Dimension von Varietäten

Yvan Ngumeteh Emma Ahrens

26. September 2018

1 Abstract

Varietäten sind die Nullstellenmengen von Idealen aus einem Polynomring. Im Folgenden charakterisieren wir die Dimension einer Varietät, indem wir das Hilbertpolynom des zugehörigen Ideals definieren und zeigen, dass der Grad des Hilbertpolynoms der Dimension der Varietät entspricht. Dafür zeigen wir unter anderem, dass der Grad der Hilbertpolynome für alle Ideale mit gleicher Nullstellenmenge identisch ist. Hierdurch erlangen wir ein tieferes Verständnis für die Zusammenhänge zwischen Punktmengen und Polynomringen, also auch zwischen Algebra und Geometrie.

2 Einleitung

Sei $S \subseteq k[X_1, \ldots, X_n]$ eine Teilmenge eines Polynomrings über einem algebraisch abgeschlossenen Körper k. Dann ist $V(S) := \{x \in k^n \mid f(x) = 0 \ \forall f \in S\}$ eine Varietät bzw. algebraische Menge. Andersherum nennt man für eine Teilmenge $V \subseteq k^n$ das Ideal $I(V) := \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0 \ \forall x \in V\}$ das Verschwindungsideal von V. Mit Hilfe von Hilbert's Nullstellensatz können wir eine Bijektion von der Menge der Wurzelideale[1] aus $k[X_1, \ldots, X_n]$ auf die Menge der Varietäten definieren. Dies gibt uns die Möglichkeit, unser Wissen über Ideale auf Varietäten zu übertragen. Wir haben schon gesehen, dass z.B. das Verschwindungsideal von Vereinigungen von Varietäten dem Schnitt der Verschwindungsideale der einzelnen Varietäten entspricht. In Abbildung 1 und 2 sind beispielhaft zwei Varietäten dargestellt.

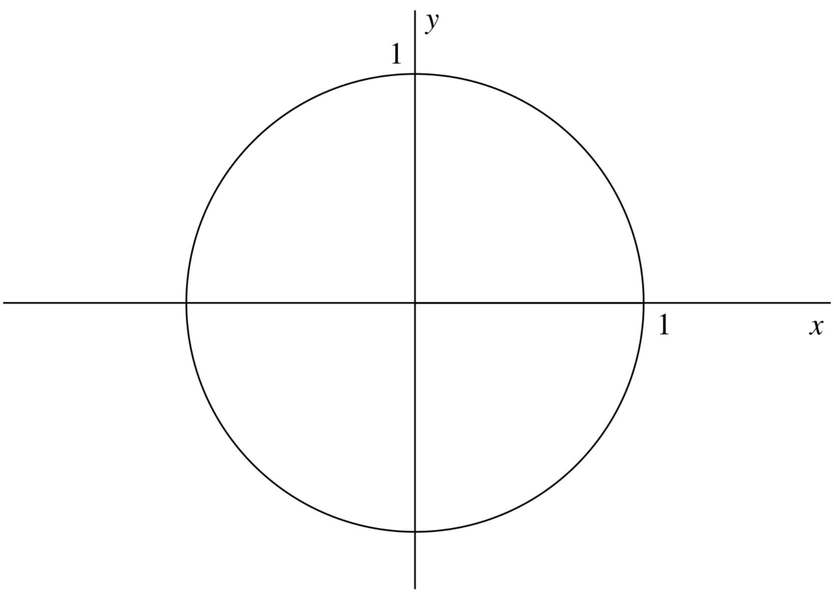

Abbildung 1: Die Varietät $V(X^2 + Y^2 - 1)$ aus [1]

[1]Ein Wurzelideal $\sqrt{I}$ ist ein Ideal für welches gilt: Sei $f^m \in \sqrt{I}$, dann ist auch $f \in \sqrt{I}$.

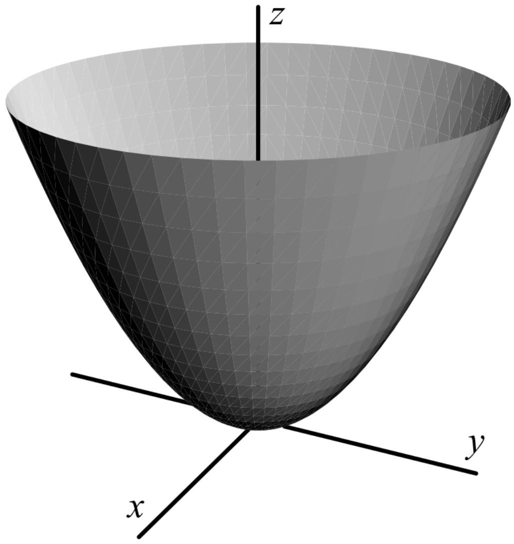

Abbildung 2: Das elliptische Paraboloid $V(Z - X^2 - Y)$ aus [1]

Im Folgenden interessieren wir uns für die Dimension einer Varietät. Intuitiv würde man die Varietät aus Abb. 1 eindimensional und die aus Abb. 2 zweidimensional nennen. Bevor wir mit der - etwas längeren - mathematischen Definition einer der Dimension einer Varietät beginnen, betrachten wir zunächst einen etwas leichteren Fall aus [1]. Für das Beispiel brauchen wir die Ebene $H_x := \{(x, y, z) \in k^3 \mid x = 0\}$ und die Gerade $H_{xy} := \{(x, y, z) \in k^3 \mid x = 0 \wedge y = 0\}$.

