

Charakterisierung von Gröbnerbasen

Satz Charakterisierung von Gröbnerbasen

Eine Menge $G = \{g_1, \dots, g_m\} \subseteq I$ ist eine Gröbnerbasis gdw für jedes $f \in I$ der Term $LT(f)$ von einem der $LT(g_i)$, $i = 1, \dots, m$ geteilt wird.

Beweis:

- \Rightarrow : Sei $G = \{g_1, \dots, g_m\}$ eine Gröbnerbasis, d.h.
$$\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_m) \rangle.$$
- Für jedes $f \in I$ gilt $LT(f) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_m) \rangle$.
- Nach Teilbarkeitssatz ist $LT(f) \in \langle LT(g_1), \dots, LT(g_m) \rangle$ gdw $LT(f)$ von einem der Terme $LT(g_i)$ geteilt wird.
- \Leftarrow : Sei $f \in I$ beliebig. Es gilt $LT(g_i) \mid LT(f)$ für ein $i \in [m]$.
- Daraus folgt $\langle LT(f) \rangle \subseteq \langle LT(g_1), \dots, LT(g_m) \rangle$.
- Da stets auch $\langle LT(g_1), \dots, LT(g_m) \rangle \subseteq \langle LT(I) \rangle$ gilt, folgt
$$\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_m) \rangle.$$

Beispiel einer Gröbnerbasis

Bsp: Gröbnerbasis. Wir verwenden lex-Ordnung in $\mathbb{R}[x, y, z]$.

- Sei $I = \langle g_1, g_2 \rangle = \langle x + z, y - z \rangle$. Zeigen: $\{g_1, g_2\}$ ist Gröbnerbasis.
- D.h. wir müssen zeigen, dass $\langle LT(g_1), LT(g_2) \rangle = \langle x, y \rangle = \langle LT(I) \rangle$.
- Es gilt offenbar $\langle x, y \rangle \subseteq \langle LT(I) \rangle$, bleibt $\langle LT(I) \rangle \subseteq \langle x, y \rangle$ zu zeigen.
- Sei $f \in I$. Wir müssen zeigen, dass $LT(f)$ von x oder y geteilt wird.
- Annahme: $f \in \mathbb{R}[z] \setminus \{0\}$.
- Wegen $f \in I$ verschwindet f auf $\mathbf{V}(x + z, y - z)$.
- D.h. f verschwindet auf allen Punkten $(-t, t, t) \in \mathbb{R}^3$. Das einzige Polynom $f \in \mathbb{R}[z]$ mit dieser Eigenschaft ist $z = 0$ (Widerspruch).
- D.h. jedes Polynom $f \in I$ enthält einen x oder einen y -Term.

ACC – Ascending Chain Condition

Satz Ascending Chain Condition (ACC)

Sei $I_1 \subseteq I_2 \subseteq \dots$ eine aufsteigende Kette von Idealen in $\mathbb{F}[x_1, \dots, x_n]$.
Dann existiert ein $N \geq 1$ mit $I_N = I_M$ für alle $M \geq N$.

Beweis:

- Wir definieren $I = \bigcup_{i=1}^{\infty} I_i$. Wir zeigen, dass I ein Ideal ist.
- Seien $f, g \in I$. Sei $f \in I_i$ und $g \in I_j$. ObdA $i \leq j$.
- Dann gilt $f, g \in I_j$ und damit $f + g \in I_j \subseteq I$.
- Analog folgt für $f \in I$, dass $f \in I_i$ für ein i und damit $hf \in I_i \subseteq I$.
- Da I ein Ideal ist, wird es endlich erzeugt. D.h. $I = \langle g_1, \dots, g_m \rangle$.
- Jeder Generator $g_j \in I$ ist in einem Ideal I_{j_i} . Sei $N = \max_i \{j_i\}$.
- Dann sind $g_1, \dots, g_m \in I_N$. Damit gilt

$$I = \langle g_1, \dots, g_m \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \dots \subseteq I.$$

Ideale definieren Varietäten

Definition Varietät eines Ideals $\mathbf{V}(I)$

Sei $I \subseteq \mathbb{F}[x_1, \dots, x_n]$ ein Ideal. Wir definieren

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \in \mathbb{F}^n \mid f(a_1, \dots, a_n) = 0 \text{ für alle } f \in I\}.$$

Satz Varietät eines Ideals $\mathbf{V}(I)$

$\mathbf{V}(I)$ ist eine Varietät. Insbesondere gilt für $I = \langle f_1, \dots, f_m \rangle$, dass

$$\mathbf{V}(I) = \mathbf{V}(f_1, \dots, f_m).$$

Beweis:

