Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§2.7 Eliminationsideale und deren Anwendungen

In diesem Abschnitt sei stets $C|K$ eine Körpererweiterung und C algebraisch abgeschlossen.

Definition 2.7.1. Sei $I \subseteq K[\underline{X}]$ ein Ideal und $r \in \{0,\dots,n\}$. Dann heißt das Ideal $I_r := I \cap K[X_{r+1},\dots,X_n]$ von $K[X_{r+1},\dots,X_n]$ das *r-te Eliminationsideal* von I.

Satz 2.7.2 (geometrische Bedeutung der Eliminationsideale)**.** *Sei $I \subseteq K[\underline{X}]$ ein Ideal, $r \in \{0,\dots,n\}$ und $\pi\colon \mathbb{A}^n \to \mathbb{A}^{n-r}$, $(x_1,\dots,x_n) \mapsto (x_{r+1},\dots,x_n)$. Dann gilt*

$$V(I_r) = \overline{\pi(V(I))}$$

(bezüglich der K-Zariskitopologie auf $\mathbb{A}^{n-r}$ [→1.4.2]), das heißt $V(I_r)$ ist die kleinste K-Untervarietät von $\mathbb{A}^{n-r}$, die $\pi(V(I))$ umfasst.

Beweis. „$\supseteq$“ folgt aus der offensichtlichen Tatsache $\pi(V(I)) \subseteq V(I_r)$ zusammen mit der Abgeschlossenheit von $V(I_r)$.

„$\subseteq$“ Sei $x \in V(I_r)$. Nach 1.4.7 gilt $\overline{\pi(V(I))} = V(I(\pi(V(I)))$, weswegen es reicht zu zeigen, dass für jedes $f \in I(\pi(V(I))$ gilt $f(x) = 0$. Sei also $f \in I(\pi(V(I))$. Fasst man f als Polynom in $K[\underline{X}]$ auf, so gilt offenbar $f \in I(V(I))$. Nach dem Hilbertschen Nullstellensatz 1.3.9 gilt aber $I(V(I)) = \sqrt{I}$, also $f^k \in I$ für ein $k \in \mathbb{N}$. Da f in $K[X_{r+1},\dots,X_n]$ liegt, gilt dies natürlich auch für f^k. Also $f^k \in I_r$. Somit $f^k(x) = 0$ und daher $f(x) = 0$. □

Satz 2.7.3. *Sei $I \subseteq K[\underline{X}]$ ein Ideal und G eine Gröbnerbasis von I bezüglich der lexikographischen Ordnung $\leq_{lex}$ auf $[\underline{X}]$ [→2.1.5(a)]. Für $r \in \{0,\dots,n\}$ ist $G_r := G \cap K[X_{r+1},\dots,X_n]$ eine Gröbnerbasis des r-ten Eliminationsideals I_r bezüglich $\leq_{lex}$.*

Beweis. Wir wenden die Charakterisierung von Gröbnerbasen eines Ideals aus 2.4.7(f) an. Sei also $r \in \{0,\dots,n\}$ und $p \in I_r$. Zu zeigen ist die Existenz eines $g \in G_r \setminus \{0\}$ mit $\mathrm{LM}(g)|\,\mathrm{LM}(p)$. Da $p \in I$ und G eine Gröbnerbasis von I ist, gibt es $g \in G \setminus \{0\}$ mit $\mathrm{LM}(g)|\,\mathrm{LM}(p)$. Wegen $p \in K[X_{r+1},\dots,X_n]$ gilt $\mathrm{LM}(p) \in [X_{r+1},\dots,X_n]$ und daher auch $\mathrm{LM}(g) \in [X_{r+1},\dots,X_n]$. Nach Definition von $\leq_{\mathrm{lex}}$ folgt daraus $g \in K[X_{r+1},\dots,X_n]$, also $g \in G_j$. □

Bemerkung 2.7.4. Offensichtlich bleibt Satz 2.7.3 richtig, wenn man statt $\leq_{\mathrm{lex}}$ eine beliebige Monomordnung $\leq$ auf $[\underline{X}]$ benutzt mit $u < X_i$ für alle $u \in [X_{r+1},\dots,X_n]$ und $i \in \{1,\dots,r\}$.

