Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 15. Februar 2022

Inhaltsverzeichnis

Buch zur Vorlesung: Die Vorlesung orientiert sich am Buch

D. A. Cox, J. Little und D. O'Shea (2006). *Ideals, varieties, and algorithms.* 3. Aufl. Undergraduate Texts in Mathematics. Springer.
In der Vorlesung behandelt werden die Kapitel:

1 Geometry, Algebra, and Algorithms

2 Gröbner Bases

3 Elimination Theory

4 **The Algebra–Geometry Dictionary**

5 Polynomial and Rational Functions on a Variety

8 Projective Algebraic Geometry

9 The Dimension of a Variety

1. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 26.10.2021

k sei stets ein Körper.

1 Erinnerung

Definition 1.1. *i) Seien $x_1, ..., x_n$ ($n \in \mathbb{N}$) endlich viele Variablen und $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}_0^n$. Definiere ein Monom (in $x_1, ..., x_n$)*

$$x^\alpha := x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$$

und

$$\text{total deg}(x^\alpha) := |\alpha| := \alpha_1 + ... + \alpha_n$$

ii) Sei k ein Körper. Ein Polynom f (in $x_1, ..., x_n$) ist eine k-linear Kombination von Monomen (in $x_1, ..., x_n$) also:

$$f = \sum a_\alpha x^\alpha \tag{1}$$

mit $a_\alpha \in k$ (endlich viele; i.e. die Summe ist endlich).

$$\text{total deg}(f) := \max_{\substack{\alpha \text{ erscheint in (1),} \\ a_\alpha \neq 0}} |\alpha|$$

Notation 1.2. *Sei $n \in \mathbb{N}$.*

i) $k[x_1, ..., x_n]$ ist der Polynomring (in n Variablen mit Koeffizienten in k)

ii) $k^n = \{(a_1, ..., a_n) \mid a_1, ..., a_n \in k\}$ ist der n-dimensionale affine Raum (über k)

Bemerkung 1.3. *Sei $f \in k[x_1, ..., x_n]$, dann induziert f eine Funktion:*

$$\begin{aligned} f\colon \quad & k^n \to k \\ & (a_1, ..., a_n) \mapsto f(a_1, ..., a_n) \end{aligned}$$

Proposition 1.4. *(Satz 3.2 Lineare Algebra 2 SoSe 2020)*
Sei k unendlich und $f \in k[x_1, ..., x_n]$, dann ist $f \equiv 0$ (identisch mit dem Nullpolynom) gdw. die Funktion

$$f\colon k^n \to k$$

die Nullfunktion ist.

Beweis.

„⇒“ Klar.

„⇐“ Per Induktion über n:

Induktionsstart $n = 1$:
Sei $f \in k[x_1]$ mit $\deg f = m \in \mathbb{N}_0$. Wenn $f \not\equiv 0$ gilt, dann hat f höchstens m Nullstellen. Aber wenn $f\colon k \to k$ die Nullfunktion ist, dann hat f unendlich viele Nullstellen (weil k unendlich ist) also ist $f \equiv 0$.

Induktionsannahme:
Es gelte für $(n-1)$ Variablen die Behauptung.

Induktionsschritt:
$n - 1 \mapsto n$: Sei $f \in k[x_1, ..., x_n] \rightsquigarrow k[x_1, ..., x_{n-1}][x_n]$, dann schreibe

$$f = \sum_{i=1}^{N} g_{\mathbf{I}}(x_1, ..., x_{n-1}) x_n^i$$

wobei $g_i \in k[x_1, ..., x_{n-1}]$.
Wir werden zeigen: Wenn $f\colon k^n \to k$ die Nullfunktion ist, dann ist $g_i \equiv 0$ (für alle

$i \in \{1, ..., N\}$).
Sei $(a_1, ..., a_{n-1}) \in k^{n-1}$ (beliebig aber fest) und betrachte $f(a_1, ..., a_{n-1}, x_n) \in k[x_n]$.
Sei $a_n \in k$, dann ist $f(a_1, ..., a_{n-1}, a_n) = 0$.
Also hat $f(a_1, ..., a_{n-1}, x_n) \in k[x_n]$ unendlich viele Nullstellen (da k unendlich ist).
Also ist $f(a_1, ..., a_{n-1}, x_n) \equiv 0$ (nach Induktionsannahme):
Also ist $g_{\mathbf{I}}(a_1, ..., a_{n-1}) = 0$ für alle $i = 1, ..., N$.
Da aber $(a_1, ..., a_{n-1})$ beliebig in k^{n-1} war, ergibt nun unsere Induktionsannahme, dass $g_i \equiv 0$ in $k[x_1, ..., x_{n-1}]$.

□

Korollar 1.5. *Sei k unendlich, $n \in \mathbb{N}$, $f, g \in k[x_1, ..., x_n]$.*
Dann gilt: $f \equiv g$ gdw. f und g ($f, g \colon k^n \to k$) die gleiche Funktion induzieren.

Vorschau auf Übungsblatt 1:

I: Sei $f \in \mathbb{C}[x_1, ..., x_n]$ und betrachte

$$f_{\restriction \mathbb{Z}^n} \colon \mathbb{Z}^n \to \mathbb{C}$$

Zu zeigen: Wenn $f_{\restriction \mathbb{Z}^n}$ die Nullfunktion ist, dann ist $f \equiv 0$.

II: Sei $f \in \mathbb{R}[x_1, x_2]$ und $X = \{(x, x) \mid x \in \mathbb{R}, x \neq 1\} \subset \mathbb{R}^2$.
Zu zeigen: Wenn f auf X verschwindet, dann gilt $f(1, 1) = 0$.

---

2 Affine Varietäten

Sei k ein Körper, $n \in \mathbb{N}$.

Definition 2.1. *Seien $f_1, ..., f_s$ ($s \in \mathbb{N}$) Polynome in $k[x_1, ..., x_n]$.*
Dann ist

$$\mathbf{V}(f_1, ..., f_s) := \{(a_1, ..., a_n) \in k^n \mid \forall i = 1, ..., s \colon f_i(a_1, ..., a_n) = 0\}$$

die durch $f_1, ..., f_s$ definierte Affine Varietät.
Diese Darstellung einer affinen Varietät (durch $f_1, ..., f_s$) heißt implizite Darstellung.

Beispiel 2.2.

- $\emptyset = \mathbf{V}(1)$

- $k^n = \mathbf{V}(0)$
- *Ist* $\{(a_1, ..., a_n)\}$ *eine affine Varietät?*

$$V((x_1 - a_1), ..., (x_n - a_n)) = \{(a_1, ..., a_n)\}$$

- *Die Lösungsmenge eines Linearen Gleichungssystems, für:*

$$S = \begin{cases} a_{11}x_1 + ... + a_{1n}x_n = 0 \\ \quad \vdots \qquad\quad \vdots \\ a_{n1}x_1 + ... + a_{nn}x_n = 0 \end{cases}$$

entspricht

$$\mathcal{L}(S) = \{(a_1, ..., a_n) \in k^n \mid (a_1, ..., a_n) \text{ ist eine Lösung für } S\}$$

Dies ist eine lineare affine Varietät, nämlich $\mathcal{L}(S) = \mathbf{V}(f_1, ..., f_n)$ *mit* $f_i = a_{i1}x_1, + ... + a_{in}x_n$ *für* $i = 1, ..., n$ *(linear weil* $f_1, ..., f_n$ *jeweils den Totalgrad* 1 *haben).*

2. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 28.10.2021

Es folgen nun weitere Beispiele für affine Varietäten.

Beispiel 2.3. *Sei $k = \mathbb{R}$ und $n = 2$.*

i) $\mathbf{V}(x^2 + y^2 - 1)$ *entspricht dem Einheitskreis in der Ebene* $\mathbb{R}^2$ *(Vergleiche Abbildung 2.3)*

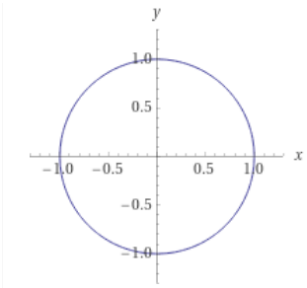


Abbildung 1: $\mathbf{V}(x^2 + y^2 - 1)$

ii) $\mathbf{V}(x^2 + y^2 + 1)$ *ist leer in* $\mathbb{R}^2$.

Allgemein:

iii) Sei $p(x)$ ein Polynom (in $k[x]$). Der Graph von $y = p(x)$ ist $\mathbf{V}(y - p(x))$ in k^2.

iv) Für $y = \frac{x^3-1}{x}$ ist der Graph gegeben durch die affine Varietät $\mathbf{V}(xy - x^3 + 1)$

Beispiele in $\mathbb{R}^3$:

v) $\mathbf{V}(z - x^2 - y^2)$ *entpricht dem in Abbildung 2.3 visualisierten elliptischen Paraboloid.*

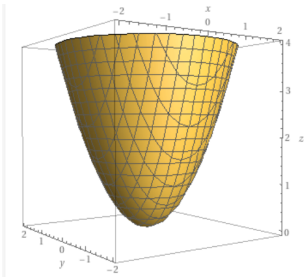


Abbildung 2: $\mathbf{V}(z - x^2 - y^2)$

vi) $\mathbf{V}(z^2 - x^2 - y^2)$ *ist in Abbildung 2.3 visualisiert.*

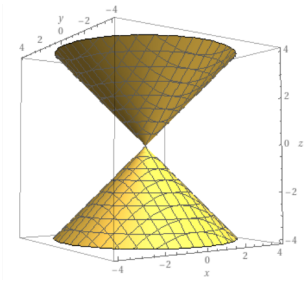


Abbildung 3: $\mathbf{V}(z^2 - x^2 - y^2)$

2.1 Eigenschaften affiner Varietäten

Proposition 2.4. *Seien $V, W \subseteq k^n$ affine Varietäten, dann sind $V \cap W$ und $V \cup W$ affine Varietäten. Genauer: Seien $V = \mathbf{V}(f_1, ..., f_s)$ und $W = \mathbf{V}(g_1, ..., g_t)$, dann gilt:*

$$V \cap W = \mathbf{V}(f_1, ..., f_s, g_1, ..., g_t) \tag{2}$$

$$V \cup W = \mathbf{V}(f_i g_j \colon 1 \leq i \leq s, 1 \leq j \leq t) \tag{3}$$

Beweis.

(2) Klar.

(3) Sei $(a_1, ..., a_n) \in V$, d.h. alle f_i's verschwinden in diesem Punkt. Dann folgt, alle $f_i g_j$ ausgewertet in diesem Punkt verschwinden.

$$V \subseteq \mathbf{V}(f_i g_j \,;\, 1 \leq i \leq s, 1 \leq j \leq t)$$

$$W \subseteq \mathbf{V}(f_i g_j \,;\, 1 \leq i \leq s, 1 \leq j \leq t)$$

Insgesamt folgt somit: $$V \cup W \subseteq \mathbf{V}(f_i g_j \,;\, 1 \leq i \leq s, 1 \leq j \leq t)$$

Umgekehrt:
Sei $(a_1, ..., a_n) \in \mathbf{V}(f_i g_j \,;\, 1 \leq i \leq s, 1 \leq j \leq t)$. Falls $(a_1, ..., a_n) \in V$ gilt, so sind wir fertig. Ansonsten existiert ein i_0 mit:

$$f_{i_0}(a_1, ..., a_n) \neq 0$$

Es gilt nach Annahme bereits: $$(f_i g_j)(a_1, ..., a_n) = 0 \qquad \forall 1 \leq j \leq t$$

Daher: $$g_j(a_1, ..., a_n) = 0 \qquad \forall 1 \leq j \leq t$$

Folglich liegt $(a_1, ..., a_n)$ in W.

□

Bemerkung 2.5. *Es folgt:*

- *Der Schnitt von endlich vielen Varietäten ist eine Varietät*

- *Die Vereinigung von endlich vielen Varietäten ist eine Varietät*

  Insbesondere ist jede endliche Untermenge von k^n eine Varietät

Definition 2.6. *Sei $V = \mathbf{V}(t_1, ..., t_s)$ eine Varietät in k^n. Eine (rationale) parametrische Darstellung (oder Repräsentation) von V, falls existent, ist gegeben durch geeignete $r_1, ..., r_n \in k(t_1, ..., t_m)$ (Erinnerung aus Algebra I + II: $k(t_1, ..., t_n) = ff(k[t_1, ..., t_n]) = Quot(k[t_1, ..., t_n])$) für die aus*

$$\begin{aligned} x_1 &= r_1(t_1, ..., t_m) \\ &\vdots \\ x_n &= r_n(t_1, ..., t_m) \end{aligned}$$

stets $(x_1, ..., x_n) \in V$ folgt.

Beispiel 2.7 (Parametrische Darstellung $\rightsquigarrow$ Implizite Darstellung)**.** *Sei $V_0 = \{(1 + t, 1 + t^2) \mid t \in \mathbb{R}\} \subset \mathbb{R}^2$, dann ist $x = 1 + t$ und damit auch $t = 1 - x$. Eingesetzt in $y = 1 + (1 - x)^2$ ergibt sich $y = x^2 - 2x + 2$. Es folgt:*

$$V_0 = \mathbf{V}(y - x^2 + 2x - 2)$$

Fragen 2.8.

1) *Hat jede affine Varietät eine rationale parametrische Darstellung?*
   Wenn ja, können wir die parametrische Darstellung aus einer gegebenen impliziten Darstellung schlussfolgern?
   D.h. ist eine Folgerung der Art

$$\begin{array}{ccc} f_1 \in k[x_1, ..., x_n] & & r_1 \in k(t_1, ..., t_m) \\ \vdots & \rightsquigarrow & \vdots \\ f_s \in k[x_1, ..., x_n] & & r_n \in k(t_1, ..., t_m) \end{array}$$

   möglich?

2) *Umgekehrt können wir eine implizite Darstellung finden, wenn bereits eine parametrische Darstellung gegeben ist? Ja - Kapitel 2, 3, 4*

Beispiel 2.9.

i) Lineare Algebra: Das LGS (Bemerke, dass jedes LGS eine Varietät beschreibt, vergleiche

Beispiel 2.2). Insbesondere wird das LGS

$$\begin{aligned} x \quad +y \quad +z \quad &= 1 \\ x \quad +2y \quad -z \quad &= 3 \end{aligned}$$

zu

$$\begin{aligned} x \quad +3z \quad &= -1 \\ y \quad -2z \quad &= 2 \end{aligned}$$

Es ergibt sich die parametrische Darstellung

$$\begin{aligned} x &= 1 - 3t \\ y &= 2 + 2t \\ z &= t \end{aligned}$$

ii) Die Varietät $\mathbf{V}(x^2+y^2-1)$ *in* $\mathbb{R}^2$ *hat die parametrische Darstellung* $x = \frac{1-t^2}{1+t^2}$ *und* $y = \frac{2t}{1+t^2}$, *denn:*
Nach den Strahlensätzen (vgl. Abbildung 4) folgt aus $\frac{t-0}{0-(-1)=\frac{y-0}{x-(-1)}}$ *bereits* $t = \frac{y}{x+1}$ *bzw.*

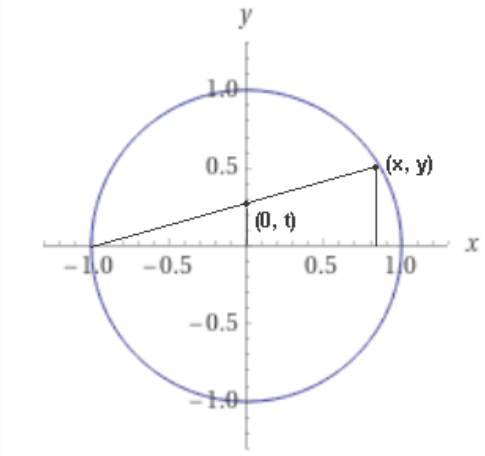


Abbildung 4: Varietät und Strahlensatz

$y = t(x+1)$ $\quad$ $(*)$ *Daher (mit* $x^2+y^2=1$*) impliziert*

$$x^2 + t^2(x+1)^2 = 1 \Rightarrow (1+t^2)x^2 + 2t^2x + (t^2-1) = 0$$

dass $x = (-1)$ *eine Lösung ist. Das Ausklammern von* $(x+1)$ *ergibt nun:*

$$(x+1)[(1+t^2)x - (1-t^2)] = 0$$

Es folgt: $x = \frac{1-t^2}{1+t^2}$.
Setzt man dies in $(*)$ *(genauer in* $y = t(x+1)$*) ein, so folgt* $y = \frac{2t}{1+t^2}$.

2.2 Ideale

§4 Ideals Kapitel 1 im Buch von Cox, Little und O'Shea 2006. Sei $I \trianglelefteq k[x_1, ..., x_n]$ und seien $f_1, ..., f_s \in k[x_1, ..., x_n]$.

Erinnerung: $\langle f_1, ..., f_s \rangle = \{\sum_{i=1}^{s} h_i f_i \colon h_i \in k[x_1, ..., x_n]\}$ ist das von $f_1, ..., f_s$ erzeugte Ideal.

Definition 2.10. *Die Menge $\{f_1, ..., f_s\}$ ist eine Basis für das Ideal I gdw. $I = \langle f_1, ..., f_s \rangle$ gilt.*

Bemerkung 2.11. *Betrachte das System*

$$(*) = \begin{cases} f_1 = 0 \\ \quad \vdots \\ f_s = 0 \end{cases}$$

Nun betrachte das System

$$(**) \sum_{i=1}^{s} h_i f_i = 0 \qquad \forall h_i \in k[x_1, ..., x_n]$$

Dann haben $(*)$ und $(**)$ die gleiche Lösungsmenge in k^n, d.h. $\mathbf{V}(f_1, ..., f_s) = \mathbf{V}(\langle f_1, ..., f_s \rangle)$ ($\mathbf{V}(\cdot)$ kann damit auch sinnvoll auf Idealen [unendlichen Mengen] definiert werden).

Proposition 2.12. *Seien $f_1, ..., f_s$ und $g_1, ..., g_t$ Basen für das Ideal I, d.h.*

$$I = \langle f_1, ..., f_s \rangle = \langle g_1, ..., g_t \rangle$$

Dann gilt $\mathbf{V}(f_1, ..., f_s) = \mathbf{V}(g_1, ..., g_t)$.

Beweis. Wir berechnen $\mathbf{V}(f_1, ..., f_s) \overset{\text{Bmk. 2.11}}{=} \mathbf{V}(\langle f_1, ..., f_s \rangle) = \mathbf{V}(\langle g_1, ..., g_t \rangle) \overset{\text{Bmk. 2.11}}{=} \mathbf{V}(g_1, ..., g_t)$. □

Beispiel 2.13 (Übung 2)**.**

i) $\langle x + y, x - y \rangle = \langle x, y \rangle$

ii) $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$

Definition 2.14. *Sei $V \subseteq k^n$ eine affine Varietät. Dann ist das Verschwindungsideal von V*

definiert als:

$$\mathbf{I}(V) := \{f \in k[x_1, ..., x_n] \mid \forall (a_1, ..., a_n) \in V \colon f(a_1, ..., a_n) = 0\}.$$

Bemerkung 2.15. *Sei* $V = \mathbf{V}(f_1, ..., f_s)$*, dann gilt*

$$\langle f_1, ..., f_s \rangle \subseteq \mathbf{I}(V).$$

Diese Inklusion kann strikt sein. Die genaue Beziehung zwischen V*,* $\langle f_1, ..., f_s \rangle$ *und* $\mathbf{I}(V)$ *wird in Kapitel 4 (Hilbert's Nullstellensatz) thematisiert.*

3. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 02.11.2021

Beispiel 2.16.

i) Betrachte $V = \mathbf{V}(x, y) = \{(0, 0)\} \subseteq k^2$.

Behauptung: $\mathbf{I}(V) = \langle x, y\rangle$.
Wir wissen bereits $\langle x, y\rangle \subseteq \mathbf{I}(V)$. *Sei nun* $f \in k[x, y]$ *so, dass* $f(0, 0) = 0$ *gilt.*
Zu zeigen: $f \in \langle x, y\rangle$
Setze $f = \sum_{i,j} a_{ij}x^i y^j$ $(a_{ij} \in k)$. *Aus* $f(0, 0) = a_{00} = 0$, *folgt:*

$$f = 0 + \sum_{(i,j)\neq(0,0)} a_{ij}x^i y^j = \left(\sum_{\substack{i,j \\ i>0}} a_{ij}x^{i-1}y^j\right) x + \left(\sum_{j>0} a_{0j}x^0 y^{j-1}\right) y \in \langle x, y\rangle$$

ii) Betrachte $V = \mathbf{V}(0) = k^n$ *für* k *unendlich. Dann ist* $\mathbf{I}(V) = \{f \in k[x_1, ..., x_n] \mid f$ *verschwindet auf* $k^n\} = \{0\}$.

iii) $\mathbf{V}(x^2, y^2) = \{(0, 0)\}$.

Behauptung: $\mathbf{I}(V) = \langle x, y\rangle$ ✓ *(siehe i))* ***Aber:*** $\langle x^2, y^2\rangle \subsetneq \langle x, y\rangle$, *weil z B.* $x \notin \langle x^2, y^2\rangle$ *gilt.*

(Sei $f \in \langle x^2, y^2\rangle$ *dann gilt* $f = h_1x^2 + h_2y^2$ *(mit* $h_1, h_2 \in k[x, y]$*), also* $\operatorname{total\deg} f \geq 2$.*)*

iv) $\mathbf{V}(x^2, y^2) = \mathbf{V}(x, y)$ *(siehe iii)) und* $\langle x^2, y^2\rangle \subsetneq \langle x, y\rangle$. *Also gilt die Umkehrung von Proposition 2.12 im Allgemeinen nicht.*

Proposition 2.17. *Seien* V, W *affine Varietäten in* k^n. *Es gilt:*

i) $V \subseteq W$ *gdw.* $\mathbf{I}(V) \supseteq \mathbf{I}(W)$

ii) $V = W$ *gdw.* $\mathbf{I}(V) = \mathbf{I}(W)$

Beweis. Es ist klar, dass *ii*) aus *i*) folgt. Es genügt also *i*) zu zeigen.
Sei $V \subseteq W$ und $f \in \mathbf{I}(W)$ d.h. f verschwindet auf W. A fortiori verschwindet f auch auf V. Es folgt $f \in \mathbf{I}(V)$.
Sei umgekehrt $\mathbf{I}(W) \subseteq \mathbf{I}(V)$.

Sei durch $g_1, ..., g_t \in k[x_1, ..., x_n]$ eine implizite Repräsentation von W beschrieben. Dann gilt $g_1, ..., g_t \in \mathbf{I}(W)$ und daher auch $g_1, ..., g_t \in \mathbf{I}(V)$. In anderen Worten: Jedes g_i verschwindet auf V. Es folgt $V \subseteq W$. □

Fragestellung:

① **Beschreibe** (algorithmisch) die Ideale $I \trianglelefteq k[x_1, ..., x_n]$.
Erinnerung an Hilberts Basissatz (siehe SoSe 2021 B4, Algebra II, 8. Vorlesung): Jedes Ideal I in $k[x_1, ..., x_n]$ ist endlich erzeugt (d.h. $k[x_1, ..., x_n]$ noethersch).

② Entscheide „algorithmisch"ob f in $\langle g_1, ..., g_t \rangle$ liegt.

③ Später: Was ist die Beziehung zwischen $\langle f_1, ..., f_s \rangle$ und $\mathbf{I}(\mathbf{V}(f_1, ..., f_s))$?

Erinnerungen zum Ring $k[x]$ (siehe LA II Skript 3,4,5):

I) Divisionsalgorithmus: Seien $f, g \in k[x]$ mit $g \neq 0$, dann existieren eindeutige $q, r \in k[x]$ mit $f = qg + r$ und $r \equiv 0$ oder $\deg r < \deg g$ (Insbesondere können q und r algorithmisch berechnet werden).

II) $k[x]$ ist ein euklidischer Ring (LA I+II).

III) $k[x]$ ist ein Hauptidealring (folgt aus euklidischer Ring)

IV) Für ein Ideal $I \neq \{0\}$ existiert ein (normiertes) Polynom f von minimalen Grad mit $I = \langle f \rangle$ wobei f minimalen Grad in I hat (und normiert ist).

V) Der ggT$(f_1, ..., f_s)$ kann algorithmisch berechnen werden. Insbesondere ist der ggT$(f_1, ..., f_s)$ ein (Haupt-)Erzeuger von $\langle f_1, ..., f_s \rangle$.

Gelten entsprechende Aussagen in $k[x_1, ..., x_n]$?

3 Gröbnerbasen

Siehe Kapitel II im Buch von Cox, Little und O'Shea 2006.

Monomiale Anordnungen:

Definition 3.1. *Eine monomiale Anordnung $>$ auf $k[x_1, ..., x_n]$ ist eine Ordnungsrelation auf $\mathbb{N}_0^n$ (oder auf $\{x^\alpha \mid \alpha \in \mathbb{N}_0^n\} = \{x_1^{\alpha_1} ... x_n^{\alpha_n} \mid (\alpha_1, ..., \alpha_n) \in \mathbb{N}_0^n\}$) mit:*

i) $>$ ist eine totale Anordnung

ii) Für alle $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ mit $\alpha > \beta$ folgt $\alpha + \gamma > \beta + \gamma$

iii) $>$ ist eine Wohlordnung.

Erinnerung: *Eine total angeordnete Menge $(S, >)$ ist wohlgeordnet falls folgende Bedingung erfüllt ist:*

> *Jedes $A \subseteq S$, $A \neq \emptyset$ hat ein kleinstes Element, d.h. es existiert ein $a_0 \in A$ mit $a_0 \leq a$ für alle $a \in A$.*

Lemma 3.2. *$(S, >)$ ist wohlgeordnet genau dann, wenn es **keine unendliche strikt absteigende** Folge in S gibt, d.h. eine Folge $s_1 > s_2 > ...$ in S terminiert nach endlich vielen Gliedern.*

Beweis.

„⇐“ Wenn $(S, >)$ keine Wohlordnung ist, dann nehme eine Teilmenge $A \subseteq S, A \neq \emptyset$ die **kein kleinstes Element besitzt**.
Sei $a_1 \in A$ beliebig, dann wähle $a_2 \in A$ so, dass $a_1 > a_2 > ...$ gilt. Iterativ liefert dies eine unendliche strikt absteigende Folge $a_1 > a_2 > a_3 > ....$

„⇒“ Sei $s_1 > s_2 > ...$ eine unendliche strikt absteigende Folge in S, dann ist die Menge $A := \{s_i \mid i \in \mathbb{N}\} \subseteq S$ nicht-leer und besitzt kein kleinstes Element.

□

Definition 3.3 (Lexikographische Ordnung auf $\mathbb{N}_0^n$)**.** *Seien $\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}_0^n$, dann definiere $\alpha >_{lex} \beta$ genau dann, wenn die erste ungleich-Null-Komponente des Vektors $\alpha - \beta$ positiv ist.*

4. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 04.11.2021

Beispiel 3.4. *Die lexikographische Ordnung aus (Definition 3.3) kann man durch* $x^\alpha >_{lex} x^\beta :\Leftrightarrow \alpha >_{lex} b$ *direkt auf* $\{x^\alpha \mid \alpha \in \mathbb{N}_0^n\}$ *übertragen.*

ⓐ *Wie sind die Variabeln in der lexikographischen Ordnung (*$>_{lex}$*) angeordnet?*

$$\begin{array}{cccccccc} \textit{Es gilt} & x_1 & >_{lex} & x_2 & >_{lex} & \ldots & >_{lex} & x_n, \\ \textit{da} & (1,0,...,0) & >_{lex} & (0,1,0,...,0) & >_{lex} & \ldots & >_{lex} & (0,...,1). \end{array}$$

ⓑ $x_1x_2^2 >_{lex} x_2^3x_3^4$

ⓐ $x_1^3x_2^2x_3^4 >_{lex} x_1^3x_2^2x_3^1$

Lemma 3.5. *Die Relation* $>_{lex}$ *auf* $\mathbb{N}_0^n$ *ist eine monomiale Anordnung.*

Beweis. Per Induktion nach n.

$$\mathbb{N}_0^n = \{(\alpha_1,...,\alpha_n) \mid \alpha_i \in \mathbb{N}_0\}$$

entspricht

$$\mathbb{N}_0^{n-1} \times \mathbb{N}_0 = \{(\alpha_1,...,\alpha_{n-1},\alpha_n) \mid (\alpha_1,...,\alpha_{n-1}) \in \mathbb{N}_0^{n-1}, \alpha_n \in \mathbb{N}_0\}$$

Dann gilt für alle $(\alpha_1,...,\alpha_n),(\beta_1,...,\beta_n) \in \mathbb{N}_0^n$:
$(\alpha_1,...,\alpha_n) >_{lex} (\beta_1,...,\beta_n)$ genau dann, wenn $((\alpha_1,...,\alpha_{n-1}),\alpha_n) >_{lex} ((\beta_1,...,\beta_{n-1}),\beta_n)$.

Induktionsstart $n = 2$:
Betrachte $\mathbb{N}_0^2$.
Für $(a,b),(c,d) \in \mathbb{N}_0^2$ gilt:

$(a,b) <_{lex} (c,d)$ gdw. $a < c$ oder $a = c$ und $b < d$.

Wir prüfen ob $i),ii)$ und $iii)$ (siehe Definition 3.1) gelten:

i) $>_{lex}$ auf $\mathbb{N}_0^2$ ist eine **totale** Anordnung (ÜA)

ii) Klar (ÜA)

iii) $(\mathbb{N}_0^2, >_{lex})$ ist wohlgeordnet:
Sei $S \subseteq \mathbb{N}_0^2, S \neq \emptyset$.