- $\mathbf{V}(I) \subseteq \mathbf{V}(f_1, \dots, f_m)$: Sei $(a_1, \dots, a_n) \in \mathbf{V}(I)$. Dann gilt $f(a_1, \dots, a_n) = 0$ für alle $f \in I$, d.h. insbesondere für $f_1, \dots, f_m \in I$.
- $\mathbf{V}(f_1, \dots, f_m) \subseteq \mathbf{V}(I)$: Sei $(a_1, \dots, a_n) \in \mathbf{V}(f_1, \dots, f_m)$ und $f \in I$.
- Wir schreiben $f = \sum_i h_i f_i$ und damit gilt

$$f(a_1, \dots, a_n) = \sum_{i=1}^m h_i(a_1, \dots, a_n) \cdot \underbrace{f_i(a_1, \dots, a_n)}_0 = 0.$$

Eindeutigkeit des Rests für Gröbnerbasen

Satz Eindeutigkeit des Rests

Sei $G = \{g_1, \dots, g_m\}$ eine Gröbnerbasis für $I \subseteq \mathbb{F}[x_1, \dots, x_n]$ und $f \in \mathbb{F}[x_1, \dots, x_n]$. Es existiert ein eindeutiger Rest r mit

- 1 Kein Term von r ist teilbar von einem der $LT(g_1), \dots, LT(g_m)$.
- 2 Es existiert ein $g \in I$ mit $f = g + r$.

Beweis:

- **Existenz:** Polynomdivision mit g_1, \dots, g_m liefert

$$f = \underbrace{a_1 g_1 + \dots + a_m g_m}_g + r, \text{ wobei } r \text{ Eigenschaft 1 besitzt.}$$

- **Eindeutigkeit:** Seien $r \neq r'$ Reste mit $f = g + r = g' + r'$.
- Es gilt $r - r' = g' - g \in I$, d.h.

$$LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_m) \rangle.$$

- Damit ist $LT(r - r')$ teilbar von einem $LT(g_i)$. D.h. einer der Terme von r oder r' wird von einem $LT(g_i)$ geteilt. (Widerspruch)

Man beachte: r ist eindeutig unabhängig von der Reihenfolge der g_i .

Idealzugehörigkeit mittels Gröbnerbasis

Satz Idealzugehörigkeit mittels Gröbnerbasis

Sei $G = \{g_1, \dots, g_m\}$ eine Gröbnerbasis für I . Es gilt $f \in I$ gdw f bei Division durch die Polynome in G Rest 0 lässt.

Beweis:

- \Leftarrow : Sei $f = a_1g_1 + \dots + a_mg_m$. Dann gilt $f \in \langle g_1, \dots, g_m \rangle = I$.
- \Rightarrow : Sei $f \in I$. Dann erfüllt die Wahl $g = f$ und $r = 0$ beide Eigenschaften des Satzes zuvor.
- Da der Rest r eindeutig bestimmt ist, muss $r = 0$ gelten.

Ziel: Konstruktion Gröbnerbasis

- Konstruiere für f_1, \dots, f_m eine Gröbnerbasis g_1, \dots, g_t mit
$$\langle f_1, \dots, f_m \rangle = \langle g_1, \dots, g_t \rangle.$$
- Erzeuge dazu eine Linearkombinationen g der f_i , deren führender Term *nicht* im durch die $LT(f_i)$ erzeugten Ideal ist.
- Wir eliminieren dazu die führenden Koeffizienten der f_i .
- Füge g zu f_1, \dots, f_m hinzu und iteriere.

Syzygien-Polynom

Definition kgV, S-Polynom (Syzygien-Polynom)

Seien $f, g \in \mathbb{F}[x_1, \dots, x_n]$ mit Multigraden $\alpha, \beta \in \mathbb{N}_0^n$.

- 1 Das *kleinste gemeinsame Vielfache* von $LM(f)$ und $LM(g)$ ist definiert als x^γ , wobei $\gamma = (\gamma_1, \dots, \gamma_n)$ mit $\gamma_i = \max_i\{\alpha_i, \beta_i\}$.
- 2 Das S-Polynom von f und g ist definiert als

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Bsp:

- Seien $f = x^3y^2 + x^4, g = 3x^4y + y^2 \in \mathbb{R}[x, y]$ in grlex-Ordnung.
- Es gilt $\alpha = (3, 2), \beta = (4, 1)$ und $\gamma = (4, 2)$. Damit ist


$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = xf - \frac{1}{3}yg = x^5 - \frac{1}{3}y^3.$$

Buchberger Kriterium

Satz Buchberger Kriterium

Sei I ein Ideal. Eine Basis $G = \{g_1, \dots, g_m\}$ ist eine Gröbnerbasis gdw für alle $i \neq j$ beim Teilen von $S(g_i, g_j)$ durch G der Rest 0 ist.

