AℓZAGK – Invariantentheorie

Ralf Donau

28 Januar 2005

Vorbereitungen zur algorithmischen Bestimmung der Hironaka Zerlegung

Algorithmus 1 *Seien $f_1, \ldots, f_m, f \in \mathbb{C}[X]$ und $I = \langle f_1, \ldots, f_m \rangle$ ein Ideal.*

Frage: *Liegt f in $\sqrt{I}$?*

Lösung: *Berechne eine reduzierte Gröbnerbasis G von $\langle f_1, \ldots, f_m, 1 - Yf \rangle$, wobei Y eine neue Variable ist. Dann gilt: $f \in \sqrt{I} \Longleftrightarrow 1 \in G$*

Der Beweis benötigt folgendes Lemma:

Lemma 1 *Sei k ein Körper, $I = \langle f_1, \ldots, f_m \rangle \subset k[X_1, \ldots, X_n]$ ein Ideal, $f \in k[X_1, \ldots, X_n]$. Dann gilt:*

$$f \in \sqrt{I} \Longleftrightarrow 1 \in \widetilde{I} = \langle f_1, \ldots, f_m, 1 - Yf \rangle \subset k[X_1, \ldots, X_n, Y]$$

Beweis:

„$\Longrightarrow$":
$f \in \sqrt{I} \implies f^m \in I \subset \widetilde{I}$ für ein $m \in \mathbb{N}$
außerdem gilt: $(1 - Yf) \in \widetilde{I}$

$$1 = Y^m f^m + (1 - Y^m f^m) = Y^m \underbrace{f^m}_{\in \widetilde{I}} + \underbrace{(1 - Yf)}_{\in \widetilde{I}} \cdot (1 + Yf + \ldots + Y^{m-1} f^{m-1})$$

Also: $1 \in \widetilde{I}$
Erinnerung: $(X^m - 1) = (X - 1)(X^{m-1} + \ldots + 1)$

„$\Longleftarrow$":
$1 \in \widetilde{I} \implies 1 = \left[\sum_{i=1}^{s} p_i(X_1, \ldots, X_n, Y) f_i \right] + q(X_1, \ldots, X_n, Y)(1 - Yf)$
mit $p_1, \ldots, p_s, q \in \mathbb{C}[X_1, \ldots, X_n, Y]$

Es gilt: $\mathbb{C}[X_1, \ldots, X_n, Y] = \mathbb{C}[X_1, \ldots, X_n][Y] \subset \mathbb{C}(X_1, \ldots, X_n)[Y]$
Ersetze Y durch $\frac{1}{f}$ in $\mathbb{C}(X_1, \ldots, X_n)$
$\Longrightarrow 1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, \frac{1}{f})$
Die Summanden sind rationale Funktionen mit Potenzen von f im Nenner. Multipliziere beide Seiten mit f^m, so daß von allen Termen der Nenner verschwindet:
$\Longrightarrow f^m = \sum_{i=1}^{s} A_i f_i \in I$ mit $A_i \in \mathbb{C}[X]$
Also : $f \in \sqrt{I}$

□

Sei $G = \{g_1 \ldots g_t\}$ reduzierte Gröbnerbasis von $\widetilde{I}$. Zu zeigen: $1 \in \widetilde{I} \Longleftrightarrow 1 \in G$

„$\Longrightarrow$":
$1 \in \widetilde{I} \Longrightarrow 1 \in \langle LT(\widetilde{I})\rangle = \langle LT(g_1) \ldots LT(g_t)\rangle$ Monomialideal
1 ist Monom vom Multigrad 0, also gilt:
$LT(g_i) \mid 1$ für ein $i \in \{1 \ldots t\} \Longrightarrow LT(g_i)$ ist konstant für ein $i \in \{1 \ldots t\}$
Da es sich um eine reduzierte Gröbnerbasis handelt, gilt $LT(g_i) = 1$. Da 1 Multigrad 0 hat und damit das kleinste Element in der Monomialordnung ist, hat g_i keine weiteren Monome. Also gilt $g_i = 1$ und damit auch $1 \in G$.

