Gröbnerbasen und Eliminationstheorie

Vortrag im Rahmen des Seminars der WE AlZAGK im
Wintersemester 2007/2008 an der Universität Bremen

Fabian Dreher

24./31.01.2008 & 07.02.2008

Vorbemerkung

Zielsetzung meines Vortrags war es auszuführen, wie Gröbnerbasen genutzt werden können, um Variablen in Systemen von Polynomgleichungen zu eliminieren und anschließend eine geometrische Deutung der Situation darzulegen.

Als Grundlage diente das Buch „Ideals, Varieties, and Algorithms" von Cox, Little und O'Shea, auf welches ich auch für die meisten hier unbewiesenen Sätze verweise.

1 Definitionen und Grundlagen

In diesem ersten Abschnitt sind im Folgenden benötigte Definitionen sowie Tatsachen über Gröbnerbasen zusammengestellt.

1.1 Definition *Seien $\alpha = (\alpha_1, \dots, \alpha_n)$ und $\beta = (\beta_1, \dots, \beta_n)$ aus $\mathbb{Z}^n_{\geq 0}$. Es gelte $\alpha > \beta$, wenn in der Differenz $\alpha - \beta \in \mathbb{Z}^n$ der Vektoren der am weitesten links stehende Eintrag ungleich Null positiv ist. Wir schreiben $x^\alpha > x^\beta$, falls $\alpha > \beta$. Die so durch $<$ gegebene Monomordnung auf $K[x_1, \dots, x_n]$ heißt* ***lexikographische Ordnung*** *(kurz: „Lex") bezüglich $x_1 > x_2 > \cdots > x_n$.*

1.2 Definition *Sei $f = \sum_\alpha a_\alpha x^\alpha \in K[x_1, \dots, x_n]$ ein Polynom ungleich Null. Sei $>$ eine Monomordnung auf $K[x_1, \dots, x_n]$.*

(1) Der Multigrad von f ist $\mathrm{multideg}(f) \coloneqq max_>\{\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0\}$.
(2) Das Leitmonom von f ist $\mathrm{LM}(f) \coloneqq x^{\mathrm{multideg}\ (f)}$.
(3) Der Leitterm von f ist $\mathrm{LT}(f) \coloneqq a_{\mathrm{multideg}\ (f)} \cdot x^{\mathrm{multideg}\ (f)}$.

Für $M \subset K[x_1, \dots, x_n]$ bezeichne $\mathrm{LT}(M)$ das von den Leittermen der Elemente aus M erzeugte Ideal, also $\mathrm{LT}(M) \coloneqq \langle\{\mathrm{LT}(f)\,|\,f \in M\}\rangle$, analog für LM.

1.3 Definition *Bezüglich einer festen Monomordnung gilt: Eine endliche Teilmenge $G = \{g_1, \dots, g_r\}$ eines Ideals $I \subset K[x_1, \dots, x_n]$ heißt* ***Gröbnerbasis*** *von I, wenn gilt $\langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_r)\rangle = \mathrm{LT}(I)$.*

Bei der Betrachtung eines Polynomrings über einem Körper erhält man eine offensichtlich äquivalente Charakterisierung von Gröbnerbasen, wenn man die Definition 1.3 statt mit LT mit LM formuliert. Für einen Polynomring über einem Ring, der kein Körper ist, gilt dies nicht. Wir werden jedoch nur Polynomringe über einem Körper K betrachten.

1.4 Satz *Bezüglich einer festen Monomordnung hat jedes Ideal $I \subset K[x_1, \dots, x_n]$, $I \neq \{0\}$, eine Gröbnerbasis. Außerdem gilt: Jede Gröbnerbasis von I ist auch Basis von I.*

2 Gröbnerbasen in der Eliminationstheorie

Um einen Eindruck davon zu erhalten, was wir mit Gröbnerbasen zu erreichen wünschen, betrachten wir folgendes System von Polynomgleichungen:

$$x^2 + y + z = 1$$
$$x + y^2 + z = 1$$
$$x + y + z^2 = 1$$

Sei $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$ das sich aus diesen Gleichungen ergebende Ideal. Eine Gröbnerbasis von I bezüglich Lex ist gegeben durch

$$\begin{aligned} g_1 &= x + y + z^2 - 1 \\ g_2 &= y^2 - y - z^2 + z \\ g_3 &= 2yz^2 + z^4 - z^2 \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2 \end{aligned}$$

Da eine Gröbnerbasis nach Satz 1.4 auch eine Basis ist, gilt $I = \langle g_1, g_2, g_3, g_4 \rangle$. Die ursprünglichen drei Gleichungen und die vier von der Gröbnerbasis stammenden haben daher die gleiche Nullstellenmenge. Wir sehen, dass in diesem Fall in der Gröbnerbasis nacheinander die Variablen eliminiert werden.

