin{array}{l} \text{Der Koeffizient von } x^\delta \text{ in } f \text{ ist } c_1 + \dots + c_s. \\ \Rightarrow c_1 + \dots + c_s = 0. \end{array} \right.$$

$$\begin{aligned} \Rightarrow f &= \sum_{i=1}^s c_i f_i = \sum_{i=1}^{s-1} c_i f_i - (c_1 + \dots + c_{s-1}) f_s \\ &= \sum_{i=1}^{s-1} c_i (f_i - f_s) = \sum_{i=1}^{s-1} c_i S(f_i, f_s) \\ &\in \text{lin}_k \{ S(f_i, f_j) : 1 \leq i, j \leq s \} \end{aligned}$$

□

2.5.5 Theorem (S-Puiseux-Kritterium). Für  $g_1, \dots, g_s \in k(x_1, \dots, x_n) \setminus \{0\}$

sind die folgenden Bedingungen Äquivalent:

- (i)  $g_1, \dots, g_s$  ist eine Gröbnerbasis von  $\mathcal{I} := \langle g_1, \dots, g_s \rangle$
- (ii)  $\text{Rem}(S(g_i, g_j), g_1, \dots, g_s) = 0$  gilt für alle  $1 \leq i < j \leq s$ .

Beweis: (i)  $\Rightarrow$  (ii): Aus dem Beweis des Hilbertschen Basisatzes folgt, dass  $\text{Ren}(f; g_1, \dots, g_s) \Rightarrow$  für alle  $f \in I$  gilt.

dass  $\text{Ren}(f; g_1, \dots, g_s) \Rightarrow$  für alle  $f \in I$  gilt.  
Also ist (ii) erfüllt, wenn  $S(g_i, g_j) \subseteq I$  gilt.

(ii)  $\Rightarrow$  (i): Sei (ii) erfüllt. Sei  $f \in I \setminus \{0\}$ . Wir zeigen, dass  $\text{LT}(f) \in \langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle$  gilt. Wir betrachten eine

Darstellung  $f = \sum_{i=1}^s h_i g_i$  mit  $h_1, \dots, h_s \in k[x_1, \dots, x_n]$

davon, dass  $\delta = \max \{\text{mdeg}(h_1 g_1), \dots, \text{mdeg}(h_s g_s)\}$

bzgl.  $\leq$  am kleinsten ist (hier: max ist das Maximum bzgl.  $\leq$ ). Wir behaupten:  $\text{mdeg}(f) = \delta$ . Das zeigen wir durch ein Widerspruchsbeweis. Angenommen, man hätte  $\text{mdeg}(f) > \delta$ . Seien

$$I = \{ i \in \{1, \dots, s\} : \text{mdeg}(h_i g_i) = \delta \} \quad \text{und}$$

$$J = \{ i \in \{1, \dots, s\} : \text{mdeg}(h_i g_i) > \delta \}$$

$$\Rightarrow f = \sum_{i \in I} h_i g_i + \sum_{j \in J} h_j g_j \quad \Rightarrow$$

$$\underbrace{f = \sum_{i \in I} LT(h_i) g_i}_{\text{mdeg } \leq \delta} + \underbrace{\sum_{i \in I} (h_i - LT(h_i)) g_i}_{\text{mdeg } = \delta} + \underbrace{\sum_{j \in J} h_j g_j}_{\text{mdeg } \geq \delta}$$

$$\Rightarrow \text{mdeg} \left( \underbrace{\sum_{i \in I} LT(h_i) g_i}_{\text{mdeg } = \delta} \right) \geq \delta$$

$\xrightarrow{\text{Lemma 2.5.4}}$

$$\sum_{i \in I} LT(h_i) g_i = \sum_{e, m \in I} c_{e, m} S \left( LT(h_e) g_e, LT(h_m) g_m \right)$$

mit gewissen  $c_{e, m} \in k$ .

