Kapitel III: Algorithmische Grundlagen

6 Was sind Gröbner-Basen?

Im Folgenden sei K ein Körper und $P = K[x_1, \ldots, x_n]$.

Ziel

Effektive Berechnung von Polynomen und Polynomidealen, z.B. $f_1, \ldots, f_s, g \in P$. Gilt $g \in \langle f_1, \ldots, f_s \rangle$, d.h.

$$g = h_1 f_1 + \ldots + h_s f_s \quad \text{mit } h_1, \ldots, h_s \in P$$

6.1 Beispiel

Seien $f_1 = x^2 - y$ und $f_2 = xy - 1$ Polynome in $P = \mathbb{Q}[x, y]$. Gilt dann $1 \in \langle f_1, f_2 \rangle$, d.h. gibt es eine Darstellung $1 = g_1 f_1 + g_2 f_2$ mit $g_1, g_2 \in P$?

6.2 Definition

Sei $\mathbb{T}^n = \{x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$ die Menge der Terme. Eine vollständige Ordnungsrelation $<_\sigma$ (bzw. einfach σ) heißt eine **Termordnung** auf $\mathbb{T}^n$ wenn

1. sie mit der Multiplikation verträglich ist (d.h. $t_1 \leq_\sigma t_2 \Rightarrow t_1 t_3 \leq_\sigma t_2 t_3$)
2. es keine unendlich echt absteigende Kette mit $t_1 >_\sigma t_2 >_\sigma \ldots$ mit $t_1, t_2, \ldots \in \mathbb{T}^n$ gibt.

6.3 Beispiel

a) Definiert man $<_{\text{Lex}}$ durch

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} <_{\text{Lex}} x_1^{\beta_1} \ldots x_n^{\beta_n} \quad \Leftrightarrow \quad \begin{cases} \alpha_1 < \beta_1 & \text{oder} & & \\ \alpha_1 = \beta_1, & \alpha_2 < \beta_2 & \text{oder} & \\ \vdots & & \ddots & \\ \alpha_1 = \beta_1, & \ldots & \alpha_{n-1} = \beta_{n-1}, & \alpha_n \leq \beta_n \end{cases}$$

so erhält man die **lexikographische Termordnung**.

b) Definiert man $<_{\text{DegRevLex}}$ bzw. $<_{\text{DRL}}$ durch

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} <_{\text{DRL}} x_1^{\beta_1} \ldots x_n^{\beta_n}$$

$$\Leftrightarrow \quad \begin{cases} \alpha_1 + \ldots + \alpha_n > \beta_1 + \ldots + \beta_n & \text{oder} & & \\ \alpha_1 + \ldots + \alpha_n = \beta_1 + \ldots + \beta_n, & \alpha_n > \beta_n & \text{oder} & \\ \alpha_1 + \ldots + \alpha_n = \beta_1 + \ldots + \beta_n, & \alpha_n = \beta_b & \alpha_{n-1} > \beta_{n-1} & \text{oder} \\ \vdots & \vdots & \ddots & \\ \alpha_1 + \ldots + \alpha_n = \beta_1 + \ldots + \beta_n, & \alpha_n = \beta_b & \ldots & \alpha_3 = \beta_3, \quad \alpha_2 \geq \beta_2 \end{cases}$$

so erhält man die **graduiert-umgekehrt-lexikographische Term**.

6.4 Satz (Dicksons Lemma)

Sei $(t_1, t_2, \ldots)$ eine Folge von Termen in $\mathbb{T}^n$ und sei $I = \langle t_1, t_2, \ldots \rangle \subseteq P$ das von ihm erzeugte **monomiale Ideal**. Dann gibt es ein $N > 0$ mit $I = \langle t_1, \ldots, t_N \rangle$.

