Ausgewählte Kapitel der Algebra/Geometrie: Gröbner-Basen

Rüdiger W. Braun

Sommersemester 2018

Inhaltsverzeichnis

1 Termordnungen

Hauptsächliche Quelle für die Vorlesung ist das Buch [1] von Cox, Little und O'Shea.

1.1 Definition. (a) Ein *Monom* ist ein Ausdruck der Form

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad \alpha \in \mathbb{N}_0^n.$$

Monome werden multipliziert gemäß der Regel

$$x^\alpha \cdot x^\beta = x^{\alpha+\beta}.$$

(b) Ein *Polynom* ist eine endliche Linearkombination von Monomen. Den Ring aller Polynome über einem Körper k bezeichnen wir mit $k[x_1, \ldots, x_n]$.

(c) Es sei $f = \sum_\alpha a_\alpha x^\alpha$ ein Polynom. Der *Totalgrad* von f ist das Maximum der Längen $|\alpha|$ mit $a_\alpha \neq 0$. Man schreibt ihn als $\deg(f)$. Das Nullpolynom hat keinen Grad.

Der Polynomring ist ein kommutativer Ring mit Eins.

1.2 Definition. Ein *Ideal* in $k[x_1, x_2, \ldots, x_n]$ ist eine Teilmenge I mit den folgenden Eigenschaften:

(a) $0 \in I$,

(b) wenn $f, g \in I$, dann auch $f + g \in I$,

(c) wenn $f \in I$ und $h \in k[x_1, \ldots, x_n]$, dann $fh \in I$.

Beispiel: Verschwindungsideal.

1.3 Definition. Sei $M \subset k[x_1, \ldots, x_n]$ eine Menge. Das kleinste Ideal, welches M umfasst, ist das von M *erzeugte Ideal.* Wir schreiben es als $\langle M \rangle$.

1.4 Lemma.

$$\langle f_1, \ldots, f_m \rangle = \left\{ \sum_{j=1}^m h_j f_j \,\middle|\, h_j \in k[x_1, \ldots, x_n] \right\}.$$

1.5 Satz (Division). *Sei* $g \in k[x] \setminus \{0\}$. *Für jedes* $f \in k[x]$ *existieren* $q, r \in k[x]$, *so dass entweder* $r = 0$ *oder* $\deg(r) < \deg(g$ *und* $f = qg + r$.

1.6 Theorem. *Jedes Ideal* $I \subseteq k[x]$ *ist ein Hauptideal.*

Das erste Ziel der Vorlesung ist der Beweis des folgenden Resultats:

1.7 Theorem (Hilbertscher Basissatz). *Sei* $I \subseteq k[x_1, \ldots, x_n]$ *ein Ideal. Dann existieren* $f_1, \ldots, f_m \in I$*, so dass*

$$I = \langle f_1, \ldots, f_m \rangle .$$

Ein solches System $(f_1, \ldots, f_m)$ bezeichnet man gelegentlich als *Basis* von I. Jede endliche Obermenge einer Basis ist wieder eine Basis.

Der Beweis von Theorem 1.6 zeigt die Bedeutung des Begriffs des Leitkoeffizienten. Um ihn verallgemeinern zu können, müssen wir die Monome anordnen.

1.8 Definition. Eine *Termordnung* ist eine Relation $>$ auf $\mathbb{N}_0^n$ mit den folgenden Eingenschaften

(a) $>$ ist eine totale Ordnung.

(b) Wenn $\alpha > \beta$ und $\gamma \in \mathbb{N}_0^n$, dann auch $\alpha + \gamma > \beta + \gamma$.

(c) $>$ ist eine *Wohlordnung,* d. h., dass jede nicht leere Teilmenge von $\mathbb{N}_0^n$ ein kleinstes Element besitzt.

Die Termordnung wird dazu verwendet, die Monome anzuordnen.

1.9 Lemma. *Eine totale Ordnung* $>$ *ist genau dann eine Wohlordnung, wenn es keine unendlich lange absteigende Kette*

$$\alpha(1) > \alpha(2) > \ldots$$

gibt.

1.10 Definition. Seien $\alpha, \beta \in \mathbb{N}_0^n$ verschieden. Wir sagen $\alpha >_{\text{lex}} \beta$, wenn das im Tupel $\alpha - \beta$ am weitesten links stehende, von Null verschiedene Argument positiv ist. Diese Ordnung bezeichnet man als *lexikografische Ordnung.*

Zusammenhang zum Lexikon erklären und Beispiele anschreiben.

1.11 Satz. *Die lexikografische Ordnung ist eine Termordnung.*

Es gilt $x_1 >_{\text{lex}} x_2 >_{\text{lex}} x_3 >_{\text{lex}} \cdots$. Durch Umnumerierung entstehen $n!$ verschiedene lexikografische Ordnungen.

1.12 Definition. Es seien $\alpha, \beta \in \mathbb{N}_0^n$ verschieden. Wir sagen $\alpha >_{\text{grlex}} \beta$, wenn

$$|\alpha| > |\beta| \text{ oder } (|\alpha| = |\beta| \text{ und } \alpha >_{\text{lex}} \beta) .$$

Diese Termordnung heißt *gradiert lexikografische Ordnung.*

1.13 Definition. Es seien $\alpha, \beta \in \mathbb{N}_0^n$ verschieden. Wir sagen $\alpha >_{\text{grevlex}} \beta$, wenn

$|\alpha| > |\beta|$ oder ($|\alpha| = |\beta|$ und der am weitesten rechts stehende, von Null verschiedene Eintrag von $\alpha - \beta$ ist negativ).

Diese Termordnung heißt *gradiert umgekehrte lexikografische Ordnung.*

1.14 Beispiel. $x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \dots$ und $(1,5,2) >_{\text{grevlex}} (4,1,3)$, während $(1,5,2) <_{\text{grlex}} (4,1,3)$. Also entsteht $>_{\text{grevlex}}$ nicht aus $>_{\text{grlex}}$, indem man die Koordinaten umnumeriert.

2 Division in Polynomringen mehrerer Veränderlicher

2.1 Definition. Sei $f = \sum_\alpha a_\alpha x^\alpha$ ein von Null verschiedenes Polynom in $k[x_1, \ldots, x_n]$ und sei $>$ eine Termordnung.

(a) Der *Multigrad* von f ist

$$\text{multideg}(f) = \max\{\alpha \in \mathbb{N}_0^n | a_\alpha \neq 0\}.$$

(b) Der *Leitkoeffizient* von f ist

$$\text{LC}(f) = a_{\text{multideg}(f)}.$$

(c) Das *führende Monom* von f ist

$$\text{LM}(f) = x^{\text{multideg}(f)}.$$

(d) Der *führende Term* von f ist

$$\text{LT}(f) = \text{LC}(f)\,\text{LM}(f).$$

2.2 Lemma. *Seien* $f, g \in k[x_1, \ldots, x_n]$ *nicht das Nullpolynom. Dann gelten*

(a) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.

(b) Falls $f + g \neq 0$, *so gilt* $\text{multideg}(f+g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. *Falls* $\text{multideg}(f) \neq \text{multideg}(g)$, *so gilt sogar die Gleichheit.*

2.3 Theorem (Divisionsalgorithmus). *Es sei* $>$ *eine Termordnung und es sei* $F = (f_1, \ldots, f_s)$ *ein Tupel in* $k[x_1, \ldots, x_n]$. *Für jedes* $f \in k[x_1, \ldots, x_n]$ *existieren* $a_1, \ldots, a_s, r \in k[x_1, \ldots, x_n]$, *so dass*

$$f = \sum_{j=1}^{s} a_j f_j + r$$

und entweder $r = 0$ *oder keines der Monome, aus denen* r *zusammengesetzt ist, ist Vielfaches eines* $\text{LM}(f_j)$.

Für alle j *mit* $a_j f_j \neq 0$ *gilt* $\text{multideg}(a_j f_j) \leq \text{multideg}(f)$.

Data : $f_1, \ldots, f_s, f$
Result : $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0;$
$p := f;$
while $p \neq 0$ **do**
  $i := 1;$
  divisionaufgetreten := **False**;
  while $i \leq s$ **and not** *divisionaufgetreten* **do**
    if $LT(f_i)$ *divides* $LT(p)$ **then**
      $a_i := a_i + LT(p)/LT(f_i);$
      $p := p - (LT(p)/LT(f_i))f_i;$
      divisionaufgetreten := **True**;
    else
      $i := i + 1;$
  if not *divisionaufgetreten* **then**
    $r := r + LT(p);$
    $p := p - LT(p);$

Algorithmus 2.1 : Divisionsalgorithmus

Zum Nachweis wird der Divisionsalgorithmus 2.1 in Pseudocode angegeben.