Überlegen wir uns nun die Dimension von der Varietät des Monomialideals $I := (Y^2Z^3, X^5Z^4, X^2YZ^2)$ in $k[X, Y, Z]$. Dann wissen wir

$$\begin{aligned} V(I) &= V(Y^2Z^3, X^5Z^4, X^2YZ^2) \\ &= V(Y^2Z^3) \cap V(X^5Z^4) \cap V(X^2YZ^2) \\ &= (H_y \cup H_z) \cap (H_x \cup H_z) \cap (H_x \cup H_y \cup H_z) \\ &= H_z \cup (H_y \cap H_x \cap (H_x \cup H_y)) \end{aligned}$$

Der Schnitt der zwei Ebenen H_x und H_y ist die Gerade H_{xy} und $H_{xy} \cap (H_x \cup H_y) = H_{xy}$, also folgt

$$V(I) = H_z \cup H_{xy}.$$

Die Varietät besteht also aus der xy-Ebene und einer Geraden, die darauf senkrecht steht. Es gibt also einen Teil, der intuitiv eindimensional erscheint und einen zweidimensionalen. Später werden wir sehen, dass die Dimension einer Varietät die maximale Dimension der einzelnen Teile der Varietät ist - für das Beispiel ist sie also 2.

3 Suchen einer k-Basis von $k[X_1, \ldots, X_n]/I$

Wir beginnen damit, für ein Ideal I eine möglichst einfache k-Basis von $k[X_1, \ldots, X_n]/I$ zu finden. Damit der Beweis unseres ersten Satzes nicht zu lang wird, müssen wir allerdings noch ein bisschen Vorarbeit leisten.

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 $a_jX^{\alpha_j}$ von f ein $g \in G$ existiert, welches $a_jX^{\alpha_j}$ 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 $a_jX^{\alpha_j}$ von f existiert ein $g \in G$, welches $a_jX^{\alpha_j}$ teilt. Dann kann man f als Linearkombination von Elementen aus G schreiben und damit liegt f nach der Definition eines Ideals in I. $\square$

Lemma 2. *Sei $(g_i)_{i\geq 1}$ eine Folge von Monomen in $k[X_1,\dots,X_n]$ mit $g_1 \succeq g_2 \succeq \dots$ 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 $G = \{g_1,\dots,g_r\}$ 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 insbesondere, dass in jeder abzählbaren Menge von Monomen ein kleinstes Element existiert.

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

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

mit $r, h_1,\dots,h_s \in k[X_1,\dots,X_n]$ 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 Rückwärtsinduktion über LT(f) beginnend mit dem größten Term.
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 $h_1,\dots,h_s, r$ durch Rückwärtseinsetzen. □

Jetzt kommen wir zu dem ersten Satz, der direkt für die Dimension von Varietäten wichtig ist.

Satz 4. *Sei $\{0\} \neq I \subseteq k[X_1,\dots,X_n]$ ein Ideal und $\preceq$ eine Monomialordnung auf $\mathbb{N}_0^n$. Sei G eine Gröbnerbasis von I mit I = (G). Dann ist eine k-Basis von $k[X_1,\dots,X_n]/I$ gegeben durch die Restklassen von X^α mit*

$$\alpha \in C(I) := \{\alpha \in \mathbb{N}_0^n \mid \ LT(g) \nmid X^\alpha \ \forall g \in G\}.$$

Beweis. Wir zeigen erst, dass die Monome mit Exponent aus C(I) ganz $k[X_1,\dots,X_n]/I$ aufspannen und anschließend, dass kein Element aus I durch echte Linearkombination solcher Monome dargestellt werden kann.
Sei $G = \{f_1,\dots,f_s\}$ und $0 \neq f \in k[X_1,\dots,X_n]$. Dann ist $f = \sum_{i=1}^{s} h_i f_i \ + r = f' + r$ nach Proposition 3 mit $r = 0$ oder $r = a_l X^{\alpha_l} + \dots + a_0$ 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 $k[X_1,\dots,X_n]/(G)$ 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 $(LT(r) \in (LT(f_1),\dots,LT(f_s))$. 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 $k[X_1,\dots,X_n]/I$. □

In Abb. 3 sieht man ein Koordinatensystem von $\mathbb{N}_0^2$. Jeder Punkt α repräsentiert dabei ein Monom X^α für welches gilt $X^\alpha = LM(f)$ für ein $f \in k[X_1,\dots,X_n]$. Die Punkte in dem grau hinterlegten Teil stehen nun für die Monome, die Elemente aus $LM(I)$ sind. Die unausgefüllten Punkte stehen für Monome aus C(I).

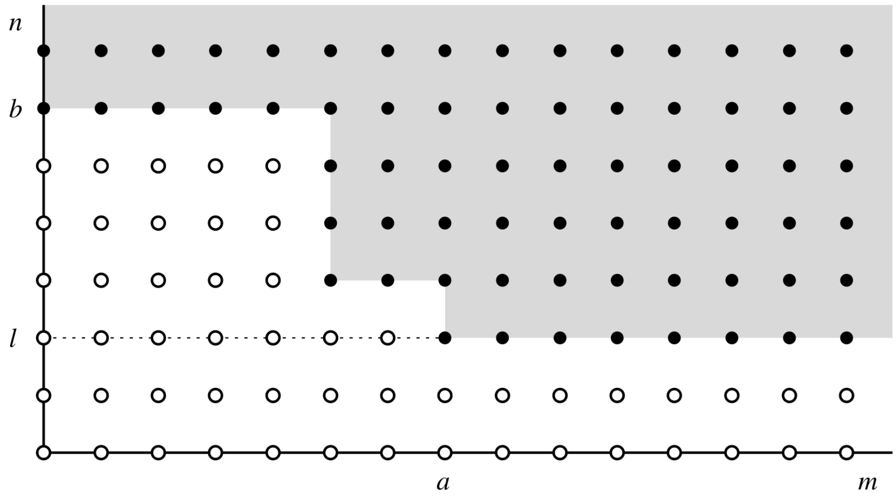

Abbildung 3: Anschauliche Darstellung von $k[X_1, \ldots, X_n]/I$ aus [1]

4 Die Hilbertfunktion

In diesem Abschnitt definieren wir uns die sogenannte Hilbertfunktion. Diese Funktion bildet eine natürliche Zahl auf die Dimension eines Faktorvektorraums ab. Bevor wir im nächsten Abschnitt beweisen, dass jede Hilbertfunktion einem Polynom entspricht, werden wir jetzt schon anhand von Beispielen sehen, dass der Grad des jeweiligen Polynoms der “intuitiven” Dimension der Varietät des Ideals entspricht, welches als Faktor für den Faktorvektorraum benutzt wurde.

