Dimension von Varietäten

Yvan Ngumeteh Emma Ahrens

16. April 2018

Inhaltsverzeichnis

1 Abstract

2 Einleitung

3 Dimension von Monomidealen

Lemma 1. *Sei $I \subseteq k[X_1, \ldots, X_n]$ ein Ideal, das von einer Menge G von Monomen erzeugt wird. Dann liegt ein Polynom $f \in k[X_1, \ldots, X_n]$ in I genau dann, wenn für jeden Term $a_j X^{\alpha_j}$ von f ein $g \in G$ existiert, welches $a_j X^{\alpha_j}$ teilt.*

Beweis. Sei $f \in I$. Dann gilt $f = \sum_{i=1}^{s} h_i g_i$ mit $h_i \in R$ und $g_i \in G$. Damit hat jeder Term die Form $h_i g_i$ und ist somit durch ein Element aus G teilbar. Sei nun andersherum $f \in k[X_1, \ldots, X_n]$ und für jeden Term $a_j X^{\alpha_j}$ von f existiert ein $g \in G$, welches $a_j X^{\alpha_j}$ teilt. Dann kann man f als Linearkombination von Elementen aus G schreiben und damit liegt f nach der Definition eines Ideals in I. □

Lemma 2. *Sei $(g_i)_{i \geq 1}$ eine Folge von Monomen in $k[X_1, \ldots, X_n]$ mit $g_1 \succeq g_2 \succeq \ldots$ für eine Monomialordnung $\preceq$. Dann existiert ein $r \in \mathbb{N}$ mit $g_n = g_r$ für alle $n \geq r$.*

Beweis. Sei $I = ((g_i)_{i \geq 1})$, dann ist I ein Ideal. Nach dem Hilbert'schen Basissatz wissen wir, dass I endlich erzeugt ist. Also existiert ein r, so dass die Menge $G = \{g_1, \ldots, g_r\}$ I erzeugt. Für ein $i \geq r$ und $g_i \in I$ existiert ein $j \in \underline{r}$, so dass $g_j \mid$ (g_i nach Lemma 1. Also $g_i \succeq g_j \succeq g_r$. Andererseits gilt nach Voraussetzung, dass $g_i \preceq g_r$, also folgt $g_i = g_r$. □

Lemma 2 sagt uns, dass jede absteigende Kette von Monomen stationär wird und insbesondere in jeder abzählbaren Menge von Monomen ein kleinstes Element existiert.

Proposition 3 (Divisionsalgorithmus)**.** *Sei $\preceq$ eine Monomialordnung und $f, f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ nicht null. Dann gilt*

$$f = \sum_{i=1}^{s} h_i f_i \; + r,$$

mit $r, h_1, \ldots, h_s \in k[X_1, \ldots, X_n]$ und $LT(h_i f_i \preceq LT(f)$ für alle $h_i \neq 0$ und $r = 0$ oder kein Term von r wird durch ein $LT(f_i)$ geteilt für $i \in \underline{s}$.

Beweis. Wir beweisen diese Proposition per TODO downward Induktion über LT(f).
Beim Induktionsschritt unterscheiden wir drei Fälle:
Sei f konstant, dann gilt $f = \sum_{i=1}^{s} 0 f_i \ + r$ mit $r := f$ und $h_i := 0$.
Falls ein $i \in \underline{s}$ existiert, so dass $LT(f_i) \mid LT(f)$, setzen wir

$$f^{(1)} := f - \frac{LT(f)}{LT(f_i)} f_i.$$

Dann gilt $f = f^{(1)} + \frac{LT(f)}{LT(f_i)} f_i$ mit $h_i = \frac{LT(f)}{LT(f_i)}$ und $LT(h_i f_i) = LT(f) \preceq LT(f)$.
Falls kein solches f_i existiert, schreiben wir

$$f^{(1)} := f - LT(f).$$

Und $f = f^{(1)} + LT(f)$ mit $r = LT(f)$ erfüllt die Bedingungen (insbesondere, dass kein Term von r durch ein $LT(f_i)$ geteilt wird).
Führe den Schritt nun induktiv auf $f^{(1)}$ durch bis $f^{(j)} = 0$ und bestimme $h_1, \ldots, h_s, r$ durch Rückwärtseinsetzen. □