Satz 2.7.5. *Seien $f_1, \dots, f_m, g_1, \dots, g_s \in K[X_1, \dots, X_n]$. Betrachte den K-Algebrenhomomorphismus*

$$\varphi\colon K[Y_1, \dots, Y_m] \to K[X_1, \dots, X_n]/(g_1, \dots, g_s),\ p \mapsto \overline{p(f_1, \dots, f_m)}.$$

(a) *Der Kern von φ ist das Eliminationsideal $J := I \cap K[\underline{Y}]$ von*

$$I := (f_1 - Y_1, \dots, f_m - Y_m, g_1, \dots, g_s) \subseteq K[\underline{X}, \underline{Y}].$$

(b) *Sei G eine Gröbnerbasis von I bezüglich der lexikographischen Ordnung auf $[\underline{X}, \underline{Y}]$. Dann ist $G \cap K[\underline{Y}]$ eine Gröbnerbasis von J bezüglich der lexikographischen Ordnung auf $[\underline{Y}]$. Sei $q \in K[\underline{X}]$ und $p \in K[\underline{X}, \underline{Y}]$ reduziert modulo G bezüglich $\leq_{lex}$ mit $q \xrightarrow[G]{*} p$. Gilt dann $p \in K[\underline{Y}]$, so $\varphi(p) = \overline{q}$, und andernfalls $\varphi^{-1}(\overline{q}) = \emptyset$.*

(c) *Der K-Morphismus $\varphi^*\colon V(g_1, \dots, g_s) \to \mathbb{A}^m$ [→1.5.11] ist gegeben durch $\varphi^*(x) = (f_1(x), \dots, f_m(x))$ für $x \in V(g_1, \dots, g_s)$ und der K-Zariskiabschluss seines Bildes ist $V(J)$.*

Beweis. Man zeigt leicht

$$(*) \qquad I \cap K[\underline{X}] = (g_1, \dots, g_s),$$

denn „$\supseteq$“ ist trivial und für „$\subseteq$“ muss man nur den K-Algebrenhomomorphismus $K[\underline{X}, \underline{Y}] \to K[\underline{X}],\ X_i \mapsto X_i,\ Y_j \mapsto f_j$ anwenden.

(a) Ist $p \in J$, so $p(f_1, \dots, f_m) \equiv_I p(Y_1, \dots, Y_m) = p \equiv_I 0$ und daher $p(f_1, \dots, f_m) \in I \cap K[\underline{X}] \overset{(*)}{=} (g_1, \dots, g_s)$, das heißt $\varphi(p) = 0$. Dies zeigt $J \subseteq \ker \varphi$. Ist umgekehrt $p \in \ker \varphi$, so $p = p(Y_1, \dots, Y_m) \equiv_I p(f_1, \dots, f_m) \equiv_I 0$ und daher $p \in I \cap K[\underline{Y}] = J$. Dies zeigt $\ker \varphi \subseteq J$.

(b) Der erste Teil der Aussage folgt aus Satz 2.7.3. Sei nun $q \in K[\underline{X}]$ und sei $p \in K[\underline{X}, \underline{Y}]$ reduziert modulo G bezüglich $\leq_{\text{lex}}$ mit $q \xrightarrow[G]{*} p$. Gilt dann $p \in K[\underline{Y}]$, so $p(f_1, \dots, f_m) \equiv_I p(Y_1, \dots, Y_m) = p \overset{G \subseteq I}{\equiv}_I q$ und daher

$$p(f_1, \dots, f_m) - q \in I \cap K[\underline{X}] \overset{(*)}{=} (g_1, \dots, g_s),$$

das heißt $\varphi(p) = \overline{q}$. Gelte schließlich $\varphi^{-1}(\overline{q}) \neq \emptyset$. Zu zeigen ist dann $p \in K[\underline{Y}]$. Wähle $p_0 \in K[\underline{Y}]$ mit $\varphi(p_0) = \overline{q}$. Dann $p_0 = p_0(Y_1, \dots, Y_m) \equiv_I p_0(f_1, \dots, f_m) \equiv_I q$ und da $\xrightarrow[G]{}$ nach 2.4.2 eindeutig reduziert, muss $p_0 \xrightarrow[G]{*} p$ gelten. Nach Wahl der Monomordnung $\leq_{\text{lex}}$ kann während dieser Reduktion zu keinem Zeitpunkt ein X_i eingeschleppt werden, das heißt $p_0 \xrightarrow[G \cap K[\underline{Y}]]{*} p$ und insbesondere $p \in K[\underline{Y}]$.