MaW: Jedes t_i mit $i > N$ ist Vielfaches eines der Terme in $\{t_1, \ldots, t_N\}$.

b) Eine mit der Multiplikation verträgliche, vollständige Ordnungsrelation $<_\sigma$ ist genau dann eine Termordnung, wenn für alle $t \in \mathbb{T}^n$ gilt: $t \geq_\sigma 1$.

Beweis:

Zu (a): Wir schließen mit vollständiger Induktion nach n.

$n = 1$: Jedes monomiale Ideal $I \subseteq K[x]$ ist von der Form $I = (x^a)$ mit $a \geq 0$.

$n > 1$: Angenommen $\langle t_1, t_2, \ldots \rangle$ ist nicht von endlich vielen t_i erzeugt. OE gelte $t_i \notin \langle t_1, \ldots, t_{i-1} \rangle$ für alle $i \geq 2$. Für $t = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ setze $t' = x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ (d.h. x_1-Potenz weglassen). Wähle in $(t_1, t_2, \ldots)$ eine Teilfolge $(u_1, u_2, \ldots)$ mit $u_i = t_{\nu(i)}$, so dass u_i in $t_{\nu(i-1)+1}, t_{\nu(i-1)+2}, \ldots$ der Term mit minimalem x_1-Exponent ist. Nach Induktionsvoraussetzung gibt es für $J = \langle u_1', u_2', \ldots \rangle \subseteq K[x_2, \ldots, x_n]$ ein $N' > 0$ mit

$$J = \langle u_1', \ldots, u_{N'}' \rangle$$

Dann sind die x_1-Exponenten der Folge $(u_1, u_2, \ldots)$ monoton zunehmend. Dann sind alle Elemente u_k mit $k > N'$ Vielfache eines der Terme in $\{u_1, \ldots, u_{N'}\}$. Wir erhalten einen Widerspruch zu

$$u_{N'+1} = t_{\nu(N'+1)} \notin \left\langle t_1, \ldots, t_{\nu(N'+1)-1} \right\rangle.$$

Zu (b): "$\Rightarrow$": Angenommen $t <_\sigma 1$, so wäre $1 >_\sigma t >_\sigma t^2 >_\sigma t^3 >_\sigma \ldots$ eine unendliche echt absteigende Folge.

"$\Leftarrow$": Sei $t_1 >_\sigma t_2 >_\sigma t_3 >_\sigma \ldots$ eine unendliche Kette. Dann folgt $t_i \notin \langle t_1, \ldots, t_{i-1} \rangle$, denn $t_i = t' t_j$ mit $j < i$ und es folgt $t_i \geq_\sigma t_j$. Damit erhalten wir einen Widerspruch zu (a). □

6.5 Definition

Sei σ eine Termordnung auf $\mathbb{T}^n$.

a) Für ein $f \in P \setminus \{0\}$ schreibe $f = c_1 t_1 + \ldots + c_s t_s$ mit $c_i \in K \setminus \{0\}$ und $t_i \in \mathbb{T}^n$. Dann heißt $\mathrm{LT}_\sigma(f) = t_1$ der **Leitterm** von f bzgl σ. Wir setzen auch $\mathrm{LM}_\sigma(f) = c_1 t_1$.

b) Für ein Polynomideal $I \subseteq P$ sei

$$\mathrm{LT}_\sigma(I) = \underbrace{\langle \mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\} \rangle}_{\text{monomiales Ideal}}$$

das **Leittermideal** von I. Wir setzen $\mathrm{LT}_\sigma((0)) = (0)$.

