

Polynomiale Involutive Basen

Seminar Involutive Basen und Auflösungen SoSe 2021

Matthias Orth

Universität Kassel

22.04.2021

- $\mathcal{P} = K[x_1, \dots, x_n]$ Polynomring über Körper K .
- $\mathbb{T}^n = \{x^\mu \mid \mu \in \mathbb{N}_0^n\}$ K -Vektorraumbasis von $\mathcal{P}$. (Basis der *Terme*.)
- $\deg(x^\mu) = |\mu| = \sum_{i=1}^n \mu_i$: *Grad* von x^μ .
- $f = \sum_{x^\mu \in \mathbb{T}^n} c_\mu x^\mu$: Darstellung von $f \in \mathcal{P}$ bzgl. Basis $\mathbb{T}^n$.
- $\{x^\mu \mid c_\mu \neq 0\}$ in obiger Summe: *Träger* $\text{supp}(f)$ von f .
- $\deg(f) = \max\{\deg(x^\mu) \mid x^\mu \in \text{supp}(f)\}$: *Grad* von f .
- Für Termordnung $\prec$ auf $\mathbb{T}^n$ und $f \neq 0$: $\text{lt}_\prec(f) = \max_\prec(\text{supp}(f))$: *Leitterm* von f .
- Für Ideal $I \trianglelefteq \mathcal{P}$: $\text{lt}_\prec(I) = \langle \text{lt}_\prec(f) \mid f \in I \setminus \{0\} \rangle$: *Leitideal* von I . (Monomiales Ideal).

- Wir kennen: Involutive Basen monomialer Ideale.
- Ziel: Geeignete Definition für polynomiale Ideale $I \subseteq \mathcal{P}$.
- Benutze: Termordnung $\prec$, Leitideal $\text{Lt}_{\prec}(I)$.
- Involutive Basen sind spezielle Gröbnerbasen
- Kombinatorische Zerlegung des Leitideals $\rightsquigarrow$ Vektorraumzerlegung des polynomialen Ideals

Multiplikative Variablen

Erinnerung: Eine involutive Division auf $\mathbb{N}_0^n$ weist einem Multiindex $\mu \in \mathcal{N} \subset \mathbb{N}_0^n$ die multiplikativen Indizes $N_{L,\mathcal{N}}(\mu)$ zu.

Definition

Sei $H \subset \mathcal{P} \setminus \{0\}$ endlich, $\prec$ eine Termordnung, L eine involutive Division auf $\mathbb{N}_0^n$. Schreibe $\text{lt}_{\prec}(H) = \{\text{lt}_{\prec}(h) \mid h \in H\}$, $\text{le}_{\prec}(H) = \{\mu \mid x^\mu \in \text{lt}_{\prec}(h)\}$, und

$$X_{L,\prec,H}(h) = \{x_i \in \{x_1, \dots, x_n\} \mid i \in N_{L,\text{le}_{\prec}(H)}(\text{le}_{\prec}(h))\}$$

für die Menge der *multiplikativen Variablen* von $h \in H$.

Die Variablen in $\{x_1, \dots, x_n\} \setminus X_{L,\prec,H}(h)$ heißen *nichtmultiplikativ* für $h \in H$.

Schreibe $\mathcal{C}_{L,\text{lt}_{\prec}(H)}(\text{lt}_{\prec}(h)) = K[X_{L,\prec,H}(h)] \cdot \text{lt}_{\prec}(h) \cap \mathbb{T}^n$. (*Involutiver Kegel*)

Definition

Die *involutive Hülle* von $H \subset \mathcal{P} \setminus \{0\}$ ist

$$\langle H \rangle_{L, \prec} = \sum_{h \in H} K[X_{L, \prec, H}(h)] \cdot h.$$

Für $H \subset \mathbb{T}^n$ schreibe kurz: $\langle H \rangle_L$, da unabhängig von $\prec$.

Beispiel

Sei $\prec$ die degrevlex-Ordnung auf $\mathbb{T}^3$ mit $x_1 \prec x_2 \prec x_3$ und sei $H = \{h\} = \{x_1 x_3^2 - x_1 x_2^2 + x_1 + x_2 + 1\}$. Dann gilt $\text{lt}_{\prec}(h) = x_1 x_3^2$. Für die Janet-Division sind alle Variablen multiplikativ für h , damit $\langle H \rangle_{J, \prec} = \langle H \rangle$. Für die Pommaret-Division ist wegen $\text{cls}(x_1 x_3^2) = 1$ nur x_1 multiplikativ für h und wir haben $\langle H \rangle_{P, \prec} = K[x_1] \cdot h \subsetneq \langle H \rangle$.

Definition

Sei $H \subset I \trianglelefteq \mathcal{P}$ endlich. Dann heißt H ...

- (i) ... *schwache involutive Basis* von I bezüglich L , $\prec$, falls $\text{lt}_{\prec}(H)$ eine schwache involutive Basis von $\text{lt}_{\prec}(I)$ bezüglich L ist,
- (ii) ... *starke involutive Basis* von I bezüglich L , $\prec$, falls $\text{lt}_{\prec}(H)$ eine starke involutive Basis von $\text{lt}_{\prec}(I)$ bezüglich L ist und keine zwei $h_1 \neq h_2 \in H$ den selben Leitterm haben.