Hierbei ist

$$S \left( \underbrace{LT(h_e) g_e}_{\text{mdeg } = \delta}, \underbrace{LT(h_m) g_m}_{\text{mdeg } = \delta} \right) = S \left( \times^{\text{mdeg}(h_e)} g_e, \times^{\text{mdeg}(h_m)} g_m \right) =$$

$\underbrace{\text{mdeg } \geq \delta}$

$$= \frac{x^\delta}{x^{\text{mdeg}(g_e)} \text{LT}(g_e)} x^{\text{mdeg}(g_e)} g_e - \frac{x^\delta}{x^{\text{mdeg}(g_m)} \text{LT}(g_m)} x^{\text{mdeg}(g_m)} g_m$$

$$= \frac{x^\delta}{\text{LT}(g_e)} g_e - \frac{x^\delta}{\text{LT}(g_m)} g_m$$

$$= x^{\delta - (\text{mdeg}(g_e) \vee \text{mdeg}(g_m))} \left( \frac{x^{\text{mdeg}(g_e) \vee \text{mdeg}(g_m)}}{\text{LT}(g_e)} g_e - \frac{x^{\text{mdeg}(g_e) \vee \text{mdeg}(g_m)}}{\text{LT}(g_m)} g_m \right)$$

$$= x^{\delta - (\text{mdeg}(g_e) \vee \text{mdeg}(g_m))} \cdot S(g_e, g_m)$$

Wegen (ii) lässt sich  $S(g_e, g_m)$  durch  $g_1, \dots, g_s$  ohne Rest teilen,  
d.h.

$$S(g_e, g_m) = \sum_{t=1}^s a_{e,m,t} g_t$$

wobei

mit gewissen  $a_{e,m,t} \in k[x_1, \dots, x_n]$  und  
 $\text{mdeg}(a_{e,m,t} g_e) \leq \text{mdeg}(S(g_e, g_m)) \leq \text{mdeg}(g_e) \vee \text{mdeg}(g_m)$

Zusammenfassend erhalten wir:

$$f = \sum_{\ell, m \in I} \sum_{t=1}^s c_{\ell, m} x^{\delta - (\text{mdeg}(g_\ell) \vee \text{mdeg}(g_m))} - a_{\ell, m_1} + g_t$$

$$+ \sum_{i \in I} (h_i - LT(h_i)) \cdot g_i + \sum_{j \in Y} h_j g_j$$

mit  $\text{mdeg} \geq \delta$  für jeden einzelnen Term.

$\Rightarrow f$  hat eine Darstellung

$$f = \sum_{i=1}^s \tilde{h}_i \cdot g_i \quad \text{mit } \tilde{h}_1, \dots, \tilde{h}_s \in k[x_1, \dots, x_n]$$

mit  $\text{mdeg}(\tilde{h}_i g_i) \leq \delta$   
für alle  $i \in \{1, \dots, s\}$

$\Rightarrow$  ↗ zur Wahl von  $\delta$ .

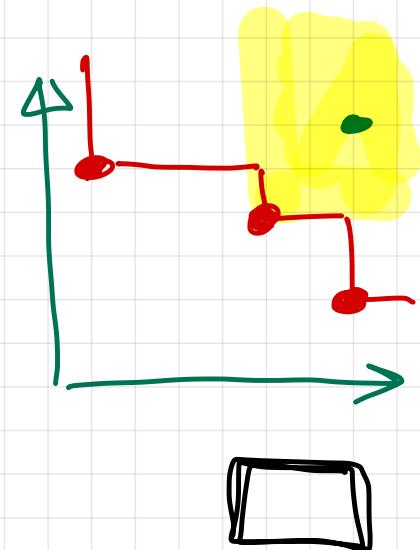
D.h. zeigt  $\text{mdeg}(f) = \delta$ .

