

Vorlesung 1

Affine algebraische Mengen und Ideale

Sei k ein Körper und seien f_1, \dots, f_s Polynome in $k[x_1, \dots, x_n]$. Bezeichnen wir als $\mathbf{V}(f_1, \dots, f_s)$ die Menge aller gemeinsamen Nullstellen dieser Polynome. Also,

$$\mathbf{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n \mid f_i(a_1, \dots, a_n) = 0 \text{ für alle } i = 1, \dots, s\}.$$

Definition. Eine Untermenge $U \subseteq k^n$ heißt (*affine*) *algebraische Menge*, wenn Polynome $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ existieren, so dass $U = \mathbf{V}(f_1, \dots, f_s)$ ist.

Beispiele. 1) $V(x^2 + y^2 - 1)$ ist ein Kreis.

2) Graph von $y = \frac{x^3-1}{x}$ ist $V(xy - x^3 + 1)$.

3) $V(z - x^2 - y^2)$ ist ein Rotationsparaboloid, $V(z^2 - x^2 - y^2)$ ist ein Kegel.

4) $V(x^2 - y^2z^2 + z^3)$.

5) $V(y - x^2, z - x^3)$.

6) $V(xz, yz)$ ist die Vereinigung einer Ebene und einer Geraden.

7) \emptyset, k^n sind auch algebraische Mengen.

8) Alle Lösungen des Systems der linearen Gleichungen

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n & = b_1, \\ & \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n & = b_m \end{cases}$$

bilden eine algebraische Menge.

9) $\{(a, a) \mid a \geq 1\}$ ist keine algebraische Menge in \mathbb{R}^2 .

Lemma. Sind U und W algebraische Mengen, so sind $U \cap W$ und $U \cup W$ es auch.

Beweis. Seien $U = \mathbf{V}(f_1, \dots, f_s)$ und $W = \mathbf{V}(g_1, \dots, g_t)$. Dann gilt

$$\begin{aligned} U \cap W &= \{f_1, \dots, f_s, g_1, \dots, g_t\}, \\ U \cup W &= \{f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t\}. \end{aligned}$$

Beispiel. $\mathbf{V}(z) \cup \mathbf{V}(x, y) = \mathbf{V}(zx, zy)$.

Probleme. Gegeben $f_1, \dots, f_s \in k[x_1, \dots, x_n]$.

• (Lösbarkeit) Können wir erkennen, ob $\mathbf{V}(f_1, \dots, f_s) \neq \emptyset$ ist?

Equivalent: ob die Gleichungen $f_1 = \dots = f_s = 0$ eine gemeinsame Lösung haben?

• (Endlichkeit) Können wir erkennen, ob $\mathbf{V}(f_1, \dots, f_s)$ endlich ist? Wenn es endlich ist, können wir die Lösungen finden?

• (Dimension) Können wir die Dimension von $\mathbf{V}(f_1, \dots, f_s)$ berechnen?

Definition. Sei k ein Körper. Eine *rationale Funktion* von t_1, \dots, t_m mit Koeffizienten in k ist eine Funktion der Form f/g , wobei $f, g \in k[t_1, \dots, t_m]$ ist und $g \neq 0$ ist. Die Menge aller rationalen Funktionen von t_1, \dots, t_m wird als $k(t_1, \dots, t_m)$ bezeichnet.

Definition. Sei V eine algebraische Menge in k^n . Die *rationale Parameterdarstellung* von V ist eine Menge rationaler Funktionen $r_1, \dots, r_n \in k(t_1, \dots, t_m)$, so dass gilt

1) für alle möglichen $t_1, \dots, t_m \in k$ liegen die Punkte $x = (x_1, \dots, x_n)$ in V , wobei

$$\begin{aligned} x_1 &= r_1(t_1, \dots, t_m), \\ x_2 &= r_2(t_1, \dots, t_m), \\ &\vdots \\ x_n &= r_n(t_1, \dots, t_m), \end{aligned}$$

ist,

2) V ist die kleinste algebraische Menge, die alle diese Punkte enthält.

Beispiel. 1) Sei V die algebraische Menge aller Lösungen des Systems

$$\begin{cases} x + y + z &= 1, \\ x + 2y - z &= 3. \end{cases}$$

Die Menge V hat folgende (rationale) Parameterdarstellung:

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

2) Die algebraische Menge $\mathbf{V}(x^2 + y^2 - 1)$ hat eine nicht rationale Parameterdarstellung

$$\begin{cases} x &= \cos(t), \\ y &= \sin(t) \end{cases}$$

und eine rationale Parameterdarstellung

$$\begin{cases} x &= \frac{1-t^2}{1+t^2}, \\ y &= \frac{2t}{1+t^2}. \end{cases}$$

3) Die algebraische Menge $\mathbf{V}(x^2 - y^2z^2 + z^3)$ hat folgende rationale Parameterdarstellung:

$$\begin{cases} x &= t(u^2 - t^2), \\ y &= u, \\ z &= u^2 - t^2. \end{cases}$$

4) Die algebraische Menge $\mathbf{V}(y - x^2, z - x^3)$ hat folgende rationale Parameterdarstellung:

$$\begin{cases} x &= t, \\ y &= t^2, \\ z &= t^3. \end{cases} \tag{1}$$

Probleme.

- (Parameterdarstellung). Hat jede algebraische Menge eine rationale Parameterdarstellung?
- (Präzisierung) Gegeben sei eine solche Parameterdarstellung von V , können wir die Polynome f_1, \dots, f_s finden, so daß $V = \mathbf{V}(f_1, \dots, f_n)$ ist?

Beispiel. Sei S die tangente Oberfläche der Kurve

$$\begin{cases} x &= t, \\ y &= t^2, \\ z &= t^3. \end{cases}$$

Es ist leicht zu beweisen, dass S die folgende Parameterdarstellung hat:

$$\begin{cases} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{cases}$$

Und es ist nicht leicht zu beweisen, dass man S mit einer Gleichung

$$-4x^3z + 3x^2y^2 - 4y^3 + 6xyz - z^2 = 0$$

definieren kann.

Definition. Ein *Ideal* in $I \subseteq k[x_1, \dots, x_n]$ ist eine Menge I mit folgenden Eigenschaften.

- (1) Wenn $f, g \in I$ ist, dann ist $f - g \in I$.
- (2) Wenn $f \in I$ und $h \in k[x_1, \dots, x_n]$ sind, dann ist $hf \in I$.

Lemma–Definition. Seien f_1, \dots, f_s Polynome aus $k[x_1, \dots, x_n]$. Bezeichnen wir

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i f_i \mid h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\}.$$

Dann ist die Menge $\langle f_1, \dots, f_s \rangle$ ein Ideal in $k[x_1, \dots, x_n]$. Dieses Ideal heißt *Ideal erzeugt von f_1, \dots, f_s* .

Definition. Ein Ideal $I \subseteq k[x_1, \dots, x_n]$ ist *endlich erzeugt*, wenn Polynome $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ existieren, so dass $I = \langle f_1, \dots, f_s \rangle$ ist. Die Polynome f_1, \dots, f_s nennt man *basis* von I . Es wird bewiesen, dass *jedes* Ideal in $k[x_1, \dots, x_n]$ endlich erzeugt ist.

Lemma. Wenn $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_s \rangle$ ist, dann ist $\mathbf{V}(f_1, \dots, f_t) = \mathbf{V}(g_1, \dots, g_s)$. Also, jedes Ideal definiert eindeutig eine algebraische Menge.

Lemma–Definition. Sei $V \subseteq k^n$ eine algebraische Menge. Dann ist die Menge

$$\mathbf{I}(V) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ für alle } (a_1, \dots, a_n) \in V\}$$

ein Ideal. Das Ideal $\mathbf{I}(V)$ heißt *Ideal von V* .

- Beispiele.** 1) $\mathbf{I}(\{(0, 0)\}) = \langle x, y \rangle$.
2) $\mathbf{I}(k^n) = \{0\}$, wenn k unendlich ist.

3) $\mathbf{I}(\mathbf{V}(y - x^2, z - x^3)) = \langle y - x^2, z - x^3 \rangle$, wenn k unendlich ist.

$$\begin{array}{ccc} \text{Polynome} & \text{Algebr. Menge} & \text{Ideal} \\ f_1, \dots, f_s & \rightarrow \mathbf{V}(f_1, \dots, f_s) & \rightarrow \mathbf{I}(\mathbf{V}(f_1, \dots, f_s)). \end{array}$$

Lemma. $\langle f_1, \dots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$. Die linke Menge kann kleiner als die rechte sein.

Beispiel. $\langle x^2, y^2 \rangle \subseteq \mathbf{I}(\mathbf{V}(x^2, y^2)) = \langle x, y \rangle$.

Lemma. Seien U, W algebraische Mengen in k^n . Dann gilt:

- 1) $U \subseteq W \Leftrightarrow \mathbf{I}(U) \supseteq \mathbf{I}(W)$,
- 2) $U = W \Leftrightarrow \mathbf{I}(U) = \mathbf{I}(W)$.

Fragen.

- Ob jedes Ideal $I \subseteq k[x_1, \dots, x_n]$ in der Form $\langle f_1, \dots, f_s \rangle$ geschrieben sein kann?
- Gegeben seien Polynome $f, f_1, \dots, f_n \in k[x_1, \dots, x_n]$. Können wir erkennen, ob f in dem Ideal $\langle f_1, \dots, f_n \rangle$ liegt?
- Gegeben seien Polynome $f_1, \dots, f_n \in k[x_1, \dots, x_n]$. Können wir eine Basis vom Ideal $\mathbf{I}(\mathbf{V}(f_1, \dots, f_n))$ berechnen?

Vorlesung 2

Ordnungen auf der Menge von Monomen und die Division in $k[x_1, \dots, x_n]$ mit einem Rest

Ein *Monom* in $k[x_1, x_2, \dots, x_n]$ ist ein Polynom der Form $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, wobei $\alpha_i \geq 0$ für alle $i = 1, \dots, n$ ist. Das Monom $x_1^0 x_2^0 \dots x_n^0$ wird als 1 bezeichnet.

Sei \mathcal{M} die Menge aller Monome des Ringes $k[x_1, x_2, \dots, x_n]$. Wir sagen, dass die Relation \succ auf \mathcal{M} eine *monomiale Ordnung* auf \mathcal{M} ist, wenn für alle $m_1, m_2 \in \mathcal{M}$ folgende Bedingungen erfüllt sind.

1. Entweder $m_1 \succ m_2$ oder $m_2 \succ m_1$ gilt.
2. $m \succ m$.
3. $(m_1 \succ m_2 \ \& \ m_2 \succ m_1) \Rightarrow (m_1 = m_2)$.
4. $(m_1 \succ m_2 \ \& \ m_2 \succ m_3) \Rightarrow (m_1 \succ m_3)$.
5. $m_1 \succ m_2 \Rightarrow m_1 m \succ m_2 m$ für alle $m \in \mathcal{M}$.
6. $m \succ 1$ für alle $m \in \mathcal{M}$.
7. Für jede Untermenge $S \subseteq \mathcal{M}$ existiert ein Monom $\tilde{m} \in S$, so dass $m \succ \tilde{m}$ für alle $m \in S$ ist.

Wir werden schreiben $m_1 \succ m_2$, wenn $m_1 \succ m_2$ und $m_1 \neq m_2$ ist. In dem Fall sagen wir, dass das Monom m_1 größer als Monom m_2 ist (bezüglich \succ).