Betrachte $\pi_1 : S \to \mathbb{N}_0$, $(a,b) \mapsto a$ (Bemerke $\pi_1(S) \neq \emptyset$ und $\pi_1(S) \subseteq \mathbb{N}_0$).
Sei $a_0 \in \mathbb{N}_0$ das kleinste Element in $\pi_1(S)$.
Betrachte die Menge $S' = \{(a_0, b) \mid (a_0, b) \in S\} \neq \emptyset$.
Definiere nun analog $\pi_2(S')$ $\pi_2 : S \to \mathbb{N}_0$, $(a,b) \mapsto b$ (wieder gilt $\pi_2(S') \neq \emptyset$, $\pi_2(S) \subseteq \mathbb{N}_0$) und betrachte folgende Untermenge von $\mathbb{N}_0$:

$$\pi_2(S') = \{b \mid (a_0, b) \in S'\} \neq 0$$

Sei b_0 das kleinste Element dieser Menge:
Behauptung: $(a_0, b_0) \in S$ ist das kleinste Element bezüglich $>_{lex}$:

Sei $(a,b) \in S$. Zu zeigen: $(a_0, b_0) \leq_{lex} (a,b)$.

Fall 1: $a = a_0$, dann ist $(a,b) \in S'$ und damit $b_0 \leq b$ (per Wahl von b_0). Wenn $b_0 = b$ gilt, dann folgt $(a,b) = (a_0, b_0)$ und wir sind fertig. Ansonsten gilt bereits $b_0 < b$ und wir sind erneut fertig.

Fall 2: Per Wahl von a_0 haben wir $a_0 \leq a$, daher gilt nun insbesondere $a_0 < a$. Also ist $(a_0, b_0) <_{lex} (a,b)$.

Induktionsannahme: $(\mathbb{N}_0^{n-1}, >_{lex})$ ist eine Wohlordnung.
Induktionsschritt: Zu zeigen: $(\mathbb{N}_0^n, >_{lex})$ ist eine Wohlordnung (ÜA). □

Definition 3.6. *Sei $>$ eine monomiale Anordnung auf $k[x_1, ..., x_n]$ und sei $f = \sum_\alpha a_\alpha x^\alpha$ ($a_\alpha \in k, \alpha \in \mathbb{N}_0^n$, $a_\alpha = 0$ alle bis auf endlich viele)*

i) Der Multigrad von f ist

$$\operatorname{multi\,deg}(f) = \max_{bzgl.\ >} (\{\alpha \in \mathbb{N}_0^n \mid a_\alpha \neq 0\})$$

ii) Der Leitkoeffizient von f ist

$$\operatorname{LC}(f) = a_{\operatorname{multi\,deg}(f)} \in k^\times$$

ii) Das Leitmonom von f ist

$$\operatorname{LM}(f) = x^{\operatorname{multi\,deg}(f)}$$

ii) Der Leitterm von f ist

$$\operatorname{LT}(f) = \operatorname{LC}(f) \operatorname{LM}(f)$$

Bemerkung 3.7. *Gegeben sei eine monomiale Anordnung $>$, dann wurde soeben der entsprechende Multigrad definiert.*
Warum arbeiten wir nicht mit $\operatorname{total\,deg}(f)$*?*
Die Idee vom Divisionsalgorithmus, schon bei $k[x]$ war, dass für den Rest r stets $\deg(r) < \deg(g)$

oder $r = 0$ gilt. Das Analogon soll nun im multivariablen Fall unter Verwendung der monomialen Anordnung $>$ und dem Multigrad betrachtet werden.

Beispiel 3.8.

$$\begin{array}{ccccc} & x^2yz^3 & & xy^2z^3 \\ \text{total deg}: & |(2,1,3)| = & 6 & = |(1,2,3)| \\ lex: & (2,1,3) & >_{lex} & (1,2,3) \end{array}$$

Definition 3.9 (Graduierte lexikographische Ordnung auf $\mathbb{N}_0^n$)**.** *Seien $\alpha, \beta \in \mathbb{N}_0^n$, setze $\alpha >_{gr\,lex} \beta$ genau dann, wenn $|\alpha| > |\beta|$ oder $|\alpha| = |\beta|$ und $\alpha >_{lex} \beta$ gilt (Englisch: Graded lexicographic).*

Lemma 3.10. *$>_{gr\,lex}$ ist eine monomiale Anordnung.*

Beweis. ÜA. □

Beispiel 3.11. *Es ist $x_1 >_{gr\,lex} x_2 >_{gr\,lex} ... >_{gr\,lex} x_n$.*

Definition 3.12.

i) Umgekehrt lexikographische Anordnung auf $\mathbb{N}_0^n$ (reverse lexicographic): Vergleiche nach „letzter Differenz " (statt nach erster, vergleiche Definition 3.3). Schreibe $>_{rev\,lex}$.

ii) Graduiert umgekehrte lexikographische Anordnung auf $\mathbb{N}_0^n$ (graded reverse lexicographic): Für $\alpha, \beta \in \mathbb{N}_0^n$ gilt $\alpha >_{gr\,rev\,lex} \beta$ gdw. $|\alpha| > |\beta|$ oder $|\alpha| = |\beta|$ und $\alpha >_{rev\,lex} \beta$.

Eigenschaften des Multigrades:
Seien $f, g \in k[x_1, ..., x_n]$ mit $f, g \not\equiv 0$, dann gilt

i) $\text{multi deg}(fg) = \text{multi deg}(f) + \text{multi deg}(g)$

ii) Wenn $f + g \not\equiv 0$, dann gilt $\text{multi deg}(f + g) \leq \max(\text{multi deg}(f), \text{multi deg}(g))$

iii) Wenn $\text{multi deg}(f) \neq \text{multi deg}(g)$ und $f + g \not\equiv 0$, dann gilt die Gleichheit in *ii*)

$$\text{multi deg}(f + g) = \max(\text{multi deg}(f), \text{multi deg}(g))$$

3.1 Divisionsalgorithmus in $k[x_1, ..., x_n]$

§3 Divisionsalgorithmus in $k[x_1, ..., x_n]$, Kapitel 2 im Buch von Cox, Little und O'Shea 2006
Ziel: Gegeben $f \in k[x_1, ..., x_n]$ und $f_1, ..., f_s \in k[x_1, ..., x_n]$, es soll nun f „durch $f_1, ..., f_s$ geteilt

“ werden. D.h. geeignete „Quotienten “ $a_1, ..., a_s \in k[x_1, ..., x_n]$ und ein „Rest “ $r \in k[x_1, ..., x_n]$ sollen gefunden werden, sodass:

$$f = a_1 f_1 + ... + a_s f_s + r \tag{4}$$

gilt und r erfüllt dabei noch weitere Eigenschaften. Insbesondere soll bestimmt werden, wann genau $r \equiv 0$ erfüllt ist.

Satz 3.13 (Divisionsalgorithmus)**.** *Sei* $>$ *eine monomiale Anordnung auf* $\mathbb{N}_0^n$
und $F = (f_1, ..., f_s)$ *ein* s*-Tupel von ungleich Null Polynomen in* $k[x_1, ..., x_n]$ *und* $f \in k[x_1, ..., x_n]$*. Dann existieren* $a_1, ..., a_s, r \in k[x_1, ..., x_n]$ *so, dass Gleichung (4) gilt, wobei* $r = 0$ *gilt oder* r *eine* k*-lineare Kombination von nicht durch* $\mathrm{LT}(f_i)$ *teilbaren Monomen ist* $(i = 1, ..., s)$*.*
Darüber hinaus gilt $\mathrm{multi\,deg}(f) \geq \mathrm{multi\,deg}(a_i f_i)$ *für alle* $i = 1, ..., s$*.*

5. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 09.11.2021

Beispiel 3.14. *Es gelte* $x >_{lex} y$.

i) Seien $f = xy^2 + 1$, $f_1 = xy + 1$ *und* $f_2 = y + 1$. *Wir bestimmen* a_1, a_2 *und* r *so, dass Gleichung (4) gilt.*
Wir starten:

$$\begin{array}{lll|l|l} a_1\text{:} & & & & \\ a_2\text{:} & & & & \\ f_1\text{:} & xy+1 & & xy^2+1 & P \\ f_2\text{:} & y+1 & & & \end{array}$$

Es ist $\mathrm{LT}(f_1) = xy$, $\mathrm{LT}(f_2) = y$ *und* $\mathrm{LT}(f) = xy^2$.
Also $\mathrm{LT}(f)$ *ist teilbar durch* $\mathrm{LT}(f_1)$ *und durch* $\mathrm{LT}(f_2)$.
Da f_1 *zuerst gelistet ist, fangen wir damit an, dass* xy^2 *geteilt durch* xy *bereits* y *ergibt.*
Nun können wir yf_1 *von* f *abziehen und erhalten das folgende Tableau:*

$$\begin{array}{lll|l|l} a_1\text{:} & y & & & \\ a_2\text{:} & & & & \\ \hline f_1\text{:} & xy+1 & & xy^2+1 & P \\ f_2\text{:} & y+1 & & -\ \underline{xy^2+y} & \\ & & & -y+1 & P \end{array}$$

Der $\mathrm{LT}(-y+1) = -y$ *ist nur durch* $\mathrm{LT}(f_2) = y$ *teilbar und*
$-y$ *geteilt durch* y *ergibt* -1.
Somit können wir $(-1)f_2$ *abziehen und erhalten folgendes Tableau:*

$$\begin{array}{lll|l|l} a_1\text{:} & y & & & \\ a_2\text{:} & -1 & & & \\ \hline f_1\text{:} & xy+1 & & xy^2+1 & P \\ f_2\text{:} & y+1 & & -\ \underline{xy^2+y} & \\ & & & -y+1 & P \\ & & & -\ \underline{-y-1} & \\ & & & 2 & P \end{array}$$

Die Leitterme $\mathrm{LT}(f_1)$, $\mathrm{LT}(f_2)$ *teilen* 2 *nicht, also setze* $r := 2$.
Es gilt

$$f = xy^2 + 1 = y(xy + 1) + (-1)(y + 1) + 2 = a_1 f_1 + a_2 f_2 + r$$

Vergleiche mit Gleichung (4).

ii) Seien $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ *und* $f_2 = y^2 - 1$. *Betrachte das Tableau*

a_1:	$x+y$		
a_2:			
f_1:	$xy-1$	$x^2y + xy^2 + y^2$	P
f_2:	y^2-1	$-\ \underline{x^2y - x}$	
		$xy^2 + x + y^2$	P
		$-\ \underline{xy^2 - y}$	
		$x + y^2 + y$	P

Obwohl $\mathrm{LT}(f_1) \not| \mathrm{LT}(x + y^2 + y)$ *und* $\mathrm{LT}(f_2) \not| \mathrm{LT}(x + y^2 + y)$ *ist* $P = x + y^2 + y$ *nicht der geeignete Rest, weil* $\mathrm{LT}(f_2) | y^2$ *gilt.*

a_1:	$x+y$			
a_2:	1			
f_1:	$xy-1$	$x^2y + xy^2 + y^2$	P	
f_2:	y^2-1	$-\ \underline{x^2y - x}$		
		$xy^2 + x + y^2$	P	
		$-\ \underline{xy^2 - y}$		
		$\underline{x + y^2 + y}$		$r = x$
		$y^2 + y$	P	
		$-\ \underline{y^2 - 1}$		
		$\underline{y + 1}$		$r = x + y$
		$\underline{1}$		$r = x + y + 1$

Es gilt

$$f = x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1(y^2-1) + (x+y+1) = a_1f_1 + a_2f_2 + r$$

Vergleiche mit Gleichung (4).

Satz 3.13 (Divisionsalgorithmus).
Sei $>$ *eine monomiale Anordnung auf* $\mathbb{N}_0^n$
und $F = (f_1, ..., f_s)$ *ein s-Tupel von ungleich Null Polynomen in* $k[x_1, ..., x_n]$ *und* $f \in k[x_1, ..., x_n]$.
Dann existieren $a_1, ..., a_s, r \in k[x_1, ..., x_n]$ *so, dass Gleichung (4) also die Gleichung*

$$f = a_1, f_1 + ... + a_sf_s + r$$

gilt, wobei $r = 0$ *gilt oder* r *eine* k*-lineare Kombination von nicht durch* $\mathrm{LT}(f_i)$ *teilbaren Monomen ist* $(i = 1, ..., s)$.
Darüber hinaus gilt $\mathrm{multi\,deg}(f) \geq \mathrm{multi\,deg}(a_if_i)$ *für alle* $i = 1, ..., s$.

Beweis. Für $k \in \mathbb{N}_0$ werden wir per Induktion folgende Folgen definieren:

- Eine Folge $(P_k)_{k\in\mathbb{N}_0}$ von Polynomen, sodass die Multigrade strikt absteigen (d.h. $\text{multi deg}(P_{k+1} < \text{multi deg}(P_k)$ für alle $k \in \mathbb{N}_0$).
- Eine Folge $(r_k)_{k\in\mathbb{N}_0}$ von Polynomen in $k[x_1, ..., x_n]$ bei der kein Term von r_k durch die Leitterme $\text{LT}(f_i)$ teilbar ist $(i = 1, ..., s)$.
- $(i_k)_{k\in\mathbb{N}_0}$ und $(a_k)_{k\in\mathbb{N}_0}$ so, dass

  $(*)_k \qquad f = P_k + r_k + a_1 f_{i_1} + ... + a_{k-1} f_{i_{k-1}}$

  erfüllt ist.

  Induktionsanfang: $k = 0$.
  Setze $P_0 = f$, $r_0 = 0$, dann treffen obige Eigenschaften offensichtlich zu.

  Induktionsannahme:
  Die oben gegebenen Angaben gelten für k.

  Induktionsschritt: $(k \to k + 1)$.

Fall 1: Kein Term von P_k ist teilbar durch $\text{LT}(f_i)$ (für alle $i = 1, ..., s$). Setze $r := P_k + r_k$ ■.

Fall 2: Sei ein Term von P_k durch ein $\text{LT}(f_i)$ teilbar (für ein $i \in \{1, ..., s\}$).
Schreibe

$$P_k = m_1 + ... + m_j + m_{j+1} + ... + m_l$$

als Summe von Monomen mit $m_1 > m_2 > ... > m_l$ und $m_1, ..., m_j$ seien nicht durch $\text{LT}(f(i))$ (für alle $i = 1, ..., s$) teilbar, aber es existiert ein $i_k \in \{1, ..., s\}$ mit m_{j+1} ist durch $\text{LT}(f_{i_k})$ teilbar. **Setze:**

$$\begin{aligned} r_{k+1} &:= (m_1 + ... + m_j) + r_k && (\dagger) \\ a_k &:= \frac{m_{j+1}}{\text{LT}(f_{i_k})} \\ P_{k+1} &:= P_k - (m_1 + ... + m_j + a_k f_{i_k}) && (\ddagger) \end{aligned}$$

Beh. 1: Mit diesen Angaben ist $(*)_{k+1}$ erfüllt.
Beh. 2: $\text{multi deg}\, P_{k+1} < \text{multi deg}\, P_k$
Beweis von Beh. 1: Aus † und ‡ folgt

$$P_{k+1} + r_{k+1} + (a_k f_{i_k}) = P_k + r_k$$

$$\begin{array}{rcl} P_{k+1} & + & P_k - (m_1 + ... + m_j + a_k f_i) \quad + \\ r_{k+1} & + \text{ entspricht der Summe} & (m_1 + ... + m_j) + r_k \quad + . \\ a_k f_{i_k} & & a_k f_{i_k} \end{array}$$

(denn die Summe

Das ergibt $P_k + r_k$)

Nun gilt per Induktionsannahme $(*)_k$, d.h.:

$$f = P_{k+1} + r_{k+1} + (a_1 f_{i_1} + ... + a_{k-1} f_{i_{k_1}}) + a_k f_{i_k}$$

Also gilt $(*)_{k+1}$, $\square_{Beh.1}$
Beweis von Beh. 2: Es gilt (wegen † und ‡) $\mathrm{LT}(a_k f_{i_k}) = m_{j+1}$ und
$\mathrm{LT}(P_k - m_1 - ... - m_j) = m_{j+1}$.
Also ist:

$$\text{multi deg}(\mathrm{LT}(P_k - m_1 - ... - m_j) - \mathrm{LT}(a_k f_{i_k})) < \text{multi deg}(P_k - m_1 - ... - m_j) \leq \text{multi deg}(P_k) \square_{Beh.2}$$

(ÜA): Für $i = 1, ..., s$ gilt $\text{multi deg}(a_i f_i) \leq \text{multi deg}(f)$. $\square$

Beispiel 3.15. *Erneute Betrachtung des Beispiels 3.14 mit $x >_{lex} y$.*
Seien $f = x^2y + xy^2 + y^2$, $f_1 = y^2 - 1$ und $f_2 = xy - 1$. Dies liefert das Tableau

a_1:	$x+1$			
a_2:	x			
f_1:	y^2-1	$x^2y + xy^2 + y^2$	P	
f_2:	$xy-1$	$- \quad \underline{xy^2 - x}$		
		$x^2y + x + y^2$	P	
		$- \quad \underline{x^2y - x}$		
		$2x + y^2$		$r = 2x$
		y^2	P	
		$- \quad \underline{y^2 - 1}$		
		1		$r = 2x + 1$

Es gilt:

$$f = x^2y + xy^2 + y^2 = (x+1)(y^2-1) + x(xy-1) + (2x+1) = a_1 f_1 + a_2 f_2 + r$$

Vergleiche mit Gleichung (4).
Im Buch von Cox, Little und O'Shea 2006, Beispiel 5 (Kapitel 2, §3, S. 68) ergibt sich einmal $r = 0$ und einmal $r \neq 0$ ($r = -x + y$).

6. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 11.11.2021

Monomiale Ideale und Dicksons Lemma

Vergleiche §4 Monomiale Ideale und Dicksons Lemma, Kapitel 2 im Buch von Cox, Little und O'Shea 2006.

Definition 3.16. *Ein Ideal $I \trianglelefteq k[x_1, ..., x_n]$ heißt monomial, wenn $I = \langle x^\alpha \mid \alpha \in A\rangle$ mit $A \subseteq \mathbb{N}_0^n$ (A darf unendlich sein) gilt.*
D.h.

$$I = \{\sum_{\alpha \in A} h_\alpha x^\alpha \mid h_\alpha \in k[x_1, ..., x_n] \text{ mit } h_\alpha = 0 \text{ bis auf endlich viele}\}$$

Notation: Sei $I \trianglelefteq k[x_1, ..., x_n]$ und setze

$$\mathrm{Mon}(I) := \{x^\beta \mid \beta \in \mathbb{N}_0^n;\ x^\beta \in I\}$$

Bemerkung 3.17. *Wenn $I = \langle x^\alpha \mid \alpha \in A\rangle$ mit $A \subseteq \mathbb{N}_0^n$, dann ist $\{x^\alpha \mid \alpha \in A\} \subseteq \mathrm{Mon}(I)$.*

Lemma 3.18. *Sei $I = \langle x^\alpha \mid \alpha \in A\rangle$ ein monomiales Ideal und x^β ein Monom ($\beta \in \mathbb{N}_0^n$).*
Dann gilt $x^\beta \in I$ genau dann, wenn ein $\alpha \in A$ existiert so, dass x^α bereits x^β teilt (d.h. es existiert ein $\gamma \in \mathbb{N}_0^n$ mit $x^\beta = x^\alpha x^\gamma$).
Insbesondere

$$\mathrm{Mon}(I) = \{x^\beta \mid \beta \in \mathbb{N}_0^n \colon\ \exists \gamma \in \mathbb{N}_0^n\, \exists \alpha \in A, \beta = \alpha + \gamma\}$$

Beweis.

„⇐“ Klar (nach Definition).

„⇒“ Sei nun $x^\beta \in I$ mit geeignetem $\beta \in \mathbb{N}_0^n$.
Dann kann man x^β schreiben als

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i} \qquad (*)$$

mit $h_i \in k[x_1, ..., x_n]$ und $\alpha_1, ..., \alpha_s \in A$.
Insbesondere kann das Polynom h_i als k-lineare Kombination von Monomen geschrieben

werden.
Setzt man diese k-lineare Kombination in die rechte Seite der Gleichung $(*)$ ein, so sieht man, dass insbesondere jeder Term auf der rechten Seite in der Gleichung $(*)$ durch das Monom $x^(a_i)$ für ein geeignetes $i \in \{1, ..., s\}$ teilbar ist. Dies gilt somit auch für die linke Seite der Gleichung $(*)$, d.h. insbesondere ist x^beta durch $x^(a_i)$ für ein geeignetes i mit $\alpha_i \in A$ teilbar.

□

Lemma 3.19. *Sei $I = \langle x^\alpha \mid \alpha \in A \rangle$ ein monomiales Ideal und $f \in k[x_1, ..., x_n]$.*
Folgende Aussagen sind äquivalent:

i) $f \in I$

ii) *Jeder Term von f liegt in I*

iii) *f ist eine k-lineare Kombination von Monomen aus I*

Beweis. *iii)* $\Rightarrow$ *ii)* $\Rightarrow$ *i)* sind klar.
Wir zeigen daher noch *i)* $\Rightarrow$ *ii)* $\Rightarrow$ *iii)*.
Die Implikation *ii)* $\Rightarrow$ *iii)* ist dabei ebenfalls klar.
Zu zeigen *i)* $\Rightarrow$ *ii)*:
Wir werden die folgende, allgemeinere Aussage beweisen:

> Wenn $f \in I$ gilt, dann ist jeder Term von f durch ein Monom x^α (für ein geeignetes $\alpha \in A$) teilbar.

Schreibe dazu

$$f = \sum_{i=1}^{k} h_i x^{\alpha_i} \qquad \text{mit geeigneten } h_i \in k[x_1, ..., x_n], \alpha_i \in A$$

Beobachte ferner $h_i = \sum_j a_{ij} x^{\gamma_{ij}}$ für geeignete $a_{ij} \in k, \gamma_{ij} \in \mathbb{N}_0^n$.
Dann gilt

$$f = \sum_i \sum_j a_{ij} (x^{\gamma_{ij} + \alpha_i})$$

Wir sehen also, dass jeder Term auf der rechten Seite dieser Gleichung durch x^α für ein geeignetes $\alpha \in A$ teilbar ist. Dies muss somit auch für die linke Seite dieser Gleichung, nämlich f, gelten. □

Korollar 3.20. *Seien I, J monomiale Ideale. Dann gilt*
$I = J$ genau, dann wenn $\mathrm{Mon}(I) = \mathrm{Mon}(J)$ erfüllt ist.

Beweis. Folgt aus Lemma 3.19 *iii)*. □

Satz 3.21 (Dicksons Lemma, DL)**.**
Sei $I = \langle x^\alpha \mid \alpha \in A\rangle$ ein monomiales Ideal.
Dann existieren geeignete $\alpha_1, ..., \alpha_s \in A$ ($s \in \mathbb{N}$) mit $I = \langle x^{\alpha_1}, ..., x^{\alpha_s}\rangle$.

Beweis. Hilberts Basissatz (siehe Algebra 2, Skript 8. Vorlesung, SoSe 2021) liefert geeignete $f_1, ..., f_l \in k[x_1, ..., x_n]$ mit $I = \langle f_1, ..., f_l\rangle$.
Lemma 3.19 impliziert, dass

jeder Term von jedem f_i durch ein x^α für ein geeignetes $\alpha \in A$ teilbar ist.

Sei $A_i \subseteq A$ die entsprechend zuzuordnende endliche Untermenge von A, für jedes $i \in \{1, ..., l\}$. Dann gilt

$$\langle f_1, ..., f_l\rangle = \langle x^\alpha \mid \alpha \in \bigcup_{i=1}^{l} A_i\rangle$$

□

Korollar 3.22. *Sei $>$ eine Relation auf $\mathbb{N}_0^n$ so, dass folgende Bedingungen erfüllt sind:*

i) $>$ ist eine totale Anordnung von $\mathbb{N}_0^n$

ii) Wenn $\alpha > \beta$ gilt, dann folgt für beliebiges gamma in N_0^n stets $\alpha + \gamma > \beta + \gamma$

Dann ist $>$ eine Wohlordnung (also eine monomiale Anordnung) genau dann, wenn die zusätzliche Bedingung

iii)' $\alpha \geq 0$ für alle $\alpha \in \mathbb{N}_0^n$

erfüllt ist. Das heißt $>$ ist eine monomiale Anordnung genau, dann wenn $i), ii), iii)'$ gelten (Vergleiche mit Definition 3.1).

Beweis.

„⇐“ Sei $>$ eine Wohlordnung und a_0 das kleinste Element in $\mathbb{N}_0^n$.
Dann ist $a_0 > 0$ (sonst wäre $a_0 < 0$, und damit auch $2a_0 < a_0$. Ein Widerspruch).

„⇒“ Wir nehmen an, dass $iii)'$ gilt. Zu zeigen: $>$ ist eine Wohlordnung (vgl. $iii)$ in Definition 3.1).
Sei $A \subseteq \mathbb{N}_0^n, A \neq \emptyset$ und sei $I = \langle x^\alpha \mid \alpha \in A\rangle$. Dicksons Lemma, Satz 3.21 liefert nun geeignete $\alpha_1, ..., \alpha_s \in A$ mit $I = \langle x^{\alpha_1}, ..., x^{\alpha_s}\rangle$.
Ohne Einschränkung gelte $\alpha_1 < ... < \alpha_s$.

Beh.: α_1 ist das kleinste Element von A.

Wenn $\alpha \in A$ gilt, dann ist x^α teilbar durch ein x^{α_i} für ein geeignetes $i \in \{1, ..., s\}$ (wegen Lemma 3.18). Also ist $\alpha = \alpha_i + \gamma$ für ein geeignetes $\gamma \in \mathbb{N}_0^n$.
Nun ist (per Annahme $iii)'$) $\gamma > 0$, also folgt

$$\alpha = \alpha_i + \gamma \geq \alpha_i + 0 \geq a_1$$

□

3.2 Hilbertscher Basissatz und Gröbnerbasen

Vergleiche §5 The Hilberts Basis Theorem and Gröbner Bases, Kapitel 2 im Buch von Cox, Little und O'Shea 2006.

Fixiere eine monomiale Anordnung $>$.

Definition 3.23. *Sei* $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$.

Bezeichne mit $\mathrm{LT}(I)$ *die Menge aller Leitterme von Elementen aus* I.
Also $\mathrm{LT}(I) := \{cx^\alpha \mid c \in k, \alpha \in \mathbb{N}_0^n \text{ und } \exists f \in I \text{ mit } \mathrm{LT}(f) = cx^\alpha\}$

und sei $\langle \mathrm{LT}(I) \rangle$ *das Ideal, das hiervon erzeugt wird.*

Proposition 3.24. *Sei* $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$, *dann gelten folgende Eigenschaften:*

i) $\langle \mathrm{LT}(I) \rangle$ *ist ein monomiales Ideal*

ii) Es existieren geeignete $g_1, ..., g_t \in I$ *mit* $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$

Beweis.

i) Klar.

ii) Dicksons Lemma, Satz 3.21

□

7. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 16.11.2021

Satz 3.25 (Explizite Aussage von Hilberts Basissatz)**.**
Sei $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$ *und wähle geeignete* $g_1, ..., g_t \in I$ *mit* $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$. *Dann gilt*

$$I = \langle g_1, ..., g_t \rangle$$

Beweis. Die Inklusion $\langle g_1, ..., g_t \rangle \subseteq I$ ist klar.
Sei nun $f \in I$. Wende den Divisionsalgorithmus auf f und $(g_1, ..., g_t)$ an und erhalte eine Darstellung $f = a_1 g_1 + ... + a_t g_t + r$ mit $a_i \in k[x_1, ..., x_n]$ und kein Monom in r ist teilbar durch $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)$.

Behauptung: $r = 0$

Beweis: Schreibe

$$r = f - \sum_{i=1}^{t} a_i g_t \in I.$$

Falls $r \neq 0$ folgt $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$.
Nach Lemma 3.18 existiert somit ein $i \in 1, .., t$, sodass $\mathrm{LT}(g_i)$ den Leitterm von r teilt. Ein Widerspruch. □

Definition 3.26. *Sei* $I \trianglelefteq k[x_1, ..., x_n]$, *dann heißt eine Untermenge* $G = \{g_1, ..., g_t\} \subseteq I$ *Gröbnerbasis von* I, *wenn*

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$$

erfüllt ist.

Korollar 3.27. *i) Eine Gröbnerbasis* $\{g_1, ..., g_t\}$ *von* I *ist eine Idealbasis von* I.

ii) Jedes $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$ *hat eine Gröbnerbasis.*

Beweis.

i) Folgt aus Satz 3.25.

ii) Folgt aus Proposition 3.24.

□

Bemerkung 3.28. *Wir wollen zwei Bemerkungen festhalten (Folgerungen aus Hilberts Basissatz):*

1. *$k[x_1, ..., x_n]$ ist noethersch und erfüllt somit die ACC (Ascending Chain Condition) für Ideale:*

   Satz 3.29. *Sei $I_1 \trianglelefteq I_2 \trianglelefteq ...$ eine Folge von Idealen in $k[x_1, ..., x_n]$, dann gibt es ein $N \in \mathbb{N}$ mit $I_k = I_N$ für alle $k > N$.* □

2.

   Definition 3.30. *Sei $I \trianglelefteq k[x_1, ..., x_n]$. Definiere*

   $$\mathbf{V}(I) := \{(a_1, ..., a_n) \in k^n \mid \forall f \in I \colon f(a_1, ..., a_n) = 0\}$$

   Proposition 3.31. *$\mathbf{V}(I)$ ist eine affine Varietät (d.h. wenn $\{g_1, ..., g_t\}$ eine Idealbasis von I ist, dann folgt $\mathbf{V}(I) = \mathbf{V}(g_1, ..., g_t)$)* □

3.3 Eigenschaften von Gröbnerbases

Vergleiche §6 Properties of Gröbner Bases im Kapitel 2 im Buch von Cox, Little und O'Shea 2006.

Proposition 3.32. *Sei $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$ und $G = \{g_1, ..., g_t\}$ eine Gröbnerbasis von I. Sei $0 \neq f \in k[x_1, ..., x_n]$, dann existiert ein eindeutiger Rest $r \in k[x_1, ..., x_n]$ mit den folgenden Eigenschaften:*

i) Kein Term von r ist teilbar durch $\mathrm{LT}(g_i)$ (für alle $i = 1, ..., t$)

ii) $f = g + r$ für ein geeignetes $g \in I$

Das heißt r ist der eindeutige Rest im Divisionsalgorithmus von f durch $(g_1, ..., g_t)$.