Die Zusatzbedingung in (ii) stellt sicher, dass jeder Leitterm $x^\mu \in \text{lt}_{\prec}(I)$ genau bzgl. einem einzigen Element $h \in H$ involutiv reduzibel ist, d.h. es existiert genau ein $h \in H$, sodass $x^\mu \in \mathcal{C}_{L, \text{lt}_{\prec}(H)}(\text{lt}_{\prec}(h))$.

Definition

Sei $H \subset \mathcal{P}$ eine endliche Menge. Ein Polynom $g \in I = \langle H \rangle$ heißt *Obstruktion zur Involution* für H bzgl. der Termordnung $\prec$ und der involutiven Division L , wenn $g \notin \langle H \rangle_{L,\prec}$.

Vorsicht! Es gibt Erzeugendensysteme, die aus anderen Gründen keine involutive Basis sind.

Beispiel

Nicht jedes $F \subset I$ mit $\langle F \rangle_{L,\prec} = I$ ist eine involutive Basis von I . Betrachte $L = P$, $F = \{x_2^2, x_1 + x_2^2\} \subset K[x_1, x_2]$, lexikographische Ordnung $\prec$ mit $x_1 \prec x_2$. Es gilt $\text{It}_{\prec}(F) = \{x_2^2\}$ und $X_{P,\prec}(x_2^2) = X_{P,\prec}(x_1 + x_2^2) = \{x_1, x_2\}$, da alle Leiterterme Klasse 2 haben. Also $\langle F \rangle_{P,\prec} = \langle F \rangle$, aber $x_1 \in I$, also $x_1 \in \text{It}_{\prec}(\langle F \rangle) \setminus \langle \text{It}_{\prec}(F) \rangle_{P,\prec}$. Also F keine involutive Basis von $\langle F \rangle$.

- Sei $G \subset I$ Gröbnerbasis von $I \trianglelefteq \mathcal{P}$, dann $\langle \text{lt}(G) \rangle = \text{lt}(I)$
- Berechne monomiale involutive Basis B von $\langle \text{lt}(G) \rangle$.
- Finde für jedes $x^\mu \in B$ ein $f_\mu \in I$ mit $\text{lt}(f) = x^\mu$
- Erhalte involutive Basis $H = \{f_\mu \mid x^\mu \in B\}$ von I
- H starke Basis $\iff B$ starke monomiale involutive Basis
- Werden besseres Rechenverfahren kennenlernen

Beispiel

Buchberger-Algorithmus $\rightsquigarrow$ Aus $F = \{x_2^2, x_1 + x_2^2\}$ berechne reduzierte Gröbnerbasis $G = \{x_2^2, x_1\}$ von $I = \langle F \rangle$. I monomial und nulldimensional $\rightsquigarrow$ finde leicht die starke Pommaret-Basis $H = \{x_1, x_1x_2, x_2^2\}$ von I .

Ermittlung starker Basen aus schwachen

Lemma

Sei H eine schwache involutive Basis von $I = \langle H \rangle$. Dann existiert eine starke involutive Basis $H' \subseteq H$ von I .

Beweis.

Folgt aus der entsprechenden Aussage für monomiale involutive Basen. Zusätzlich müssen unter Umständen noch Elemente entfernt werden, damit die Leiterterme der Basiselemente paarweise verschieden sind. $\square$

Beispiel

Betrachte $K[x_1, x_2]$ mit degrevlex-Ordnung $\prec$ mit $x_1 \prec x_2$. Aus der schwachen Pommaret-Basis $\{1 + x_1, x_1 + x_1^2, x_2, x_2 + x_1 + 1\}$ erhalte die starke Pommaret-Basis $\{1 + x_1, x_2\}$.

Involutive Basen: Beispiele (1)

Beispiel

Betrachte $F = \{f_1, f_2, f_3\} \subset K[x, y, z]$ und Ideal $I = \langle F \rangle \trianglelefteq K[x, y, z]$, wobei $f_1 = z^2 - xy$, $f_2 = yz - x$ und $f_3 = y^2 - z$. Wähle $\prec$ als degrevlex-Ordnung mit $x \prec y \prec z$. Man kann nachrechnen, dass $\text{lt}_{\prec}(I) = \langle z^2, yz, y^2 \rangle = \langle \text{lt}_{\prec}(F) \rangle$. Wegen $X_P(z^2) = \{x, y, z\}$, $X_P(yz) = \{x, y\}$ und $X_P(y^2) = \{x, y\}$ gilt auch $\langle \text{lt}_{\prec}(F) \rangle_P = \text{lt}_{\prec}(I)$. Leiterterme von f_1, f_2, f_3 paarweise verschieden $\rightsquigarrow F$ starke Pommaret- und Janet-Basis von I .