Bezeichnungen. Jedes Polynom $f \in k[x_1, \dots, x_n]$ ist eine Summe von Monomen mit Koeffizienten aus k . Das größere von den Monomen (bezüglich \succ) heißt *leitendes Monom* von f und wird als $\text{LM}(f)$ bezeichnet. Die Koeffizient bei $\text{LM}(f)$ in f heißt *leitendes*

Koeffizient von f und wird als $\text{LK}(f)$ bezeichnet. Das Produkt $\text{LK}(f) \cdot \text{LM}(f)$ heißt *leitendes Mitglied von f* und wird als $\text{LMG}(f)$ bezeichnet. Wenn $\text{LM}(f) = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ ist, dann heißt das Vektor $\alpha = (\alpha_1, \dots, \alpha_n)$ *Multigrad von f* und wird als $\text{MGRAD}(f)$ bezeichnet. Wir werden schreiben $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$.

Beispiel. *Lexikographische monomiale Ordnung:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \succ_{\text{lex}} x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} \Leftrightarrow \exists i : \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Satz. Sei \succ eine monomiale Ordnung auf der Menge \mathcal{M} aller Monome aus $k[x_1, \dots, x_n]$. Sei $F = (f_1, \dots, f_s)$ ein Tupel von Polynomen aus $k[x_1, \dots, x_n]$. Dann kann jedes Polynom $f \in k[x_1, \dots, x_n]$ in der Form

$$f = q_1 f_1 + \dots + q_s f_s + r$$

dargestellt sein, wobei $q_1, \dots, q_s, r \in k[x_1, \dots, x_n]$ ist und kein Monom von r ist durch $\text{LM}(f_i)$ teilbar, $i = 1, \dots, s$.

Solch ein r heißt *Rest von f modulo F* .

Beispiel 1. Seien $f = x^2 y + xy^2 + y^2$, $F = (f_1, f_2)$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. Wir werden lexikographische Ordnung auf der Menge \mathcal{M} aller Monome aus $k[x, y]$ benutzen, wobei $x \succ_{\text{lex}} y$ ist. Das leitende Monom eines Polynomes wird immer an der ersten Stelle stehen. Wir werden versuchen, die leitenden Monome von f und aller weiteren Polynome \tilde{f} mit Hilfe der leitenden Monome $\text{LM}(f_1)$ und $\text{LM}(f_2)$ eliminieren. Wenn es unmöglich ist, nehmen wir $\text{LM}(\tilde{f})$ zum Rest hinzu:

$$\begin{array}{r}
 x^2 y + xy^2 + y^2 \\
 - \\
 x^2 y - x \\
 \hline
 xy^2 + x + y^2 \\
 - \\
 xy^2 - y \\
 \hline
 x + y^2 + y \\
 \hline
 y^2 + y \\
 - \\
 y^2 - 1 \\
 \hline
 y + 1 \\
 \hline
 1 \\
 \hline
 0
 \end{array}
 \quad
 \begin{array}{l}
 \xrightarrow{\text{in } r} \\
 \\
 \xrightarrow{\text{in } r} \\
 \xrightarrow{\text{in } r}
 \end{array}
 \quad
 \begin{array}{l}
 x \\
 \\
 y \\
 1
 \end{array}$$

Daraus folgt

$$x^2 y + xy^2 + y^2 = (x + y) \cdot \underbrace{(xy - 1)}_{f_1} + 1 \cdot \underbrace{(y^2 - 1)}_{f_2} + \underbrace{x + y + 1}_r.$$

Aber die Division ist nicht eindeutig – im einigen Schritten können wir f_2 sowohl als auch f_1 benutzen. Das führt uns zu einem anderem Rest:

$$\begin{array}{r}
x^2y + xy^2 + y^2 \\
- \\
x^2y - x \\
\hline
xy^2 + x + y^2 \\
- \\
xy^2 - x \\
\hline
2x + y^2 \\
\hline
y^2 \\
- \\
y^2 - 1 \\
\hline
1 \\
\hline
0
\end{array}
\quad \xrightarrow{\text{in } r} \quad
\begin{array}{r}
2x \\
1 \\
0
\end{array}$$

$$x^2y + xy^2 + y^2 = x \cdot \underbrace{(xy - 1)}_{f_1} + (x + 1) \cdot \underbrace{(y^2 - 1)}_{f_2} + \underbrace{2x + 1}_r.$$

Beispiel 2. Seien $f = xy^2 - x$, $F = (f_1, f_2)$, $f_1 = xy + 1$, $f_2 = y^2 - 1$. Dann gilt

$$\begin{aligned}
xy^2 - x &= y(xy + 1) + 0(y^2 - 1) + (-x - y) \\
xy^2 - x &= 0(xy + 1) + x(y^2 - 1) + 0.
\end{aligned}$$

Wir sehen, dass Polynom $xy^2 - x$ in dem Ideal $\langle xy + 1, y^2 - 1 \rangle$ liegt, obwohl einer seiner Reste ungleich 0 ist!

Unser Ziel. Für gegebene Polynome $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ solche Polynome g_1, \dots, g_t finden, dass gilt:

- (1) $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$.
- (2) Für jedes Polynom $f \in k[x_1, \dots, x_n]$ existiert nur ein Rest von f modulo (g_1, \dots, g_t) .
- (3) Dieser Rest gleich 0 nur dann, wenn $f \in I$ ist.

Vorlesung 3

Hilberts Basissatz und Gröbner Basis für ein Ideal

Lemma (Dickson). Jede Menge von Monomen $X \subseteq k[x_1, \dots, x_n]$ enthält eine endliche Untermenge $Y \subseteq X$, so dass jedes Monom aus X ein Mehrfaches eines Monomes aus Y ist.

Mitgliedschaftsproblem für monomiale Ideale. Seien m_1, \dots, m_k Monome und sei f ein Polynom in $k[x_1, \dots, x_n]$. Es gilt $f \in \langle m_1, \dots, m_k \rangle$ nur dann, wenn jedes Monom von f durch eines Monom m_i teilbar ist.

Hilberts Basissatz. Sei k ein Körper. Dann ist jedes Ideal $I \subseteq k[x_1, \dots, x_n]$ endlich erzeugt.

Beweis. Fixieren wir eine monomiale Ordnung \succ und betrachten wir das Ideal $\langle \text{LM}(f) \mid f \in I \rangle$. Nach Lemma von Dickson existieren Polynome $f_1, \dots, f_s \in I$, so dass gilt

$$\langle \text{LM}(f) \mid f \in I \rangle = \langle \text{LM}(f_1), \dots, \text{LM}(f_s) \rangle. \quad (1)$$

Behauptung: $I = \langle f_1, \dots, f_s \rangle$. In der Tat, von einer Seite ist

$$f = q_1 f_1 + \dots + q_s f_s + r,$$

wobei $r = 0$ ist oder alle Monome von r nicht durch $\text{LM}(f_1), \dots, \text{LM}(f_s)$ teilbar sind. Von anderer Seite ist $r \in I$ und so existieren Polynome $h_1, \dots, h_s \in k[x_1, \dots, x_n]$ mit

$$\text{LM}(r) = \sum_{i=1}^s h_i \cdot \text{LM}(f_i).$$

Deshalb ist $\text{LM}(r)$ durch einen $\text{LM}(f_i)$ teilbar. Also, ist $r = 0$.

Folgerung. Sei $I_1 \subseteq I_2 \subseteq \dots$ eine unendliche Kette von wachsenden Idealen in $k[x_1, \dots, x_n]$. Dann existiert ein $m \geq 1$, so dass $I_m = I_{m+1} = \dots$ ist.

Definition. Sei \succ eine monomiale Ordnung. Eine endliche Untermenge $G = \{f_1, \dots, f_s\} \subseteq I$ heißt *Gröbner Basis von I* , wenn (1) gilt.

Satz. Für jedes Ideal $I \subseteq k[x_1, \dots, x_n]$ und jede monomiale Ordnung \succ existiert eine Gröbner Basis von I . Diese Basis erzeugt I .

Beweis folgt aus dem Beweis von Hilberts Basissatzes.

Beispiele. Betrachten wir die lexikografische Ordnung \succ , wobei $x \succ y \succ z$ ist.

1) Sei $I = \langle x + z, y - z \rangle$. Dann ist $\{x + z, y - z\}$ eine Gröbner Basis für I .

2) Sei $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Dann ist $\{x^3 - 2xy, x^2y - 2y^2 + x\}$ keine Gröbner Basis für I .

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

Eigenschaften von Gröbner Basis

Satz. Sei I ein Ideal in $k[x_1, \dots, x_n]$, sei $G = \{g_1, \dots, g_s\}$ eine Gröbner Basis für I und sei f ein Polynom aus $k[x_1, \dots, x_n]$. Dann existiert ein einziges Polynom $r \in k[x_1, \dots, x_n]$ so dass folgende Bedingungen gelten.

- 1) Kein Monom von r ist durch $\text{LM}(g_1), \dots, \text{LM}(g_s)$ teilbar.
- 2) Es existiert ein $h \in I$, so dass $f = h + r$ gilt.

Beweis. Existenz ist eine Folge von Divisions-Algorithmus. Einzigkeit: Wenn $f = h_1 + r_1 = h_2 + r_2$ ist, dann ist $r_1 - r_2 \in I$. Deshalb existiert $g_i \in G$, so dass $\text{LM}(r_1 - r_2)$ durch $\text{LM}(g_i)$ teilbar ist. Aber ist $\text{LM}(r_1 - r_2) \subseteq (\text{Monome von } r_1) \cup (\text{Monome von } r_2)$. Ein Widerspruch.

Wir bezeichnen $r = \text{Rest}_G(f)$

Folgerung 1. Wenn wir f durch G teilen, dann erhalten wir ein einziges r , egal, welche Wege von Division wir nehmen.

Folgerung 2. $f \in I \Leftrightarrow \text{Rest}_G(f) = 0$.

Definition. Seien f, g zwei Polynome aus $k[x_1, \dots, x_n]$ und seien $\text{LMG}(f) = ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ und $\text{LMG}(g) = bx_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$ ihre leitende Mitglieder, wobei $a, b \in k$ ist. Sei $\gamma_i = \max(\alpha_i, \beta_i)$, $i = 1, \dots, n$. Bezeichnen wir

$$x^\gamma = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_n^{\gamma_n},$$

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

Bemerkung. 1) Es gilt $\text{MGRAD}(S(f, g)) \prec \gamma$.

2) Das Polynom $S(f, g)$ liegt in dem Ideal $\langle f, g \rangle$.

Beispiel. Seien $f = x^3 y^2 - x^2 y^3 + x$ und $g = 3x^4 y + y$. Nehmen wir die lex-Ordnung mit $y \succ z \succ x$. Dann gilt

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

Satz (Buchbergers Kriterium). Sei $I = \langle g_1, \dots, g_s \rangle$ ein Ideal in $k[x_1, \dots, x_n]$. Die Menge $G = \{g_1, \dots, g_s\}$ ist eine Gröbner Basis für I nur dann, wenn $\text{Rest}_G S(g_i, g_j) = 0$ für alle $i \neq j$ ist.

Beispiele. 1) Sei $I = \langle y - x^2, z - x^3 \rangle$ ein Ideal in $\mathbb{R}[x, y, z]$. Sei \succ die lex-Ordnung, wobei $y \succ z \succ x$ ist. Dann ist

$$\begin{aligned} S(y - x^2, z - x^3) &= \frac{yz}{y} \cdot (y - x^2) - \frac{yz}{z} \cdot (z - x^3) \\ &= -zx^2 + yx^3 \end{aligned}$$

und

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

Deshalb ist $G\{y - x^2, z - x^3\}$ eine Gröbner Basis von I bezüglich \succ .

2) G ist keine Gröbner Basis für I bezüglich der lex-Ordnung, wobei $x \succ y \succ z$ ist.