2.4 Beispiel. Wir verwenden $>_{lex}$ mit $x > y$. Es sei $f = x^2y + xy^2 + y^2$ und $F = (xy - 1, y^2 - 1)$. Wie erhalten

$$x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1.$$

2.5 Beispiel. Wir verwenden wieder $>_{lex}$ mit $x > y$. Wir teilen $f = xy^2 - x$ durch $F = (f_1, f_2)$, wobei $f_1 = xy + 1$ und $f_2 = y^2 - 1$. Man erhält

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y).$$

Teilt man dagegen durch (f_2, f_1), so erhält man

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0.$$

Im Gegensatz zum Fall einer Veränderlichen löst der Divisionsalgorithmus das Problem der Idealmitgliedschaft also nicht.

In der Tat gilt $x + y \in \langle xy + 1, y^2 - 1 \rangle$, denn $x + y = y(xy + 1) - x(y^2 - 1)$. Diese Darstellung nutzt Auslöschungseffekte.

3 Das Lemma von Dickson

3.1 Definition. Ein Ideal im Polynomring heißt *Monomideal,* wenn es von Monomen erzeugt wird.

3.2 Satz. *Zwei Monomideale sind genau dann gleich, wenn sie dieselben Monome enthalten.*

3.3 Lemma. *Es sei* I *ein Monomideal und es sei* $f \in k[x_1, \ldots, x_n]$*. Dann sind äquivalent:*

(a) $f \in I$*.*

(b) Jeder Term von f *liegt in* I*.*

(c) f *ist eine* k*-lineare Kombination von Monomen in* I*.*

3.4 Korollar. *Set* $I = \langle x^\alpha \mid \alpha \in A \rangle$ *ein Monomideal. Ein Monom* x^β *liegt genau dann in* I*, wenn es ein* $\alpha \in A$ *gibt, so dass* x^β *ein Vielfaches von* x^α *ist.*

Diagramm für $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$ hinmalen.

3.5 Theorem (Lemma von Dickson). *Es sei* I *ein Monomideal. Dann besitzt* I *ein endliches Erzeugendensystem, welches aus Monomen besteht.*

3.6 Bemerkung. Wenn $I = \langle x^\alpha \mid \alpha \in A \rangle$, dann existiert ein endliches Erzeugendensystem aus Elementen der Form x^α mit $\alpha \in A$.

3.7 Satz. *Eine Relation* $>$ *auf* $\mathbb{N}_0^n$ *ist genau dann eine Termordnung, wenn sie folgenden Eigenschaften hat.*

(a) $>$ *ist eine totale Ordnung.*

(b) Wenn $\alpha > \beta$ *und* $\gamma \in \mathbb{N}_0^n$*, dann auch* $\alpha + \gamma > \beta + \gamma$*.*

(c) 0 *ist das kleinste Element von* $\mathbb{N}_0^n$*.*

4 Gröbner-Basen

4.1 Definition. Es sei eine Termordnung bestimmt. Für ein Ideal $I \neq \{0\}$ setzen wir

$$LT(I) = \{c\,LT(f) | c \in k^*, f \in I \setminus \{0\}\}.$$

4.2 Bemerkung. Wenn $I = \langle f_1, \ldots, f_s\rangle$ dann gilt $\langle LT(f_1), \ldots, LT(f_s)\rangle \subset \langle LT(I)\rangle$. Die andere Inklusion gilt im allgemeinen nicht. Dies zeigt das Beispiel $I = \langle f_1, f_2\rangle$ mit

$$f_1 = x^3 - 2xy, \quad f_2 = x^2y - 2y^2 + x,$$

versehen mit $>_{grlex}$.

Es gilt nämlich

$$x^2 = x \cdot (x^2 - 2y^2 + x) - y \cdot (x^3 - 2xy).$$

Also $x^2 \in \langle LT(I)\rangle$, während nach Korollar 3.4 alle nicht-trivialen Elemente von $\langle LT(f_1), LT(f_2)\rangle$ mindestens den Grad 3 haben.

4.3 Definition. Es sei $I \subset k[x_1, \ldots, x_n]$ ein Ideal und es sei eine Termordnung $>$ gewählt. Eine *Gröbner-Basis* von I bezüglich $>$ ist eine endliche Teilmenge $\{g_1, \ldots, g_t\}$, so dass $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.

4.4 Satz. *Wenn $\{g_1, \ldots, g_t\}$ eine Gröbner-Basis von I ist, dann ist diese Menge auch eine Basis von I (also ein endliches Erzeugendensystem).*

4.5 Theorem (Hilbertscher Basissatz in der Version von Buchberger). *Jedes Ideal in $k[x_1, \ldots, x_n]$ besitzt eine Basis. Sie kann als Gröbner-Basis gewählt werden.*

Obwohl der Beweis des Lemmas von Dickson konstruktiv ist, haben wir noch keinen Algorithmus zur Bestimmung der Gröbner-Basis.

4.6 Beispiel. Im Polynom $\mathbb{R}[x, y, z]$ betrachten wir das Ideal $I = \langle g_1, g_2\rangle$ mit $g_1 = x + z$ und $g_2 = y - z$. Wir zeigen, dass $\{g_1, g_2\}$ eine Gröbner-Basis von I bezüglich $>_{lex}$ ist.

Es gilt $\langle LT(g_1), LT(g_2)\rangle = \langle x, y\rangle$. Wir müssen also zeigen, dass es kein Polynom $f \in I$ gibt, welches nur von z abhängt. Betrachte $V := \{(-t, t, t) | t \in \mathbb{R}\}$. Sowohl g_1 als auch g_2 verschwinden auf V. Also muss das auch f tun. Aber f ist von der Gestalt $f(x, y, z) = g(z)$. Da f auf V verschwindet, verschwindet g auf $\mathbb{R}$. Also $f = 0$.n

4.7 Theorem (Aufsteigende Kettenbedingung). *Es sei*

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset k[x_1, \ldots, x_n]$$

eine aufsteigende Kette von Idealen in $k[x_1, \ldots, x_n]$. *Dann wird die Kette stationär, d. h. es gibt* $N \in \mathbb{N}$, *so dass* $I_n = I_N$ *für alle* $n \geq N$.

4.8 Satz. *Es sei* I *ein Ideal in* $k[x_1, \ldots, x_n]$ *und es sei* $\{g_1, \ldots, g_s\}$ *eine Gröbner-Basis von* I *bezüglich der Termordnung* $>$. *Zu jedem* $f \in k[x_1, \ldots, x_n]$ *existiert ein eindeutiges* $r \in k[x_1, \ldots, x_n]$ *mit den folgenden Eigenschaften:*

(a) Kein Term von r *ist durch ein* $LT(g_j)$ *teilbar.*

(b) Es gibt $g \in I$ *mit* $f = g + r$.

Insbesondere kommt aus bei der Division durch eine Gröbner-Basis auf die Reihenfolge der Elemente nicht an.

4.9 Definition. Wir schreiben $\overline{f}^F$ für den Rest von f bei Division durch $F = (f_1, \ldots, f_s)$.

4.10 Korollar. *Es sei* G *eine Gröbner-Basis für das Ideal* I. *Dann gilt* $f \in I$ *genau dann, wenn* $\overline{f}^G = 0$.

4.11 Definition. Auf $k[x_1, \ldots, x_n]$ sei eine Termordnung festgelegt. Es seien $f, g \in k[x_1, \ldots, x_n] \setminus \{0\}$.

(a) Falls $\text{multideg}(f) = \alpha$ und $\text{multideg}(g) = \beta$, dann definieren wir γ durch $\gamma_j = \max(\alpha_j, \beta_j)$, $j = 1, \ldots, n$ und bezeichnen x^γ als *kleinstes gemeinsames Vielfaches* von x^α und x^β.

