Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§2.6 Minimale und reduzierte Gröbnerbasen

In diesem Abschnitt sei stets K ein Körper. Ferner sei eine Monomordnung $\leq$ auf $[\underline{X}]$ fixiert.

Lemma 2.6.1. *Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge*

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \&\ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich [→2.1.9].

Beweis. Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$. Dann $w \in (M')$.

Zu (b). Sei $M'' \subseteq [\underline{X}]$ mit $I = (M'')$. Sei $v \in M'$. Zu zeigen ist $v \in M''$. Wegen $v \in M \subseteq I = (M'')$ gibt es $w \in M''$ mit $w|v$. Wegen $M'' \subseteq I = (M)$ gibt es $u \in M$ mit $u|w$. Also $u|w|v$, woraus wegen $v \in M'$ und $u \in M$ folgt $u = w = v$, insbesondere $v = w \in M''$. □

Lemma 2.6.2. *Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal* [→2.1.11]. *Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt. Es ist M endlich und das kleinste aus Monomen bestehende Erzeugendensystem von I. Man erhält M aus jedem anderen aus Monomen bestehenden Erzeugendensystem M' von I, indem man die bezüglich der Teilerrelation auf M' nicht minimalen Elemente aus M' entfernt.*

Beweis. Um die Eindeutigkeit zu zeigen, sei $M \subseteq [\underline{X}]$ mit $I = (M)$ und $\forall u, v \in M : (u \neq v \implies u \nmid v)$. Mit der Notation von 2.6.1 gilt dann offenbar $M = M'$ und M' ist nach 2.6.1 durch I eindeutig bestimmt. Die Existenz und die restlichen Aussagen folgen ebenfalls aus 2.6.1. □

Definition 2.6.3. Eine Gröbnerbasis $G \subseteq K[\underline{X}]$ heißt *minimal*, wenn sie (bezüglich Inklusion) minimal unter allen Gröbnerbasen des von G erzeugten Ideals ist.

Proposition 2.6.4. *Sei $G \subseteq K[\underline{X}] \setminus \{0\}$ endlich und $I := (G)$. Dann sind äquivalent:*

(a) *G ist eine minimale Gröbnerbasis.*

(b) *G ist eine Gröbnerbasis derart, dass kein Leitmonom eines Elements von G das Leitmonom eines anderen Elements von G teilt.*

(c) *Je zwei verschiedene Elemente von G haben verschiedene Leitmonome und*

$$\{\mathrm{LM}(g) \mid g \in G\}$$

ist das kleinste aus Monomen bestehende Erzeugendensystem von $L(I)$ [→2.4.2(j)].

Beweis. (a) $\Longrightarrow$ (b) und (c) $\Longrightarrow$ (a) folgen aus 2.4.7(g), (b) $\Longrightarrow$ (c) aus 2.6.2. □

Satz 2.6.5. *Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I (bezüglich derselben Monomordnung $\leq$), so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.*

Beweis. Die zweite Aussage ist klar mit 2.6.4(c). Um die Existenz einer minimalen Gröbnerbasis von I zu zeigen, wähle man zunächst gemäß Satz 2.4.8 eine beliebige Gröbnerbasis $G \subseteq K[\underline{X}] \setminus \{0\}$ von I. Offensichtlich gibt es $H \subseteq G$ mit

$$(\{\mathrm{LM}(g) \mid g \in G\}) = (\{\mathrm{LM}(h) \mid h \in H\})$$

derart, dass kein Leitmonom eines Elements von H das Leitmonom eines anderen Elements von H teilt. Wegen $(\{\mathrm{LM}(h) \mid h \in H\}) = (\{\mathrm{LM}(g) \mid g \in G\}) = L(I)$ ist mit 2.4.7(g) auch H eine Gröbnerbasis von I. Nach 2.6.4 ist H eine minimale Gröbnerbasis. □

Bemerkung 2.6.6. Es ist klar, wie man zu einer gegebenen endlichen Menge $F \subseteq K[\underline{X}]$ eine minimale Gröbnerbasis H von (F) berechnet: Berechne mit dem Buchberger-Algorithmus 2.5.6 eine Gröbnerbasis G von (F) und verkleinere G zu H wie im Beweis von Satz 2.6.5.

Definition 2.6.7. (a) Ein Polynom $f \in K[\underline{X}]$ heißt *normiert* (bezüglich $\leq$), wenn $f \neq 0$ und $\mathrm{LC}(f) = 1$.

