GRÖBNERBASEN UND REGULARITÄT

Vortrag 2: Gröbner Basen und das Eliminationsideal

Sophia Feil

26. Oktober 2016

Inhaltsverzeichnis

0 Einführung

In diesem Vortrag wollen wir uns mit sogenannten Eliminationsidealen und deren Anwendungen beschäftigen. Diese Arbeit orientiert sich sowohl inhaltlich als auch strukturell an G.Kempers Buch A Course in Commutative Algebra [Kem10].

Für diesen Vortrag wird grundlegendes Wissen der Algebraischen Geometrie benötigt, welches im ersten Kapitel von A Course in Commutative Algebra [Kem10] behandelt wird.

Hier jedoch einige für diesen Vortrag ausschlaggebende Aspekte:

Mit $K[x_1, \ldots, x_n]$ bezeichen wir den Polynomring in n-Variablen über einem Körper K und mit $I \subset K[x_1, \ldots, x_n]$ ein Ideal in diesem Polynomring. Das Ideal

$$\sqrt{I} := \{f \in K[x_1, \ldots, x_n] | \text{ es existiert } k \in \mathbb{N} : f^k \in I\}$$

wird das Radikalideal von I genannte.

Sei $N \subset K^n$ eine Teilmenge, so notieren wir mit

$$\mathcal{I}(N) := \{f \in K[x_1, \ldots, x_n] | f(x) = 0 \text{ für alle } x \in N\}$$

das Verschwindungsideal von N. Weiter definieren wir für eine Teilmenge $M \subset K[x_1, \ldots, x_n]$ die Menge

$$\mathcal{V}(M) := \{x \in K | f(x) = 0 \text{ für alle } f \in M\}.$$

Man nennt $X \subset K^n$ eine affine Varietät, falls es ein Ideal $I \subset K[x_1, \ldots, x_n]$ gibt, sodass $X = \mathcal{V}(I)$.

Für eine affine Varietät $X \subset K^n$ bezeichnen wir mit $K[X] := {}^{K[x_1, \ldots, x_n]}\!/_{\mathcal{I}(X)}$ den sogenannten Koordinatenring von X.

Ein Morphismus von affinen Varietäten $X \in K^m$ und $Y \in K^n$, ist eine Abbildung $f : X \longrightarrow Y$, für die gilt $f(P) = (f_1(P), \ldots, f_n(P))$, für $f_1, \ldots, f_n \in K[x_1, \ldots, x_m]$. Die Menge aller Morphismen zwischen X und Y wird mit $\mathrm{Mor}(X, Y)$ bezeichnet.

1 Berechnung von Eliminationsidealen mithilfe Gröbnerbasen

Definition 1.1. *Sei $S := \{x_{i_1}, \ldots, x_{i_k}\} \subset \{x_1, \ldots, x_n\}$ eine Menge von Unbekannten.*

1. *Für ein Ideal $I \subset K[x_1, \ldots, x_n]$, nennen wir das Ideal*

$$I_S := K[x_{i_1}, \ldots, x_{i_k}] \cap I$$

*das S-**Eliminationsideal** von I.*

2. *Eine Monomordnung (vgl. Vortrag 1) $\leq$ auf $K[x_1, \ldots, x_n]$ wird S-**Eliminationsordnung** genannt, falls für $\overline{S} := \{x_1, \ldots, x_n\} \setminus S$ gilt*

$$t < x_j \text{ für alle } x_j \in \overline{S} \text{ und für alle Monome } t \in K[x_{i_1}, \ldots, x_{i_k}]\,.$$

Wir wollen nun einige Beispiele für Eliminationsordnungen betrachten. Hierzu verwenden wir Beispiele von Monomordnungen aus Vortrag 1.

Beispiel 1.2.

1. Sei $K[x_1, \ldots, x_n]$ ein Polynomring, $\leq_1$ eine Monomordnung auf $K[x_1, \ldots, x_k]$ und $\leq_2$ eine Monomordnung auf $K[x_{k+1}, \ldots, x_n]$. Wir betrachten die durch $\leq_2$ dominierte Block-Ordnung. Diese Monomordnung ist eine $\{x_1, \ldots, x_k\}$-Eliminationsordnung, denn sei $t = x_1^{e_1} \cdots x_n^{e_n} \in K[x_1, \ldots, x_k]$ ein Monom und $x_i \in \{x_{k+1}, \ldots, x_n\}$ so gilt $x_{k+1}^{e_{k+1}} \cdots x_n^{e_n} = 1 \leq_2 x_i$. Insbesondere ist dies eine echte Ungleichung, da $x_i \neq 1$. Daher erhalten wir nach Definition der Block-Ordnung $t < x_i$ und somit die Behauptung.

2. Lexikographische Ordnung ist eine $\{x_k, \ldots, x_n\}$-Eliminationsordnung für jedes $k = 1, \ldots, n$.

3. Jede Monomordnung ist eine Eliminationsordnung für $S = \{x_1, \ldots, x_n\}$ und $S = \varnothing$.

Im nächsten Theorem wollen wir verstehen, wie Eliminationsideale und Gröbnerbasen zusammenhängen.