6.6 Beispiel

a) Sei $\sigma = \mathrm{Lex}$ und $I = \left\langle x^2 - y, xy - 1 \right\rangle \subseteq P = \mathbb{Q}[x, y]$. $\mathrm{LT}_\sigma\left(x^2 - y\right) = x^2$ und $\mathrm{LT}_\sigma(xy - 1) = xy$. Also folgt $\left\langle x^2, xy \right\rangle \subseteq \mathrm{LT}_\sigma(I)$. Gleichheit gilt nicht, denn

$$\begin{aligned} x - y^2 &= y\left(x^2 - y\right) - x(xy - 1) \in I \\ y^3 - 1 &= -y\left(x - y^2\right) + (xy - 1) \in I \end{aligned}$$

wobei $\mathrm{LT}_\sigma\left(x - y^2\right) = x$ und $\mathrm{LT}\left(y^3 - 1\right) = y^3$. Daher wissen wir $\mathrm{LT}_\sigma(I) \supseteq \left\langle x^2, xy, x, y^3 \right\rangle = \left\langle x, y^3 \right\rangle$

b) Sei $\sigma = \text{Lex}$ und $I = \langle x^2 - y, y^2 - 1\rangle$. Dann gilt $\text{LT}_\sigma(I) = \langle x^2, y^2\rangle$.

b) Für $\sigma = \text{Lex}$ und $I = \langle x^2 - y, xy - 1\rangle$ gilt $\text{LT}_\sigma(I) \subseteq \langle x, y^3\rangle$, denn

$$\begin{aligned} x - y^2 &= y\left(x^2 - y\right) - x\left(xy - 1\right) \in I \\ y^3 - 1 &= -y\left(x - y^2\right) + \left(xy - 1\right) \in I \end{aligned}$$

6.7 Definition

Sei $I = \langle f_1, \ldots, f_s\rangle \subseteq P$ ein von Polynomen $f_i \neq 0$ erzeugtes Polynomideal und σ eine Termordnung. Die Menge $G = \{f_1, \ldots, f_s\}$ heißt eine **σ-Gröbner-Basis** (σ-GB) von I wenn $\text{LT}(I) = \langle \text{LT}_\sigma(f_1), \ldots, \text{LT}_\sigma(f_s)\rangle$ gilt.

6.8 Beispiel

In Beispiel 6.6.a gilt $I = \langle g_1, g_2\rangle$ mit $g_1 = x - y^2$ und $g_2 = y^3 - 1$, denn $f_1, f_2 \in \langle g_1, g_2\rangle$. Die Menge $G = \{g_1, g_2\}$ ist sogar eine σ-Gröbner-Basis von I, d.h. es gilt sogar $\text{LT}_\sigma(I) = \langle x, y^3\rangle$.

6.9 Satz (Existenz von Gröbnerbasen)

Sei σ eine Termordnung und $I \subseteq P$ ein Ideal. Dann gibt es eine endliche σ-Gröbner-Basis $G = \{g_1, \ldots, g_s\}$ von I. Ferner gilt: $I = \langle g_1, \ldots, g_s\rangle$. Insbesondere ist I endlich erzeugt (Hilbertscher Basissatz).

Beweis: Nach Satz 6.4.a (Dicksons Lemma) ist das monomiale Ideal $\text{LT}_\sigma(I) = \langle \text{LT}_\sigma(f) \mid f \in I \setminus \{0\}\rangle$ von endlich vielen $\text{LT}_\sigma(f_1), \ldots, \text{LT}_\sigma(f_2)$ erzeugt. Damit ist $G = \{f_1, \ldots, f_s\}$ eine σ-Gröbnerbasis von I.

Nun zeigen wir $I = \langle f_1, \ldots, f_s\rangle$. Angenommen es gibt ein $f \in I \setminus \langle f_1, \ldots, f_s\rangle$. Dann gibt es dann ein solche f mit minimalem Leitterm. Schreibe $\text{LM}_\sigma(f) = c\,\text{LM}_\sigma(f_i)\,t$ mit $c \in K$, $i \in \{1, \ldots, s\}$ und $t \in \mathbb{T}^n$. Dann besitzt $f - ctf_i \in I \setminus \langle f_1, \ldots, f_s\rangle$ einen kleineren Leitterm als f. Wir erhalten einen Widerspruch. □

Mit Hilfe von Gröbnerbasen kann man das **Idealzugehörigkeitsproblem** effektiv lösen.