(b) Eine Menge $F \subseteq K[\underline{X}]$ heißt *normiert* (bezüglich $\leq$), wenn jedes ihrer Elemente normiert ist.

(c) Eine Menge $F \subseteq K[\underline{X}]$ heißt *reduziert* (bezüglich $\leq$), wenn F normiert ist und jedes $f \in F$ reduziert modulo $F \setminus \{f\}$ ist [→2.4.1(b)].

Proposition 2.6.8. *Jede reduzierte Gröbnerbasis ist minimal.*

Beweis. Sei $G \subseteq K[\underline{X}]$ eine reduzierte Gröbnerbasis. Dann gilt $G \subseteq K[\underline{X}] \setminus \{0\}$ und 2.6.4(b) ist erfüllt. □

Satz 2.6.9. *Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.*

Beweis. Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach 2.6.8 minimal sind, gilt nach 2.6.5 $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar (zum Beispiel mit 2.4.11) $\mathrm{red}(G) = \mathrm{red}(H)$ [→2.4.1(b)]. Wegen $g \in \mathrm{red}(G \setminus \{g\})$ gilt $M(g) \setminus \{u\} \subseteq \mathrm{red}(G)$. Analog $M(h) \setminus \{u\} \subseteq \mathrm{red}(H)$. Da g und h normiert sind, haben wir $M(g-h) \subseteq (M(g) \cup M(h)) \setminus \{u\} \subseteq \mathrm{red}(G) = \mathrm{red}(H)$ und daher $g - h \in \mathrm{red}(G)$. Andererseits $g - h \in I$ und daher $g - h \xrightarrow[G]{*} 0$. Es folgt $g - h = 0$, also $g = h \in H$.

Existenz Wähle mit 2.6.5 eine minimale Gröbnerbasis G von I. Wähle zu jedem $g \in G$ ein $g' \in \mathrm{red}(G \setminus \{g\})$ mit $g \xrightarrow[G\setminus\{g\}]{*} g'$. Wegen der Minimalität von G gilt $\mathrm{LM}(g') = \mathrm{LM}(g)$ für alle $g \in G$ [→2.6.4(b)]. Nach 2.4.7(g) ist mit G auch $H := \{g' \mid g \in G\}$ eine Gröbnerbasis von I. Wieder mit 2.4.11 sieht man $\mathrm{red}(G \setminus \{g\}) = \mathrm{red}(H \setminus \{g'\})$ für alle $g \in G$. Somit $g' \in \mathrm{red}(H \setminus \{g'\})$ für alle $g \in G$, das heißt H ist reduziert. □

Algorithmus 2.6.10 (Interreduktionsalgorithmus)**.**

Eingabe: $F \subseteq K[\underline{X}]$ endlich

Ausgabe: $G \subseteq K[\underline{X}]$ endlich und reduziert mit $(G) = (F)$ derart, dass G eine Gröbnerbasis ist, falls F eine ist.

$G \leftarrow F$;

solange es $g \in G$ gibt mit $g \notin \mathrm{red}(G \setminus \{g\})$

$\quad$ (wähle $g \in G$ mit $g \notin \mathrm{red}(G \setminus \{g\})$;

$\quad$ wähle $h \in K[\underline{X}]$ mit $g \xrightarrow[G\setminus\{g\}]{} h$;

$\quad$ $G \leftarrow (G \setminus \{g\}) \cup \{h\})$;

$G \leftarrow \{\frac{g}{\mathrm{LC}(g)} \mid g \in G \setminus \{0\}\}$

Beweis. Terminierung Angenommen der Algorithmus terminiert nicht. Wähle dann $s \in \mathbb{N}$ und $g_1^{(0)}, \ldots, g_s^{(0)} \in K[\underline{X}]$ mit $F = \{g_1^{(0)}, \ldots, g_s^{(0)}\}$. Dann gilt zu Beginn des ersten Schleifendurchlaufs $G = \{g_1^{(0)}, \ldots, g_s^{(0)}\}$. Wir nehmen an zu Beginn des i-ten Schleifendurchlaufs ($i \in \mathbb{N}$) gelte $G = \{g_1^{(i-1)}, \ldots, g_s^{(i-1)})$ für schon definierte $g_1^{(i-1)}, \ldots, g_s^{(i-1)} \in K[\underline{X}]$. Sind g und h wie in diesem Durchlauf gewählt, dann definieren wir $g_1^{(i)}, \ldots, g_s^{(i)} \in K[\underline{X}]$ durch

$$g_j^{(i)} := \begin{cases} g_j^{(i-1)} & \text{falls } g_j^{(i-1)} \neq g \\ h & \text{falls } g_j^{(i-1)} = g \end{cases} \qquad (j \in \{1, \ldots, s\}).$$