Anschließend beweisen wir noch das Lemma von Macaulay, welches besagt, dass die Hilbertfunktion zu dem Ideal $I \subseteq k[X_1, \ldots, X_n]$ die selbe ist wie die Hilbertfunktion zu dem Ideal $LT(I)$. Damit vereinfachen wir die nachfolgenden Überlegungen und sehen auch, warum wir uns in einem der Beispiele Abb. 3 anschauen und alle anderen Informationen über das unterliegende Ideal vernachlässigen können.

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.

Nun wollen wir uns ein paar beispielhafte Hilbertfunktionen anschauen. Für eines der Beispiel brauchen wir ein bisschen Kombinatorik, die wir im nächsten Lemma beweisen wollen. Und zwar wollen wir eine Aussage über die Anzahl der Tupel aus $\mathbb{N}_0^n$ machen, welche vom Betrag kleiner sind als eine bestimmte natürliche Zahl s.

Lemma 6. *Es gilt $|M_{n,s}| := |\{\alpha \in \mathbb{N}_0^n \mid |\alpha| \leq s\}| = \binom{s+n}{s}$.*

Beweis. Induktionsanfang: Sei $n = 2$, $s \in \mathbb{N}$ fest und $\alpha = (\alpha_1, \alpha_2) \in \mathbb{N}_0^2$. Wähle $\alpha_1 \in \{0, \ldots, s\}$. Dann muss $\alpha_2 \in \{0, \ldots, s - \alpha_1\}$ gelten, damit $|\alpha| = \alpha_1 + \alpha_2 \leq s$. Nun wissen wir, dass

$$\begin{aligned} |M_{2,s}| &= \sum_{i=0}^{s} s - i + 1 = s(s+1) - \frac{s(s+1)}{2} + (s+1) \\ &= (s+1)(s - \frac{s}{2} + 1) = (s+1)(2s - s + 2)\frac{1}{2} \\ &= (s+1)(s+2)\frac{1}{2} = \frac{(s+1)!}{2!\, s!} = \binom{s+2}{s} \end{aligned}$$

Induktionsvoraussetzung: Die Behauptung gelte für ein $n \in \mathbb{N}_{\geq 2}$.

Induktionsschritt: Sei $n \in \mathbb{N}_{\geq 2}$ mit $|M_{n,s}| = \binom{s+n}{s}$. Wir betrachten $\alpha \in \mathbb{N}_0^{n+1}$ und können α auch schreiben als $\alpha = (\beta, \alpha_{n+1})$ mit $\beta \in \mathbb{N}_0^n$. Sei $\alpha_{n+1} \in \{0, \ldots, s\}$, dann muss $\beta \in M_{n,s-\alpha_{n+1}}$ sein, damit $|\alpha| \leq s$. Also folgt mit der Induktionsvoraussetzung und einer Indexverschiebung

$$\begin{aligned} |M_{n+1,s}| &= \sum_{i=0}^{s} |M_{n,s-i}| = \sum_{i=0}^{s} \binom{s-i+n}{s-i} \\ &= \sum_{i=0}^{s} \binom{i+n}{i} = \binom{s+(n+1)}{s} \end{aligned}$$

Damit folgt die Behauptung nach dem Induktionsprinzip. □

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 mit Satz 4 und Lemma 6

$$\begin{aligned} {}^aHF_I(s) &= dim_k(k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) \\ &= dim_k(k[X_1, \ldots, X_n]_{\leq s}) \\ &= |\{X^\alpha \in k[X_1, \ldots, X_n] \mid deg(X^\alpha) \leq s\}| \\ &= |\{\alpha \in \mathbb{N}_0^n \mid |\alpha| \leq s\}| = |M_{n,s}| \\ &= \binom{s+n}{s} = \binom{s+n}{n} \\ &= \frac{1}{n!}(s+n)(s+n-1)\cdots(s+1) \\ &= \frac{1}{n!}s^n + \frac{1}{n!}\binom{n+1}{2}s^{n-1} + \cdots + 1. \end{aligned}$$

- Gehen wir noch einmal kurz zu Abb. 3 zurück. Hier betrachten wir ein Ideal I aus $k[X, Y]$. Es gilt ${}^aHF_I(6) = 27$, ${}^aHF_I(8) = 38$ und ${}^aHF_I(9) = 41$. Für $s \geq 11$ gilt ${}^aHF_I(s+1) = {}^aHF_I(s) + 2$, die Funktion wächst also linear. Man kann die Hilbertfunktion sogar direkt an der Abbildung ablesen: Für $s \geq 7$ gilt ${}^aHF_I(s) = 2 * s + 23$.

Überlegen wir uns kurz den Zusammenhang zwischen der „gefühlten“Dimension einer Varietät und dem Grad der Hilbertfunktion. Im ersten Beispiel ist $V(I) = \{0\}$ und die gefühlte Dimension ist 0. Dies entspricht auch dem Grad der Hilbertfunktion. Im zweiten Beispiel ist $V(I) = k^n$ mit Dimension n und auch die Hilbertfunktion hat den Grad n. Für die Varietät aus Abb. 3 gilt $V(I) = \{(x, y) \in k^2 \mid y = 0\} = H_y$. Also ist $V(I)$ intuitiv eindimensional, was ebenfalls dem Grad der Hilbertfunktion entspricht.