Theorem 1.3. *(Berechnung von Eliminationsidealen)*
Sei $I \subset K[x_1, \ldots, x_n]$ ein Ideal und $S := \{x_{i_1}, \ldots, x_{i_k}\} \subset \{x_1, \ldots, x_n\}$. Sei $\leq$ eine S-Eliminationsordnung und G eine Gröbnerbasis von I bzgl. dieser Ordnung. So ist

$$G_S := K[x_{i_1}, \ldots, x_{i_k}] \cap G$$

eine Gröbnerbasis von I_S bzgl. der eingeschränkten Monomordnung $\leq$ auf $K[x_{i_1}, \ldots, x_{i_k}]$.

Beweis. Offensichtlich gilt $G_S = K[x_{i_1}, \ldots, x_{i_k}] \cap G \subset K[x_{i_1}, \ldots, x_{i_k}] \cap I = I_S$.
Wir wollen beweisen, dass $\mathcal{L}(I_S) = \mathcal{L}(G_S)$.
Dazu zeigen wir, dass für alle $0 \neq f \in I_S$ ein $h \in G_S$ existiert, sodass $\mathcal{LM}(h)$ ein Teiler von $\mathcal{LM}(f)$ ist.

Sei also $0 \neq f \in I_S \subset I$. Dann existiert nach Definition einer Gröbnerbasis ein $g \in G$, sodass $\mathcal{LM}(g)$ das Monom $\mathcal{LM}(f)$ teilt.

Also genügt es zu zeigen, dass g bereits in $K[x_{i_1}, \ldots, x_{i_k}]$ liegt. Insbesondere ist es ausreichend zu zeigen, dass $\mathrm{Mon}(g)$ eine Teilmenge von $K[x_{i_1}, \ldots, x_{i_k}]$ ist.

Sei $x_1^{e_1} \cdots x_n^{e_n} =: t \in \mathrm{Mon}(g)$. Aus der Definition des Leitmonoms folgt, dass $t \leq \mathcal{LM}(g)$. Angenommen $t \notin K[x_{i_1}, \ldots, x_{i_k}]$, so würde folgen, dass ein $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$ existiert mit $0 < e_j$ und somit wäre $\mathcal{LM}(g) \leq \mathcal{LM}(f) < x_j \leq t$, wobei die mittlere Ungleichung folgt, da $\leq$ eine S-Eliminationsordnung ist. Dies ist ein Widerspruch zur Annahme und folglich erhalten wir $g \in K[x_{i_1}, \ldots, x_{i_k}]$. □

Zusammenfassend besagt das Theorem also, dass wir für ein Ideals $I \subset K[x_1, \ldots, x_n]$, nur eine Gröbnerbasis von I bzgl. einer Eliminationsordnung bestimmen müssen, um eine Gröbnerbasis und somit Erzeuger von I_S zu erhalten.

Beispiel 1.4. [vgl.Kap.2 §5 CLO15, S.77] Sei $I := \langle x_1 + x_3, x_2 - x_3 \rangle \subset \mathbb{R}[x_1, x_2, x_3]$ ein Ideal. Bzgl. der lexikographischen Ordnung ist $G := \{x_1 + x_3, x_2 - x_3\}$ eine Gröbnerbasis von I. Um diese Aussage einzusehen, müssen wir zeigen, dass für alle $0 \neq f \in I$ gilt, dass $\mathcal{LM}(x_1 + x_3) = x_1$, oder $\mathcal{LM}(x_2 - x_3) = x_2$ das Leitmonom von f teilt. Sei also $0 \neq f \in I$ von der Form $f = h(x_1 + x_3) + p(x_2 - x_3)$.

Angenommen die Behauptung gilt nicht, so ist $f \in \mathbb{R}[x_3]$, denn $\mathcal{LM}(f) \in \mathbb{R}[x_3]$ und somit muss bereits $\mathrm{Mon}(f) \subset \mathbb{R}[x_3]$ gelten. Außerdem muss für $f = h(x_1 + x_3) + p(x_2 - x_3)$ gelten, dass $f(-r, r, r) = 0$ für alle $r \in \mathbb{R}$ und daraus würde folgen, dass $f = 0$ sein muss. Dies ist ein Wiederspruch zur Annahme.

Da die lexikographische Ordnung eine $\{x_2, x_3\}$-Eliminationsordnung ist, erhalten wir nach Theorem 1.3 beispielsweise $I_{\{x_2,x_3\}} = \left\langle G_{\{x_2,x_3\}} \right\rangle = \langle x_2 - x_3 \rangle$ als das $\{x_2, x_3\}$-Eliminationsideal von I.

Bemerkung 1.5. Für ein Ideal $I \subset K[x_1, \ldots, x_n]$ ist es möglich mithilfe von Gröbnerbasen und Eliminationsidealen, die Dimension des Ringes $K[x_1, \ldots, x_n]/I$ zu berechnen. Allerdings ist diese Methode im Allgemeinen eher unpraktisch, weshalb wir an dieser Stelle auf den fünften Vortrag verweisen in dem eine gute Methode behandelt wird, die Dimension von affinen Algebren zu berechnen.

