Affine Varietät

Definition Affine Varietät

Seien $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ für einen Körper $\mathbb{F}$. Wir bezeichnen

$$\mathbf{V}(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ für } i = 1, \ldots, m\}$$

als die durch $f_1, \ldots, f_m$ definierte *affine Varietät*.

Anmerkungen:

- $\mathbf{V}(f_1, \ldots, f_m)$ ist die gemeinsame Nullstellenmenge von $f_1, \ldots, f_m$.
- Für Beispiele verwenden wir oft den Körper $\mathbb{F} = \mathbb{R}$, für die Kryptographie $\mathbb{F} = \mathbb{F}_p$.

Beispiele:

- $\mathbf{V}(x^2 + y^2 - 1)$ ist in $\mathbb{R}^2$ der Einheitskreis mit Mittelpunkt $\mathbf{0}$.
- $\mathbf{V}(x^2 + y^2 - z^2)$ liefert im $\mathbb{R}^3$ einen Doppelkegel.
- $\mathbf{V}(y - x^2, z - x^3)$ liefert als Schnitt zweier Flächen eine Kurve.
- $\mathbf{V}(xz, yz)$ ist die Vereinigung der (x, y)-Ebene mit der z-Achse.

Spezialfall Lineare Varietät

Definition Lineare Varietät

Sei $A \in \mathbb{F}^{m \times n}$ und $\mathbf{b} \in \mathbb{F}^m$. Dann definieren die Lösungen $\mathbf{V} = \{\mathbf{x} \in \mathbb{F}^n \mid A\mathbf{x} = \mathbf{b}\}$ eine *lineare Varietät*.

Anmerkungen:

- Sei $\mathrm{rang}(A) = r$. Dann besitzt **V** Dimension $n - r$. D.h. dim(**V**) wird von der Anzahl linear unabhängiger Gleichungen bestimmt.

Mehr Ziele:

1. **Lösbarkeit:**
   Gilt $\mathbf{V}(f_1, \ldots, f_m) \neq \emptyset$, d.h. ist $f_1 = \ldots = f_m = 0$ lösbar?
2. **Endlichkeit:**
   Ist $\mathbf{V}(f_1, \ldots, f_m)$ endlich? Können wir alle Lösungen bestimmen?

Abgeschlossenheit unter Vereinigung und Schnitt

Satz Abgeschlossenheit unter Vereinigung und Schnitt

Seien V, W affine Varietäten. Dann sind auch $V \cap W$ und $V \cup W$ affine Varietäten.

Beweis:

- Seien $V = \mathbf{V}(f_1, \ldots, f_m)$ und $W = \mathbf{W}(g_1, \ldots, g_\ell)$. Sei $\mathbf{x} \in V \cap W$.
- Dann verschwindet $\mathbf{x}$ sowohl auf $f_1, \ldots, f_m$ als auch auf $g_1, \ldots, g_\ell$.
- Damit verschwindet $\mathbf{x}$ auf $f_1, \ldots, f_m, g_1, \ldots, g_\ell$, d.h.
$$V \cap W = \mathbf{V}(f_1, \ldots, f_m, g_1, \ldots, g_\ell).$$
- Wir zeigen weiterhin: $V \cup W = \mathbf{V}(f_i g_j \mid i = 1, \ldots, m, j = 1, \ldots, \ell)$.
- $V \cup W \subseteq \mathbf{V}(f_i g_j)$: Sei $\mathbf{x} \in V \cup W$, oBda $\mathbf{x} \in V$.
- Dann verschwindet $\mathbf{x}$ auf allen f_i und damit auf allen $f_i g_j$.
- $\mathbf{V}(f_i g_j) \subseteq V \cup W$: Sei $\mathbf{x} \in \mathbf{V}(f_i g_j)$.
- Falls $\mathbf{x} \in V$, gilt $\mathbf{x} \in V \cup W$. Sonst folgt $f_{i'}(\mathbf{x}) \neq 0$ für ein $i' \in [m]$.
- Andererseits verschwindet $\mathbf{x}$ auf allen $f_{i'} g_j$.
- Damit verschwindet $\mathbf{x}$ auf allen g_j. D.h. es gilt $\mathbf{x} \in W$.