(b) Das *S-Polynom* von f und g ist definiert durch

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

4.12 Beispiel. Seien $f = x^3y^2 - x^2y^3 + x$ und $g = 3x^4y + y^2$ in $\mathbb{R}[x, y]$, versehen mit $>_{\text{grlex}}$. Dann gilt

$$S(f, g) = -x^3y^3 + x^2 - \frac{1}{3}y^3.$$

4.13 Lemma. *Es seien* $f_1, \ldots, f_s$ *Polynome in* $k[x_1, \ldots, x_n]$, *die alle denselben Multigrad* δ *besitzen. Es seien* $c_1, \ldots, c_s \in k$ *so gewählt, dass* $\text{multideg}\left(\sum_{i=1}^s c_i f_i\right) < \delta$. *Dann existieren* $a_{i,j} \in k$, *so dass*

$$\sum_{i=1}^{s} c_i f_i = \sum_{i<j} a_{i,j} S(f_i, f_j).$$

Data : $F = (f_1, \ldots, f_s)$
Result : Gröbner-Basis G von $\langle f_1, \ldots, f_s \rangle$ mit $F \subset G$
$G := F$;
repeat
  $G' := G$;
  for *jedes Paar* (p, q) *in* G' *mit* $p \neq q$ **do**
    $S := \overline{S(p,q)}^{G'}$;
    if $S \neq 0$ **then**
      $G := G' \cup \{S\}$
until $G = G'$;

Algorithmus 4.1 : Algorithmus von Buchberger

Man beachte, dass $\text{multideg}(S(f_i, f_j)) < \delta$.

4.14 Theorem (Kriterium von Buchberger). *Es sei* I *ein Polynomideal und es sei* $G = (g_1, \ldots, g_s)$ *ein Erzeugendensystem von* I. *Dann sind äquivalent*

(a) G *ist eine Gröbner-Basis*

(b) Für alle Paare (i, j) *mit* $i \neq j$ *gilt*

$$\overline{S(g_i, g_j)}^{G} = 0.$$

Da es bei Punkt (a) nicht auf die Reihenfolge ankommt, gilt das auch für Punkt (b).

4.15 Beispiel. Wie in Aufgabe 4 sei $\mathbb{R}[x, y]$ mit $>_{lex}$ versehen und es seien

$$f_1 = xy^2 - x, \quad f_2 = x - y^3.$$

Dann

$$S(f_1, f_2) = \frac{xy^2}{xy^2} f_1 - \frac{xy^2}{x} f_2 = xy^2 - x - xy^2 + y^5 = -x + y^5.$$

Wegen

$$\overline{-x + y^5}^{(f_1, f_2)} = y^5 - y^3$$

ist $G = \{f_1, f_2\}$ keine Gröbner-Basis von $\langle G \rangle$. Wir setzen $G_1 = \{f_1, f_2, f_3\}$ für $f_3 = y^5 - y^3$. Dann gelten

$$S(f_1, f_3) = 0 \text{ und } S(f_2, f_3) = xy^3 - y^8.$$

Wegen

$$\overline{S(f_2, f_3)}^{G_1} = 0$$

ist G_1 eine Gröbner-Basis von $\langle f_1, f_2 \rangle$. Über Redundanzen reden wir später.

4.16 Theorem. *Der Algorithmus 4.1 berechnet eine Gröbner-Basis.*

Damit haben wir das Problem der Idealmitgliedschaft gelöst.

4.17 Definition. Eine Gröbner-Basis heißt *minimal*, wenn

(a) $LC(p) = 1$ für alle $p \in G$.

(b) Für alle $p \in G$ gilt $LT(p) \notin \langle LT(G \setminus \{p\})\rangle$.

4.18 Beispiel. $G = \{x - y^3, y^5 - y^3\}$ ist eine minimale Gröbner-Basis von $I := \langle xy^2 - x, x - y^3\rangle$.

Es ist klar, dass es minimale Gröbner-Basen gibt.

4.19 Satz. *Alle minimalen Gröbner-Basen eines Ideals zur selben Termordnung haben dieselbe Anzahl an Elementen. Genauer gilt:*
Wenn G *und* $\widetilde{G}$ *zwei minimale Gröbner-Basen von* I *zur selben Termordnung sind, dann* $LT(G) = LT(\widetilde{G})$, *wobei* $LT(G) = \{LT(g) | g \in G\}$.

4.20 Definition. Eine Gröbner-Basis G heißt *reduziert,* wenn

(a) $LC(p) = 1$ für alle $p \in G$.

(b) Für jedes $p \in G$ liegt kein Monom von p in $\langle LT(G \setminus \{p\})\rangle$.

4.21 Beispiel. Die Gröbner-Basis G aus Beispiel 4.18 ist reduziert. Ein Beispiel einer nicht reduzierten, minimalen Gröbner-Basis ist $G_1 = \{x - y^5, y^5 - y^3\}$.

4.22 Theorem. *Es sei* $I \neq \{0\}$ *ein Polynomideal. Zu jeder Termordnung existiert eine eindeutig bestimmte reduzierte Gröbner-Basis.*

Damit haben wir eine direkte Lösung des Problems der Idealgleichheit.

4.23 Definition. Auf $k[x_1, \ldots, x_n]$ sei eine Termordnung festgelegt, ferner sei $G = \{g_1, \ldots, g_t\}$ eine Teilmenge des Poylnomrings (nicht notwendig eine Gröbner-Basis). Man sagt, dass $f \in k[x_1, \ldots, x_n]$ *modulo* G *zu* 0 *reduziert* wird, wenn f geschrieben werden kann als

$$f = \sum_{j=1}^{t} a_j g_j,$$

wobei $\text{multideg}(f) \geq \text{multideg}(a_j g_j)$ für alle j mit $a_j g_j \neq 0$. Man schreibt dann

$$f \to_G 0.$$

Es ist klar, dass die Bedingung $\bar{f}^G = 0$ die Reduziertheit modulo G impliziert. Damit kann man das Buchbergersche Kriterium wie folgt aussprechen:

4.24 Theorem. *Es sei* I *ein Polynomideal und es sei* $G = (g_1, \ldots, g_s)$ *ein Erzeugendensystem von* I. *Dann sind äquivalent*

(a) G *ist eine Gröbner-Basis.*

(b) Für alle Paare (i, j) *mit* $i \neq j$ *gilt*

$$S(g_i, g_j) \to_G 0.$$

4.25 Satz. *Der Algorithmus von Buchberger führt auch dann zu einer Gröbner-Basis, wenn Paare* (p, q)*, deren S-Polynom einmal dividiert wurde, nicht mehr berücksichtigt werden.*

5 Symmetrische Polynome

5.1 Definition. Ein Polynom heißt *symmetrisch,* wenn $f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$ für jede Permutation π.

5.2 Definition. Für $j = 1, \ldots, n$ definieren wir $\sigma_j \in k[x_1, \ldots, x_n]$ durch

$$\sigma_j = \sum_{i_1 < \cdots < i_j} x_{i_1} \cdots x_{i_j}.$$

Die σ_j sind die *elementarsymmetrischen Polynome.*

5.3 Theorem. *Jedes symmetrische Polynom lässt sich eindeutig als Polynom in den elementarsymmetrischen Polynomen schreiben.*

5.4 Theorem. *Im Ring* $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ *sei eine Termordnung fixiert, bei der alle Monome, die mindestens ein* x_j *enthalten, größer sind als alle Polynome, die nur aus* y_j *bestehen. Es sei* G *eine Gröbner-Basis des Ideals*

$$I = \langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle,$$

wobei die σ_i *Polynome in den* x_j *sind. Für vorgelegtes* $f \in k[x_1, \ldots, x_n]$ *sei* $g \coloneqq \overline{f}^G$. *Dann gelten*

(a) f *ist genau dann symmetrisch, wenn* $g \in k[y_1, \ldots, y_n]$.

(b) Falls f *symmetrisch ist, dann* $f = g(\sigma_1, \ldots, \sigma_n)$, *wenn* g *als Polynom in den* y_i *verstanden wird.*

In Cox, Little und O'Shea wird die Gröbner-Basis für das Ideal I aus Theorem 5.4 und $>_{lex}$ beschrieben.

5.5 Bezeichnung. Die Funktionen $s_k = \sum_{j=1}^{n} x_j^k$ heißen *Potenzfunktionen.*

5.6 Lemma (Newtonsche Identitäten). *Es gelten*

$$s_\ell + \sum_{j=1}^{\ell-1} (-1)^j \sigma_j s_{\ell-j} + (-1)^\ell \ell \sigma_\ell = 0, \qquad 1 \le \ell \le n,$$

$$s_\ell + \sum_{j=1}^{n} (-1)^j \sigma_j s_{\ell-j} = 0, \qquad \ell > n.$$

Beweis. Als Übung. □

5.7 Satz. *Es sei* k *ein Körper der Charakteristik* 0. *Dann lässt sich jedes symmetrische Polynom in* $k[x_1, \ldots, x_n]$ *als Polynom in den Potenzfunktionen schreiben.*

6 Invariante Polynome

6.1 Definition. Eine *endliche Matrixgruppe* H ist eine endliche Untergruppe einer $GL_n(k)$.

6.2 Beispiel. Es sei $\tau \in S_n$ eine Permutation von $\{1, \ldots, n\}$. Wir definieren eine lineare Abbildung $k^n \to k^n$ durch

$$(x_1, \ldots, x_n) \mapsto \left(x_{\tau(1)}, \ldots, x_{\tau(n)}\right).$$

Die zugehörige Matrix bezüglich der Standardbasis bezeichnen wir mit M_τ. Dann ist $\{M_\tau | \tau \in S_n\}$ eine endliche Matrixgruppe, die zur symmetrischen Gruppe S_n isomorph ist. Da jede endliche Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe ist, ist auch jede endliche Gruppe isomorph zu einer endlichen Matrixgruppe.

