# Multigrad

## **Definition** Multigrad, führender Term

Sei $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{F}[x_1, \ldots, x_n]$ und sei $>$ eine Monomordnung.

1. Der *Multigrad* von $f$ ist $\text{multigrad}(f) = \max\{\alpha \in \mathbb{N}_0^n \mid a_\alpha \neq 0\}$.
2. Der *führende Koeffizient* von $f$ ist $LC(f) = a_{\text{multigrad}(f)}$.
3. Das *führende Monom* von $f$ ist $LM(f) = x^{\text{multigrad}(f)}$.
4. Der *führende Term* von $f$ ist $LT(f) = LC(f) \cdot LM(f)$.

**Bsp:** Sei $f = x^2yz^3 + 2x^3 + 3y^2z$. Dann gilt für $>_{lex}$

$\text{multigrad}(f) = (3,0,0)$, $LC(f) = 2$, $LM(f) = x^3$ und $LT(f) = 2x^3$.

## **Satz** Eigenschaften des Multigrads

Seien $f, g \in \mathbb{F}[x_1, \ldots, x_n] \setminus \{0\}$. Dann gilt:

1. $\text{multigrad}(fg) = \text{multigrad}(f) + \text{multigrad}(g)$.
2. $\text{multigrad}(f+g) \leq \max\{\text{multigrad}(f), \text{multigrad}(g)\}$ für $f + g \neq 0$.

**Beweis:** Übungsaufgabe.

# High-Level Beschreibung für Division in $\mathbb{F}[x_1, \ldots, x_n]$

**Ziel:** Algorithmus für Polynomdivision in $\mathbb{F}[x_1, \ldots, x_n]$.

**Gegeben:** $f, f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$

**Gesucht:** Darstellung $f = a_1 f_1 + \ldots + a_m f_m + r$ mit $a_1, \ldots, a_m, r \in \mathbb{F}[x_1, \ldots, x_n]$ und keiner der Terme in $r$ ist teilbar von einem der Terme $LT(f_1), \ldots, LT(f_m)$.

## **Algorithmus** High-Level Beschreibung Polynomdivision

EINGABE: $f, f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$

1. Teile sukzessive durch die Polynome $f_1, \ldots, f_m$ mit Rest $r$.
2. Falls $r \neq 0$ und $r$ nicht weiter teilbar, entferne $LM(r)$ und iteriere.

AUSGABE: $f = a_1 f_1 + \ldots + a_m f_m + r$

**Bsp:** Wir verwenden lexikographische Ordnung.

- Sei $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y - 1$.
- $f : f_1 = x + y$ mit Rest $r = x + y^2 + y$. Wir entfernen $x$ aus $r$.
- $(y^2 - y) : f_2 = y + 2$ mit Rest $r = 2$. Wir entfernen 2 aus $r$.
- Wir erhalten insgesamt $f = (x + y) \cdot f_1 + 1 \cdot f_2 + x + 2$.

# Divisionsalgorithmus für $\mathbb{F}[x_1, \ldots, x_n]$

## Algorithmus DIVISION

EINGABE: $f, f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$

1. Setze $p := f, r := 0$ und $a_1 := 0, \ldots, a_m := 0$.
2. WHILE $p \neq 0$
   1. Falls $LT(f_i)$ teilt $LT(p)$, setze $a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$ und $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i$. (Teste Teilbarkeit von $LT(p)$ in der Reihenfolge $f_1, \ldots, f_m$.)
   2. Sonst setze $p := p - LT(p)$ und $r := r + LT(p)$.

AUSGABE: $f = a_1 f_1 + \ldots + a_m f_m + r$

**Korrektheit:**

- Invariante $f = a_1 f_1 + \ldots + a_m f_m + p + r$ gilt in Schritt 1.
- Schritt 2.1 erhält die Invariante, falls $LT(f_i)$ den Term $LT(p)$ teilt, da
$$a_i f_i + p = (a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}) f_i + p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i.$$
- Schritt 2.2 erhält die Invariante: $p + r = (p - LT(p)) + (r + LT(p))$.

# Divisionsalgorithmus für $\mathbb{F}[x_1, \ldots, x_n]$

**Terminierung:**

- z.z.: Modifikationen verringern $\mathrm{multigrad}(p)$ oder erzeugen $p = 0$.
- Schritt 2.1 eliminiert $LT(p)$ mittels $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i$.
- Schritt 2.2 eliminiert ebenfalls $LT(p)$ mittels $p := p - LT(p)$.
- Damit verringert sich der Multigrad in Schritt 2.1 und in Schritt 2.2.
- Monomordnung: Die Sequenz der Multigrade muss terminieren.
- D.h. wir erhalten $p = 0$ und damit $f = a_1 f_1 + \ldots + a_m f_m + r$.