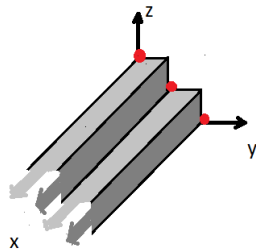


Figure: Escalier und Janet-Basis des Leitideals $\text{lt}_{\prec}(I)$

Involutive Basen: Beispiele (2)

Beispiel

Sei wieder $F = \{f_1, f_2, f_3\} \subset K[x, y, z]$ und $I = \langle F \rangle$, mit $f_1 = z^2 - xy$, $f_2 = yz - x$ und $f_3 = y^2 - z$. Wähle deglex-Ordnung $\prec$ mit $z \prec y \prec x$. Es gilt $\text{lt}_\prec(I) = \langle xy, yz, y^2, z^3 \rangle \neq \langle \text{lt}_\prec(F) \rangle$. Wegen $X_P(z^3) = \{x, y, z\}$, $X_P(yz) = \{x, y\}$, $X_P(y^2) = \{x, y\}$, $X_P(xy) = \{x\}$ und $X_P(yz^2) = \{x, y\}$ ist $\{xy, yz, y^2, z^3, yz^2\}$ starke Pommaret-Basis von $\text{lt}_\prec(I)$. Mit $f_4 = z^3 - x^2$ und $f_5 = yz^2 - xz$ erhalte starke Pommaret- und auch Janet-Basis $G = \{f_1, \dots, f_5\}$ von I .

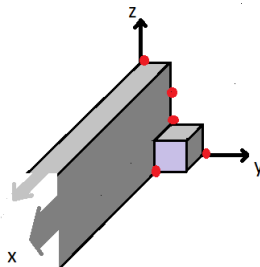


Figure: Escalier und Janet-Basis des Leitideals $\text{lt}_\prec(I)$

Involutive Basen: Beispiele (3)

Beispiel

Sei wieder $F = \{f_1, f_2, f_3\} \subset K[x, y, z]$ und $I = \langle F \rangle$, wobei $f_1 = z^2 - xy$, $f_2 = yz - x$ und $f_3 = y^2 - z$. Wähle $\prec$ als lex-Ordnung, $z \prec y \prec x$. Dann $\text{Lt}_{\prec}(I) = \langle x, y^2 \rangle = \langle \text{Lt}_{\prec}(F) \rangle$. Wir haben $\text{Lt}_{\prec}(F) = \{x, xy, y^2\}$; wegen $N_{J, \text{Lt}_{\prec}(F)}(x) = \{x, z\}$, $N_{J, \text{Lt}_{\prec}(F)}(xy) = \{x, z\}$ und $N_{J, \text{Lt}_{\prec}(F)}(y^2) = \{x, y, z\}$ ist dies monomiale Janet-Basis von $\text{Lt}_{\prec}(I)$. Also F starke Janet-Basis von I . Die Menge $\{x^\nu \in \text{Lt}_{\prec}(I) \mid x^\nu / x_{\text{cls}(\nu)} \notin \text{Lt}_{\prec}(I)\}$ ist nicht endlich $\rightsquigarrow I$ hat bzgl. dieser Termordnung *keine* Pommaret-Basis.

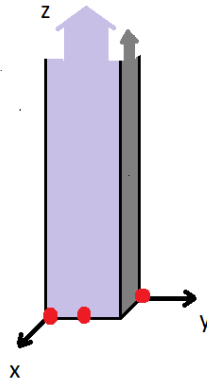


Figure: Escalier und Janet-Basis des Leitideals $\text{Lt}_{\prec}(I)$

Involutive (Leitterm-)Reduzierbarkeit

Definition

Sei $0 \neq g \in \mathcal{P}$ ein Polynom, $F \subset \mathcal{P} \setminus \{0\}$ endliche Menge von Polynomen. Sei L eine involutive Division und $\prec$ eine Termordnung. g heit...

- ① ... *involutiv Leitterm-reduzibel* bzgl. F , L und $\prec$, wenn
$$\exists \text{lt}_{\prec}(f) \in \text{lt}_{\prec}(F) : \text{lt}_{\prec}(f) |_{L, \text{lt}_{\prec}(F)} \text{lt}_{\prec}(g),$$
- ② ... *involutiv reduzibel* bzgl. F , L , $\prec$, wenn
$$\exists \text{lt}_{\prec}(f) \in \text{lt}_{\prec}(F), x^{\nu} \in \text{supp}(g) : \text{lt}_{\prec}(f) |_{L, \text{lt}_{\prec}(F)} x^{\nu}.$$

Jedes involutiv Leitterm-reduzible Polynom ist auch involutiv reduzibel, Umkehrung i.A. falsch.

Beispiel

Sei $F = \{x_2^2, x_1 + x_2^2\}$, $\prec$ degrevlex-Ordnung mit $x_1 \prec x_2$ und $L = P$; dann $g = x_1^3 + x_2^2$ involutiv reduzibel bzgl. F , aber nicht involutiv Leitterm-reduzibel; jedes $f \in F$ involutiv Leitterm-reduzibel bzgl. $F \setminus \{f\}$.