Beweis. Die Existenz von r mit den Eigenschaften $i)$ und $ii)$ wurde bereits im Satz Satz 3.13 (Divisionsalgorithmus) bewiesen.

Eindeutigkeit: Erfüllen $r, r' \in k[x_1, ..., x_n]$ die Eigenschaften $i)$ und $ii)$ mit

$$f = g + r = g' + r'.$$

Dann folgt $r - r' = g' - g \in I$.
Falls $r - r' \neq 0$ gilt, folgt hieraus $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$.
Nach Lemma 3.18) existiert somit ein $i \in \{1, ..., t\}$, sodass $\mathrm{LT}(g_i)$ den Leitterm $\mathrm{LT}(r - r')$ teilt. Jedoch ist $\mathrm{LT}(r - r')$ ein Term von r oder r'. Dies liefert somit einen Widerspruch zur Eigenschaft $i)$ von r oder r'. □

Korollar 3.33. *Sei $G = \{g_1, ..., g_t\}$ eine Gröbnerbasis von I und $0 \neq f \in k[x_1, ..., x_n]$.*
Dann gilt $f \in I$ gdw. der Rest von f im Divisionsalgorithmus durch G gleich Null ist. □

Definition 3.34 (und Notation)**.** *Sei $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$, G eine Gröbnerbasis von I und $0 \neq f \in k[x_1, ..., x_n]$.*
Bezeichne mit $\overline{f}^{G}$ den Rest von f im Divisionsalgorithmus durch G (in beliebiger Reihenfolge).

Wir wollen nun entscheiden können, ob eine gegebene Idealbasis $\{g_1, ..., g_t\}$ eine Gröbnerbasis von I ist. Dafür werden wir die sogenannten „S-Polynome“ einführen.

Definition 3.35. *Seien $0 \neq f, g \in k[x_1, ..., x_n]$.*

Setze $\mathrm{multi\,deg}(f) =: \alpha =: (\alpha_1, ..., \alpha_n)$, $\mathrm{multi\,deg}(g) =: \beta =: (\beta_1, ..., \beta_n)$ *und*
$\mathbb{N}_0^n \ni \gamma := (\gamma_1, ..., \gamma_n)$ *für* $\gamma_i = \max(\alpha_i, \beta_i)$.
Betrachte ferner $x^\gamma := \mathrm{kgV}(\mathrm{LM}(f), \mathrm{LM}(g))$.

Das S-Polynom $S(f, g)$ entspricht nun:

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

Bemerkung 3.36.

i) $S(f, g) \in \langle f, g \rangle$

ii) $S(g, f) = -S(f, g)$

iii) Aus $\mathrm{multi\,deg}(f) = \mathrm{multi\,deg}(g) = \gamma$ *folgt* $\mathrm{multi\,deg}(S(f, g)) < \gamma$ *und $S(f, g)$ ist eine k-lineare Kombination von f und g*

iv) $\mathrm{multi\,deg}(S(f, g)) < \mathrm{multi\,deg}(\mathrm{kgV}(\mathrm{LM}(f), \mathrm{LM}(g)))$

Beispiel 3.37. *Fixiere $>_{gr\,lex}$ als monomiale Anordnung und betrachte die Polynome*

$f = x^3y^2 - x^2y^3 + x$ *und*

$g = 3x^4y + y^2$

in $\mathbb{R}[x,y]$.
Dann ist $\gamma = (x^4, y^2)$ *und*

$$S(f,g) = \frac{x^4y^2}{x^3y^2}f - \frac{x^4y^2}{3x^4y}g = xf - \frac{1}{3}yg = -x^3y^3 + x^2 - \frac{1}{3}y^3$$

8. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 18.11.2021

Lemma 3.38. *Seien $f_1, ..., f_s \neq 0$ in $k[x_1, ..., x_n]$ und $c_1, ..., c_s \in k^\times$.*
Sei $\text{multi deg}(f_i) = \text{multi deg}(f_j) = \delta$ *für alle* $i, j \in \{1, ..., s\}$.
Dann gilt:

i) $\text{multi deg}\, S(f_i, f_k) < \delta$ *für alle* $i \neq k$, $i, k \in \{1, ..., s\}$

ii) Aus $\text{multi deg}(\sum_{i=1}^s c_i f_i) < \delta$*folgt, dass* $\sum_{i=1}^s c_i f_i$ *als k-lineare Kombination von den S-Polynomen* $S(f_j, f_k)$ *(für* $1 \leq j, k \leq s$*) geschrieben werden kann.*

Beweis. Zu zeigen *ii*):

- Setze $d_i := \text{LC}(f_i)$

  und bemerke, dass diese Vorrausetzung in $\sum_{i=1}^s c_i f_i$ bereits $\sum_{i=1}^s c_i d_i = 0$ impliziert.

- Setze $p_i := \frac{f_i}{d_i}$.

  Schreibe die k-lineare Kombination nun wie folgt als Teleskopsumme um:

$$\begin{aligned}\sum_{i=1}^s c_i f_i &= \sum_{i=1}^s c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) \\ &\quad + ... \\ &\quad + (c_1 d_1 + ... + c_{s-1} d_{s-1})(p_{s-1} - p_s) + \underbrace{(c_1 d_1 + ... + c_s d_s)}_{=0} p_s.\end{aligned}$$

  Berechne $S(f_j, f_k)$:
  $\text{LT}(f_i) = d_i x^\delta$ und damit

$$(*) \qquad S(f_j, f_k) = x^\delta \left(\frac{f_j}{d_j x^\delta} - \frac{f_k}{d_k x^\delta} \right) = p_j - p_k$$

  Damit wurde *ii*) bewiesen.

i) folgt unmittelbar aus $(*)$. □

Satz 3.39 (Buchbergers Kriterium)**.** *Sei* $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$ *und* $G = \{g_1, ..., g_t\}$ *eine Idealbasis von I. Genau dann ist G eine Gröbnerbasis von I wenn für alle* $i \neq j$ *der Rest von* $S(g_i, g_j)$ *im Divisionsalgorithmus durch G gleich Null ist.*

Beweis.

„⇒“ Da G eine Gröberbasis ist und $S(g_i, g_j) \in I$ gilt, folgt aus Korollar 3.27 sofort $\overline{S(g_i, g_j)}^G = 0$.

„⇐“ Sei $f \in I$, $f \neq 0$. Zu zeigen:

$$(1) \qquad \mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$$

Schreibe hierfür

$$(2) \qquad f = \sum_{i=1}^{t} h_i g_i \text{ mit geeigneten } h_i \in k[x_1, ..., x_n].$$

Dann folgt

$$(3) \qquad \mathrm{multi\,deg}(f) \leq \max_i(\mathrm{multi\,deg}(g_i)).$$

Fall die Gleichheit in (3) gilt, dann existiert ein geeignetes $i \in \{1, ..., t\}$ mit $\mathrm{multi\,deg}(f) = \mathrm{multi\,deg}(h_i g_i)$. In diesem Fall ist $\mathrm{LT}(f)$ teilbar durch $\mathrm{LT}(g_i)$ und folglich ist (1) erfüllt.
Ansonsten setze $m(i) := \mathrm{multi\,deg}(h_i g_i)$ und $\delta := \max(m(1), ..., m(t))$.
Dann gilt $\mathrm{multi\,deg}(f) \leq \delta$.
Betrachte nun die nicht-leere Menge

$$\{\delta \mid \delta = \max(m(1), ..., m(t)) \text{ für eine Darstellung (2) von } f\}$$

Dann gibt es ein minimales δ in dieser Menge, da $\mathbb{N}_0^n$ Wohlgeordnet ist.

Behauptung: Wenn δ minimal ist, dann muss in (3) Gleichheit gelten.

Beweis per Widerspruch:
Sei δ minimal und $\mathrm{multi\,deg}(f) < \delta$.
Analysiere eine Darstellung (2):

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \underbrace{\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i}_{(I)} + \underbrace{\sum_{m(i)=\delta} (h_i - \mathrm{LT}(hi)) g_i}_{(II)} + \underbrace{\sum_{m(i)<\delta} h_i g_i}_{(III)}$$

Es ist klar, dass $\mathrm{multi\,deg}(II) < \delta$ und $\mathrm{multi\,deg}(III) < \delta$ gilt.
Es folgt somit unmittelbar auch $\mathrm{multi\,deg}(I) < \delta$.
Schreibe $\mathrm{LT}(h_i) = c_i x^{\alpha_i}$ und betrachte nochmals (I):

$$(I) = \sum_{m(i)=\delta} c_i x^{\alpha_i} g_i$$

mit $c_i \in k$.
Setze $f_i := x^{\alpha_i} g_i$. Dies liefert $\sum_i c_i f_i$ wie im Ansatz von Lemma 3.38.

Also kann man (I) als k-lineare Kombination der $\underbrace{S(x^{\alpha_j}g_j, x^{\alpha_k}g_k)}_{\text{multi deg davon} < \delta}$ (für $j,k = 1,...,t$ mit $j \neq k$) geschrieben werden.
Berechne

$$S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) = x^{\delta-\gamma_{jk}}S(g_j, g_k)$$

für $x^{\gamma_{jk}} = \text{kgV}(\text{LM}(g_j), \text{LM}(g_k))$.
Das heißt es existiert ein $c_{jk} \in k$ mit

$$(5) \qquad \sum_{m(i)=\delta} \text{LT}(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S(g_j, g_k).$$

Nun kann der Divisionsalgorithmus angewendet werden. Die Voraussetzungen ergeben:

$$(6) \qquad S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk}g_i \text{ für geeignete } a_{ijk} \in k[x_1, ..., x_n].$$

$$(7) \qquad \text{multi deg}(a_{ijk}g_i) \leq \text{multi deg}(S(g_j, g_k)) \text{ für alle } i,j,k \in \{1,...,t\}$$

Es sollen nun $(5), (6)$ und (7) ausgenutzt werden. Schreibe

$$x^{\delta-\gamma_{jk}}S(g_j, g_k) = \sum b_{ijk}g_i$$

für $b_{ijk} := x^{\delta-\gamma_{jk}}a_{ijk}$.
Aus (7) und Bemerkung 3.36 folgt

$$(8) \qquad \text{multi deg}(b_{ijk}g_i) \leq \text{multi deg}(x^{\delta-\gamma_{jk}}S(g_j, g_k)) < \delta$$

Mit (6) und liefert nun das Einsetzen in (5)

$$\sum_{m(i)=\delta} \text{LT}(h_i)g_i = \sum_{j,k} c_{jk}\left(\sum_{i=1}^{t} b_{ijk}g_i\right) = \sum_{i=1}^{t} \tilde{h}_i$$

mit $\tilde{h}_i := \sum_{i=1}^{t}\left(\sum_{j,k} c_{jk}b_{ijk}\right)g_i$. Insbesondere gilt jedoch wegen (8) bereits $\text{multi deg}(\tilde{h}_i) < \delta$. Ein Widerspruch.

□

9. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 23.11.2021

Beispiel 3.40. *Betrachte das Ideal* $I = \langle y - x^2, z - x^3 \rangle$ *in* $\mathbb{R}[y, z, x]$.

Beh.: $G = \{y - x^2, z - x^3\}$ *ist eine Gröbnerbasis von* I *bzgl.* $>_{lex}$ *mit* $y >_{lex} z >_{lex} x$.

Es soll Satz 3.39 (das Buchberger-Kriterium) ausgenutz werden:
Berechne

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Der Divisionsalgorithmus liefert nun

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0.$$

Also ist G *eine Gröbnerbasis von* I *bzgl.* $<_{lex}$ *in* $R[y, z, x]$.

Achtung: G *ist keine Gröbnerbasis für* $>_{lex}$ *mit* $x >_{lex} y >_{lex} z$ *in* $\mathbb{R}[x, y, z]$.

Beispiel 3.41. *Betrachte* $k[x, y]$ *mit* $>_{gr\,lex}$.
$f_1 = x^3 - 2xy$
$f_2 = x^2y - 2y^2 + x$
$I = \langle f_1, f_2 \rangle$ *bemerke, dass* $\{f_1, f_2\}$ *keine Gröbnerbasis von* I *bzgl.* $>_{grlex}$ *ist, weil*
$x^2 = xf_2 - yf_1 \in I$ *(also* $\mathrm{LT}(x^2) = x^2 \in \mathrm{LT}(I)$*) aber* $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = \langle x^3, x^2y \rangle$.
Wir wollen nun $F = (f_1, f_2)$ *„ergänzen“ bis das Buchberger-Kriterium (Satz 3.39) erfüllt ist und damit eine Gröbnerbasis konstruiert wurde.*
Berechne $S(f_1, f_2) = -x^2 \in I$.
Der Divisionsalgorithmus von $S(f_1, f_2)$ *durch* F *ergibt als Rest* $-x^2 \neq 0$.
Setze $f_3 := -x^2$ *und betrachte* $F = (f_1, f_2, f_3)$. *Berechne:*

- $S(f_1, f_2) = f_3$ *also* $\overline{S(f_1, f_2)}^F = 0$ ✓
- $S(f_1, f_3) = -2xy$ *und* $\overline{S(f_1, f_3)}^F = -2xy \neq 0$ ×

Setze $f_4 := -2xy$ *und betrachte* $F = (f_1, f_2, f_3, f_4)$. *Berechne:*

- $\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0$ ✓

- $S(f_1, f_4) = -2xy^2 = yf_4$ *also* $\overline{S(f_1, f_4)}^F = 0$ ✓
- $S(f_2, f_3) = -2y^2 + x$ *also* $\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$ ×

Setze $f_5 := -2y^2 + x$.
Nachrechnen (des Buchberger-Kriteriums) beweist nun, dass $F = \{f_1, ..., f_5\}$ *eine Gröbnerbasis von* I *bzgl.* $<_{grlex}$ *ist.*

Sei $>$ im folgenden eine monomiale Anordnung.

Satz 3.42 (Buchberger-Algorithmus)**.**
Sei $I \trianglelefteq k[x_1, ..., x_n]$ *und* $F = (f_1, ..., f_s)$ *eine Idealbasis von* I. *Dann kann* F *zu einer Gröbnerbasis* $G = \{g_1, ..., g_t\}$ *erweitert werden, indem* F *durch Reste der S-Polynome erweitert wird (vgl. Beispiel 3.41).*

Beweis. Setze zunächst $G' := F$.
Nehme an, dass G' bereits aufgebaut wurde. Definiere

$$G = G' \cup \{\text{ungleich-Null-Reste der } S\text{-Polynome über } G'\}$$

Da $G' \subseteq G$ per Definition gilt, folgt

$$(*) \qquad \langle \mathrm{LT}(G') \rangle \subseteq \langle \mathrm{LT}(G) \rangle.$$

Beh.: Aus $G' \subsetneq G$ folgt $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$.

Beweis: Falls $r \neq 0$ ein Rest (der S-Polynome) im Divisionsalgorithmus durch G' ist, dann ist $\mathrm{LT}(r)$ **nicht** teilbar durch $\mathrm{LT}(G')$. Daher

$$0 \neq r \in G \setminus G' \Rightarrow \mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle \setminus \langle \mathrm{LT}(G') \rangle \quad \square_{Beh.}$$

Damit ist die Inklusion in $(*)$ strikt.
Das zeigt: Dies zeigt, dass nach endlich vielen Schritten $G \setminus G' = \emptyset$ erreicht wird, denn sonst würden wir eine strikt steigende Folge von Idealen erzeugen, was ein Widerspruch dazu ist, dass $k[x_1, ..., x_n]$ noethersch ist. $\square$

Es kann nun die Frage gestellt werden, ob in Buchbergers Algorithmus ggfs. zu viele Erzeuger konstruiert werden.

Lemma 3.43. *Sei* G *eine Gröbnerbasis und* $p \in G$ *mit* $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$.
Dann ist $G \setminus \{p\}$ *auch eine Gröbnerbasis.*

Beweis. $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(G \setminus \{p\}) \rangle$. $\square$

Definition 3.44. *Eine Gröbnerbasis G von I ist eine minimale Gröbnerbasis, wenn folgende Eigenschaften erfüllt sind:*

i) $\mathrm{LC}(p) = 1$ *für alle* $p \in G$

ii) Für alle $p \in G$ *ist* $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G \setminus \{p\}) \rangle$

Beispiel 3.45 (Fortsetzung von Beispiel 3.41)**.** *Sei k unendlich.*
Betrachte nochmals $\langle f_1, f_2, f_3, f_4, f_5 \rangle$.
$\mathrm{LT}(f_1)x^3 = -x\,\mathrm{LT}(f_3)$. *Damit kann Lemma 3.43 angewendet werden.*
$\mathrm{LT}(f_2) = -\frac{1}{2}x\,\mathrm{LT}(f_4)$. *Damit kann Lemma 3.43 angewendet werden.*
Eine minimale Gröbnerbasis ist damit $\{\tilde{f}_3 := x^2, \tilde{f}_4 := xy, \tilde{f}_5 := y^2 - \frac{1}{2}x\}$.
ÜA: *Auch* $\{\hat{f}_3 = x^2 + axy, \hat{f}_4 = xy, \hat{f}_5 = y^2 - \frac{1}{2}x\}$ *ist für jedes* $a \in k$ *eine minimale Gröbnerbasis von I.*
Es ist somit ersichtlich, dass unendlich viele minimale Gröbnerbasen existieren können.

Definition 3.46. *Eine reduzierte Gröbnerbasis G von I ist eine Gröbnerbasis mit*

i) $\mathrm{LT}(p) = 1$ *für alle* $p \in G$

ii) Für alle $p \in G$ *liegt kein Term von p in* $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Proposition 3.47. *Sei* $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$ *und* $>$ *eine monomiale Anordnung.*
Dann existiert eine eindeutige reduzierte Gröbnerbais von I.

Beweis durch einen Algorithmus. Sei G eine minimale Gröbnerbasis von I. Ein $g \in G$ sei reduziert für G, wenn Bedingung *ii)* aus Definition 3.46 für g erfüllt ist.
Die g's der gegebenen minimalen Gröbnerbasis können nun algorithmisch durch reduzierte g's ersetzt werden. Dies sichert die Existenz einer reduzierten Gröbnerbasis.
Sei $g \in G$ und setze $g' = \overline{g}^{G \setminus \{g\}}$, sowie $G' = G \setminus \{g\} \cup g'$.
ÜA: Nach endlich vielen Schritten gilt $g' = g$, d.h. der Algorithmus terminiert, und die erzeugten g's sind reduziert.
ÜA: Die konstruierte reduzierte Gröbnerbasis ist eindeutig. □

10. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 25.11.2021

4 Eliminationstheorie

Vergleiche Kapitel 3 im Buch von Cox, Little und O'Shea 2006.
Wir werden in diesem Kapitel Methoden untersuchen, die uns ermöglichen Punkte $a \in k^n$ mit $a \in \mathbf{V}(I)$ ($\mathbf{V}(I)$ eine affine Varietät) zu bestimmen.

Beispiel 4.1 (Motivation)**.** *Betrachte das System von polynomieller Gleichungen in* $\mathbb{C}[x, y, z]$*:*

$$\begin{aligned} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1 \end{aligned}$$

Welche $(x, y, z) \in \mathbb{C}^3$ *lösen dieses System?*
Betrachte $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1\rangle$.
Finde eine Gröbnerbasis G *von* I *bzgl.* $>_{lex}$ *(also* $I = \langle G\rangle$*. Betrachte hierfür*

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

Die Nullstellen von g_4 *in* $\mathbb{C}$ *findet man durch die Betrachtung von*

$$z^2(z-1)^2(z^2 + 2z - 1) = 0.$$

Diese sind $z = 0, 1, -1 \pm \sqrt{2}$*. Einsetzen dieser* $g_2 = 0$ *bzw. in* $g_3 = 0$ *ergibt nun mögliche* y*-Lösungen. Darauffolgendes einsetzen in* $g_1 = 0$ *bestimmt sodann die Lösungskoordinate für* x*. So ergeben sich alle Lösungen:*

$$(1, 0, 0), (0, 1, 0), (0, 0, 1),$$

$$\begin{aligned} &(-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}), \\ &(-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}). \end{aligned}$$

Bemerke: $g_4 \in I \cap \mathbb{C}[z]$

Definition 4.2. *Sei $I \trianglelefteq k[x_1, ..., x_n]$ und sei $l \in \{0, ..., n\}$.*
Definiere $I_l = I \cap k[x_{l+1}, ..., x_n]$.

Terminologie: *I_l heißt l-tes Eliminationsideal von I.*

Bemerke

1) $I_l \trianglelefteq k[x_{l+1}, ..., x_n]$

2) $I_0 = I$

Satz 4.3 (Eliminationssatz)**.**
Sei $I \trianglelefteq k[x_1, ..., x_n]$ und G eine Gröbnerbasis von I bezüglich $>_{lex}$.
Dann ist G_l eine Gröbnerbasis von I_l für $G_l := G \cap k[x_{l+1}, ..., x_n]$ $(0 \leq l \leq n)$.

Beweis. Sei $l \in \{0, ..., n\}$. Per Definition gilt $G_l \subseteq I_l$, und

$$\langle \mathrm{LT}(I_l) \rangle = \langle \mathrm{LT}(G_l) \rangle$$

ist zu zeigen.
Die Inklusion "$\supseteq$" ist klar.
Es bleibt zu zeigen zeigen:

$$\langle \mathrm{LT}(I_l) \rangle \subseteq \langle \mathrm{LT}(G_l) \rangle$$

Sei $f \in I_l$. Zu zeigen: $\mathrm{LT}(f)$ ist teilbar durch $\mathrm{LT}(g)$ für ein geeignetes $g \in G_l$.

- Da $f \in I_l$ ist $f \in I$ klar erfüllt. Weil G zusätzlich eine Gröbnerbasis von I ist, existiert ein $g \in G$ so, dass $\mathrm{LT}(f)$ teilbar durch $\mathrm{LT}(g)$ ist.
- Da $f \in I_l$ gilt, folgt $\mathrm{LT}(g) \in k[x_{l+1}, ..., x_n]$
- Da $x_1 >_{lex} ... >_{lex} x_n$ gilt, folgt nun $g \in k[x_{l+1}, ..., x_n]$

□

Ansatz des Fortsetzungssatzes: Betrachte $\mathbf{V}(I) = \{(a_1, ..., a_n) \in k^n \mid \forall f \in I \colon f(a_1, ..., a_n) = 0\}$
und $\mathbf{V}(I_l) = \{(a_{l+1}, ..., a_n) \in k \mid \forall g \in I_l \colon g(a_{l+1}, ..., a_n) = 0\}$

Frage 4.4. *Sei $(a_{l+1}, ...a_n) \in \mathbf{V}(I_l)$. Wann kann diese Lösung fortsetzen zu $(a_1, ..., a_l, a_{l+1}, ..., a_n) \in \mathbf{V}(I)$ fortgesetzt werden?*

Terminologie: $(a_{l+1}, ..., a_n) \in \mathbf{V}(I_l)$ ist eine partielle Lösung mit $f_1 = 0, ..., f_s = 0$ wobei $\langle f_1, ..., f_s \rangle = I$

Satz 4.5 (Fortsetzungssatz)**.** *Sei* $\overbrace{k \text{ algebraisch abgeschlossen}}^{ⓐ}$*. Sei* $I = \langle f_1, ..., f_s \rangle \trianglelefteq k[x_1, ..., x_n]$*. Betrachte* I_1 *und für alle* $i \in \{1, ..., s\}$ *interpretiere* $f_i \in k[x_2, ..., x_n][x_1]$ *mit geeigneten* $0 \neq g_i \in k[x_2, ..., x_n]$*, sodass*

$$f_i = g_{\mathbf{I}}(x_2, ..., x_n)x_1^{N_i} + \text{ Terme mit Grad kleiner } N_i$$

mit $\deg(f_i) = N_i$ *gilt.*

Sei $(a_2, ..., a_n) \in \mathbf{V}(I_1)$ *eine partielle Lösung mit* $\overbrace{(a_2, ..., a_n) \notin \mathbf{V}(g_1, ..., g_s)}^{ⓑ}$*. Dann existiert ein* $a_1 \in k$ *mit* $(a_1, a_2, ..., a_n) \in \mathbf{V}(I)$

Beweis. Später. □

Beispiel 4.6 (Gegenbeispiele zu den Voraussetzugen ⓐ und ⓑ)**.**

ⓐ*: Betrachte das System*

$$x^2 = y$$
$$x^2 = z$$

über $k = \mathbb{R}$ *statt über* $\mathbb{C}$ *(d.h. in einem nicht algebraisch abgeschlossenen Körper). Dann ist* (a, a) *eine Partielle Lösung für* $a \in \mathbb{R}$*.*
Wenn $a < 0$ *gilt, dass existiert kein* x *mit* $x^2 = a$*.*

ⓑ*: Betrachte das System*

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

Eine partielle Lösung hiervon ist $(y, z) = (a, a)$ *mit* $a \in k$*.*
Jedoch kann $(0, 0)$ *nicht fortgesetzt werden. Hier war die Bedingung* ⓑ *verletzt. Insbesondere gilt nämlich*

$$f_1 = xy - 1 = g_1 x - 1 \in k[y, z][x]$$
$$f_2 = xz - 1 = g_2 x - 1 \in k[y, z][x]$$

mit $g_1 = y$*,* $g_2 = z$ *und* $g_1(0, 0) = g_2(0, 0) = 0$*.*

Wir wollen nun Korollare von Satz 4.5 (Fortsetzungssatz), sowie seine geometrische Bedeutung diskutieren.

Korollar 4.7. *Sei $I = \langle f_1, ..., f_s \rangle \trianglelefteq k[x_1, ..., x_n]$ und k algebraisch abgeschlossen.*
Es existiere ein $i \in \{1, ..., s\}$ mit

$$f_i = c_i x_1^{N_i} + ...$$

wobei $0 \neq c_i \in k$. Sei $(a_2, ..., a_n) \in \mathbf{V}(I_1)$ eine partielle Lösung.
Dann existiert ein $a_1 \in k$ mit $(a_1, a_2, ..., a_n) \in \mathbf{V}(I)$. □

Sei k algebraisch abgeschlossen.
Sei $V = \mathbf{V}(f_1, ..., f_s) \subseteq k^n$ und $l \in \{0, ..., n\}$. Betrachte die Projektion

$$\pi_l : k^n \to k^{n-l}$$
$$(a_1, ..., a_n) \mapsto (a_{l+1}, ..., a_n).$$

Untersuche nun $\pi_l(V) \subseteq k^{n-l}$. Bemerke hierbei, dass $\mathbf{V}(I_l)$ eine affine Varietät in k^{n-l} ist.

Lemma 4.8. *Es gilt $\pi_l(V) \subseteq \mathbf{V}(I_l)$.*

Beweis. Sei $f \in I_l$ und sei $(a_1, ..., a_n) \in V$.
Es gilt $f(a_1, ..., a_n) = 0$. Da aber $f \in I_l$, gilt auch $f(\underbrace{a_{l+1}, ..., a_n}_{\pi_l(a_1, ..., a_n)}) = 0$. □

Bemerkung 4.9. *$\pi_l(V)$ ist die Menge aller fortsetzbaren partiellen Lösungen.*

11. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 30.11.2021

Satz 4.10. *Sei k algebraisch abgeschlossen, und $V = \mathbf{V}(\langle f_1, ..., f_s\rangle)$ mit $f_1, ..., f_s \in k[x_1, ..., x_n]$, dann gilt*

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, ..., g_s) \cap \mathbf{V}(I_1))$$

(und die g_i's sind definiert wie im Fortsetzungs-Satz 4.5). □

Korollar 4.11. *Sei k algebraisch abgeschlossen und $V = \mathbf{V}(\langle f_1, ..., f_s\rangle)$ mit $f_1, ..., f_s \in k[x_1, ..., x_n]$. Nehme weiter an, es existiert ein $i \in \{1, ..., s\}$ mit*

$$f_i = \underbrace{c}_{0 \neq c \in k} x_1^N + \underbrace{\quad . \ . \ . \quad}_{\text{Terme mit (bezgl. } x_1\text{) Grad kleiner als } N}$$

Dann gilt $\mathbf{V}(I_1) = \pi_1(V)$. □

4.1 Faktorielle Ringe und Resultante

Erinnerungen aus der Algebra I und II (Insbesondere Algebra I Skript 6).

Definition 4.12.

- *Sei R faktoriell, dann ist jedes irreduzible Element ein Primelement.*
- *$R = k[x_1, ..., x_n]$ ist faktoriell (wenn k ein Körper ist)*

Resultante: Betrachte $k[x]$ und seien $f, g \in k[x]$ gegeben.

Zu entscheiden: Haben f, g einen gemeinsamen Faktor?

Sei dazu $l := \deg f > 0$ und $m := \deg g > 0$.

Wann gibt es ein $h \in k[x]$ mit $\deg h > 0$ sodass gilt $h|f$ und $h|g$?

Wir kennen bisher zwei Methoden:

- Falls $k[x]$ faktoriell ist, dann faktorisiere f und g und vergleiche die Faktoren.
- Berechne den $\mathrm{ggT}(f, g)$

Lemma 4.13. *Seien $f, g \in k[x]$ und $l := \deg f > 0$ und $m := \deg g > 0$. Dann haben f und g einen gemeinsamen Faktor h (mit $\deg h > 0$)) genau dann, wenn geeignete $A, B \in k[x]$ existieren mit:*

i) A und B sind nicht beide Null.

ii) $\deg(A) < m$ und $\deg(B) < l$.

iii) $Af + Bg = 0$

Beweis.