2 Kerne von K-Algebren Homomorphismen

Lemma 2.1. *Seien* $A := K[y_1, \ldots, y_m]/I$ *und* $B := K[x_1, \ldots, x_n]/J$ *zwei* K*-Algebren und*

$$\phi : B \longrightarrow A \quad \textit{und} \quad \pi : K[x_1, \ldots, x_n] \longrightarrow B$$

K-Algebren Homomorphismen, wobei π *die kanonische Projektion ist. Definiere*

$$\psi := \phi \circ \pi : K[x_1, \ldots, x_n] \longrightarrow A\,.$$

So gilt $\ker(\phi) = \ker(\psi)/J$.

Beweis. Sei $x + J =: \overline{x} \in \ker(\phi)$ und sei $x \in K[x_1, \ldots, x_n]$ ein beliebiger Repräsentant von $\overline{x}$, so gilt $\psi(x) = \phi \circ \pi(x) = \phi(\overline{x}) = 0$, also ist $x \in \ker(\psi)$ und somit $\overline{x} \in {}^{\ker(\psi)}\!/_{J}$.

Sei umgekehrt $y + J =: \overline{y} \in {}^{\ker(\psi)}\!/_{J}$, so ist $y \in \ker(\psi)$. Folglich ist $0 = \psi(y) = \phi \circ \pi(y) = \phi(\overline{y})$.

□

Also folgt aus dem Lemma, dass wir um den Kern eines Homomorphismus $\phi : B \longrightarrow A$ wie im Lemma zu berechnen, ohne Einschränkung annehmen können, dass B ein Polynomring $K[x_1, \ldots, x_n]$ ist.

Die folgende Proposition stellt einen Zusammenhang zwischen Kernen von K-Algebren Homomorphismen und Eliminationsidealen her.

Proposition 2.2. *Sei $\phi : K[x_1, \ldots, x_n] \longrightarrow A := {}^{K[y_1, \ldots, y_m]}\!/_{I}$ ein K-Algebren Homomorphismus und $\phi(x_i) = g_i + I =: \overline{g_i}$ mit $g_i \in K[y_1, \ldots, y_m]$ für alle i.*

Definieren wir

$$J := \langle I \cup \{g_1 - x_1, \ldots, g_n - x_n\} \rangle_{K[x_1, \ldots, x_n, y_1, \ldots, y_m]} ,$$

so gilt

$$\ker(\phi) = K[x_1, \ldots, x_n] \cap J .$$

Beweis. Bevor wir die Proposition beweisen, wollen wir zwei Zwischenbehauptungen beweisen.

Zwischenbehauptung 1:
Aus $f \in K[x_1, \ldots, x_n]$ folgt $f(g_1, \ldots, g_n) - f \in J$, wobei $f(g_1, \ldots, g_n) \in K[y_1, \ldots, y_m]$ das Polynom f ausgewertet an der Stelle $(g_1, \ldots, g_n)$ ist.

Beweis. Es gilt

$$\begin{aligned} &f(g_1, \ldots, g_n) - f(x_1, \ldots, x_n) = \\ &f(g_1, \ldots, g_n) - f(x_1, g_2, \ldots, g_n) + f(x_1, g_2, \ldots, g_n) - f(x_1, x_2, g_3, \ldots, g_n) + \\ &f(x_1, x_2, g_3, \ldots, g_n) - \cdots + f(x_1, \ldots, x_{n-1}, g_n) - f(x_1, \ldots, x_n) \in J , \end{aligned}$$

da $f(x_1, \ldots, x_{i-1}, g_i, \ldots, g_n) - f(x_1, \ldots, x_i, g_{i+1}, \ldots, g_n) \in J$ für alle i.

Zwischenbehauptung 2:
Ein Polynom $f \in K[x_1, \ldots, x_n]$ ist genau dann im Kern von ϕ, wenn $f(g_1, \ldots, g_n) \in I$.

Beweis. Sei $f = \sum_{j_1, \ldots, j_n} a_{j_1, \ldots, j_n} x_1^{j_1} \cdots x_n^{j_n}$, wobei $a_{j_1, \ldots, j_n} \in K$ und $j_i \in \mathbb{N}$. Dann gilt

$$\begin{aligned} \phi(f) = 0 &\Leftrightarrow \phi(f) \in I \\ &\Leftrightarrow \sum_{j_1, \ldots, j_n} a_{j_1, \ldots, j_n} \phi(x_1)^{j_1} \cdots \phi(x_n)^{j_n} \in I \\ &\Leftrightarrow \sum_{j_1, \ldots, j_n} a_{j_1, \ldots, j_n} (g_1 + I)^{j_1} \cdots (g_n + I)^{j_n} \in I \\ &\Leftrightarrow \sum_{j_1, \ldots, j_n} a_{j_1, \ldots, j_n} g_1^{j_1} \cdots g_n^{j_n} + I \in I \\ &\Leftrightarrow f(g_1, \ldots, g_n) \in I \end{aligned}$$

Nun zum Beweis der Proposition:
Sei $f \in \ker(\phi) \subset K[x_1, \ldots, x_n]$, so folgt mit Zwischenbeh. 2, dass $f(g_1, \ldots, g_n) \in I \subset J$. Mit Zwischenbeh. 1 erhalten wir dann

$$f = f(g_1, \ldots, g_n) - (f(g_1, \ldots, g_n) - f) \in J\,.$$

Also folgt insgesamt $f \in K[x_1, \ldots, x_n] \cap J$.