Auf diese Weise stellen wir sicher, dass zu Ende des i-ten Schleifendurchlaufs gilt $G = \{g_1^{(i)}, \ldots, g_s^{(i)}\}$ und

$$(*) \qquad (M(g_1^{(i-1)}), \ldots, M(g_s^{(i-1)})) \succ (M(g_1^{(i)}), \ldots, M(g_s^{(i)})),$$

wobei $\preceq$ die Halbordnung auf $(\mathscr{P}_{\text{fin}}([\underline{X}]))^s$ [→2.1.20] ist, die definiert ist durch

$$(U_1, \ldots, U_s) \preceq (V_1, \ldots, V_s) \iff \forall i \in \{1, \ldots, s\} : U_i \leq' V_i$$

und $\leq'$ die in 2.1.21 definierte Wohlordnung auf $\mathscr{P}_{\text{fin}}([\underline{X}])$ ist (siehe Beweis von 2.1.24). Dass mit $>'$ auch $\succ$ noethersch ist, ist ein Widerspruch dazu, dass wir rekursiv eine Folge $(g_1^{(i)}, \ldots, g_s^{(i)})_{i \in \mathbb{N}_0}$ erhalten mit $(*)$ für $i \in \mathbb{N}$. ↯

Korrektheit Folgende Aussagen sind Schleifeninvarianten, das heißt sie gelten am Ende eines Schleifendurchlaufs, sofern sie am Anfang desselben Durchlaufs gegolten haben:

(a) $G \subseteq K[\underline{X}]$ ist endlich mit $(G) = (F)$.

(b) G ist eine Gröbnerbasis, falls F eine war.

Für (a) ist das schnell zu sehen. Für (b) sei nun F eine Gröbnerbasis. Dann reicht es gemäß 2.4.2(j) zu zeigen, dass

$$(**) \qquad L(I) = (\{\mathrm{LM}(f) \mid f \in G \setminus \{0\}\})$$

mit $I := (F)$ eine Schleifeninvariante ist. Sei also $G \subseteq K[\underline{X}]$ mit $(G) = I$ und $(**)$ und seien $g \in G$ und $h \in K[\underline{X}]$ mit $g \underset{G \setminus \{g\}}{\longrightarrow} h$. Wir zeigen

$$L(I) = (\{\mathrm{LM}(f) \mid f \in ((G \setminus \{g\}) \cup \{h\}) \setminus \{0\}\}) =: J.$$

Falls $h \neq 0$ und $\mathrm{LM}(g) = \mathrm{LM}(h)$, so ist dies wegen $(**)$ trivial. Andernfalls haben wir $g \underset{G \setminus \{g\}}{\longrightarrow} h$ $[\mathrm{LM}(g)]$, weswegen

$$\mathrm{LM}(g) \in (\{\mathrm{LM}(f) \mid f \in (G \setminus \{g\}) \setminus \{0\}\}) =: L$$

und daher $L(I) \overset{(**)}{\subseteq} L \subseteq J \overset{G \cup \{h\} \subseteq I}{\subseteq} L(I)$, also insbesondere $L(I) = J$. □

Bemerkung 2.6.11. Wie versprochen sehen wir jetzt, dass Gröbnerbasen gleichzeitig den euklidischen Algorithmus für Polynome in einer Variablen [→2.1.1(a)] als auch den Gauß-Algorithmus für lineare Polynome [→2.1.1(b)] verallgemeinern: Seien nämlich $f_1, \ldots, f_s \in K[\underline{X}]$ und $I := (f_1, \ldots, f_s)$.

(a) Gelte $n = 1$, also $\underline{X} = X$. Dann gibt es genau ein $g \in K[\underline{X}]$ mit $I = (g)$ und g normiert oder $g = 0$. Dann ist $\{g\} \setminus \{0\}$ die eindeutig bestimmte reduzierte Gröbnerbasis von I.