(c) Für alle $x \in V(g_1, \ldots, g_s)$ gilt $\mathrm{ev}_{\varphi^*(x)} = \mathrm{ev}_x \circ \varphi$ und daher

$$\begin{aligned}\varphi^*(x) &= (\mathrm{ev}_{\varphi^*(x)}(Y_1), \ldots, \mathrm{ev}_{\varphi^*(x)}(Y_m)) \\ &= (\mathrm{ev}_x(\varphi(Y_1)), \ldots, \mathrm{ev}_x(\varphi(Y_m))) \\ &= (\mathrm{ev}_x(\overline{f_1}), \ldots, \mathrm{ev}_x(\overline{f_m})) \\ &= (f_1(x), \ldots, f_m(x))\end{aligned}$$

für $x \in V(g_1, \ldots, g_s)$. Sei $h \in K[\underline{Y}]$. Dann

$$\begin{aligned}h \in I(\varphi^*(V(g_1, \ldots, g_s))) &\iff \forall x \in V(g_1, \ldots, g_s) : h(\varphi^*(x)) = 0 \\ &\iff \forall x \in V(g_1, \ldots, g_s) : h(f_1(x), \ldots, f_m(x)) = 0 \\ &\iff h(f_1, \ldots, f_m) \in I(V(g_1, \ldots, g_s)) \\ &\overset{1.3.9}{\iff} h(f_1, \ldots, f_m) \in \sqrt{(g_1, \ldots, g_s)} \\ &\iff \exists k \in \mathbb{N} : (h(f_1, \ldots, f_m))^k \in (g_1, \ldots, g_s) \\ &\iff \exists k \in \mathbb{N} : h^k(f_1, \ldots, f_m) \in (g_1, \ldots, g_s) \\ &\iff \exists k \in \mathbb{N} : \varphi(h^k) = 0 \\ &\iff \exists k \in \mathbb{N} : h^k \in \ker \varphi \\ &\iff \exists k \in \mathbb{N} : h^k \in J \\ &\iff h \in \sqrt{J}.\end{aligned}$$

Es folgt $\sqrt{J} = I(\varphi^*(V(g_1, \ldots, g_s)))$ und daher

$$V(J) \overset{1.2.3}{=} V(\sqrt{J}) = V(I(\varphi^*(V(g_1, \ldots, g_s)))) \overset{1.4.7}{=} \overline{\varphi^*(V(g_1, \ldots, g_s))}.$$

□

Bemerkung 2.7.6. Man überlegt sich leicht, dass Satz 2.7.5 im Wesentlichen folgende Probleme löst:

(a) Berechnung des Kerns eines Homomorphismus zwischen zwei affinen K-Algebren.

(b) Entscheidung, ob ein Element im Bild eines Homomorphismus zwischen zwei affinen K-Algebren liegt, und gegebenenfalls Berechnung eines Urbilds.

(c) Beschreibung des K-Zariskiabschlusses des Bildes eines K-Morphismus von affinen Varietäten.

Beachte nämlich, dass man in (a) und in (b) Œ davon ausgehen kann, dass der K-Algebrenhomomorphismus auf einer Polynomalgebra definiert ist [→1.1.22(c)] und dass jeder K-Algebrenhomomorphismus $K[\underline{Y}] \to K[\underline{X}]/(g_1, \ldots, g_s)$ von der in 2.7.5 gegebenen Form ist (wähle $f_i \in K[\underline{X}]$ mit $\varphi(Y_i) = \overline{f_i}$).