2.1 Definition *Für ein Ideal $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$ heißt das durch $I_k := I \cap K[x_{k+1}, \dots, x_n]$ gegebene Ideal in $K[x_{k+1}, \dots, x_n]$ das k-te **Eliminationsideal**.*

Mit dem Begriff des Eliminationsideals lässt sich nun die am Beispiel gemachte Beobachtung allgemein formulieren.

2.2 Satz (Eliminationssatz) *Sei $I \subset K[x_1, \dots, x_n]$ ein Ideal und sei $G = \{g_1, \dots, g_r\}$ eine Gröbnerbasis von I bezüglich Lex mit $x_1 > x_2 > \dots > x_n$. Dann ist $G_k = G \cap K[x_{k+1}, \dots, x_n]$ eine Gröbnerbasis des k-ten Eliminationsideals I_k.*

Beweis. Sei k fest gewählt. Es sei oBdA $G_k = \{g_1, \dots, g_s\}$. Wir zeigen zuerst, dass $\{\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\}$ eine Basis von $\mathrm{LT}(I) \cap K[x_{k+1}, \dots, x_n]$ bildet.
Sei $m \in \mathrm{LT}(I) \cap K[x_{k+1}, \dots, x_n]$ ein Monom. Da G eine Gröbnerbasis von I ist, muss m ein Vielfaches von $\mathrm{LT}(g_i)$ für ein $1 \leq i \leq r$ sein. Es folgt $\mathrm{LT}(g_i) \in K[x_{k+1}, \dots, x_n]$ und damit auch $\mathrm{LM}(g_i) \in K[x_{k+1}, \dots, x_n]$. Wegen der Benutzung von Lex kann g_i kein Monom enthalten, das ein $x_1, \dots, x_k$ enthält, da dieses Monom dann größer wäre als $\mathrm{LM}(g_i)$. Folglich gilt $g_i \in K[x_{k+1}, \dots, x_n]$ und somit $g_i \in G_k$, also $i \leq s$.
$\mathrm{LT}(I)$ ist ein Monomideal, und somit ist auch $\mathrm{LT}(I) \cap K[x_{k+1}, \dots, x_n]$ ein Monomideal. Da, wie soeben gezeigt, $\{\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\}$ alle Monome in $\mathrm{LT}(I) \cap K[x_{k+1}, \dots, x_n]$ erzeugt, ist $\{\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\}$ eine Basis von $\mathrm{LT}(I) \cap K[x_{k+1}, \dots, x_n]$.
Offensichtlich gilt $\mathrm{LT}(I_k) \subset \mathrm{LT}(I) \cap K[x_{k+1}, \dots, x_n]$; auf Grund unseres vorigen Ergebnisses und $G_k \subset I_k$ gilt sogar Gleichheit. Also ist G_k eine Gröbnerbasis von I_k. ■

Gröbnerbasen bezüglich Lex erlauben die systematische Elimination von Variablen in Systemen von Polynomgleichungen.

2.3 Definition *Sei K algebraisch abgeschlossen. Seien $f_1, \dots, f_r \in K[x_1, \dots, x_n]$.*

$$V(f_1, \dots, f_r) := \{(a_1, \dots, a_n) \in K^n | f_i(a_1, \dots, a_n) = 0, 1 \leq i \leq r\}$$

*heißt die durch $f_1, \dots, f_r$ gegebene **affine Varietät**.*

Nun, da wir mittels Gröbnerbasen die Eliminationsideale I_k beschreiben können, stellt sich die Frage, welche partiellen Lösungen $(a_{k+1}, \dots, a_n) \in V(I_k)$ zu vollständigen Lösungen in $V(I)$ erweitert werden können. Ein hinreichendes Kriterium gibt der Erweiterungssatz.