Vorlesung 4

Beweis von Buchbergers Kriterium

Lemma. Seien f_1, \dots, f_s Polynome aus $k[x_1, \dots, x_n]$, die den gleichen Multigrad δ haben. Wenn $\text{MGRAD}(\sum_{i=1}^s f_i) \prec \delta$ ist, dann ist $\sum_{i=1}^s f_i$ eine lineare Kombination von $S(f_i, f_j)$ mit Koeffizienten aus k . Außerdem ist $\text{MGRAD}(S(f_i, f_j)) \prec \delta$.

Beweis. Sei $\text{LMG}(f_i) = c_i x^\delta$. Dann ist $\sum_{i=1}^s c_i = 0$, weil $\text{MGRAD}(\sum_{i=1}^s f_i) \prec \delta$ ist. Außerdem gilt

$$S(f, g) = \frac{x^\delta}{c_i x^\delta} f_i - \frac{x^\delta}{c_j x^\delta} f_j = \frac{f_i}{c_i} - \frac{f_j}{c_j}.$$

Deshalb gilt

$$\begin{aligned} \sum_{i=1}^s f_i &= c_1 \left(\frac{f_1}{c_1} - \frac{f_2}{c_2} \right) + (c_1 + c_2) \left(\frac{f_2}{c_2} - \frac{f_3}{c_3} \right) + \dots + (c_1 + c_2 + \dots + c_{s-1}) \left(\frac{f_{s-1}}{c_{s-1}} - \frac{f_s}{c_s} \right) + \sum_{i=1}^s c_i \frac{f_s}{c_s} \\ &= c_1 S(f_1, f_2) + (c_1 + c_2) S(f_2, f_3) + \dots + (c_1 + c_2 + \dots + c_{s-1}) S(f_{s-1}, f_s) + 0. \end{aligned}$$

Satz (Buchbergers Kriterium). Sei $I = \langle g_1, \dots, g_s \rangle$ ein Ideal in $k[x_1, \dots, x_n]$. Die Menge $G = \{g_1, \dots, g_s\}$ ist eine Gröbner Basis für I nur dann, wenn $\text{Rest}_G S(g_i, g_j) = 0$ für alle $i \neq j$ ist.

Beweis. Sei G eine Gröbner Basis für I . Dann ist der Rest jedes Polynoms von I modulo G gleich 0. Da $S(g_i, g_j)$ im Ideal I liegt, haben wir $\text{Rest}_G S(g_i, g_j) = 0$.

Jetzt sei $\text{Rest}_G S(g_i, g_j) = 0$ für alle $i \neq j$. Beweisen wir, dass G eine Gröbner Basis von I ist. Also müssen wir folgendes beweisen: Sei $f \in I$, dann ist $\text{LM}(f)$ durch ein $\text{LM}(g_i)$ teilbar.

Da $f \in I$ ist, existieren Polynome h_1, \dots, h_s , so dass $f = \sum_{i=1}^s h_i g_i$ gilt. Bezeichnen wir $m(i) = \text{MGRAD}(h_i g_i)$ und $\delta = \max m(i)$. Dann ist es klar, dass $\text{MGRAD}(f) \preceq \delta$ ist.

Fall 1: $\text{MGRAD}(f) = \delta$. Dann existiert i_0 , so dass $\text{MGRAD}(f) = \text{MGRAD}(h_{i_0} g_{i_0})$ gilt. Dann ist $\text{LM}(f) = \text{LM}(h_{i_0} g_{i_0})$ und so ist $\text{LM}(f)$ durch $\text{LM}(g_{i_0})$ teilbar. Das bedeutet, dass G eine Gröbner Basis für I ist.

Fall 2: $\text{MGRAD}(f) \prec \delta$. Dann werden wir beweisen, dass andere Polynome h'_1, \dots, h'_s existieren, so dass $f = \sum_{i=1}^s h'_i g_i$ und $\text{MGRAD}(h'_i g_i) \prec \delta$ gilt ($i = 1, \dots, s$).

Weil δ nicht unendlich fallen kann, erhalten wir irgendwann Fall 1. Also, sei $\text{MGRAD}(f) \prec \delta$. Wir haben

$$f = \sum_{m(i)=\delta} \text{LMG}(h_i) g_i + \sum_{m(i)<\delta} (h_i - \text{LMG}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \quad (1)$$

Da der Multigrad von f und die Multigrade aller Mitglieder in den letzten zwei Summen kleiner als δ sind, ist der Multigrad der ersten Summe kleiner als δ . Nach dem Lemma ist $\sum_{m(i)=\delta} \text{LMG}(h_i) g_i$ eine lineare Kombination von $S(\text{LMG}(h_i) g_i, \text{LMG}(h_j) g_j)$.

Weiterhin sind folgende Punkte wichtig.

- Der Multigrad von $S(\text{LMG}(h_i)g_i, \text{LMG}(h_j)g_j)$ ist kleiner als δ (siehe das Lemma).
- Das Polynom $S(\text{LMG}(h_i)g_i, \text{LMG}(h_j)g_j)$ ist ein Mehrfaches von $S(g_i, g_j)$.
- Nach der Voraussetzung ist $\text{Rest}_G S(g_i, g_j) = 0$. Mit Hilfe des Divisions-Algorithmus können wir $S(g_i, g_j)$ in der folgenden Form aufschreiben: $S(g_i, g_j) = \sum_{k=1}^s p_k g_k$, wobei die Multigrade von $p_k g_k$ nicht größer sind als der Multigrad von $S(g_i, g_j)$.

Diese Punkte ermöglichen uns, die erste Summe in (1) in der Form $\sum_{k=1}^s r_k g_k$ umzuschreiben, wobei der Multigrad von $r_k g_k$ kleiner ist als δ . Wie wir schon bemerkt haben, sind die Multigrade aller Mitglieder in den letzten zwei Summen kleiner als δ .

Deshalb existieren die Polynome h'_1, \dots, h'_s , so dass $f = \sum_{i=1}^s h'_i g_i$ und $\text{MGRAD}(h'_i g_i) \prec \delta$ gilt ($i = 1, \dots, s$).

Vorlesungen 5-6

Buchbergers Algorithmus, minimale und irreduzible Gröbner Basen

Satz (Buchbergers Algorithmus). Sei $I = \langle f_1, \dots, f_s \rangle \neq 0$ ein Ideal in $k[x_1, \dots, x_n]$. Dann kann eine Gröbner Basis für I in einer endlichen Anzahl von Schritten mit folgendem Algorithmus konstruiert sein.

1) Setzen wir $F_0 = \langle f_1, \dots, f_s \rangle$.

2) Nehmen wir an, dass F_i schon konstruiert ist. Berechnen wir $\text{Rest}_{F_i} S(p, q)$ für alle verschiedene $p, q \in F_i$.

Wenn für alle $p, q \in F_i$ gilt $\text{Rest}_{F_i} S(p, q) = 0$, dann ist F_i eine Gröbner Basis für I . In dem Fall beenden wir weitere Berechnungen.

Wenn $p, q \in F_i$ existieren, so dass $r = \text{Rest}_{F_i} S(p, q) \neq 0$ gilt, dann setzen wir $F_{i+1} = F_i \cup \{r\}$ und wir setzen die Berechnungen fort.

Beweis – Hinweis. Angesichts Buchbergers Kriterium müssen wir nur das beweisen, dass der Algorithmus angehalten wird. Wenn das nicht eingehalten wird, dann werden wir eine unendliche wachsende Kette von Mengen haben: $F_0 \subset F_1 \subset F_2 \subset \dots$. Dann haben wir eine unendliche wachsende Kette von Idealen: $\langle \text{LM}(F_0) \rangle \subset \langle \text{LM}(F_1) \rangle \subset \langle \text{LM}(F_2) \rangle \subset \dots$. Das ist ein Widerspruch.

Lemma. Sei I ein Ideal in $k[x_1, \dots, x_n]$ und sei G eine Gröbner Basis für I . Sei $p \in G$ ein Polynom mit $\text{LM}(p) \in \langle \text{LM}(G \setminus \{p\}) \rangle$. Dann ist $G \setminus \{p\}$ auch eine Gröbner Basis für I .

Beweis. Der Beweis folgt aus der Definition der Gröbner Basis und aus der Formel $\langle \text{LM}(I) \rangle = \langle \text{LM}(G) \rangle = \langle \text{LM}(G \setminus \{p\}) \rangle$.

Definition. Eine Gröbner Basis G für ein Ideal I heißt *minimal*, wenn gilt:

- (1) $\text{LK}(p) = 1$ für alle $p \in G$,
- (2) $\text{LM}(p) \notin \langle \text{LM}(G \setminus \{p\}) \rangle$.

Satz. Sei I ein Ideal in $k[x_1, \dots, x_n]$. Dann existiert für jede monomiale Ordnung eine minimale Gröbner Basis für I .

Beweis. Sei G eine Gröbner Basis für I . Wenn ein Polynom $p \in G$ mit $\text{LM}(p) \in \langle \text{LM}(G \setminus \{p\}) \rangle$ existiert, dann setzen wir $G := G \setminus \{p\}$ und wiederholen die Eliminierung mit dem neuen G . Am Ende dieses Prozesses erhalten wir eine Gröbner Basis G , die die Bedingung (2) erfüllt. Mit einer Division können wir auch die Bedingung (1) erfüllen.

Beispiel. Sei $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ ein Ideal in $k[x, y]$. Dann hat I folgende Gröbner Basis bezüglich \succ_{grlex} :

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2y - 2y^2 + x, \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

Nach dem Eliminierungsprozess erhalten wir die minimale Gröbner Basis:

$$\begin{aligned}\tilde{f}_1 &= x^2, \\ \tilde{f}_4 &= xy, \\ \tilde{f}_5 &= y^2 - \frac{1}{2}x.\end{aligned}$$

Aber die minimale Gröbner Basis ist nicht einzig. Zum Beispiel für alle $a \in k$ ist

$$\begin{aligned}\tilde{f}_1 &= x^2 + axy, \\ \tilde{f}_4 &= xy, \\ \tilde{f}_5 &= y^2 - \frac{1}{2}x.\end{aligned}$$

auch eine minimale Gröbner Basis für I .

Unser Ziel ist, eine einzige minimale Gröbner Basis kanonisch auszuwählen.

Lemma. Seien G und \tilde{G} zwei minimale Gröbner Basen für I . Dann ist $\text{LM}(G) = \text{LM}(\tilde{G})$.

Beweis. Wir haben $\langle \text{LM}(I) \rangle = \langle \text{LM}(G) \rangle = \langle \text{LM}(\tilde{G}) \rangle$. Dann existiert für jedes $p \in G$ ein $\tilde{p} \in \tilde{G}$, so dass gilt $\text{LM}(\tilde{p}) \mid \text{LM}(p)$. Analog existiert $q \in G$, so dass gilt $\text{LM}(q) \mid \text{LM}(\tilde{p})$. Also gilt

$$\text{LM}(q) \mid \text{LM}(\tilde{p}) \mid \text{LM}(p).$$

Nehmen wir an, dass $q \neq p$ ist. Dann ist $\text{LM}(q) \in \text{LM}(G \setminus \{p\})$ und so ist $\text{LM}(p) \in \langle \text{LM}(G \setminus \{p\}) \rangle$. Ein Widerspruch mit der Minimalität von G . Also ist $p = q$ und deshalb ist $\text{LM}(\tilde{p}) = \text{LM}(p)$.

Definition. Eine Gröbner Basis G für ein Ideal I heißt *irreduzibel*, wenn folgende Bedingungen gelten:

- (1) $\text{LK}(p) = 1$ für alle $p \in G$.
- (2) Wenn m ein Monom von $p \in G$ ist, dann ist $m \notin \langle \text{LM}(G \setminus \{p\}) \rangle$.

