# Gröbnerbasen in Monoid- und Gruppenringen

Karsten Hiddemann

5. November 2003

**Zusammenfassung**

Gröbnerbasen, entwickelt von Bruno Buchberger für kommutative Polynomringe, finden immer häufiger Anwendung bei der Lösung algorithmischer Probleme. Dieser Seminarvortrag baut auf dem Vortrag "Termersetzung in Monoidringen" auf und betrachtet Gröbnerbasen in Monoid- und Gruppenringen, welche durch Wortersetzungssysteme präsentiert werden. Neben Algorithmen zur Berechnung von Gröbnerbasen soll auf ausgewählte Anwendungen, wie z.B. das Enthaltenseinsproblem für Ideale, eingegangen werden.

## 1 Grundlagen

Im folgenden sei der Monoid $\mathcal{M}$ stets endlich präsentiert durch das total geordnete, noethersche, konfluente Termersetzungssystem $(\Sigma, T)$ und $\mathbb{K}[\mathcal{M}]$ sei der zugehörige kommutative Polynomring über $M$ mit Koeffizienten aus $\mathbb{K}$. Seien nun $p \in \mathbb{K}[\mathcal{M}]$, $F \subseteq \mathbb{K}[\mathcal{M}]$ gegeben. Wir wollen entscheiden können, ob $p \in \text{ideal}_r(F)$, d.h. ob $p \equiv_{\text{ideal}_r(F)} 0$ ist. Alleinige Reduktionen am Leitterm (wie bei der Polynomdivision in $\mathbb{K}[x]$) reichen hier nicht aus, denn durch die Termersetzungen könnte der Grad von $p$ dabei steigen. Es wurde daher das Prinzip der starken Reduktion $p \to_f^s q$ von rechts an einem Monom $\alpha \cdot t$ eingeführt, welche durchführbar ist, falls es ein $w \in M$ gibt mit $\text{LT}(f * w) = t$ so, daß gilt $q = p - \alpha \cdot \text{LC}(f * w)^{-1} \cdot f * w$. Diese ist tatsächlich noethersch, und für die auf Mengen erweiterte starke Reduktion von rechts gilt $p \overset{*}{\leftrightarrow}{}_F^s q$ genau dann, wenn $p - q \in \text{ideal}_r(F)$, d.h. es gilt $\overset{*}{\leftrightarrow}{}_F^s = \equiv_{\text{ideal}_r(F)}$.

**Definition 1.1.** Eine Teilmenge $G \subseteq \mathbb{K}[\mathcal{M}]$ heißt *starke Gröbnerbasis*, wenn gilt, daß $\overset{*}{\longleftrightarrow}{}_G^s = \equiv_{\text{ideal}_r(G)}$ und $\longrightarrow_G^s$ konfluent ist.

## 2 Rechts-Reduktion und Gröbnerbasen

Um nun eine Menge als Gröbnerbasis nachzuweisen genügt es, auf lokale Konfluenz zu untersuchen, da die Reduktion noethersch ist. Doch selbst dieses ist algorithmisch nicht gut zu lösen, denn wir haben zu viel Freiheit bei der Wahl der $f$ und $w$ und im Allgemeinen müssen dazu unendlich viele solcher Paare betrachtet werden. Man schränkt nun die Menge der Reduktionen ein, indem gefordert wird, daß die Multiplikation mit $w$ den Leitterm von $f$ an seiner Leitposition beläßt.

**Definition 2.1.** Seien $p$, $f$ zwei Polynome ungleich Null aus $\mathbb{K}[\mathcal{M}]$. Wir sagen f *reduziert $p$ von rechts* zu $q$ an einem Monom $\alpha \cdot t$ in einem Schritt, $p \longrightarrow_f^r q$, falls ein $w \in \mathcal{M}$ existiert, so daß

(a) $\text{LT}(f * w) = \text{LT}(f) \circ w = t$ und

(b) $q = p - \alpha \cdot \text{LC}(f * w)^{-1} \cdot f * w$.