Im Folgenden sei $\boldsymbol{K}$ **stets algebraisch abgeschlossen**.

2.4 Satz (Erweiterungssatz) *Sei $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$ und sei I_1 das erste Eliminationsideal von I. Für $1 \leq i \leq r$ schreibe man f_i in der Form*

$$f_i = g_i(x_2, \dots, x_n) x_1^{N_i} + Terme, in\ denen\ x_1\ den\ Grad < N_i\ hat$$

wobei $N_i \geq 0$ und $g_i \in K[x_2, \dots, x_n]$ ungleich Null. Sei $(a_2, \dots, a_n) \in V(I_1)$. Wenn $(a_2, \dots, a_n) \notin V(g_1, \dots, g_r)$, so gibt es ein $a_1 \in K$, so dass $(a_1, a_2, \dots, a_n) \in V(I)$.

2.5 Folgerung *Sei $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$ und sei ein f_i von der Form*

$$f_i = c x_1^N + Terme, in\ denen\ x_1\ den\ Grad < N\ hat$$

wobei $N > 0$ und $c \in K, c \neq 0$. Dann gibt es für jedes $(a_2, \dots, a_n) \in V(I_1)$ ein $a_1 \in K$, so dass $(a_1, a_2, \dots, a_n) \in V(I)$.

Beweis. Sei $(a_2, \dots, a_n) \in V(I_1)$. In der Notation des Erweiterungssatzes gilt $g_i = c \neq 0$, woraus folgt $V(g_1, \dots, g_r) = \emptyset$. Also $(a_2, \dots, a_n) \notin V(g_1, \dots, g_n)$ und somit sichert der Erweiterungssatz die Existenz eines geeigneten $a_1 \in K$. ∎

Ein Beweis des Erweiterungssatzes findet sich bei (Cox, Little, & O'Shea, S. 162). Wir werden uns an dieser Stelle auf den Beweis eines Spezialfalls beschränken. Die benötigten Tatsachen über Resultanten sind, um den Lesefluss nicht unnötig zu stören, nach Abschnitt 0 ausgelagert.

2.6 Satz *Sei $I := \langle f, g \rangle \in K[x_1, \dots, x_n]$, wobei $f = a_0 x_1^l + a_1 x_1^{l-1} + \cdots + a_l$ mit $a_i \in K[x_2, \dots, x_n], a_0 \neq 0, l \geq 1$ und $g = b_0 x_1^m + b_1 x_1^{m-1} + \cdots + b_m$ mit $b_i \in K[x_2, \dots, x_n]$, $b_0 \neq 0, m \geq 1$. Sei $(c_2, \dots, c_n) \in V(I_1)$. Wenn $(c_2, \dots, c_n) \notin V(a_0, b_0)$, dann existiert ein $c_1 \in K$, so dass $(c_1, c_2, \dots, c_n) \in V(f, g)$.*

Beweis. Es sei $c = (c_2, \dots, c_n)$. Wir schreiben kurz $f(x_1, c) = f(x_1, c_2, \dots, c_n)$. Im folgenden werden wir zeigen, dass $f(x_1, c)$ und $g(x_1, c)$ eine gemeinsame Nullstelle c_1 haben, die uns den benötigten Punkt $(c_1, c_2, \dots, c_n) \in V(f, g)$ liefert.
Nehmen wir zuerst an, dass $a_0(c)$ und $b_0(c)$ beide ungleich Null sind, also

$$f(x_1, c) = a_0(c) x_1^l + \cdots + a_l(c), \quad a_0(c) \neq 0$$
$$g(x_1, c) = b_0(c) x_1^m + \cdots + b_l(c), \quad b_0(c) \neq 0$$