Sei umgekehrt $f \in K[x_1, \ldots, x_n] \cap J$. Analog zur Argumentation oben, folgt $f(g_1, \ldots, g_n) \in J$, somit wird $f(g_1, \ldots, g_n)$ von Elementen aus $I \cup \{g_1 - x_1, \ldots, g_n - x_n\}$ erzeugt. Also ist

$$f(g_1, \ldots, g_n) = \sum_{i=1}^{r} h_i f_i + \sum_{j=1}^{n} p_j (g_j - x_j)\,,$$

wobei $h_i, p_j \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ und $f_i \in I$. Da $f(g_1, \ldots, g_n)$ in $K[y_1, \ldots, y_m]$ liegt und somit unabhängig von den x_j ist, folgt, dass alle p_j trivial sein müssen. Wir erhalten daher $f(g_1, \ldots, g_n) = \sum_{i=1}^{r} h_i f_i \in I$ und nach Zwischenbeh. 2 gilt $f \in \ker(\phi)$. □

Bemerkung 2.3. Aus Theorem 1.3 und Proposition 2.2 erhalten wir folgende Erkenntnis:

Sei $J \subset K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ wie in Proposition 2.2, $\leq$ eine $\{x_1, \ldots, x_n\}$-Eliminationsordnung und G eine Gröbnerbasis von J bzgl. $\leq$. So ist $G_x := K[x_1, \ldots, x_n] \cap G$ eine Gröbnerbasis von $J_x := K[x_1, \ldots, x_n] \cap J$ bzgl. der Einschränkung von $\leq$ auf $K[x_1, \ldots, x_n]$ nach Theorem 1.3. Des Weiteren erhalten wir mit Proposition 2.2, dass G_x eine Gröbnerbasis von $\ker(\phi) = J_x$ ist.

Den bisher vernachlässigten Teil $G_y := G \setminus G_x$ der Gröbnerbasis G werden wir im letzten Kapitel genauer betrachten.

3 Anwendung in der Algebraischen Geometrie

Wir behandeln nun Anwendungen von Eliminationsidealen im Hinblick auf die algebraische Geometrie.

Seien in diesem Kapitel R, S Ringe und $\phi : R \longrightarrow S$ ein Ringhomomorphismus. Wir notieren mit ϕ^* die von ϕ induzierte Abbildung auf den Spektren der Ringe.

$$\phi^* : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R) \quad , \quad \mathfrak{p} \longmapsto \phi^{-1}(\mathfrak{p})\,.$$

Proposition 3.1. *Für den Zariski Abschluss, des Bildes von ϕ^*, gilt*

$$\overline{\mathrm{im}(\phi^*)} = \mathcal{V}(\ker(\phi))$$

Beweis. Wir wollen die Proposition in zwei Schritten zeigen. Erstens gilt

$$\overline{\mathrm{im}(\phi^*)} = \mathcal{V}\left(\mathcal{I}\left(\mathrm{im}(\phi^*)\right)\right) = \mathcal{V}\left(\bigcap_{\mathfrak{p} \in \mathrm{im}(\phi^*)} \mathfrak{p}\right) = \mathcal{V}\left(\bigcap_{\mathfrak{q} \in \mathrm{Spec}(S)} \phi^*(\mathfrak{q})\right) \tag{1}$$

und zweitens erhalten wir

$$\begin{aligned}\bigcap_{\mathfrak{q}\in\mathrm{Spec}(S)} \phi^*(\mathfrak{q}) = \bigcap_{\mathfrak{q}\in\mathrm{Spec}(S)} \phi^{-1}(\mathfrak{q}) = \phi^{-1}\left(\bigcap_{\mathfrak{q}\in\mathrm{Spec}(S)} \mathfrak{q}\right) \\ = \phi^{-1}\left(\sqrt{\langle 0\rangle}\right) = \sqrt{\phi^{-1}(\{0\})} = \sqrt{\ker(\phi)}\end{aligned} \tag{2}$$

Aus (1) und (2) folgt

$$\begin{aligned}\overline{\mathrm{im}(\phi^*)} &= \mathcal{V}\left(\bigcap_{\mathfrak{q}\in\mathrm{Spec}(S)} \phi^*(\mathfrak{q})\right) = \mathcal{V}\left(\sqrt{\ker(\phi)}\right) = \mathcal{V}\left(\mathcal{I}\left(\mathcal{V}\left((\ker(\phi)\right)\right)\right) = \overline{\mathcal{V}\left(\ker(\phi)\right)} \\ &= \mathcal{V}\left(\ker(\phi)\right)\ ,\end{aligned}$$

wobei die letzte Gleichung nach Definition der Zariski Topologie gilt.