Divisionsalgorithmus (1)

Algorithm 1: Involutive Polynomdivision

Data: Poly. $g \in \mathcal{P}$, endl. Menge $F = \{f_1, \dots, f_m\} \subset \mathcal{P} \setminus \{0\}$, inv. Div. L , Termordg. $\prec$, endl. Kontextmenge $\hat{F} \supset F$

Result: Polynome $r \in \mathcal{P}$, $q_1, \dots, q_m$ mit $q_i \in K[X_{L, \prec, \hat{F}}(f_i)]$, r nicht involutiv reduzibel bzgl. F im Kontext $\hat{F}$, $g = r + \sum_{i=1}^m q_i \cdot f_i$

begin

```
   $r \leftarrow g$ ;  $[q_1, \dots, q_m] \leftarrow [0, \dots, 0]$ 
  while  $\exists x^\nu \in \text{supp}(r), f_i \in F : \text{lt}(f_i)|_{L, \text{lt}_\prec(\hat{F})} x^\nu$  do
     $r \leftarrow r - (\text{lc}(r) / \text{lc}(f_i))(x^\nu / \text{lt}(f_i))f_i$ 
     $q_i \leftarrow q_i + (\text{lc}(r) / \text{lc}(f_i))(x^\nu / \text{lt}(f_i))$ 
  return  $r, q_1, \dots, q_m$ 
```

Bemerkung

Oft wird man für die Kontextmenge einfach F selbst nehmen.

Divisionsalgorithmus (2)

Satz

Der Algorithmus `InvolutivePolynomdivision` ist korrekt und terminiert.

Beweis.

- $\text{It}(\hat{F})$ ändert sich nicht; Korrektheit bei Terminierung klar
- Kodiere inv. reduzible Terme von $\text{supp}(r)$ in Blättern eines Baumes
- Jeder Schleifendurchlauf: reduzierbarer Term ersetzt durch endlich viele neue Terme.
- Reduzible neue Terme $\rightsquigarrow$ Kinder des bearbeiteten Knotens, außer bei Weghebungen von Termen; Dann kann der Baum verkleinert werden.
- Wenn kein neuer Term reduzibel $\rightsquigarrow$ bearbeiteter Knoten markiert
- Kinder immer $\prec$ -kleiner als Elternknoten, $\prec$ Wohlordnung, Lemma von König $\rightsquigarrow$ Terminierung.



Involutive Leitterm-Autoreduktion (1)

Definition

Die endliche Menge $H \subset \mathcal{P} \setminus \{0\}$ heißt *involutiv Leitterm-autoreduziert* bzgl. der Termordnung $\prec$ und der involutiven Division L , wenn die Menge von Termen $\text{lt}_{\prec}(H)$ L -involutiv autoreduziert ist und keine zwei Polynome $h_1 \neq h_2 \in H$ denselben $\prec$ -Leitterm haben.

Ziel: Bestimme für Menge $H \subset \mathcal{P}$ eine Leitterm-autoreduzierte Menge $\tilde{H} \subset \langle H \rangle$ mit $\langle \tilde{H} \rangle = \langle H \rangle$.

Beispiel

Man darf *nicht* einfach Polynome entfernen, nur weil ihr Leitterm doppelt auftaucht: Sei $H = \{x_2^2, x_1 + x_2^2\} \subset K[x_1, x_2]$, $\prec$ lex-Ordnung mit $x_1 \prec x_2$. Es gilt $\text{lt}_{\prec}(x_2^2) = \text{lt}_{\prec}(x_1 + x_2^2) = x_2^2$. Zwar sind die Mengen $\{x_2^2\}, \{x_1 + x_2^2\}$ für sich genommen involutiv Leitterm-autoreduziert (da einelementig), aber keine von beiden erzeugt das Element $x_1 \in \langle H \rangle$.

Involutive Leitterm-Autoreduktion (2)

Algorithm 2: Involutive Leitterm-Autoreduktion

Data: endl. Menge $F \subset \mathcal{P} \setminus \{0\}$, inv. Division L , Termordnung $\prec$

Result: inv. Leitterm-autoreduzierte Menge $\tilde{F}$ mit $\langle \tilde{F} \rangle = \langle F \rangle$

begin

$\tilde{F} \leftarrow F$

while $\exists f \neq g \in \tilde{F} : \text{lt}(f)|_{L, \text{lt}(\tilde{F})} \text{lt}(g)$ **do**

$\hat{g} \leftarrow g - (\text{lc}(g)/\text{lc}(f))(\text{lt}(g)/\text{lt}(f))f$

if $\hat{g} = 0$ **then**

$\tilde{F} \leftarrow \tilde{F} \setminus \{g\}$

else

$\tilde{F} \leftarrow (\tilde{F} \setminus \{g\}) \cup \{\hat{g}\}$

return $\tilde{F}$

Involutive Leitterm-Autoreduktion (3)

Bemerkung

Der Algorithmus *InvolutiveLeittermAutoreduktion* ist korrekt und terminiert. (Korrektheit: klar; Terminierung: Konstruiere geeignete Wohlordnung auf $(\mathbb{T}^n)^{|F|}$.)

Beispiel

- 1 Wende den Algorithmus auf $F = \{x_2^2, x_1 + x_2^2\}$ an, mit $\prec$ der lex-Ordnung mit $x_1 \prec x_2$ und der Pommaret-Division. Die `while`-Schleife wird nur einmal durchlaufen; je nach dem, welches Element als f und welches als g interpretiert wird, erhält man $\tilde{F} = \{x_1, x_2^2\}$ oder $\tilde{F} = \{-x_1, x_1 + x_2^2\}$.
- 2 Ändere in diesem Beispiel die Termordnung zur lex-Ordnung mit $x_1 \succ x_2$. Dann gilt $\text{lt}(x_1 + x_2^2) = x_1$ und somit ist F bereits involutiv Leitterm-autoreduziert.