Der Grad in x_1 von $f(x_1, c)$ und f beziehungsweise von $g(x_1, c)$ und g stimmt also überein. Nach Satz 4.2 gilt $h := \mathrm{Res}(f, g, x_1) \in I_1$, also $h(c) = 0$, da $c \in V(I_1)$ nach Voraussetzung. Wegen $0 = h(c) = (\mathrm{Res}(f, g, x_1))(c) = \mathrm{Res}(f(x_1, c), g(x_1, c), x_1)$, weil die Grade der Polynome übereinstimmen, gibt es nach Folgerung 4.3 eine gemeinsame Nullstelle $c_1 \in K$ von $f(x_1, c)$ und $g(x_1, c)$, mit der gilt $(c_1, c) \in V(f, g)$.
Nun ist der Fall zu betrachten, dass $a_0(c)$ und $b_0(c)$ nicht beide ungleich Null sind. Unsere Voraussetzung sichert aber, dass höchstens eins von beiden Null ist. Nehmen wir also oBdA an, dass $a_0(c) \neq 0$ und $b_0(c) = 0$. Dann ist der Grad von $g(x_1, c)$ in x_1 echt kleiner als m und wir können nicht mehr wie zuvor Resultantenbildung und Einsetzen vertauschen.
Wir modifizieren nun die Basis des Ideals $\langle f, g \rangle$. Sei $N \in \mathbb{N}$ so gewählt, dass N größer ist als der Grad von g in x_1. Es gilt $\langle f, g \rangle = \langle f, g + x_1^N f \rangle$ und $g + x_1^N f$ hat bezüglich x_1 den Leitkoeffizienten a_0, für den gilt $a_0(c) \neq 0$. Daher lässt sich auf $f, g + x_1^N f$ unser erstes Argument anwenden, das uns eine gemeinsame Nullstelle c_1 liefert, so dass $(c_1, c) \in V(f, g + x_1^N f)$. Wegen $\langle f, g \rangle = \langle f, g + x_1^N f \rangle$ gilt auch $(c_1, c) \in V(f, g)$.s ∎

Der Erweiterungssatz sagt nur etwas über das erste Eliminationsideal aus, doch da I_{k+1} das erste Eliminationsideal von I_k ist, lässt sich der Erweiterungssatz mehrfach anwenden, wenn mehr als eine Variable eliminiert wird.

Zu beachten ist, dass $g_1, \dots, g_r$ und damit $V(g_1, \dots, g_r)$ von den gewählten Erzeugern des Ideals I abhängen. Im folgenden Abschnitt werden wir daher die im Erweiterungssatz auftretenden affinen Varietäten näher betrachten.

3 Geometrische Deutung der Elimination

Es sei auch weiterhin K stets algebraisch abgeschlossen. Es bezeichne $\pi_k: K^n \to K^{n-k}$ die Projektionsabbildung $(a_1, \dots, a_n) \mapsto (a_{k+1}, \dots, a_n)$.

Wir wollen einen Zusammenhang zwischen der Projektion $\pi_k(V(I))$ einer affinen Varietät $V(I)$ und dem entsprechenden Eliminationsideal I_k formulieren.

3.1 Lemma *Sei $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$ und $V = V(I) \subset K^n$ und sei I_k das k-te Eliminationsideal von I. Dann gilt $\pi_k(V) \subset V(I_k)$ in K^{n-k}.*

Beweis. Sei $f \in I_k$. Wegen $f \in I$ verschwindet f an den Punkten $(a_1, \dots, a_n) \in V$. Weil f nur $x_{k+1}, \dots, x_n$ enthält, gilt $f(a_{k+1}, \dots, a_n) = f(\pi_k(a_1, \dots, a_n)) = 0$. Also verschwindet f an allen Punkten von $\pi_k(V)$. ∎

Es ist festzuhalten, dass $\pi_k(V(I))$ im Allgemeinen keine affine Varietät ist, wie das folgende Beispiel zeigt.

Beispiel. Wir betrachten die Gleichungen

$$xy = 1$$
$$xz = 1$$

Und das zugehörige Ideal $I = \langle xy - 1, xz - 1 \rangle$. Das erste Eliminationsideal ist $I_1 = \langle y - z \rangle$. Es gilt „$\supset$" wegen $y - z = -y \cdot (xz - 1) + z \cdot (xy - 1) \in I$; die umgekehrte Inklusion lässt sich mittels elementarer Rechnung verifizieren. Es gilt:

$$V(I) = \left\{ \left(\frac{1}{a}, a, a \right) \middle| a \in K, a \neq 0 \right\}$$
$$\pi_1(V(I)) = \{(a, a) | a \in K, a \neq 0\}$$
$$V(I_1) = \{(a, a) | a \in K\}$$

Eine bildliche Darstellung dieser Situation findet sich bei (Cox, Little, & O'Shea, S. 122). $\pi_1(V(I))$ ist hier keine affine Varietät, da der Punkt $(0,0)$ fehlt.