6.3 Bezeichnung. Es sei $H \leq GL_n(k)$ eine endliche Matrixgruppe. Sie operiert wie folgt auf $k[x_1, \ldots, x_n]$

$$M.f(x) = f(Mx), \quad M \in H, f \in k[x_1, \ldots, x_n].$$

6.4 Beispiel.

$$A := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$$

und $f = x^2 + xy + y^2$. Dann $A.f = \frac{3}{2}x^2 + \frac{1}{2}y^2$.

6.5 Definition. Ein Polynom $f \in k[x_1, \ldots, x_n]$ ist *invariant* unter H, wenn $M.f = f$ für alle $M \in H$.

Die Menge aller unter H invarianten Polynome wird mit $k[x_1, \ldots, x_n]^H$ bezeichnet.

6.6 Beispiel. Durch Koeffizientenvergleich sehen wir, dass ein homogenes Polynom f vom Grad 2 genau dann invariant unter A (also unter der von A erzeugten Untergruppe von $GL_2(\mathbb{R})$) ist, wenn f ein Vielfaches von $x^2 + y^2$ ist.

6.7 Lemma. *(a)* $k[x_1, \ldots, x_n]^H$ *ist ein Unterring von* $k[x_1, \ldots, x_n]$ *mit derselben Eins.*

(b) Ein Polynom gehört genau dann zu $k[x_1, \ldots, x_n]^H$*, wenn dies für alle seine homogenen Komponenten gilt.*

6.8 Bezeichnung. Seien $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. Dann setzen wir

$$k[f_1, \ldots, f_m] = \{g(f_1, \ldots, f_m) | g \in k[x_1, \ldots, x_m]\}.$$

$k[f_1, \ldots, f_m]$ ist die von $f_1, \ldots, f_m$ *erzeugte Ringerweiterung* von k.

6.9 Definition. Seien $H \subset GL_n(k)$ eine endliche Matrixgruppe und k ein Körper, dessen Charakteristik $|H|$ nicht teilt. Der *Reynolds-Operator* ist definiert durch

$$R_H \colon k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n],$$
$$R_H(f) = \frac{1}{|H|} \sum_{A \in H} A.f$$

6.10 Satz. *Seien $H \subset GL_n(k)$ eine endliche Matrixgruppe und k ein Körper, dessen Charakteristik $|H|$ nicht teilt. Der Reynolds-Operator R_H ist eine k-lineare Projektion auf $k[x_1, \ldots, x_n]^H$.*

Ferner gilt $R_H(fg) = fR_H(g)$, falls $f \in k[x_1, \ldots, x_n]^H$.

6.11 Beispiel. Für $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ ist $\langle A \rangle = C_4$ die zyklische Gruppe der Ordnung 4. Es gilt

$$R_{C_4}(f)(x, y) = \frac{1}{4}\left(f(x, y) + f(-y, x) + f(-x, -y) + f(y, -x)\right).$$

Damit erhalten wir

$$R_{C_4}(x^2) = \frac{1}{2}(x^2 + y^2),$$
$$R_{C_4}(xy) = 0,$$
$$R_{C_4}(x^3y) = \frac{1}{2}(x^3y - xy^3),$$
$$R_{C_4}(x^2y^2) = x^2y^2.$$

6.12 Theorem (E. Noether). *Es seien $H \leq GL_n(k)$ eine endliche Matrixgruppe und k ein Körper der Charakteristik 0. Dann gilt*

$$k[x_1, \ldots, x_n]^H = k\left[R_H(x^\beta) \middle| |\beta| \leq |H|\right].$$

Der folgende Satz löst das Problem der Unterringmitgliedschaft. Wir haben ihn im Prinzip schon verwendet.

6.13 Satz. *Es sei k ein Körper und es seien $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. Es sei G eine Gröbner-Basis von $I := \langle f_1 - y_1, \ldots, f_m - y_m \rangle \subseteq k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ bezüglich einer Termordnung, bei der alle Monome, die ein x enthalten, größer sind als alle Monome, die das nicht tun. Für $f \in k[x_1, \ldots, x_n]$ sei $g = \overline{f}^G$. Dann liegt f genau dann in $k[f_1, \ldots, f_m]$, wenn g nur von y abhängt. In diesem Fall gilt $f = g(f_1, \ldots, f_m)$.*

In dem Buch von Sturmfels [2] wird ein Algorithmus vorgestellt, der in den meisten Fällen effizienter ist.

6.14 Definition. (a) Ein Polynom ist *homogen* vom Grad ℓ, wenn alle seine Terme den Totalgrad ℓ haben.

(b) Jedes Polynom kann geschrieben werden als $f = \sum f_\ell$, wobei f_ℓ homogen vom Grad ℓ ist. Man bezeichnet dann f_ℓ als die ℓ-te *homogene Komponente.*

(c) Ein Ideal ist *homogen,* wenn es von homogenen Polynomen erzeugt wird.

(d) Eine Termordnung $<$ *respektiert den Totalgrad,* wenn aus $|\alpha| < |\beta|$ bereits $\alpha < \beta$ folgt.

6.15 Satz. *Es sei* I *ein homogenes Ideal. Ein Polynom* f *liegt genau dann in* I*, wenn dies für alle seine homogenen Komponenten gilt.*

6.16 Satz. *Es sei* I *ein homogenes Ideal, es sei* $>$ *eine Termordnung, welche den Totalgrad respektiert, und es sei* G *die reduzierte Gröbner-Basis von* I *bezüglich* $>$*. Dann sind alle Elemente von* G *homogen.*

6.17 Satz. *Es sei* $H \leq GL_n(k)$ *eine endliche Matrixgruppe und es sei* k *ein Körper, dessen Charakteristik kein Teiler von* $|H|$ *ist. Es sei* I *das von den nicht-konstanten, homogenen Invarianten erzeugte Ideal in* $k[x_1, \ldots, x_n]$*. Wenn* $I = \langle g_1, \ldots, g_t \rangle$ *für homogene* g_j*, dann gilt auch*

$$I = \langle R_H(g_1), \ldots, R_H(g_t) \rangle .$$

6.18 Theorem (Hilbert). *Es sei* $H \leq GL_n(k)$ *eine endliche Matrixgruppe über einem Körper* k*, dessen Charakteristik die Gruppenordnung* $|H|$ *nicht teilt. Es sei* I *das von den nicht-konstanten, homogenen Invarianten erzeugte Ideal in* $k[x_1, \ldots, x_n]$*. Wenn*

$$I = \langle f_1, \ldots, f_m \rangle$$

für homogene Invarianten $f_1, \ldots, f_m$*, dann*

$$k[x_1, \ldots, x_n]^H = k[f_1, \ldots, f_m].$$

7 Eliminationstheorie

Eliminate, eliminate, eliminate!
Eliminate the eliminators of Elimination theory!

S. A. Abhyankar

7.1 Definition. Es sei $I \subseteq k[x_1, \ldots, x_n]$ ein Ideal und es sei $\ell \in \{1, \ldots, n-1\}$. Das ℓ-te *Eliminationsideal* I_ℓ ist das durch

$$I_\ell := I \cap k[x_{\ell+1}, \ldots, x_n]$$

definierte Ideal in $k[x_{\ell+1}, \ldots, x_n]$.

7.2 Theorem (Eliminationssatz). *Es sei $I \subseteq k[x_1, \ldots, x_n]$ ein Ideal und es sei G eine Gröbner-Basis von I bezüglich $>_{lex}$ mit $x_1 > x_2 > \cdots > x_n$. Für $1 \leq \ell \leq n-1$ ist*

$$G_\ell := G \cap k[x_{\ell+1}, \ldots, x_n]$$

eine Gröbner-Basis des ℓ-ten Eliminationsideals.