Zerlegungssatz für Leiterterm-autoreduzierte Mengen (1)

Satz

Sei $F \subset \mathcal{P} \setminus \{0\}$ eine endliche Menge, $\prec$ eine Termordnung, L eine involutive Division. Wenn F L -involativ Leiterterm-autoreduziert ist, dann besitzt die involutive Hülle von F die Darstellung

$$\langle F \rangle_{L,\prec} = \bigoplus_{f \in F} K[X_{L,\prec,F}(f)] \cdot f$$

als direkte Summe von K -Vektorräumen.

Beispiel

Die Voraussetzungen des Satzes implizieren *nicht*, dass $\langle F \rangle_{L,\prec} = \langle F \rangle$, wie man an dem monomialen Beispiel $F = \{x_1\} \subset K[x_1, x_2]$, zusammen mit der Pommaret-Division P , leicht sehen kann.

Zerlegungssatz für Leiterterm-autoreduzierte Mengen (2)

Beweis.

Sei F L -involutiv Leiterterm-autoreduziert. Wir müssen zeigen, dass nur eine Darstellung der 0 in $\langle F \rangle_{L, \prec}$ existiert. Dazu:

- Sei $\sum_{f \in F} P_f \cdot f \in \langle F \rangle_{L, \prec}$, nicht alle $P_f = 0$.
- F Leiterterm-autoreduziert $\implies \text{lt}_{\prec}(P_f \cdot f) \in \mathcal{C}_{L, \text{lt}_{\prec}(F)}(\text{lt}_{\prec}(f))$ (für $f \in F$ mit $P_f \neq 0$) paarweise verschieden
- Sei $x^{\mu} := \text{lt}_{\prec}(P_{f_{\max}} \cdot f_{\max})$ das $\prec$ -Maximum dieser Terme
- Es folgt $\text{lt}_{\prec}(\sum_{f \in F} P_f \cdot f) = x^{\mu}$, Summe also $\neq 0$.



Involutive Normalform (1)

Folgerung

Sei $\emptyset \neq F \subset \mathcal{P} \setminus \{0\}$ involutiv Leiterterm-autoreduziert bzgl. der involutiven Division L und der Termordnung $\prec$. Dann gilt:

- ① $\mathcal{P} = \langle \mathbb{T}^n \setminus \langle \text{lt}_{\prec}(F) \rangle_L \rangle_K \oplus \langle F \rangle_{L, \prec}$.
- ② Jedes Polynom $g \in \mathcal{P}$ besitzt eine eindeutige Normalform $\text{NF}_{F, L, \prec}(g) \in \langle \mathbb{T}^n \setminus \langle \text{lt}_{\prec}(F) \rangle_L \rangle_K$ mit $g - \text{NF}_{F, L, \prec}(g) \in \langle F \rangle_{L, \prec}$.

Beweis.

- Es reicht, Teil 1 zu zeigen; Teil 2 folgt dann sofort.
- " + " folgt aus der Anwendung des Algorithmus `InvolutivePolynomdivision` auf ein allgemeines Polynom $g \in \mathcal{P}$.
- " $\oplus$ " folgt dann aus dem Beweis des letzten Satzes, denn für jedes Polynom $0 \neq h \in \langle F \rangle_{L, \prec}$ wurde hergeleitet, dass $\text{lt}_{\prec}(h) \in \langle \text{lt}_{\prec}(F) \rangle_L$.



Involutive Normalform (2)

Folgerung

Sei $\emptyset \neq F = \{f_1, \dots, f_m\} \subset \mathcal{P} \setminus \{0\}$ involutiv Leiterterm-autoreduziert bzgl. der involutiven Division L und der Termordnung $\prec$. Dann gilt folgende Zerlegung von $\mathcal{P}$ als K -Vektorraum:

$$\mathcal{P} = \langle \mathbb{T}^n \setminus \langle \text{lt}_{\prec}(F) \rangle_L \rangle_K \oplus \left(\bigoplus_{f \in F} K[X_{L, \prec, F}(f)] \cdot f \right),$$

und jedes Polynom $g \in \mathcal{P}$ besitzt eine eindeutige Darstellung $g = \text{NF}_{F, L, \prec}(g) + \sum_{f \in F} P_f \cdot f$ mit $P_f \in K[X_{L, \prec, F}(f)]$. Die Abbildung

$$\begin{aligned} \mathcal{P} &\longrightarrow \langle \mathbb{T}^n \setminus \langle \text{lt}_{\prec}(F) \rangle_L \rangle_K \times K[X_{L, \prec, F}(f_1)] \times \cdots \times K[X_{L, \prec, F}(f_m)], \\ g &\mapsto (\text{NF}_{F, L, \prec}(g), P_{f_1}, \dots, P_{f_m}) \end{aligned}$$

ist K -linear.