□

Bemerkung 3.2. An dieser Stelle wollen wir uns die Bijektion zwischen den Morphismen affiner Varietäten $X \in K^m$ und $Y \in K^n$ und den K-Algebren Homomorphismen der Koordinatenringe

$$\begin{aligned}\mathrm{Mor}(X,Y) &\longleftrightarrow \mathrm{Hom}_K\left(K[Y],K[X]\right) \\ f=(f_1,\ldots,f_n) &\longmapsto \begin{cases} \phi : K[Y] \longrightarrow K[X] \\ y_i + \mathcal{I}(Y) \longmapsto f_i + \mathcal{I}(X)\end{cases}\end{aligned}$$

in Erinnerung rufen, welche in Kapitel 3.1 [Kem10, S. 45] ausführlich behandelt wurde.

Korollar 3.3. *Sei $f : X \longrightarrow Y$ ein Morphismus von affinen Varietäten über einem algebraisch abgeschlossenen Körper K, welcher von $\phi : K[Y] \longrightarrow K[X]$ induziert wurde. So gilt*

$$\overline{f(X)} = \mathcal{V}_Y(\ker(\phi))\,.$$

Beweis. Folgt direkt aus Proposition 3.1 und da für affine Varietäten X und Y über einem algebraisch abgeschlossenen Körper gilt, dass

$$\mathrm{Hom}_K\left(K[Y],K[X]\right) \longrightarrow \mathrm{Mor}(\mathrm{Spec}(K[X]),\mathrm{Spec}(K[Y]))$$

eine Verallgemeinerung der Abbildung

$$\mathrm{Hom}_K\left(K[Y],K[X]\right) \longrightarrow \mathrm{Mor}(X,Y)$$

aus Bemerkung 3.2 ist. [vgl. Kem10, S.48] □

Bemerkung 3.4. Wir erhalten durch Proposition 2.2 eine Methode den Zariski Abschluss eines Bildes von einem Morphismen affiner Varietäten zu bestimmen.

Proposition 3.5. *Sei $X \subset K^n$ eine affine Varietät über einem algebraisch abgeschlossenen Körper K, welche durch das Ideal $I \subset K[x_1, \dots x_n]$ gegeben ist, d.h. $X = \mathcal{V}(I)$. Sei weiter $S := \{x_{i_1}, \dots x_{i_r}\}$ eine Menge von Unbekannten und*

$$\pi_S : K^n \longrightarrow K^r\,, \quad (\zeta_1, \dots \zeta_n) \longmapsto (\zeta_{i_1}, \dots, \zeta_{i_r})$$

so gilt für das Bild von $\pi_{S|_X}$

$$\overline{\pi_S(X)} = \mathcal{V}_{K^r}(I_S)\,.$$

Beweis. Um Korollar 3.3 anzuwenden, müssen wir den zu $\pi_{S|_X}$ zugehörigen Homomorphismus $\phi : K[K^r] \longrightarrow K[X]$ bestimmen und zeigen, dass $\mathcal{V}(\ker(\phi)) = \mathcal{V}(I_S)$ ist. Offensichtlich gilt, dass $\pi_S = (x_{i_1}, \dots, x_{i_r})$ ist, wobei man das Polynom $x_{i_j} \in K[x_1, \dots, x_n]$ auch als Projektion auf die i_j-te Komponente betrachten kann. Nach Bemerkung 3.2 erhalten wir also für ϕ folgende Abbildungsvorschrift:

$$\begin{aligned} \phi : K[x_{i_1}, \dots, x_{i_r}] = K[K^r] &\longrightarrow K[X] = {K[x_1, \dots, x_n]}/{\mathcal{I}(X)} \\ x_{i_j} &\longmapsto x_{i_j} + \mathcal{I}(X). \end{aligned}$$

Es bleibt zu zeigen, dass $\mathcal{V}(\ker(\phi)) = \mathcal{V}(I_S)$. Es genügt hierbei zu zeigen, dass $\ker(\phi) = \sqrt{I_S}$, denn $\mathcal{V}(\sqrt{I_S}) = \mathcal{V}(\sqrt{I}) \cup \mathcal{V}(K[x_{i_1}, \dots, x_{i_r}]) = \mathcal{V}(I) \cup \mathcal{V}(K[x_{i_1}, \dots, x_{i_r}]) = \mathcal{V}(I_S)$.

Sei $a \in \sqrt{I_S}$, so ist $a \in K[x_{i_1}, \dots, x_{i_r}] \cap \sqrt{I} = K[x_{i_1}, \dots, x_{i_r}] \cap \mathcal{I}(X)$, also gilt nach Definition von ϕ auch $a \in \ker(\phi)$.