Beweisskizze:

- \Rightarrow : Sei G eine Gröbnerbasis.
- Da $S(g_i, g_j) \in I$ liefert die Teilung durch G Rest 0.
- \Leftarrow : Sei $f \in I$ beliebig. Wir müssen zeigen, dass
$$LT(f) \in \langle LT(g_1), \dots, LT(g_m) \rangle.$$
- Da $f \in I = \langle g_1, \dots, g_m \rangle$ gilt $f = \sum_i h_i g_i$. Daraus folgt
$$\text{multigrad}(f) \leq \max_i \{ \text{multigrad}(h_i g_i) \}.$$
- Müssen zeigen: $\text{multigrad}(f) = \max_i \{ \text{multigrad}(h_i g_i) \}$ für ein i .
- Damit $LT(g_i) \mid LT(f)$, woraus $LT(f) \in \langle LT(g_1), \dots, LT(g_m) \rangle$ folgt.
- Annahme: $\text{multigrad}(f) < \max_i \{ \text{multigrad}(h_i g_i) \}$. D.h. es werden Terme eliminiert. Dies kann nur durch S-Polynome geschehen.
- Aufgrund der Teilbarkeit der S-Polynome gilt $S(g_i, g_j) = \sum_k h'_k g_k$.
- D.h. wir können alle Eliminationen entfernen. (Widerspruch) 

Beispiel Gröbnerbasis

Bsp:

- Wir verifizieren erneut die Basis $f_1 = x + z$, $f_2 = y - z$ in $\mathbb{R}[x, y, z]$.
- Es gilt $S(f_1, f_2) = y \cdot f_1 - x \cdot f_2 = yz + xz$.
- Division mit f_1, f_2 liefert $S(f_1, f_2) = z \cdot f_1 + z \cdot f_2$.
- Damit ist $\{f_1, f_2\}$ wirklich eine Gröbnerbasis für $\langle f_1, f_2 \rangle$.

Buchberger Algorithmus

Algorithmus BUCHBERGER

EINGABE: $F = \{f_1, \dots, f_m\}$ mit $I = \langle f_1, \dots, f_m \rangle$

- 1 Setze $G := F$.
- 2 WHILE ($\exists g_i \neq g_j \in G$, so dass $S(g_i, g_j) : G$ Rest $r \neq 0$ lässt)
 - 1 $G := G \cup \{r\}$.

AUSGABE: Gröbnerbasis G für I mit $F \subseteq G$

Beispiel Gröbnerbasen-Berechnung

Bsp:

- Seien $f_1 = x^2y + xy$, $f_2 = xy^2 + 1 \in \mathbb{R}[x, y]$ in grlex-Ordnung.
- $S(f_1, f_2) = yf_1 - xf_2 = xy^2 - x$. Division liefert
$$S(f_1, f_2) = 1 \cdot f_2 - x - 1.$$
- Wir fügen $f_3 = -x - 1$ zur Basis hinzu.
- $S(f_1, f_3) = f_1 + xyf_3 = 0$ und $S(f_2, f_3) = f_2 + y^2f_3 = -y^2 + 1$.
- Wir fügen $f_4 = -y^2 + 1$ zur Basis hinzu.
- $S(f_1, f_4)$, $S(f_2, f_4)$, $S(f_3, f_4)$ verschwinden bei Basisdivision.
- D.h. $\{x^2y + xy, xy^2 + 1, -x - 1, -y^2 + 1\}$ ist Gröbnerbasis für I .

Notation für Ideale und Division

Sei $G = \{g_1, \dots, g_m\}$ und $f \in \mathbb{F}[x_1, \dots, x_n]$. Wir schreiben vereinfacht

$$\langle G \rangle = \langle g_1, \dots, g_m \rangle \text{ und } \langle LT(G) \rangle = \langle LT(g_1), \dots, LT(g_m) \rangle.$$

Wir notieren mit \bar{f}^G den Rest der Division von f durch G .

Korrektheit von BUCHBERGER

Satz

Algorithmus BUCHBERGER terminiert nach endlich vielen Schritten mit einer Gröbnerbasis.