Involutive Normalform (3)

Bemerkung

Wenn die endliche Menge $F \subset \mathcal{P} \setminus \{0\}$ nicht L -involativ Leiterterm-autoreduziert ist, dann gilt höchstens eine der Zerlegungen $\langle F \rangle_{L, \prec} = \bigoplus_{f \in F} K[X_{L, \prec, F}(f)] \cdot f$ und $\mathcal{P} = \langle \mathbb{T}^n \setminus \langle \text{lt}_{\prec}(F) \rangle_L \rangle_K \oplus \langle F \rangle_{L, \prec}$.

Beispiel

- $F_1 = \{x_1, x_1^2\} \subset K[x_1]$ ist bzgl. der Pommaret-Division nicht involativ Leiterterm-autoreduziert, und $K[x_1] \cdot x_1 \cap K[x_1] \cdot x_1^2 \neq \{0\}$; aber trotzdem $K[x_1] = \langle 1 \rangle_K \oplus \langle F_1 \rangle_{P, \prec}$. Involutive Normalformen bzgl. F_1 sind eindeutig ($\text{NF}_{F_1, P}(\sum g_\ell x_1^\ell) = g_0$).
- $F_2 = \{1 + x_1 x_2, x_1 x_2\} \subset K[x_1, x_2]$ ist nicht P -involativ Leiterterm-autoreduziert. Aber $K[x_1] \cdot (1 + x_1 x_2) \cap K[x_1] \cdot x_1 x_2 = \{0\}$. Jedoch ist $1 \in \langle \mathbb{T}^2 \setminus \mathcal{C}_P(x_1 x_2) \rangle_K \cap \langle F_2 \rangle_{P, \prec}$. $x_1 x_2$ hat keine eindeutige involutive Normalform bzgl. F_2 .

Vollständige involutive Autoreduktion (1)

Definition

Die endliche Menge $H \subset \mathcal{P} \setminus \{0\}$ heißt *vollständig involtiv autoreduziert* bzgl. der Termordnung $\prec$ und der involtiven Division L , wenn sie L -involtiv Leiterterm-autoreduziert ist und kein Term im Träger eines Polynoms $h \in H$ L -involtiv teilbar (im Kontext $\text{It}_{\prec}(H)$) durch einen der Leiterterme aus $\text{It}_{\prec}(H)$ ist.

Vollständige involutive Autoreduktion (2)

Algorithm 3: Vollständige involutive Autoreduktion

Data: endl. Menge $F \subset \mathcal{P} \setminus \{0\}$, inv. Division L , Termordnung $\prec$

Result: Vollständig involutiv autoreduzierte Menge $\tilde{F}$ mit $\langle \tilde{F} \rangle = \langle F \rangle$

begin

$\tilde{F} \leftarrow F$

$\tilde{F} \leftarrow \text{InvolutiveLeittermAutoreduktion}(\tilde{F}, L, \prec)$

foreach $f \in \tilde{F}$ **do**

$f \leftarrow \text{InvolutivePolynomdivision}(f, \tilde{F} \setminus \{f\}, L, \prec, \tilde{F})$

return $\tilde{F}$

Fakt

Der Algorithmus `VollständigeInvolutiveAutoreduktion` ist korrekt und terminiert.

Satz

Seien $H \subset I \setminus \{0\}$ eine endliche Teilmenge des Ideals $I \trianglelefteq \mathcal{P}$. Dann sind die folgenden Aussagen äquivalent:

- (i) H ist schwache involutive Basis von I bzgl. $L, \prec$
- (ii) Für alle $f \in I$ existiert eine involutive Standarddarstellung

$$f = \sum_{h \in H} P_h \cdot h, \quad P_h \in K[X_{L, \prec, H}(h)], \quad \text{lt}_{\prec}(P_h \cdot h) \preceq \text{lt}_{\prec}(f) \quad \forall h \in H.$$

- (iii) $\langle H \rangle_{L, \prec} = I$ und $\langle \text{lt}_{\prec}(H) \rangle_L = \text{lt}_{\prec}(I)$.

Charakterisierung schwacher involutiver Basen (2)

Beweis.

"(i) $\Rightarrow$ (ii):" Folgt aus Anwendung von `InvolutivePolynomdivision` auf ein allgemeines Polynom $f \in I$ und die Menge H .

"(ii) $\Rightarrow$ (iii):" Sei $f \in I$ beliebig. Aus der Standarddarstellung in (ii) $\Rightarrow \exists h \in H : \text{lt}_{\prec}(P_h \cdot h) = \text{lt}_{\prec}(P_h) \cdot \text{lt}_{\prec}(h) = \text{lt}_{\prec}(f) \Rightarrow \text{lt}_{\prec}(f) \in \langle \text{lt}_{\prec}(H) \rangle_L$.
 $f \in I$ war beliebig $\rightsquigarrow \langle \text{lt}_{\prec}(H) \rangle_L = \text{lt}_{\prec}(I)$. Außerdem folgt $\langle H \rangle_{L, \prec} = I$ sofort aus (ii).