„$\Longleftarrow$":
trivial, denn $\langle G\rangle = \widetilde{I}$

□

Algorithmus 2 *Seien $f_1, \ldots, f_m \in \mathbb{C}[X]$ nicht–konstante homogene Polynome.*

Frage: *Existiert $a \in \mathbb{C}^n$ mit $a \neq 0$, so daß $f_1(a) = \ldots = f_m(a) = 0$?*

Bemerkung: Es existiert ganau dann eine Lösung $\neq 0$, wenn $\sqrt{I} \neq \langle X_1, \ldots, X_n\rangle$.

Lösung: *Berechne eine reduzierte Gröbnerbasis G des Ideals $I = \langle f_1, \ldots, f_m\rangle$ bezüglich lex oder revlex. Es gilt: $\sqrt{I} = \langle X_1, \ldots, X_n\rangle \Longleftrightarrow$ für jedes $i \in \{1 \ldots n\}$ gehört ein Monom der Form $X_i^{j_i}$ mit $j_i \in \mathbb{N}$ zu $LT(G)$.*

Der Einfachheit wegen habe ich die Koeffizienten vor den Monomen weggelassen. Beweis:

„$\Longrightarrow$":
Sei $G = \{g_1 \ldots g_t\}$ reduzierte Gröbnerbasis von I.
$\sqrt{I} = \langle X_1, \ldots, X_n\rangle \Longrightarrow \forall i \in \{1 \ldots n\}\ \exists \widetilde{j_i} \in \mathbb{N} : X_i^{\widetilde{j_i}} \in I$
$\Longrightarrow \forall i : X_i^{\widetilde{j_i}} \in \langle LT(I)\rangle = \langle LT(g_1) \ldots LT(g_t)\rangle$ Monomialideal
$\Longrightarrow \forall i \in \{1 \ldots n\}\ \exists k_i \in \{1 \ldots s\} : LT(g_{k_i}) \mid X_i^{\widetilde{j_i}}$
$\Longrightarrow \forall i \in \{1 \ldots n\}\ \exists j_i \in \mathbb{N} : LT(g_{k_i}) = X_i^{j_i} \in LT(G)$

Für die umgekehrte Implikation wird ein Lemma benötigt:

Lemma 2 *Die reduzierte Gröbnerbasis eines homogenen Ideals besteht aus homogenen Polynomen.*

Zu zeigen:

1. Seien f und g homogene Polynome. Dann ist das S-Polynom $S(f,g)$ homogen.
2. Man verwende den Divisionsalgorithmus, um ein homogenes Polynom f durch homogene Polynome $f_1, \ldots, f_s$ zu dividieren. Dann ist der Divisionsrest r homogen.
3. Ein homogenes Ideal hat eine homogene Gröbnerbasis.
4. Die Behauptung

Zu 1.

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

wobei x^γ das kleinste gemeinsame Vielfache von $LT(f)$ und $LT(g)$ ist. Sei $f = \sum_{i=1}^{n} a_i X^{\alpha_i}$ und $g = \sum_{j=1}^{m} b_j X^{\beta_j}$. Es gilt $LT(f) = a_t X^{\alpha_t}$ für ein $t \in \{1 \ldots n\}$ und $LT(g) = b_s X^{\beta_s}$ für ein $s \in \{1 \ldots m\}$. Da f und g homogen sind, gilt $\deg(a_1 X^{\alpha_1}) = \ldots = \deg(a_n X^{\alpha_n})$ und $\deg(b_1 X^{\beta_1}) = \ldots = \deg(b_m X^{\beta_m})$.
Also:

$$\begin{aligned} S(f,g) &= \frac{X^\gamma}{a_t X^{\alpha_t}} \cdot \sum_{i=1}^{n} a_i X^{\alpha_i} - \frac{X^\gamma}{b_s X^{\beta_s}} \cdot \sum_{j=1}^{m} b_j X^{\beta_j} \\ &= \sum_{i=1}^{n} \overline{a}_i \frac{X^\gamma}{X^{\alpha_t}} \cdot X^{\alpha_i} + \sum_{j=1}^{m} \overline{b}_j \frac{X^\gamma}{X^{\beta_s}} \cdot X^{\beta_j} \end{aligned}$$

$$\text{mit } \overline{a}_i = \tfrac{a_i}{a_t} \text{ und } \overline{b}_j = -\tfrac{b_j}{b_s}$$