7.3 Beispiel. Wir untersuchen das Ideal

$$I = \left\langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \right\rangle.$$

Bezüglich $>_{lex}$ besitzt es die Gröbner-Basis $\{g_1, g_2, g_3, g_4\}$ mit

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

Es gilt $g_4 = z^2(z-1)^2(z^2+2z-1)$. Wir untersuchen die vier Nullstellen getrennt:

$z = 0$: Dann $g_3(y, 0) = 0$, $g_2(y, 0) = y^2 - y$. Falls $y = 0$, so erhalten wir $x = 1$ und im Fall $y = 1$ erhalten wir $x = 0$.

$z = 1$: Dann $g_3(y, 0) = 2y$ und $g_2(y, 0) = y^2 - y$. Also $y = 0$ und $x = 0$.

$z = -1+\sqrt{2}$: Dann $g_3(y, -1+\sqrt{2}) = (6-4\sqrt{2})y + 14 - 10\sqrt{2}$ und $g_2(y, -1+\sqrt{2}) = y^2 - y - 4 + 3\sqrt{2}$. In der Tat ist $-1+\sqrt{2}$ eine Nullstelle davon. Damit bekommt man dann auch $x = -1+\sqrt{2}$.

Für $V \coloneqq \left\{(x,y,z) \in \mathbb{C}^3 \middle| \forall f \in I : f(x,y,z) = 0\right\}$ gilt also

$$V = \{(0,0,1),(0,1,0),(1,0,0),(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}),\\ (-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2})\}.$$

7.4 Definition. Für ein Ideal $I \subseteq k[x_1,\ldots,x_n]$ setzen wir

$$V((I) \coloneqq \{x \in k^n | f(x) = 0 \text{ für alle } f \in I\}.$$

V ist eine *affine Varietät.*

7.5 Bezeichnung. Für $0 \leq k < n$ bezeichnet $\pi_k \colon k^n \to k^{n-k}$ die Projektion

$$(x_1,\ldots,x_n) \mapsto (x_{k+1},\ldots,x_n).$$

7.6 Beispiel. Betrachte $I = \langle xy-1, xz-1\rangle$. Eine Gröbner-Basis zu $>_{lex}$ ist $G = \{f_1,f_2\}$ mit

$$f_1 = xz-1,$$
$$f_2 = y-z.$$

Dann gelten

$$I_1 = \langle y-z\rangle \quad \text{und} \quad I_2 = \langle 0\rangle.$$

Entsprechend

$$V(I) = \left\{\left(\frac{1}{c},c,c\right)\middle| c \in k\setminus\{0\}\right\}, \quad V(I_1) = \{(c,c)|c \in k\} \quad \text{und} \quad V(I_2) = k.$$

Man beachte, dass $\pi_1(V(I)) \neq V(I_1)$.

Das im letzten Beispiel auftretende Problem kann man auf zwei Weisen behandeln. Einerseits kann man zu $V(I)$ unendlich ferne Punkte hinzufügen, andererseits kann man algorithmisch bestimmen, welche Punkte ausgelassen werden.

7.7 Theorem (Ausdehnungssatz). *Sei* k *ein algebraisch abgeschlossener Körper und sei* $I = \langle f_1,\ldots,f_s\rangle$ *ein Ideal in* $k[x_1,\ldots,x_n]$. *Mit* I_1 *werde das erste Eliminationsideal von* I *bezeichnet. Für* $1 \leq i \leq s$ *schreiben wir* f_i *in der Form*

$$f_i = g_i(x_2,\ldots,x_n)x_1^{N_i} + b_i,$$

wobei $N_i \in \mathbb{N}_0$, $g_i \in k[x_2,\ldots,x_n]$ *nicht das Nullpolynom ist und* $b_i \in k[x_1,\ldots,x_n]$ *in* x_1 *einen kleineren Grad als* N_i *besitzt.*

Ist nun $(a_2,\ldots,a_n) \in V(I_1)$ *mit* $g_i(a_2,\ldots,a_n) \neq 0$ *für mindestens ein* i, *dann existiert* a_1, *so dass* $(a_1,\ldots,a_n) \in V(I)$.

Wir werden diesen Satz später beweisen, nachdem wir den Begriff der Resultanten eingeführt haben.

7.8 Bezeichnung. In der Situation des Ausdehnungssatzes sagen wir, dass die *Partiallösung* $(a_2, \dots, a_n)$ die *Ausdehnung* $(a_1, \dots, a_n)$ besitzt.

7.9 Beispiel. In Beispiel 7.6 ist $g_1 = z$. Also besitzt $(c, c) \in V(I_1)$ eine Ausdehnung, falls $c \neq 0$. Wenn wir stattdessen $f_2 = xy - 1$ setzen, erhalten wir dieselbe Bedingung.

7.10 Korollar. *Sei* k *ein algebraisch abgeschlossener Körper und sei* $I = \langle f_1, \dots, f_n \rangle$ *ein Ideal in* $k[x_1, \dots, x_n]$. *Falls für* $1 \leq i \leq s$ *das Poylnom* f_i *geschrieben werden kann als*

$$f_i = x_1^{N_i} + b_i, \tag{7.1}$$

wobei der Grad von b_i *in* x_1 *kleiner als* N_i *ist, dann besitzt jede Partiallösung* $(a_2, \dots, a_n) \in V(I_1)$ *eine Ausdehnung.*

Ein Polynom wie in (7.1) heißt *Weierstraß-Polynom.*

7.11 Beispiel. Es sei $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$. Eine Gröbner-Basis bezüglich $>_{lex}$ ist $G = \{f_1, f_2\}$ mit

$$\begin{aligned} f_1 &= x + y^3 z + y z^3 - yz, \\ f_2 &= y^4 z^2 + y^2 z^4 - y^2 z^2 + 1. \end{aligned}$$

Also $I_1 = \langle f_2 \rangle$ und $I_2 = \{0\}$. Also ist jedes $c \in k$ eine Partiallösung in $V(I_2)$. Um zu prüfen, ob sie eine Ausdehnung nach $V(I_1)$ hat, schreiben wir f_2 wie im Ausdehnungssatz. Dann ist $g = z^4$. Daher besitzt jedes $c \neq 0$ eine Ausdehnung $(b, c) in V(I_1)$. Wegen des Korollars besitzt jedes $(b, c) \in V(I_1)$ eine Ausdehnung nach $V(I)$.

7.12 Beispiel. Betrachte $I = \langle xy - 4, x^3 - y^2 - 1 \rangle \subset \mathbb{C}[x, y]$. Eine Gröbner-Basis bezüglich $>_{lex}$ ist gegeben durch

$$\begin{aligned} f_1 &= 16x - y^2 - y^4, \\ f_2 &= y^5 + y^3 - 64. \end{aligned}$$

Reduktion modulo 5 zeigt, dass f_2 irreduzibel ist. (`sagemath` bestimmt die Galoisgruppe als S_5.) Wenn c eine der fünf Wurzeln von f_2 ist, dann läßt sich diese Partiallösung ausdehnen zu $\left(\frac{4}{c}, c\right)$.

7.13 Lemma. *Es sei* I_ℓ *das* ℓ*-te Eliminationsideal. Dann gilt* $\pi_\ell(V) \subset V(I_\ell)$.

7.14 Theorem. *Es sei* k *ein algebraisch abgeschlossener Körper und es sei* $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$ *ein Ideal. Ferner sei* $f_i = g_i x_1^{N_i} + b_i$ *wie im Ausdehnungssatz. Dann gilt*

$$V(I_1) = \pi_1(V) \cup \big(V(g_1, \dots, g_s) \cap V(I_1)\big).$$

7.15 Beispiel. Es seien

$$f_1 = (y - z)x^2 + xy - 1,$$
$$f_2 = (y - z)x^2 + xz - 1.$$

Dann $I = \langle xy - 1, xz - 1\rangle$. Dieses Beispiel hatte wir bereits betrachtet. Es gilt

$$V(I_1) = \{(c, c) | c \in k\}.$$

Wegen $g_1 = g_2 = y - z$ gilt in diesem Fall $V(g_1, g_2) = V(I_1)$.

8 Resultanten

8.1 Satz (Euklidischer Algorithmus). *Es sei* R *ein euklidischer Ring. Für zwei Elemente* $x, y \in R \setminus \{0\}$ *definiert man rekursiv* $z_0, z_1, \dots \in R$ *durch*

$$z_0 = x$$
$$z_1 = y$$
$$z_{i+1} = \begin{cases} \text{Rest von } z_{i-1} \text{ bei Division durch } z_i, & \text{wenn } z_i \neq 0, \\ 0, & \text{sonst.} \end{cases}$$

Dann gibt es ein n *mit* $z_{n+1} = 0$. *Falls* n *der kleinste Index mit dieser Eigenschaft ist, so gilt* $z_n = \mathrm{ggT}(x, y)$. *Für jedes* i *existieren* $a_i, b_i \in R$ *mit* $z_i = a_i x + b_i y$.