(b) Gelte $\deg f_i \leq 1$ für alle $i \in \{1, \ldots, s\}$. Dann gibt es eindeutig bestimmte

$$g_i = \sum_{j=1}^{n} a_{ij} X_j + b_i \qquad (i \in \{1, \ldots, s\}, a_{ij}, b_i \in K)$$

derart, dass mit $A := (a_{ij})_{1 \leq i \leq s, 1 \leq j \leq n}$ und

$$b := \begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix}$$

die Matrix $(A\ b) \in K^{s \times (n+1)}$ in reduzierter Stufenform ist und

$$Kf_1 + \ldots + Kf_s = Kg_1 + \ldots + Kg_s$$

[→LA §5.1, §5.3]. Ist $\leq$ eine Termordnung mit $X_1 \geq X_2 \geq \cdots \geq X_n$, so ist im Fall $1 \notin \{g_1, \ldots, g_s\}$ die Menge $\{g_1, \ldots, g_s\} \setminus \{0\}$ und sonst $\{1\}$ eine reduzierte Gröbnerbasis von I. Dies sieht man mit dem Buchberger-Kriterium 2.5.4 zusammen mit dem folgenden Lemma.

Lemma 2.6.12. *Seien $f, g \in K[\underline{X}] \setminus \{0\}$ derart, dass kein X_i gleichzeitig* $\mathrm{LM}(f)$ *und* $\mathrm{LM}(g)$ *teilt (man sagt, „f und g haben disjunkte Leitterme"). Dann* $\mathrm{spol}(f, g) \xrightarrow[\{f,g\}]{*} 0$.

Beweis. Schreibe $f = \sum_{i=1}^{k} a_i u_i$ und $g = \sum_{j=1}^{\ell} b_j v_j$ mit $k, \ell \in \mathbb{N}$, $a_i, b_j \in K^\times$ und $u_i, v_j \in [\underline{X}]$, wobei $u_1 > \ldots > u_k$ und $v_1 > \ldots > v_\ell$ gelte. Nach Voraussetzung gilt $\mathrm{lcm}(u_1, v_1) = u_1 v_1$ und daher nach 2.5.3

$$\mathrm{spol}(f, g) = b_1 v_1 f - a_1 u_1 g = \underbrace{b_1 v_1 \sum_{i=2}^{k} a_i u_i}_{=:p} - \underbrace{a_1 u_1 \sum_{j=2}^{\ell} b_j v_j}_{=:q}.$$

Es gilt $M(p) \cap M(q) = \emptyset$, denn sonst gäbe es $i \in \{2, \ldots, k\}$ und $j \in \{2, \ldots, \ell\}$ mit $v_1 u_i = u_1 v_j$ und es gälte $u_1 v_1 = \mathrm{lcm}(u_1, v_1) \mid v_1 u_i$ und damit $u_1 v_1 \leq v_1 u_i \leq v_1 u_1 = u_1 v_1$, was $u_1 v_1 = u_i v_1$ also $u_1 = u_i$ implizierte $\lightning$. Jedes der $\ell - 1$ Monome von q ist also ein Monom von $\mathrm{spol}(f, g)$ und wird von $u_1 = \mathrm{LM}(f)$ geteilt. Wir addieren nun nacheinander $b_\ell v_\ell f, b_{\ell-1} v_{\ell-1} f, \ldots, b_2 v_2 f$ zu $\mathrm{spol}(f, g)$ und überlegen uns, dass dies jeweils ein Reduktionsschritt modulo f ist: In der Tat, hat man schon $b_\ell v_\ell f + \ldots + b_j v_j f$ $(2 < j \leq \ell)$ addiert, so sind die Monome $v_{j-1} u_1, \ldots, v_2 u_1$ immer noch vorhanden, denn jedes von ihnen ist echt größer als jedes Monom von $b_\ell v_\ell f + \cdots + b_j v_j f$. Daher

$$\begin{aligned} \mathrm{spol}(f, g) \xrightarrow[f]{\ell-1} p + \left(\sum_{i=2}^{k} a_i u_i\right) \sum_{j=2}^{\ell} b_j v_j &= \left(\sum_{i=2}^{k} a_i u_i\right) \left(b_1 v_1 + \sum_{j=2}^{\ell} b_j v_j\right) \\ &= \left(\sum_{i=2}^{k} a_i u_i\right) g \xrightarrow[g]{k-1} 0. \end{aligned}$$

□