Genau wie vorher definieren wir nun:

**Definition 2.2.** Eine Teilmenge $G \subseteq \mathbb{K}[\mathcal{M}]$ heißt *Rechts-Gröbnerbasis*, wenn gilt, daß $\overset{*}{\longleftrightarrow}{}^{r}_{G} = \equiv_{\mathrm{ideal}_r(G)}$ und $\longrightarrow^r_G$ konfluent ist.

**Lemma 2.3.** *$p \overset{*}{\longleftrightarrow}{}^{r}_{F} q$ impliziert $p - q \in \mathrm{ideal}_r(F)$ bzw. äquivalent $p \equiv_{\mathrm{ideal}_r(F)} q$.*

*Beweis.* Der Fall $p = q$ ist klar. Sei nun $p \overset{k}{\longleftrightarrow}{}^{r}_{F} p_k \longleftrightarrow^r_F q$, Induktion über $k$: Es ist $q = p_k - \alpha \cdot f * w$ und damit dann auch $p - q = p - p_k + \alpha \cdot f * w \in \mathrm{ideal}_r(F)$. □

Wie im letzten Vortrag gezeigt gilt die Umkehrung im Allgemeinen aber nicht, Reduktion von rechts beschreibt nicht mehr die Idealkongruenz. Durch Saturierung der reduzierenden Menge wird dieses aber wieder sichergestellt.

**Definition 2.4.** $F \subseteq \mathbb{K}[\mathcal{M}]$ heißt *saturiert*, wenn gilt $f * w \longrightarrow^r_F 0$ in einem Schritt für alle $f \in F, w \in \mathcal{M}, f * w \neq 0$.

**Lemma 2.5.** *Sei $F$ saturiert. Dann hat jedes Polynom $0 \neq g \in \mathrm{ideal}_r(F)$ eine Darstellung der Form $g = \sum_{i=1}^{k} \alpha_i f_i * w_i$ mit $\mathrm{LT}(f_i * w_i) = \mathrm{LT}(f_i) \circ w_i$.*

*Beweis.* Sei $g = \sum_{j=1}^{k} \alpha_j f_j * w_j$ und $i$ so, daß $\mathrm{LT}(f_i * w_i) \neq \mathrm{LT}(f_i) \circ w_i$. Dann gilt $f_i * w_i \longrightarrow^r_F 0$, d.h. $f_i * w_i = \beta_i \cdot f_i' * w_i'$ mit $\mathrm{LT}(f_i' * w_i') = \mathrm{LT}(f_i') \circ w_i'$. Ersetze also $f_i * w_i$ durch $\beta_i \cdot f_i' * w_i'$, durch Iteration erhält man die gewünschte Darstellung. □

Wie kann nun festgestellt werden, ob eine Menge eine Gröbnerbasis ist? Zur Klärung dieser Frage brauchen wir zur Vorbereitung erst noch das

**Lemma 2.6 (Translation Lemma).** *Sei $F \subseteq \mathbb{K}[\mathcal{M}]$ und $p, q, h \in \mathbb{K}[\mathcal{M}]$.*

*(a) Sei $p - q \longrightarrow^r_F h$, dann existieren $p', q' \in \mathbb{K}[\mathcal{M}]$ so, daß $p \overset{*}{\longrightarrow}{}^{r}_{F} p'$, $q \overset{*}{\longrightarrow}{}^{r}_{F} q'$ und $h = p' - q'$.*

*(b) Sei $0$ eine Normalform von $p - q$ bzgl. $\longrightarrow^r_F$. Dann existiert $g \in \mathbb{K}[\mathcal{M}]$ so, daß $p \overset{*}{\longrightarrow}{}^{r}_{F} g$ und $q \overset{*}{\longrightarrow}{}^{r}_{F} g$.*

*Beweis.*

(a) Sei also $p - q \longrightarrow^r_F h = p - q - \alpha \cdot f * w$ mit $\mathrm{LT}(f * w) = \mathrm{LT}(f) \circ w = t$. Angenommen, $t$ ist sowohl Term von $p$ als auch von $q$, wobei $\alpha_1 t$ das Monom in $p$ sei und $\alpha_2 t$ das in $q$. Dann sind beide reduzierbar in $t$ und es ist $\alpha_1 - \alpha_2 = \alpha$. Sei nun $t$ nur Term in einem der beiden Polynome, O.B.d.A. in $p$. Dann ist $q' = q$ und $p \longrightarrow^r_F p - \alpha \cdot f * w$. Insgesamt ergibt sich dann $p' - q' = p - q - \alpha \cdot f * w = h$.

