Polynomdivision

Definition führender Term

Sei $f = a_m x^m + \ldots + a_0 \in \mathbb{F}[x]$. Dann bezeichnen wir den *führenden Term* von f mit $LT(f) = a_m x^m$.

Anmerkung:

- Für $f, g \in \mathbb{F}[x]$ gilt: $\text{grad}(f) \leq \text{grad}(g) \Leftrightarrow \text{LT}(f)$ teilt $\text{LT}(g)$.

Algorithmus Polynomdivision

EINGABE: $f, g \in \mathbb{F}[x]$ mit $\text{grad}(g) < \text{grad}(f)$

1. Setze $q := 0$ und $r := f$.
2. WHILE ($r \neq 0$ und $\text{LT}(g)$ teilt $\text{LT}(r)$)
   1. Setze $q := q + \frac{\text{LT}(r)}{\text{LT}(g)}$ und $r := r - \frac{\text{LT}(r)}{\text{LT}(g)} \cdot g$.

AUSGABE: q, r mit $\text{grad}(r) < \text{grad}(g)$ und $f = qg + r$

Invariante: $f = qg + r = (q + \frac{\text{LT}(r)}{\text{LT}(g)}) \cdot g + r - \frac{\text{LT}(r)}{\text{LT}(g)} \cdot g$.

Jedes Ideal in $\mathbb{F}[x]$ wird von einem Polynom erzeugt.

Satz Jedes Ideal in $\mathbb{F}[x]$ ist ein Hauptideal.

Für jedes Ideal I in $\mathbb{F}[x]$ gilt $I = \langle f \rangle$ für ein $f \in \mathbb{F}[x]$, wobei f eindeutig ist bis auf Multiplikation mit Konstanten ungleich Null.

Beweis:

- Sei $I = \{0\}$, dann gilt $I = \langle 0 \rangle$.
- Andernfalls wähle $f \in I \setminus \{0\}$ minimalen Grads.
- Behauptung: $I = \langle f \rangle$. Es gilt $\langle f \rangle \subseteq I$, da I ein Ideal ist.
- $I \subseteq \langle f \rangle$: Sei $g \in I$ beliebig. Wir berechnen q, r mit
$$g = qf + r \text{ und } \mathrm{grad}(r) < \mathrm{grad}(f).$$
- Da I ein Ideal ist, gilt $qf \in I$ und ferner $r = g - qf \in I$.
- Wegen $\mathrm{grad}(r) < \mathrm{grad}(f)$, folgt $r = 0$ aufgrund von f's Minimalität.
- Daher gilt $g = qf \in \langle f \rangle$.

Jedes Ideal in $\mathbb{F}[x]$ wird von einem Polynom erzeugt.

Beweis der Eindeutigkeit:

- Angenommen $\langle f \rangle = \langle g \rangle$.
- Aus $f \in \langle g \rangle$ folgt $f = hg$ für ein $h \in \mathbb{F}[x]$.
- Damit gilt $\text{grad}(f) = \text{grad}(h) + \text{grad}(g)$, d.h. $\text{grad}(g) \leq \text{grad}(f)$.
- Vertauschen von f und g liefert analog $\text{grad}(f) \leq \text{grad}(g)$.
- Damit gilt $\text{grad}(g) = \text{grad}(f)$ und f, g unterscheiden sich durch Multiplikation mit einem konstanten Polynom h, $\text{grad}(h) = 0$.

Definition Hauptideal

Ein Ideal, das von einem Polynom erzeugt wird, heißt *Hauptideal*.

Problem:
Wie finden wir z.B. im Hauptideal $\langle x^4 - 1, x^6 - 1 \rangle$ einen Generator?

Der ggT ist ein Generator

Satz ggT ist Generator

Seien $f, g \in \mathbb{F}[x]$. Dann gilt $\langle f, g \rangle = \langle \mathrm{ggT}(f, g) \rangle$.

Beweis:

- Jedes Ideal I in $\mathbb{F}[x]$ ist ein Hauptideal.
- D.h. $I = \langle f, g \rangle = \langle h \rangle$ für ein $h \in \mathbb{F}[x]$.
- Der Generator h ist ein gemeinsamer Teiler von f, g, da $f, g \in \langle h \rangle$.
- Um zu zeigen, dass $h = \mathrm{ggT}(f, g)$, müssen wir zeigen, dass jeder gemeinsame Teiler von f, g auch h teilt und h somit der ggT ist.
- Sei p ein beliebiger gemeinsamer Teiler von f, g.
- D.h. $f = ap$ und $g = bp$ für $a, b \in \mathbb{F}[x]$.
- Wegen $h \in \langle f, g \rangle$ existieren $c, d \in \mathbb{F}[x]$ mit $h = cf + dg$. Es folgt
$$h = cap + dbp = (ca + dp)p.$$
- Damit teilt p das Polynom h, und es muss $h = \mathrm{ggT}(f, g)$ gelten.

Beispiele für Basisdarstellung und Idealzugehörigkeit

Bsp Basisdarstellung:

- Wir berechnen einen Generator von $I = \langle x^4 - 1, x^6 - 1 \rangle$.
- Der Euklidische Algorithmus für Polynome liefert
$$\mathrm{ggT}(x^4 - 1, x^6 - 1) = x^2 - 1.$$
- Damit gilt $I = \langle x^2 - 1 \rangle$.