Im nächsten Lemma zeigen wir erst einmal, dass es keinen Unterschied macht, ob wir die Hilbertfunktion bezüglich des Ideals I oder des Ideals $LT(I)$ betrachten.

Lemma 7 (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

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

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

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

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 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 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 $g \in I$. Dann existiert ein $i \in \underline{m}$ mit $LM(f) = LM(f_i)$, weil $f \in I$, 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 $f^{(1)} \in I$. 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 und B ist eine Basis von I. $\square$

5 Das Hilbert-Polynom und die Dimension affiner-Varietäten

Im folgenden sei $n \in$ N beliebig aber fest.

Definition 8. *Sei $I \subset k[X_1, \dots, X_n]$ ein nicht triviales Ideal und $\preceq$ eine Monomiale Ordnung auf ${\mathbb{N}_0}^n$. Man nennt eine endliche Menge $G \subseteq I - \{0\}$ eine Gröbner-Basis von I, falls die Monome $LT(g)$ $(g \in G)$ das Ideal*

$$(LT(I)) := (LT(f) : 0 \neq f \in I) \subseteq k[X_1, \dots, X_n]$$

erzeugen.

Nach dem Hilbert'sche Basissatz besitzt jedes nicht triviales Ideal eine Gröbner-Basis.

Satz 9. *Sei* $I \trianglelefteq k[X_1, \ldots, X_n]$*, dann existiert ein eindeutiges Polynom* ${}^aHP_I(t) \in \mathbb{Q}[t]$ *(t ist eine Variable) und* $s_0 \geq 0$*, sodass* ${}^aHP_I(s) = {}^aHF_I(s) = dim_k\ (k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s})$*, für alle* $s \geq s_0$*. Weiterhin besitzt* ${}^aHP_I(t)$ *folgende Eigenschaften:*

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

Beweis. Wir bemerken, dass ${}^aHP_I$(t) sobald existent eindeutig ist, da es ein Polynom ist. Es muss also nur die Existenz nachgewiesen werden. Im Folgenden ist $s \in \mathbb{N}_0$ beliebig aber fest gewählt, falls nicht anders spezifiziert wird.

Für die trivialen Fälle $I = (0)$ gilt, wegen ${}^aHF_I$(s)$= dim_k\ (k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) = |M| = \binom{n+s}{s}, \forall s \in \mathbb{N}_0$.
Oder $I = k[X_1, \ldots, X_n]$,wegen ${}^aHF_I$(s)$= dim_k\ (k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}) = 0, \forall s \in \mathbb{N}_0$ (also ${}^aHP_I \equiv 0$ ist das Nullpolynom !) die Behauptungen.
Wir gehen im Folgenden in fünf Schritten vor.

1. Nehmen wir also an, dass I nicht trivial ist. Sei G eine Gröbner-Basis von I (bzgl. eine graduierte lexikographische Ordnung) und $M = \{\alpha \in \mathbb{N}_0^n : \exists\ f \in G \text{ sodass } LM(f) = X^\alpha\}$

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

Die Mächtigkeit von M ist endlich , da nach dem Hilbert'sche Basissatz G eine endliche Menge von Polynomen ist. Wir setzen im Folgenden

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

Behauptung: $\forall s \geq 0$ gilt ${}^aHF_I$(s)$= |C(I)_{\leq s}|$.

Beweis. Nach Lemma 7 gilt ${}^aHF_I$(s)$={}^aHF_{(LT(I))}$(s), für alle $\in s \geq 0$. 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 Definition (1.2.7)(Buchberger), dass $H = \{X^\beta : \beta \in M\}$ eine Gröebner-Basis von (LT(I)) ist. Mit Satz 4 bilden die Restklassen von X^α $(\alpha \in C(I))$ eine k-Vektorraum-Basis von $k[X_1, \ldots, X_n]/(LT(I))$. Daraus folgt die Behauptung.

□

2. Seien $J \subseteq \underline{n}$ und eine Abbildung $\tau : J \longrightarrow \mathbb{N}_0$ gegeben. Wir definieren

$$C(J, \tau) := \{\alpha \in (\mathbb{N}_0)^n : \alpha_j = \tau(j), \forall \in J\}$$

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

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

Beweis. Für $\beta := (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n$, definiert man

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

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

$$(\star\star) \quad C(J, \tau) \cap C(J\prime, \tau\prime) = \begin{cases} \emptyset & , falls\ \tau(j) \neq \tau\prime(j) \text{ für einige } j \in J \cap J\prime \\ C(J \cup J\prime, \tau_0) & , sonst \end{cases}$$

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

Aber es gilt $\alpha \in C(\beta) \Leftrightarrow \alpha_i < \beta_i$ für einige $i \in \underline{n}$. Also gilt,

$$\begin{aligned} C(\beta) &= \bigcup_{i=1}^{n} \bigcup_{t_i=1}^{\beta_i - 1} \{\alpha \in {\mathbb{N}_0}^n : a_i = t_i\} \\ &= \bigcup_{i=1}^{n} \bigcup_{t_i=1}^{\beta_i - 1} C(i, \tau : i \mapsto t_i) \end{aligned}$$

Da $|M|$ endlich und die $C(\beta)$ jeweils endliche Vereinigungen von Mengen von Typ $C(J,\tau)$ ist, folgt die Behauptung aus ($\star\star$).