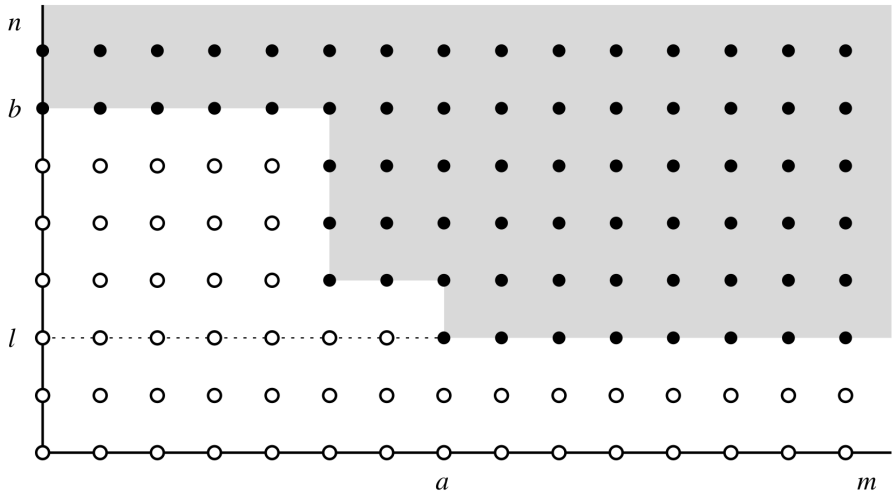
Evtl. Beispiel, dass diese Form nicht eindeutig ist.

Satz 4. *Sei $\{0\} \neq I \subseteq k[X_1, \ldots, X_n]$ ein Ideal und $\preceq$ eine Monomialordnung auf $Z^n_{\geq 0}$. Sei G eine Gröbnerbasis von I mit $I = (G)$. Dann ist eine k-Basis von $k[X_1, \ldots, X_n]/I$ gegeben durch die Restklassen von X^α mit*

$$\alpha \in C(I) := \{\alpha \in Z^n_{\geq 0} \mid LT(g) \nmid X^\alpha \quad \forall g \in G\}.$$

Beweis. Wir zeigen erst, dass die Monome mit Exponent aus C(I) ganz $k[X_1, \ldots, X_n]/I$ aufspannen und anschließend, dass kein Element aus I durch echte Linearkombination solcher Monome dargestellt werden kann.
Sei $G = \{f_1, \ldots, f_s\}$ und $0 \neq f \in k[X_1, \ldots, X_n]$. Dann ist $f = \sum_{i=1}^{s} h_i f_i \ + r = f' + r$ nach Proposition 3 mit $r = 0$ oder $r = a_l X^{\alpha_l} + \ldots + a_0$ mit $LT(f_i) \nmid X^{\alpha_j}$ für jedes $i \in \underline{s}$ und $j \in \underline{l}$. Also ist r eine Linearkombination von Monomen X^{α_j} mit $\alpha_j \in C(I)$. Es gilt außerdem $[f] = [r]$ in $k[X_1, \ldots, X_n]/(G)$ und damit erzeugen die Monome mit $\alpha \in C(I)$ den ganzen Restklassenring.
Angenommen es existiert $f = f' + r \in I$ mit $r \neq 0$ und f' und r wie oben. Dann gilt $0 \neq r = f - f'$. Da $f \in I$ und $f' \in I$ folgt $r \in I$, womit folgt, dass $(LT(r) \in (LT(f_1), \ldots, LT(f_s))$. Nach Lemma 1 existiert dann ein f_i mit $LT(f_i) \mid LT(r)$. Dies ist ein Widerspruch, also folgt $r = 0$ und die Restklassen von X^α mit $\alpha \in C(I)$ sind linear unabhängig in $k[X_1, \ldots, X_n]/I$. □

Was sagt uns Beispiel 1.2.9?? TODO



Bildchen mit Punkten und Erklärung dazu. Wir betrachten das ‘Wachstum’ von $k[X_1, \ldots, X_n]/I$