„⇒“ Sei h ein gemeinsamer Faktor, dann schreibe $f = hf_1$ und $g = hg_1$ mit $f_1, g_1 \in k[x]$ und $\deg f_1 < l$ und $\deg g_1 < m$.
Berechne

$$g_1 f + (-f_1)g = g_1 h f_1 - f_1 h g_1 = 0.$$

Setze $A = g_1$ und $B := -f_1$ ✓

„⇐“ Seien $A, B \in k[x]$ sodass $i), ii)$ und $iii)$ erfüllt sind. Ohne Einschränkung gelte $B \neq 0$.
Wenn f und g keinen gemeinsamen Faktor haben, dann ist $\mathrm{ggT}(f, g) = 1$.
Also existieren $\tilde{A}, \tilde{B} \in k[x]$ mit

$$\tilde{A}f + \tilde{B}g = 1$$

Nach Multiplikation mit B ergibt sich:

$$B = \tilde{A}Bf + \tilde{B}\underbrace{Bg}_{=-Af} = \tilde{A}Bf - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f$$

Da $B \neq 0$ folgt $\deg B \geq l$. Das ist ein Widerspruch zu $ii)$. □

Wir untersuchen $iii)$:

- Schreibe

$$f = a_0 x^l + ... + a_l \qquad a_0 \neq 0, a_i \in k$$
$$g = b_0 x^m + ... + b_m \qquad b_0 \neq 0, b_i \in k$$

Wir wollen $c_0, ..., c_{m-1} \in k$ nicht alle gleich Null **und** $d_0, ..., d_{l-1} \in k$ nicht alle gleich Null finden sodass

$$A := c_0 x^{m-1} + ... + c_{m-1} \text{ und}$$
$$B := d_0 x^{l-1} + ... + d_{l-1}$$

die Gleichung in $iii)$ erfüllen.
Das bedeutet, wenn wir die Koeffizienten von $iii)$ berechnen, dann sollen sie alle gleich

Null sein (Koeffizientenvergleich der rechten und linken Seite von *iii*)). Also berechnen wir nun

$$\begin{aligned} a_0\underline{c_0} + b_0\underline{d_0} = 0 \quad &= \text{Koeffizient von } x^{l+m-1} \\ a_1\underline{c_0} + a_0\underline{c_1} + b_1\underline{d_0} + b_0\underline{d_1} = 0 \quad &= \text{Koeffizient von } x^{l+m-2} \\ \vdots \qquad\qquad\qquad\qquad\qquad &\qquad\qquad \vdots \\ a_l\underline{c_{m-1}} + b_m\underline{d_{l-1}} = 0 \quad &= \text{Koeffizient von } \ x^0 \end{aligned} \tag{5}$$

und erhalten so ein Homogenes Lineares Quadratisches Gleichungssystem mit $l+m$ Zeilen und Spalten (die Variablen sind die c's und d's - unterstrichen).

Definition 4.14. *Seien*

$$\begin{aligned} f = a_0x^l + ... + a_l \quad &\in k[x] \text{ mit } l > 0 \\ g = b_0x^m + ... + b_m &\in k[x] \text{ mit } m > 0. \end{aligned}$$

Die Sylvestermatrix $\mathrm{Syl}(f,g,x)$ *ist diese* $(l+m)\times(l+m)$ *Matrix, also:*

$$\mathrm{Syl}(f,g,x) = \left(\begin{array}{cccc|cccc} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ \vdots & a_1 & \ddots & & \vdots & b_1 & b_0 & \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & b_1 & \ddots \\ a_l & \vdots & & a_1 & b_m & \vdots & \vdots & \ddots \\ & a_l & & \vdots & & b_m & \vdots & \\ & & \ddots & \vdots & & & b_m & \\ & & & a_l & & & & \ddots \\ & & & & & & & b_m \end{array}\right) \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \left.\begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right\} l+m \text{ Zeilen}$$

$$\underbrace{\qquad\qquad}_{m \text{ Spalten}} \qquad\qquad \underbrace{\qquad\qquad\qquad\qquad}_{l \text{ Spalten}}$$

wobei die freien Einträge 0 *sind.*

Die Resultante *von* f *und* g *ist*

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

Bemerkung 4.15. *Seien* $f,g \in k[x]$. *Wenn* $\mathrm{Res}(f,g,x) = 0$, *dann haben* f *und* g *einen gemeinsamen Faktor (das LGS (5) hat dann eine nicht triviale Lösung, damit liefert Lemma 4.13 die Existenz eines gemeinsamen Faktors).*

Löst man das LGS (5) so, dass $A = c_0x^{m-1} + ... + c_{m-1} \neq 0$ *minimalen Grad hat, dann ist* g/A *ein gemeinsamer Faktor, denn:*

Da $Af + Bg = 0$ (wobei $B = d_0x^{l-1} + ... + d_{l-1}$) und $k[x]$ ein Faktorieller Ring ist, können wir die Faktorisierung (als Produkt von irreduziblen Elementen in $k[x]$) von A und f und von B und g vergleichen.
Aus der Minimalität des Grades von A folgt, dass A und B keinen gemeinsamen irreduziblen Faktor haben (sonst könnte dieser aus der Gleichung $Af + Bg = 0$ gekürzt werden, Widerspruch zur Minimalität des Grades von A).
Also muss A schon g teilen und $g/A \in k[x]$ ist ein Faktor von g $(= Ag/A)$ und von $f = -Bg/A$ $(\Leftrightarrow Af + Bg = 0)$.

g/A ist dabei bis auf Assoziiertheit der größte gemeinsame Teiler.

Beispiel 4.16.

- *Sei $f(x) = 3x^3 + 2x^2 + x + 1$ und $g(x) = x^5$, dann ist*

$$\mathrm{Syl}(f,g,x) = \left(\begin{array}{ccccc|ccc} 3 & & & & & 1 & & \\ 2 & 3 & & & & 0 & 1 & \\ 1 & 2 & 3 & & & 0 & 0 & 1 \\ 1 & 1 & 2 & 3 & & 0 & 0 & 0 \\ & 1 & 1 & 2 & 3 & 0 & 0 & 0 \\ & & 1 & 1 & 2 & 0 & 0 & 0 \\ & & & 1 & 1 & & 0 & 0 \\ & & & & 1 & & & 0 \end{array}\right)$$

  wobei die freien Einträge 0 sind.

- *Sei $f = 2x^2 + 3x + 1$ und $g = 7x^2 + x + 3$, dann ist*

$$\mathrm{Syl}(f,g,x) = \left(\begin{array}{cc|cc} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{array}\right)$$

12. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 02.12.2021

Proposition 4.17. *Seien*

$$f = a_0x^l + ... + a_l \quad \in k[x] \text{ mit } l > 0, a_0 \neq 0$$
$$g = b_0x^m + ... + b_m \in k[x] \text{ mit } m > 0, b_0 \neq 0.$$

dann gilt:

i) f und g haben einen gemeinsamen Faktor $h \in k[x]$ mit $\deg h > 0$ genau dann, wenn $\mathrm{Res}(f, g, x) = 0$.

ii) $\mathrm{Res}(f, g, x) \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$, d.h. die Resultante ist ein Polynom in den Variablen $a_0, ..., a_l, b_0, ..., b_m$ mit Koeffizienten in $\mathbb{Z}$.

Beweis.

i) Folgt aus der Diskussion in der 11. Vorlesung bzgl. System (5).

ii) Bezeichne mit S_{ij} den ij-ten Eintrag von $\mathrm{Syl}(f, g, x)$, setzte $t := l + m$ und berechne die Determinante (siehe Lineare Algebra II):

$$\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x)) = \sum_{\sigma \in S_t} \mathrm{sign}(\sigma) \underbrace{S_{1\sigma(1)} \cdot ... \cdot S_{t\sigma(t)}}_{\substack{\text{Ein Produkt mit} \\ \text{Faktoren } a_i,\ b_j,\ 0}}$$

Die Behauptung folgt.

□

Beispiel 4.18. *i) Seien $f = 2x^2 + 3x + 1$ und $g = 7x^2 + x + 3$ Polynome in $\mathbb{Q}[x]$, berechne die Resultante:*

$$\mathrm{Res}(f, g, x) = \det \begin{pmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix} = 153 \neq 0$$

Daher haben f und g keinen gemeinsamen Faktor in $\mathbb{Q}[x]$.
Bemerke: Über F_{153} hätten sie hingegen einen gemeinsamen Faktor.

ii) Seien $f = xy - 1$ und $g = x^2 + y^2 - 4$ Polynome in $\mathbb{R}[x, y]$. Dann können f und g als Polynome über den Körper $\mathbb{R}(y) = \mathrm{Quot}(\mathbb{R}[y])$ also als Polynome in $\mathbb{R}(y)[x]$ gesehen werden.
Damit kann die Resultante berechnet werden:

$$\mathrm{Res}(f, g, x) = \det \begin{pmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2 - 4 \end{pmatrix} = y^4 - 4y^2 + 1 \in \mathbb{R}[y]$$

Frage: *Gilt* $\mathrm{Res}(f, g, x) \in \underbrace{\langle f, g \rangle}_{\trianglelefteq \mathbb{R}[x,y]} \cap \mathbb{R}[y]$*?*

Proposition 4.19. *Seien*

$$f = a_0 x^l + ... + a_l \quad \in k[x] \text{ mit } l > 0, a_0 \neq 0$$
$$g = b_0 x^m + ... + b_m \in k[x] \text{ mit } m > 0, b_0 \neq 0.$$

dann existieren $A, B \in k[x]$ mit $\mathrm{Res}(f, g, x) = Af + Bg$ und

(*) $A, B \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$, d.h. A und B sind Polynome in den Variablen $a_0, ..., a_l, b_0, ..., b_m$ mit Koeffizienten in $\mathbb{Z}$.

Beweis.

Fall 1: $\mathrm{Res}(f, g, x) = 0$, setze $A = B = 0$, Fertig.

Fall 2: $\mathrm{Res}(f, g, x) \neq 0$. Dann sind f und g relativ prim zueinander, also existieren $\tilde{A}$ und $\tilde{B}$ mit

$$\tilde{A}f + \tilde{B}g = 1 \tag{6}$$

Schreibe

$$\tilde{A} = c_0 x^{m-1} + ... + c_{m-1} \in k[x] \qquad \tilde{B} = d_0 x^{l-1} + ... + d_{l-1} \in k[x]$$

Es ergibt sich durch Koeffizientenvergleich Folgendes LGS (vergleiche mit System (5)):

$$\begin{aligned} a_0\underline{c_0} + b_0\underline{d_0} = 0 \quad &= \text{Koeffizient von } x^{l+m-1} \\ a_1\underline{c_0} + a_0\underline{c_1} + b_1\underline{d_0} + b_0\underline{d_1} = 0 \quad &= \text{Koeffizient von } x^{l+m-2} \\ \vdots \qquad\qquad\qquad\qquad\qquad &\quad\ \vdots \\ a_l\underline{c_{m-1}} + b_m\underline{d_{l-1}} = \mathbf{1} \quad &= \text{Koeffizient von } \ x^0 \end{aligned} \tag{7}$$

Wobei die Koeffizientenmatrix $\mathrm{Syl}(f, g, x)$ ist.
Die Determinante der Koeffizientenmatrix vom LGS (7) ist gleich der Determinante von $\mathrm{Syl}(f, g, x)$ ist - also gleich der $\mathrm{Res}(f, g, x)$.

Da $\text{Res}(f,g,x) \neq 0$ hat LGS (7) damit eine Eindeutige Lösung.
Nun nutze Cramers-Formel zur Berechnung der Lösung, also der Werte für $c_0, ..., c_{m-1}, d_0, ..., d_{l-1}$:

$$c_0 = \frac{1}{\text{Res}(f,g,x)} \det \underbrace{\begin{pmatrix} 0 & & & & b_0 & & & & \\ 0 & a_0 & & & b_1 & b_0 & & & \\ \vdots & a_1 & \ddots & & \vdots & b_1 & b_0 & & \\ & \vdots & \ddots & a_0 & \vdots & \vdots & b_1 & \ddots & \\ & \vdots & & a_1 & b_m & \vdots & \vdots & \ddots & b_0 \\ & a_l & & \vdots & & b_m & \vdots & & b_1 \\ 0 & & \ddots & \vdots & & & b_m & & \vdots \\ 1 & & & a_l & & & & \ddots & \vdots \end{pmatrix}}_{\substack{\text{Die Matrix Syl}(f,g,x), \text{ wobei die erste Spalte} \\ \text{durch } (0,0,...,1)^T \text{ ersetzt wurde}}}$$

Also folgt

$$c_0 = \frac{\text{Ein Polynom in } \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]}{\text{Res}(f,g,x)} =: \frac{p_0}{\text{Res}(f,g,x)} \text{ mit } p_0 \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$$

Analog folgt

$$c_i = \frac{p_1}{\text{Res}(f,g,x)} \text{ mit } p_i \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$$
$$d_j = \frac{q_j}{\text{Res}(f,g,x)} \text{ mit } q_j \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$$

$A := \text{Res}(f,g,x)\tilde{A} \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$ und
$B := \text{Res}(f,g,x)\tilde{B} \in \mathbb{Z}[a_0, ..., a_l, b_0, ..., b_m]$, erfüllen A, B also $(*)$, und wegen Gleichung (6) gilt auch

$$Af + Bg = \text{Res}(f,g,x)$$

□

4.2 Resultanten und Fortsetzungssatz

§6 Resultants and Extension Theorem Kapitel 3 im Buch von Cox, Little und O'Shea 2006.

Proposition 4.20. *Seien $f, g \in k[x_1, ..., x_n]$, also auch $f, g \in k(x_2, ..., x_n)[x_1]$ und sei der Grad von f und g in x_1 jeweils größer Null (*$\deg f > 0$ *und* $\deg g > 0$ *als Polynome in $k(x_2, ..., x_n)[x_1]$). Dann gelten:*

i) $\text{Res}(f,g,x_1) \in \langle f,g \rangle \cap k[x_2, ..., x_n]$ *(also für $I := \langle f,g \rangle$ gilt* $\text{Res}(f,g,x_1) \in I_1$*)*

ii) $\text{Res}(f,g,x_1) = 0$ *genau dann, wenn f und g einen gemeinsamen Faktor $h \in k[x_2, ..., x_n][x_1]$*

mit $\deg h > 0$ *(Grad in* x_1*).*

Beweis.

i) Aus Proposition 4.17 *i)* folgt $\mathrm{Res}(f, g, x_1) \in k[x_2, ..., x_n]$.
Aus Proposition 4.19 folgt $\mathrm{Res}(f, g, x_1) \in \langle f, g \rangle \trianglelefteq k[x_2, ..., x_n]$.

ii) Nach Proposition 4.17 *ii)* folgt, dass f und g einen gemeinsamen Faktor $h \in k(x_2, ..., x_n)[x_1]$ haben. Nach dem Lemma von Gauß folgt $h \in k[x_2, ..., x_n][x_1]$.

□

13. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 07.12.2021

Korollar 4.21. *Sei k algebraisch abgeschlossen, $f, g \in k[x_1, ..., x_n]$. Dann haben f und g eine gemeinsame Nullstelle in k genau dann, wenn* $\mathrm{Res}(f, g, x) = 0$. $\square$

Notation: Für $f \in k[x_1, ..., x_n] = k[x_2, ..., x_n][x_1] \subset k(x_2, ..., x_n)[x_1]$ schreiben wir von nun an $\deg_{x_1} f$ für den Grad von f als Polynom in der Variablen x_1 über den Körper $k(x_2, ..., x_n)$.

Proposition 4.22. *Sei k algebraisch abgeschlossen und $f, g \in k[x_1, ..., x_n]$ mit* $\deg_{x_1} f = l > 0$ *und* $\deg_{x_1} g = m > 0$. *Sei $c := (c_2, ..., c_n) \in k^{n-1}$ so, dass gelten:*

i) $f(x_1, c) \in k[x_1]$ hat Grad l (also $a_0(c) \neq 0$).

ii) $g(x_1, c) \in k[x_1]$ hat Grad $p \in \mathbb{N}$ mit $p \leq m$.

Schreibe

$$f = a_0 x_1^l + ... + a_l \quad \text{mit } a_0 \neq 0$$
$$g = b_0 x_1^m + ... + b_m \text{ mit } b_0 \neq 0.$$

wobei $f, g \in k[x_1, ..., x_n]$ und $a_0, ..., a_l, b_0, ..., b_m \in k[x_2, ..., x_n]$.
Sei $h := \mathrm{Res}(f, g, x_1) \in k[x_2, ..., x_n]$, dann gilt $h(c) = a_0(c)^{m-p} \mathrm{Res}(f(x_1, c), g(x_1, c), x_1)$.

Beweis. Berechne

$$(*) \qquad h(c) = \det \underbrace{\left(\begin{array}{cccc|cccc} a_0(c) & & & & b_0(c) & & & \\ a_1(c) & a_0(c) & & & b_1(c) & b_0(c) & & \\ \vdots & a_1(c) & \ddots & & \vdots & b_1(c) & b_0(c) & \\ \vdots & \vdots & \ddots & a_0(c) & \vdots & \vdots & b_1(c) & \ddots \\ a_l(c) & \vdots & & a_1(c) & b_m(c) & \vdots & \vdots & \ddots \\ & a_l(c) & & \vdots & & b_m(c) & \vdots & \\ & & \ddots & \vdots & & & b_m(c) & \\ & & & a_l(c) & & & \ddots & \vdots \\ & & & & & & & b_m \end{array}\right)}_{\substack{m \text{ Spalten} \\ l \text{ Spalten}}} \Bigg\} \substack{l+m \\ \text{Zeilen}}$$

Wir führen eine Induktion nach $m - p$.

Induktionsanfang: $m = p$
Das heißt

$$\begin{aligned} f(x_1, c) &= a_0(c)x_1^l + ... + a_l(c) \quad \in k[x_1] \text{ mit } a_0(c) \neq 0 \\ g(x_1, c) &= b_0(c)x_1^m + ... + b_m(c) \in k[x_1] \text{ mit } b_0(c) \neq 0. \end{aligned}$$

Vergleiche die Resultante davon mit $h(c)$ aus $(*)$ und erhalte

$$h(c) = \operatorname{Res}(f(x_1, c), g(x_1, c), x_1)$$

wie gewünscht.

$p = m - 1$:
Also $b_0(c) = 0$ aber $b_1(c) \neq 0$.
Wir wollen zeigen, dass $h(c) = a_0(c) \operatorname{Res}(f(x_1, c), g(x_1, c), x_1)$.
Betrachte $(*)$

$$h(c) = \det \left(\begin{array}{cccc|ccccc} \underline{a_0(c)} & & & & b_0(c) = 0 & & & & \\ \hline a_1(c) & a_0(c) & & & b_1(c) & b_0(c){=}0 & & & \\ \vdots & a_1(c) & \ddots & & \vdots & b_1(c) & b_0(c){=}0 & & \\ \vdots & \vdots & \ddots & a_0(c) & \vdots & \vdots & b_1(c) & \ddots & \\ a_l(c) & \vdots & & a_1(c) & b_m(c) & \vdots & \vdots & \ddots & b_0(c){=}0 \\ & a_l(c) & & \vdots & & b_m(c) & \vdots & & b_1(c) \\ & & \ddots & \vdots & & & b_m(c) & & \vdots \\ & & & a_l(c) & & & & \ddots & \vdots \\ & & & & & & & & b_m \end{array} \right) \left.\vphantom{\begin{array}{c} 1\\1\\1\\1\\1\\1\\1\\1\\1 \end{array}}\right\} \begin{array}{c} l+m \\ \text{Zeilen} \end{array}$$

m Spalten, l Spalten

und nutze die Kofaktoren-Entwicklung der Determinante (in der ersten Zeile) und erhalte:

$$h(c) = a_0(c) \det \left(\begin{array}{ccc|ccccc} a_0(c) & & & b_1(c) & b_0(c) = 0 & & & \\ a_1(c) & \ddots & & \vdots & b_1(c) & b_0(c) = 0 & & \\ \vdots & \ddots & a_0(c) & \vdots & \vdots & b_1(c) & \ddots & \\ \vdots & & a_1(c) & b_m(c) & \vdots & \vdots & \ddots & b_0(c) = 0 \\ a_l(c) & & \vdots & & b_m(c) & \vdots & & b_1(c) \\ & \ddots & \vdots & & & b_m(c) & & \vdots \\ & & a_l(c) & & & & \ddots & \vdots \\ & & & & & & & b_m \end{array} \right) \left.\vphantom{\begin{array}{c} 1\\1\\1\\1\\1\\1\\1\\1 \end{array}}\right\} \begin{array}{c} l+m-1 \\ \text{Zeilen} \end{array}$$

$m-1$ Spalten, l Spalten

wie gewünscht.

ÜÄ: Führe den Induktionsschritt durch. □

Satz 4.5 (Fortsetzungssatz - *Vgl. §6, Kapitel 3 im Buch*).
Sei k algebraisch abgeschlossen. Sei $I = \langle f_1, ..., f_s \rangle \trianglelefteq k[x_1, ..., x_n]$.
Betrachte I_1 und für alle $i \in \{1, ..., s\}$ interpretiere $f_i \in k[x_2, ..., x_n][x_1]$ mit geeigneten $0 \neq g_i \in k[x_2, ..., x_n]$, sodass

$$f_i = g_{\mathbf{I}}(x_2, ..., x_n)x_1^{N_i} + \text{ Terme mit Grad kleiner } N_i$$

mit $\deg_{x_1}(f_i) = N_i$ gilt.
Sei $c = (c_2, ..., c_n) \in \mathbf{V}(I_1)$ eine partielle Lösung mit $c \notin \mathbf{V}(g_1, ..., g_s)$. Dann existiert ein $c_1 \in k$ mit $(c_1, c_2, ..., c_n) \in \mathbf{V}(I)$

Beweis. Betrachte

$$\begin{aligned} \phi\colon k[x_1, ..., x_n] &\to k[x_1] \\ f(x_1, ..., x_n) &\mapsto f(x_1, c) \end{aligned}$$

und bemerke: ϕ ist ein Ring-Homomorphismus.
Daher $\phi(I) \trianglelefteq k[x_1]$.
Da $k[x_1]$ ein Hauptidealbereich ist, existiert ein $u \in k[x_1]$ mit

$$(*) \qquad \{f(x_1, c) \mid f \in I\} = \langle u \rangle$$

Nun gilt einer der Fälle:

Fall 1: u ist nicht konstant.
Dann existiert ein $c_1 \in k$ mit $u(c_1) = 0$ (da k algebraisch abgeschlossen ist).
Dann folgt mit $(*)$, dass $f(x_1, c) = 0$ für alle $f \in I$ gilt.
Damit folgt $(c_1, c) \in \mathbf{V}(I)$, wie gewünscht ✓

Fall 2: $u = 0$. ✓

Fall 3: $u = u_0 \in k^\times$.
Es existiert wegen $(*)$ also ein $f \in I$ mit $f(x_1, c) = 0$.
Da $c \notin \mathbf{V}(g_1, ..., g_s)$ existiert ein $i \in \{1, ..., s\}$ mit $g_i(c) \neq 0$.
Betrachte

$$h = \text{Res}(f_i, f, x_1) \in k[x_2, ..., x_n]$$

Dann folgt aus Proposition 4.22 angewendet auf f_i, f

$$h(c) = g_{\mathbf{I}}(c)^{\deg_{x_1} f} \underbrace{\text{Res}(f_{\mathbf{I}}(x_1, c), u_0, x_1)}_{= u_0^{N_i} \text{ nach ÜB 6, Aufgabe 1}}$$

Also

$$h(c) = \underbrace{g_{\mathbf{I}}(c)^{\deg_{x_1} f}}_{\neq 0} \underbrace{u_0^{N_i}}_{\neq 0} \neq 0$$

Andererseits folgt aus $h \in I_1$ (was aus 4.20 folgt), dass $h(c) = 0$ gilt (weil $c \in \mathbf{V}(I_1)$). Ein Widerspruch.

□

14. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 09.12.2021

5 Algebra-Geometrie Lexikon

Siehe Kapitel IV im Buch von Cox, Little und O'Shea 2006.

$$\begin{array}{ll} I \trianglelefteq k[x_1, ..., x_n] & \text{(algebraisch)} \\ \mathbf{V}(I) \subseteq k^n & \text{(geometrisch)} \end{array}$$

5.1 Hilbert's Nullstellensatz (HNS)

§1 Hilbert's Nullstellensatz im Buch von Cox, Little und O'Shea 2006.

Wir wissen bereits: Sei $V \subseteq k^n$ eine affine Varietät, dann ist $\mathbf{I}(V)$ ein Ideal in $k[x_1, ..., x_n]$, also:

$$\text{Affine Varietät} \rightsquigarrow \text{Ideal}$$

Umgekehrt sei $I \trianglelefteq k[x_1, ..., x_n]$, also $I = \langle f_1, ..., f_s \rangle$ (HBS) und damit ist $\mathbf{V}(I) \subseteq k^n$ eine affine Varietät, also:

$$\text{Ideal} \rightsquigarrow \text{Affine Varietät}$$

1) Was ist die Beziehung zwischen den Varietäten V und $\mathbf{V}(\mathbf{I}(V))$?

2) Was ist die Beziehung zwischen den Idealen I und $\mathbf{I}(\mathbf{V}(I))$?

Satz 5.1 (Schwacher Nullstellensatz)**.** *Sei k algebraisch abgeschlossen und $I \trianglelefteq k[x_1, ..., x_n]$ mit $\mathbf{V}(I) = \emptyset$.*
Dann gilt $I = k[x_1, ..., x_n]$.

Bemerkung 5.2. *Der Schwache Nullstellensatz bedeutet: Sei k algebraisch abgeschlossen und $I = \langle f_1, ..., f_s \rangle \trianglelefteq k[x_1, ..., x_n]$. Wenn $I \neq k[x_1, ..., x_n]$, dann gilt $\mathbf{V}(I) \neq \emptyset$.*

Beweis. Per Induktion nach $n \in \mathbb{N}$ zeigen wir

$$\mathbf{V}(I) = \emptyset \Rightarrow 1 \in I$$

woraus die Behauptung folgt.

Induktionsanfang $n = 1$:

Wähle $f \in k[x_1]$ mit $I = \langle f \rangle$ ($k[x_1]$ ist ein Hauptidealbereich [HIB]).
Dann folgt aus $\mathbf{V}(I) = \emptyset$ also f ist konstant und ungleich Null (sonst hat f eine Nullstelle und $\mathbf{V}(I)$ ist nicht leer).
Daher $f \in k^\times$ und es folgt $1 \in I$, also $I = k[x_1]$. ✓

Induktionsannahme: Es gelte für $k[x_2, ..., x_n]$

Induktionsschritt:

Sei nun $I = \langle f_1, ..., f_s \rangle \trianglelefteq k[x_1, ..., x_n]$ mit $\mathbf{V}(I) = \emptyset$.
Ohne Einschränkung gilt $f_1 \notin k$.
Sei

$$N := \text{total deg } f_1 \in \mathbb{N}$$

wir machen einen linearen Variablen Wechsel, d.h. wir setzen für ein gegebenes Element $(a_2, ..., a_n) \in k^{n-1}$

$$\begin{array}{l|l} x_1 = \tilde{x_1} & \tilde{x_1} = x_1 \\ x_2 = \tilde{x_2} + a_2\tilde{x_1} & \tilde{x_2} = x_2 - a_2x_1 \\ \vdots & \vdots \\ x_n = \tilde{x_n} + a_n\tilde{x_1} & \tilde{x_n} = x_n - a_nx_1 \end{array}$$

Dann können wir f_1 wie folgt umschreiben:

$$\begin{aligned} f_1(x_1, ..., x_n) &= f_1(\tilde{x_1}, \tilde{x_2} + a_2\tilde{x_1}, ..., \tilde{x_n} + a_n\tilde{x_1}) \\ &=: \tilde{f_1}(\tilde{x_1}, ..., \tilde{x_n}) \\ &\overset{\text{ÜA}}{=} \underbrace{c(a_2, ..., a_n)}_{\substack{c \in k[x_2,...,x_n] \text{ist ein} \\ \text{ungleich Null Polynom}}} \tilde{x_1}^N + \text{ Terme mit } \deg_{x_1} < N \end{aligned}$$

D.h. wir betrachten $\tilde{x} := T(x)$ wobei $x = (x_1, ..., x_n)$ und $T\colon k^n \to k^n$ ist definiert durch

$$\begin{aligned} T(x_1) &= x_1 \\ T(x_2) &= x_2 - a_2x_1 \\ &\vdots \\ T(x_n) &= x_n - a_nx_n \end{aligned}$$

Also T geschrieben als Matrix

$$\begin{pmatrix} 1 & -a_2 & -a_3 & ... & -a_n \\ & 1 & 0 & ... & 0 \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

ist Invertierbar.
Also $T \in \mathcal{L}(k^n, k^n)$ invertierbar.
Damit induziert T einen Ring-Homomorphismus

$$\begin{aligned} \rightsquigarrow\colon k[x_1, ..., x_n] &\to k[\tilde{x_1}, ..., \tilde{x_n}] = k[x_1, ..., x_n] \\ f &\mapsto f \circ T =: \tilde{f} \end{aligned}$$

Und es gilt das Kommutative Diagramm:

$$\begin{array}{ccccc} & k[x_1, ..., x_n] & \to & k[\tilde{x_1}, ..., \tilde{x_n}] & \\ \text{Evaluieren} & \big| & \circlearrowleft & \big| & \text{Evaluieren} \\ & k^n & \overset{T}{\longleftrightarrow} & k^n & \end{array}$$

Wähle $(a_2, ..., a_n) \in k^{n-1}$ so, dass $c(a_2, ..., a_n) \in k^\times$ (das geht weil k algebraisch abgeschlossen und damit unendlich ist).
Sei $\tilde{I} = \{\tilde{f} \mid f \in I\} \trianglelefteq k[\tilde{x_1}, ..., \tilde{x_n}]$ und $\mathbf{V}(\tilde{I}) = \emptyset$.
Wir zeigen nun: $1 \in \tilde{I}$.
Da

$$\tilde{f_1}(\tilde{x_1}, ..., \tilde{x_n}) = \underbrace{c(a_2, ..., a_n)}_{\in k^\times} \tilde{x_1}^N + \text{ Terme mit } \deg_{x_1} < N$$

können wir Korollar 4.11 - ein Korollar vom Fortsetzungssatz - anwenden und bekommen

$$\mathbf{V}(\tilde{I_1}) = \pi_1(\mathbf{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset$$

Mit der Induktionsannahme folgt nun $1 \in \tilde{I_1} \subseteq \tilde{I}$, damit auch $1 \in I$.