$\Rightarrow \text{mdeg}(f) = \text{mdeg}(h_i g_i)$  hier ein  $i \in \{1, \dots, r\}$  (3)

$\Rightarrow \text{mdeg}(f) = \text{mdeg}(h_i) + \text{mdeg}(g_i)$

$\Rightarrow \text{mdeg}(f) \geq \text{mdeg}(g_i)$

$\Rightarrow LT(f) \in \langle LT(g_1), \dots, LT(g_s) \rangle$



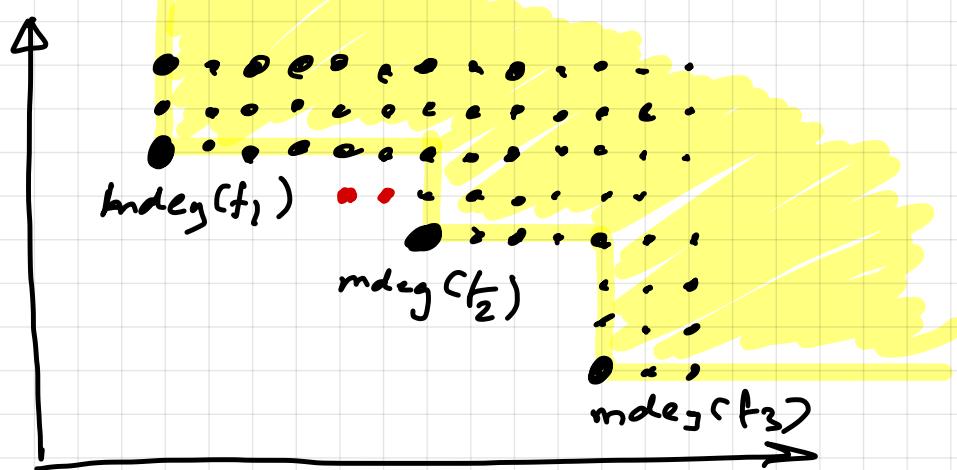
## 2.6. Der Algorithmus von Buchberger

$$I = \langle f_1, \dots, f_m \rangle \xrightarrow{\text{Algorithmus}}$$

Algorithmus

$$I = \langle g_1, \dots, g_s \rangle$$

Gröbnerbasis



2.6.1. Theorem. Es gibt einen Algorithmus, der für gegebene

$f_1, \dots, f_s \in k[x_1, \dots, x_n] \setminus \{0\}$  eine Gröbnerbasis von  $\langle f_1, \dots, f_s \rangle$  konstruiert.

Beweis: Der Algorithmus:

Gröbner-Basis ( $f_1, \dots, f_s$ )

Annahme:  $f_1, \dots, f_s \in k[x_1, \dots, x_n] \setminus \{0\}$

Ergebnis: Rückgabe einer Gröbnerbasis von  $\langle f_1, \dots, f_s \rangle$ .

1:  $G := (f_1, \dots, f_s)$

2: while True

3: Sei  $R$  die Liste aller Reste  $\text{Rem}(S(g, \tilde{g}); G)$

mit  $g$  und  $\tilde{g}$  aus  $G$ , die keine Nullpolynom enth.

4: If  $R$  leere Liste :

5:     return  $G$

6:     end

7: Für  $R$  zu  $G$  hinz.

8: end

Zu jeder Zeit der Ausführung gilt  $\langle G \rangle = \langle f_1, \dots, f_s \rangle$ . (33)

Wir starten mit  $G = \langle f_1, \dots, f_s \rangle$  und entfernen die Polynome aus  $G$ .  $\Rightarrow \langle f_1, \dots, f_s \rangle \subseteq \langle G \rangle$ .

Andererseits ist das Polynom  $S(G, \tilde{g})$  im Ideal von  $\langle G \rangle$  und somit auch  $\text{Res}(S(G, \tilde{g}); G)$

Das zeigt, dass beim Hinzufügen der neuen Polynome zu  $G$  das Ideal  $\langle G \rangle$  nicht größer wird.

Das zeigt  $\langle f_1, \dots, f_s \rangle = \langle G \rangle$ .