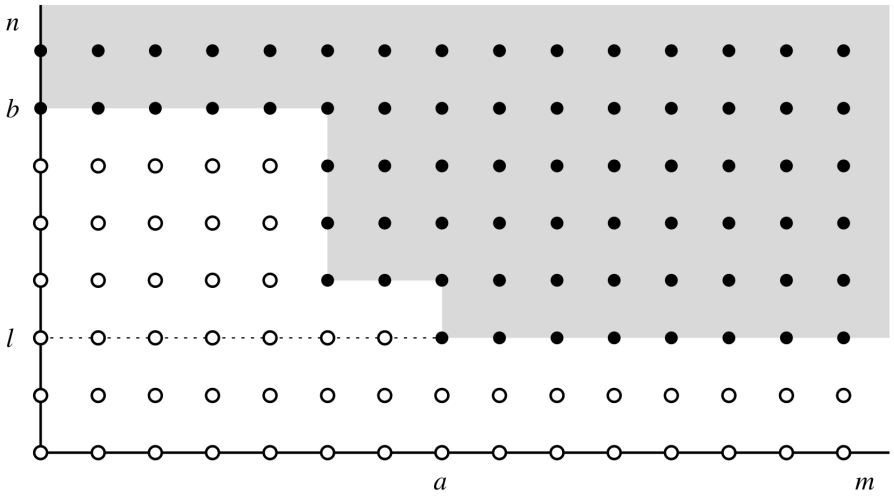


Abbildung 1: Anschauliche Darstellung von $k[X_1, \ldots, X_n]/I$ aus [3]

Definition 5. *Sei $I \subseteq k[X_1, \ldots, X_n]$ ein Ideal und $s \in \mathbb{N}_0$. Dann definiere $I_{\leq s} := I \cap k[X_1, \ldots, X_n]_{\leq s}$. Nun gilt, dass $k[X_1, \ldots, X_n]_{\leq s}$ ein endlich dimensionaler Vektorraum über k mit $I_{\leq s}$ als Teilraum ist. Wir können die Funktion*

$$^aHF_I : \mathbb{N}_0 \to \mathbb{N}_0, \quad s \mapsto dim_k(k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s})$$

definieren, die (affine) Hilbertfunktion von I genannt wird.

Ein paar Beispiele

- Sei $I = k[X_1, \ldots, X_n]$. Dann ist

$$\begin{aligned} ^aHF_I(s) &= dim_k(k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) \\ &= dim_k(k[X_1, \ldots, X_n]_{\leq s}/k[X_1, \ldots, X_n]_{\leq s}) \\ &= dim_k(\emptyset) \\ &= 0 \end{aligned}$$

  für alle $s \in \mathbb{N}_0$.

- Sei nun $I = \{0\}$. Dann ist

$$\begin{aligned} ^aHF_I(s) &= dim_k(k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) \\ &= dim_k(k[X_1, \ldots, X_n]_{\leq s}) \\ &= |\{X^\alpha \in Z^n_{\geq 0} \mid |\alpha| \leq s\}| \\ &= \sum_{i=1}^{s} |\{X^\alpha \in Z^n_{\geq 0} \mid |\alpha| = i\}| \\ &= TODO \\ &= \sum_{i=1}^{s} \binom{n-1+k}{k} \\ &= \binom{s+n}{s} = \binom{s+n}{n} \\ &= \frac{1}{n!}(s+n)(s+n-1)\cdots(s+1) \\ &= \frac{1}{n!}s^n + \frac{1}{n!}\binom{n+1}{2}s^{n-1} + \cdots + 1. \end{aligned}$$

Zu beachten ist hier, dass der Grad der Hilbertfunktion n ist, also der Dimension von $k[X_1, \ldots, X_n]/I$ entspricht. Dies werden wir im Folgenden näher betrachten.

- Einfaches Beispiel aus CLOS. TODO

Lemma 6 (Macaulay)**.** *Sei $\preceq$ eine gradierte lexikographische Monomialordnung und $I \subseteq k[X_1, \ldots, X_n]$ ein Ideal. Dann ist ${}^aHF_I(s) = {}^aHF_{LT(I)}(s)$ für alle $s \in \mathbb{N}_0$.*

Beweis. Zunächst definieren wir uns die Menge

$$D := \{LM(f) \mid 0 \neq f \in I_{\leq s}\} = \{LM(f_1), \ldots, LM(f_m)\}$$

für ein $m \in \mathbb{N}_0$ und $f_i \in I_{\leq s}$ für alle $i \in \underline{m}$. Die zweite Gleichheit gilt aufgrund der Endlichkeit von $I_{\leq s}$. Wir betrachten außerdem die Menge

$$B := \{f_1, \ldots, f_m\}.$$

Die Elemente aus B entsprechen denen aus der Menge D.

Wir zeigen nun, dass D eine k-Basis von $(LT(I))_{\leq s}$ und B eine k-Basis von $I_{\leq s}$ ist. Dann folgt nämlich, dass die beiden Mengen die selbe Kardinalität und die erzeugten Vektorräume die selbe Dimension haben, womit das Lemma von Macaulay gezeigt ist.