Satz 2.7.7 (Implizitierung rationaler Parametrisierungen). *Seien $f_1, \ldots, f_m, g_1, \ldots, g_m \in K[\underline{X}]$, $g := g_1 \cdots g_m$, sei $L|K$ eine Körpererweiterung und L ein unendlicher Körper, der ein Unterkörper von C ist (zum Beispiel C der algebraische Abschluss von L). Betrachte die Abbildung*

$$\begin{aligned} \varphi\colon L^n \setminus V(g) &\to L^m \\ x &\mapsto \left(\frac{f_1(x)}{g_1(x)}, \ldots, \frac{f_m(x)}{g_m(x)}\right) \end{aligned}$$

und das Eliminationsideal $J := I \cap K[Y_1, \ldots, Y_m]$ des Ideals

$$I := (g_1 Y_1 - f_1, \ldots, g_m Y_m - f_m, gT - 1) \subseteq K[T, \underline{X}, \underline{Y}].$$

Dann ist $V(J) \cap L^m$ der K-Zariskiabschluss des Bildes von φ in L^m (die K-Zariskitopologie auf L^m wurde in 1.4.5 definiert).

Beweis. Betrachte die Projektion

$$\pi\colon C^{1+n+m} \to C^m,\ (t, x, y) \mapsto y \qquad (t \in C, x \in C^n, y \in C^m).$$

Dann gilt offensichtlich $\pi(V(I) \cap L^{1+n+m}) = \varphi(L^n \setminus V(g))$. Satz 2.7.2 besagt $V(J) = \overline{\pi(V(I))}$. Falls $L = C$, so sind wir also bereits fertig. Den allgemeinen Fall führen wir mittels

$$\begin{aligned} \tilde{\varphi}\colon C^n \setminus V(g) &\to C^m \\ x &\mapsto \left(\frac{f_1(x)}{g_1(x)}, \ldots, \frac{f_m(x)}{g_m(x)}\right) \end{aligned}$$

darauf zurück, indem wir zeigen, dass $\tilde{\varphi}(C^n \setminus V(g))$ im K-Zariskiabschluss von $\varphi(L^n \setminus V(g))$ in $\mathbb{A}^n = C^n$ enthalten ist. Dann stimmen nämlich die K-Zariskiabschlüsse von $\tilde{\varphi}(C^n \setminus V(g))$ und $\varphi(L^n \setminus V(g))$ in $\mathbb{A}^n$ überein, und deren Schnitt mit L^m ist einerseits nach dem schon bewiesenen Fall $L = C$ gleich $V(J) \cap L^m$ und andererseits gleich dem K-Zariskiabschluss von $\varphi(L^n \setminus V(g))$ in L^m. Sei also $h \in K[\underline{X}]$ mit $h \in I(\varphi(L^n \setminus V(g)))$. Zu zeigen ist $h \in I(\tilde{\varphi}(C^n \setminus V(g)))$. Ist $g = 0$, so $V(g) = C^n$ und es ist nichts zu zeigen. Also Œ $g \neq 0$. Die rationale Funktion $r := h\left(\frac{f_1}{g_1}, \ldots, \frac{f_m}{g_m}\right) \in K(\underline{X})$ verschwindet auf $L^n \setminus V(g)$. Wähle $k \in \mathbb{N}$ mit $g^k r \in K[\underline{X}]$. Dann verschwindet auch $g^k r$ auf $L^n \setminus V(g)$ und $g^{k+1} r$ sogar auf L^n. Wegen $\#L = \infty$ folgt mit 1.2.10 $g^{k+1} r = 0$. Somit $r = 0$ und daher $h \in I(\tilde{\varphi}(C^n \setminus V(g)))$. □

Satz 2.7.8 (Berechnung des Schnitts von Idealen und von Kongruenzklassen). *Seien $m \in \mathbb{N}$ und $I_1, \ldots, I_m$ Ideale von $K[\underline{X}]$. Für das Eliminationsideal $J \cap K[\underline{X}]$ des Ideals*

$$J := (\{T_1 + \ldots + T_m - 1\} \cup \{T_i g \mid i \in \{1, \ldots, m\}, g \in I_i\}) \subseteq K[\underline{T}, \underline{X}]$$

gilt dann

$$J \cap K[\underline{X}] = I_1 \cap \ldots \cap I_m.$$

Seien weiter $f_1, \ldots, f_m \in K[\underline{X}]$ gegeben und

$$L := (f_1 + I_1) \cap \ldots \cap (f_m + I_m) = \{f \in K[\underline{X}] \mid f \equiv_{I_1} f_1, \ldots, f \equiv_{I_m} f_m\}.$$