□

Satz 5.3 (Hilberts Nullstellensatz (HNSS))**.** *Sei k algebraisch abgeschlossen und $f \in \mathbf{I}(\mathbf{V}(f_1, ..., f_s))$. Dann existiert ein $m \in \mathbb{N}$ mit $f^m \in \langle f_1, ..., f_s \rangle$.*

Bemerkung 5.4. *Hilberts Nullstellensatz impliziert den Schwachen Nullstellensatz:*

Sei $I = \langle f_1, ..., f_s \rangle$ mit $\mathbf{V}(I) = \emptyset$, dann gilt sofort $1 \in \mathbf{I}(\mathbf{V}(I))$ und mit HNSS also $1^m \in I$ (für ein geeignetes $m \in \mathbb{N}$). Das bedeutet $1 \in I$. $\square$

Nun zeigen wir auch die andere Richtung und beweisen HNSS.

Beweis. Ohne Einschränkung $f \neq 0$.
Betrachte

$$\hat{I} = \langle f_1, ..., f_s, 1 - yf \rangle \trianglelefteq k[x_1, ..., x_n, y]$$

Beh.: $\mathbf{V}(\hat{I}) = \emptyset$

Bew.: Sei $(a_1, ..., a_n, a_{n+1}) \in k^{n+1}$.

Fall 1: $(a_1, ..., a_n) \in \mathbf{V}(f_1, ..., f_s)$ und damit

$$f(a_1, ..., a_n) = 0$$

und $1 - a_{n+1} f(a_1, ..., a_n) = 1 \neq 0$, also $(a_1, ..., a_n, a_{n+1}) \notin \mathbf{V}(\hat{I})$.

Fall 2: $f_i(a_1, ..., a_n) \neq 0$ für ein $i \in \{1, ..., s\}$. Dann gilt

$$f_i(a_1, ..., a_n, a_{n+1}) = f_i(a_1, ..., a_n) \neq 0$$

also wieder $(a_1, ..., a_n, a_{n+1}) \notin \mathbf{V}(\hat{I})$. ■

Nun folgt aus dem Schwachen Nullstellensatz $1 \in \hat{I}$ also

$$1 = \sum_{i=1}^{s} \underbrace{p_i}_{\in k[x_1,...,x_n,y]} f_i + \underbrace{q}_{\in k[x_1,...,x_n,y]} (1 - yf)$$

Setze $y = \frac{1}{f}$ (nun sind wir im Quotientenkörper) und erhalte

$$1 = \sum_{i=1}^{s} p_i(x_1, ..., x_n, \frac{1}{f}) f_i$$

Wähle m so groß, dass diese Gleichung multipliziert mit f^m nicht mehr im Quotientenkörper ist, d.h alle Nenner (nur Potenzen von f stehen im Nenner) werden zu 1 gekürzt. $\square$

15. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 14.12.2021

Sei k Körper.

Definition 5.5 (Erinnerung)**.** *Sei $I \trianglelefteq k[x_1, ..., x_n]$.*

i) I ist radikal, wenn aus $f^m \in I$ (für ein geeignetes $m \in \mathbb{N}$) schon $f \in I$ folgt.

ii) Das Radikalideal von I wird bezeichnet durch $\sqrt{I}$ und ist definiert als

$$\sqrt{I} := \{f \in k[x_1, ..., x_n] \mid \exists m \in \mathbb{N}\colon f^m \in I\}$$

Bemerkung 5.6. *Es gilt für $I \trianglelefteq k[x_1, ..., x_n]$*

- *$\sqrt{I} \trianglelefteq k[x_1, ..., x_n]$ (also $\sqrt{I}$ ist ein Ideal).*
- *$I \subseteq \sqrt{I}$ und $\sqrt{\sqrt{I}} = \sqrt{I}$ (siehe Übungsblatt 2).*
- *I ist radikal genau dann, wenn $I = \sqrt{I}$.*
- *Sei $J \trianglelefteq k[x_1, ..., x_n]$ mit $I \subseteq J$, dann folgt $\sqrt{I} \subseteq \sqrt{J}$.*

Lemma 5.7. *Sei $V \subseteq k^n$ eine affine Varietät, dann ist $\mathbf{I}(V)$ radikal.*

Beweis. Sei $f^m \in \mathbf{I}(V)$ für ein geeignetes $m \in \mathbb{N}$ und $x \in V$, dann ist $f^m(x) = 0 = (f(x))^m$, also $f(x) = 0$ und damit $f \in \mathbf{I}(V)$. □

Satz 5.8 (Hilberts Nullstellensatz - starke Version)**.**
Sei k algebraisch abgeschlossen und $I \trianglelefteq k[x_1, ..., x_n]$. Dann gilt

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

Beweis. Wir haben $I \subseteq \mathbf{I}(\mathbf{V}(I))$ (siehe Bemerkung 2.15) also $\sqrt{I} \subseteq \sqrt{\mathbf{I}(\mathbf{V}(I))} \overset{L.5.7}{=} \mathbf{I}(\mathbf{V}(I))$.
Umgekehrt sei $f \in \mathbf{I}(\mathbf{V}(I))$, dann folgt $f \in \sqrt{I}$ aus Hilberts Nullstellensatz 5.3. □

Satz 5.9 (Ideal-Varietät-Korrespondenz)**.**

i) Die Abbildungen

$$\textit{Affine Varietäten} \xrightarrow{\mathbf{I}} \textit{Ideale}$$

und

$$\textit{Ideale} \xrightarrow{\mathbf{V}} \textit{Affine Varietäten}$$

sind Inklusionsumkehrend (Kontavariant).
D.h.

$$\textit{wenn } I_1 \subseteq I_2 \textit{ dann } \mathbf{V}(I_1) \supseteq \mathbf{V}(I_2),$$

und

$$\textit{wenn } V_1 \subseteq V_2 \textit{ dann } \mathbf{I}(V_1) \supseteq \mathbf{I}(V_2).$$

ii) a) Für eine Varietät V gilt immer

$$(*) \qquad \mathbf{V}(\mathbf{I}(V)) = V$$

***Es folgt:** Die Abbildung I ist immer injektiv.*

b) Für ein Ideal I gilt immer

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

*(**Es folgt:** Die Abbildung V ist nicht injektiv.)*

iii) Sei k algebraisch abgeschlossen und betrachte die restringierten Abbildungen

$$\textit{Affine Varietäten} \xrightarrow{\mathbf{I}} \textit{Radikalideale}$$

und

$$\textit{Radikalideale} \xrightarrow{\mathbf{V}} \textit{Affine Varietäten}$$

Dann sind I und V bijektiv und zueinander invers.

Beweis.

i) Proposition 2.17 + ÜÄ.

ii) a) Wir prüfen $(*)$.
Sei $x \in V$. Für $f \in \mathbf{I}(V)$ folgt per Definition $f(x) = 0$.
Damit $x \in \mathbf{V}(\mathbf{I}(V))$.
Also $V \subseteq \mathbf{V}(\mathbf{I}(V))$.
Umgekehrt sei $V = \mathbf{V}(\langle f_1, ..., f_s \rangle)$, dann $f_1, ..., f_s \in \mathbf{I}(V)$.
Also $\langle f_1, ..., f_s \rangle \subseteq \mathbf{I}(V)$. Es folgt aus $i)$, dass

$$\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_1, ..., f_s \rangle) = V$$

b) Wir prüfen zunächst $\mathbf{V}(I) \subseteq \mathbf{V}(\sqrt{I})$.
Sei $x \in \mathbf{V}(I)$ und $f^m \in I$, dann $f^m(x) = 0 = (f(x))^m$, also $f(x) = 0$ und $x \in \mathbf{V}(\sqrt{I})$.
Umgekehrt prüfen wir $\mathbf{V}(I) \supseteq \mathbf{V}(\sqrt{I})$.
Es gilt $I \subseteq \sqrt{I}$ und damit nach $i)$ schon $\mathbf{V}(I) \supseteq \mathbf{V}(\sqrt{I})$.

iii) I ist wohldefiniert weil $\mathbf{I}(V)$ immer ein Radikalideal ist (siehe Lemma 5.7).
Wir haben schon bewiesen $\mathbf{V}(\mathbf{I}(V)) = V$.
Wir müssen nur noch prüfen, dass für ein Radikalideal I schon $\mathbf{I}(\mathbf{V}(I)) = I$ gilt. Das folgt aus dem Starken Nullstellensatz 5.8.

□

5.2 Idealsumme, Produkt und Durchschnitt

Vergleiche mit Kapitel 4, §3 im Buch.
Sei k ein Körper.

Seien im folgenden $I, J \trianglelefteq k[x_1, ..., x_n]$ Ideale so, dass $I = \langle f_1, ..., f_s \rangle$ und $J = \langle g_1, ..., g_t \rangle$.

Proposition 5.10 (Erinnerung)**.** *Es gilt*

$$I + J = \langle f_1, ..., f_s, g_1, ..., g_t \rangle$$

Satz 5.11 (Idealsumme)**.** *Es gilt*

$$\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$$

Beweis. Siehe Proposition 2.4 ($I \cap J = \mathbf{V}(f_1, ..., f_s, g_1, ..., g_t)$). □

Proposition 5.12 (Erinnerung)**.** *Es gilt*

$$IJ = \langle \{ f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t \} \rangle$$

Satz 5.13 (Idealprodukt)**.** *Es gilt*

$$\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$$

Beweis. Siehe Proposition 2.4 ($I \cup J = \mathbf{V}(\{ f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t \})$). □

Proposition 5.14 (Erinnerung)**.** *Es gilt*

$$I \cap J \trianglelefteq k[x_1, ..., x_n] \text{ (also } I \cap J \text{ ist ein Ideal).}$$

Satz 5.15 (Idealdurchschnitt)**.** *Es gilt*

$$\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$$

5.3 Zariskiabschluss

Vergleiche mit Kapitel 4, §4 im Buch.
Sei k ein Körper.

Definition 5.16. *Sei $S \subseteq k^n$ eine Untermenge.*
Setze $\mathbf{I}(S) = \{f \in k[x_1, ..., x_n] \mid \forall a \in S\colon f(a) = 0\}$.

Proposition 5.17. *Sei $S \subseteq k^n$, dann ist $\mathbf{I}(S)$ ein Radialideal und $\mathbf{V}(\mathbf{I}(S))$ ist die kleinste affine Varietät in K^n die S enthält.*
(D.h. wenn $W \subseteq k^n$ eine affine Varietät mit $S \subseteq W$ ist, dann folgt $\mathbf{V}(\mathbf{I}(S)) \subseteq W$).

Beweis. Sei $W \supseteq S$ eine affine Varietät. Dann gilt $\mathbf{I}(W) \subseteq \mathbf{I}(S)$ und es folgt $\mathbf{V}(\mathbf{I}(W)) \supseteq \mathbf{V}(\mathbf{I}(S))$.
Aber $\mathbf{V}(\mathbf{I}(W)) = W$ (folgt aus Satz 5.9). □

Definition 5.18. *i) Sei $S \subseteq k^n$. Der Zariski-Abschluss von S bezeichnet durch $\bar{S}$ ist die kleinste affine Varietät die S enthält. D.h $\bar{S} = \mathbf{V}(\mathbf{I}(S))$.*

ii) Sei $S \subseteq k^n$, V eine affine Varietät in k^n mit $S \subseteq V$. S ist Zariskidicht in V genau dann, wenn $V = \bar{S}$.

Lemma 5.19. *Seien $S, T \subseteq k^n$. Es gelten:*

i) $\mathbf{I}(\bar{S}) = \mathbf{I}(S)$

ii) $S \subseteq T \Rightarrow \bar{S} \subseteq \bar{T}$

iii) $\overline{S \cup T} = \bar{S} \cup \bar{T}$

16. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 16.12.2021

Erinnerung: Es ist $\pi_l \colon k^n \to k^{n-l}$ die Projektionsabbildung auf die letzten $n-l$ Koordinaten.

Satz 5.20. *Sei k algebraisch abgeschlossen und $V = \mathbf{V}(f_1, ..., f_s) \subset k^n$ eine affine Varietät und I_l das l'te Eliminationsideal. Dann gilt*

$$\overline{\pi_l(V)} = \mathbf{V}(I_l) \qquad \textit{d.h. } \overline{\pi_l(V)} \textit{ ist Zariskidicht in } \mathbf{V}(I_l)$$

Beweis.

„$\subseteq$“ Wir müssen zeigen, dass

$$\mathbf{V}(\mathbf{I}(\pi_l(V))) = \mathbf{V}(I_l)$$

in Lemma 4.8 hatten wir

$$\pi_l(V) \subseteq \mathbf{V}(I_l)$$

Aus Satz 5.9 i) und ii) folgt nun schon

$$\mathbf{V}(\mathbf{I}(\pi_l(V))) \subseteq \mathbf{V}(I_l)$$

„$\supseteq$“ Sei $f \in \mathbf{I}(\pi_l(V))$. Das heißt $f(a_{l+1}, ..., a_n) = 0$ für alle $(a_{l+1}, ..., a_n) \in \pi_l(V)$.
Also gilt auch $f(a_1, ..., a_n) = 0$ für alle $(a_1, ..., a_n) \in V$.
Hilberts Nullstellensatz impliziert nun

$$f^N \in \langle f_1, ..., f_s \rangle$$

für ein geeignetes $N \in \mathbb{N}$. Dann folgt

$$f^N \in \langle f_1, ..., f_s \rangle \cap k[x_{l+1}, ..., x_n] = I_l$$

und damit $f \in \sqrt{I_l}$, also

$$\mathbf{I}(\pi_l(V)) \subseteq \sqrt{I_l}$$

Anwenden von $\mathbf{V}$ auf beiden Seiten liefert (wegen Satz 5.9)

$$\mathbf{V}(\mathbf{I}(\pi_l(V))) \supseteq \mathbf{V}(\sqrt{I_l})$$

und Satz 5.9 ii) liefert die Behauptung.

□

Wir wollen nun Quotientenideale und das Verhalten der Abbildung $\mathbf{V}$ diesbezüglich studieren.

Erinnerung: Seien $I, J \trianglelefteq k[x_1, ..., x_n]$. Der Idealquotient $(I\colon J)$ ist wie folgend definiert:

$$(I\colon J) := \{f \in k[x_1, ..., x_n] \mid \forall g \in J\colon fg \in I\} = \{f \in k[x_1, ..., x_n] \mid \forall fJ \subseteq I\}$$

Proposition 5.21. *Seien $I, J \trianglelefteq k[x_1, ..., x_n]$. Dann gilt*

i) $(I\colon J) \trianglelefteq k[x_1, ..., x_n]$

ii) $I \subseteq (I\colon J)$

Beweis.

i) ÜA

ii) Sei $f \in I$, da I ein Ideal ist folgt $fg \in I$ für alle $g \in k[x_1, ..., x_n]$ also auch für alle $g \in J$.

□

Satz 5.22. *Sei k ein Körper und $I, J \trianglelefteq k[x_1, ..., x_n]$. Dann gelten*

i) $\mathbf{V}(I\colon J) \supseteq \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$

ii) Wenn k algebraisch abgeschlossen ist und I radikal, dann gilt die Gleichheit also

$$\mathbf{V}(I\colon J) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$$

Beweis.

i) Um die Behauptung zu zeigen reicht es

$$(I\colon J) \subseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$$

zu zeigen (und dann $\mathbf{V}$ auf beiden Seiten anzuwenden).
Also sei $f \in (I\colon J)$ und $x \in \mathbf{V}(I) \setminus \mathbf{V}(J)$. Zu Zeigen ist: $f(x) = 0$.
Dann gilt für alle $g \in J$ schon $fg \in I$ also

$$f(x)g(x) = 0$$

Aber $x \notin \mathbf{V}(J)$ und damit existiert ein $g \in J$ mit $g(x) \neq 0$, also folgt $f(x) = 0$.

ii) Wir zeigen

$$\mathbf{V}(I\colon J) \subseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J)))$$

und damit die Behauptung.
Also sei $x \in \mathbf{V}(I\colon J)$ und $h \in \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. Zu zeigen: $h(x) = 0$.
Wenn $g \in J$ gilt, dann verschwindet hg auf $\mathbf{V}(I)$ weil

- h verschwindet auf $\mathbf{V}(I) \setminus \mathbf{V}(J)$
- g verschwindet auf $\mathbf{V}(J)$

Es folgt nun aus Hilberts Nullstellensatz, dass

$$hg \in \sqrt{I}$$

da $\sqrt{I} = I$ nach Voraussetzung gilt folgt also $hg \in I$ für alle $g \in J$ und damit $h \in (I\colon J)$.
Aus der Wahl von x folgt nun $h(x) = 0$.

□

Korollar 5.23. *Seien V, W affine Varietäten. Dann gilt*

$$(\mathbf{I}(V)\colon \mathbf{I}(W)) = \mathbf{I}(V \setminus W)$$

Beweis.

„⊆“ Im Beweis von Satz 5.22 *i)* haben wir gezeigt

$$(I\colon J) \subseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$$

Setze $I := \mathbf{I}(V)$ und $J := \mathbf{I}(W)$. Dann bekommen wir

$$(\mathbf{I}(V)\colon \mathbf{I}(W)) \subseteq \mathbf{I}(\mathbf{V}(\mathbf{I}(V)) \setminus \mathbf{V}(\mathbf{I}(W))) = \mathbf{I}(V \setminus W)$$

„⊇“ Sei $f \in \mathbf{I}(V \setminus W)$. Zu zeigen: $f \in (\mathbf{I}(V)\colon \mathbf{I}(W))$.
Also zu zeigen: Für alle $g \in \mathbf{I}(W)$ gilt $fg \in \mathbf{I}(V)$.
Sei $x \in V$, zu zeigen: $(fg)(x) = 0$ für $g \in \mathbf{I}(W)$.
Das folgt da: Für $x \in V \setminus W$ gilt $f(x) = 0$, und für $x \in W$ gilt $g(x) = 0$.

□

5.4 Irreduzible Varietäten und Primideale

Vergleiche Kapitel 4, §5 im Buch.
Sei k ein Körper.

Definition 5.24. *Eine affine Varietät $V \subseteq k^n$ heißt irreduzibel falls gilt:*

Wenn $V = V_1 \cup V_2$ für affine Varietäten $V_1, V_2 \subseteq k^n$ dann $V = V_1$ oder $V = V_2$.

Proposition 5.25. *Sei $V \subseteq k^n$ eine affine Varietät. Dann ist V irreduzibel genau dann, wenn $\mathbf{I}(V)$ ein Primideal ist.*

Beweis.

„⇒“ Seien $f, g \in k[x_1, ..., x_n]$ mit $fg \in \mathbf{I}(V)$.
Setze $V_1 := V \cap \mathbf{V}(f)$ und $V_2 := V \cap \mathbf{V}(g)$.
Dann sind V_1, V_2 affine Varietäten und weil $fg \in \mathbf{I}(V)$ gilt

$$V = V_1 \cup V_2$$

Da V irreduzibel ist gilt $V = V_1$ oder $V = V_2$. Also entweder verschwindet f auf V also $f \in \mathbf{I}(V)$ oder
es verschwindet g auf V also $g \in \mathbf{I}(V)$.

„⇐“ Sei $V = V_1 \cup V_2$ wobei V_1, V_2 affine Varietäten sind.
Betrachte den Fall $V \neq V_1$ (sonst sind wir fertig).
Wir zeigen: $V = V_2$ indem wir zeigen $\mathbf{I}(V) = \mathbf{I}(V_2)$ ($\mathbf{I}$ ist injektiv, Satz 5.9).

„⊆“ Bemerke $V_2 \subseteq V$ und damit $I(V) \subseteq I(V_2)$.

„⊇“ Sei also $f \in \mathbf{I}(V_2)$, zu zeigen $f \in \mathbf{I}(V)$.
Bemerke: Es gilt $I(V) \subseteq I(V_1)$ (analog zu „⊆“). Falls auch gilt $I(V) \supseteq I(V_1)$ folgt also aus $\mathbf{I}(V_1) = \mathbf{I}(V)$ schon $V = V_1$ (entgegen unserer Annahme). Also betrachte den Fall $I(V) \subsetneq I(V_1)$. Sei $g \in \mathbf{I}(V_1) \setminus \mathbf{I}(V)$.
Da $V = V_1 \cup V_2$ gilt, verschwindet fg auf V.
Es folgt $fg \in \mathbf{I}(V)$ und da $\mathbf{I}(V)$ prim ist und $g \notin \mathbf{I}(V)$ folgt $f \in \mathbf{I}(V)$.

□

Korollar 5.26. *Sei k algebraisch abgeschlossen. Dann definieren die Abbildungen $\mathbf{I}$ und $\mathbf{V}$ eine bijektive Korrespondenz zwischen irreduziblen Varietäten und Primidealen.*

Beweis. Folgt zusammen mit Satz 5.9) *iii*) da Primideale auch Radikalideale sind. □

17. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 21.12.2021

Definition 5.27. *Seien $V \subseteq k^m$ und $W \subseteq k^n$ affine Varietäten und sei*

$$\varnothing \colon V \to W$$

eine Abbildung. $\varnothing$ ist eine polynomiale Abbildung (oder reguläre Abbildung) genau dann, wenn es $f_1, ..., f_n \in k[x_1, ..., x_m]$ gibt mit

$$\varnothing(a_1, ..., a_m) = (f_1(a_1, ..., a_m), ..., f_n(a_1, ..., a_m))$$

für $(a_1, ..., a_m) \in V$.

Definition 5.28. *Sei $V \subseteq k^n$ eine affine Varietät. Eine Polynomiale Parametrisierung von V ist eine polynomiale Abbildung*

$$F \colon k^m \to k^n \qquad \text{Für geeignetes } m \in \mathbb{N}$$

mit $V = \overline{F(k^m)}$.

Fakt: Eine affine Varietät W ist der Zariskiabschluss von einer Menge S genau dann, wenn $\mathbf{I}(W) = \mathbf{I}(S)$.

Beweis.

„$\Rightarrow$“ $S \subseteq W$ impliziert $\mathbf{I}(S) \supseteq \mathbf{I}(W)$.
Umgekehrt sei $f \in \mathbf{I}(S)$ und $x \in W$, also $x \in \mathbf{V}(\mathbf{I}(S))$ (siehe Definition 5.18) und damit $f(x) = 0$.

„$\Leftarrow$“ Es gilt $\mathbf{I}(W) = \mathbf{I}(S)$, anwenden von $\mathbf{V}$ auf beiden Seiten ergibt $\underbrace{\mathbf{V}(\mathbf{I}(W)}_{=W} = \mathbf{V}(\mathbf{I}(S))$.

□

Proposition 5.29. *Sei k ein unendilcher Körper und $V \subseteq k^n$ eine affine Varietät mit polynomialer Parametrisierung $F = (f_1, ..., f_n)$. Dann ist V eine irreduzible Varietät.*

Beweis. Sei F durch $f_1, ..., f_n \in k[t_1, ..., t_m]$ gegeben und $g \in k[x_1, ..., x_n]$.
Dann ist $g \circ F = g(f_1, ..., f_n)$ ein Polynom in $k[t_1, ..., t_m]$.

Wir wollen zeigen, dass $\mathbf{I}(V) = \mathbf{I}(\overline{F(k^m)})$ ein Primideal ist, denn damit ist V nach Proposition 5.25 eine irreduzible Varietät.
Sei $S := F(k^m)$, es ist $\mathbf{I}(V) = \mathbf{I}(S)$ (wegen dem oben genannten Fakt).

Behauptung: $\mathbf{I}(S) = \{g \in k[x_1, ..., x_n] \mid g \circ F = 0\}$

Beweis: Sei $g \in \mathbf{I}(S)$, also per Definition $g(a_1, ..., a_n) = 0$ für alle $(a_1, ..., a_n) \in S$.
Damit gilt $g(f_1(t_1, ..., t_m), ..., f_n(t_1, ..., t_m)) = 0$ für alle $(t_1, ..., t_m) \in k^m$.
Da k unendlich ist folgt nun $g \circ F = 0$.
ÜÄ: Es folgt aus $g \circ F = 0$ bereits $g \in \mathbf{I}(S)$.

Also $\mathbf{I}(V) = \mathbf{I}(S) = \{g \in k[x_1, ..., x_n] \mid g \circ F = 0\}$.
Sei $gh \in \mathbf{I}(V)$, dann ist $(gh) \circ F \overset{\text{ÜA}}{=} (g \circ F)(h \circ F) = 0$ und damit $g \circ F = 0$ oder $h \circ F = 0$. Also $h \in \mathbf{I}(V)$ oder $g \in \mathbf{I}(V)$. □

Definition 5.30. *Sei $V \subseteq k^n$ eine affine Varietät. Eine rationale Parametrisierung von V ist eine rationale Abbildung*

$$F \colon (k^m \setminus W) \to k^n$$

so, dass $f_1, ..., f_n, g_1, ..., g_n \in k[t_1, \ldots, t_m]$ existieren mit

i) $F(t_1, ..., t_m) = \left(\frac{f_1(t_1,...,t_m)}{g_1(t_1,...,t_m)}, ..., \frac{f_n(t_1,...,t_m)}{g_n(t_1,...,t_m)}\right)$ *und* $W = \mathbf{V}(g_1 g_2 ... g_n)$.

ii) $V = \overline{F(k^m \setminus W)}$

Proposition 5.31. *Sei k ein unendlicher Körper und $V \subset k^n$ eine affine Varietät mit rationaler Parametrisierung $F = \left(\frac{f_1}{g_1}, ..., \frac{f_n}{g_n}\right)$. Dann ist V eine irreduzible Varietät.*

Beweis. Wir wollen zeigen, dass $\mathbf{I}(V)$ ein Primideal ist (denn damit ist V nach Proposition 5.25 eine irreduzible Varietät).

ÜA 1: Sei $h \in k[x_1, ..., x_n]$ mit $\operatorname{total\,deg} h = N$, dann ist $(g_1 g_2 ... g_n)^N (h \circ F) \in k[t_1, ..., t_m]$.

ÜA 2: Sei $h \in k[x_1, ..., x_n]$ und $(t_1, ..., t_m) \in k^m \setminus W$, dann gilt (da k unendlich ist) für $(t_1, ..., t_m) \in k^m \setminus W$: $(g_1 g_2 ... g_n)^N (h \circ F)(t_1, ..., t_m) = 0$ genau dann, wenn $(h \circ F)(t_1, ..., t_m) = 0$.

ÜA 1, ÜA 2 und Aufgabe 8.3 aus den Übungen ergeben zusammen

$$\mathbf{I}(V) = \{h \in k[x_1, ..., x_n] \mid (g_1 g_2 ... g_n)^{\operatorname{total\,deg} h} (h \circ F) = 0\}$$

Es bleibt zu zeigen: $\mathbf{I}(V)$ ist ein Primideal.
Seien $p, q \in \mathbf{I}(V)$, setzte $M := \operatorname{total\,deg} p$ und $N := \operatorname{total\,deg} q$.

Es gilt also

$$\left((g_1 g_2 ... g_n)^{M+N}\right)((pq) \circ F) = 0$$

damit also

$$(g_1 g_2 ... g_n)^M (p \circ F))(g_1 g_2 ... g_n)^N (q \circ F)) = 0$$

und damit $(g_1 g_2 ... g_n)^M (p \circ F)) = 0$ oder $(g_1 g_2 ... g_n)^N (q \circ F)) = 0$ also $p \in \mathbf{I}(V)$ oder $q \in \mathbf{I}(V)$. □

Proposition 5.32 (Analogon für maximale Ideale)**.** *Sei k algebraisch abgeschlossen und $I \trianglelefteq k[x_1, ..., x_n]$.*
Wenn I maximal ist, dann hat $\mathbf{V}(I)$ genau einen Punkt. Wenn I radikal ist, dann gilt die Umkehrung auch.

Beweis. Sei k algebraisch abgeschlossen und $I \trianglelefteq k[x_1, ..., x_n]$ ein Maximalideal. Dann gibt es nach ÜA 8.2 $(a_1, ..., a_n) \in k^n$ mit $I = \langle x_1 - a_1, ..., x_n - a_n \rangle$ und damit $\mathbf{V}(I) = \{(a_1, ..., a_n)\}$.

Sei nun I radikal und sei $\mathbf{V}(I) = (a_1, \ldots, a_n)$. Sei nun $J = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Dies ist radikal. Dann ist $\mathbf{V}(I) \subseteq \mathbf{V}(J)$ und daher $I = \sqrt{I} = \mathbf{I}(\mathbf{V}(I)) \supseteq \mathbf{I}(\mathbf{V}(J)) = J$ und, da J maximal ist, gilt $I = J$. □

5.5 Zerlegung von Varietäten als Vereinigung von irreduziblen

Vergleiche Kapitel 4, §6 im Buch.

Definition 5.33 (DCC)**.** *Sei $V_1 \supseteq V_2 \supseteq ...$ eine inklusionsabsteigende Folge von affine Varietäten.*
Dann gibt es ein $N \in \mathbb{N}$ mit $V_N = V_{N+1} = ...$

Beweis. Betrachte $\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq ...$ und nutze, dass $k[x_1, ..., x_n]$ noethersch ist. □

Satz 5.34. *Sei $V \subseteq k^n$ eine affine Varietät, dann gibt es irreduzible Varietäten $V_1, ..., V_m$ mit $V = V_1 \cup ... \cup V_m$*

Beweis. Angenommen die Behauptung gilt nicht für V.
Dann ist V nicht irreduzibel.
Also existieren affine Varietäten $V_1, V_1' \subsetneq V$ mit $V = V_1 \cup V_1'$.
Da die Behauptung nicht für V gilt, gilt sie OE auch nicht für V_1 (Falls die Behauptung für V_1 und V_1' gleichzeitig gilt, dann gilt sie auch für V). Dann ist V_1 nicht irreduzibel.
Also existieren affine Varietäten $V_2, V_2' \subsetneq V_1$ mit $V_1 = V_2 \cup V_2'$
So finden wir eine strikte inkusionsabsteigende Folge $V \supsetneq V_1 \supsetneq V_2 ...$, ein Widerspruch. □

Definition 5.35. *Sei V eine affine Varietät. Eine Zerlegung*

$$V = V_1 \cup ... \cup V_m \qquad \text{wobei } V_1, ..., V_m \text{ irreduzible Varietäten}$$

heißt minimale Zerlegung, wenn $V_i \not\subseteq V_j$ für alle $i \neq j$ gilt.