Ideal

Definition Ideal

Eine Menge $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ heißt *Ideal* falls Folgendes gilt.

1. $0 \in I$.
2. Falls $f, g \in I$, dann ist $f + g \in I$.
3. Für $f \in I$ und $h \in \mathbb{F}[x_1, \ldots, x_n]$ gilt $hf \in I$.

Definition Polynomideal

Seien $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$. Dann bezeichnen wir mit

$$\langle f_1, \ldots, f_m \rangle = \{\sum_{i=1}^m h_i f_i \mid h_i \in \mathbb{F}[x_1, \ldots, x_n]\}$$

das *von* $f_1, \ldots, f_m$ *generierte Ideal*.

Anmerkung: $I = \langle f_1, \ldots, f_m \rangle$ ist ein Ideal.

- Sei $I = \langle f_1, \ldots, f_m \rangle$. $0 \in I$ wegen $0 = \sum_i 0 \cdot f_i$.
- Seien $f = \sum_i p_i f_i$, $g = \sum q_i f_i \in I$ und $h \in \mathbb{F}[x_1, \ldots, x_n]$. Dann gilt
$$f + g = \sum_i (p_i + q_i) f_i \in I \text{ und } hf = \sum_i (hp_i) f_i \in I.$$

Varietäten und Ideale

Definition Basis eines Ideals

Ein Ideal I heißt *endlich erzeugt mit Basis* $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, falls $I = \langle f_1, \ldots, f_m \rangle$.

Satz Varietäten hängen nur vom Ideal ab

Seien $f_1, \ldots, f_m$ und $g_1, \ldots, g_\ell$ Basen eines Ideals I. Dann gilt

$$\mathbf{V}(f_1, \ldots, f_m) = \mathbf{V}(g_1, \ldots, g_\ell).$$

Beweis:

- Zeigen $\mathbf{V}(f_1, \ldots, f_m) \subseteq \mathbf{V}(g_1, \ldots, g_\ell)$. Umkehrung folgt analog.
- Sei $\mathbf{x} \in \mathbf{V}(f_1, \ldots, f_m)$. D.h. $f_i(\mathbf{x}) = 0$ für alle $i = 1, \ldots, m$.
- Da die f_i eine Basis von I bilden, können wir jedes g_j schreiben als $$g_j = \sum_{i=1}^{m} h_i f_i \text{ für } j = 1, \ldots, \ell.$$
- Damit gilt $g_j(\mathbf{x}) = \sum_i h_i(\mathbf{x}) \cdot f_i(\mathbf{x}) = 0$. D.h. $x \in \mathbf{V}(g_1, \ldots, g_\ell)$.

Bsp: Es gilt $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ (Übung), d.h. $\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}$.

Das Ideal einer Varietät

Frage: Welche Polynome verschwinden auf $\mathbf{V}(f_1, \ldots, f_m)$?

Definition Ideal einer Varietät

Sei V eine affine Varietät. Dann ist das Ideal von V definiert als

$$\mathbf{I}(V) = \{f \in \mathbb{F}[x_1, \ldots, x_n] \mid f(\mathbf{x}) = 0 \text{ für alle } x \in V\}.$$

Satz $\mathbf{I}(V)$ ist ein Ideal

Sei V eine affine Varietät. Dann ist $\mathbf{I}(V)$ ein Ideal.

Beweis:

- $0 \in \mathbf{I}(V)$, da das Nullpolynom auf allen Punkten verschwindet.
- Seien $f, g \in \mathbf{I}(V)$ und $h \in \mathbb{F}[x_1, \ldots, x_n]$. Für $\mathbf{x} \in V$ folgt
$$\underbrace{f(\mathbf{x})}_{=0} + \underbrace{g(\mathbf{x})}_{=0} = 0 \text{ und } h(\mathbf{x}) \cdot \underbrace{f(\mathbf{x})}_{=0} = 0.$$
- Damit gilt $f + g \in \mathbf{I}(V)$ und $hf \in \mathbf{I}(V)$.