# Reihenfolge ist wichtig

**Bsp:** Wie zuvor $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ und $f_2 = y - 1$.

- Wir vertauschen aber nun die Reihenfolge in $f_2, f_1$ bei der Division.
- Wir erhalten $f : f_2 = x^2 + xy + x + y + 1$ mit Rest $p = 1$.
- Dies liefert die Darstellung

$$f = (x^2 + xy + x + y + 1) \cdot f_2 + 0 \cdot f_1 + 1.$$

- Bei Reihenfolge $(f_1, f_2)$ erhielten wir dagegen die Darstellung

$$f = (x + y) \cdot f_1 + (y + 2) \cdot f_2 + (x + 2).$$

- D.h. der Rest $r$ hängt von der Reihenfolge der Division ab.

# Idealzugehörigkeit

**Idealzugehörigkeit:**

$f \in \langle f_1, \ldots, f_m \rangle$ falls $f = a_1 f_1 + \ldots + a_m f_m$. D.h. falls $r = 0$.

**Bsp:** Wir betrachten $f = xy^2 - x$, $f_1 = xy + 1$ und $f_2 = y^2 - 1$.

- Mit lexikographischer Ordnung und Reihenfolge $(f_1, f_2)$ erhalten wir
$$f = y \cdot f_1 + 0 \cdot f_2 - x - y.$$
- Reihenfolge $(f_2, f_1)$ liefert aber
$$f = x \cdot f_2 + 0 \cdot f_1.$$
- D.h. $f$ ist im Ideal $\langle f_1, f_2 \rangle$.
- Allerdings liefert nur $(f_2, f_1)$ die hinreichende Bedingung $r = 0$.

**Ziel:**

- Definiere geeignete Generatormenge $G$ für $I = \langle f_1, \ldots, f_m \rangle$.
- Beim Teilen durch $G$ soll der Rest $r$ eindeutig bestimmt sein.
- Rest $r = 0$ soll äquivalent zur Zugehörigkeit im Ideal $I$ sein.
- Sogenannte Gröbnerbasen sind geeignete Generatormengen.

# Monomideal

## **Definition** Monomideal

Ein Ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ heißt *Monomideal* falls eine (unendliche) Menge $A \subseteq \mathbb{N}_0^n$ existiert, so dass $I$ aus Polynomen der Form $\sum_{\alpha \in A} h_\alpha x^\alpha$ besteht. Wir schreiben dann $I = \langle x^\alpha \mid \alpha \in A \rangle$.

**Bsp:** Für $A = \{(1,4),(2,2),(3,1)\}$ erhalten wir $I = \langle xy^4, x^2y^2, x^3y \rangle$.

## **Satz** Teilbarkeitssatz

Sei $I = \langle x^\alpha \mid \alpha \in A \rangle$ ein Monomideal. Ein Monom $x^\beta$ liegt in $I$ gdw $x^\alpha$ teilt $x^\beta$ für ein $\alpha \in A$.

**Beweis:**

- $\Leftarrow$: Falls $x^\beta = x^\gamma \cdot x^\alpha$, dann folgt $x^\beta \in I$.
- $\Rightarrow$: Sei $x^\beta \in I$, d.h. $x^\beta = \sum_i h_i x^{\alpha^{(i)}}$ mit $h_i \in \mathbb{F}[x_1, \ldots, x_n]$, $\alpha^{(i)} \in A$.
- Multipliziere $h_i x^{\alpha^{(i)}}$ aus. Jedes Monom ist teilbar durch ein $x^{\alpha^{(i)}}$.
- Die Summe kollabiert aber zu einem einzigen Monom $x^\beta$.
- Damit muss auch das Monom $x^\beta$ durch ein $x^{\alpha^{(i)}}$ teilbar sein.

# Gleichheit von Monomidealen

## **Satz** Darstellung aus Monomen

Sei $I$ ein Monomideal und $f \in \mathbb{F}[x_1, \ldots, x_n]$. Dann gilt $f \in I$ gdw $f$ eine $\mathbb{F}$-Linearkombination von Monomen in $I$ ist.

**Beweis:**

- $\Rightarrow$: Sei $f = \sum_i h_i x^{\alpha(i)}$.
- Ausmultiplizieren von $h_i x^{\alpha(i)}$ liefert Monome der Form $cx^\gamma$ mit $c \in \mathbb{F}$ und $x^{\alpha(i)} \mid x^\gamma$. Nach Teilbarkeitssatz ist $x^\gamma$ ein Monom in $I$.
- Damit können wir $f$ in der gewünschten Form schreiben
$$f = \sum_i c_i x^{\gamma(i)} \text{ mit } c_i \in \mathbb{F},\ x^{\gamma(i)} \in I.$$
- $\Leftarrow$: Folgt aus der Abgeschlossenheit von $I$ gegenüber Addition.