8.2 Lemma. *Es seien seien* $f, g \in k[x]$ *Polynome von den Graden* $\ell > 0$ *und* $m > 0$. *Dann haben* f *und* g *genau dann einen gemeinsamen Teiler, wenn es* $A, B \in k[x]$ *gibt, so dass*

(a) Mindestens eins der beiden Polynome A *und* B *ist nicht das Nullpolynom.*

(b) A *hat höchstens den Grad* $m - 1$ *und* B *hat höchstens den Grad* $\ell - 1$.

(c) $Af + Bg = 0$.

8.3 Definition. Es seien $f, g \in k[x]$ nicht-konstante Polynome, geschrieben als

$$f = a_0 x^\ell + a_1 x^{\ell-1} + \cdots + a_\ell, \qquad a_0 \neq 0,$$
$$g = b_0 x^m + b_1 x^{m-1} + \cdots + b_m, \qquad b_0 \neq 0.$$

Dann definieren wir die *Sylvester-Matrix* von f und g bezüglich x als

$$\mathrm{Syl}(f, g, x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_\ell & & & & b_m & & & \\ & a_\ell & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_\ell & & & & b_m \end{pmatrix} \in k^{(m+\ell)\times(m+\ell)}.$$

Die *Resultante* von f und g bezüglich x ist definiert als

$$\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x)).$$

8.4 Lemma. $\mathrm{Res}(f, g, x))$ *ist ein Polynom in den Koeffizienten von* f *und* g*, dessen Koeffizienten ganze Zahlen sind.*

8.5 Satz. *Es seien* $f, g \in k[x]$ *nicht-konstante Polynome. Sie besitzen genau dann einen gemeinsamen Teiler in* $k[x]$*, wenn* $\mathrm{Res}(f, g, x) = 0$*.*

8.6 Beispiel. $\mathrm{Res}(x^4 + 3x^2 + 2, x^3 + 4x^2 + x + 4, x) = 0$.

8.7 Satz. *Sei* k *ein Körper und seien* $f, g \in k[x_1, \ldots, x_n]$ *nicht-konstante Polynome. Dann gibt es* $A, B \in k[x_1, \ldots, x_n]$*, so dass* $Af+Bg = \mathrm{Res}(f, g, x_1)$*. Die Koeffizienten von* A *und* B *sind ganzzahlige Polynome in den Koeffizienten von* f *und* g*.*

In den Anwendungen liegen f und g in $k[y][x]$. Dann wird der Satz auf den Körper $k(y)$ angewandt. Die Zusatzaussage zeigt dann, dass $A, B \in k[y][x]$.

Eine von 0 verschiedene Nichteinheit p in einem Integritätsring heißt *irreduzibel,* wenn aus $p = xy$ folgt, dass eines der beiden Elemente eine Einheit ist. Es heißt *prim,* wenn aus $p|xy$ bereits $p|x$ oder $p|y$ folgt. In einem faktoriellen Ring sind die irreduzibeln Elemente genau die Primelemente. Nach dem Satz von Gauß ist der Polynomring $k[x_1, \ldots, x_n]$ faktoriell.

8.8 Lemma. *Seien* $f, g \in k[x_1, \ldots, x_n]$ *Polynome mit positivem Grad in* x_1*. Dann haben* f *und* g *genau dann einen gemeinsamen Faktor in* $k[x_1, \ldots, x_n]$ *mit positivem Grad in* x_1*, wenn sie in* $k(x_2, \ldots, x_n)[x_1]$ *einen gemeinsamen Faktor haben.*

8.9 Satz. *Seien* $f, g \in k[x_1, \ldots, x_n]$ *mit positivem Grad in* x_1*.*

(a) $\mathrm{Res}(f, g, x_1)$ *liegt in dem Eliminationsideal* $\langle f, g\rangle \cap k[x_2, \ldots, x_n]$*.*

(b) $\mathrm{Res}(f, g, x_1)$ *verschwindet genau dann, wenn* f *und* g *in* $k[x_1, \ldots, x_n]$ *einen gemeinsamen Faktor mit positivem Grad in* x_1 *haben.*

8.10 Satz. *Es sei* k *ein algebraisch abgeschlossener Körper und es seien* $f, g \in k[x_1, \ldots, x_n]$*. Wir schreiben sie als*

$$\begin{aligned} f &= a_0 x_1^{\ell} + \cdots + a_{\ell}, \quad a_0 \neq 0, \\ g &= b_0 x_1^{m} + \cdots + b_m, \quad b_0 \neq 0. \end{aligned} \tag{8.1}$$

Falls $\mathrm{Res}(f, g, x_1)$ *in* $(c_2, \ldots, c_n) \in k^{n-1}$ *verschwindet, so gilt*

(a) $a_0(c_2, \ldots, c_n) = 0$ *oder* $b_0(c_2, \ldots, c_n) = 0$

oder

(a) es gibt $c_1 \in k$*, so dass* f *und* g *in* $(c_1, c_2, \ldots, c_n)$ *verschwinden.*

8.11 Satz. *Es sei* k *ein algebraisch abgeschlossener Körper, es seien* $f, g \in k[x_1, \ldots, x_n]$ *Polynome von den jeweiligen Graden* ℓ *und* m *in* x_1 *und es sei* $c = (c_2, \ldots, c_n) \in k^{n-1}$ *derart, dass:*

(a) Das Polynom $f(x_1, c) \in k[x_1]$ *hat den Grad* ℓ*.*

(b) Das Polynom $g(x_1, c) \in k[x_1]$ *hat den Grad* $p \leq m$*.*

Dann gilt für das Polynom $h \coloneqq \operatorname{Res}(f, g, x_1) \in k[x_2, \ldots, x_n]$ *und* a_0 *wie in* (8.1)

$$h(c) = a_0(c)^{m-p} \operatorname{Res}(f(x_1, c), g(x_1, c), x_1).$$

Damit kann man nun den Ausdehnungssatz beweisen.

9 Projektive Varietäten

9.1 Definition. Es sei k ein Körper. Der *affine Raum* der Dimension n ist der k^n. Der *projektive Raum* der Dimension n ist definoert als

$$\mathbb{P}^n(k) = \left(k^{n+1} \setminus \{0\}\right) / \sim,$$

wobei $x \sim y$ genau dann, wenn es $\lambda \in k$ gibt, so dass $x = \lambda y$.

Wir schreiben die Elemente von $\mathbb{P}^n(k)$ als $p = [x_0 : x_1 : \cdots : x_n]$ und bezeichnen $(x_0, \ldots, x_n)$ als homogene Koordinaten von p.

Die Relation $\sim$ ist offenbar eine Äquivalenzrelation.

9.2 Bemerkung. Die folgenden Abbildungen sind offenbar injektiv

$$\begin{aligned}
&\varphi_0 \colon k^n \to \mathbb{P}^n(k), && (x_1, \ldots, x_n) \mapsto [1 : x_1 : x_2 : \cdots : x_n],\\
&\varphi_1 \colon k^n \to \mathbb{P}^n(k), && (x_1, \ldots, x_n) \mapsto [x_1 : 1 : x_2 : \cdots : x_n],\\
&\ldots\\
&\varphi_n \colon k^n \to \mathbb{P}^n(k), && (x_1, \ldots, x_n) \mapsto [x_1 : x_2 : \cdots : x_n : 1].
\end{aligned}$$

Üblicherweise bettet man den affinen Raum durch die Abbildung φ_0 in den projektiven Raum ein. Die Punkte

$$\mathbb{P}^n(k) \setminus \varphi_0(k^n) = \{[0 : x_1 : \cdots : x_n] | (x_1, \ldots, x_n) \in k^n \setminus \{0\}\}$$

sind die *unendlich fernen Punkte* des $\mathbb{P}^n(k)$.

Jeder Punkt $p \in \mathbb{P}^1(k)$ liegt im Bild mindestens eines φ_j. In der Sprache der Mannigfaltigkeiten sind die φ_j lokale Parametrisierungen des $\mathbb{P}^n(k)$.

9.3 Beispiel. $\mathbb{P}^1(\mathbb{C})$ ist die aus der Funktionentheorie bekannte Riemannsche Zahlensphäre. Sie besitzt genau einen unendlich fernen Punkt, nämlich $[0 : 1]$.