Für den Grad der einzelnen Monome von $S(f,g)$ gilt:

$$\begin{aligned} \deg \frac{X^\gamma}{X^{\alpha_t}} \cdot X^{\alpha_i} &= \deg X^\gamma \underbrace{- \deg X^{\alpha_t} + \deg X^{\alpha_i}}_{0} = \deg X^\gamma \\ \deg \frac{X^\gamma}{X^{\beta_s}} \cdot X^{\beta_j} &= \deg X^\gamma \end{aligned}$$

$$\text{mit } i \in \{1 \ldots n\} \text{ und } j \in \{1 \ldots m\}$$

Da $S(f,g)$ eine Summe von Monomen vom Grad $\deg X^\gamma$ ist, ist $S(f,g)$ ein homogenes Polynom.

Zu 2.

Wir erhalten die Darstellung $f = \sum_{i=1}^{s} a_i f_i + r$ durch folgenden Algorithmus:

$p := f$
$a_1 := 0, \ldots, a_s = 0, r := 0$
Solange $LT(p)$ von $LT(f_i)$ geteilt wird für ein $i \in \{1 \ldots s\}$:

$$a_i := a_i + LT(p)/LT(f_i) \text{ und } p := p - (LT(p)/LT(f_i))f_i$$

Falls $LT(p)$ nicht durch $LT(f_i)$ teilbar ist für ein $i \in \{1 \ldots s\}$:

$$p := p - LT(p) \text{ und } r := r + LT(p)$$

Falls $p = 0$ exit, sonst nochmal.

In der vorletzten Zeile des obigen Algorithmus werden p und r verändert. Der Anfangswert von p ist ein homogenes Polynom, welches in jedem Schritt homogen bleibt und seinen Grad behält, da $LT(p)$ denselben Grad wie p hat. r hat den Anfangswert 0 und mit jedem Schritt wird zu r ein Monom addiert, welches denselben Grad wie p hat. Deshalb bleibt r in jedem Schritt homogen.

Zu 3.

In dem Buchberger Algorithmus wird ein Erzeugendensystem (EZS) eines Ideals durch geeignete Elemente zu einer Gröbnerbasis ergänzt. Ein homogenes Ideal besitzt ein homogenes EZS. In jedem Schritt des Buchberger Algorithmus wird das S-Polynom von zwei Elementen des EZS gebildet und anschließend mit Rest durch das EZS dividiert. Dieser Rest wird zum EZS hinzugefügt. In 1. und 2. haben wir gesehen, daß diese Schritte homogene Polynome ergeben. Also bleibt das EZS in jedem Schritt homogen.

Zu 4.

Beim Reduzieren einer Gröbnerbasis werden Elemente aus dem EZS entfernt, oder es werden Elemente vom EZS durch andere Elemente vom EZS dividiert und hinzugefügt, wobei die Gröbnerbasis homogen bleibt.

□

Zurück zum vorherigen Beweis.
ohne Einschränkung gelte $X_1 < X_2 < \ldots < X_n$. Weiterhin gelte $X_i^{j_i} \in LT(G)$ für alle $i \in \{1 \ldots n\}$. Behauptung: $\forall i \in \{1 \ldots n\} : X_i \in \sqrt{I}$
Beweis durch Induktion nach i:

$i = 1$**:**

Sei $g \in G$ mit $LT(g) = X_1^{j_1}$. Alle weiteren Terme von g haben eine kleinere Monomialordnung als $X_1^{j_1}$. Wegen der verwendeten Ordnung kämen nur Monome der Form X_1^k mit $0 \leq k < j_1$ in Frage. Also gilt $g = X_1^{j_1} \in G \subset I \subset \sqrt{I}$.