Als Erstes wollen wir zeigen, dass D eine k-Basis von $(LT(I))_{\leq s}$ ist. Da D die Leitmonome der Elemente aus I enthält, ist D offensichtlich linear unabhängig. Wir zeigen also, dass das Erzeugnis von D ganz $(LT(I))_{\leq s}$ aufspannt: Dazu betrachten wir ein beliebiges $g \in (LT(I))_{\leq s}$. Es gilt $deg(g) \leq s$ und da D alle $LT(I)$ mit Grad $\leq s$ enthält, kann man schreiben $g = \sum_{i=1}^{m} h_i LT(f_i)$ mit $h_i \in k$ für alle $i \in \underline{m}$. Also ist $g \in (D)$ und damit spannt D ganz $(LT(I))_{\leq s}$ auf. Es folgt also, dass D eine k-Basis von $(LT(I))_{\leq s}$ ist.

Jetzt zeigen wir, dass B eine k-Basis von $I_{\leq s}$ ist. Die lineare Unabhängigkeit der einzelnen Elemente können wir durch einen einfachen Widerspruchsbeweis zeigen: Sei $0 = \sum_{i=1}^{m} h_i f_i$, $h_i \in k$ für alle $i \in \underline{m}$, und es existiert ein $i \in \underline{m}$ mit $h_i \neq 0$. Da $f_i \neq 0$ ist, existiert mindestens ein $i \neq j \in \underline{m}$ mit $h_j \neq 0$. Ohne Beschränkung der Allgemeinheit kann man annehmen, dass genau zwei Koeffizienten $\neq 0$ existieren. Dann gilt

$$\begin{aligned} 0 = \sum_{i=1}^{m} h_i f_i &= h_i f_i + h_j f_j \\ \Leftrightarrow -h_j f_j &= h_i f_i \\ \Leftrightarrow -\frac{h_j}{h_i} f_j &= f_i. \end{aligned}$$

Also gilt $LM(f_j) = LM(f_i)$, dies ist aber ein Widerspruch zur Definition der Menge B, also ist B linear unabhängig.
Wir wählen nun ein $g \in I_{\leq s}$. Dann existiert ein $i \in \underline{m}$ mit $LM(f) = LM(f_i)$, weil $f \in I_{\leq s}$, also auch $LM(f) \in D$. Wir definieren

$$\begin{aligned} f^{(1)} &:= f - \frac{LM(f)}{LM(f_i)} f_i \\ \Leftrightarrow f &= f^{(1)} + \frac{LM(f)}{LM(f_i)} f_i. \end{aligned}$$

Es gilt $LM(f) = LM(\frac{LM(f)}{LM(f_i)} f_i)$, also folgt $LM(f^{(1)}) \preceq LM(f)$, da wir die Monome unter gradierter lexikographischer Ordnung betrachten. Für $f^{(1)}$ existiert wie für f wieder ein $j \in \underline{m}$ mit $LM(f) = LM(f_j)$, da $f^{(1)} \in I_{\leq s}$. Wir definieren $f^{(2)}$ analog zu oben und es folgt $LM(f^{(2)}) \preceq LM(f^{(1)})$. Das machen wir induktiv weiter bis $f^{(l)} = 0$ für ein $l \in \mathbb{N}$. Der Algorithmus endet nach endlich vielen Iterationen, da $LM(f) \succeq LM(f^{(1)}) \succeq LM(f^{(2)}) \succeq \cdots$. Also kann man g als k-Linearkombination von Elementen aus B schreiben, damit spannt B ganz $I_{\leq s}$ und B ist eine Basis von $I_{\leq s}$. □

4 Dimension von beliebigen Idealen

4.1 Das Hilbert-Polynom

Im folgenden sei $n \in \mathrm{N}$ fest.

Satz 7. *Sei $I \subset k[X_1, \ldots, X_n]$, dann existiert es einen eindeutigen Polynom ${}^aHP_I(t) \in \mathrm{Q}[t]$ (mit t eine variable) und $s_0 \geq 0$, sodass ${}^aHP_I(s) = {}^aHF_I(s) = dim_k\ (k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s})$, $\forall s \geq s_0$. Weiterhin besitzt ${}^aHP_I(t)$ folgende Eigenschaften:*

- Der Grad von ${}^aHP_I(\mathrm{t})$ ist der größte $d \in \mathrm{N}$, sodass es $1 \leq i_1 < i_2 < i_3 < ... < i_d \leq n$ existieren mit $I \cap k[X_{i_1}, \ldots, X_{i_d}] = \emptyset$.
- Sei $d = grad({}^aHP_I(\mathrm{t}))$. Dann gilt ${}^aHP_I(\mathrm{t}) = \sum_{k=0}^{d} a_k t^k$ mit $a_k d! \in \mathrm{Z}, \forall k \in \underline{d_0}$ und $a_k d! > 0$