Bemerkung 2. Aus (2) folgt:

wenn m ein Monom von $p \in G$ ist und $p \neq \text{LM}(p)$ ist, dann ist $m \notin \langle \text{LM}(G) \rangle$.

Satz. Sei I ein Ideal in $k[x_1, \dots, x_n]$. Dann existiert für jede monomiale Ordnung eine einzige irreduzible Gröbner Basis für I .

Beweis. Zuerst beweisen wir die Existenz. Sei $G = \{g_1, g_2, \dots, g_k\}$ eine minimale Gröbner Basis für I . Berechnen wir $g'_1 = \text{Rest}_{G \setminus \{g_1\}}(g_1)$ und setzen wir $G_1 = \{g'_1, g_2, \dots, g_n\}$.

BEHAUPTUNG. Die folgenden Eigenschaften gelten.

- 1) $g' \in I$.
- 2) $\text{LM}(g'_1) = \text{LM}(g_1)$.
- 3) Für jedes Monom m von g'_1 gilt $m \notin \langle \text{LM}(G \setminus \{g_1\}) \rangle$.

Beweis. Die Eigenschaften 1) und 3) folgen aus dem Divisionprozess. Beweisen wir 2). Da Basis G minimal ist, haben wir $\text{LM}(g_1) \notin \langle \text{LM}(G \setminus \{g_1\}) \rangle$. Deshalb kann $\text{LM}(g_1)$ nicht mit der Division durch $G \setminus \{g_1\}$ gelöscht sein. Also kommt $\text{LM}(g_1)$ in $\text{Rest}_{G \setminus \{g_1\}}(g_1)$. Daraus folgt $\text{LM}(g'_1) = \text{LM}(g_1)$.

Wir setzen den Beweis des Satzes fort. Berechnen wir $g'_2 = \text{Rest}_{G_1 \setminus \{g_2\}}(g_2)$ und setzen wir $G_2 = \{g'_1, g'_2, \dots, g_n\}$. Setzen wir es so fort, erhalten wir eine Menge

$G_n = \{g'_1, g'_2, \dots, g'_n\}$. Dann ist G_n eine Gröbner Basis für I . Das folgt aus den Gleichungen $\text{LM}(G) = \text{LM}(G_1) = \dots = \text{LM}(G_n)$. Nach der Bedingung 3) ist die Basis G_n irreduzibel.

Einzigkeit. Seien G und \tilde{G} zwei irreduzible Gröbner Basen. Da sie minimal sind, gilt $\text{LM}(G) = \text{LM}(\tilde{G})$. Seien $g \in G$ und $\tilde{g} \in \tilde{G}$ zwei Polynome mit $\text{LM}(g) = \text{LM}(\tilde{g})$. Wir haben

$$I \ni g - \tilde{g} \Rightarrow \text{Rest}_G(g - \tilde{g}) = 0.$$

Von anderer Seite ist

$$\text{LM}(g - \tilde{g}) \prec \text{LM}(g) = \text{LM}(\tilde{g}).$$

Merken wir an, dass $m = \text{LM}(g - \tilde{g})$ ein Monom von g oder \tilde{g} ist. Da m nicht leitendes Monom in g und in \tilde{g} ist, haben wir $m \notin \langle \text{LM}(G) \rangle = \langle \text{LM}(\tilde{G}) \rangle$ nach der Bemerkung 2. Deshalb geht $\text{LM}(g - \tilde{g})$ in $\text{Rest}_G(g - \tilde{g})$. Da dieser Rest gleich 0 ist, haben wir $g - \tilde{g} = 0$.

Satz 5. Seien $f, g \in k[x]$ zwei Polynome der Grade $l > 0$ und $m > 0$ entsprechend. Dann existieren Polynome $A, B \in k[x]$, so dass gelten

- (1) $A \neq 0, B \neq 0$,
- (2) $\text{Grad}_x(A) \leq m - 1, \text{Grad}_x(B) \leq l - 1$.
- (3) $Af + Bg = \mathbf{Res}(f, g; x)$.

Die Koeffizienten von A und B sind ganzzahlige Polynome von Koeffizienten f, g .

Beispiel. Seien $f = xy - 1, g = x^2 + y^2 - 4$. Dann ist $\mathbf{Res}(f, g; x) = y^4 - 4y^2 + 1$,

$$-(yx + 1)f + y^2g = y^4 - 4y^2 + 1.$$

Verabredung. Sei $f \in k[x_1, \dots, x_n]$ ein Polynom. Wir werden sagen, dass f hängt von x_1 ab, wenn $\text{Grad}_{x_1}(f) > 0$ ist.

Satz 6. Seien $f, g \in k[x_1, \dots, x_n]$ zwei Polynome, die von x_1 abhängen. Die folgenden Aussagen sind äquivalent:

- (1) Die Polynome f, g haben einen gemeinsamen Faktor, und der Faktor hängt von x_1 ab.
- (2) $\mathbf{Res}(f, g; x_1) = 0$.

Folgerung 7. Sei k ein algebraisch abgeschlossener Körper und seien $f, g \in k[x] \setminus k$. Die Polynome f, g haben eine gemeinsame Nullstelle nur dann, wenn $\mathbf{Res}(f, g; x) = 0$ ist.

Vorlesungen 8-9

Eliminationstheorie

Definition. Sei $I = \langle f_1, \dots, f_s \rangle$ ein Ideal im $k[x_1, \dots, x_n]$. Das l -en *Eliminationsideal* von I ist ein Ideal

$$I_l = I \cap k[x_{l+1}, \dots, x_n]$$

in dem Ring $k[x_{l+1}, \dots, x_n]$.

Eliminationsatz. Sei $I = \langle f_1, \dots, f_s \rangle$ ein Ideal im $k[x_1, \dots, x_n]$ und sei G eine Gröbner Basis von I bezüglich der lex-Ordnung \succ , wobei $x_1 \succ x_2 \succ \dots \succ x_n$ ist. Dann ist für alle $0 \leq l \leq n$ die Menge

$$G_l = G \cap k[x_{l+1}, \dots, x_n]$$

eine Gröbner Basis vom l -en Eliminationsideal I_l .

Beweis. Es ist klar, dass G_l in I_l liegt. Die Menge G_l ist eine Gröbner Basis für I_l nur dann, wenn für jeden $f \in I_l$ ein $g \in G_l$ mit $\text{LM}(g) | \text{LM}(f)$ existiert.

Sei $f \in I_l$. Dann ist $f \in I$, deshalb existiert ein $g \in G$ mit $\text{LM}(g) | \text{LM}(f)$. Da $\text{LM}(f) \in k[x_{l+1}, \dots, x_n]$ ist, ist $\text{LM}(g) \in k[x_{l+1}, \dots, x_n]$ auch. Daraus folgt $g \in k[x_{l+1}, \dots, x_n]$.

Folgendes Lemma hilft, den Erweiterungssatz zu beweisen.

Lemma. Seien $f, g \in k[x_1, \dots, x_n]$ zwei Polynome, die von x_1 abhängen. Sei I_1 das erste Eliminationsideal von $I = \langle f, g \rangle$. Dann gelten:

- 1) $\text{Res}(f, g; x_1) \in I_1$, wobei I_1 das erste Eliminationsideal von $I = \langle f, g \rangle$ ist.
- 2) $\text{Res}(f, g; x_1) = 0$ nur dann, wenn f und g einen gemeinsamen Faktor haben und der Faktor hängt von x_1 ab.

Erweiterungssatz für zwei Polynome. Sei k ein algebraisch abgeschlossener Körper. Seien f, g zwei Polynome aus $k[x_1, \dots, x_n]$:

$$\begin{aligned} f &= a_0(x_2, \dots, x_n)x_1^l + \dots + a_l, \text{ wobei } l > 0 \text{ und } a_0 \neq 0 \text{ ist,} \\ g &= b_0(x_2, \dots, x_n)x_1^m + \dots + b_m, \text{ wobei } m > 0 \text{ und } b_0 \neq 0 \text{ ist.} \end{aligned}$$

Sei (c_2, \dots, c_n) eine Nullstelle von $\text{Res}(f, g; x_1)$. Wenn $a_0(c_2, \dots, c_n) \neq 0$ oder $b_0(c_2, \dots, c_n) \neq 0$ ist, dann existiert $c_1 \in k$, so dass (c_1, c_2, \dots, c_n) eine gemeinsame Nullstelle von f, g ist.

Beweis. Nach den Bedingungen gilt

$$0 = \text{Res}(f, g; x_1) \Big|_{\substack{(x_2, \dots, x_n) \\ = (c_2, \dots, c_n)}} = \text{Res}(f(x_1, c_2, \dots, c_n), g(x_1, c_2, \dots, c_n); x_1).$$

Nach der Folgerung 7 existiert eine gemeinsame Nullstelle von Polynomen $f(x_1, c_2, \dots, c_n)$ und $g(x_1, c_2, \dots, c_n)$. Bezeichnen wir diese Nullstelle als c_1 .

Um den Erweiterungssatz für einige Polynome zu beweisen, müssen wir verallgemeinerte Resultanten einiger Polynome definieren.

Definition. Seien $f_1, f_2, \dots, f_s \in k[x_1, \dots, x_n]$. Nehmen wir neue Unbekannte u_2, \dots, u_n und bilden das Polynom $u_2 f_2 + \dots + u_s f_s \in k[u_2, \dots, u_s, x_1, \dots, x_n]$. Dann haben wir

$$\mathbf{Res}(f_1, u_2 f_2 + \dots + u_s f_s; x_1) \in k[u_2, \dots, u_s, x_1, \dots, x_n].$$

Schreiben wir diesen Resultant in der Form

$$\mathbf{Res}(f_1, u_2 f_2 + \dots + u_s f_s; x_1) = \sum_{\alpha} h_{\alpha} u^{\alpha},$$

wobei $\alpha = (\alpha_2, \dots, \alpha_s)$, $u^{\alpha} = u_2^{\alpha_2} \dots u_s^{\alpha_s}$ und $h_{\alpha} \in k[x_2, \dots, x_n]$ ist. Die Polynome h_{α} heißen *verallgemeinerte Resultanten* von f_1, f_2, \dots, f_s .

Lemma. Sei $I = \langle f_1, f_2, \dots, f_s \rangle$ ein Ideal in $k[x_1, \dots, x_n]$. Dann liegen alle verallgemeinerte Resultanten von f_1, f_2, \dots, f_n in dem ersten Eliminationsideal I_1 .

Erweiterungssatz. Sei k ein algebraisch abgeschlossener Körper. Sei $I = \langle f_1, \dots, f_s \rangle$ ein Ideal in $k[x_1, \dots, x_n]$ und sei I_1 das erste Eliminationsideal von I . Für alle $1 \leq i \leq s$, schreiben wir f_i in der Form

$$f_i = g_i(x_2, \dots, x_n) x_1^{n_i} + \text{Mitglieder, in denen der Grad von } x_1 \text{ kleiner als } n_i \text{ ist,}$$

wobei $g_i \neq 0$ ist. Sei

$$(c_2, \dots, c_n) \in \mathbf{V}(I_1).$$

Wenn ein $i \in \{1, \dots, s\}$ mit $g_i(c_2, \dots, c_n) \neq 0$ existiert, dann existiert ein $c_1 \in k$ mit

$$(c_1, c_2, \dots, c_n) \in \mathbf{V}(I).$$

Vorlesung 10

Nullstellensatz von Hilbert

Lemma 1. Jeder algebraisch abgeschlossene Körper ist unendlich.