□

3. Behauptung: Für alle (J,τ) im 2.Fall, existiert ein eindeutiges Polynom $F_{J,\tau}(s) \in \mathbb{Q}[t]$ mit $grad(F_{J,\tau}) = n - |J|$ und $F_{J,\tau}(s) = \left|C(J,\tau)_{\leq s}\right|$, für alle $s \geq |\tau| := \sum_{j \in J} \tau(j)$

   Beweis. Sei $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}_0$, sodass $\gamma_j = 0$, falls $j \notin J$ und $\gamma_j = \tau(j)$, falls $j \in J$. Dann gilt $C(J,\tau)$ ist die Menge von $\alpha + \gamma$, wo $\alpha = (\alpha_1, \ldots, \alpha_n) \in {\mathbb{N}_0}^n$ ist, sodass $\alpha_j = 0, \forall j \in J$. Daraus folgt, dass $\left|C(J,\tau)_{\leq s}\right|$ die Anzahl von Monomen in den Variablen X_j $(j \notin J)$, sodass multipliziert mit X^γ, der Grad maximal s beträgt.
   Dies wiederum entspricht der Anzahl von Monomen in $d := n - |J|$ Variablen deren höchstens Grad $s - |\gamma|$ beträgt, da die Variablen mit Indizes in J eine durch τ vorgegebene Potenz haben und der Grad des gesamten Produkts nach oben durch s beschränkt ist. Wichtig hierbei zu beachten ist, dass $|\gamma| = |\tau|$ gilt. Deswegen gilt,

$$\begin{aligned} \left|C(J,\tau)_{\leq s}\right| &= \binom{n - |J| + s - |\gamma|}{s - |\gamma|} = \binom{d + s - |\gamma|}{s - |\gamma|} \\ &= \binom{d + s - |\gamma|}{d} = \frac{(d + s - |\gamma|)(d + s - |\gamma - 1| \ldots (s - |\gamma + 1|))}{d!} \\ &= \frac{s^d + O(s)}{d!} =: F_{J,\tau}(s) \end{aligned}$$

   ,wobei $grad(O(s)) < d$ gilt. Da die Koeffizienten des obigen Polynoms eindeutig durch d und $|\gamma|$ festgelegt sind, folgt die Eindeutigkeit von $F_{J,\tau}$. Hierbei hat der Leitkoeffizient von $F_{J,\tau}$ die Form $\frac{1}{d!} > 0$. □

4. Sei $m \in \mathbb{N}_0$ beliebig aber fest. Falls $A_1, \ldots, A_m$ endliche Teilmengen von einer Menge T sind, dann lässt sich die Mächtigkeit deren Vereinigung mittels dem Inklusion-Exklusion-Prinzip durch

$$|A_1 \cup \ldots \cup A_m| = \sum_{r=1}^{m} (-1)^{r-1} \sum_{J \subset \underline{n}, |J| = r} |\bigcap_{j \in J} A_j|$$

   berechnen. Diese Formel lässt sich mittels Vollständige-Induktion über m oder leicht aus der Siebformel von Sylvester-Poincare aus der Stochastik (siehe [2]) beweisen. Wir wenden im Folgenden dem Inklusion-Exklusion-Prinzip auf die Berechnung von ${}^aHF_I(s) = \left|C(J,\tau)_{\leq s}\right|$ an.
   Aus ($\star$) existiert $l \in \mathbb{N}_0$ und $((J_i,\tau_i))_{i \in \underline{l}}$, sodass

$$C(I) = \bigcup_{(J,\tau) \in \chi} C(J,\tau) = \bigcup_{i \in \underline{l}} C(J_i, \tau_i)$$

Sei $s_0 := \max\{|\tau_i| : i \in \underline{l}\} + 1$. Für $s \geq s_0$ gilt aus 2.Fall für alle $i \in \underline{l}$, dass

$$\left|C(J_i,\tau_i)_{\leq s}\right| = \frac{s^{d_i} + O(s)}{d_i!}, \text{ mit } grad(O(s)) < d_i = n - |J_i|$$

Weiterhin haben wir im 2.Fall gesehen, dass der Schnitt von Mengen der Form $C(J,\tau)$ entweder leer oder von der Form $C(J_0,\tau_0)$ mit $J_0 \supseteq J$ (mit $J_0 \neq J$, falls die Tupel im Schnitt nicht gleich sind.). Aus dem 2.Fall gilt, dass $\left|C(J,\tau)_{\leq s}\right|$ für $s \geq |\tau|$ die Werte eines eindeutigen Polynom $F_{J,\tau} \in \mathbb{Q}[t]$ annimmt, dessen Koeffizienten eindeutig durch $d = n - |J|$ und $|\tau|$ ($= |\gamma|$ nach Definition τ) festgelegt sind. Daraus folgt für $s \geq s_0$ die Existenz von ${}^aHP_I \in \mathbb{Q}[t]$ aus dem Inklusion-Exklusion-Prinzip. Sei dann d_0, der größte $d \geq 0$, sodass es existiert ein Tupel (J,τ) mit $C(J,\tau) \subset C(I)$ und $d = n - |J|$. Dann gilt

$${}^aHP_I(t) = \sum_{(J,\tau)\in\chi,\, d_0+|J|=n} F_{J,\tau}(t) + \Omega(t), \text{ mit } grad(\Omega) < d_0$$

Aus dem 2.Fall erhält man, dass die Terme von Grad d_0 aufgrund deren positiven Leitkoeffizienten in der letzte Summe nicht verschwinden. Also $grad({}^aHP_I(\mathrm{t})) = d_0$ und der führende Koeffizient ist $\frac{a}{d_0} > 0$ mit $a \in \mathbb{N}_0$

5. In diesem letzten Unterpunkt beweisen wir die Aussage in a). Aus dem 4.Fall gilt, dass $grad({}^aHP_I)$ die größte natürliche Zahl d ist, sodass es ein $J \subset \underline{n}$ von $|J| = n - d$ und $\tau : J \to \mathbb{N}_0$ mit $C(J,\tau) \subset C(I)$ existiert. Dies auch äquivalent mit der Aussage, dass $grad({}^aHP_I)$ gegeben ist, durch $n - m$, wobei $m \in \mathbb{N}$ die minimale Anzahl von Variablen $X_{i_1}, \ldots, X_{i_m}$ bezeichnet, sodass $\alpha = (0, \ldots, \alpha_{i_1} = 1, 0, \ldots, 0, \alpha_{i_m} = 1, 0, 0) \in C(I)$ gilt.