Umgekehrt sei $a \in \ker(\phi)$. Dann ist $a \in K[x_{i_1}, \dots, x_{i_r}] \cap \mathcal{I}(X) = K[x_{i_1}, \dots, x_{i_r}] \cap \sqrt{I} = \sqrt{I_S}$.

Also folgt insgesamt mit Korollar 3.3

$$\overline{\pi_S(X)} = \mathcal{V}_{K^r}(\ker(\phi)) = \mathcal{V}_{K^r}(\sqrt{I_S}) = \mathcal{V}_{K^r}(I_S)\,.$$

□

Nun wollen wir behandeln wie man ein polynomiales Gleichungssystem, welches eine endlichen Lösungsmenge besitzt, mithilfe von Eliminationsidealen lösen kann. Wenn wir dies in der Sprache der algebraischen Geometrie formulieren, erhalten wir den folgenden Algorithmus.

Algorithmus 3.6. Sei $I \subset K[x_1, \dots, x_n]$ ein Ideal und K ein algebraisch abgeschlossener Körper. Sei außerdem $X := \mathcal{V}(I)$ eine endliche affine Varietät. Der folgende Algorithmus berechnet X.

Da X endlich und K algebraisch abgeschlossen ist, ist auch $\pi_{\{x_k, \dots, x_n\}}(X)$ endlich und somit abgeschlossen. Also erhalten wir aus Proposition 3.5 folgende Gleichung

$$\pi_{\{x_k, \dots, x_n\}}(X) = \mathcal{V}_{K^k}(I_{\{x_k, \dots, x_n\}})$$

Insbesondere folgt, dass $I_{\{x_k, \dots, x_n\}} \neq \{0\}$, denn $\pi_{\{x_k, \dots, x_n\}}(X) \neq K^k$, da K als algebraisch abgeschlossener Körper unendlich viele Elemente besitzt.

1. Berechne eine Gröbnerbasis G von I bzgl. der lexikographischen Ordnung $\leq$. Diese ist eine $\{x_k, \dots, x_n\}$-Eliminationsordnung für alle k. Somit ist $G_k := K[x_k, \dots, x_n] \cap G$ eine Gröbnerbasis von $I_k := I_{\{x_k,\dots,x_n\}}$ nach Theorem 1.3.

2. Sei $I_n \subset K[x_n]$. Da $K[x_n]$ ein Hauptidealring ist, existiert ein $0 \neq g \in K[x_n]$ mit $I_n = \langle g \rangle$.

   Wir wissen, dass $\pi_{\{x_n\}}(X) = \mathcal{V}(I_n) = \mathcal{V}(g)$, also sind alle Nullstellen ζ von g im Bild von $\pi_{\{x_n\}}$, daher existiert ein $(a_1, \dots, a_{n-1}, \zeta) \in X$, mit $a_i \in K$.

3. Betrachten wir nun das Ideal I_{n-1}, welches von den Elementen aus $G_{n-1} = \{f_1, \dots f_l\} \subset K[x_{n-1}, x_n]$ erzeugt wird. Sei ζ eine Nullstelle von g aus Schritt (2) und definiere $\widetilde{f}_i := f_i(-, \zeta) \in K[x_{n-1}]$. Sei weiter η eine Nullstelle aller $\widetilde{f}_i$, so ist $(\eta, \zeta) \in \mathcal{V}(f_1, \dots f_l) = \mathcal{V}(I_{n-1}) = \pi_{\{x_{n-1},x_n\}}(X)$. Also existiert ein $(a_1, \dots, a_{n-2}, \eta, \zeta) \in X$, mit $a_i \in K$.

4. Fahren wir wie in Schritt (3) fort, bis wir bei $I_1 = I$ ankommen, so erhalten wir alle Punkte von X.

Dieses Vorgehen zum Lösen polynomialer Gleichungssystheme ist vermutlich der Grund für den Name „Eliminationsideal“ .

4 Der Vernachlässigte Teil der Gröbnerbasis

Dieses letzte Kapitel ist wichtig für Vortrag 3.

Proposition 4.1. *(Der vernachlässigte Teil der Gröbnerbasis)*
Sei $\phi : K[x_1, \dots, x_n] \longrightarrow A := {}^{K[y_1,\dots,y_m]}\!/_{I}$ ein K-Algebren Homomorphismus und $\phi(x_i) = g_i + I =: \overline{g_i}$ mit $g_i \in K[y_1, \dots, y_m]$ für alle i.
Wir setzen $R := \mathrm{im}(\phi) \subset A$ und definieren den R-Algebren Homomorphismen

$$\Psi : R[y_1, \dots, y_m] \longrightarrow A\,, \quad y_i \longmapsto y_i + I$$

und den Ringhomomorphismus

$$\Phi : K[x_1, \dots, x_n, y_1, \dots, y_m] \cong K[x_1, \dots, x_n][y_1, \dots, y_m] \longrightarrow R[y_1, \dots, y_m]$$

wobei Φ gegeben ist, indem man die Koeffizienten f in $K[x_1, \dots, x_n]$ auf $\phi(f)$ abbildet.
Wie in Proposition 2.2 definieren wir

$$J := \langle I \cup \{g_1 - x_1, \dots, g_n - x_n\} \rangle_{K[x_1,\dots,x_n,y_1,\dots,y_m]}\,.$$