Satz 5.36. *Sei V eine affine Varietät, dann existiert eine eindeutige minimale Zerlegung (eindeutig bis auf die Nummerierung).*

Beweis. ÜA: Es existiert eine minimale Zerlegung.
Zu zeigen bleibt die Eindeutigkeit.
Seien $V = V_1 \cup ... \cup V_m$ und $V = V_1' \cup ... \cup V_l'$ minimale Zerlegungen.
Es gilt $V_i \cap V = V_i$ also

$$V_i = V_i \cap (V_1 \cup ... \cup V_m) = (V_i \cap V_1') \cup ... \cup (V_i \cap V_l')$$

und da V_i irreduzibel ist also $V_i = V_i \cap V_j'$ für ein geeignetes j.
Also

$$V_i \subseteq V_j'$$

Analog argumentieren wir mit V_j' und erhalten

$$V_j' \subseteq V_k$$

für ein geeignetes k.
Also $V_i \subseteq V_j' \subseteq V_k$ und per Minimalität folgt $V_i = V_j' = V_k$ □

Satz 5.37. *Sei k algebraisch abgeschlossen und I ein Radikalideal. Dann hat I eine (bis auf Umnummerierung) eindeutige Darstellung*

$$I = P_1 \cap ... \cap P_m$$

mit Primidealen $P_1, ..., P_m$ mit $P_i \not\subseteq P_j$ für $i \neq j$.

Beweis. Da I radikal ist und k algebraisch abgeschlossen existiert eine affine Varietät V mit $I = \mathbf{I}(V)$.
Sei $V = V_1 \cup ... \cup V_m$ eine minimale Zerlegung von V, also insbesondere $V_1, ..., V_m$ sind irreduzibel.
Dann folgt $\mathbf{I}(V) = \mathbf{I}(V_1) \cap ... \cap \mathbf{I}(V_m)$ und $\mathbf{I}(V_1), ..., \mathbf{I}(V_m)$ sind Primideale. □

18. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 11.01.2022

6 Polynomielle und rationale Abbildungen auf affinen Varietäten

Siehe Kapitel 5 im Buch von Cox, Little und O'Shea 2006.

6.1 Polynomielle Abbildungen

Motivation: Wir haben bereits polynomielle Abbildungen der Form

$$\begin{array}{rccc} f\colon & V & \longrightarrow & W \\ & \cap & & \cap \\ & k^m & & k^n \end{array}$$

untersucht. Nun wollen wir den Sonderfall $W = k$ tiefer studieren.

Definition 6.1. *In diesem Fall heißt die polynomielle Abbildung*

$$\begin{array}{rccc} \phi\colon & V & \longrightarrow & k \end{array}$$

eine skalare polynomielle Abbildung. D. h., es gibt ein Polynom $p \in k[x_1, \ldots, x_n]$, mit

$$\phi(a_1, \ldots, a_n) = p(a_1, \ldots, a_n), \quad \text{für alle } (a_1, \ldots, a_n) \in V.$$

Beispiel 6.2. *Wenn wir in Definition 6.1 $p := x_i$ setzen, dann heißt ϕ i-te Koordinatenfunktion, für alle $i = 1, \ldots, m$.*

Definition 6.3. *Wir bezeichnen mit $k[V]$ die Menge aller skalaren polynomiellen Abbildungen $\phi\colon V \to k$.*

Wir versehen $k[V]$ mit punktweisen Verknüpfungen:

$$\begin{array}{rl} (\phi + \psi)(\underline{a}) & = \phi(\underline{a}) + \psi(\underline{a}) \\ (\phi\psi)(\underline{a}) & = \phi(\underline{a})\psi(\underline{a}) \end{array}$$

für alle $\underline{a} = (a_1, \ldots, a_m) \in V$. Mit diesen Operationen ist $k[V]$ ein kommutativer Ring mit Eins. Eigentlich ist $k[V]$ eine k-Algebra (ÜA).

Wir nennen $k[V]$ den Koordinatenring von V.

Wir wollen nun $k[V]$ näher untersuchen. Dafür werden die Homomorphiesätze aus der Algebra I eine wichtige Rolle spielen.

Proposition 6.4. *Seien k ein Körper und $V \subseteq k^m$ eine affine Varietät. Die Abbildung*

$$\begin{array}{ccc} k[x_1,\ldots,x_n] & \to & k[V] \\ p & \mapsto & \begin{pmatrix} p\colon & V & \to & k \\ & \underline{a} & \mapsto & p(\underline{a}) \end{pmatrix} \end{array} \quad \text{skalare polynomielle Abbildung}$$

ist ein surjektiver Ringhomomorphismus mit Kern $\mathbf{I}(V)$. Insbesondere gilt

$$k[V] \simeq k[x_1,\ldots,x_m]/\mathbf{I}(V).$$

Darüber hinaus gelten folgende Aussagen:

- *$k[V]$ ist durch die Restklassen $x_i + I(V)$, $i = 1,\ldots,m$ der Koordinatenfunktionen bezüglich des Ideals $I(V)$ erzeugt.*
- *$k[V]$ ist genau dann integer, wenn V eine irreduzible Varietät ist.* □

Erinnerung: (Satz 5.9, Theorem 7 auf Seite 177 im Buch) Sei k algebraisch abgeschlossen. Dann sind die Abbildungen

$$\{\text{Affine Varietäten in } k^n\} \xrightarrow{\mathbf{I}} \{\text{Radikalideale in } k[x_1,\ldots,x_n]\}$$

und

$$\{\text{Radikalideale in } k[x_1,\ldots,x_n]\} \xrightarrow{\mathbf{V}} \{\text{Affine Varietäten in } k^n\}$$

kontravariant, bijektiv und zueinander invers.

Nun wollen wir dieses Resultat verallgemeinern, indem wir k^n durch eine allgemeine affine Varietät $V \subseteq k^n$ und $k[x_1,\ldots,x_n]$ durch $k[V]$ ersetzen.

Erinnerung aus der B3: Sei $I \trianglelefteq k[x_1,\ldots,x_n]$ fest. Es gibt eine bijektive Korrespondenz

$$\begin{array}{ccc} \left\{ \begin{array}{c} J \trianglelefteq k[x_1,\ldots,x_n] \\ \text{mit } I \trianglelefteq J \end{array} \right\} & \longrightarrow & \left\{ \tilde{J} \trianglelefteq k[x_1,\ldots,x_n]/I \right\} \\ J & \longmapsto & J/I. \end{array}$$

Proposition 6.5 (Prop. 10, Seite 226 im Buch)**.** *Seien k ein Körper und $V \subseteq k^n$ eine affine Varietät. Es gibt eine bijektive Korrespondenz*

$$\begin{array}{ccc} \left\{ \begin{array}{c} J \trianglelefteq k[x_1, \ldots, x_n] \\ \textit{mit } \mathbf{I}(V) \trianglelefteq J \end{array} \right\} & \longrightarrow & \left\{ \tilde{J} \trianglelefteq k[V] \right\} \\ J & \longmapsto & \tilde{J} = J/\mathbf{I}(V). \end{array}$$

Darunter werden radikale (bzw. maximale) Ideale auf radikale (bzw. maximale) Ideale abgebildet.

Satz 6.6 (Theorem 5 auf Seite 240 im Buch)**.** *Seien k ein algebraisch abgeschlossener Körper und $V \subseteq k^m$ eine affine Varietät. Die folgende zwei Abbildungen sind inklusionsumkehrend, bijektiv und zueinander invers.*

$$\left\{ \begin{array}{c} \textit{Affine Untervarietäten} \\ W \subseteq V \end{array} \right\} \underset{\mathbf{V}_V}{\overset{\mathbf{I}_V}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{Radikalideale} \\ I \trianglelefteq k[V] \end{array} \right\}, \tag{8}$$

wobei $\mathbf{I}_V(W) := \mathbf{I}(W)/\mathbf{I}(V)$, und, gegeben $\tilde{J} \trianglelefteq k[V]$, wähle ein geeignetes $J \trianglelefteq k[x_1, \ldots, x_n]$ mit $\tilde{J} = J/\mathbf{I}(V)$. Dies existiert nach Proposition 6.5 und hat die Eigenschaft $\mathbf{I}(V) \trianglelefteq J$. Setze $\mathbf{V}_V(\tilde{J}) := \mathbf{V}(J)$. □

Zusatz: Unter der Korrespondenz (8) werden Punkte in V auf maximale Ideale in $k[V]$ abgebildet.

Beweis. Sei $\mathbf{I}(V) \trianglelefteq J \trianglelefteq k[x_1, \ldots, x_n]$ so, dass $J/\mathbf{I}(V)$ maximal in $k[V]$ ist. Dann ist $J \trianglelefteq k[x_1, \ldots, x_n]$ maximal und daher radikal. Also ist $\mathbf{V}(J)$ ein Punkt $(a_1, \ldots, a_n) \in k^n$. Aber nach der Kontravarianz von $\mathbf{V}_V$ ist $(a_1, \ldots, a_n) = \mathbf{V}(J) \in V$.

Sei umgekehrt $(a_1, \ldots, a_n) \in V$. Dann ist $\langle x - a_1, \ldots, x - a_n \rangle =: J$ maximal mit $\mathbf{I}(V) \trianglelefteq J$ (Kontravarianz). Daher ist $J/\mathbf{I}(V)$ maximal in $k[V]$. □

19. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 13.01.2022

Kapitel 5, Abschnitt 3 im Buch von Cox, Little und O'Shea 2006

Bemerkung 6.7. *Im Buch wird oft von "Ring homomorphism that is the identity on the constant functions $k \in k[V]$" geredet. Wir reden hier von* Homomorphismen von k-Algebren. *Diese sind notwendigerweise die Identität auf k. In der Tat*
seien A, B zwei k-Algebren. Dann gelten
$c1_A = c$ *und* $c1_B = c$ *für alle* $c \in k$. *(#)*
Sei nun $\Phi\colon A \to B$ ein Homomorphismus von k-Algebren. Dann ist Φ ein Ringhomomorphismus und ein Homomorphismus von k-Vektorräumen. Es folgt also

$$\begin{aligned}\Phi(c) &= \Phi(c1_a) \quad [(\#)] \\ &= c\Phi(1_a) \quad [\textit{Linearität}] \\ &= c1_B \quad [\textit{Ringhomomorphismus}] \\ &= c \quad [(\#)].\end{aligned}$$

Proposition 6.8 (Ch.5, §4, Proposition 8)**.** *Sei k ein Körper und seien $V \subseteq k^m$, $W \subseteq k^n$ affine Varietäten.*

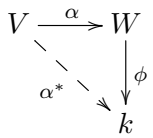
(i) Sei $\alpha\colon V \to W$ eine polynomielle Abbildung. Dann ist die Abbildung

$$\begin{array}{rccc} \alpha^*\colon & k[W] & \longrightarrow & k[V] \\ & \phi & \longmapsto & \phi \circ \alpha \end{array}$$

ein Homomorphismus von k-Algebren.

(ii) Sei umgekehrt $f\colon k[W] \to k[V]$ ein Homomorphismus von k-Algebren. Dann existiert eine eindeutige polynomielle Abbildung $\alpha\colon V \to W$ mit $\alpha^* = f$.

Bevor wir die Proposition beweisen, erklären wir sie anhand von Diagrammen:
Die Abbildung α^* ist durch folgendes kommutatives Diagramm definiert:



Um dies mit Nebenklassen zu erklären, sei $p \in k[y_1, \ldots, y_n]$. Dann ist

$$\alpha^*(p + \mathbf{I}(W)) = (p + \mathbf{I}(W)) \circ \alpha = (p \circ \alpha) + \mathbf{I}(V) \tag{9}$$

und wir haben folgendes Diagramm von Koordinatenringen

$$\begin{array}{ccc} k[W] & \xrightarrow{\alpha^*} & k[V] \\ {\scriptstyle \iota_W}\downarrow & & \downarrow{\scriptstyle \iota_V} \\ k[y_1, \ldots, y_n]/\mathbf{I}(W) & \xrightarrow{\alpha^*} & k[x_1, \ldots, x_m]/\mathbf{I}(V) \end{array} \qquad \begin{array}{ccc} \phi & \longmapsto & \phi \circ \alpha \\ \downarrow & & \downarrow \\ p + \mathbf{I}(W) & \longmapsto & (p \circ \alpha) + \mathbf{I}(V) \end{array}$$

wobei ι_W (bzw. ι_V) der Isomorphismus vom Koordinatenring mit dem Quotientenring ist (Vergleich Prop. 6.4). Nun beweisen wir die Proposition.

Beweis von Proposition 6.8. (i) Da α eine polynomielle Abbildung ist, existieren $a_1, \ldots, a_n \in k[x_1, \ldots, x_m]$ mit

$$\alpha(x_1, \ldots, x_n) = (a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)).$$

Sei nun $\phi\colon W \to k$ und sei $p \in k[y_1, \ldots, y_n]$ so, dass $\phi = p + \mathbf{I}(W)$. Es gilt dann

$$\phi \circ \alpha(x_1, \ldots, x_m) = p(a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)) + \mathbf{I}(V)$$

und somit ist die Abbildung wohldefiniert.
Weiter ist α^* ein Homomorphismums von k-Algebren (ÜA). Dies zeigt (i).

(ii) Sei $f\colon k[W] \to k[V]$ ein Homomorphismus von k-Algebren. Betrachte die Elemente

$$f(y_1 + \mathbf{I}(W)), \ldots, f(y_n + \mathbf{I}(W)) \in k[x_1, \ldots, x_m]/\mathbf{I}(V).$$

Es gibt Polynome $a_1, \ldots, a_n \in k[x_1, \ldots, x_m]$ mit $f(y_i + \mathbf{I}(W)) = a_i + \mathbf{I}(V)$ für alle $i = 1, \ldots, n$. Setze

$$\alpha := (a_1, \ldots, a_n)$$

Nach Definition ist α eine polynomielle Abbildung. Wir müssen noch zeigen

(a) $\alpha(V) \subseteq W$;

(b) $\alpha^* = f$;

(c) α ist eindeutig bestimmt.

Zunächst bemerken wir, dass für alle $p \in k[y_1, \ldots, y_n]$

$$f(p + \mathbf{I}(W)) = (p \circ \alpha) + \mathbf{I}(V) = (p + \mathbf{I}(W)) \circ \alpha \tag{10}$$

gilt.

Beweis von (a). Aus $\mathbf{V}(\mathbf{I}(W)) = W$ folgt $W = \{z \in k^m \mid p(z) = 0, \ \forall p \in \mathbf{I}(W)\}$. Um zu zeigen, dass $z \in W$ gilt, genügt also zu zeigen, dass für alle $p \in \mathbf{I}(W)$ schon $p(z) = 0$ gilt.
Sei also $(c_1, \ldots, c_m) \in V$ und sei $p \in \mathbf{I}(W)$ beliebig. Wir wollen zeigen, dass $p(\alpha(c_1, \ldots, c_m)) = 0$ gilt. Da $p \in \mathbf{I}(W)$ ist, ist $p + \mathbf{I}(W) = 0$ in $k[W]$. Da f ein Homomorphismus von k-Algebren ist, haben wir $0 = f(p + \mathbf{I}(W)) = p \circ \alpha + \mathbf{I}(V)$. Also $p \circ \alpha \in \mathbf{I}(V) \Rightarrow p \circ \alpha(c_1, \ldots, c_m) = 0$. Somit ist $p(\alpha(c_1, \ldots, c_m)) = 0$ für alle $p \in \mathbf{I}(W)$, d.h., $\alpha(c_1, \ldots, c_m) \in W$, wie gewünscht. $\square_{(a)}$

Beweis von (b). Nach Definition von α^* gilt

$$\alpha^*(p + \mathbf{I}(W)) = p \circ \alpha + \mathbf{I}(V) = f(p + \mathbf{I}(V)).$$

$\square_{(b)}$

Beweis von (c). Sei $\beta \colon V \to W$ eine weitere polynomielle Abbildung mit $\beta^* = f$. Da β polynomiell ist, existieren Polynome $b_1, \ldots, b_n \in k[x_1, \ldots, x_m]$ mit

$$\beta(x_1, \ldots, x_m) = (b_1(x_1, \ldots, x_m), \ldots, b_n(x_1, \ldots, x_m)).$$

Berechne für alle $i = 1, \ldots, n$

$$\begin{aligned} f(y_i + \mathbf{I}(W)) &= \beta^*(y_i + \mathbf{I}(W)) \\ &= (y_i + \mathbf{I}(W)) \circ \beta \\ &= b_i + \mathbf{I}(V) \end{aligned}$$

und ähnlich

$$\begin{aligned} f(y_i + \mathbf{I}(W)) &= \alpha^*(y_i + \mathbf{I}(W)) \\ &= (y_i + \mathbf{I}(W)) \circ \alpha \\ &= a_i + \mathbf{I}(V) \end{aligned}$$

Daraus folgt

$$a_i + \mathbf{I}(V) = b_i + \mathbf{I}(V), \quad \forall i = 1, \ldots, n$$

D.h., $a_i - b_i \in \mathbf{I}(V)$ und somit $a_i = b_i$ auf V. Daraus folgt, dass $\alpha = \beta$ auf V gilt. $\square_{(c)}$ $\square$

Bemerkung 6.9. *(o)* $\mathrm{Id}_V \colon V \to V$ *ist eine polynomiale Abbildung.*

(i) Für polynomielle Abbildungen γ, δ gilt $\gamma = \delta \Rightarrow \gamma^* = \delta^*$; Proposition 6.8 zeigt, dass die Umkehrung auch gilt.

(ii) Seien V_1, V_2, V_3 affine Varietäten und $\alpha \colon V_1 \to V_2$, $\beta \colon V_2 \to V_3$ polynomielle Abbildungen. Dann gilt $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$.

Definition 6.10 (Ch.5 §4 Def. 3)**.** *Sei k ein Körper und seien $V \subseteq k^m$ und $W \subseteq k^n$ affine Varietäten. Wir sagen, dass V und W zueinander isomorph sind, falls polynomielle Abbildungen $\alpha\colon V \to W$ und $\beta\colon W \to V$ existieren, mit $\alpha \circ \beta = \mathrm{Id}_W$ und $\beta \circ \alpha = \mathrm{Id}_V$.*

Satz 6.11 (Ch. 5 §4 Theorem 9)**.** *Sei k ein Körper und seien $V \subseteq k^m$ und $W \subseteq k^n$ affine Varietäten. V und W sind genau dann als affine Varietäten isomorph, wenn $k[V]$ und $k[W]$ als k-Algebren isomorph sind:*

$$V \simeq W \iff k[V] \simeq k[W].$$

Beweis. ($\Rightarrow$) Seien $\alpha\colon V \to W$ und $\beta\colon W \to V$ polynomielle Abbildungen, mit $\alpha \circ \beta = \mathrm{Id}_W$ und $\beta \circ \alpha = \mathrm{Id}_V$. Dann gilt

$$\beta^* \circ \alpha^* = (\alpha \circ \beta)^* = (\mathrm{Id}_W)^* = \mathrm{Id}_{k[W]}$$

und ähnlich $\alpha^* \circ \beta^* = \mathrm{Id}_{k[V]}$. So sind α^* und β^* (zueinander inverse) Isomorphismen zwischen $k[V]$ und $k[W]$, also $k[V] \simeq k[W]$.

($\Leftarrow$) Bemerke zunächst, dass Id_W eine polynomielle Abbildung ist, die $\mathrm{Id}_W^*(\phi) = \phi$ für alle $\phi \in k[W]$ erfüllt. Sei nun $f\colon k[W] \to k[V]$ ein Isomorphismus von k-Algebren. Dann ist $f^{-1}\colon k[V] \to k[W]$ auch ein Isomorphismus von k-Algebren. Proposition 6.8(ii) liefert eindeutige $\alpha\colon V \to W$ und $\beta\colon W \to V$ mit $f = \alpha^*$ und $f^{-1} = \beta^*$. Wir wollen jetzt zeigen, dass $\alpha = \beta^{-1}$. Es gelten

$$(\alpha \circ \beta)^* = \beta^* \circ \alpha^* = f^{-1} \circ f = \mathrm{Id}_{k[W]}$$

und

$$(\beta \circ \alpha)^* = \alpha^* \circ \beta^* = f \circ f^{-1} = \mathrm{Id}_{k[V]}$$

Aus der Eindeutigkeit von α (bzw. β) folgt, dass $\alpha = \beta^{-1}$ (bzw. $\beta = \alpha^{-1}$) gelten muss. □

20. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 18.01.2022

Kapitel 5, Abschnitt 3 im Buch von Cox, Little und O'Shea 2006

7 Algorithmisches Rechnen in $\mathbf{k[x_1, \ldots, x_n]/I}$

Erinnerung: die folgende beide Resultaten über Gröbnerbasen wurden in der 7. Vorlesung gezeigt.

Proposition 7.1 (Prop. 3.32, oder Ch.2, §6, Prop. 1 im Buch). *Sei* $\{0\} \neq I \trianglelefteq k[x_1, ..., x_n]$ *und* $G = \{g_1, ..., g_t\}$ *eine Gröbnerbasis von* I. *Sei* $0 \neq f \in k[x_1, ..., x_n]$, *dann existiert ein eindeutiger Rest* $r \in k[x_1, ..., x_n]$ *mit den folgenden Eigenschaften:*

i) Kein Term von r *ist teilbar durch* $\mathrm{LT}(g_i)$ *(für alle* $i = 1, ..., t$*)*

ii) $f = g + r$ *für ein geeignetes* $g \in I$

Das heißt r *ist der eindeutige Rest im Divisionsalgorithmus von* f *durch* $(g_1, ..., g_t)$. □

Korollar 7.2 (Kor. 3.33 oder Ch. 2, §6, Cor. 2 im Buch). *Sei* $G = \{g_1, ..., g_t\}$ *eine Gröbnerbasis von* I *und* $0 \neq f \in k[x_1, ..., x_n]$.
Dann gilt $f \in I$ *gdw. der Rest von* f *im Divisionsalgorithmus durch* G *gleich Null ist.*
Gleiche Aussage in äquivalenten Notationen:

$$\begin{aligned} \bar{f}^G = 0 &\Leftrightarrow f \equiv 0 \pmod{I} \\ &\Leftrightarrow [f] = 0 \\ &\Leftrightarrow \bar{f} = 0. \end{aligned}$$

□

Proposition 7.3 (Ch. 5, §3, Prop 1). *Seien* $>$ *eine monomiale Anordnung auf* $k[x_1, \ldots, x_n]$ *und* $I \trianglelefteq k[x_1, \ldots, x_n]$. *Betrachte den* k*-Vektorraum* $S = \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}$. *Dann*

(i) Für alle $f \in k[x_1, \ldots, x_n]$ *existiert ein eindeutiges* $r \in S$ *so, dass* $f \equiv r \pmod{I}$;

(ii) die Menge $\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}$ *ist* k*-linear unabhängig* $\pmod{I}$.

Beweis. (i) Sei G eine Gröbnerbasis für I und setze $r := \bar{f}^G$. Proposition 3.32 impliziert, dass $f - r \in I$.

(ii) Seien $c_\alpha \in k^\times$ so, dass $\sum c_\alpha x^\alpha = 0 \pmod I$. Dann ist $\sum c_\alpha \in I$. Nach Definition von Leittermideal gilt dann $\mathrm{LT}\left(\sum c_\alpha\right) \in \mathrm{LT}(I)$. Nun $\mathrm{LT}\left(\sum c_\alpha\right) = c_\gamma x^\gamma$ für ein gewisses γ mit $c_\gamma \neq 0$. Aber $x^\gamma \notin \mathrm{LT}(I)$. Widerspruch.

□

Erinnerung: in ÜB 3 wurden folgende Identitäten gezeigt (Ch.2, §6, Exercise 12). Seien $f, g \in k[x_1, \ldots, x_n]$, $I \trianglelefteq k[x_1, \ldots, x_n]$ und G eine Gröbnerbasis für I. Sei, weiter, $S = \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I)\rangle\}$. Dann gelten

(i) $[f] + [g] = [\bar{f} + \bar{g}]$ und $\bar{f} + \bar{g} \in S$

(ii) $[f] \cdot [g] = [\overline{\bar{f} \cdot \bar{g}}^G]$ und $\overline{\bar{f} \cdot \bar{g}}^G \in S$

Proposition 7.4 (Ch. 5, §3, Prop 4)**.** *Seien $I \trianglelefteq k[x_1, \ldots, x_n]$ und G eine Gröbnerbasis von I bezüglich einer monomialen Anordnung $>$ auf $k[x_1, \ldots, x_n]$. Betrachte den k-Vektorraum $S = \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I)\rangle\}$. Dann ist die Funktion*

$$\begin{array}{rccc} \Phi\colon & k[x_1, \ldots, x_n] & \to & S \\ & f & \mapsto & \bar{f}^G \end{array}$$

eine surjektive k-lineare Abbildung mit $\ker \Phi = I$.

Beweis. Φ ist offensichtlich wohldefiniert. Seien nun $f, g \in k[x_1, \ldots, x_n]$ und $c \in k$. Es gelten

- $\Phi(f + g) = \overline{f + g}^G \overset{\text{ÜB3}}{=} \bar{f}^G + \bar{g}^G = \Phi(f) + \Phi(g)$.
- $\Phi(cf) = \overline{cf}^G \overset{\text{ÜA}}{=} c\bar{f}^G = c\Phi(f)$.

Für die Surjektivität, sei $f := \sum c_\alpha x^\alpha \in S$. Dann ist offensichtlich $\Phi(f) = f$.

Zuletzt, Korollar 3.33 sagt genau, dass $f \in I \iff \bar{f}^G = \Phi(f) = 0$, d. h., $\ker \Phi = I$. □

Bemerkung 7.5. *Wegen der Eigenschaft $[f] \cdot [g] = [\overline{\bar{f} \cdot \bar{g}}^G]$, ist Φ bloß ein Isomorphismus von k-Vektorräume, aber nicht von k-Algebren, da er nicht multiplikativ ist.*

Anwendung: nun wollen wir algorithmisch bestimmen, ob eine Varietät $V \subseteq k^n$ endlich ist, für den Fall wo k algebraisch abgeschlossen ist.

Satz 7.6 (Charakterisierung von endlichen Varietäten über algebraisch abgeschlossenen Körpern – Ch. 5, §3, Th. 6)**.** *Seien k ein alg. abgeschlossener Körper und $V = \mathbf{V}(I) \subseteq k^n$ eine affine Varietät. Seien weiter $>$ eine monomiale Anordnung auf $k[x_1, \ldots, x_n]$, G eine Gröbnerbasis für I und $S = \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I)\rangle\}$. Die folgende Aussagen sind äquivalent*

(i) V *ist endlich;*

(ii) Für alle $i \in \{1, \ldots, n\}$ *gibt es ein* $m_i \in \mathbb{N}_0$ *mit* $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$*;*

(iii) Für alle $i \in \{1, \ldots, n\}$ *gibt es ein* $n_i \in \mathbb{N}_0$ *und ein* $g \in G$ *mit* $x_i^{n_i} = \mathrm{LM}(g)$*;*

(iv) $\dim_k S$ *ist endlich;*

(v) $\dim_k k[x_1, \ldots, x_n]/I$ *ist endlich.*

Beweis. $(iv) \iff (v)$ folgt direkt aus Proposition 7.4.
$(ii) \iff (iii)$ folgt aus Lemma 3.18 (ÜA).
$(i) \Rightarrow (ii)$. Wir unterscheiden zwei Fälle:

Fall 1: $V = \emptyset$. Nach dem Nullstellensatz ist dann $1 \in I$. Wir können also setzen $m_i = 0$ für alle i, dann ist $x_i^{m_i} = 1 \in \langle \mathrm{LT}(I) \rangle$.

Fall 2: $V \neq \emptyset$. Für jedes $i \in \{1, \ldots, n\}$ sei $\{a_j \mid j = 1, \ldots, l_i\}$ die Menge aller Elementen aus k mit $a_j = \pi_i(P)$ für ein $P \in V$. Also die Menge aller i-ten Koordinaten von Punkten von V. Setze nun

$$f(x_i) := \prod_{j=1}^{l_i} (x_i - a_j)$$

Dann verschwindet f auf V, d. h., $f \in \mathbf{I}(V)$. Der Nullstellensatz ergibt dann ein $m \in \mathbb{N}_0$ mit $f^m \in I$. Dann ist $\mathrm{LM}(f^m) = x_i^{ml_i} \in \langle \mathrm{LM}(I) \rangle$. Die Behauptung ist somit mit $m_i := ml_i$ bewiesen.
$(ii) \Rightarrow (iv)$. Aus (ii) folgt, dass $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \in \langle \mathrm{LT}(I) \rangle$ wenn $\alpha_i \geq m_i$. Es gilt also $x^\alpha \notin \langle \mathrm{LT}(I) \rangle \Rightarrow \alpha_i < m_i$ für alle i. Dann $\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\} \subseteq \{x^\alpha \mid 1 \leq \alpha_i \leq m_i\}$ und ist damit endlich. Also auch $\dim_k S < \infty$.
$(v) \Rightarrow (i)$. Sei $i \in \{1, \ldots, n\}$ fest. Betrachte $\{[x_i^j] \mid j \in \mathbb{N}_0\}$. Diese Menge muss k-linear abhängig sein (nach (v), weil sie unendlich ist). Dann existieren $m_i \in \mathbb{N}_0$ und $c_j \in k$ für $j = 0, \ldots, m_i$ so, dass

$$\sum_{j=0}^{m_i} c_j [x_i^j] = \left[\sum_{j=0}^{m_i} c_j x_i^j \right] = [0]$$

das heißt, $q_i := \sum_{j=0}^{m_i} c_j x_i^j \in I \subseteq \mathbf{I}(V)$ und, daher, verschwinden die q_i's auf V. Ein von 0 verschiedenes Polynom hat endlich viele verschiedene Wurzeln. Daher können die Punkte von V nur endlich viele verschiedene i-te Koordinaten, für alle i und, somit, es gibt insgesamt endlich viele Punkte in V. □

21. Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 20.01.2022

Lemma 7.7. *Sei k ein Körper und seien $p_1, \ldots, p_m \in k^n$ paarweise verschiedene Elemente. Dann existieren $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ so, dass $f_i(p_j) = \delta_{ij}$ für alle $i, j = 1, \ldots, m$.*

Beweis. **Behauptung:** Es existiert $f_1 \in k[x_1, \ldots, x_n]$ mit $f_1(p_i) = 1$ und $f_1(p_j) = 0$ für alle $j = 2, \ldots, m$.