$\pi_1(V(I))$ enthält genau jene partiellen Lösungen, die zu vollständigen Lösungen erweitert werden können. Die Frage der Erweiterbarkeit behandelte der Erweiterungssatz 2.4, seine Aussage lässt sich auch geometrisch formulieren.

3.2 Satz (Geometrischer Erweiterungssatz) *Sei $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$ und $V = V(I) \subset K^n$ und seien g_i, $1 \leq i \leq r$, wie im Ergänzungssatz 2.4. Sei I_1 das erste Eliminationsideal von I. Dann gilt $V(I_1) = \pi_1(V) \cup (V(g_1, \dots, g_r) \cap V(I_1))$ in K^{n-1}.*

Beweis. Wegen Lemma 3.1 gilt „$\supset$". Es reicht nun zu zeigen, dass auch $V(I_1) \setminus \pi_1(V) \subset V(g_1, \dots, g_r)$. Sei $(a_2, \dots, a_n) \in V(I_1) \setminus \pi_1(V)$. $(a_2, \dots, a_n)$ lässt sich folglich nicht zu einem Element von $V(f_1, \dots, f_r)$ ergänzen. Daher folgt aus Satz 2.4, dass $(a_2, \dots, a_n) \in V(g_1, \dots, g_r)$. ■

Der geometrische Erweiterungssatz besagt, dass $V(I_1)$ aus der Projektion $\pi_1(V)$ und möglicherweise noch aus einem Teil, der in $V(g_1, \dots, g_r)$ liegt, besteht. Wie im Anschluss an den Erweiterungssatz erwähnt, ist $V(g_1, \dots, g_r)$ von den gewählten Erzeugern von I abhängig und kann außerordentlich groß sein. Es ist sogar möglich, dass $V(g_1, \dots, g_r) = V(I_1)$ gilt, was dazu führt, dass mittels des geometrischen Erweiterungssatzes keine Information über die Größe von $\pi_1(V)$ gewonnen werden kann.

Beispiel. Betrachten wir wieder die Situation des vorherigen Beispiels mit den Gleichungen $xy = 1$ und $xz = 1$. Es gilt

$$I = \langle xy - 1, xz - 1 \rangle = \langle (y - z)x^2 + xy - 1, (y - z)x^2 + xz - 1 \rangle$$

Die Erzeuger $f_1 = (y - z)x^2 + xy - 1$, $f_2 = (y - z)x^2 + xz - 1$ haben beide den Leitkoeffizienten $g_1 = g_2 = y - z$ bezüglich x, was bedeutet, dass in diesem Fall gilt $V(g_1, g_2) = V(y - z) = V(I_1)$.

Der Abschlusssatz formuliert einen von den Erzeugern unabhängigen Zusammenhang zwischen $\pi_1(V)$ und $V(I_1)$.

3.3 Satz (Abschlusssatz) *Sei $V = V(f_1, \dots, f_r) \subset K^n$ und sei I_1 das erste Eliminationsideal von $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$. Dann gilt:*

(1) $V(I_1)$ ist die kleinste affine Varietät, die $\pi_1(V) \subset K^{n-1}$ enthält.

(2) Wenn $V \neq \emptyset$, dann gibt es eine affine Varietät $U \subsetneq V(I_1)$, so dass $V(I_1) \setminus U \subset \pi_1(V)$.

Im Beweis werden die folgenden Schreibweisen sowie die in Abschnitt 0 aufgeführten Aussagen 4.4 und 4.5 (Hilbertscher Nullstellensatz) benötigt. Für eine Menge $M \subset K^n$ sei $I(M) \coloneqq \{f \in K[x_1, \dots, x_n] | \forall x \in M : f(x) = 0\}$. Man beachte, dass $I(M)$ ein Ideal ist. Für ein Ideal $I \subset K[x_1, \dots, x_n]$ bezeichne $\operatorname{rad} I \coloneqq \{f | \exists m > 0 : f^m \in I\}$ das zu I gehörende Radikalideal.