"(iii) $\Rightarrow$ (i):" trivial. □

Charakterisierung starker involutiver Basen (1)

Satz

Seien $H \subset I \setminus \{0\}$ eine endliche Teilmenge des Ideals $I \trianglelefteq \mathcal{P}$. Dann sind die folgenden Aussagen äquivalent:

- (i) H ist **starke** involutive Basis von I bzgl. $L, \prec$
- (ii) Für alle $f \in I$ existiert eine **eindeutige** involutive Standarddarstellung

$$f = \sum_{h \in H} P_h \cdot h, \quad P_h \in K[X_{L, \prec, H}(h)], \quad \text{lt}_{\prec}(P_h \cdot h) \preceq \text{lt}_{\prec}(f) \quad \forall h \in H.$$

- (iii) H ist **L -involativ Leitterm-autoreduziert**, $\langle H \rangle_{L, \prec} = I$ und $\langle \text{lt}_{\prec}(H) \rangle_L = \text{lt}_{\prec}(I)$.
- (iv) H ist **L -involativ Leitterm-autoreduziert** und $\langle \text{lt}_{\prec}(H) \rangle_L = \text{lt}_{\prec}(I)$.

Charakterisierung starker involutiver Basen (2)

Beweis.

"(i) $\Rightarrow$ (ii)": H starke inv. Basis $\Rightarrow \text{lt}_{\prec}(H)$ inv. autoreduziert $\Rightarrow H$ involutiv Leiterterm-autoreduziert $\Rightarrow$ Eindeutigkeit. Existenz folgt aus Anwendung des Algorithmus `InvolutivePolynomdivision` auf f und H .

"(ii) $\Rightarrow$ (iii)":

- Existenz der Standarddarstellung $\Rightarrow$ (wie bei schwachen Basen) $\langle \text{lt}_{\prec}(H) \rangle_L = \text{lt}_{\prec}(I)$. Damit H involutive Basis und $\langle H \rangle_{L,\prec} = I$.
- Insbesondere besitzt jedes $f \in I$ die involutive H -Normalform 0.
- Wäre H nicht inv. Leiterterm-autoreduziert, dann gäbe es $h_1 \neq h_2 \in H$ mit $\text{lt}_{\prec}(h_1) \mid_{L, \text{lt}_{\prec}(H)} \text{lt}_{\prec}(h_2)$; h_2 hätte dann mindestens zwei verschiedene inv. Standarddarstellungen: $h_2 = 1 \cdot h_2$ und eine Darstellung $h_2 = (\text{lc}(h_2)/\text{lc}(h_1))(\text{lt}_{\prec}(h_2)/\text{lt}_{\prec}(h_1)) \cdot h_1 + \dots$, in der der Koeffizient P_{h_2} vor h_2 verschwindet.

"(iii) $\Rightarrow$ (iv)": trivial; "(iv) $\Rightarrow$ (i)": klar. □

Folgerung

Sei $\{0\} \neq I \trianglelefteq \mathcal{P}$ ein Ideal, $\prec$ eine Termordnung, L eine involutive Division und $H \subset I \setminus \{0\}$ eine schwache L -involutive Basis von I . Dann gilt:

- 1 $\langle H \rangle_{L, \prec} = I$ und H ist $\prec$ -Gröbnerbasis von I
- 2 $\mathcal{P} = \langle \mathbb{T}^n \setminus \text{lt}_{\prec}(I) \rangle_K \oplus I$
- 3 Jedes $f \in \mathcal{P}$ besitzt eindeutige involutive Normalform $\text{NF}_{H, \prec, L}(f)$; die Normalformabbildung ist K -linear.

Beispiel

$F = \{x_1, x_1^2\} \subset K[x_1]$ ist eine schwache Pommaret-Basis von $I = \langle F \rangle$. F enthält die Gröbnerbasis $\{x_1\}$. Es gilt $\mathcal{P} = \langle 1 \rangle_K \oplus I$. Jedes $f = \sum f_\ell x_1^\ell$ besitzt seinen konstanten Term f_0 als eindeutige Pommaret- F -Normalform.

Folgerung

Seien I , $\prec$, L wie oben und sei $H = \{h_1, \dots, h_m\} \subset I$ eine starke L -involutive Basis von I . Dann gilt zusätzlich:

- 1 $I = \bigoplus_{h \in H} K[X_{L, \prec, H}(h)] \cdot h$.
- 2 Jedes $f \in I$ besitzt eindeutige involutive Darstellung $f = \sum_{h \in H} P_h \cdot h$ mit $P_h \in K[X_{L, \prec, H}(h)]$ und diese ist eine Standarddarstellung mit $|\{h \in H \mid \text{lt}_{\prec}(P_h \cdot h) = \text{lt}_{\prec}(f)\}| = 1$
- 3 Die Standarddarstellungsabbildung

$$I \longrightarrow K[X_{L, \prec, H}(h_1)] \times \cdots \times K[X_{L, \prec, H}(h_m)], \quad f \mapsto (P_{h_1}, \dots, P_{h_m})$$

ist K -linear.

Beispiel

Betrachte die starke Pommaret-Basis $F = \{f_1, f_2, f_3\} \subset K[x, y, z]$ des Ideals $I = \langle F \rangle \trianglelefteq K[x, y, z]$ bzgl. der degrevlex-Ordnung mit $x \prec y \prec z$, wobei $f_1 = z^2 - xy$, $f_2 = yz - x$ und $f_3 = y^2 - z$.