Lemma 2. Sei k ein unendlicher Körper und sei $g \in k[x_1, \dots, x_n]$ ein Polynom. Dann existieren a_1, \dots, a_n , so dass $g(a_1, \dots, a_n) \neq 0$ gilt.

Lemma 3. Jedes Ideal in dem Ring $k[x_1]$ kann mit einem Polynom erzeugt sein.

Definition. Sei $f = \sum_{\alpha} b_{\alpha} x^{\alpha} = \sum_{\alpha} b_{\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ ein Polynom in $k[x_1, \dots, x_n]$. Totale Grad von f ist $\max_{\alpha} \{\alpha_1 + \alpha_2 + \dots + \alpha_n\}$.

Satz 4. Sei k ein algebraisch abgeschlossener Körper und sei $I \subset k[x_1, \dots, x_n]$ ein Ideal mit $\mathbf{V}(I) = \emptyset$. Dann ist $I = k[x_1, \dots, x_n]$.

Beweis. Der Beweis wird per Induktion verlaufen. Für $n = 1$ folgt der Beweis aus dem Lemma 1. Sei $n > 1$. Es ist klar, dass $I \neq 0$ ist. Sei $I = \langle f_1, \dots, f_s \rangle$, wobei f_1, \dots, f_s nichtnullische Polynome sind. Wir können annehmen, dass f_1 keine Konstante ist, sonst ist $I = k[x_1, \dots, x_n]$ und wir sind fertig. Wir translieren unser Problem in einen anderen Ring $k[\tilde{x}_1, \dots, \tilde{x}_n]$, indem \tilde{f}_1 (das Analog von f_1) eine gute Form haben wird.

Seien $a_2, \dots, a_n \in k$ beliebige Elemente (später werden wir sie speziell auswählen). Definieren wir eine Abbildung $\phi : k[x_1, \dots, x_n] \rightarrow k[\tilde{x}_1, \dots, \tilde{x}_n]$ mit den Formeln

$$\begin{aligned} x_1 &\mapsto \tilde{x}_1, \\ x_2 &\mapsto \tilde{x}_2 + a_2 \tilde{x}_1, \\ &\dots \\ x_n &\mapsto \tilde{x}_n + a_n \tilde{x}_1. \end{aligned}$$

Es ist leicht nachzuprüfen, dass ϕ ein Isomorphismus ist. Sei N totale Grad von f_1 . Dann hat \tilde{f}_1 folgende Form:

$$\tilde{f}_1 = g_1(a_2, \dots, a_n) \tilde{x}_1^N + \text{Mitglieder mit } \tilde{x}_1^i, \quad i < N,$$

wobei $g_1(a_2, \dots, a_n)$ ein Polynom von a_2, \dots, a_n ist. Jetzt wählen wir a_2, \dots, a_n so, dass $g_1(a_2, \dots, a_n) \neq 0$ ist (siehe Lemma 2). Mit der Bezeichnung $\tilde{I} = \phi(I)$ haben wir $\tilde{I} = \langle \tilde{f}_1, \dots, \tilde{f}_s \rangle$.

BEHAUPTUNG. Sei $\tilde{I}_1 = \tilde{I} \cap k[\tilde{x}_2, \dots, \tilde{x}_n]$ erstes Eliminationsideal von \tilde{I} . Dann ist

$$\mathbf{V}(\tilde{I}_1) = \emptyset.$$

Beweis. Nehmen wir an, dass existiert $(c_2, \dots, c_n) \in \mathbf{V}(\tilde{I}_1)$. Nach dem Erweiterungssatz (merken Sie an, dass $g_1(a_2, \dots, a_n) \neq 0$ ist) existiert $c_1 \in k$, so dass $(c_1, c_2, \dots, c_n) \in \mathbf{V}(\tilde{I})$ gilt. Aber ist $\mathbf{V}(\tilde{I}) = \phi(\mathbf{V}(I)) = \emptyset$. Ein Widerspruch.

Fortsetzung des Hauptbeweises. Nach Induktion haben wir $\tilde{I}_1 = k[\tilde{x}_2, \dots, \tilde{x}_n]$. Deshalb ist $1 \in \tilde{I}_1 \subseteq \tilde{I}$. Deshalb gilt $\tilde{I} = k[\tilde{x}_1, \dots, \tilde{x}_n]$. Also gilt $I = k[x_1, \dots, x_n]$.

Folgerung. Sei k ein algebraisch abgeschlossener Körper und sei $I \subsetneq k[x_1, \dots, x_n]$ ein Ideal. Dann existiert eine gemeinsame Nullstelle in k^n für alle $f \in I$.

Erinnern wir uns an zwei Definitionen.

Definition 1. Sei I ein Ideal in $k[x_1, \dots, x_n]$. Eine algebraische Menge $\mathbf{V}(I) \subseteq k^n$ ist die Menge aller gemeinsamen Nullstellen der Polynome aus I .

Definition 2. Sei $V \subseteq k^n$ eine Menge. Dann ist die Menge

$$\mathbf{I}(V) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ für alle } (a_1, \dots, a_n) \in V\}$$

ein Ideal. Das Ideal $\mathbf{I}(V)$ heißt *Ideal von V* .

Wichtig ist zu verstehen, was $\mathbf{I}(\mathbf{V}(I))$ ist. Sei $I = \langle f_1, \dots, f_s \rangle$. Ein Polynom f liegt in $\mathbf{I}(\mathbf{V}(I))$ nur dann, wenn folgende Implikation gilt:

$$(\forall i \quad f_i(a_1, \dots, a_n) = 0) \Rightarrow f(a_1, \dots, a_n) = 0. \quad (1)$$

Definition von Radikal. Sei I ein Ideal in $k[x_1, \dots, x_n]$. Die Menge

$$\sqrt{I} = \{f \in k[x_1, \dots, x_n] \mid \exists m \geq 1 : f^m \in I\}$$

heißt *Radikal von I* .

Behauptung. \sqrt{I} ist ein Ideal in $k[x_1, \dots, x_n]$.

Hilbertscher Nullstellensatz. Sei I ein Ideal in $k[x_1, \dots, x_n]$. Dann gilt

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

Beweis. Es ist klar, dass $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$ gilt. In der Tat, wenn $f^m(a_1, \dots, a_n) = 0$ ist, dann ist auch $f(a_1, \dots, a_n) = 0$.

Beweisen wir $\sqrt{I} \supseteq \mathbf{I}(\mathbf{V}(I))$. Sei $f \in \mathbf{I}(\mathbf{V}(I))$, wobei $I = \langle f_1, \dots, f_s \rangle$ ist. Wir müssen beweisen, dass eine natürliche Zahl $m \geq 1$ und Polynome A_1, \dots, A_s mit

$$f^m = \sum_{i=1}^s A_i f_i. \quad (2)$$

existieren. Sei y eine neue Unbekannte. Betrachten wir das Ideal

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

Wir behaupten, dass $\mathbf{V}(\tilde{I}) = \emptyset$ ist. In der Tat, nach (1) gilt: wenn (a_1, \dots, a_n) eine gemeinsame Nullstelle von f_1, \dots, f_s ist, dann ist (a_1, \dots, a_n) eine Nullstelle von f , und so ist keine Nullstelle von $1 - yf$.

Also gilt $\mathbf{V}(\tilde{I}) = \emptyset$. Daraus folgt $\tilde{I} = k[x_1, \dots, x_n, y]$ (siehe Satz 4). Das bedeutet, dass 1 in \tilde{I} liegt, und so Polynome p_1, \dots, p_s, q existieren, so dass gilt

$$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(1 - yf).$$

Setzen wir $y = 1/f(x_1, \dots, x_n)$. Dann erhalten wir

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

Nach eine passende Multiplikation mit f^m erhalten wir die gewünschte Gleichung (2).

Vorlesung 11

Zariski Abschluss und Abschluss-Satz

Satz. Sei k ein Körper. Dann gelten die folgenden Eigenschaften:

- (1) $(I_1 \subseteq I_2) \Rightarrow (\mathbf{V}(I_1) \supseteq \mathbf{V}(I_2))$,
- (2) $(S_1 \subseteq S_2) \Rightarrow (\mathbf{I}(S_1) \supseteq \mathbf{I}(S_2))$,
- (3) $S \subseteq \mathbf{V}(\mathbf{I}(S))$,
- (4) $I \subseteq \mathbf{I}(\mathbf{V}(S))$,
- (5) $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$.

Definition. Ein Ideal $I \subseteq k[x_1, \dots, x_n]$ heißt *radikales Ideal*, wenn $I = \sqrt{I}$ ist.

Behauptung. Sei $S \subseteq k^n$ eine Untermenge. Dann ist $\mathbf{I}(S)$ ein radikales Ideal.

Satz. Sei k ein Körper. Betrachten wir zwei Abbildungen:

$$\begin{array}{ccc} & \mathbf{I} & \\ & \longrightarrow & \\ \text{algebraische Mengen} & & \text{radikale Ideale.} \\ & \mathbf{V} & \\ & \longleftarrow & \end{array}$$

Wenn S eine algebraische Menge ist, dann gilt $\mathbf{V}(\mathbf{I}(S)) = S$. Daraus folgt, dass \mathbf{I} eine Injektion ist.

Wenn k ein algebraisch abgeschlossener Körper ist, dann sind \mathbf{I} und \mathbf{V} inverse Bijektionen.

Folgerung. Sei k ein algebraisch abgeschlossener Körper. Dann ist

$$\mathbf{V}(I_1) = \mathbf{V}(I_2) \Leftrightarrow \sqrt{I_1} = \sqrt{I_2}.$$

Lemma – Definition. Sei S eine Untermenge von k^n . Dann ist $\mathbf{V}(\mathbf{I}(S))$ die kleinste algebraische Menge, die S enthält. Diese algebraische Menge heißt *Zariski Abschluss* von S und wird bezeichnet als \overline{S} .

Definition. Sei $\pi_l : k^n \mapsto k^{n-l}$ eine Projektion: $\pi_l(x_1, \dots, x_n) = (x_{l+1}, \dots, x_n)$.

Abschluss-Satz. Sei k ein algebraisch abgeschlossener Körper. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal und sei I_l das l -en Eliminationsideal von I . Dann gelten:

- 1) $\mathbf{V}(I_l)$ ist der Zariski Abschluss von $\pi_l(\mathbf{V}(I))$.
- 2) Wenn $\mathbf{V}(I) \neq \emptyset$ ist, existiert eine algebraische Menge $W \subsetneq \mathbf{V}(I_l)$, so dass gilt

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

Beweis. 1) Nach dem Lemma, müssen wir folgende Formel beweisen:

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

Nach der Folgerung und der Behauptung ist das äquivalent:

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

Wir haben $f \in \mathbf{I}(\pi_l(\mathbf{V}(I)))$ nur dann, wenn $f \in k[x_{l+1}, \dots, x_n]$ und $f(c_{l+1}, \dots, c_n) = 0$ für alle $(c_{l+1}, \dots, c_n) \in \pi_l(\mathbf{V}(I))$ ist.

Das geschieht nur dann, wenn $f \in k[x_{l+1}, \dots, x_n]$ und $f(c_1, \dots, c_n) = 0$ für alle $(c_1, \dots, c_n) \in \mathbf{V}(I)$ ist.

Nach dem Hilbertschen Satz geschieht das nur dann, wenn $f \in k[x_{l+1}, \dots, x_n]$ und $f \in \sqrt{I}$ ist.

Das ist äquivalent $f \in \sqrt{I_l}$.