9.4 Definition. Für homogene Polynome $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ bezeichnen wir

$$V(f_1, \ldots, f_s) \coloneqq \{[x_0 : \cdots : x_n] | f_j(x_0, \ldots, x_n) = 0, j = 1, \ldots, s\}$$

als die durch $f_1, \ldots, f_S$ definierte *projektive Varietät.*

9.5 Beispiel. In $\mathbb{P}^3(\mathbb{C})$ sei $V = V(f_1, f_2)$, wobei

$$f_1 = x_1^2 - x_2 x_0, \quad f_2 = x_1^3 - x_3 x_0^2.$$

Wir identifizieren $\mathbb{C}^3$ wieder mit $\{[1 : x_1 : x_2 : x_3] | (x_1, x_2, x_3) \in \mathbb{C}^4\}$. Dann liegt $[1 : x_1 : x_2 : x_3]$ genau dann in V, wenn $x_1^2 - x_2 = 0$ und $x_1^3 - x_3 = 0$.

Die Gleichung, welche die unendlich ferne Ebene im $\mathbb{P}^3(\mathbb{C})$ beschreibt, ist $g(x_0, \ldots, x_3) := x_0 = 0$. Es gibt aber keinen Grund zu der Annahme, dass etwa $W := V(f_1, f_2, g)$ die Menge der unendlich fernen Punkte von V beschreibt. In der Tat gilt nämlich $W = \{[0 : 0 : x_2 : x_3] | (x_2, x_3) \in \mathbb{C}^2 \setminus \{0\}\}$, was uns anschaulich nicht überzeugt.

9.6 Definition. Es sei $V \subset k^n$ eine affine Varietät. Die kleinste projektive Varietät, welche $\{[1 : x_1 : \cdots : x_n] | (x_1, \ldots, x_n) \in V\}$ umfasst, ist der *projektive Abschluss* von V.

Im folgenden schreiben wir das Tupel der Unbestimmten $(x_0, x_1, \ldots, x_n)$ als (x_0, x).

9.7 Definition. Es sei $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ ein Polynom vom Totalgrad ℓ. Dann bezeichnet man

$$f^h := \sum_\alpha a_\alpha x^\alpha x_0^{\ell - |\alpha|} \in k[x_0, \ldots, x_n]$$

als *Homogenisierung* von f.

Umgekehrt bezeichnet man für homogenes $F \in k[x_0, \ldots, x_n]$ das Polynom $F(1, x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ als *Dehomogenisierung* von F.

9.8 Satz. *Die Homogenisierung f^h von f ist homogen. Sie hat denselben Totalgrad wie f.*

Dehomogenisiert man die Homogenisierung von f, so erhält man f zurück. Homogenisiert man die Dehomogenisierung eines homogenen Polynoms $F \in k[x_0, \ldots, x_n]$, so erhält man ein Polynom der Form $x_0^{-d}F$, wobei $d \geq 0$.

9.9 Lemma.

$$f^h = x_0^\ell f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right),$$

wobei ℓ den Grad von f bezeichnet.

9.10 Definition. Wenn I ein Ideal in $k[x_1, \ldots, x_n]$ ist, dann ist die *Homogenisierung* von I gleich dem homogenen Ideal

$$I^h = \langle f^h | f \in I \rangle \subset k[x_0, x_1, \ldots, x_n].$$

Wir schreiben die Monome von $k[x_0, x_1, \ldots, x_n]$ wieder als $x^\alpha x_0^d$, wobei $\alpha \in \mathbb{N}_0^n$.

9.11 Definition. Es sei $>$ eine Termordnung auf $k[x_1, \ldots, x_n]$, welche den Totalgrad respektiert. Wir definieren die Termordnung $>_h$ dadurch, dass $x^\alpha x_0^d >_h x^\beta x_0^e$ genau dann, wenn $x^\alpha > x^\beta$ oder $\alpha = \beta$ und $d > e$.

9.12 Lemma. *Es sei $>$ eine Termordnung, welche den Totalgrad respektiert und es sei $f \in k[x_1, \ldots, x_n]$. Dann gilt*

$$LM_{>_h}(f^h) = LM_>(f).$$

9.13 Theorem. *Es sei* I *ein Ideal in* $k[x_1, \ldots, x_n]$ *und es sei* $>$ *eine Termordnung, welche den Totalgrad respektiert. Ist nun* G *eine Gröbnerbasis von* I *bezüglich* $>$*, so ist* $G^h := \{g^h | g \in G\}$ *eine Gröbnerbasis von* I^h *bezüglich* $>_h$.

9.14 Beispiel. Sei $I = \langle x_2 - x_1^2, x_3 - x_1^2 \rangle$ das bereits früher betrachtete Ideal in $\mathbb{C}[x_1, x_2, x_3]$. Eine Gröbnerbasis bezüglich $>_{\text{grevlex}}$ ist

$$G = \{x_1^2 - x_2, x_1x_2 - x_3, x_1x_3 - x_2^2\}.$$

Daher

$$I^h = \langle x_1^2 - x_0x_2, x_1x_2 - x_0x_3, x_1x_3 - x_2^2 \rangle .$$

Die unendlich fernen Punkte in $V(I^h)$ sind dann die Lösungen von

$$x_1^2 = 0, x_1x_2 = 0, x_1x_2 - x_2^2 = 0.$$

$V(I^h)$ besitzt nur einen unendlich fernen Punkt, nämlich $[0 : 0 : 0 : 1]$.

Zum Verständnis dieses Beispiels wird der Nullstellensatz benötigt.

10 Der Nullstellensatz

10.1 Theorem (Schwacher Nullstellensatz). *Es sei* k *ein algebraisch abgeschlossener Körper und es sei* $I \subset k[x_1, \ldots, x_n]$ *ein Ideal, für welches* $V(I) = \emptyset$ *gilt. Dann* $I = k[x_1, \ldots, x_n]$.

10.2 Definition. Für eine Teilmenge $V \subset k^n$ bezeichnen wir mit

$$I(V) \coloneqq \{f \in k[x_1, \ldots, x_n] | f(x) = 0 \text{ für alle } x \in V\}$$

das *Verschwindungsideal* von V.

10.3 Theorem (Hilbertscher Nullstellensatz). *Sei* k *ein algebraisch abgeschlossener Körper und seien* $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, *so dass* $f \in I(V(f_1, \ldots, f_s))$. *Dann existiert* $m \in \mathbb{N}$, *so dass*

$$f^m \in \langle f_1, \ldots, f_s \rangle .$$

10.4 Definition. Es sei k ein Körper und $I \subset k[x_1, \ldots, x_n]$ ein Ideal. Das *Radikal* von I ist definiert als

$$\sqrt{I} \coloneqq \{f | \exists m : f^m \in I\} .$$

10.5 Lemma. $\sqrt{I}$ *ist ein Ideal.*

10.6 Theorem (Nullstellensatz). *Sei* k *ein algebraisch abgeschlossener Körper und sei* $I \subset k[x_1, \ldots, x_n]$ *ein Ideal. Dann gilt*

$$I(V(I)) = \sqrt{I}.$$

Die Gleichung $V = V(I(V))$ ist dagegen trivial.

10.7 Definition. Eine Varietät (affin oder projektiv) heißt *irreduzibel*, wenn folgendes gilt:

Wenn $V = U \cup W$ mit Varietäten U und W, dann $V = U$ oder $V = W$.

10.8 Theorem. *Es sei* k *ein Körper mit unendlich vielen Elementen.*

(a) Wenn

$$V_1 \supset V_2 \supset \ldots$$

eine absteigende Kette von projektiven Varietäten im $\mathbb{P}^n(k)$ *ist, so gibt es ein* N *mit* $V_N = V_m$ *für alle* $m \geq N$.

(b) Jede projektive Varietät V *im* $\mathbb{P}^n(k)$ *kann als endliche Vereinigung*

$$V = V_1 \cup \cdots \cup V_m$$

irreduzibler projektiver Varietäten geschrieben werden. Verlangt man $V_i \not\subset V_j$ *für* $i \neq j$*, so sind die* V_i *eindeutig bis auf die Reihenfolge.*

10.9 Definition. Die V_i bezeichnet man als die *irreduziblen Komponenten* von V.

10.10 Satz. *Sei* k *ein Körper und sei* $V \subset k^n$ *eine affine Varietät und sei* $W \subset \mathbb{P}^n(k)$ *der projektive Abschluss von* V*. Dann gelten*

(a) $W \cap k^n = V$.

(b) Wenn V *irreduzibel ist, dann auch* W.