Sei $\leq$ eine $\{x_1, \dots, x_n\}$-Eliminationsordnung, G eine Gröbnerbasis von J bzgl. dieser Ordnung. Sei weiter $G_x := K[x_1, \dots, x_n] \cap G$ und $G_y := G \setminus G_x$ sei der Rest der Gröbnerbasis.
Dann gelten folgende Aussagen:

1. *G_x ist eine Gröbnerbasis von $\ker(\phi)$ bzgl. der Einschränkung von $\leq$ auf $K[x_1, \dots, x_n]$.*

2. $\ker(\Psi) = \langle \Phi(G_y) \rangle_{R[y_1,\dots,y_m]}$.

3. *Ist $\leq$ die Block-Ordnung bzgl. der Monomordnungen $\leq_x$ auf $K[x_1,\dots,x_n]$ und $\leq_y$ auf $K[y_1,\dots,y_m]$ welche durch $\leq_y$ dominiert wird, so gilt $\Phi(G_y)$ ist eine Gröbnerbasis von* $\ker(\Psi)$ *bezüglich $\leq_y$.*

Beweis. 1. Siehe Bemerkung 2.3.

2. Sei $g \in G_y$. Dann ist g insbesondere ein Element von $G \subset J$. Also gilt

$$g = h + \sum_{i=1}^{n} p_i(g_i - x_i)$$

wobei $p_i \in K[x_1,\dots,x_n,y_1,\dots,y_m]$ und $h \in I$. Also erhalten wir

$$\begin{aligned}\Psi(\Phi(g)) &= \Psi(\Phi(h)) + \Psi\left(\sum_{i=1}^{n} \Phi(p_i)\left(\Phi(g_i) - \Phi(x_i)\right)\right) \\ &= \Psi(\Phi(h)) + \Psi\left(\sum_{i=1}^{n} \Phi(p_i)\left(g_i - \phi(x_i)\right)\right) .\end{aligned}$$

Da $g_i - \phi(x_i) \in I$, $\Phi(h) = h \in I \subset K[y_1,\dots,y_m]$ und $\Psi(a) = 0 \in A$ für alle $a \in I$, folgt $\Psi(\Phi(g)) = 0 \in A$, also gilt $\Phi(G_y) \subset \ker(\Psi)$.

Sei umgekehrt $f \in \ker(\Psi)$. Da Φ offensichtlich surjektiv ist, existiert ein $F \in K[x_1,\dots,x_n,y_1,\dots,y_m]$ mit $\Phi(F) = f$.

Zwischenbehauptung: $F \in J$:

Beweis. Im folgenden nutzen wir die Multi-Index-Notation $\alpha := (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$ und $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Zudem definieren wir $\overline{g} := (\overline{g_1},\dots,\overline{g_n})$. Sei

$$F = \sum_{\alpha,\beta} a_{\alpha,\beta} \cdot x^\alpha y^\beta \text{ mit } a_{\alpha,\beta} \in K .$$

Dann ist $f = \Phi(F) = \sum_{\alpha,\beta} a_{\alpha,\beta} \cdot \overline{g}^\alpha y^\beta$. Da f auch im Kern von Ψ ist, muss $\overline{g}^\alpha = 0$ in R sein, oder $y^\beta \in I$ gelten. Im ersten Fall folgt $\phi(x^\alpha) = \overline{g}^\alpha = 0$, also ist $x^\alpha \in \ker(\phi) = J \cap K[x_1,\dots,x_n] \subset J$ nach Proposition 2.2 und somit ist $a_{\alpha,\beta} \cdot x^\alpha y^\beta \in J$. Tritt der zweite Fall ein, so ist $a_{\alpha,\beta} \cdot x^\alpha y^\beta \in I \subset J$. Insgesamt folgt $F \in J$.

Mit der Zwischenbehauptung erhalten wir $F \in \langle G_x \cup G_y \rangle_{K[x_1,\dots,x_n,y_1,\dots,y_m]}$, also gilt weiter, dass $f \in \langle \Phi(G_x \cup G_y) \rangle_{R[y_1,\dots,y_m]} = \langle \Phi(G_x) \cup \Phi(G_y) \rangle_{R[y_1,\dots,y_m]}$. Es ist jedoch $\Phi(G_x) = 0$, denn für $g \in G_x = K[x_1,\dots,x_n] \cap G \subset \ker(\phi)$ folgt $\Phi(g) = \phi(g) = 0$. Somit ergibt sich $f \in \langle \Phi(G_y) \rangle_{R[y_1,\dots,y_m]}$.

Um Teil 3. der Proposition zu beweisen, benötigen wir folgendes Lemma.