6.10 Satz

Sei σ eine Termordnung, $I \subseteq P$ ein Ideal und sei $G = \{g_1, \ldots, g_s\}$ eine σ-Gröbnerbasis von I.

a) An jedem Polynom $f \in P \setminus \{0\}$ kann man nur endlich viele Reduktionsschritte mittels $\xrightarrow{G}$ durchführen. Ein Reduktionsschritt mittels $\xrightarrow{G}$ ist dabei eine Subtraktion $f \xrightarrow{G} f - ctg_i$ mit $c \in K$, $t \in \mathbb{T}^n$ und $g_i \in G$, so dass der Term $t\,\text{LT}(g_i)$ in der Differenz nicht mehr vorkommt.

b) Führt man an einem Polynom $f \in P \setminus \{0\}$ so viele Reduktionsschritte mittels $\xrightarrow{G}$ wie möglich durch, so ist das Ergebnis eindeutig bestimmt. Es heißt die Normalform von f bzgl. I und wird mit $\text{NF}_{\sigma,I}(f)$ bezeichnet.

c) Der Träger von $\text{NF}_{\sigma,I}$ ist in $\mathcal{O}_\sigma(I) = \mathbb{T}^n \setminus \text{LT}_\sigma(I)$ enthalten.

d) Für $f \in P$ gilt $f \in I$ genau dann, wenn $\text{NF}_{\sigma,I}(f) = 0$.

Sammelt man dabei die in $f \xrightarrow{G} 0$ verwendeten Subtrahenden, so erhält man eine Darstellung

$$f = \sum_{i=1}^{s} h_i g_i \quad \text{mit } h_i \in P \text{ und } \text{LT}_\sigma(h_i g_i) \leq \text{LT}_\sigma(f)$$

[Explizite Idealzugehörigkeit]

Beweis:

Zu (a): Angenommen $f = f_0 \xrightarrow{G} f_1 \xrightarrow{G} \ldots$ ist eine unendliche Kette echter Reduktionsschritte. In jedem f_i gibt es dann einen bzgl. σ maximalen Term t_i mit der Eigenschaft dass er später reduziert wird. Dann ist $t_1 \geq_\sigma t_2 \geq_\sigma \ldots$ eine nicht stationäre unendliche Kette. Dies ist ein Widerspruch zu σ Termordnung.

Zu $(b), (c)$: Seien $f \xrightarrow{G} f'$ und $f \xrightarrow{G} f''$ Ketten, so dass f', f'' nicht weiter reduzierbar bzgl. $\xrightarrow{G}$ sind. Dann ist kein Term von f' oder f'' in $\mathrm{LT}_\sigma(I)$ enthalten. Also sind alle Terme von $f' - f''$ in $\mathcal{O}_\sigma(I)$ enthalten. Andererseits gilt:

$$f' - f'' = (f - f'') - (f - f') \in I$$

und daher folgt

$$\mathrm{LT}_\sigma(f - f') \in \mathrm{LT}_\sigma(I) \quad \text{(kann nicht sein)} \quad \text{oder} \quad f' - f'' = 0$$

Damit $f' = f''$.

Zu (d): "$\Leftarrow$" folgt aus $f \xrightarrow{G} \mathrm{NF}_{\sigma,I}(f) = 0$ durch Sammeln der Subtrahenden. "$\Rightarrow$" Es gibt eine Kette

$$f = \sum_{i=1}^{s} h_i g_i \xrightarrow{G} 0$$

Wegen (b) ist dann $\mathrm{NF}_{\sigma,I}(f) = 0$. Der zweite Teil von (d) ist klar. □