- Das Polynom $g_1 = yz^2 + y^2z$ hat die F -Normalform $\text{NF}_{F, \prec, P}(g_1) = xz + xy$
- $g_1 - \text{NF}(g_1)$ hat die Standarddarstellung $yf_1 + yf_2 + xf_3$
- $g_2 = yz^2$ hat die F -Normalform $\text{NF}_{F, \prec, P}(g_2) = xz$
- $g_2 - \text{NF}(g_2)$ hat die Standarddarstellung $yf_1 + xf_3$
- Es folgt wegen der K -Linearität der Normalform und der Standarddarstellung: $g_3 = g_1 - g_2 = y^2z$ hat die F -Normalform $\text{NF}_{F, \prec, P}(g_3) = xy$ und $g_3 - \text{NF}(g_3)$ hat die Standarddarstellung yf_2 .

Minimale involutive Basen (1)

Definition

Sei $H \subset I \setminus \{0\}$ eine starke involutive Basis des Ideals $I \trianglelefteq \mathcal{P}$ bzgl. der involutiven Division L und der Termordnung $\prec$. Dann heit H ...

- ① ... *minimal*, wenn $\text{lt}_{\prec}(H)$ eine minimale L -involutive Basis von $\text{lt}_{\prec}(I)$ im monomialen Sinne ist,
- ② ... *reduziert minimal*, wenn H minimal und vollstndig involutiv autoreduziert ist und $\text{lc}(h) = 1$ fr alle $h \in H$ gilt.

Satz

Sei $\{0\} \neq I \trianglelefteq \mathcal{P}$ ein Ideal, L eine involutive Division, fr die jedes monomiale Ideal eine minimale L -involutive Basis besitzt und $\prec$ eine Termordnung. Dann besitzt I genau eine reduzierte minimale L -involutive Basis $H \subset I$.

Minimale involutive Basen (2)

Beweis.

- Existenz: Zur minimalen L -involutiven Basis B von $\text{It}_{\prec}(I)$ gibt es zu jedem $x^{\mu} \in B$ ein normiertes Polynom $f_{\mu} \in I$ mit $\text{It}_{\prec}(f_{\mu}) = x^{\mu}$. Wende auf $\{f_{\mu} \mid x^{\mu} \in B\}$ den Algorithmus `VollständigeInvolutiveAutoreduktion` an.
- Eindeutigkeit: Seien zwei reduzierte minimale involutive Basen $\{f_{\mu} \mid x^{\mu} \in B\}$, $\{g_{\mu} \mid x^{\mu} \in B\}$ von I gegeben. Es gilt $\forall x^{\mu} \in B$: $\text{supp}(f_{\mu} - g_{\mu}) \subseteq \mathbb{T}^n \setminus \text{It}_{\prec}(I)$ und $f_{\mu} - g_{\mu} \in I$. Also $f_{\mu} - g_{\mu} = 0$.



- Falls minimale involutive Basis MIB von I existiert: Einfaches Komplexitätsmaß: Vergleich zu reduzierter Gröbnerbasis RGB
- Quotient $Q(I) := |MIB(I)|/|RGB(I)|$ misst, wie groß die minimale involutive Basis im Verhältnis zur reduzierten Gröbnerbasis ist
- Für verschiedene Typen von Idealen kann $Q(I)$ nahe bei 1 sein, für andere ziemlich hoch
- *stabile monomiale Ideale*: Pommaretbasis existiert und $Q(I) = 1$
- *torische Ideale*: $Q(I)$ unter Umständen sehr hoch für die Janetdivision.

Spezialfall: Nulldimensionale Ideale

Fakt

Sei $\{0\} \neq I \subseteq \mathcal{P}$ ein nulldimensionales Ideal. Dann ist $\dim(\text{lt}_{\prec}(I)) = 0$ für jede Termordnung $\prec$, und sowohl für die Pommaret-Division P als auch für die Janet-Division J existiert die reduzierte minimale involutive Basis von I . Diese beiden Basen sind sogar gleich.

Beispiel

Pommaret-Basen betrachtet man meistens bezüglich der degrevlex-Termordnung $\prec$ mit $x_1 \prec x_2 \prec \dots \prec x_n$. Ein einfaches nicht-monomiales Beispiel in $K[x_1, x_2]$ ist die Basis $H = \{x_2^2 + x_2 + 1, x_1x_2 + x_2, x_1 + 1\}$, die sowohl die reduzierte minimale Janet- als auch Pommaret-Basis des 0-dimensionalen Ideals $\langle H \rangle$ bzgl. dieser degrevlex-Ordnung ist.

-  SEILER, W. M. : *A combinatorial approach to involution and δ -regularity I: Involutive bases in polynomial algebras of solvable type.* Appl. Alg. Eng. Comm. Comp., 20:207-259, 2009.
-  SEILER, W. M. : *Involution - The Formal Theory of Differential Equations and its Applications in Computer Algebra.* Springer, 2010.
-  GERDT, V. P.; BLINKOV, Yu. A. : *Involutive Bases of Polynomial Ideals.* Math. Comput. Simul., 45:519-542, 1998.