In der Tat: Seien $a \neq b \in k^n$. Dann existiert $j \leq n$ mit $a_j \neq b_j$. Setze

$$g := \frac{x_j - b_j}{a_j - b_j}.$$

Man prüft dann leicht, dass $g(a) = 1$ und $g(b) = 0$ gelten. Wiederhole dieses Verfahren für alle Paare p_1, p_i, $i = 2, \ldots, m$ anstatt a, b, und erhalte Polynome $g_2, \ldots, g_m$ so, dass $g_i(p_1) = 1$ und $g_i(p_j) = 0$ für alle $j \geq 2$. Setze nun $f_1 := \prod_{i=2}^{m} g_i$. Dann erfüllt f_1 die verlangte Eigenschaft. $\square_{\textbf{Beh.}}$

Wiederhole für alle anderen Punkte $p_2, \ldots, p_m$ und bekomme die restlichen Polynome $f_2, \ldots, f_m$. $\square$

Satz 7.8 (Kardinalität einer endlichen Varietät – Ch. 5, §3, Prop. 8)**.** *Sei k algebraisch abgeschlossen und sei $V = \mathbf{V}(I) \subseteq k^n$ eine endliche affine Varietät. Dann gelten*

(i) $|V| \leq \dim_k (k[x_1, \ldots, x_n]/I)$ *wobei* $\dim_k$ *die Dimension als k-Vektorraum bezeichnet.*

(ii) Falls $I = \sqrt{I}$ ein Radikalideal ist, dann gilt $|V| = \dim_k (k[x_1, \ldots, x_n]/I)$.

Beweis. Sei $m := |V|$ und schreibe $V = \{p_1, \ldots, p_m\}$. Lemma 7.7 liefert Polynomen $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ mit $f_i(p_j) = \delta_{ij}$.

(i) Wir zeigen, dass die Nebenklassen $[f_1], \ldots, [f_m] \in k[x_1, \ldots, x_n]/I$ linear unabhängig sind. Seien also $a_1, \ldots, a_m \in k$ mit $\sum a_i[f_i] = [0]$. Also $\tilde{f} := \sum a_i f_i \in I$ und daher verschwindet $\tilde{f}$ auf V. Für alle $j = 1, \ldots, m$ gilt also $\tilde{f}(p_j) = a_j = 0$. Dies zeigt die k-lineare Unabhängigkeit der $[f_i]$'s und somit

$$|V| = m \leq \dim_k (k[x_1, \ldots, x_n]/I).$$

(ii) Sei nun I radikal. Aus (i) wissen wir, dass $[f_1], \ldots, [f_m]$ linear unabhängig sind. Es genügt also zu zeigen, dass sie $k[x_1, \ldots, x_n]/I$ erzeugen. Sei also $[g] \in k[x_1, \ldots, x_n]/I$ beliebig.

Setze $a_i := g(p_i)$ und

$$h := g - \sum_{i=1}^{m} a_i f_i.$$

Es gilt also $h(p_j) = 0$ für alle $j = 1, \ldots, m$ und somit $h \in \mathbf{I}(V) = \sqrt{I} = I$. Also

$$[g] - \sum_{i=1}^{m} a_i [f_i] = [h] = [0]$$

d.h., $[g]$ ist eine k-Linearkombination der $[f_i]$'s, wie gewünscht.

□

Korollar 7.9 (Ch.5, §3, Cor. 7)**.** *Seien k algebraisch abgeschlossen und $I \trianglelefteq k[x_1, \ldots, x_n]$ so, dass für jedes $i = 1, \ldots, n$ ein $m_i \in \mathbb{N}_0$ gibt, mit $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$. Dann ist $|\mathbf{V}(I)| \leq m_1 \cdots m_n$.*

Beweis. Im Beweis vom Satz 7.6 (Implikation $(ii) \Rightarrow (iv)$) wurde gezeigt, dass $|\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}| \leq m_1 \cdots m_n$ gilt. Daraus folgt, dass $\dim_k \mathrm{Span}_k (\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}) \leq m_1 \cdots m_n$ gilt. Satz 7.8 ergibt nun

$$|\mathbf{V}(I)| \leq \dim_k(k[x_1, \ldots, x_n]/I) \leq \dim_k \mathrm{Span}_k (\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}) \leq m_1 \cdots m_n$$

□

Übungsaufgabe: Sei $I \trianglelefteq k[x_1, \ldots, x_n]$ so, dass es für alle i ein $m_i \in \mathbb{N}_0$ mit $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$ gibt. Geben Sie ein Kriterium an, um zu bestimmen, ob $\mathbf{V}(I)$ genau $m_1 \cdots m_n$ Punkte enthält.

8 Rationale Funktionen auf Varietäten

Ch. 5, §5 im Buch.

Definition 8.1 (Ch. 5, §5, Def. 4)**.** *Seien $V \subseteq k^m$ und $W \subseteq k^n$ irreduzible affine Varietäten. Eine rationale Abbildung ϕ von V nach W ist eine Abbildung die durch rationalen Funktionen dargestellt ist:*

$$\phi(x_1, \ldots, x_m) = \left(\frac{f_1(x_1, \ldots, x_m)}{g_1(x_1, \ldots, x_m)}, \ldots, \frac{f_n(x_1, \ldots, x_m)}{g_n(x_1, \ldots, x_m)} \right) \qquad \text{mit } g_i \not\equiv 0$$

so, dass

(i) ϕ auf einem Punkt $p \in V$ definiert ist, d.h., $\mathbf{V}_V(g_1 \cdots g_n) \subsetneq V$;

(ii) für alle $(a_1, \ldots, a_m) \in V$, auf denen ϕ definiert ist, $\phi(a_1, \ldots, a_m) \in W$ gilt.

Notation 8.2. *Eine rationale Abbildung wird mit $\phi\colon V \dashrightarrow W$ bezeichnet. Dabei ist zu bemerken, dass ϕ keine echte Funktion im mengentheoretischen Sinn ist, da V nicht der echte Definitionsbereich ist.*

Definition 8.3. *Sei $V \subseteq k^n$ eine irreduzible affine Varietät. Die Menge $k(V)$ aller skalaren rationalen Funktionen $\phi\colon V \dashrightarrow k$ heißt der Körper der rationalen Funktionen auf V.*

Bemerkung 8.4. *Die Korrespondenz*

$$\begin{array}{ccc} \mathrm{Quot}(k[V]) & \longrightarrow & k(V) \\ [f]/[g] & \longmapsto & \Big(\phi\colon \quad V \quad \dashrightarrow \quad k\Big), \end{array}$$

wobei ϕ durch f/g dargestellt ist, ist ein wohldefinierter Körperisomorphismus.

Wir bemerken auch, die Gleichheit folgender Ausdrücken:

$$\begin{aligned} \left\{ \frac{\phi}{\psi} : \phi, \psi \in k[V],\ \psi \neq 0 \right\} &= \left\{ \frac{\bar{f}}{\bar{g}} : f, g \in k[x_1, \ldots, x_m],\ g \notin \mathbf{I}(V) \right\} \\ &= \left\{ \frac{[f]}{[g]} : f, g \in k[x_1, \ldots, x_m],\ [g] \neq [0] \right\} \end{aligned}$$

22 Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 25.01.2022

In dieser Vorlesung untersuchen wir weiter die rationale Abbildungen und bereiten wir uns für die Untersuchung der birationalen Äquivalenz vor. Zunächst definieren wir, wenn zwei rationale Abbildungen gleich sind.

Definition 8.5 (Ch. 5, §5, 5 – Gleichheit von rationalen Abbildungen)**.** *Seien $V \subseteq k^m$ und $W \subseteq k^n$ affine Varietäten, wobei V irreduzible ist. Seien, ferner, $\phi, \psi \colon V \dashrightarrow W$ rationale Abbildungen, dargestellt durch*

$$\phi = \left(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}\right) \qquad \textit{und} \qquad \psi = \left(\frac{h_1}{k_1}, \ldots, \frac{h_n}{k_n}\right)$$

mit $f_i, g_i, h_i, k_i \in k[x_1, \ldots, x_m]$. Wir sagen, dass ϕ und ψ gleich sind ($\phi = \psi$), falls für alle $i = 1, \ldots, n$

$$f_i k_i - h_i g_i \in \mathbf{I}(V)$$

gilt.

Nun geben wir eine geometrische Interpretation des obigen Begriffs von Gleichheit an. Dafür brauchen wir erst eine Erinnerung aus der 15. Vorlesung.

Definition 8.6. *(Def. 5.18) Sei $S \subseteq k^n$. Der Zariski Abschluss von S in k^n ist die Varietät $\bar{S} = \mathbf{V}(\mathbf{I}(S))$. Insbesondere, weil $V = \mathbf{V}(\mathbf{I}(V))$ für jede Varietät V gilt, dann sind die affine Varietäten genau die Zariski-abgeschlossene Mengen in k^n.*

Nun ist eine Varietät $V \subseteq k^n$, versehen mit der Zariski Topologie, ein topologischer Raum. Die Zariski-abgeschlossene Teilmengen von V sind die affine Untervarietäten von V. Daher sind die Zariski-offene Teilmengen genau die Mengen der Form $U = V \setminus V'$ wobei V' eine Untervarietät von V ist.

Proposition 8.7 (Ch. 5, §5, Prop. 6)**.** *Seien $V \subseteq k^m$ und $W \subseteq k^n$ affine Varietäten, wobei V irreduzible ist. Seien, ferner, $\phi, \psi \colon V \dashrightarrow W$ rationale Abbildungen. Dann sind ϕ und ψ genau dann gleich, wenn es eine echte Untervarietät $V' \subset V$ gibt, sodass*

(i) ϕ, ψ sind definiert auf $V \setminus V'$

(ii) für alle $p \in V \setminus V'$ gilt $\phi(p) = \psi(p)$

Anders gesagt, ϕ und ψ sind genau dann gleich, wenn sie auf einer Zariski-offene Teilmenge von V abstimmen.

Für den Beweis brauchen wir ein

Lemma 8.8. *Sei $V \subseteq k^m$ eine irreduzible affine Varietät und sei $V' \subset V$ eine echte Untervarietät. Dann gelten*

(i) $\mathbf{I}(V) \subsetneq \mathbf{I}(V')$

(ii) $\mathbf{I}(V) = \mathbf{I}(V \setminus V')$

(iii) Aus (ii) folgt direkt, dass für alle $h \in k[x_1, \ldots, x_m]$ gilt, dass h genau dann auf V verschwindet, wenn es auf $V \setminus V'$ verschwindet.

Beweis. (i) Da $V' \subset V$, folgt aus der Kontravarianz von $\mathbf{I}$, dass $\mathbf{I}(V) \subseteq \mathbf{I}(V')$. Gleichheit kann nicht gelten, sonst würde aus $\mathbf{I}(V) = \mathbf{I}(V')$ direkt $V = \mathbf{V}(\mathbf{I}(V)) = \mathbf{V}(\mathbf{I}(V')) = V'$ folgen.

(ii) Nochmal aus der Kontravarianz folgt $(V \setminus V') \subset V \Rightarrow \mathbf{I}(V) \subseteq \mathbf{I}(V \setminus V')$. Zum Widerspruch, nehmen wir an, dass die Inklusion echt sei. Sei also $f \notin \mathbf{I}(V)$ mit $f \in \mathbf{I}(V \setminus V')$. Sei nun $g \in \mathbf{I}(V')$ beliebig. Dann gilt $fg \in \mathbf{I}(V)$. Da V irreduzible und, daher, $\mathbf{I}(V)$ Prim ist, aus $f \notin \mathbf{I}(V)$ folgt $g \in \mathbf{I}(V)$. Es gilt also $\mathbf{I}(V') \subseteq \mathbf{I}(V)$. Die andere Inklusion gilt nach der Kontravarianz und somit $\mathbf{I}(V) = \mathbf{I}(V')$. Widerspruch zu (i).

□

Nun können wir die Proposition beweisen

Beweis von Prop. 8.7. Seien $\phi = (f_1/g_1, \ldots, f_n/g_n)$ und $\psi = (h_1/k_1, \ldots, h_n/k_n)$ mit $\phi = \psi$. Setze $V_1 = \mathbf{V}(g_1 \cdots g_n)$ und $V_2 = \mathbf{V}(k_1 \cdots k_n)$.Nach der Definition von rationalen Abbildungen sind V_1, V_2 echte Untervarietäten von V. Da aber V irreduzibel ist, gilt also dass auch $V' := V_1 \cup V_2$ eine echte Untervarietät ist (sonst wäre $V = V_1 \cup V_2$ eine Zerlegung von V). Dann sind ϕ und ψ auf $V \setminus V'$ definiert. Außerdem gilt $f_i k_i - h_i g_i \in \mathbf{I}(V)$ für alle $i = 1, \ldots, n$. Es folgt dann, dass $f_i/g_i = h_i/k_i$ auf V und, insbesondere, auf $V \setminus V'$.

Umgekehrt, sei $V' \subsetneq V$ eine echte Untervarietät so, dass für jeden $p \in V \setminus V'$ die Gleichung $\phi(p) = \psi(p)$ gilt. Insbesondere, gilt $f_i/g_i = h_i/k_i$ auf $V \setminus V'$, d.h. $f_i/g_i - h_i/k_i$ verschwindet auf $V \setminus V'$ für alle $i = 1, \ldots, n$. Lemma 8.8 liefert dann $f_i/g_i - h_i/k_i \in \mathbf{I}(V)$. □

Jetzt bestimmen wir, wenn die Verknüpfung zweier rationalen Abbildungen definiert ist.

Definition 8.9 (Ch. 5, §5, Def. 7)**.** *Seien $V \subseteq k^m$, $W \subseteq k^n$, $Z \subseteq k^l$ drei affine irreduzible Varietäten und seien $\phi\colon V \dashrightarrow W$ und $\psi\colon W \dashrightarrow Z$ rationale Abbildungen. Wir sagen, dass $\psi \circ \phi\colon V \dashrightarrow Z$ definiert ist, falls es einen Punkt $p \in V$ gibt, so dass ϕ auf p und ψ auf $\phi(p)$ definiert sind.*

Proposition 8.10 (Ch. 5, §5, Prop. 8)**.** *Seien $V \subseteq k^m$, $W \subseteq k^n$, $Z \subseteq k^l$ drei affine irreduzible Varietäten und seien $\phi\colon V \dashrightarrow W$ und $\psi\colon W \dashrightarrow Z$ rationale Abbildungen so, dass $\psi \circ \phi$ definiert ist. Dann gibt es eine echte Untervarietät $V' \subsetneq V$ mit*

(i) ϕ ist auf $V \setminus V'$ definiert und ψ ist auf $\phi(V \setminus V')$ definiert.

(ii) $\psi \circ \phi\colon V \dashrightarrow Z$ ist eine rationale Abbildung definiert auf $V \setminus V'$.

Beweis. Seien $\phi = (f_1/g_1, \ldots, f_n/g_n)$ und $\psi = (h_1/k_1, \ldots, h_l/k_l)$. Wir ersetzen (formal)

$$\frac{h_j(f_1/g_1, \ldots, f_n/g_n)}{k_j(f_1/g_1, \ldots, f_n/g_n)}$$

für alle $j = 1, \ldots, l$. Nachdem wir mit einer geeigneten Potenz $(g_1 \cdots g_n)^M$ multiplizieren, damit alle Nenner von $h_j(f_1/g_1, \ldots, f_n/g_n)$ und $k_j(f_1/g_1, \ldots, f_n/g_n)$ gekürzt werden, können wir schreiben

$$\frac{P_j}{Q_j} = \frac{(g_1 \cdots g_n)^M h_j(f_1/g_1, \ldots, f_n/g_n)}{(g_1 \cdots g_n)^M k_j(f_1/g_1, \ldots, f_n/g_n)}$$

wobei $P_j, Q_j \in k[x_1, \ldots, x_m]$. Die durch $(P_1/Q_1, \ldots, P_l/Q_l)$ dargestellte rationale Abbildung ist also unser Kandidat für $\psi \circ \phi$.

Setze nun $V' := \mathbf{V}_V(g_1 \cdots g_n \cdot Q_1 \cdots Q_l) \subseteq V$. Dann ist ϕ auf $V \setminus V'$ definiert und ψ auf $\phi(V \setminus V')$. Es bleibt zu zeigen, dass $V' \neq V$. Nach Annahme, gibt es einen Punkt $p \in V$ so, dass $\phi(p)$ und $\psi(\phi(p))$ definiert sind. Dies bedeutet, dass für alle $i = 1, \ldots, n$ und alle $j = 1, \ldots, l$

$$g_i(p) \neq 0 \qquad \text{und} \qquad k_j(f_1(p)/g_1(p), \ldots, f_n(p)/g_n(p)) \neq 0$$

gelten. Es folgt, dass $Q_j(p) \neq 0$ und, daher, $p \in V \setminus V'$ und, somit, $V \neq V'$. □

23 Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 27.01.2022

Definition 8.11 (Ch. 5, §5, Def. 9 – Birationale Äquivalenz)**.** *Seien $V \subseteq k^m$ und $W \subseteq k^n$ irreduzible affine Varietäten.*

(i) Wir sagen, dass V und W birational äquivalent sind, falls es rationale Abbildungen $\phi\colon V \dashrightarrow W$ und $\psi\colon W \dashrightarrow V$ existieren, so dass $\phi\circ\psi$ und $\psi\circ\phi$ definiert mit $\phi\circ\psi = \mathrm{Id}_W$ und $\psi\circ\phi = \mathrm{Id}_V$ sind.

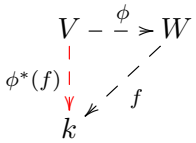
Birationale Äquivalenz ist eine Äquivalenzrelation (ÜA).

(ii) Eine rationale Varietät ist eine Varietät die birational äquivalent zu k^n ist, für ein $n \in \mathbb{N}_0$.

Satz 8.12 (Ch. 5, §5, Theorem 10 – Charakterisierung von birational äquivalenten Varietäten)**.** *Zwei irreduzible affine Varietäten $V \subseteq k^m$ und $W \subseteq k^n$ sind genau dann birational äquivalent, wenn es eine k-Isomorphie $\iota\colon k(V) \to k(W)$ gibt ("k-Isomorphie" bedeutet, dass $\iota|_k = \mathrm{Id}_k$ gilt).*

Beweis. Die Rückrichtung "$\Leftarrow$" wird im Übungsblatt 12 gezeigt (Hinweis: Ch. 5, §4, Satz 9).

"$\Rightarrow$". Seien $\phi\colon V \dashrightarrow W$ und $\psi\colon W \dashrightarrow V$ rationale Abbildungen mit $\phi\circ\psi = \mathrm{Id}_W$ und $\psi\circ\phi = \mathrm{Id}_V$. Um einen Isomorphismus $\phi^*\colon k(W) \to k(V)$ zu definieren, betrachten wir $\phi\colon V \dashrightarrow W$ und $f\colon W \dashrightarrow k$, für jedes $f \in k(W)$. Wir definieren also $\phi^*(f) := f\circ\phi$



Nun wollen wir zeigen, dass $\phi^*(f)$ eine rationale Abbildung ist, d.h., dass ein $p \in V$ existiert so dass $f(\phi(p))$ definiert ist.
Behauptung: Wenn $\phi\circ\psi = \mathrm{Id}_W$, dann gibt es eine echte Untervarietät $W' \subsetneq W$ mit

$$\begin{cases} \psi \text{ ist auf } W \setminus W' \text{ definiert,} \\ \phi \text{ ist auf } \psi(W \setminus W') \text{ definiert,} \\ \phi\circ\psi \text{ ist gleich } \mathrm{Id}_W \text{ auf } W \setminus W'. \end{cases} \tag{11}$$

Beweis der Behauptung: Proposition 8.10 liefert eine echte Untervarietät $W_1 \subsetneq W$ so, dass ψ ist auf $W \setminus W_1$ definiert und ϕ auf $\psi(W \setminus W_1)$ definiert ist. Proposition 8.7 liefert nun eine echte Untervarietät $W_2 \subsetneq W$ so, dass $\phi\circ\psi$ die Identität auf $W \setminus W_2$ ist. Da W irreduzibel ist, ist $W' = W_1 \cup W_2$ eine echte Untervarietät von W. Es folgt nun, dass (11) von W' erfüllt ist.$\square_{Beh.}$

Um zu zeigen, dass $f \circ \phi$ definiert ist, wähle Räpresentanten $g, h \in k[x_1, \ldots, x_n]$ mit $g \neq 0$ und $f = h/g$ und setze $W'' = \mathbf{V}_W(g)$. So ist f auf $W \setminus W''$ definiert. Sei nun $q \in W \setminus (W' \cup W'')$ (dies ist auch nicht leer, weil W irreduzibel ist). Sei dann $p := \psi(q) \in V$. Aus der Bedingungen (11) folgt, dass $\phi(p)$ definiert ist und, weil $\phi(p) = q \notin W''$, ist f auf $\phi(p)$ definiert. Somit ist $\phi^*(f) = f \circ \phi$ als Element aus $k(V)$ definiert und daher ist auch

$$\begin{array}{rccc} \phi^*\colon & k(W) & \longrightarrow & k(V) \\ & f & \longmapsto & f \circ \phi \end{array}$$

wohldefiniert.

Analog definieren wir $\psi^*\colon k(V) \to k(W)$.

ϕ^* und ψ^* sind Homomorphismen (ÜA).

Wir zeigen nun, dass ϕ^* und ψ^* zueinander invers sind. Sei $f \in k(W)$ und betrachte

$$(\psi^* \circ \phi^*)(f) = f \circ \phi \circ \psi.$$

Auf $W \setminus (W' \cup W'')$ gilt $f \circ \phi \circ \psi = f$, also $f \circ \phi \circ \psi$ und f sind gleich in $k(W)$. Analog zeigt man, dass $h \circ \psi \circ \phi = h$ in $k(V)$, für alle $h \in k(V)$ und somit ist der Satz bewiesen.

□

9 Projektive algebraische Geometrie

9.1 Die Projektive Ebene

ÜA: Cox, Little und O'Shea 2006, Ch. 8, §1 lesen.

9.2 Der Projektive Raum

Seien k ein Körper und $n \in \mathbb{N}_0$.

Definition 9.1. *(i) Wir definieren eine Äquivalenzrelation $\sim$ auf $k^{n+1} \setminus \{0\}$ durch*

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists \lambda \in k^\times : (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$$

Also es werden Punkte miteinander identifiziert, die auf derselben Geraden durch den Ursprung liegen.

(ii) Der <u>n-dimensionaler projektiver Raum über k</u> ist die Menge aller Äquivalenzklassen

$$\begin{aligned} \mathbb{P}^n(k) &:= (k^{n+1} \setminus \{0\})/\sim \\ &= \{[(x_0, \ldots, x_n)]_\sim \mid (x_0, \ldots, x_n) \in k^{n+1} \setminus \{0\}\} \end{aligned}$$

(iii) Wir schreiben $(x_0 : \ldots : x_n)$ für $[(x_0, \ldots, x_n)]_\sim \in \mathbb{P}^n(k)$ und nenne diese die <u>homogenen Koordinaten</u> von $(x_0, \ldots, x_n)$.

Bemerkung 9.2. *Bezeichnet $\mathcal{L}$ die Menge aller Ursprungsgeraden in k^{n+1}, dann ist $\mathbb{P}^n(k) \simeq \mathcal{L}$.*

Proposition 9.3 (Ch. 8, §2, Prop. 2)**.** *Sei*

$$U_0 = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n(k) \mid x_0 \neq 0\}$$

Die Abbildung

$$\begin{array}{rccc} \phi\colon & k^n & \to & U_0 \\ & (x_1, \ldots, x_n) & \mapsto & (1 : x_1 : \ldots : x_n) \end{array}$$

ist eine Bijektion. Damit wird k^n in $\mathbb{P}^n(k)$ eingebettet.

Beweis. ϕ ist wohldefiniert. In der Tat, seien $p, p' \in U_0$ mit $p \sim p'$, d.h., $p = (x_0 : \ldots : x_n)$, $p' = (y_0 : \ldots : y_n)$ und es gibt $\lambda \in k^\times$ mit $y_i = \lambda x_i$. Dann gilt

$$\psi(p') = \left(\frac{y_1}{y_0}, \cdots, \frac{y_n}{y_0}\right) = \left(\frac{\lambda x_1}{\lambda x_0}, \cdots, \frac{\lambda x_n}{\lambda x_0}\right) = \left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right).$$

Um die Bijektivität zu zeigen, definieren wir eine inverse Abbildung ψ durch

$$\begin{array}{rccc} \psi\colon & U_0 & \to & k^n \\ & (x_0 : \ldots : x_n) & \mapsto & \left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \end{array}$$

Dies ist auch wohldefiniert, da für $(x_0 : \ldots : x_n) \in U_0$ schon $x_0 \neq 0$ ist.

Sei nun $(x_1, \ldots, x_n) \in k^n$. Dann ist

$$\psi(\phi((x_1, \ldots, x_n))) = \psi(1 : x_1 : \ldots : x_n) = \left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right) = (x_1, \ldots, x_n)$$

also $\psi \circ \phi = \mathrm{Id}_{k^n}$.

Sei umgekehrt $(x_0 : \ldots : x_n) \in U_0$. Dann ist

$$\phi(\psi(x_0 : \ldots : x_n)) = \phi\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) = \left(1 : \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) = (x_0 : \ldots : x_n)$$

wobei wir in der letzten Gleichung mit $x_0 \in k^\times$ multipliziert haben, und daher bezeichnen $\left(1 : \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$ und $(x_0 : \ldots : x_n)$ den gleichen Punkt in $\mathbb{P}^n(k)$. □

24 Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 01.02.2022

Sei k stets ein Körper.

Sei $H := \{p \in \mathbb{P}^n(k) \mid p = (0 : x_1 : \ldots : x_n)\}$. Aus Proposition 9.3 folgt, dass

$$\mathbb{P}^n(k) = U_0 \dot\cup H.$$

Bemerke, dass $H \simeq \mathbb{P}^{n-1}(k)$, woraus

$$\mathbb{P}^n(k) = k^n \dot\cup \mathbb{P}^{n-1}(k)$$

folgt.

Terminologie: H heißt die Hyperebene im Unendlichen.

Konvention: Der Raum $\mathbb{P}^0(k)$ besteht aus einem einzigen Punkt, den wir mit "∞" bezeichnen und der Punkt im Unendlichen genannt wird: $\mathbb{P}^0(k) = \{\infty\}$. Dann ist $\mathbb{P}^1(k) = k \cup \{\infty\}$.

Korollar 9.4 (Ch. 8, §2, Cor. 3)**.** *Für jedes $i = 1, \ldots, n$ setze*

$$U_i = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n(k) \mid x_i \neq 0\}.$$

Dann gelten

(i) Es gibt eine bijektive Abbildung $\psi\colon U_i \to k^n$;

(ii) $\mathbb{P}^n(k) \setminus U_i \simeq \mathbb{P}^{n-1}(k)$

(iii) $\mathbb{P}^n(k) = \bigcup_{i=0}^n U_i$ □

Ziel: Wir wollen nun den Begriff einer "projektiven Varietät" einführen. Im projektiven Raum $\mathbb{P}^n(k)$ werden Punkte identifiziert, die Vielfache voneinander sind.

Problem: Sei $f = x_1 - x_2^2 \in \mathbb{R}[x_0, x_1, x_3]$ und betrachte die affine Varietät $V = \mathbf{V}(f) \subseteq \mathbb{R}^3$. Dann gilt $f(1, 4, 2) = 0$, aber $f(2, 8, 4) = -8 \neq 0$. Also $p = (1, 4, 2) \in V$ und $2p = (2, 8, 4) \notin V$.

Wir wollen also unsere projektiven Varietäten durch Polynomen f definieren, die die folgende Eigenschaft erfüllen:

$$\forall (x_0, \ldots, x_n) \in k^{n+1},\ \ \forall \lambda \in k^\times \qquad f(x_0, \ldots, x_n) = 0 \Rightarrow f(\lambda x_0, \ldots, \lambda x_n) = 0$$

oder anders geschrieben

$$f(x_0, \ldots, x_n) = 0 \Rightarrow f(x_0 : \ldots : x_n) = 0.$$

Definition 9.5. *Ein Polynom $f \in k[x_0 \dots, x_n]$ heißt homogen, falls $d \in \mathbb{N}$ existiert, so dass alle Monome von f Totalgrad d haben.*

Lemma 9.6. *Seien $f \in k[x_0, \dots, x_n]$ ein homogenes Polynom mit* $\operatorname{total\,deg}(f) = d \in \mathbb{N}$, *$\lambda \in k^\times$ und $(x_0, \dots, x_n) \in k^{n+1}$. Es gilt*

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$$

Beweis. Sei $g(x_0, \dots, x_n) = x_0^{d_0} \cdots x_n^{d_n}$ ein Monom von f (also $\sum_{i=0}^n d_i = d$). Dann gilt

$$g(\lambda x_0, \dots, \lambda x_n) = \lambda^{d_0} x_0^{d_0} \cdots \lambda^{d_n} x_n^{d_n} = \lambda^{d_0} \cdots \lambda^{d_n} x_0^{d_0} \cdots x_n^{d_n} = \lambda^d g(\lambda x_0, \dots, \lambda x_n).$$

Seien nun $g_1, \dots, g_t$ alle Monome von f, also $f = \sum_{i=1}^t g_i(x_0, \dots, x_n)$. Dann

$$\begin{aligned} f(\lambda x_0, \dots, \lambda x_n) &= \sum_{i=1}^t g_i(\lambda x_0, \dots, \lambda x_n) \\ &= \sum_{i=1}^t \lambda^d g_i(x_0, \dots, x_n) \\ &= \lambda^d \sum_{i=1}^t g_i(x_0, \dots, x_n) \\ &= \lambda^d f(x_0, \dots, x_n) \end{aligned}$$

□

Proposition 9.7 (Ch. 8, §2, Prop. 4)**.** *Seien $f \in k[x_0, \dots, x_n]$ ein homogenes Polynom mit* $\operatorname{total\,deg}(f) = d \in \mathbb{N}$, *$\lambda \in k^\times$ und $(x_0, \dots, x_n) \in k^{n+1} \setminus \{0\}$. Dann gilt*

$$f(x_0, \dots, x_n) = 0 \Rightarrow f(\lambda x_0, \dots, \lambda x_n) = 0.$$

Beweis. Angenommen $f(x_0, \dots, x_n) = 0$. Aus Lemma 9.6 folgt direkt

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n) = \lambda^d \cdot 0 = 0.$$

□

Insbesondere für ein homogenes Polynom $f \in k[x_0, \dots, x_n]$ ist

$$\mathbb{V}(f) := \{p \in \mathbb{P}^n(k) \mid f(p) = 0\}$$

eine wohldefinierte Teilmenge von $\mathbb{P}^n(k)$.