(b) Der Fall $p - q = 0$ ist klar. Sei nun $p - q \longrightarrow^r_F h \overset{k}{\longrightarrow}{}^{r}_{F} 0$, wir verwenden wieder Induktion über $k$. Nach (a) ist $h = p' - q'$ und auf diese läßt sich die Induktionsvoraussetzung anwenden.

□

**Satz 2.7.** *Sei $F$ eine saturierte Menge in $\mathbb{K}[\mathcal{M}]$. Dann sind äquivalent:*

*(a) $F$ ist eine Rechts-Gröbnerbasis*

*(b) $g \overset{*}{\longrightarrow}{}^{r}_{F} 0 \ \forall g \in \mathrm{ideal}_r(F)$.*

*Beweis.*

"⇒" Es gilt $g \in \mathrm{ideal}_r(F) \Leftrightarrow g \overset{*}{\longleftrightarrow}{}^{r}_{F} 0$. Da $\longrightarrow^r_F$ konfluent ist und 0 irreduzibel, folgt aber induktiv $g \overset{*}{\longrightarrow}{}^{r}_{F} 0$.

"$\Leftarrow$" Zunächst ist zu zeigen, daß $\overset{*}{\longleftrightarrow}{}^{r}_{F} = \equiv_{\mathrm{ideal}_r(F)}$. "$\subseteq$" ist klar nach 2.3. Zu "$\supseteq$": Sei also $p \equiv q \Leftrightarrow p = q + \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$. Da die Summe in $\mathrm{ideal}_r(F)$ liegt, kann man diese nach 2.5 durch Reduktionsschritte beschreiben, d.h. $p \overset{*}{\longleftrightarrow}{}^{r}_{F} q$. Nun ist noch zu zeigen, daß $\longrightarrow^{r}_{F}$ konfluent ist, da noethersch, reicht es aus, lokale Konfluenz nachzuweisen. Sei also $g \longrightarrow^{r}_{F} g_1$, $g \longrightarrow^{r}_{F} g_2$ und $g_1 \neq g_2$. Dann ist $g_1 - g_2 \in \mathrm{ideal}_r(F)$ und, da nach Voraussetzung $g_1 - g_2 \overset{*}{\longrightarrow}{}^{r}_{F} 0$, liefert das Translation Lemma 2.6 die Behauptung.

□

Es ist noch nicht ganz klar, welche Reduktionen wir beim Test auf die lokale Konfluenz nun im einzelnen betrachten müssen. Schwierig zu entscheiden sind diejenigen, die den gleichen Term reduzieren, diese bilden für uns kritische Paare. Wir definieren wie bei Buchberger's Ansatz:

**Definition 2.8.** Seien $p_1, p_2 \in \mathbb{K}[\mathcal{M}]$. Jedes Paar $w_1, w_2 \in \mathcal{M}$ mit $\mathrm{LT}(p_1 * w_1) = \mathrm{LT}(p_1) \circ w_1 = \mathrm{LT}(p_2) \circ w_2 = \mathrm{LT}(p_2 * w_2)$ definiert ein *Rechts-s-Polynom* durch

$$\mathrm{spol}_r(p_1, p_2, w_1, w_2) = \mathrm{LC}(p_1 * w_1)^{-1} \cdot p_1 * w_1 - \mathrm{LC}(p_2 * w_2)^{-1} \cdot p_2 * w_2$$

Wir bezeichnen die Menge aller solcher Paare mit $U_{p_1,p_2} \subseteq M \times M$

**Satz 2.9.** *Sei $F$ eine saturierte Menge in $\mathbb{K}[\mathcal{M}]$. Dann sind äquivalent:*

*(a)* $g \overset{*}{\longrightarrow}{}^{r}_{F} 0 \ \forall g \in \mathrm{ideal}_r(F)$