(c) Keine irreduzible Komponente von W *besteht nur aus unendlich fernen Punkten.*

In Zukunft unterscheiden wir affine Verschwindungsideale bzw. Varietäten von ihren projektiven Gegenstücken, indem wir den Index a anbringen.

10.11 Theorem. *Es sei* k *ein algebraisch abgeschlossener Körper und es sei* $I \subset k[x_1, \ldots, x_n]$ *ein Ideal. Dann ist* $V(I^h) \subset \mathbb{P}^n(k)$ *der projektive Abschluss von* $V_a(I) \subset k^n$.

10.12 Theorem (Schwacher projektiver Nullstellensatz). *Es sei* k *ein algebraisch abgeschlossener Körper und es sei* $I \subset k[x_0, \ldots, x_n]$ *ein homogenes Ideal. Dann sind äquivalent:*

(a) $V(I) \subset \mathbb{P}^n(k)$ *ist leer.*

(b) Wenn G *eine reduzierte Gröbnerbasis vom* I *ist, dann gibt es für jedes* $i \in \{0, \ldots, n\}$ *ein* $g \in G$*, so dass* $\mathrm{LT}(g)$ *eine Potenz von* x_i *ist.*

(c) Es gibt $r \in \mathbb{N}$*, so dass* $\langle x_0, \ldots, x_n \rangle^r \subset I$.

Bemerkung. Das Ideal $\langle x_0, \ldots, x_n \rangle$ bezeichnet man als das *irrelevante Ideal.*

11 Projektive Eliminationstheorie

Wir schreiben die Elemente von $\mathbb{P}^n(k) \times k^n$ in der Form $(x_0 : x_1, \ldots, x_n; y_1, \ldots, y_n)$.

11.1 Definition. (a) Ein $F \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$ heißt homogen in x, wenn es $\ell \in \mathbb{N}_0$ und $h_\alpha \in k[y_1, \ldots, y_m]$ gibt, so dass

$$F = \sum_{|\alpha|=\ell} h_\alpha(y_1, \ldots, y_m) x^\alpha.$$

(b) Wenn $f \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ in x den Grad d hat, dann ist die partielle Honogenisierung von f gleich

$$f^h(x_0, \ldots, x_n, y_1, \ldots, y_m) = x_0^d f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}, y_1, \ldots, y_m\right).$$

(c) Wenn $F_1, \ldots, F_s \in k[x_0, x_1, \ldots, x_n, y_1, \ldots, y_m]$ homogen in x sind, dann ist die Varietät $V(F_1, \ldots, F_s)$ definiert durch

$$\begin{aligned} &V(F_1, \ldots, F_s) \\ &= \{(x_0 : x_1 : \cdots : x_n; y_1, \ldots, y_m) | \forall i \forall \lambda \neq 0 : F_i(\lambda x_0, \ldots, \lambda x_n, y_1, \ldots, y_m) = 0\}. \end{aligned}$$

11.2 Beispiel. Sei $f = x_1 y_1^2 - x_1 + 1$ und sei $I = \langle f_1 \rangle \subset \mathbb{C}[x_1, x_2]$. Dann $I_1 = \{0\}$, aber für $y_1 = \pm 1$ macht der Ausdehnungssatz keine Aussage — und es gibt in der Tat auch keine Ausdehnung. Wir homogenisieren partiell

$$f^h = x_1 y_1^2 - x_1 + x_0$$

und betrachten die zugehörige Varietät in $\mathbb{P}^1(\mathbb{C}) \times \mathbb{C}$

$$V(f^h) = \left\{(1 - y_1^2 : 1; y_1) \middle| y_1 \in \mathbb{C}\right\}.$$

Definiert man die Projektion $\pi\colon \mathbb{P}^(\mathbb{C}) \times \mathbb{C} \to \mathbb{C}$ durch $(x_0 : x_1; y_1) \mapsto y_1$, so gilt $\pi(V(f^h)) = \mathbb{C}$.

Achtung: Beim Zeichnen des Graphen muss die (y_1, x_1)-Ebene verwendet werden, wenn die Projektion vertikal erfolgen soll.

11.3 Definition. Sei $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$ ein Ideal, welches von Polynomen erzeugt wird, die homogen in x sind. Dann bezeichnen wir

$$\hat{I} := \{f \in k[y_1, \ldots, y_m] | \forall i \exists e_i \in \mathbb{N}_0 : x_i^{e_i} f \in I\}$$

als *projektives Eliminationsideal von* I.

11.4 Satz. *Sei* $V = V(F_1, \ldots, F_s) \subset \mathbb{P}^n(k) \times k^m$ *durch Polynome definiert, die homogen in* x *sind, und sei* $\pi\colon \mathbb{P}^n(k) \times k^m$ *die kanonische Projektion. Dann gilt*

$$\pi(V) \subset V_a(\hat{I}).$$

Beweis. Im $\mathbb{P}^n(k)$ verschwindet mindestens eine Komponente nicht, daher haben die Faktoren $x_0^{e_i}$ keinen Einfluss. □

11.5 Theorem (Projektiver Ausdehnungssatz). *Sei* k *ein algebraisch abgeschlossener Körper und sei* $V = V(F_1, \ldots, F_s)$ *durch Polynome erklärt, die homogen in* x *sind. Es sei* $I = \langle F_1, \ldots, F_s \rangle$ *und es sei* $\hat{I}$ *das zugehörige projektive Eliminationsideal. Dann gilt*

$$\pi(V) = V(\hat{I}).$$

Beweis. Wir nehmen zum Widerspruch die Existenz eines $c \in V(\hat{I})$ an, so dass

$$\{x | \forall i : F_i(x, c) = 0\} = \emptyset.$$

Dann sagt der schwache projektive Nullstellensatz, dass es ein $r \in \mathbb{N}$ gibt, so dass

$$\langle x_0, \ldots, x_n \rangle^r \subset \langle F_1(x, c), \ldots, F_s(x, c) \rangle .$$

Daher existiert zu jedem α mit $|\alpha| = r$ Polynome $H_i \in k[x_0, \ldots, x_n]$, so dass

$$x^\alpha = \sum_{i=1}^{s} H_i(x) F_i(x, c).$$

Ohne Einschränkung sind die H_i homogen. Der Grad von F_i in x sei d_i. Zerlegt man die H_i in ihre Terme, so sieht man, dass

$$\left\{ x^\beta F_i(x, c) \middle| 1 \leq i \leq s, |\beta| = r - d_i \right\}$$

den Raum aller homogenen Polynome vom Grad r aufspannt. Es gibt also eine Basis dieses Raums der Form $g_1, \ldots, g_{N_r}$ von Polynomen der Form

$$g_j(x) = x^{\beta_j} F_{i_j}(x, c).$$

Wir setzen $G_j(x, y) = x^{\beta_j} F_{i_j}(x, y)$. Diese G_j können in die x^α entwickelt werden

$$G_j = \sum_{|\alpha|=r} a_{j,\alpha}(y_1, \ldots, y_m) x^\alpha. \tag{11.1}$$

Es sei

$$D(y_1, \ldots, y_m) = \det\left((a_{j,\alpha}(y_1, \ldots, y_m))_{\substack{1 \leq j \leq N_r \\ |\alpha|=r}} \right).$$

Für $y = c$ bilden die $G_j(x, c)$ eine Basis, also

$$D(c) \neq 0. \tag{11.2}$$

Wir interpretieren nun eqrefeq:G als lineares Gleichungssystem mit Koeffizienten in $k(y_1, \ldots, y_m)$. Dann

$$x^\alpha = \frac{\det M_\alpha}{D(y_1, \ldots, y_m}),$$

wobei M_α die Matrix aus der Cramerschen Regel ist. Nun multipliziert man den Nenner hoch und entwickelt M_α nach der Spalte, welche die G_j enthält, so sieht man

$$x^\alpha D(y_1, \ldots, y_m) = \sum_{j_1}^{N_r} H_{j,\alpha} G_j.$$

Die G_j sind aber Vielfache der F_i, also

$$x^\alpha D(y_1, \ldots, y_m) \in \langle F_1, \ldots, F_s \rangle = I.$$

Das bedeutet $D(y_1, \ldots, y_m) \in \hat{I}$. Wegen $c \in V(\hat{I})$ gilt $D(c) = 0$ im Widerspruch zu (11.2). □

Literaturverzeichnis

[1] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer, Cham, fourth ed., 2015. An introduction to computational algebraic geometry and commutative algebra.

[2] B. Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, SpringerWienNewYork, Vienna, second ed., 2008.