Bsp Idealzugehörigkeit:

- Sei $I = \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$. Ist $x^2 + 2x + 1 \in I$?
- Es gilt $\mathrm{ggT}(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = x - 1$. D.h. $I = \langle x - 1 \rangle$.
- Division mit Rest liefert $x^2 + 2x + 1 = (x + 3)(x - 1) + 4$.
- D.h. $x^2 + 2x + 1$ ist nicht in I, da es nicht von $x - 1$ geteilt wird.

Bsp Lösbarkeit:

$\{1\}$ ist die Lösungsmenge des polynomiellen Gleichungssystems

$$\left| \begin{array}{rcl} x^3 - 3x & = & -2 \\ x^4 & = & 1 \\ x^6 & = & 1 \end{array} \right|.$$

Monomordnung

Ziel: geeignete Monomordnung in $\mathbb{F}[x_1, \ldots, x_n]$

- Monomordnung soll verträglich mit der Polynommultiplikation sein.
- Wir identifizieren Monome $\mathbf{x}^\alpha := x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ mit ihrem Exponentenvektor $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.

Definition Monomordnung

Eine Monomordnung auf $\mathbb{F}[x_1, \ldots, x_n]$ ist eine Relation $>$ auf $\mathbb{N}_0^n$ mit:

1. $>$ ist eine totale Ordnung auf $\mathbb{N}_0^n$.
2. Seien $\alpha, \beta \in \mathbb{N}_0^n$ mit $\alpha > \beta$. Dann gilt für alle $\gamma \in \mathbb{N}_0^n$
$$\alpha + \gamma > \beta + \gamma$$ (Verträglichkeit mit Monommultiplikation).
3. $>$ ist noethersch, d.h. jede strikt fallende Sequenz $\alpha_1 > \alpha_2 > \ldots$ in $\mathbb{N}_0^n$ terminiert.

Bsp:

- Die Ordnung $\ldots > 2 > 1 > 0$ erfüllt obige Bedingungen auf $\mathbb{N}_0$.
- Damit ist die Gradordnung eine Monomordnung auf $\mathbb{F}[x]$.

Lexikographische Ordnung

Definition Lexikographische Ordnung $>_{lex}$

Seien $\alpha, \beta \in \mathbb{N}_0^n$. Definiere $\alpha >_{lex} \beta$, falls in $\alpha - \beta$ der von links erste Nicht-Null Eintrag positiv ist. Wir schreiben $x^\alpha >_{lex} x^\beta$ für $\alpha >_{lex} \beta$.

Bsp:

- $(2,3,4) >_{lex} (1,5,6)$ und $(2,3,4) >_{lex} (2,1,5)$.
- $(1,0,\ldots,0) >_{lex} (0,1,0\ldots,0) >_{lex} \ldots >_{lex} (0,\ldots,0,1)$, so dass
$$x_1 >_{lex} \ldots >_{lex} x_n.$$
- Wir verwenden ebenfalls $x >_{lex} y >_{lex} z$. Damit gilt z.B. $x > y^3z^5$.
- Für die alphabetische Ordnung $a > b > \ldots > z$, erhalten wir eine Wörterbuchsortierung mit z.B. Kryptanalyse > Kryptographie.

Satz

Die lexikographische Ordnung $>_{lex}$ ist eine Monomordnung.

Beweis: Übungsaufgabe.

Andere wichtige Monomordnungen

Definition Grad-Lexikographische Ordnung $>_{grlex}$

Seien $\alpha, \beta \in \mathbb{N}_0^n$ und $|\alpha| = \sum_i \alpha_i, |\beta| = \sum_i \beta_i$. Definiere $\alpha >_{grlex} \beta$ falls

$$|\alpha| > |\beta| \quad \text{oder} \quad |\alpha| = |\beta| \text{ und } \alpha >_{lex} \beta.$$

- **Bsp:** $(1,2,3) >_{grlex} (2,2,1)$ und $(1,3,2) >_{grlex} (1,2,3)$.
- Wie bei der lexikographischen Ordnung gilt $x_1 >_{grlex} \ldots >_{grlex} x_n$.

Definition Gradreverse-Lexikographische Ordnung $>_{grevlex}$

Seien $\alpha, \beta \in \mathbb{N}_0^n$. Wir definieren $\alpha >_{grevlex} \beta$ falls

$$|\alpha| > |\beta| \quad \text{oder} \quad |\alpha| = |\beta| \text{ und der von rechts erste Nicht-Null Eintrag in } \alpha - \beta \text{ ist negativ.}$$

- **Bsp:** $(1,2,4) >_{grevlex} (3,2,1)$ und $(1,2,3) >_{grevlex} (0,3,3)$.
- Man beachte, dass z.B. $xy^2z^3 >_{lex} y^3z^3$ und $xy^2z^3 >_{grevlex} y^3z^3$.
- Es gilt $x_1 >_{grevlex} \ldots >_{grevlex} x_n$.