## **Korollar** Gleichheit von Monomidealen

Zwei Monomideale sind gleich gdw sie dieselben Monome enthalten.

# Dicksons Lemma

## **Lemma** Dicksons Lemma

Jedes Monomideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ besitzt eine endliche Basis $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(m)} \rangle$.

**Beweis** per Induktion über die Anzahl der Variablen $n$:

- $n = 1$: $I = \langle x_1^\alpha \mid \alpha \in A \rangle$. Sei $\beta$ das kleinste Element in $A \subseteq \mathbb{N}_0$.
- Daher gilt $x_1^\beta \mid x_1^\alpha$ für alle $\alpha \in A$. D.h. $I = \langle x_1^\beta \rangle$.
- $n - 1 \rightarrow n$: Wir verwenden die Variablen $x_1, \ldots, x_{n-1}, y$.
- D.h. Monome besitzen die Form $x^\alpha y^t$ mit $\alpha \in \mathbb{N}_0^{n-1}$ und $t \in \mathbb{N}_0$.
- Sei $J$ die Projektion von $I$ auf $\mathbb{F}[x_1, \ldots, x_{n-1}]$. D.h. $J$ wird generiert von denjenigen Monomen $x^\alpha$, für welche $x^\alpha y^t \in I$ für ein $t \geq 0$.
- IV: Wir schreiben $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(m)} \rangle$. Für $i = 1, \ldots, m$ gilt $x^{\alpha(i)} y^{t_i} \in I$ für ein festes $t_i \geq 0$. Sei $t = \max_i\{t_i\}$.
- Für jedes feste $k = 0, \ldots, t-1$ definiere $J_k \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}]$ als die Projektion derjenigen Monome in $I$, die genau $y^k$ enthalten.

# Dicksons Lemma

**Beweis:** (Fortsetzung)

- Nach IV: $J_k = \langle x^{\alpha_k^{(1)}}, \ldots, x^{\alpha_k^{(m_k)}} \rangle$ für $k = 0, \ldots, t-1$.
- Wir behaupten, dass $I$ von folgender Monomliste $L$ generiert wird.

$$\begin{array}{rlll} \text{aus } J: & x^{\alpha^{(1)}} y^t, & \ldots & , x^{\alpha^{(m)}} y^t \\ \text{aus } J_0: & x^{\alpha_0^{(1)}} y^0, & \ldots & , x^{\alpha_0^{(m_0)}} y^0 \\ & \vdots & & \vdots \\ \text{aus } J_{t-1}: & x^{\alpha_{t-1}^{(1)}} y^{t-1}, & \ldots & , x^{\alpha_{m-1}^{(m_{t-1})}} y^{t-1} \end{array}$$

- $\langle L \rangle \subseteq I$: Die Monome in unserer Liste $L$ sind alle in $I$. Dies folgt für die Elemente $x^{\alpha_k^{(i)}} y^k$ nach Konstruktion der Elemente in $J_k$.
- Für die Elemente $x^{\alpha^{(i)}} y^t$ gilt dies aufgrund der Maximalität von $t$.
- $I \subseteq \langle L \rangle$: Jedes $x^\alpha y^p \in I$ wird von einem Listenmonom geteilt.
- Sei $p \geq t$. Dann teilt ein $x^{\alpha^{(i)}} y^t$ nach Konstruktion von $J$.
- Sei $p < t$. Dann teilt ein $x^{\alpha_p^{(i)}} y^p$ nach Konstruktion von $J_p$.
- D.h. $\langle L \rangle$ und $I$ enthalten dieselben Monome und sind daher gleich.

# Idealzugehörigkeit in Monomidealen

## **Lemma** Dicksons Lemma (Teil II)

Jedes Monomideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ besitzt eine endliche Basis $I = \langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}} \rangle$ mit $a^{(i)} \in A$.

**Beweis:** Übungsaufgabe.

## **Satz** Idealzugehörigkeit in Monomidealen

Sei $I = \langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}} \rangle$ ein Monomideal. Dann gilt $f \in I$ gdw $f$ bei Division durch $x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}$ Rest 0 lässt.