Dann gilt

$$L = f + (I_1 \cap \ldots \cap I_m) = f + (J \cap K[\underline{X}])$$

für alle $f \in L$. Sei nun ferner G eine Gröbnerbasis von J bezüglich der lexikographischen Ordnung $\leq_{lex}$ auf $[\underline{T}, \underline{X}]$ und $h \in K[\underline{T}, \underline{X}]$ reduziert modulo G mit $T_1 f_1 + \ldots + T_m f_m \xrightarrow[G]{*} h$. Dann

$$L \neq \emptyset \iff h \in K[\underline{X}] \iff h \in L.$$

Beweis. Wir zeigen zunächst $J \cap K[\underline{X}] = I_1 \cap \ldots \cap I_m$.

„$\supseteq$“ Sei $g \in I_1 \cap \ldots \cap I_m$. Dann $g = 1 \cdot g \equiv_J (T_1 + \ldots + T_m)g = T_1 g + \ldots + T_m g \equiv_J 0$, also $g \in J$.

„$\subseteq$“ Sei $g \in J \cap K[\underline{X}]$ und $i \in \{1, \ldots, m\}$. Zu zeigen: $g \in I_i$. Es gibt $h \in K[\underline{X}]$ und $h_1 \in I_1, \ldots, h_m \in I_m$ mit $g = h(T_1 + \ldots + T_m - 1) + \sum_{j=1}^{m} T_j h_j$. Wende den K-Algebrenhomomorphismus $\varphi\colon K[\underline{T}, \underline{X}] \to K[\underline{X}]$ mit $\varphi(X_j) = X_j$ für $j \in \{1, \ldots, n\}$ und $\varphi(T_j) = \delta_{ij}$ für $j \in \{1, \ldots, m\}$ an. Dann

$$g = \varphi(g) = \varphi(h) \underbrace{\varphi(T_1 + \ldots + T_m - 1)}_{=0} + h_i = h_i \in I_i.$$

Seien nun weiter $f_1, \ldots, f_m \in K[\underline{X}]$ und $L := (f_1 + I_1) \cap \ldots \cap (f_m + I_m)$. Man sieht sofort, dass $L = f + (I_1 \cap \ldots \cap I_m)$ ist für alle $f \in L$. Sei schließlich G eine Gröbnerbasis von J bezüglich der lexikographischen Ordnung $\leq_{\text{lex}}$ auf $[\underline{T}, \underline{X}]$ und $h \in K[\underline{T}, \underline{X}]$ reduziert modulo G mit $T_1 f_1 + \ldots + T_m f_m \xrightarrow[G]{*} h$. Es reicht zu zeigen:

(a) $L \neq \emptyset \implies h \in K[\underline{X}]$

(b) $h \in K[\underline{X}] \implies h \in L$

Zu (a). Gelte $L \neq \emptyset$. Wähle $p \in L$. Dann

$$p - (T_1 f_1 + \ldots + T_m f_m) = \sum_{i=1}^{m} T_i (p - f_i) + (1 - \sum_{i=1}^{m} T_i) p \in J.$$

Da somit $p \equiv_J T_1 f_1 + \ldots + T_m f_m$ und $\xrightarrow[G]{}$ eindeutig reduziert, folgt $p \xrightarrow[G]{*} h$. Nach Wahl der Monomordnung $\leq_{\text{lex}}$ gilt mit $p \in K[\underline{X}]$ dann aber auch $h \in K[\underline{X}]$.

Zu (b). Gelte $h \in K[\underline{X}]$. Zu zeigen: $h \in L$. Sei $i \in \{1, \ldots, m\}$. Zu zeigen: $h \equiv_{I_i} f_i$. Aus $h - (T_1 f_1 + \ldots + T_m f_m) \in J$ folgt wie oben durch Einsetzen von 1 für T_i und 0 für T_j für $j \neq i$, dass $h - f_i \in I_i$. □