Beispiel: Ideal einer Varietät

Bsp Ideal einer Varietät

$\mathbf{I}(\{(0,0)\}) = \langle x, y\rangle \subseteq \mathbb{F}[x,y]$.

Beweis:

- $\langle x, y\rangle \subseteq \mathbf{I}(\{(0,0)\})$: Sei $f \in \langle x, y\rangle$. Dann gilt
$$f(x,y) = h_1(x,y)\cdot x + h_2(x,y)\cdot y.$$
- Damit ist $f(0,0) = 0$ und es folgt $f \in \mathbf{I}(\{(0,0)\})$.
- $\mathbf{I}(\{(0,0)\}) \subseteq \langle x, y\rangle$: Sei $f \in \mathbf{I}(\{(0,0)\})$. Dann gilt
$$f(x,y) = \sum_{i,j} a_{ij}x^iy^j \text{ mit } f(0,0) = 0.$$
- Es folgt $a_{00} = 0$ und damit
$$f(x,y) = \left(\sum_{i,j,i>0} a_{ij}x^{i-1}y^j\right)\cdot x + \left(\sum_{j>0} a_{0j}y^{j-1}\right)\cdot y \in \langle x, y\rangle.$$

Polynome $\to$ Varietät $\to$ Ideal

Frage: Gilt $\langle f_1, \ldots, f_m \rangle = \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$? Antwort: Leider nicht.

Satz

Es gilt $\langle f_1, \ldots, f_m \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$, aber i. Allg. keine Gleichheit.

Beweis:

- Sei $f \in \langle f_1, \ldots, f_m \rangle$, d.h. $f = \sum_{i=1}^{n} h_i f_i$ für Polynome h_i.
- Die Polynome $f_1, \ldots, f_m$ verschwinden auf allen $\mathbf{x} \in \mathbf{V}(f_1, \ldots, f_m)$.
- Damit gilt $f(\mathbf{x}) = 0$ für $\mathbf{x} \in \mathbf{V}(f_1, \ldots, f_m)$, d.h. $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$.

- **Gegenbeispiel** für Gleichheit: $\mathbf{I}(\mathbf{V}(x^2, y^2)) \not\subseteq \langle x^2, y^2 \rangle$.
- Die Gleichungen $x^2 = y^2 = 0$ implizieren $\mathbf{V}(x^2, y^2) = \{(0,0)\}$.
- Aus dem Beispiel zuvor folgt $\mathbf{I}(\mathbf{V}(x^2, y^2)) = \mathbf{I}(\{(0,0)\}) = \langle x, y \rangle$.
- Es gilt aber $\langle x, y \rangle \not\subseteq \langle x^2, y^2 \rangle$, da z.B. x nicht in der Form $h_1 \cdot x^2 + h_2 \cdot y^2$ dargestellt werden kann.

Beziehung zwischen Varietäten und ihren Idealen

Satz

Seien $V, W \subseteq \mathbb{F}^n$ affine Varietäten. Dann gilt

1. $V \subseteq W$ gdw $\mathbf{I}(W) \subseteq \mathbf{I}(V)$.
2. $V = W$ gdw $\mathbf{I}(V) = \mathbf{I}(W)$.

Beweis:

- $\Rightarrow$: Sei $V \subseteq W$ und $f \in \mathbf{I}(W)$.
- Dann verschwindet f auf allen $\mathbf{x} \in W$ und damit auf allen $\mathbf{x} \in V$.
- Damit folgt $f \in \mathbf{I}(V)$.
- $\Leftarrow$: Sei $\mathbf{I}(W) \subseteq \mathbf{I}(V)$.
- Sei die affine Varietät W definiert durch die Polynome $f_1, \ldots, f_m$.
- Dann gilt $f_1, \ldots, f_m \in \mathbf{I}(W) \subseteq \mathbf{I}(V)$.
- D.h. $f_1, \ldots, f_m$ verschwinden insbesondere auf den Punkten aus V.
- Da W aus *allen* gemeinsamen Nst. der f_i besteht, folgt $V \subseteq W$.
- 2 folgt aus 1: $V = W$ gilt gdw $V \subseteq W$ und $W \subseteq V$ gdw $V = W$.