   Behauptung: Es gilt: $I \cap k\,[X_j : j \notin J] = (0)$, für alle Tupel (J,τ) sodass $C(J,\tau) \subset C(I)$.

   Beweis. Angenommen es existiere $0 \neq f \in I \cap k\,[X_j : j \notin J]$. Dann gilt $0 \neq LT(f) \in LT(I) \cap k\,[X_j : j \notin J]$. Schreibt man weiterhin

$$LT(f) = aX^{\alpha}, \text{ mit } a \in k^*, \alpha \in {\mathbb{N}_0}^n$$

   mit $\alpha_j = 0$, $\forall j \in J$ und $\gamma + \alpha \in C(J,\tau) \subset C(I)$ für ein $\gamma \in C(J,\tau)$, dann gilt

$$aX^{\gamma+\alpha} = aX^{\gamma}LT(f) \in (LT(I)) \Rightarrow \exists \beta \in M : X^{\beta} \nmid X^{\gamma+\alpha}$$

   Dies ist ein Widerspruch zu $\gamma + \alpha \in C(I)$, woraus die Behauptung folgt.

   □

   Da die letzte Aussage für jedes der in ($\star$) vorkommenden J gültig ist und $grad({}^aHP_I) = |\{X_j : j \notin J\}|$ für ein mindestens eines solchen J gilt, folgt

$$\begin{aligned} grad({}^aHP_I(t)) &\leq \max\{d \in \underline{n} : \exists J \subset \underline{n}\, mit\, I \cap K[X_j : j \in J] = (0)\} \\ &= \max\{d \in \underline{n} : \exists i_1, \ldots, i_n \underline{n} \text{ mit } 1 \leq i_1 < \ldots < i_n \leq n \text{ und } I \cap K[X_j : j \notin J] = (0)\} := d_0 \end{aligned}$$

   , da jedes J in ($\star$) Teilmengen von $\underline{n}$ sind.
   Andererseits, falls $1 \leq i_1 < \ldots < i_{d_0} \leq n$, so gewählt sind, dass $I \cap K[X_{i_1}, \ldots, X_{i_{d_0}}] = 0$, dann ist die kanonische Abbildung

$$\Pi : K[X_{i_1}, \ldots, X_{i_{d_0}}] \to k[X_1, \ldots, X_n]/I$$

   injektiv und es folgt für alle $s \in \mathbb{N}_0$

$$\begin{aligned} {}^aHP_I(s) = {}^aHF_I(s) &= dim_k((k[X_1, \ldots, X_n]/I)_{\leq s}) \geq dim_k((K[X_{i_1}, \ldots, X_{i_{d_0}}])_{\leq s}) \\ &= \binom{s + d_0}{s} = \frac{s^{d_0} + O(s)}{d_0!} \end{aligned}$$

   Da $grad(\binom{s+d_0}{s}) = d_0$ folgt $grad({}^aHP_I) \geq d_0$. Daraus folgt $grad({}^aHP_I) = d_0$, was zu zeigen war.

$\square$

Beispiel in COX, Kap 9.

Definition 10. *Sei $V \subset k^n$ eine algebraische Menge und ${}^a HP_{I(V)}(t)$ ist das Hilbert-Polynom von $I(V) \trianglelefteq k[X_1, \ldots, X_n]$ (nach Satz 9 ist wohldefiniert und eindeutig). Für $V \neq \emptyset$ (d.h. $I(V) \neq k[X_1, \ldots, X_n]$), wird die Dimension definiert als*

$$dim(V) = grad({}^a HP_{I(V)}).$$

Eine etwas handlichere Charakterisierung ist nach Satz 9 durch:

$$dim(I(V)) = \max \{d \in \underline{n} : \exists\, 1 \leq i_1 < \ldots < i_d \leq n \text{ mit } I \cap K[X_{i_1}, \ldots, X_{i_d}] = \{0\}\}$$

gegeben.

Beispiel 1.2.6 in der Ausabeitung.[TODO]

c) Behauptung: Sei $V \subset k^n$ algebraisch und $W \subseteq V$ eine abgeschlossene Teilmenge. Dann gilt $dim(W) \leq dim(V)$.

Beweis. Sei $I(V) \subset k[X_1, \ldots, X_n]$ und $I(W) \subset k[X_1, \ldots, X_n]$. Da $W \subseteq V$ gilt

$\Rightarrow I(V) \subseteq I(W)$

$\Rightarrow I(V)_{\leq s} \subseteq I(W)_{\leq s}$

$\Rightarrow {}^a HF_{I(V)}(s) = dim_k((k[X_1, \ldots, X_n]/I(V))_{\leq s}) \geq dim_k((k[X_1, \ldots, X_n]/I(W))_{\leq s}) = {}^a HF_{I(W)}(s), \ \forall s \in \mathbb{N}_0$

$\Rightarrow {}^a HP_{I(V)}(s) \geq {}^a HP_{I(W)}(s), \ \forall s \in \mathbb{N}_0$

$\overset{\text{Wachstum Argument für Polynome}}{\Rightarrow} grad({}^a HP_{I(V)}) \geq grad({}^a HP_{I(W)})$