**Beweis:**

- $\Leftarrow$: Aus $f = h_1 \cdot x^{\alpha^{(1)}} + \ldots + h_m \cdot x^{\alpha^{(m)}} + 0$ folgt $f \in I$.
- $\Rightarrow$: Nach *Satz zur Darstellung aus Monomen* folgt, dass $f \in I$ gwd
$$f = \sum_i c_i x^{\gamma^{(i)}} \text{ mit } x^{\gamma^{(i)}} \in I.$$
- Andererseits ist $x^{\gamma^{(i)}} \in I$ gwd $x^{\alpha^{(j)}}$ teilt $x^{\gamma^{(i)}}$ für ein $j \in [m]$.
- Damit wird jeder Term in $f$ von einem der $x^{\alpha^{(j)}}$ geteilt.
- Sukzessives Teilen von $f$ durch $x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}$ liefert also Rest 0.

# Das Ideal der führenden Terme

## **Definition** Ideal der führenden Terme

Sei $I \subseteq \mathbb{F}[x_1, \ldots, x_n] \setminus \{0\}$ ein Ideal, $LT(I)$ die Menge führender Terme

$$LT(I) = \{cx^\alpha \mid \text{es existiert } f \in I \text{ mit } LT(f) = cx^\alpha\}.$$

Dann heißt $\langle LT(I)\rangle$ das *Ideal der führenden Monome von* $I$.

**Anmerkung:**

- Sei $I = \langle f_1, \ldots, f_m\rangle$. Es gilt $LT(f_i) \in LT(I) \subseteq LT(I)$ für alle $i \in [m]$.
- Daher folgt $\langle LT(f_1), \ldots, LT(f_n)\rangle \subseteq \langle LT(I)\rangle$.
- Andererseits kann $LT(I)$ weitere Element enthalten.
- Sei $I = \langle f_1, f_2\rangle$ mit $f_1 = x^3 - 2xy$ und $f_2 = x^2y + x - 2y^2$.
- Es gilt $x^2 \in I$ wegen $x^2 = -y \cdot f_1 - x \cdot f_2$. D.h. $x^2 \in \langle LT(I)\rangle$.
- Aber $x^2$ wird weder von $LT(f_1) = x^3$ noch von $LT(f_2) = x^2y$ geteilt.
- Daraus folgt, dass $x^2$ nicht im Monomideal $\langle LT(f_1), LT(f_2)\rangle$ ist.

# Existenz einer Gröbnerbasis

## **Definition** Gröbnerbasis

Eine Menge $G = \{g_1, \ldots, g_m\} \subseteq I$ heißt *Gröbnerbasis* falls

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_n) \rangle.$$

## **Satz** Existenz einer Gröbnerbasis

Sei $I$ ein Ideal. Dann ist $\langle LT(I) \rangle$ ein Monomideal und es existiert eine Gröbnerbasis $\{g_1, \ldots, g_m\} \subseteq I$ mit $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle$.

**Beweis:**

- Es gilt $\langle \{LT(g) \mid g \in I \setminus \{0\}\} \rangle = \langle \{LM(g) \mid g \in \setminus \{0\}\} \rangle$.
- Die führenden Monome von $I$ generieren aber ein Monomideal.
- Dickson's Lemma: $\langle LT(I) \rangle$ wird endlich generiert, d.h.
$$\langle LT(I) \rangle = \langle LM(g_1), \ldots, LM(g_m) \rangle \text{ für } g_1, \ldots, g_m \in I.$$
- Aus obiger Gleichung folgt $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle$.

# Hilbert Basissatz

## Satz Hilbert Basissatz

Jedes Ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ wird endlich generiert, d.h.

$$I = \langle g_1, \ldots, g_m \rangle \text{ für } g_1, \ldots, g_m \in I.$$

**Beweis:**

- Falls $I = \{0\}$, verwende 0 als Generator. Sei also $I \neq \{0\}$.
- Wir wissen, dass $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle$ für $g_i \in I$.
- Behauptung: $I = \langle g_1, \ldots, g_m \rangle$. Es gilt $\langle g_1, \ldots, g_m \rangle \subseteq I$, da $g_i \in I$.
- $I \subseteq \langle g_1, \ldots, g_m \rangle$: Sei $f \in I$ beliebig.
- Teilen von $f$ durch $g_1, \ldots, g_m$ liefert $f = a_1 g_1 + \ldots + a_m g_m + r$.
- Kein Term von $r$ wird von einem der $LT(g_1), \ldots, LT(g_m)$ geteilt.
- Angenommen $r \neq 0$. Es gilt $r = f - a_1 g_1 - \ldots - a_m g_m \in I$.
- Aus $r \in I$ folgt $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle$.
- Dann muss aber nach Teilbarkeitskeitssatz $LT(r)$ von einem der Terme $LT(g_i)$ geteilt werden. (Widerspruch)
- D.h. es folgt $r = 0$ und damit $f \in \langle g_1, \ldots, g_m \rangle$.