*(b)* $\mathrm{spol}_r(f_k, f_l, w_k, w_l) \overset{*}{\longrightarrow}{}^{r}_{F} 0 \ \forall f_k, f_l \in F, (w_k, w_l) \in U_{f_k,f_l}$

*Beweis.*

"$\Rightarrow$" klar, da $\mathrm{spol}_r(f_k, f_l, w_k, w_l) \in \mathrm{ideal}_r(F)$

"$\Leftarrow$" Falls $h \in \mathrm{ideal}_r(F)$ und $h \longrightarrow^{r}_{f} h'$, so ist auch $h' \in \mathrm{ideal}_r(F)$. Da die Reduktion noethersch ist, reicht es zu zeigen: Jedes $0 \neq g \in \mathrm{ideal}_r(F)$ ist reduzibel. Sei also $g$ nach 2.5 von der Form $g = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$ mit $\mathrm{LT}(f_i * w_i) = \mathrm{LT}(f_i) \circ w_i$. Sei bezüglich dieser Repräsentierung $t = \max\{\mathrm{LT}(f_j * w_j) \mid j = 1, \ldots, m\}$ und $K$ die Anzahl der $f_j * w_j$, die $t$ als Term enthalten. Dann ist $t \geq \mathrm{LT}(g)$ und falls $\mathrm{LT}(g) = t$, so ist $g$ reduzibel an $t$. Sei nun $t > \mathrm{LT}(g)$. Das heißt es gibt also zwei Polynome $f_k, f_l$ aus obiger Repräsentierung so, daß $t = \mathrm{LT}(f_k * w_k) = \mathrm{LT}(f_k) \circ w_k = \mathrm{LT}(f_l) \circ w_l = \mathrm{LT}(f_l * w_l)$, also bilden diese ein s-Polynom. Wir ändern nun unsere Präsentierung entsprechend diesem s-Polynom ab: O.B.d.A. $\mathrm{spol}_r(f_k, f_l, w_k, w_l) \neq 0$. Da $\mathrm{spol}_r(f_k, f_l, w_k, w_l) \overset{*}{\longrightarrow}{}^{r}_{F} 0$ ist $\mathrm{spol}_r(f_k, f_l, w_k, w_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, $\delta_i \in \mathbb{K}^*, h_i \in F, v_i \in \mathcal{M}$ mit $\mathrm{LT}(\mathrm{spol}_r(f_k, f_l, w_k, w_l)) < t$, da $t$ herausgekürzt wird. Damit erhalten wir:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \ & \alpha_k \cdot f_k * w_k + \alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \ & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{\mathrm{spol}_r(f_k, f_l, w_k, w_l)} \\
= \ & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i)
\end{aligned}$$

mit $\beta_k$ und $\beta_l$ passend gewählt und entweder verschwindet der Term $t$ hierbei (falls $\alpha_k + \alpha'_l \cdot \beta_k = 0$) oder $K$ sinkt, da $t$ im zweiten Teil ersetzt wurde. Dieser Prozeß läßt sich iterieren und er ist endlich, da die Reduktion die Termordnung verkleinert und man sich daher irgendwann im Fall $\mathrm{LT}(g) = t$ befindet.

□

# 3 Präfix-Reduktion

Obwohl man nun Gröbnerbasen durch s-Polynome charakterisieren kann, ist ein endlicher Test meist nicht möglich. Daher schwächen wir die Reduktion weiter ab.

**Definition 3.1.** Seien $p$, $f$ zwei Polynome ungleich Null aus $\mathbb{K}[\mathcal{M}]$. Wir sagen f *präfix-reduziert p von rechts* zu $q$ an einem Monom $\alpha \cdot t$ in einem Schritt, $p \longrightarrow_f^p q$, falls ein $w \in \mathcal{M}$ existiert, so daß

(a) $\mathrm{LT}(f)w \equiv t$, d.h. $\mathrm{LT}(f)$ ist Präfix von $t$, und

(b) $q = p - \alpha \cdot \mathrm{LC}(f)^{-1} \cdot f * w$.