Vorlesung 12

Summen, Produkte und Überschneidungen von Idealen

Definition. Seien I, J zwei Ideale in $k[x_1, \dots, x_n]$.
Die *Summe* von I und J ist das Ideal

$$I + J = \{f + g \mid f \in I, g \in J\}.$$

Das *Produkt* von I und J ist das Ideal

$$I \cdot J = \langle fg \mid f \in I, g \in J \rangle.$$

Behauptung. Seien $I = \langle f_1, \dots, f_r \rangle$ und $J = \langle g_1, \dots, g_s \rangle$ zwei Ideale. Dann ist

$$I + J = \langle f_1, \dots, f_r, g_1, \dots, g_s \rangle.$$

und

$$I \cdot J = \langle f_i g_j \mid 1 \leq i \leq r, 1 \leq j \leq s \rangle.$$

Satz. Seien I, J zwei Ideale in $k[x_1, \dots, x_n]$. Dann ist $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$ und $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(I \cap J)$.

Definition 2. Seien f, g zwei Polynome aus $k[x_1, \dots, x_n]$. Ein Polynom $h \in k[x_1, \dots, x_n]$ heißt ein *großer gemeinsamer Teiler von f und g* (bezeichnet als $\mathbf{ggT}(f, g)$), wenn

- (1) h ein Teiler von f und g ist,
- (2) jeder Teiler von f und g ein Teiler von h ist.

Definition 3. Seien f, g zwei Polynome aus $k[x_1, \dots, x_n]$. Ein Polynom $h \in k[x_1, \dots, x_n]$ heißt ein *kleiner gemeinsamer Vielfacher von f und g* (bezeichnet als $\mathbf{kgV}(f, g)$), wenn gilt:

- (1) f und g Teiler von h sind,
- (2) wenn f und g Teiler eines Polynoms sind, dann ist h es auch.

Behauptung. Es gilt

$$\mathbf{ggT}(f, g) = \frac{fg}{\mathbf{kgV}(f, g)}.$$

Satz. Seien f, g zwei Polynome aus $k[x_1, \dots, x_n]$. Dann ist

$$\langle f \rangle \cap \langle g \rangle = \langle \mathbf{kgV}(f, g) \rangle.$$

Satz. Seien I, J zwei Ideale in $k[x_1, \dots, x_n]$. Dann gilt

$$I \cap J = (tI + (1-t)J) \cap k[x_1, \dots, x_n],$$

wobei t eine neue Unbekannte ist.

Ein Algorithmus für die Berechnung der Überschneidung zweier Ideale.

Seien $I = \langle f_1, \dots, f_r \rangle$ und $J = \langle g_1, \dots, g_s \rangle$ zwei Ideale in $k[x_1, \dots, x_n]$.

Schritt 1. Schreiben wir das Ideal $\langle tf_1, \dots, tf_r, (1-t)g_1, \dots, (1-t)g_s \rangle \subseteq k[x_1, \dots, x_n, t]$ auf.

Schritt 2. Berechnen wir eine Gröbner Basis G des Ideals bezüglich der *lex*-Ordnung, wobei $t \succ x_1 \succ \dots \succ x_n$ ist.

Schritt 3. Die Überschneidung $G \cap k[x_1, \dots, x_n]$ ist eine Gröbner Basis von $I \cap J$.

Vorlesung 13

Irreduzible algebraische Mengen, Primideale und maximale Ideale

Definition 1. Eine algebraische Menge $V \subseteq k^n$ heißt *irreduzibel*, wenn aus $V = V_1 \cup V_2$ (V_1, V_2 sind algebraische Mengen) folgt $V = V_1$ oder $V = V_2$.

Definition 2. Ein Ideal $I \subseteq k[x_1, \dots, x_n]$ heißt Primideal, wenn aus $fg \in I$ ($f, g \in k[x_1, \dots, x_n]$) folgt $f \in I$ oder $g \in I$.

Bemerkung. Jedes Primideal ist ein radikales Ideal.

Behauptung. Sei $V \subseteq k^n$ eine algebraische Menge. Dann gilt:

$$(V \text{ ist irreduzibel}) \Leftrightarrow (\mathbf{I}(V) \text{ ist ein Primideal}).$$

Folgerung. Sei k ein algebraisch abgeschlossener Körper. Dann sind die Abbildungen \mathbf{I} und \mathbf{V} im folgenden Schema zueinander inverse Bijektionen:

$$\begin{array}{ccc} \text{irreduzible algebraische Mengen} & \begin{array}{c} \xrightarrow{\mathbf{I}} \\ \xleftarrow{\mathbf{V}} \end{array} & \text{Primideale.} \end{array}$$

Erinnern wir uns an folgende Definition.

Definition. Sei V eine algebraische Menge in k^n . Man sagt, dass V eine *rationale Parameterdarstellung* hat, wenn rationale Funktionen $r_1, \dots, r_n \in k(t_1, \dots, t_m)$ existieren, so dass gilt

1) für alle möglichen $t_1, \dots, t_m \in k$ liegen die Punkte $x = (x_1, \dots, x_n)$ in V , wobei

$$\begin{aligned} x_1 &= r_1(t_1, \dots, t_m), \\ x_2 &= r_2(t_1, \dots, t_m), \\ &\vdots \\ x_n &= r_n(t_1, \dots, t_m), \end{aligned}$$

ist,

2) V ist die kleinste algebraische Menge, die alle diese Punkte enthält. Mit anderen Worten ist V der Zariski Abschluss der Menge

$$\{(r_1(t_1, \dots, t_m), \dots, r_n(t_1, \dots, t_m)) \mid t_1, \dots, t_m \in k\}.$$

Satz. Sei k ein unendlicher Körper. Jede algebraische Menge in k^n , die eine rationale Parameterdarstellung hat, ist irreduzibel.

Definition 3. Ein Ideal $I \subseteq k[x_1, \dots, x_n]$ heißt maximal, wenn

- 1) $I \neq k[x_1, \dots, x_n]$ ist und
- 2) für alle Ideale $J \subseteq k[x_1, \dots, x_n]$ mit $I \subseteq J \subseteq k[x_1, \dots, x_n]$ entweder $J = I$ oder $J = k[x_1, \dots, x_n]$ ist.

Behauptung. Jedes maximale Ideal ist ein Primideal.

Satz. 1) Sei k ein beliebiger Körper. Für jedes Tupel $(a_1, \dots, a_n) \in k^n$ ist das Ideal $\langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq k[x_1, \dots, x_n]$ maximal.

2) Sei k ein algebraisch abgeschlossener Körper. Dann hat jedes maximale Ideal $I \in k[x_1, \dots, x_n]$ die Form $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$.

Folgerung. Sei k ein algebraisch abgeschlossener Körper. Dann sind die Abbildungen **I** und **V** im folgenden Schema zueinander inverse Bijektionen:

$$\begin{array}{ccc} & \mathbf{I} & \\ & \xrightarrow{\quad} & \\ \text{Punkte in } k^n & & \text{maximale Ideale in } k[x_1, \dots, x_n] \\ & \mathbf{V} & \\ & \xleftarrow{\quad} & \end{array}$$

Vorlesung 14

Quotient von zwei Idealen

Behauptung. Seien V, W zwei algebraische Mengen, $V \subseteq W$. Dann gilt

$$W = V \cup \overline{(W \setminus V)}.$$

Lemma-Definition. Seien I, J zwei Ideale in $k[x_1, \dots, x_n]$. Dann ist

$$I : J = \{f \in k[x_1, \dots, x_n] \mid fg \in I \forall g \in J\}$$

ein Ideal. Das Ideal heißt *Quotient von I und J* . Es gilt $I \subseteq I : J$.

Satz. Seien I, J Ideale in $k[x_1, \dots, x_n]$. Dann gilt

$$\mathbf{V}(I : J) \supseteq \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}.$$

Wenn k ein algebraisch abgeschlossener Körper ist, dann gilt

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

Folgerung. Seien V, W zwei algebraische Mengen in k^n . Dann gilt

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

Behauptung. Seien I, I_i, J, J_i und K Ideale in $k[x_1, \dots, x_n]$, $1 \leq i \leq r$. Dann gelten

- (1) $(\bigcap_{i=1}^r I_i) : J = \bigcap_{i=1}^r (I_i : J)$,
- (2) $I : (\sum_{i=1}^r J_i) = \bigcap_{i=1}^r (I : J_i)$,
- (3) $I : \langle f_1, f_2, \dots, f_r \rangle = \bigcap_{i=1}^r (I : \langle f_i \rangle)$.

Satz. Sei I ein Ideal und sei g ein Polynom in $k[x_1, \dots, x_n]$. Wenn h_1, \dots, h_p eine Basis von $I \cap \langle g \rangle$ ist, dann ist $\{h_1/g, \dots, h_p/g\}$ eine Basis von $I : \langle g \rangle$.

Folgerung. Gegeben zwei Ideale $I = \langle f_1, \dots, f_s \rangle$ und $J = \langle g_1, \dots, g_t \rangle$ in $k[x_1, \dots, x_n]$, dann kann man eine Basis von $I : J$ algorithmisch finden.

Vorlesung 15

Zerlegung von algebraischen Mengen in irreduzible algebraische Mengen. Zerlegung von radikalen Idealen in Primideale

Satz. Sei $V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$ eine sinkende Kette der algebraischen Mengen in k^n . Dann existiert eine natürliche N , so dass gilt $V_N = V_{N+1} = \dots$.

Satz. Sei $V \subseteq k^n$ eine algebraische Menge. Dann kann V in der Form

$$V = V_1 \cup \dots \cup V_m$$

dargestellt sein, wobei jede V_i eine irreduzible Menge ist.

Definition. Sei $V \subseteq k^n$ eine algebraische Menge. Eine Zerlegung $V = V_1 \cup \dots \cup V_m$, wobei alle V_i irreduzibel sind, heißt *minimal*, wenn $V_i \not\subseteq V_j$ für $i \neq j$ ist.

Satz. Sei $V \subseteq k^n$ eine algebraische Menge. Dann existiert eine minimale Zerlegung von V in irreduzible Mengen: $V = V_1 \cup \dots \cup V_m$. Wenn $V = V'_1 \cup \dots \cup V'_m$ eine andere minimale Zerlegung von V ist, dann ist $m = m'$ und, nach einer Permutation, ist $V_i = V'_i$ für alle $i = 1, \dots, m$.

Satz. Sei k ein algebraisch abgeschlossener Körper und sei I ein radikales Ideal in $k[x_1, \dots, x_n]$. Dann ist I eine Überschneidung der Primideale:

$$I = P_1 \cap \dots \cap P_m,$$

so dass $P_i \not\subseteq P_j$ für $i \neq j$ gilt. Die Menge solcher Primideale ist einzig.

Lemma 1. Sei P ein Primideal und sei f ein Polynom in $k[x_1, \dots, x_n]$. Dann gilt

$$P : \langle f \rangle = \begin{cases} k[x_1, \dots, x_n], & \text{falls } f \in P \text{ ist,} \\ P, & \text{falls } f \notin P \text{ ist.} \end{cases}$$

Lemma 2. Sei P ein Primideal und seien I_1, \dots, I_r Ideale in $k[x_1, \dots, x_n]$, so dass $P = \bigcap_{i=1}^r I_i$ ist. Dann ist $P = I_i$ für ein i .

Satz. Sei k ein algebraisch abgeschlossener Körper und sei $I \subseteq k[x_1, \dots, x_n]$ ein echtes radikales Ideal. Seien P_1, \dots, P_m Primideale, so dass

$$I = P_1 \cap \dots \cap P_m$$

gilt und $P_i \not\subseteq P_j$ für $i \neq j$ ist. Dann gilt

$$\{P_1, \dots, P_r\} = (\text{Die Menge aller Primideale in } k[x_1, \dots, x_n]) \cap \{I : \langle f \rangle \mid f \in k[x_1, \dots, x_n]\}.$$

Vorlesung 16

Zerlegung von Idealen in Pseudoprimeale

Definition 1. Ein Ideal $I \subseteq k[x_1, \dots, x_n]$ heißt *pseudoprime*, wenn aus $fg \in I$ (wobei $f, g \in k[x_1, \dots, x_n]$ ist) folgt $f \in I$ oder $g^m \in I$ für einen $m \in \mathbb{N}$.