$\overset{\text{Definition}}{\Rightarrow} dim(I(V)) \geq dim(I(W))$

$\square$

Daraus lässt sich erkennen, dass die obige Definition der Dimension einer affine-Varietät und seinem Analogon für k-Vektorräume gewisse Ähnlichkeiten aufweisen, denn das obige Ergebnis für k-Vektorräume bekanntlich gilt. Die folgende Proposition jedoch hebt den ersten Unterschied zwischen diesen beiden Strukturen hervor und lautet

Proposition 11. *Sei $V \subseteq k^n$ algebraisch und $V = \bigcup_{i \in \underline{r}} V_i$ eine Zerlegung in irreduziblen Komponenten (vgl. Proposition 1.1.11). Dann gilt*

$$dim(V) = \max \{dim(V_i) : i \in \underline{r}\}$$

Beweis. Mit Bsp 1.2.16 c) gilt $dim(V_i) \leq dim(V), \ \forall i \in \underline{r}$. Sei nun $d := dim(V)$. Es gilt mit Satz 9, dass es existiert $1 \leq i_1 < \ldots < i_d \leq n$ mit $I \cap K[X_{i_1}, \ldots, X_{i_d}] = \{0\}$.

Angenommen $dim(V_i) < d, \ \forall i \in \underline{r}$. Daraus folgt $\forall i \in \underline{r}$, dass es existiert $0 \neq F_j \in I(V_j) \cap K[X_{i_1}, \ldots, X_{i_d}]$.

$$\Rightarrow 0 \neq F := \prod_{j=1}^{r} F_j \in \bigcap_{j=1}^{r} I(V_j) \cap K[X_{i_1}, \ldots, X_{i_d}] = I(V) \cap K[X_{i_1}, \ldots, X_{i_d}]$$

$$\Rightarrow I(V) \cap K[X_{i_1}, \ldots, X_{i_d}] \neq (0)$$

Dies ist ein Widerspruch zur Definition von d. Somit gilt die Behauptung.

$\square$

Beispiel: [TODO]

Im Folgenden wollen wir eine andere Charakterisierung von $dim(V)$ angeben.

Definition 12. *Sei A eine $k-$Algebra (kommutativer, assoziativer $k-$Algebra mit 1). Man nennt $a_1, \dots, a_m \in A$ algebraisch unabhängig, falls*

$$\forall\ F \in k[X_1, \dots, X_m]/\{0\} \text{ gilt } F(a_1, \dots, a_m) \neq 0.$$

Man definiert

$$\partial_k(A) := \sup\{m \geq 0 :\ \exists\ m \text{ algebraisch unabhängige Elemente in } A\}$$

Bemerkung: Falls A ein Körper ist, dann nennt man $\partial_k(A)$ der transcendenz Grad von A über k.

Eigenschaften von $\partial_k(A)$: [TODO]

Proposition 13. *Sei $A := k[X_1, \dots, X_n]/I$ mit $I \trianglelefteq k[X_1, \dots, X_n]$ ein echtes Ideal. Dann gilt $grad({}^aHP_I) = \partial_k(A)$. Ist A weiterhin einen Integrietätsbereich (IB) und K ist der Quotienten-Körper von A, dann gilt*

$$grad({}^aHP_I) = \partial_k(A) = \partial_k(K).$$

Insbesondere gilt $dim(V) = \partial_k(A[V])$ für jede nicht-leere algebraische $V \subset k^n$.

Beweis. Sei $[f]$ das Bild von $f \in k[X_1, \dots, X_n]$ unter dem kanonischen Epimorphismus $k[X_1, \dots, X_n] \to A$. Dann gilt

1. Sei $d = grad({}^aHP_I)$. Dann gilt Nach Satz 9 $a)$ gilt $\exists\, 1 \leq i_1 < \ldots < i_d \leq n$ mit $I \cap k[X_{i_1}, \dots, X_{i_d}] = (0)$

$$\begin{aligned} &\Rightarrow\ \forall\ F \in k[Y_1, \dots, Y_d] \setminus \{0\} \text{ gilt } A \ni F([X_{i_1}], \dots, [X_{i_d}]) = [F(X_{i_1}, \dots, X_{i_d})] \neq 0 \in A \\ &\Rightarrow\ \partial_k(A) \geq d \end{aligned}$$

   Insbesondere ist $[X_{i_1}], \dots, [X_{i_d}] \in A$ algebraisch unabhängig in A.

2. Setzt man $R = K$ (falls A ein Integritätsbereich) und $R = A$ sonst. Dann gilt $\partial_k(A) \leq \partial_k(R) =: r$ (da $A \subseteq R$). Wir zeigen nun, dass $d \leq r$ gilt.

   Behauptung: Falls $\phi_1, \dots, \phi_r \in R$ algebraisch unabhängig ist, dann gilt $r \leq d$.

   Beweis. Dazu sei $\phi_i := \frac{[f_i]}{[f]}$ mit $f_i,\ f \in k[X_1, \dots, X_n]$ mit $f \neq 0$ (falls $R = K$) oder $f = 1$ (falls $R = A$). Weiter seien $N = \max\{grad(f), grad(f_1), \dots, grad(f_r)\}$ und $k[Y_1, \dots, Y_r]$ (Y_i sind Variablen) der Polynomring.
   Für $s \geq 0$ beliebig aber fest, konstruieren wir folgende Injektive Abbildung

$$\Lambda : k[Y_1, \dots, Y_r]_{\leq s} \to k[X_1, \dots, X_n]_{\leq Ns}/I_{\leq Ns}$$