Beweis:

- **Korrektheit:** Als Invariante gilt, dass G das Ideal I generiert.
- Sei $S(g_i, g_j) = \sum_i a_i g_i + r$. Da $S(g_i, g_j), \sum_i a_i g_i \in I$ ist auch $r \in I$.
- Wir fügen also nur Element aus I zu G hinzu.
- Buchberger Kriterium: G ist bei Terminierung eine Gröbnerbasis.
- **Terminierung:** Sei $G = \{g_1, \dots, g_m\}$.
- Sei $G' = G \cup \{r\}$ in Schritt 2.1. Da r in G aufgenommen wird, wird $LT(r)$ von keinem der $LT(g_i)$ geteilt. D.h.
$$\langle LT(G) \rangle \subset \langle LT(G') \rangle, \text{ da } G \subset G' \text{ und } LT(r) \in \langle LT(G') \rangle.$$
- Damit entsteht in Schritt 2.1 eine aufsteigende Kette von Idealen
$$\langle LT(G) \rangle \subset \langle LT(G') \rangle \subset \langle LT(G'') \rangle \subset \dots$$
- Nach ACC stabilisiert die Kette nach endlich vielen Schritten.

Minimale Gröbnerbasis

Beobachtung: Gröbnerbasen enthalten oft unnötige Generatoren.

Satz Elimination von Generatoren

Sei G eine Gröbnerbasis für I . Sei $g \in G$ mit $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$.
Dann ist $G \setminus \{g\}$ eine Gröbnerbasis von I .

Beweis:

- Da G eine Gröbnerbasis ist, gilt $\langle LT(G) \rangle = \langle LT(I) \rangle$.
- Wegen $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$ folgt
$$\langle LT(G \setminus \{g\}) \rangle = \langle LT(G) \rangle = \langle LT(I) \rangle.$$
- Damit ist auch $G \setminus \{g\}$ eine Gröbnerbasis.

Definition Minimale Gröbnerbasis

Wir nennen eine Gröbnerbasis G *minimal*, falls für alle $g \in G$ gilt:

- 1 $LT(g) \notin \langle LT(G \setminus \{g\}) \rangle$.
- 2 $LC(g) = 1$.

Minimierung einer Gröbnerbasis

Algorithmus MINIMIERE GRÖBNER

EINGABE: Gröbnerbasis B

- 1 Für alle $g \in G$: Falls $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$, setze $G := G \setminus \{g\}$.
- 2 Für alle $g \in G$: Setze $g := \frac{g}{LC(g)}$.

AUSGABE: minimale Gröbnerbasis

Beispiel: Gröbnerbasis $\{x^2y + xy, xy^2 + 1, -x - 1, -y^2 + 1\}$ (grlex)

- Wir können g_1 eliminieren, da $LT(g_1) = x^2y = -xy \cdot LT(g_3)$.
- Ferner können wir g_2 eliminieren, da $LT(g_2) = xy^2 = -x \cdot LT(g_4)$.
- Damit ist $\{x + 1, y^2 - 1\}$ eine minimale Gröbnerbasis.
- Leider sind minimale Gröbnerbasen nicht eindeutig.
- Die folgenden Basen sind ebenfalls minimal für die grlex-Ordnung
 $\{x + 1, y^2 + a(x + 1) - 1\}$ mit $a \in \mathbb{Z}$.

Reduzierte Gröbnerbasis

Definition reduzierte Gröbnerbasis

Wir nennen eine Gröbnerbasis G *reduziert*, falls für alle $g \in G$ gilt:

- 1 Kein Monom von g liegt in $LT(G \setminus \{g\})$.
- 2 $LC(g) = 1$.

Algorithmus REDUZIERE GRÖBNER

EINGABE: minimale Gröbnerbasis G

- 1 Für alle $g \in G$
 - 1 Sei $g' := \bar{g}^{G \setminus \{g\}}$.
 - 2 Setze $G := G \setminus \{g\} \cup \{g'\}$.

AUSGABE: reduzierte Gröbnerbasis G

Reduzierte Gröbnerbasis

Satz Korrektheit REDUZIERE GRÖBNER

Algorithmus REDUZIERE GRÖBNER berechnet eine reduzierte Gröbnerbasis.

Beweis:

- Wir bezeichnen ein Polynom $g \in G$ als reduziert, falls kein Monom von g in $\langle LT(G \setminus \{g\}) \rangle$ liegt (Eigenschaft 1).
- Ein reduziertes g bleibt reduziert, sofern sich die führenden Terme von G nicht ändern.
- In Schritt 1.1 gilt $LT(g') = LT(g)$, da aufgrund von G 's Minimalität $LT(g)$ von keinem der führenden Terme in $LT(G \setminus \{g\})$ geteilt wird.
- D.h. führende Terme bleiben unverändert und $\langle LT(G') \rangle = \langle LT(G) \rangle$.
- Damit ist G' in Schritt 1.2 ebenfalls eine minimale Gröbnerbasis.
- Da wir alle $g \in G$ reduzieren, ist G bei Terminierung reduziert.