Beispiel. Das Ideal $\langle x^2, y \rangle \subseteq k[x, y]$ ist ein Pseudoprimeal, aber kein Primeal.

Definition 2. Ein Ideal $I \subseteq k[x_1, \dots, x_n]$ heißt *irreduzibel*, wenn aus $I = I_1 \cap I_2$ (wobei I_1, I_2 Ideale sind) folgt $I = I_1$ oder $I = I_2$.

Lemma. (1) Jedes Ideal $I \subseteq k[x_1, \dots, x_n]$ ist eine Überschneidung der endlichen Anzahl von irreduziblen Idealen.

(2) Jedes irreduzible Ideal ist ein Pseudoprimeal.

Definition 3. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal. Eine *Pseudoprime-Zerlegung* von I ist eine Darstellung

$$I = P_1 \cap \dots \cap P_r,$$

wobei P_1, \dots, P_r Pseudoprimeale sind und $r < \infty$ ist. Diese Zerlegung heißt *minimal*, wenn $\sqrt{P_{i_1}} \neq \sqrt{P_{i_2}}$ für $i_1 \neq i_2$ ist und $\bigcap_{j \neq i} P_j \not\subseteq P_i$ für alle $i = 1, \dots, r$ ist.

Beispiel. Das Ideal $I = \langle x^2, y \rangle \subseteq k[x, y]$ hat zwei minimale Pseudoprime-Zerlegungen:

$$I = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x^2, y \rangle.$$

Satz (Lasker – Nöther). Jedes Ideal $I \subseteq k[x_1, \dots, x_n]$ hat eine minimale Pseudoprime-Zerlegung. Seien $I = P_1 \cap \dots \cap P_r$ und $I = Q_1 \cap \dots \cap Q_s$ zwei solche Zerlegungen. Dann ist $\{\sqrt{P_1}, \dots, \sqrt{P_r}\} = \{\sqrt{Q_1}, \dots, \sqrt{Q_s}\}$.

Vorlesung 17

Algorithmische Berechnungen in $k[x_1, \dots, x_n]/I$

I. Faktoring.

Sei R ein Ring und sei $I \subseteq R$ ein Ideal. Für $r_1, r_2 \in R$ schreiben wir $r_1 \sim r_2$, wenn $r_1 - r_2 \in I$ ist. Die Relation \sim ist eine Äquivalenz-Relation, also für alle $r_1, r_2, r_3 \in R$ gilt:

- 1) $r_1 \sim r_1$,
- 2) $r_1 \sim r_2 \Rightarrow r_2 \sim r_1$,
- 3) $(r_1 \sim r_2 \ \& \ r_2 \sim r_3) \Rightarrow r_1 \sim r_3$.

Die Äquivalenz-Klasse von r ist die Menge $[r] = \{r' \mid r' \sim r\}$. Merken wir an, dass zwei Äquivalenz-Klassen $[r_1]$ und $[r_2]$ nur dann gleich sind, wenn $r_1 - r_2 \in I$ ist. Bezeichnen wir als R/I die Menge aller Äquivalenz-Klassen:

$$R/I = \{[r] \mid r \in R\}.$$

Definieren wir natürlicherweise eine Addition und eine Multiplikation auf R/I :

$$\begin{aligned} [r_1] + [r_2] &= [r_1 + r_2], \\ [r_1] \cdot [r_2] &= [r_1 r_2]. \end{aligned}$$

Dann ist R/I ein Ring. Dieser Ring heißt *Faktoring* von R modulo I .

Beispiel. Sei $R = \mathbb{R}[x]$ und sei $I = \langle x^2 - 2 \rangle$. Jedes $f \in R$ kann in der folgenden Form dargestellt sein

$$f = (x^2 - 2)h + (ax + b).$$

Solche Darstellung ist einzig. Dann ist $f \sim (ax + b)$ und so ist $[f] = [ax + b]$. Also ist

$$R/I = \{[ax + b] \mid a, b \in \mathbb{R}\}.$$

Es ist klar:

$$\begin{aligned} [a_1x + b_1] + [a_2x + b_2] &= [(a_1 + a_2)x + (b_1 + b_2)], \\ [a_1x + b_1] \cdot [a_2x + b_2] &= [a_1a_2x^2 + (a_1b_2 + b_1a_2)x + b_1b_2] \\ &= [(a_1a_2x^2 + (a_1b_2 + b_1a_2)x + b_1b_2) - a_1a_2(x^2 - 2)] \\ &= [(a_1b_2 + b_1a_2)x + (b_1b_2 + 2a_1a_2)]. \end{aligned}$$

II. Der Ring $k[x_1, \dots, x_n]/I$.

Fixieren wir eine monomiale Ordnung \succ auf $k[x_1, \dots, x_n]$. Erinnern wir uns an einen Satz über die Gröbner Basis.

Satz 1. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal, sei $G = \{g_1, \dots, g_s\}$ eine Gröbner Basis für I und sei f ein Polynom aus $k[x_1, \dots, x_n]$. Dann existiert ein einziges Polynom $r \in k[x_1, \dots, x_n]$, so dass folgende Bedingungen gelten:

- 1) Kein Monom von r ist durch $\text{LM}(g_1), \dots, \text{LM}(g_s)$ teilbar.
- 2) Es existiert ein Polynom $h \in I$, so dass $f = h + r$ gilt.

Dieses r heißt *Rest von f modulo G* und ist als $\text{Rest}_G(f)$ bezeichnet.

Folgerung. Die Polynome f, g mit $f - g \in I$ haben gleiche Reste modulo G .

Bezeichnung. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal und sei $G = \{g_1, \dots, g_s\}$ eine Gröbner Basis von I . Bezeichnen wir als V_G den Vektorraum über k mit der Basis

$$\begin{aligned} B_G &= \{x^\alpha \mid x^\alpha \notin \langle \text{LM}(I) \rangle\} \\ &= \{x^\alpha \mid x^\alpha \notin \langle \text{LM}(g_1), \dots, \text{LM}(g_s) \rangle\} \\ &= \{x^\alpha \mid \text{LM}(g_i) \nmid x^\alpha \text{ für alle } i = 1, \dots, s\}. \end{aligned}$$

Also, V_G ist die Menge aller Summen der Form

$$\sum_{x^\alpha \in B_G} c_\alpha x^\alpha,$$

wobei nur eine endliche Anzahl von c_α ungleich 0 ist.

Satz 2. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal und sei $G = \{g_1, \dots, g_s\}$ eine Gröbner Basis von I . Dann sind die additive Gruppe des Ringes $k[x_1, \dots, x_n]/I$ und die additive Gruppe des Raums V_G isomorph.

Beweis. Definieren wir eine Abbildung

$$\phi : k[x_1, \dots, x_n]/I \rightarrow V \tag{1}$$

mit der Regel

$$[f] \mapsto \text{Rest}_G(f).$$

Die Abbildung ϕ ist korrekt definiert: wenn $[f] = [g]$ ist, dann ist $f - g \in I$ und, nach der Folgerung, ist $\text{Rest}_G(f) = \text{Rest}_G(g)$. Mit Hilfe des Satzes 1 kann man zeigen, dass ϕ ein Isomorphismus ist.

Satz 3. Sei ϕ die Abbildung (1). Für alle $f, g \in k[x_1, \dots, x_n]$ gilt

$$\phi([f][g]) = \text{Rest}_G(\phi([f])\phi([g])).$$

Satz 4. Sei k ein algebraisch abgeschlossener Körper und sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal. Sei G eine Gröbner Basis für I bezüglich einer monomiale Ordnung auf $k[x_1, \dots, x_n]$. Die folgenden Behauptungen sind äquivalent.

- (1) Die Menge $\mathbf{V}(I)$ ist endlich.
- (2) Für alle $i = 1, \dots, n$ existiert eine natürliche Zahl $m_i \geq 0$ mit $x_i^{m_i} \in \langle \text{LM}(I) \rangle$.
- (3) Für alle $i = 1, \dots, n$ existieren $m_i \geq 0$ und $g_i \in G$ mit $x_i^{m_i} = \text{LM}(g_i)$.
- (4) Der Vektorraum V_G hat eine endliche Dimension.
- (5) Der Vektorraum $k[x_1, \dots, x_n]/I$ hat eine endliche Dimension.

Satz 5. Sei k ein algebraisch abgeschlossener Körper und sei \succ eine monomiale Ordnung auf $k[x_1, \dots, x_n]$. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal mit der Bedingung:

$$\text{für alle } i = 1, \dots, n \text{ existiert } m_i \geq 0 \text{ mit } x_i^{m_i} \in \langle \text{LM}(I) \rangle.$$

Dann gilt

$$|\mathbf{V}(I)| \leq m_1 m_2 \dots m_s.$$

Satz 6. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal. Wenn $\mathbf{V}(I)$ endlich ist, dann gelten:

(1) $|\mathbf{V}(I)| \leq \dim(k[x_1, \dots, x_n]/I)$,

(2) $|\mathbf{V}(I)| = \dim(k[x_1, \dots, x_n]/I)$, wenn I ein radikale Ideal ist und k ein algebraisch abgeschlossener Körper ist.

Vorlesung 18

Der Koordinatenring der algebraischen Menge

Definition 1. Seien $V \subseteq k^m$ und $W \subseteq k^n$ zwei algebraische Mengen. Eine Abbildung $\phi : V \rightarrow W$ heißt *polynomial*, wenn Polynome $f_1, \dots, f_n \in k[x_1, \dots, x_m]$ existieren, so dass für alle $(a_1, \dots, a_m) \in V$ gilt

$$\phi(a_1, \dots, a_m) = (f_1(a_1, \dots, a_m), \dots, f_n(a_1, \dots, a_m)).$$

Im einfachen Fall $n = 1$, $W = k$ erhalten wir folgende Definition.

Definition 2. Sei $V \subseteq k^m$ eine algebraische Menge. Eine Funktion $\phi : V \rightarrow k$ heißt *polynomial*, wenn ein Polynom $f \in k[x_1, \dots, x_m]$ existiert, so dass für alle $(a_1, \dots, a_m) \in V$ gilt

$$\phi(a_1, \dots, a_m) = f(a_1, \dots, a_m).$$

In dem Fall sagen wir, dass das Polynom f die Funktion ϕ *repräsentiert*. Verschiedene Polynome können dieselbe Funktion repräsentieren.

Behauptung. Sei $\phi : V \rightarrow k$ eine polynomiale Funktion und sei f ein Polynom, das ϕ repräsentiert. Ein Polynom g repräsentiert ϕ nur dann, wenn $g - f \in \mathbf{I}(V)$ gilt.

Definition – Lemma. Sei $V \subseteq k^m$ eine algebraische Menge. Bezeichnen wir als $k[V]$ die Menge aller polynomialen Funktionen $\phi : V \rightarrow k$. Natürlicherweise definiert man die Addition und die Multiplikation zweier polynomialer Funktionen. Dann ist $k[V]$ ein kommutativer Ring mit 1. Der Ring $k[V]$ heißt *Koordinatenring* von V .

Satz 1. Die Ringe $k[V]$ und $k[x_1, \dots, x_n]/\mathbf{I}(V)$ sind isomorph und der Isomorphismus operiert auf k identisch.