$i > 1$**:**

Gelte $X_1, \ldots, X_{i-1} \in \sqrt{I}$. Sei $g \in G$ mit $LT(g) = X_i^{j_i}$. Alle weiteren Monome von g haben die Form $X_i^{k_i} \cdot X_{i-1}^{k_{i-1}} \cdot \ldots \cdot X_1^{k_1}$ mit $k_1 + \ldots + k_i = j_i$ und $k_i < j_i$, da g ein homogenes Polynom ist und $X_i^{j_i}$ das größte Monom. Da $k_i < j_i$, gilt $k_t \geq 1$ für ein $t \in \{1 \ldots i-1\}$, also liegt jedes Monom dieser Form in $\sqrt{I}$ nach Induktionsvoraussetzung. Daher läßt sich g darstellen als $g = X_i^{j_i} + r$ mit $r \in \sqrt{I}$. Wegen $I \subset \sqrt{I}$ gilt $g \in \sqrt{I}$, und damit liegt $X_i^{j_i}$ in $\sqrt{I}$. Daraus folgt $X_i \in \sqrt{I}$.

Also gilt: $\langle X_1, \ldots, X_n \rangle \subset \sqrt{I}$. $\sqrt{I} \neq \langle 1 \rangle$, da $f_1, \ldots, f_m$ nicht–konstante Polynome sind. Also: $\langle X_1, \ldots, X_n \rangle = \sqrt{I}$

□

Algorithmus 3 *Sei* $F := \{f_1, \ldots, f_m\} \subset \mathbb{C}[X]$ *Teilmenge*

Frage: *Ist* F *algebraisch abhängig ? Wenn ja, gib ein Polynom* $P \neq 0$ *in* m *Veränderlichen an, so daß* $P(f_1, \ldots, f_m) = 0$ *in* $\mathbb{C}[X]$.

Lösung: *Führe* m *neue Variablen ein, die neuen Variablen sind* $Y = (Y_1 \ldots Y_m)$*, und berechne eine Gröbnerbasis* G *von* $\langle (f_1 - Y_1) \ldots (f_m - Y_m) \rangle$ *bezüglich lex induziert durch* $X_1 > \ldots > X_n > Y_1 > \ldots > Y_m$*. Sei* $G' := G \cap \mathbb{C}[Y]$ *die Menge der Polynome in* G*, die nicht von* $X_1, \ldots, X_n$ *abhängen.* F *ist genau dann algebraisch unabhängig , wenn* $G' = \emptyset$*.*
Insbesondere: $P \in G' \implies P(f_1, \ldots, f_m) = 0$ *in* $\mathbb{C}[X]$.

Der Beweis benötigt folgendes Lemma:

Lemma 3 *Seien* $f_1, \ldots, f_m \in \mathbb{C}[X]$, $I = \langle (f_1 - Y_1) \ldots (f_m - Y_m) \rangle \subset \mathbb{C}[X, Y]$. *Sei* $P \in \mathbb{C}[X, Y]$. *Dann gilt:*

$$P \in I \iff P(X_1, \ldots, X_n, f_1(X_1, \ldots, X_n), \ldots, f_m(X_1, \ldots, X_n)) = 0$$

Um die Lesbarkeit zu verbessern, ersetze ich $f_i(X_1, \ldots, X_n)$ durch f_i.
Folgerung aus Lemma 3: Für $P \in \mathbb{C}[Y]$ gilt $P \in I \iff P(f_1, \ldots, f_m) = 0$
Insbesondere gilt $P \in G' = G \cap \mathbb{C}[Y] \subset I \cap \mathbb{C}[Y] \implies P(f_1, \ldots, f_m) = 0$
Beweis:

„$\implies$":
trivial

„$\impliedby$":
Gelte $P(X_1, \ldots, X_n, f_1, \ldots, f_m) = 0$.
Beweis durch Induktion nach m:

$m = 0$**:**
$I = \langle \emptyset \rangle = 0$
$P(X_1, \ldots, X_n) = 0 \implies P = 0 \implies P \in I$

$m > 0$**:**

Sei die Behauptung für Polynome aus $\mathbb{C}[X, Y_1 \dots Y_{m-1}]$ bewiesen.
Da $\mathbb{C}[X, Y_1 \dots Y_m] \simeq \mathbb{C}[X, Y_1 \dots Y_{m-1}][Y_m]$, hat P folgende Darstellung:

$$P = \sum_{\mu=0}^{N} a_\mu(X_1, \dots, X_n, Y_1 \dots Y_{m-1}) \cdot Y_m^\mu$$

wobei $a_\mu \in \mathbb{C}[X, Y_1 \dots Y_{m-1}]$ für $\mu = 0 \dots N$.

$$Y_m^\mu = ((Y_m - f_m) + f_m)^\mu = \sum_{k=0}^{\mu} \binom{\mu}{k} (Y_m - f_m)^k \cdot f_m^{\mu-k}$$

Also:

$$\begin{aligned} P &= \sum_{\mu=0}^{N} \sum_{k=0}^{\mu} a_\mu(X_1, \dots, X_n, Y_1 \dots Y_{m-1}) \cdot f_m^{\mu-k} \cdot \binom{\mu}{k} (Y_m - f_m)^k \\ &= \sum_{\mu=0}^{N} b_\mu(X_1, \dots, X_n, Y_1 \dots Y_{m-1})(Y_m - f_m)^\mu \end{aligned}$$

Jedes Glied dieser Summe liegt in I, denn

für $\mu = 0$:
$P(X_1, \dots, X_n, f_1, \dots, f_m) = 0$
$\implies b_0(X_1, \dots, X_n, f_1 \dots f_{m-1}) = 0$, denn $(f_i - f_i)^\mu = 0$ für $\mu \geq 1$
$\implies b_0 \in \langle (f_1 - Y_1) \dots (f_{m-1} - Y_{m-1}) \rangle \subset I$
(nach Induktionsvoraussetzung)

für $\mu > 0$:
$(f_m - Y_m)^\mu \in I$, da $(f_m - Y_m) \in I$

Also gilt: $P \in I$.

□

Zurück zum vorherigen Beweis.
Daher reicht es zu zeigen: $I \cap \mathbb{C}[Y] = \{0\} \iff G \cap \mathbb{C}[Y] = \emptyset$

„$\implies$":
trivial, denn $G \subset I$ und $0 \notin G$

„$\impliedby$":

$$\begin{aligned} G \cap \mathbb{C}[Y] = \emptyset \quad &\implies \quad \text{Jedes } g \in G \text{ hängt von } X_1, \dots, X_n \text{ ab.} \\ &\implies \quad \text{ein Monom, welches für ein } i \in \{1 \dots n\} \text{ eine Potenz} \\ &\qquad\quad \text{von } X_i \text{ enthält, ist kleinster Term in } LT(G). \\ &\implies \quad \text{Jedes } m \in LT(I) \text{ enthält einen Term aus } \{X_1, \dots, X_n\}. \\ &\implies \quad I \cap \mathbb{C}[Y] = \{0\} \end{aligned}$$

F algebraisch abhängig $\Longleftrightarrow I \cap \mathbb{C}[Y] \neq \{0\} \Longleftrightarrow G \cap \mathbb{C}[Y] \neq \emptyset$
Die erste Äquivalenz folgt aus Lemma 3 und die zweite Äquivalenz haben wir soeben bewiesen.

□

Literatur

David Cox, John Little, Donal O'Shea : ,,Ideals, Varieties and Algorithms"
Springer, New York etc., 1992

Bernd Sturmfels : ,,Algorithms in Invariant Theory"
Springer, Wien, 1993