Beweis. Zu (1): Nach Lemma 4.4 gilt es zu zeigen, dass $V(I_1) = V(I(\pi_1(V)))$. Man beachte, dass $I(\cdot)$ und $V(\cdot)$ jeweils inklusionsumkehrend wirken.
Nach Lemma 3.1 gilt $\pi_1(V) \subset V(I_1)$. Da $V(I(\pi_1(V))$ die kleinste $\pi_1(V)$ enthaltende Varietät ist, gilt also $V(I_1) \supset V(I(\pi_1(V))$.
Betrachten wir nun ein Polynom $f \in I(\pi_1(V)) \subset K[x_2, \dots, x_n]$. Aufgefasst als Element von $K[x_1, \dots, x_n]$ gilt offenbar $f \in I(V)$. Wegen $V = V(I)$ und dem Hilbertschen Nullstellensatz (4.5) folgt $f \in \operatorname{rad} I$. Sei N so gewählt, dass $f^N \in I$. Da f nicht von x_1 abhängt, hängt auch f^N nicht von x_1 ab, und es gilt $f^N \in I \cap K[x_2, \dots, x_n] = I_1$, also $f \in \operatorname{rad} I_1$. Dies bedeutet $I(\pi_1(V)) \subset \operatorname{rad} I_1$. Es folgt $V(I_1) = V(\operatorname{rad} I_1) \subset V(I(\pi_1(V)))$.

Zu (2): Wir werden die Zerlegung $V(I_1) = \pi_1(V) \cup (V(g_1, \dots, g_r) \cap V(I_1))$ aus Satz 3.2 verwenden. Es sei $W \coloneqq V(g_1, \dots, g_r) \cap V(I_1)$. W ist als Durchschnitt zweier affiner Varietäten selbst eine affine Varietät (Cox, Little, & O'Shea, S. 11). Aus der Zerlegung folgt $V(I_1) \setminus W \subset \pi_1(V)$. Falls $W \neq V(I_1)$, so sind wir mittels der Setzung $U = W$ fertig.
Nehmen wir nun an, dass $W = V(I_1)$. Da W von den definierenden Elementen von V abhängt, werden wir versuchen, durch eine Veränderung dieser Gleichungen W in geeigneter Weise zu modifizieren.

Aus $W = V(I_1)$ folgt, dass $V = V(f_1, \dots, f_r, g_1, \dots, g_r)$. „$\subset$“ ist offensichtlich, da mehr Gleichungen hinzu genommen werden. „$\supset$“ gilt, da $\pi_1(V) \subset V(I_1) = W \subset V(g_1, \dots, g_r)$ und somit auch die g_i bei $(a_1, \dots, a_n) \in V$ verschwinden.

Sei $\tilde{I} = \langle f_1, \dots, f_r, g_1, \dots, g_r \rangle$. I und $\tilde{I}$ können verschieden sein, haben jedoch die gleiche Varietät V. Auch die zugehörigen ersten Eliminationsideale können verschieden sein, nach (1) gilt jedoch, dass die entsprechenden Varietäten jeweils die kleinste $\pi_1(V)$ Umfassende sind und somit $V(I_1) = V(\tilde{I}_1)$.

Nun suchen wir eine andere Basis von $\tilde{I}$. Betrachten wir dazu die Definition der g_i per

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + Terme, in\ denen\ x_1\ den\ Grad < N_i\ hat$$

wobei $N_i \geq 0$ und $g_i \in \mathbb{C}[x_2, \dots, x_n]$ ungleich Null.

Sei $\tilde{f}_i \coloneqq f_i - g_i x_1^{N_i}$. Dabei sind die $\tilde{f}_i$ entweder Null oder haben einen echt kleineren Grad in x_1 als das zugehörige f_i. Es gilt $\tilde{I} = \langle \tilde{f}_1, \dots, \tilde{f}_r, g_1, \dots, g_r \rangle$. Mit Satz 3.2 erhalten wir eine neue Zerlegung $V(I_1) = V(\tilde{I}_1) = \pi_1(V) \cup \widetilde{W}$. Wegen $W = V(I_1)$ gilt $\widetilde{W} \subset W$.