**Definition 3.2.** $F \subseteq \mathbb{K}[\mathcal{M}]$ heißt *präfix-saturiert*, wenn gilt $f * w \longrightarrow_F^p 0$ in einem Schritt für alle $f \in F, w \in \mathcal{M}, f * w \neq 0$.

**Definition 3.3.** Eine Teilmenge $G \subseteq \mathbb{K}[\mathcal{M}]$ heißt *Präfix-Gröbnerbasis*, wenn gilt, daß $\overset{*}{\longleftrightarrow}_G^p = \equiv_{\mathrm{ideal}_r(G)}$ und $\longrightarrow_G^p$ konfluent ist.

**Definition 3.4.** Seien $p_1, p_2 \in \mathbb{K}[\mathcal{M}]$ und $w \in \mathcal{M}$ so, daß $\mathrm{LT}(p_1) \equiv \mathrm{LT}(p_2)w$, dann ist das *Präfix-s-Polynom* definiert durch

$$\mathrm{spol}_p(p_1, p_2) = \mathrm{LC}(p_1)^{-1} \cdot p_1 - \mathrm{LC}(p_2)^{-1} \cdot p_2 * w$$

Auch in diesem Fall haben wir wieder:

**Satz 3.5.** *Sei $F$ eine präfix-saturierte Menge in $\mathbb{K}[\mathcal{M}]$. Dann sind äquivalent:*

*(a)* $g \overset{*}{\longrightarrow}_F^p 0 \ \forall g \in \mathrm{ideal}_r(F)$

*(b)* $\mathrm{spol}_p(f_1, f_2) \overset{*}{\longrightarrow}_F^p 0 \ \forall f_k, f_l \in F$.

Der Algorithmus zur Berechnung einer Gröbnerbasis sieht nun wie folgt aus:

**PROZEDUR PRÄFIX GRÖBNER BASIS**

**Gegeben:** Endliche Polynommenge $F \subseteq \mathbb{K}[\mathcal{M}]$

**Gesucht:** $GB(F)$, eine Präfix-Gröbnerbasis von $F$

**Benutzt:** $SAT_p$, eine Präfix-saturierende Prozedur für Polynome.

**Initialisierung:**

$G := \cup_{f \in F} \ SAT_p(f)$ sei die präfix-saturierte Menge zu $F$.

Bilde die kritischen Paare $B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2 \ \}$.

**Programmablauf:**

★ Solange $B$ nicht leer ist, nehme ein Paar $(q_1, q_2)$ aus $B$ heraus.

Falls $\mathrm{spol}_p(q_1, q_2)$ existiert:

- Sei $h$ die Normalform von $\mathrm{spol}_p(q_1, q_2)$ bzgl. Präfix-Reduktion mit $G$
- Falls $h \neq 0$, dann füge $SAT_p(h)$ zu $G$ hinzu und die neuen kritischen Paare zu $B$, d.h. $B := B \cup \{(f, \tilde{h}), (\tilde{h}, f) \mid f \in G, \tilde{h} \in SAT_p(h)\}$.
- Weiter bei ★.

**Ausgabe:** $GB(F) := G$;

Es gibt zwei Stellen, an denen es möglich ist, daß diese Prozedur nicht terminiert: $SAT_p(g)$ könnte nicht terminieren und es kann sein, daß $B$ nie leer wird.

# Literatur


[1] B. Reinert, *Tutorial on Gröbner Bases in Monoid and Groups Rings*, Federated Logic Conference '99 Workshop on Gröbner Bases and Rewriting Techniques, 1999.

[2] Krister Forsman, *The Hitch Hiker's Guide to Gröbner Bases: commutative algebra for amateurs*, Contemp. Math., Amer. Math. Soc. **298** (2002), 21–42.

[3] B. Reinert, *Gröbnerbasen*, manuscript for a lecture given in the winter term 1996/97 (1996).

[4] B. Reinert, *On Gröbner Bases in Monoid and Group Rings*, Phdthesis, Fachbereich Informatik, Universität Kaiserslautern, 1995.