Multigrad

Definition Multigrad, führender Term

Sei $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{F}[x_1, \ldots, x_n] \setminus \{0\}$ 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 f 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 $f = (x + y) \cdot f_1 + (y + 2) \cdot f_2 + x + 2$.

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: $p + r = (p - LT(p)) + (r + LT(p))$.
- Bei Terminierung gilt $p = 0$. Damit besitzt f die gewünschte Form.

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

Terminierung:

- z.z.: Modifikationen verringern $\text{multigrad}(p)$ oder erzeugen $p = 0$.
- Schritt 2.1 eliminiert $LT(p)$ mittels $p := p - \frac{\text{LT}(p)}{\text{LT}(f_i)} \cdot f_i$.
- 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^β liegt in I gdw x^α teilt x^β 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^β.
- Damit muss auch das Monom x^β 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 $f = \sum_i h_i x^{\alpha(i)} \in I$.
- Ausmultiplizieren von $h_i x^{\alpha(i)}$ liefert Monome der Form cx^γ mit $c \in \mathbb{F}$ und $x^{\alpha(i)} \mid x^\gamma$. Nach Teilbarkeitssatz ist x^γ 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.