Interessante Probleme

Ziel: Löse die folgenden Probleme algorithmisch.

1. **Basisdarstellung:**
   Stelle jedes Ideal I mittels einer endlichen Basis $\langle f_1, \ldots, f_m \rangle$ dar.
2. **Idealzugehörigkeit:**
   Entscheide, ob f im Ideal $\langle f_1, \ldots, f_m \rangle$ liegt.
3. **Lösbarkeit von polynomiellen Gleichungssystemen:**
   Bestimme alle gemeinsamen Lösungen von

$$\left| \begin{array}{ccc} f_1 & = & 0 \\ & \vdots & \\ f_m & = & 0 \end{array} \right| .$$

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: $\mathrm{grad}(f) \leq \mathrm{grad}(g) \Leftrightarrow \mathrm{LT}(f)$ teilt $\mathrm{LT}(g)$.

Algorithmus Polynomdivision

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

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

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

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

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 $g = qf + r$.
- Da I ein Ideal ist, gilt $qf \in I$ und ferner $r = g - qf \in I$.
- Wegen $\deg(r) < \deg(f)$, folgt $r = 0$ aufgrund der Minimalität von f.
- 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 $\mathrm{grad}(f) = \mathrm{grad}(h) + \mathrm{grad}(g)$, d.h. $\mathrm{grad}(g) \leq \mathrm{grad}(f)$.
- Vertauschen von f und g liefert analog $\mathrm{grad}(f) \leq \mathrm{grad}(h)$.
- Damit gilt $\mathrm{grad}(g) = \mathrm{grad}(f)$ und f, g unterscheiden sich durch Multiplikation mit einem konstanten Polynom h, $\mathrm{grad}(h) = 0$.

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

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

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 $\gamma \in \mathbb{N}_0^n$

   $$\alpha + \gamma > \beta + \gamma \text{ (Verträglichkeit mit Monommultiplikation).}$$
3. $>$ ist eine Wohlordnung auf $\mathbb{N}_0^n$. D.h. jede nicht-leere Teilmenge von $\mathbb{N}_0^n$ enthält ein kleinstes Element.

Bsp:

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

Wohlordnung

Anmerkung:
Wohlordnung wird uns Terminierung von Algorithmen liefern.

Lemma zur Wohlordnung

Eine Relation $>$ ist eine Wohlordnung gdw jede strikt fallende Sequenz $\alpha_1 > \alpha_2 > \ldots$ in $\mathbb{N}_0^n$ terminiert.

Beweis:

- keine Wohlordung $\Rightarrow$ Sequenz terminiert nicht:
- Sei $S \subseteq \mathbb{N}_0^n$ eine Menge ohne minimales Element.
- Wähle $\alpha_1 \in S$. Da α_1 nicht minimal in S ist, existiert $\alpha_2 < \alpha_1$, usw.
- Sequenz terminiert nicht $\Rightarrow$ keine Wohlordung:
- Sei $\alpha_1 > \alpha_2 > \ldots$ eine Sequenz. Definiere $S = \{\alpha_i \mid i \in \mathbb{N}\}$.
- S besitzt kein minimales Element, d.h. $>$ ist keine Wohlordnung.

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. $x > y^3 z^5$.
- 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

$|\alpha| > |\beta|$ oder $|\alpha| = |\beta|$ und der von rechts erste Nicht-Null Eintrag in $\alpha - \beta$ 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 $x_1 >_{grevlex} \ldots >_{grevlex} x_n$.