Definition 9.8 (Ch. 8, §2, Def. 5 – Projektive Varietät)**.** *Seien $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ homogene Polynome. Dann heißt*

$$\mathbb{V}(f_1, \ldots, f_s) := \{p \in \mathbb{P}^n(k) \mid f_i(p) = 0, \ \ \forall i = 1, \ldots, s\}$$

eine projektive Varietät.

Die nächste Proposition erklärt den Zusammenhang zwischen affinen und projektiven Varietäten. Seien hierzu ϕ, ψ wie in Proposition 9.3.

Proposition 9.9 (Ch. 8, §2, Prop. 6)**.** *Seien $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ homogene Polynome und sei $V = \mathbb{V}(f_1, \ldots, f_s) \subseteq \mathbb{P}^n(k)$ die entsprechende projektive Varietät. Für jedes $i = 1, \ldots, s$ setze $g_i(x_1, \ldots, x_n) := f(1, x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Sei $W' := \mathbf{V}(g_1, \ldots, g_s) \subseteq k^n$ die durch $g_1, \ldots, g_s$ definierte affine Varietät. Zuletzt sei $W := V \cap U_0$. Dann gilt*

$$\phi(W') = W.$$

Beweis. Wir zeigen, dass

(i) $\phi(W') \subseteq W$

(ii) $\psi(W) \subseteq W'$.

Die Behauptung folgt dann aus der Tatsache, dass ϕ und ψ zueinander invers sind.

(i) Sei $(a_1, \ldots, a_n) \in W'$. Dann ist $(1 : a_1 : \ldots : a_n) \in U_0$ und es gilt $0 = g_i(a_1, \ldots, a_n) = f_i(1; a_1 : \ldots : a_n)$. Also $\phi(a_1, \ldots, a_n) \in W$ und somit $\phi(W') \subseteq W$.

(ii) Sei nun $p \in W$. Da $p \in U_0$, können wir schreiben $p = (1 : a_1 : \ldots : a_n)$. Da aber $p \in V$ gilt, haben wir auch $g_i(a_1, \ldots, a_n) = f_i(1 : a_1 : \ldots : a_n) = 0$. Also $\psi(p) \in W'$ und somit $\psi(W) \subseteq W'$.

□

Zunächst zeigen wir, wie man aus einem beliebigen Polynom ein homogenes Polynom konstruieren kann.

Proposition 9.10 (Ch. 8, §2, Prop. 7)**.** *Sei $g(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ ein beliebiges Polynom mit* $\operatorname{total\,deg}(g) = d \in \mathbb{N}$.

(i) Sei $g = \sum_{i=0}^{d} g_i$ die Zerlegung von g in homogenen Komponenten, wobei $\operatorname{total\,deg}(g_i) = i$. *Dann ist*

$$g^h = \sum_{i=0}^{d} g_i(x_1, \ldots, x_n) x_0^{d-i}$$

ein homogenes Polynom in $k[x_0, \ldots, x_n]$ mit $\operatorname{total\,deg}(g^h) = d$. *Das Polynom g^h heißt die Homogenisierung von g.*

Beispiel 9.11. *Sei* $f = x_2 - x_1^3 + x_1^2 \in \mathbb{R}[x_1, x_2]$. *Dann ist* $f^h = x_0^2 x_2 + x_0 x_2^2 - x_1^3$.

25 Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 03.02.2022

Wir fangen mit einem Korollar zu Proposition 9.9 an. Sei hierzu ϕ wie in Proposition 9.3.

Korollar 9.12. *Sei $W' = \mathbf{V}(g_1, \ldots, g_s) \subseteq k^n$ eine affine Varietät und sei $V = \mathbb{V}(g_1^h, \ldots, g_s^h) \subseteq \mathbb{P}^n(k)$ die zugeordnete projektive Varietät. Dann gilt*

$$\phi(W') = V \cap U_0.$$

□

Wie im Fall der affinen Varietäten wollen wir eine Korrespondenz zwischen projektiven Varietäten und (geeigneten) Idealen feststellen.

9.3 Projektives Algebra-Geometrie-Lexikon

Definition 9.13 (Ch. 8, §3, Def. 1)**.** *Ein Ideal $I \trianglelefteq k[x_0, \ldots, x_n]$ heißt homogen, falls für jedes Polynom $f \in I$ alle homogene Komponenten von f zum Ideal I gehören.*

Beispiel 9.14. *(Nicht-homogenes Ideal) Das Ideal $I = \langle y - x^2 \rangle \trianglelefteq k[x, y]$ ist nicht homogen. Die homogene Komponenten von $y - x^2$ sind $f_0 = 0$; $f_1 = y$ und $f_2 = -x^2$. Man sieht leicht, dass $f_1, f_2 \notin I$.*

Satz 9.15 (Ch. 8, §3, Theorem 2 – Charakterisierung von homogenen Idealen)**.** *Sei $I \trianglelefteq k[x_0, \ldots, x_n]$. Dann sind äquivalent:*

(i) Das Ideal I ist homogen.

(ii) Es existieren homogene Polynome $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ so, dass $I = \langle f_1, \ldots, f_s \rangle$ (I ist von homogenen Polynomen erzeugt).

(iii) Eine reduzierte Gröbnerbasis von I besteht aus homogenen Polynomen.

Beweis. $(ii) \Rightarrow (i)$. Sei $I = \langle f_1, \ldots, f_s \rangle$ mit f_i homogen. Sei nun $g = \sum_{j=1}^{s} A_j f_j \in I$, wobei die A_j Polynome sind. Sei nun $A_j = \sum_{i=0}^{d_j} A_{ji}$ die Zerlegung von A_j in homogenen Komponenten. Dann gilt

$$g = \sum_{j=1}^{s} A_j f_j = \sum_{j=1}^{s} \sum_{i=0}^{d_j} A_{ji} f_j, \tag{12}$$

wobei $A_{ji}f_j$ ein homogenes Polynom ist, für alle $j = 0, \ldots, \text{total deg}(f)$ und alle $i = 0, \ldots, d_j$. Dass heißt, (12) ist die Zerlegung von g in homogenen Komponenten. Und weil sie alle Vielfachen der f_j sind, gehören sie alle dem Ideal I.

$(i) \Rightarrow (ii)$. Sei I ein homogenes Ideal. Der Hilbertsche Nullstellensatz liefert Polynome $F_1, \ldots, F_t \in k[x_0, \ldots, x_n]$ so, dass $I = \langle F_1, \ldots, F_t \rangle$. Für alle $j = 1, \ldots, t$ sei $F_j = \sum_{i=0}^{d_j} F_{ji}$ di Zerlegung von F_j in homogenen Komponenten. Dann ist $F_{ji} \in I$, weil I homogen ist. Sei nun $I' = \langle F_{ji} \mid j = 1, \ldots, t; i = 0, \ldots, d_j \rangle$. Aus $F_{ji} \in I$ folgt direkt $I' \subseteq I$. Aber die F_{ji} erzeugen die F_j, also $I = \langle F_1, \ldots, F_t \rangle \subseteq I'$. Schließlich gilt $I = I'$ und $\{F_{ji} \mid j = 1, \ldots, t; i = 0, \ldots, d_j\}$ ist eine Menge von homogenen Erzeuger von I.

$(ii) \Leftrightarrow (iii)$ ÜB 13. □

Definition 9.16. *Sei $I \trianglelefteq k[x_0, \ldots, x_n]$ ein homogenes Ideal. Schreibe*

$$\mathbb{V}(I) := \{p \in \mathbb{P}^n(k) \mid f(p) = 0, \ \ \forall f \in I\}.$$

Proposition 9.17 (Ch. 8, §3, Prop. 3)**.** *Sei $I = \langle f_1, \ldots, f_s \rangle \trianglelefteq k[x_0, \ldots, x_n]$ ein homogenes Ideal, wobei f_i homogen sind. Dann gilt*

$$\mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_s).$$

Insbesondere ist $\mathbb{V}(I)$ eine projektive Varietät.

Beweis. Die Inklusion $\mathbb{V}(I) \subseteq \mathbb{V}(f_1, \ldots, f_s)$ ist klar, weil $\{f_1, \ldots, f_s\} \subseteq I$.

Seien umgekehrt $p = (a_0 : \ldots : a_n) \in \mathbb{V}(f_1, \ldots, f_s)$ und $g = \sum_{j=1}^{s} A_j f_j \in I$ mit $A_j \in k[x_0, \ldots, x_n]$. Seien auch $\lambda \in k^\times$ und $d_j := \text{total deg}(f_j)$. Dann gilt

$$\begin{aligned} g(\lambda a_0, \ldots, \lambda a_n) &= \sum A_j(\lambda a_0, \ldots, \lambda a_n) f_j(\lambda a_0, \ldots, \lambda a_n) \\ &= \sum A_j(\lambda a_0, \ldots, \lambda a_n) \lambda^{d_j} f_j(a_0, \ldots, a_n) \\ &= \sum A_j(\lambda a_0, \ldots, \lambda a_n) \lambda^{d_j} \cdot 0 \\ &= 0. \end{aligned}$$

Dies zeigt genau, dass $p \in \mathbb{V}(I)$, wie gewünscht. □

Somit haben wir eine projektive Varietät einem homogenen Ideal zugeordnet. Nun stellen wir die andere Richtung fest.

Proposition 9.18 (Ch. 8, §3, Prop. 4)**.** *Sei k unendlich und sei $V \subseteq \mathbb{P}^n(k)$ eine projektive Varietät. Dann ist*

$$\mathbb{I}(V) := \{f \in k[x_0, \ldots, x_n] \mid f(p) = 0 \ \ \forall p \in V\}$$

ein homogenes Ideal.

Beweis. Es ist klar, dass $\mathbb{I}(V)$ ein Ideal ist. Sei nun $f \in \mathbb{I}(V)$ mit $\operatorname{total\,deg}(f) = d$ und sei $\sum_{j=0}^{d} f_j$ die Zerlegung von f in homogene Komponenten. Seien $p = (a_0 : \ldots : a_n) \in V$ und $\lambda \in k^\times$. Dann gilt

$$0 = f(\lambda a_0, \ldots, \lambda a_n) = \sum_{j=0}^{d} f_j(\lambda a_0, \ldots, \lambda a_n) = \sum_{j=0}^{d} f_j \lambda^j (a_0, \ldots, a_n).$$

Setze $c_j := f_j(a_0, \ldots, a_n) \in k$ und $f_{(a_0,\ldots,a_n)}(x) := \sum_{i=0}^{d} c_j x^j \in k[x]$. Dann gilt $f_{(a_0,\ldots,a_n)}(\lambda) = 0$ für alle $\lambda \in k^\times$. Da es unendlich viele solche λ gibt, folgt, dass $f_{(a_0,\ldots,a_n)} \equiv 0$ ist. Somit ist $c_j = f_j(a_0, \ldots, a_n) = 0$ für alle j, d.h., $f_j \in \mathbb{I}(V)$ für alle j, was zeigt, dass $\mathbb{I}(V)$ homogen ist. □

Aus Propositionen 9.17 und 9.18 bekommen wir:

Satz 9.19 (Ch. 8, §3, Theorem 5)**.** *Sei k unendlich. Die Abbildungen*

$$\left\{\begin{array}{c}\textit{Projektive Varietäten}\\ \textit{in } \mathbb{P}^n(k)\end{array}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{array}{c}\textit{Homogene Ideale}\\ \textit{in } k[x_0, \ldots, x_n]\end{array}\right\}$$

sind inklusionsumkehrend (kontravariant) und, für alle $V \subseteq \mathbb{P}^n(k)$ gilt

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

Also $\mathbb{I}$ ist immer injektiv.

26 Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 8.2.2022

Definition 9.20 (Irreduzible projektive Varietät)**.** *Eine projektive Varietät $V \subseteq \mathbb{P}^n(k)$ heißt irreduzibel, falls sie keine Vereinigung von zwei echten Untervarietäten ist. Also aus $V = V_1 \cup V_2$, wobei V_i Untervarietäten von V sind, folgt $V = V_1$ oder $V = V_2$.*

Satz 9.21 (Ch. 8, §3, Theorem 6)**.** *Sei k unendlich.*

(i) Für jede absteigende Folge von projektiven Varietäten

$$V_1 \supseteq V_2 \supseteq \dots$$

gibt es ein $N \in \mathbb{N}$ so, dass $V_i = V_N$ für alle $i \geq N$.

(ii) Jede projektive Varietät $V \subseteq \mathbb{P}^n(k)$ hat eine endliche Zerlegung

$$V_1 \cup \ldots \cup V_m,$$

wobei $m \in \mathbb{N}$ und V_i irreduzible Varietäten mit $V_i \not\subseteq V_j$ für $i \neq j$ sind.

Beweis. (i) Satz 9.19 liefert eine folge

$$\mathbb{I}(V_1) \subseteq \mathbb{I}(V_2) \subseteq \dots$$

von homogenen Idealen in $k[x_0, \dots, x_n]$. Da dies Noethersch ist, muss die Folge anhalten: Es gibt $N \in \mathbb{N}$ so, dass $\mathbb{I}(V_N) = \mathbb{I}(V_{N+1}) = \dots$. Aus der Injektivität von $\mathbb{I}$ folgt nun, dass $V_N = V_{N+1} \dots$.

(ii) Folgt direkt aus (i), genau wie in dem affinen Fall.

□

Proposition 9.22 (Ch. 8, §3, Prop. 7)**.** *Sei $I \trianglelefteq k[x_0, \dots, x_n]$ ein homogenes Ideal. Dann ist $\sqrt{I}$ homogen.*

Beweis. Sei $0 \neq f \in \sqrt{I}$. Dann existiert $m \in \mathbb{N}$ mit $f^m \in I$. Sei nun $f = \sum_{i=0}^{d} f_i$ die homogene Zerlegung von f.
ÜA: Wenn $\nu = \operatorname{total\,deg} f$, dann gilt $(f^m)_\nu = f_d^m$.
Da I homogen ist, gilt $(f^m)_\nu \in I$ und somit $f_d \in \sqrt{I}$. Setze nun $g = f - f_d = \sum_{i=0}^{d-1} f_i$. Wiederhole

das Verfahren und bekomme $f_{d-1} \in \sqrt{I}$. Per Induktion nach $\operatorname{total\,deg} f$ finden wir, dass alle homogene Komponente von f in $\sqrt{I}$ liegen, d.h., $\sqrt{I}$ ist homogen. □

Erinnerung: Sei k algebraisch abgeschlossen und sei $I \trianglelefteq k[x_1, \ldots, x_n]$ ein Ideal. Dann:
Schwacher affiner Nullstellensatz (saNSS): $\mathbf{V}(I) = \emptyset \iff I = k[x_1, \ldots, x_n]$.
Starker affiner Nullstellensatz aNSS: $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Im projektiven Fall gilt diese Charakterisierung des Ideals einer leeren Varietät nicht:

Beispiel 9.23. *Sei $I_0 = \langle x_0, \ldots, x_n \rangle$. Dies ist ein echtes homogenes Ideal von $k[x_0, \ldots, x_n]$. Der einzige Punkt, in dem alle x_i verschwinden, wäre $(0 : \ldots : 0) \notin \mathbb{P}^n(k)$. Also $\mathbb{V}(I_0) = \emptyset$, obwohl $I_0 \neq k[x_0, \ldots, x_n]$.*

Das entsprechende Resultat zum saNSS beweisen wir jetzt. Zunächst führen wir eine Definition/Notation ein.

Definition 9.24. *(Affiner Kegel) Sei $V = \mathbb{V}(I) \subseteq \mathbb{P}^n(k)$ eine projektive Varietät und setze $C_V := \mathbf{V}(I) \subseteq k^n$ (affine Varietät). Dann heißt C_V der affine Kegel von V.*

Satz 9.25 (Ch. 8, §3, Theorem 8 – schwacher projektiver Nullstellensatz – spNSS)**.** *Seien k algebraisch abgeschlossen, $I \trianglelefteq k[x_0, \ldots, x_n]$ ein homogenes Ideal und $V := \mathbb{V}(I)$. Sei weiter G eine reduzierte Gröbnerbasis für I, bezüglich einer beliebigen monomialen Anordnung. Die folgende Bedingungen sind äquivalent:*

(i) $V = \emptyset$.

(ii) Für alle $i = 1, \ldots, n$ gibt es $g \in G$ und $m_i \in \mathbb{N}$ mit $\operatorname{LT}(g) = x^{m_i}$.

(iii) Für alle $i = 1, \ldots, n$ gibt es $m_i \in \mathbb{N}_0$ mit $x^{m_i} \in I$.

(iv) Es gibt $r \in \mathbb{N}$ mit $r \geq 1$ und $\langle x_0, \ldots, x_n \rangle^r \subseteq I$.

Beweis. $(ii) \Rightarrow (i)$. Die Bedingung (ii) impliziert, dass C_V eine endliche Menge ist (sieh Satz 7.6). Angenommen $V \neq \emptyset$, sei $p = (a_0 : \ldots : a_n) \in V$. Dann gilt, für alle $\lambda \in k^\times$, dass $(\lambda a_0, \ldots, \lambda a_n) \in C_V$. Da k unendlich ist, widerspricht dies der Endlichkeit von C_V. Somit muss $V = \emptyset$ gelten.
$(ii) \Leftrightarrow (iii)$. Analog zu Satz 7.6.
$(iv) \Rightarrow (iii)$. Klar.
$(i) \Rightarrow (iv)$. Aus $V = \emptyset$ folgt, dass $C_V = \emptyset$ oder $C_V = \{(0, \ldots, 0)\}$ gilt. Es folgt $\mathbf{I}(\{(0, \ldots, 0)\}) \subseteq \mathbf{I}(C_V)$. Aber $\mathbf{I}(\{(0, \ldots, 0)\}) = \langle x_0, \ldots, x_n \rangle$. Also $\langle x_0, \ldots, x_n \rangle \subseteq \mathbf{I}(C_V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ und somit (sieh ÜA unten!) ist $\langle x_0, \ldots, x_n \rangle^r \subseteq I$ für ein gewisses $r \in \mathbb{N}$. □

ÜA – Ch. IV, §3, Ex. 12: Seien J_1, J_2 Ideale mit $J_1 \subseteq \sqrt{J_2}$. Dann existiert $r \in \mathbb{N}$ mit $J_1^r \subseteq J_2$.
Hinweis: Hilbertscher Basissatz.

Satz 9.26 (Ch. 8, §3, Theorem 9 – starker projektiver Nullstellensatz – pNSS)**.** *Sei k algebraisch abgeschlossen und sei $I \trianglelefteq k[x_0, \ldots, x_n]$ ein homogenes Ideal mit $\mathbb{V}(I) \neq \emptyset$. Dann gilt*

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

Beweis. Sei $V = \mathbb{V}(I)$.
Behauptung: $\mathbf{I}(C_V) = \mathbb{I}(V)$.
Beweis: Sei $f \in \mathbf{I}(C_V)$ und sei $p = (a_0 : \ldots : a_n) \in V$. Dann ist $p \subseteq C_V$ als Teilmenge enthalten, d.h., f verschwindet auf $(\lambda a_0, \ldots, \lambda a_n)$ für alle $\lambda \in k^\times$. Dies ist äquivalent dazu, dass f auf p (projektiver Punkt) verschwindet. Da $p \in V$ beliebig war, gilt $f \in \mathbb{I}(V)$, also $\mathbf{I}(C_V) \subseteq \mathbb{I}(V)$.
Umgekehrt, sei $f \in \mathbb{I}(V)$. Dann verschwindet f auf $C_V \setminus \{0\}$. Um zu zeigen, dass f auf 0 verschwindet, sei $f = \sum_{i=0}^{d} f_i$ die homogene Zerlegung von f. Da $\mathbb{I}(V)$ homogen ist, gilt $f_i \in \mathbb{I}(V)$ für alle i. Insbesondere $f_0 \in \mathbb{I}(V)$. Dies impliziert $f_0 = 0$. Dann hat f keinen konstanten Term, und somit $f(0, \ldots, 0) = 0$. Also $f \in \mathbf{I}(C_V)$ und $\mathbb{I}(V) \subseteq \mathbf{I}(C_V)$ $\square_{Beh.}$

Nun können wir schließen

$$\sqrt{I} \overset{\text{aNSS}}{=} \mathbf{I}(\mathbf{V}(I)) \overset{Beh.}{=} \mathbb{I}(V) \overset{\text{def. von } V}{=} \mathbb{I}(\mathbb{V}(I)).$$

$\square$

10 Dimension einer Varietät

Es gibt mehrere Möglichkeiten, um die Dimension einer affinen Varietät zu definieren. Sei also $V \subseteq k^n$ eine affine Varietät.

Reelle algebraische Geometrie I – WS 22/23:
Betrachte den Koordinatenring $k[V]$. Definiere $\dim_k V$ als die Krulldimension von $k[V]$.
Hier:

(i) Betrachte für eine irreduzible Varietät V den Funktionenkörper $k(V)$. Definiere $\dim_k V$ als der Transzendenzgrad $\operatorname{tr.deg}_k k(V)$.

(ii) Für eine allgemeine Varietät V sei $V = \bigcup V_i$ die irreduzible Zerlegung von V und setze $\dim_k V = \max \dim_k V_i$.

Definition 10.1. *Eine Körpererweiterung K/k heißt transzendent, falls sie nicht algebraisch ist.*

Definition 10.2. *Sei K/k eine Körpererweiterung und seien $a_1, \ldots, a_n \in K$. Dann heißen*

$a_1, \ldots, a_n$ algebraisch abhängig, falls der Homomorphismus

$$\begin{array}{rccc} \mathrm{ev}_{\underline{a}}\colon & k[x_1, \ldots, x_n] & \to & K \\ & f & \mapsto & f(a_1, \ldots, a_n) \end{array}$$

einen nichttrivialen Kern hat. D. h., falls es ein $f \in k[x_1, \ldots, x_n] \setminus \{0\}$ gibt mit $f(a_1, \ldots, a_n) = 0$. Die Elemente $a_1, \ldots, a_n$ sind algebraisch unabhängig, wenn sie nicht algebraisch abhängig sind.

27 Skript zur Vorlesung: Algorithmische Algebraische Geometrie
Prof. Dr. Salma Kuhlmann
WS2021/2022: 10.2.2022

Quelle für diese letzte Vorlesung: O. Zariski und P. Samuel (1975). *Commutative algebra. Vol. I.* Graduate Texts in Mathematics, Vol. 29. Springer, Kapitel II, §12, Seiten 95–100.

Sei K/k stets eine Körpererweiterung.

Beispiel 10.3. *(i) Sei $K = k(x_1, \ldots, x_n)$. Dann sind die Elemente $x_1, \ldots, x_n$ algebraisch unabhängig über k (ÜA).*

(ii) Sei umgekehrt K/k eine beliebige Körpererweiterung. Dann sind Elemente $a_1, \ldots, a_n \in K$ genau dann algebraisch unabhängig über k, wenn $k(a_1, \ldots, a_n) = k(x_1, \ldots, x_n)$. Dies folgt direkt aus der Definition von linearer Unabhängigkeit, da die Abbildung

$$\begin{array}{rccc} \mathrm{ev}_{\underline{a}}\colon & k[x_1, \ldots, x_n] & \to & K \\ & f/g & \mapsto & \frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)} \end{array}$$

ein Isomorphismus ist.

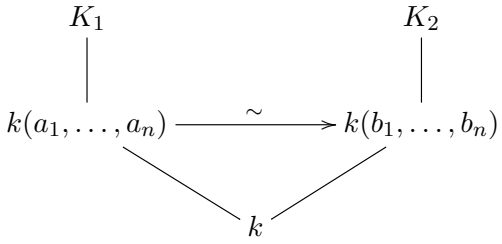
Definition 10.4. *(i) Eine Teilmenge $X \subseteq K$ heißt <u>algebraisch unabhängig über k</u>, falls jede endliche Teilmenge von X algebraisch unabhängig ist.*

(ii) Ist $X \subseteq K/k$ algebraisch unabhängig, so heißt X <u>Transzendenzmenge</u>.

(iii) Ist X eine Transzendenzmenge, so heißt die Erweiterung $k(X)/k$ <u>rein transzendent</u>.

Beispiel 10.5. *(i) $k(x_1, \ldots, x_n)/k$ ist rein transzendent.*

(ii) Seien K_1/k und K_2/k Körpererweiterungen und seien $\{a_1, \ldots, a_n\} \subseteq K_1$, $\{b_1, \ldots, b_n\} \subseteq K_2$ Transzendenzmengen. Dann gibt es einen Isomorphismus $k(a_1, \ldots, a_n) \simeq k(b_1, \ldots, b_n)$.



Lemma 10.6 (Zariski und Samuel 1975, Seite 96)**.** *Sei $Y \subseteq K/k$ eine Transzendenzmenge und sei $x \in K \setminus Y$. Dann ist $Y \cup \{x\}$ genau dann eine Transzendenzmenge, wenn x transzendent über $k(Y)$ ist.*

Beweis. "$\Leftarrow$". Sei x transzendent über $k(Y)$ und sei $Y' = Y \cup \{x\}$. Seien $y_1, \ldots, y_n \in Y \cup \{x\}$ und ohne Einschränkung $y_n = x$. Sei nun $f \in k[x_1, \ldots, x_n]$ mit $f(y_1, \ldots, y_{n-1}, x) = 0$. Dann ist x eine Nullstelle von $f(y_1, \ldots, y_{n-1}, x_n) \in k(Y)[x_n]$. Da x transzendent über $k(Y)$ ist, muss $f(y_1, \ldots, y_{n-1}, x_n) \equiv 0$ sein. Schreibe nun

$$f(y_1, \ldots, y_{n-1}, x_n) = A_0(x_1, \ldots, x_{n-1})x_n^d + \ldots + A_d(x_1, \ldots, x_{n-1}).$$

Dann gilt $A_i(x_1, \ldots, x_{n-1})$ für alle $i = 0, \ldots, n-1$. Nun ist Y eine Transzendenzmenge, also gilt $A_i \equiv 0$ für alle i. Somit ist $f(x_1, \ldots, x_n) \equiv 0$. Also $Y \cup \{x\}$ ist eine Transzendenzmenge.
"$\Rightarrow$". ÜA. □

Definition 10.7. *Eine Transzendenzmenge $Y \subseteq K/k$ heißt Transzendenzbasis von K/k, falls Y maximal bezüglich Inklusion für die Eigenschaft "Transzendenzmenge zu sein" ist.*

Korollar 10.8. *Eine Transzendenzmenge $T \subseteq K/k$ ist genau dann eine Transzendenzbasis, wenn die Erweiterung $K/k(T)$ algebraisch ist, d.h., wenn K der relative algebraische Abschluss von $k(T)$ in K ist.* □

Definition 10.9. *Sei $X \subseteq K$. Der Span von X, bezeichnet als $S(X)$, ist der relative algebraische Abschluss von $k(X)$ in K.*

Satz 10.10 (Zariski und Samuel 1975, Seite 97)**.** *Es gelten folgende Eigenschaften:*

(S1) $X \subseteq Y \Rightarrow S(X) \subseteq S(Y)$. *(Monotonie)*

(S2) Für alle $x \in S$ existiert eine endliche Teilmenge $Y \subseteq X$ mit $x \in S(Y)$. (Reduktion auf Endlichen)

(S3) $X \subseteq S(X)$ *für alle* $X \subseteq K$.

(S4) $S(S(X)) = S(X)$. *(Idempotenz)*

(S5) $y \in S(X \cup \{x\}) \wedge y \notin S(X) \Rightarrow x \in S(X \cup \{y\})$. *(Austausch)*

Beweis. ÜA. □

Definition 10.11. *(i) $X \subseteq K/k$ ist erzeugend, falls $K = S(X)$;*

(ii) $X \subseteq K/k$ *ist frei, falls für alle* $x \in X$ *gilt* $x \notin S(X \setminus \{x\})$.

Bemerkung 10.12. *$X \subseteq K/k$ ist genau dann eine Transzendenzbasis, wenn X frei und erzeugend ist.*

Satz 10.13 (Zariski und Samuel 1975, Seiten 99–100)**.** *Sei K/k eine Körpererweiterung. Dann gilt:*

(i) Es existiert eine Transzendenzbasis für K/k.

(ii) Alle Transzendenzbasen haben die gleiche Kardinalität. Insbesondere wenn eine Transzendenzbasis endlich ist, dann haben alle Transzendenzbasen die gleiche Anzahl von Elementen. □

Definition 10.14. *Der Transzendenzgrad von K/k, bezeichnet mit* $\mathrm{tr.deg}_k K$*, ist die Kardinalität einer Transzendenzbasis von K/k.*

Definition 10.15 (Dimension einer affinen Varietät)**.** *(i) Sei $V \subseteq k^n$ eine **irreduzible** affine Varietät. Dann definiert man die Dimension von V über k als*

$$\dim_k V := \mathrm{tr.deg}_k k(V).$$

(ii) Sei nun $V \subseteq k^n$ eine beliebige affine Varietät und sei $V = \bigcup_{i=1}^m V_i$ die Zerlegung von V in irreduzible Komponenten. Dann definiert man die Dimension von V über k als

$$\dim_k V := \min\{\dim_k V_i \mid i = 1, \ldots, m\}.$$

Literatur

Cox, D. A., J. Little und D. O'Shea (2006). *Ideals, varieties, and algorithms*. 3. Aufl. Undergraduate Texts in Mathematics. Springer.

Zariski, O. und P. Samuel (1975). *Commutative algebra. Vol. I*. Graduate Texts in Mathematics, Vol. 29. Springer.