Beweis. Wir bemerken dass ${}^aHP_I(\mathrm{t})$ eindeutig ist, da es ein Polynom ist. Es nur die Existenz nachgewiesen werden. Sei $M = \{\alpha \in \mathrm{N}_0 : |\alpha| \leq s\}$

- Für die trivialen Fällen $I = (0)$ hat man, wegen ${}^aHF_I(\mathrm{s}) = dim_k\ (k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) = |M| = \binom{n+s}{s}, \forall s \in \mathrm{N}_0$.
  Oder $I = k[X_1, \ldots, X_n]$ gilt ${}^aHF_I(\mathrm{s}) = dim_k\ (k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) = 0, \forall s \in \mathrm{N}_0$ und somit entspricht in diesem Fall ${}^aHP_I = 0$ (Das Nullpolynom !) Nehmen wir also an, dass I nicht trivial ist. Sei G eine Gröbner-Basis von I (bzgl. eine graduierte lexikographische Ordnung) und

  $$\{LM(g) : g \in G\} = \{X_\beta : \beta \in M\}$$

  wir setzen

  $$C(I) := \{\alpha \in \mathrm{N}_0 : X^\beta \nmid X^\alpha \forall \in \beta \in M\} \text{ und } C(I)_{\leq s} := C(I) \cap \{\alpha \in \mathrm{N}_0 : |\alpha| \leq s\}$$

  Behauptung: Für $s \geq 0$ gilt ${}^aHF_I(\mathrm{s}) = |C(I)_{\leq s}|$, $\forall s \geq 0$.
  Für den Beweis benutzt man (Macaulay), dann gilt ${}^aHF_I(\mathrm{s}) = {}^aHF_{(LT(I))}(\mathrm{s})$, $\forall \in s \geq 0$. Das heißt,

  $$dim_k(k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) = dim_k(k[X_1, \ldots, X_n]_{\leq s}/(LT(I))_{\leq s}).$$

  Weiterhin gilt mit der Buchberger-Definition (1.2.7), dass $\{X^\beta : \beta \in M\}$ ist eine Gröebner-Basis von (LT(I)), deshalb mit Satz 1.2.8 habt man, dass die Restklassen von X^β ($\alpha \in C(I)$) bilden eine K-Vektorraum Basis von $k[X_1, \ldots, X_n]/(\mathrm{LT(I)})$. Daraus folgt die Behauptung.
- Sei $J \subseteq \underline{n}$ und eine Funktion $\tau : J \longrightarrow \mathrm{N}_0$. Wir definieren

  $$C(J, \tau) := \{\alpha \in N : \alpha_j = \tau(j), \forall \in J\}$$

  Behauptung: Es existiert eine endliche Anzahl χ von Tupeln (J,τ), sodass

  $$C(I) = \bigcup_{(J,\tau) \in \chi}$$

  Proof. Für $\beta := (\beta_1, \ldots, \beta_n) \in \mathrm{N}_0$, definiert man

  $$C(\beta) := \{\alpha \in {\mathrm{N}_0}^n : X^\beta \nmid X^\alpha\}$$

  Dann haben wir $C(I) = \bigcap_{\beta \in M} C(\beta)$. Weiterhin bemerken wir, dass falls $(J, \tau), (J\prime, \tau\prime)$ zwei Tupeln, wie oben definiert bezeichnet, dann gilt

  $$C(J, \tau) \cap C(J\prime, \tau\prime) = \begin{cases} \emptyset, & falls \tau(j) = \tau\prime(j) \\ C(J \cup J\prime, \tau_0), & sonst \end{cases}$$

wobei $\tau_0 : J \cup J\prime \longrightarrow \mathrm{N}_0,\ j \mapsto \tau_0(j) = \begin{cases} \tau(j), & fallsj \in J \\ \tau\prime(j), & fallsj \in J\prime \\ 0, & sonst \end{cases}$.

Das heißt man kann O.B.d.A annehmen, dass in

□

[Beweis]

□

Literatur

[1] Heuser, Harro: *Lehrbuch der Analysis.* 15. Aufl. Vieweg-Verlag, Braunschweig-Wiesbaden, 2003

[2] Gröger, Detlef ; Marti, Kurt: *Grundkurs Mathematik für Ingenieure, Natur- und Wirtschaftswissenschaftler.* 2. Aufl. Physica-Verlag, 2004

[3] Cox, David; Little, John; O'Shea, Donal: *Ideals, Varieties, and Algorithms.* Third Edition Springer-Verlag, 2007