Falls $\widetilde{W}$ echt kleiner als W ist, haben wir mittels der Setzung $U = \widetilde{W}$ ein geeignete Varietät gefunden. Falls $\widetilde{W} = W = V(I_1)$, so wiederholen wir den Prozess.

Betrachten wir nun, was passiert, falls immer $V(I_1)$ herauskommt. Bei jedem Schritt verringert sich der Grad in x_1 der erzeugenden Elemente (oder sie werden Null), was bedeutet, dass schließlich alle Erzeuger den Grad 0 in x_1 haben werden. Da x_1 in den definierenden Gleichungen von V dann nicht mehr auftritt, folgt $\pi_1(V) = V(I_1)$. In diesem Fall ist $U = \emptyset$ eine geeignete Varietät. ■

Die exakte Struktur von $\pi_1(V)$ kann wie folgt beschrieben werden: Es gibt affine Varietäten $Z_i \subset W_i \subset K^{n-1}$ für $1 \leq i \leq l$, so dass gilt

$$\pi_1(V) = \bigcup_{i=1}^{l} (W_i - I_i)$$

Allgemein heißt eine Menge dieser Gestalt „konstruierbar“.

Wie beim Erweiterungssatz in Form von Folgerung 2.5, so gibt es auch geometrisch eine analoge einfache Situation.

3.4 Folgerung *Sei $I = \langle f_1, \dots, f_r \rangle \subset K[x_1, \dots, x_n]$ und sei ein f_i von der Gestalt*

$$f_i = c x_1^N + Terme, in\ denen\ x_1\ den\ Grad < N\ hat$$

wobei $c \in K, c \neq 0, N > 0$. Sei I_1 das erste Eliminationsideal. Dann gilt für $V = V(I)$:

$$\pi_1(V) = V(I_1)$$

4 Allgemeine Ergebnisse

In diesem Abschnitt sind die zuvor benötigten Ergebnisse über Resultanten und algebraische Geometrie gesammelt. Zum Thema Resultanten sei auch auf (Haase, 2007) (online verfügbar) verwiesen.

4.1 Definition *Seien* $f, g \in K[x_1, \dots, x_n]$ *mit*

$$f = a_0 x_1^l + \dots + a_l, \qquad a_0 \neq 0, l \geq 1$$
$$g = b_0 x_1^m + \dots + b_m, \qquad b_0 \neq 0, m \geq 1$$

Die Resultante von f *und* g *bezüglich* x_1 *ist die Determinante*

$$Res(f, g, x_1) = det \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ & a_l & \ddots & & & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}$$

4.2 Satz *Seien* $f, g \in K[x_1, \dots, x_n]$ *Polynome von positivem Grad in* x_1*. Dann gilt:*

(1) $Res(f, g, x_1) \in \langle f, g \rangle \cap K[x_2, \dots, x_n]$

(2) $Res(f, g, x_1) = 0$ *genau dann, wenn* f *und* g *einen gemeinsamen Faktor in* $K[x_1, \dots, x_n]$ *haben, der positiven Grad in* x_1 *hat.*

(Cox, Little, & O'Shea, S. 159)

4.3 Folgerung *Sei* K *algebraisch abgeschlossen. Dann gilt für* $f, g \in K[x]$*:* $Res(f, g, x) = 0$ *genau dann, wenn* f *und* g *eine gemeinsame Nullstelle in* K *haben.*

4.4 Lemma *Sei* $M \subset K^n$*. Dann ist* $V(I(M))$ *die kleinste affine Varietät, die* M *enthält. (Cox, Little, & O'Shea, S. 191)*

4.5 Satz (Hilbertscher Nullstellensatz) *Sei* K *algebraisch abgeschlossen und sei* $I \subset K[x_1, \dots, x_n]$ *ein Ideal. Dann gilt* $I(V(I)) = rad\, I$*. (Cox, Little, & O'Shea, S. 175)*

5 Literaturverzeichnis

Cox, D., Little, J., & O'Shea, D. (1992). *Ideals, Varieties, and Algorithms.* New York: Springer.

Eisenbud, D. (2004). *Commutative Algebra with a View Toward Algebraic Geometry.* New York: Springer.

Haase, S. (2007). *Resultanten.*
Von http://www.math.uni-bremen.de/~gamst/SeminarGaloisTheorie.pdf abgerufen