Lemma 4.2. *Seien die Voraussetzungen dieselben wie in Proposition 4.1 3. Sei f ein Polynom in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ mit der Eigenschaft, dass kein $g \in G_x$ existiert, so dass $\mathcal{LM}(g)$ ein Teiler von $\mathcal{LM}(f)$ ist. Fassen wir f als Element in $K[x_1, \ldots, x_n][y_1, \ldots, y_m]$ auf, so können wir das Leitmonom $\mathcal{LM}_y(f)$ und den Leitkoeffizienten $\mathcal{LC}_y(f)$ bzgl. der Monomordnung $\leq_y$ bestimmen. Dann gilt*

$$\mathcal{LC}(\Phi(f)) = \phi(\mathcal{LC}_y(f))\,, \tag{3}$$

sowie

$$\mathcal{LM}(f) = \mathcal{LM}_y(\Phi(f)) \cdot \mathcal{LM}(\mathcal{LC}_y(f))\,. \tag{4}$$

Beweis. Nach der Definition der Block-Ordnung, erhalten wir die Gleichung

$$\mathcal{LM}(f) = \mathcal{LM}_y(f) \cdot \mathcal{LM}(\mathcal{LC}_y(f))\,, \tag{5}$$

also bleibt zu zeigen, dass $\mathcal{LM}_y(\Phi(f)) = \mathcal{LM}_y(f)$.

Angenommen dies gilt nicht. Da $\Phi(y_i) = y_i$, folgt $\mathcal{LM}_y(\Phi(f)) \neq \mathcal{LM}_y(f)$ genau dann, wenn der Leitkoeffizient $\mathcal{LC}_y(f)$ im Kern von Φ liegt, mit anderen Worten, falls $\phi(\mathcal{LC}_y(f)) = 0$.

Sei also $\mathcal{LC}_y(f) \in \ker(\phi)$. Somit existiert $g \in G_x$ mit der Eigenschaft, dass $\mathcal{LM}(\mathcal{LC}_y(f))$ von $\mathcal{LM}(g)$ geteilt wird. Dann folgt jedoch mit (5), dass $\mathcal{LM}(g)$ insbesondere $\mathcal{LM}_y(f) \cdot \mathcal{LM}(\mathcal{LC}_y(f)) = \mathcal{LM}(f)$ teilt. Dies ist ein Widerspruch zu den Voraussetzungen.

Insgesamt erhalten wir Gleichung (4) und da wir zudem gezeigt haben, dass $\mathcal{LM}_y(\Phi(f)) = \mathcal{LM}_y(f)$, sieht man leicht, dass auch Gleichung (3) gelten muss.

□

3. Um die dritte Aussage von Proposition 4.1 zu beweisen genügt es zu zeigen, dass für $0 \neq f \in \ker(\Psi)$ ein $g \in G_y$ existiert mit der Eigenschaft, dass $\mathcal{LM}_y(f)$ durch $\mathcal{LM}_y(\Phi(g))$ geteilt wird. Wie im Beweis von Proposition 4.1 2. finden wir ein $F \in J$ mit $\Phi(F) = f$.

   Nach Definition, gilt für eine Normalform F^* von F bzgl. G_x

   $$F - F^* = \sum_{i=1}^{d} p_i \tilde{g}_i\,,$$

   mit $\{\tilde{g}_1, \ldots, \tilde{g}_d\} = G_x$ und $p_i \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Deshalb folgt

   $$\Phi(F) - \Phi(F^*) = \sum_{i=1}^{d} \Phi(p_i)\Phi(\tilde{g}_i) = \sum_{i=1}^{d} \Phi(p_i)\phi(\tilde{g}_i) = 0\,, \tag{6}$$

   wobei die vorletzte Gleichung gilt, da $\tilde{g}_i \in K[x_1, \ldots x_n]$ und die letzte, da $G_x \subset \ker(\phi)$. Somit ist $\Phi(F) = \Phi(F^*)$ und wir können ohne Einschränkung annehmen, dass F eine Normalform bzgl. G_x ist. Also wird kein Element in $\mathrm{Mon}(F)$ durch irgendein $\mathcal{LM}(\tilde{g}_i)$

mit $\tilde{g}_i \in G_x$ geteilt. Da F jedoch in J ist, muss es ein $g \in G = G_x \cup G_y$ geben, sodass $\mathcal{LM}(g)$ das Leitmonom $\mathcal{LM}(F)$ teilt und folglich ist $g \in G_y$. Wenn man nun Lemma 4.2 (4) auf F und g anwendet und ausnutzen, dass $\mathcal{LM}(\mathcal{LC}_y(g)), \mathcal{LM}(\mathcal{LC}_y(F)) \in K[x_1, \ldots, x_n]$, sowie $\mathcal{LM}_y(\Phi(g)), \mathcal{LM}_y(\Phi(F)) \in K[y_1, \ldots, y_m]$, so erhält man, dass $\mathcal{LM}_y(\Phi(g))$ das Leitmonom $\mathcal{LM}_y(\Phi(F)) = \mathcal{LM}(f)$ teilt. Dies zeigt die Behauptung.

□

Literatur

[CLO15] D.A. Cox, J. Little und D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 9783319167213.

[Kem10] G. Kemper. *A Course in Commutative Algebra*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2010. ISBN: 9783642035456.