6.11 Bemerkung

a) Zu $f_1, \ldots, f_s \in P$ heißt

$$\mathrm{Syz}_P(f_1, \ldots, f_s) = \{(h_1, \ldots, h_s) \in P^s \mid h_1 f_2 + \ldots + h_s f_s = 0\}$$

der **Syzygienmodul** von $(f_1, \ldots, f_s)$. Es ist ein P-Untermodul von P^s. Man kann mit einer σ-Gröbnerbasis $I = \langle f_1, \ldots, f_s \rangle$ ein Erzeugendensystem dieses Syzygienmoduls berechnen.

b) Sind $g, f_1, \ldots, f_s \in P$ beliebige Polynome, so kann man auch Reduktionsschritte $g \xrightarrow{F} g - ctf_i$ definieren. Wenn man jetzt soviele Reduktionsschritte wie möglich macht, so ist das Ergebnis i.A. nicht eindeutig bestimmt. Verwendet man die Vorschriften:

1. es wird stets der größte reduzierbare Term in g wegreduziert
2. es wird stets das f_i mit kleinstmöglichen i verwendet

Dann heißt das Ergebnis der **normale Rest** der Division von $F = (f_1, \ldots, f_s)$ und wird mit $\mathrm{NR}_{\sigma,F}(g)$ bezeichnet.

6.12 Theorem (Buchbergers Algorithmus)

Sei $F = (f_1, \ldots, f_s)$ ein Tupel von Polynomen $\neq 0$, das ein Ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq P$ erzeugt und sei σ eine Termordnung. Für $i = 1, \ldots, s$ schreibe $\mathrm{LM}_\sigma(f_i) = c_i t_i$ mit $c_i \in K$ und $t_i \in \mathbb{T}^n$. Betrachte die folgenden Instruktionen:

1. Setze $s' = s$, $G = F$ und $B = \{(i, j) \mid 1 \leq i < j \leq s\}$.
2. Ist $B = \emptyset$, so gib G aus und stoppe.
3. Wähle ein Paar $(i, j) \in B$ und streiche es aus B.

4. Berechne das S-Polynom

$$S_{ij} = \frac{1}{c_i}\frac{\mathrm{kgV}(t_i, t_j)}{t_i} f_i - \frac{1}{c_j}\frac{\mathrm{kgV}(t_i, t_j)}{t_j} f_j$$

wobei $\mathrm{LM}_\sigma(f_k) = c_k t_k$ mit $c_k \in K$, $t_k \in \mathbb{T}^n$ gelte. Dann berechne

$$S'_{ij} \quad = \quad \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$$

Gilt $S'_{ij} = 0$, so fahre mit (2) fort.

5. Erhöhe s' um eins, setze $f_{s'} = S'_{ij}$ und füge $\{(i, s') \mid 1 \leq i \leq s'\}$ zu B hinzu. Dann fahre mit (2) fort.

Dies ist ein Algorithmus, der eine σ-Gröbnerbasis $G = (f_1, \ldots, f_s)$ von I berechnet.

Beweisskizze (Vgl. [KR1], §2.5):

Endlichkeit: Schritt (5) wird nur endlich oft durchlaufen, und zwar nur wenn ein Polynom S'_{ij} gefunden wird mit

$$\mathrm{LT}_\sigma\left(S'_{ij}\right) \in \mathrm{LT}_\sigma(I) \setminus \langle \mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_{s'})\rangle$$

Die aufsteigende Kette $\langle \mathrm{LT}_\sigma(f_1)\rangle \subseteq \langle \mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2)\rangle \subseteq \ldots$ wird stationär (Dicksons Lemma). Also wird wird B nur endlich oft vergrößert. Da in (3) stets ein Paar aus B gestrichen wird, ist B irgendwann leer.

Korrektheit: Verwendet das Buchberger-Kriterium: Genau dann ist $G = (f_1, \ldots, f_{s'})$ ein σ-Gröbnerbasis von I, wenn für $1 \leq i < j \leq s'$ gilt:

$$\mathrm{NR}_{\sigma,G}(S_{ij}) \quad = \quad 0$$

□