   Es gilt für $g \in k[Y_1, \dots, Y_r]_{\leq s}$, dass $f^s g(\frac{f_1}{f}, \dots, \frac{f_r}{f}) \in k[X_1, \dots, X_n]_{\leq Ns}$, da bei jedem Monom in den Variablen $(Y_1, \dots, Y_r)$ von g gilt, dass

$$\begin{aligned} f^s Y^\alpha &= f^s \frac{{f_1}^{\alpha_1} \cdot \ldots \cdot {f_r}^{\alpha_r}}{f^{|\alpha|}} \text{ mit } |\alpha| \leq s \\ &= f^{s-|\alpha|} {f_1}^{\alpha_1} \cdot \ldots \cdot {f_r}^{\alpha_r} \text{ mit } N = \max\{grad(f), grad(f_1), \dots, grad(f_r)\}. \end{aligned}$$

Sei $\beta(g) = f^s g(\frac{f_1}{f}, \ldots, \frac{f_r}{f}) + I_{\leq Ns}$. Wir zeigen nun, dass β injektiv ist. Dazu sei $g \in k[Y_1, \ldots, Y_r]_{\leq s}$, sodass $f^s g(\frac{f_1}{f}, \ldots, \frac{f_r}{f}) \in I_{\leq Ns} \subset I$. In R bedeutet dies

$$\begin{aligned} [f]^s g(\phi_1, \ldots, \phi_r) = 0 &\overset{[f]\neq 0, R\ IB}{\Rightarrow} g(\phi_1, \ldots, \phi_r) = 0 \\ &\overset{f_i, f \neq 0 \in k[X_1,\ldots,X_n] \text{ bel gewählt}}{\Rightarrow} g = 0 \\ &\Rightarrow \beta \text{ ist injektiv} \end{aligned}$$

Also ${}^a HP_I(Ns) \geq dim_k(k[Y_1, \ldots, Y_r]_{\leq s}) = \binom{r+s}{r} = \frac{(r+s)(r+s-1).....(s+1)}{r!}$, für alle $s \in \mathbb{N}_0$. Für s groß genug gilt ${}^a HP_I(Ns) = O(s^d)$ und $\binom{r+s}{r} = O(s^r)$. Daraus folgt $d \geq r$. □

Also insgesamt gilt $d = r$ und somit $grad({}^a HP_I) = \partial_k(A) = \partial_k(K)$ sowie $dim(V) = \partial_k(A[V])$ mit $A[V]/I(V)$ für beliebige $V \subset k^n$.

□

Beispiel in Ausarbeitung:[TODO]

In Bsp 1.2.6 c) wurde gezeigt, dass für $V \subseteq k^n$ algebraisch und $W \subseteq V$ abgeschlossene Teilmenge ist: $dim(W) \leq dim(V)$. Das folgende Lemma verschärft diese Aussage für irreduziblen algebraischer Mengen.

Lemma 14. *Sei $V \subseteq k^n$ irreduzible algebraischer Menge und $W \subseteq V$ abgeschlossenen Teilmenge. Dann gilt $dim(W) < dim(V)$, falls W echte Teilmenge von V ist.*

Beweis. Es gilt wegen Bsp 1.2.16 c), dass $dim(W) \leq dim(V)$. Angenommen es gelte $d := dim(W) = dim(V)$. Dann gilt $I(V) \subsetneq I(W)$ mit (1.1.7). Sei $0 \neq f \in I(W) \setminus I(V)$. Mit Satz 9 gilt, dass es $i_1, i_2, i_3, \ldots, i_d \in \mathbb{N}$ mit $1 \leq i_1 < \ldots < i_d \leq n$ mit $I(W) \cap K[X_{i_1}, \ldots, X_{i_d}] = (0)$ existieren. Mit Proposition.9.1 gilt weiterhin, dass $[X_{i_1}], \ldots, [X_{i_d}] \in A[W]$ algebraisch unabhängig in $A[W]$ ist. Nun gilt $f, X_{i_1}, \ldots, X_{i_d}$ kann nicht mehr algebraisch unabhängig sein modulo $I(V)$ (Nach Definition von d). D.h. es existiert $0 \neq F \in k[Y, Y_1, \ldots, Y_d]$ sodass $F(f, X_{i_1}, \ldots, X_{i_d}) \in I(V)$. Da V irreduzibel ist, gilt $I(V)$ ist ein Primideal. Man kann also annehmen, dass $F \in k[Y, Y_1, \ldots, Y_d]$ ist irreduzibel. Schreibt man F wie folgt,

$$F(Y, Y_1, \ldots, Y_d) = \sum_{i=0}^{r} F_i Y^i, \text{ mit } F_i \in k[Y_1, \ldots, Y_d].$$

Es gilt, da F irreduzibel ist, dass $Y \nmid F$. Daraus folgt $F_0(Y_1, \ldots, Y_d) \neq 0 \in k[Y_1, \ldots, Y_d]$. Nun gilt, da $I(V) \subset I(W)$

$$\begin{aligned} &F_0(X_{i_1}, \ldots, X_{i_d}) + I(W) = F(f, X_{i_1}, \ldots, X_{i_d}) + I(W) = I(W) \\ &\Rightarrow\ F_0(X_{i_1}, \ldots, X_{i_d}) + I(W) = I(W) \\ &\Rightarrow\ F_0([X_{i_1}], \ldots, [X_{i_d}]) \in A[W] \\ &\Rightarrow\ [X_{i_1}], \ldots, [X_{i_d}] \in A[W] \text{ ist nicht algebraisch unabhängig in } A[W], \text{ da } F_0(Y_1, \ldots, Y_d) \neq 0 \text{ (Widerspruch)} \end{aligned}$$

Also unsere Annahme muss falsch gewesen sein und es gilt $dim(V) > dim(W)$ □

Literatur

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

[2] Udo Kamps, Erhard Cramer : *Grundzüge der Stochastik, Skript für Bachelorstudierende.* 2. Aufl. §3, Seite 36

[3] Geck, Meinolf: *An introduction to algebraic geometry and algebraic groups* Clarendon Press - Oxford, 2003