Definieren wir polynomiale Funktionen $[x_i] : V \rightarrow k$ mit der Regel $[x_i](a_1, \dots, a_m) = a_i$. Nach dem Satz ist jede polynomiale Funktion $\phi : V \rightarrow k$ ein Polynom von $[x_1], \dots, [x_n]$.

Definition 3. Zwei algebraische Mengen $V \subseteq k^m$ und $W \subseteq k^n$ heißen *isomorph*, wenn zwei polynomiale Abbildungen $\alpha : V \rightarrow W$ und $\beta : W \rightarrow V$ existieren, so dass $\alpha \circ \beta = id_W$ und $\beta \circ \alpha = id_V$ gelten.

Definition 4. Sei $V \subseteq k^m$ eine algebraische Menge und sei c ein Element aus k . Eine konstante Funktion $\phi_c : V \rightarrow k$ ist mit der Regel $\phi_c(a_1, \dots, a_m) = c$ für alle $(a_1, \dots, a_m) \in V$ definiert.

Dann können wir eine natürliche Einbettung $k \subseteq k[V]$ mit der Regel $c \mapsto \phi_c$ ($c \in k$) definieren.

Satz¹ 2. Seien $V \subseteq k^m$ und $W \subseteq k^n$ zwei algebraischen Mengen.

(1) Sei $\alpha : V \rightarrow W$ eine polynomiale Abbildung. Wenn $\phi : W \rightarrow k$ eine polynomiale Funktion ist, dann ist $\phi \circ \alpha : V \rightarrow k$ es auch. Definieren wir eine Abbildung

$$\alpha^* : k[W] \rightarrow k[V]$$

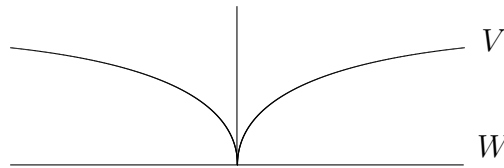
¹Der Satz ist ohne Beweis gegeben.

mit der Regel $\phi \mapsto \phi \circ \alpha$, $\phi \in k[V]$. Diese Abbildung α^* ist ein Ringhomomorphismus, so dass $\alpha^*(c) = c$ für alle $c \in k$ gilt.

(2) Sei $f : k[W] \rightarrow k[V]$ ein Ringisomorphismus, so dass $f|_k = id$ ist. Dann existiert eine einzige polynomiale Abbildung $\alpha : V \rightarrow W$, so dass $\alpha^* = f$ gilt.

Satz² 3. Zwei algebraische Mengen $V \subseteq k^m$ und $W \subseteq k^n$ sind isomorph, wenn ein Ringisomorphismus $f : k[V] \rightarrow k[W]$ mit $f|_k = id$ existiert.

Beispiel. Die algebraischen Mengen $V = \mathbf{V}(y^5 - x^2) \subseteq \mathbb{R}^2$ und $W = \mathbb{R}^1 \subseteq \mathbb{R}^1$ sind nicht isomorph.



Beweis. Merken wir an, dass $W = \mathbf{V}(\{0\}) = \mathbb{R}^1$ ist. Nehmen wir an, dass die algebraischen Mengen V und W isomorph sind. Dann sind ihre Koordinatenringe $\mathbb{R}[V]$ und $\mathbb{R}[W]$ isomorph. Genauer: es existiert ein Ringisomorphismus $f : \mathbb{R}[V] \rightarrow \mathbb{R}[W]$ mit $f|_{\mathbb{R}} = id$. Nach Satz 1 gelten:

$$\begin{aligned}\mathbb{R}[V] &\cong \mathbb{R}[x, y]/\langle y^5 - x^2 \rangle, \\ \mathbb{R}[W] &\cong \mathbb{R}[z]/\langle 0 \rangle,\end{aligned}$$

wobei die Begrenzungen beider Isomorphismen auf \mathbb{R} identisch sind. Deshalb existiert ein Ringisomorphismus

$$\phi : \mathbb{R}[x, y]/\langle y^5 - x^2 \rangle \rightarrow \mathbb{R}[z]$$

mit $\phi|_{\mathbb{R}} = id$. Bezeichnen wir $p(z) = \phi([x])$ und $q(z) = \phi([y])$. Da $[x^2] = [y^5]$ ist, ist $p^2(z) = q^5(z)$. Deshalb existiert ein Polynom $u(z) \in \mathbb{R}[z]$ mit $q(z) = u(z)^2$. Dann ist $p(z) = \pm u(z)^5$.

Jedes Element des Ringes $\mathbb{R}[x, y]/\langle y^5 - x^2 \rangle$ ist ein Polynom von $[x]$ und $[y]$. Deshalb ist jedes Element des Ringes $\mathbb{R}[z]$ ein Polynom von $p(z)$ und $q(z)$. Also ist z ein Polynom von $u(z)^2$ und $u(z)^5$, was unmöglich ist. Ein Widerspruch. Deshalb sind die algebraischen Mengen V und W nicht isomorph.

²Der Satz ist ohne Beweis gegeben.

Vorlesung 19-20

Rationale Funktionen auf algebraischen Mengen

Sei $V \subseteq k^n$ eine algebraische Menge. Seien $f, g \in k[x_1, \dots, x_n]$, so dass g nicht identisch 0 auf V ist. Dann ist die Funktion

$$\frac{f}{g} : V \setminus \mathbf{V}(g) \rightarrow k$$

definiert.

Definition 1. Eine beliebige Funktion $\Phi : U \rightarrow k$, wobei $\emptyset \neq U \subseteq V$ ist, heißt *rational auf V* , wenn zwei Polynome $f, g \in k[x_1, \dots, x_n]$ existieren, so dass $U = V \setminus \mathbf{V}(g)$ ist und $\Phi(u) = \frac{f}{g}(u)$ für alle $u \in U$ ist.

Diese Funktion wird auch als $\Phi : V- \rightarrow k$ bezeichnet. Die Bezeichnung widerspiegelt das Faktum, dass der Definitionsbereich von Φ kleiner sein kann als V . Wir werden sagen, dass Φ als $\frac{f}{g}$ repräsentiert ist.

Definition 2. Zwei rationale Funktionen $\Phi_1 : V- \rightarrow k$ und $\Phi_2 : V- \rightarrow k$ heißen *äquivalent* (man schreibt $\Phi_1 \sim \Phi_2$), wenn eine echte Untermenge $V' \subset V$ existiert, so dass Φ_1 und Φ_2 auf $V \setminus V'$ definiert sind und $\Phi_1(u) = \Phi_2(u)$ für alle $u \in V \setminus V'$ ist.

Lemma. Sei $V \subseteq k^n$ eine algebraische Menge. Die Menge V ist irreduzibel nur dann, wenn für alle zwei Polynome $g_1, g_2 \in k[x_1, \dots, x_n]$, die nicht identisch 0 auf V sind, folgt, dass ihr Produkt $g_1 g_2$ auch nicht identisch 0 auf V ist.

Satz. Sei V eine *irreduzible* algebraische Menge. Seien Φ_1, Φ_2 zwei rationale Funktionen auf V und sei $\frac{f_i}{g_i}$ ein Repräsentant von Φ_i ($i = 1, 2$). Dann gilt

$$\Phi_1 \sim \Phi_2 \iff f_1 g_2 - f_2 g_1 \in \mathbf{I}(V).$$

Beweis. \Rightarrow : Nehmen wir an $\Phi_1 \sim \Phi_2$. Dann existiert eine echte Untermenge $V' \subset V$, so dass $\Phi_1(u) = \Phi_2(u)$ für alle $u \in V \setminus V'$ gilt. Dann gilt $(f_1 g_2 - g_1 f_2)(u) = 0$ für alle $u \in V \setminus V'$. Daraus folgt

$$V = V' \cup (\mathbf{V}(f_1 g_2 - g_1 f_2) \cap V).$$

Da V' eine echte algebraische Untermenge der irreduziblen Menge V ist, gilt

$$\mathbf{V}(f_1 g_2 - g_1 f_2) \cap V = V,$$

also gilt $f_1 g_2 - f_2 g_1 \in \mathbf{I}(V)$.

\Leftarrow : Jetzt nehmen wir an, dass $f_1 g_2 - f_2 g_1 \in \mathbf{I}(V)$ gilt. Setzen wir $V' = (\mathbf{V}(g_1) \cap V) \cup (\mathbf{V}(g_2) \cap V)$. Dann ist V' die Vereinigung von zwei echten algebraischen Untermengen von V . Da V irreduzibel ist, ist V' auch eine echte algebraische Untermenge von V . Aus

der Voraussetzung $f_1g_2 - f_2g_1 \in \mathbf{I}(V)$ entspringt, dass $\Phi_1(u) = \Phi_2(u)$ für alle $u \in V \setminus V'$ ist. Also gilt $\Phi_1 \sim \Phi_2$.

Die Äquivalenzklasse einer rationalen Funktion Φ wird als $[\Phi]$ bezeichnet. Die Menge aller Äquivalenzklassen wird als $k(V)$ bezeichnet:

$$k(V) = \{[\Phi] \mid \Phi \text{ ist eine rationale Funktion auf } V\}.$$

Man kann die Äquivalenzklasse natürlicherweise addieren und multiplizieren.

Satz. Sei V eine irreduzible algebraische Menge. Dann ist $k(V)$ ein Körper.

Der Körper $k(V)$ heißt *Körper rationaler Funktionen auf V* .

Sei $V \subseteq k^n$ eine algebraische Menge. Durch $k[V]$ haben wir die Menge aller polynomi-
alen Funktionen $\phi : V \rightarrow k$ bezeichnet (siehe Vorlesung 18). Wir haben bewiesen, dass die
Ringe $k[V]$ und $k[x_1, \dots, x_n]/\mathbf{I}(V)$ isomorph sind. Wenn f ein Polynom in $k[x_1, \dots, x_n]$
ist, bezeichnen wir als $[f]$ seine Klasse in dem Faktor-Ring $k[x_1, \dots, x_n]/\mathbf{I}(V)$.

Satz. Es gilt $k(V) \cong \{[f]/[g] \mid f, g \in k[x_1, \dots, x_n], g \notin \mathbf{I}(V)\}$. Der Isomorphismus ist
nach der Regel gegeben:

$$[\Phi] \rightarrow [f]/[g],$$

wobei f/g ein Repräsentant von Φ ist.

Beispiel. Sei $V = \mathbf{V}(y^5 - x^2) \subseteq \mathbb{R}^2$ und $W = \mathbb{R}^1 = \mathbf{V}(\{0\}) \subseteq \mathbb{R}^1$. Dann sind V und
 W irreduzible algebraische Mengen. Außerdem ist $\mathbb{R}(V) \cong \mathbb{R}(W)$.

Hinweis. Die Menge V hat die polynomiale Parameterdarstellung $(x, y) = (t^5, t^2)$,
 $t \in \mathbb{R}$. Deshalb ist V irreduzibel. Offenbar ist W auch irreduzibel. Man kann beweisen,
dass $\mathbf{I}(V) = \langle y^5 - x^2 \rangle$ und $\mathbf{I}(W) = \{0\}$ ist. Deshalb gelten

$$\mathbb{R}[V] \cong \mathbb{R}[x, y]/\langle y^5 - x^2 \rangle \quad \text{und} \quad \mathbb{R}[W] \cong \mathbb{R}[z].$$

Man kann beweisen, dass

$$k(V) \cong \mathbb{R}(y) + x\mathbb{R}(y) \quad \text{und} \quad \mathbb{R}(W) \cong \mathbb{R}(z)$$

ist, wobei die Multiplikation in dem Körper $\mathbb{R}(y) + x\mathbb{R}(y)$ nach der folgenden Regel gegeben
ist:

$$(a(y) + xb(y))(c(y) + xd(y)) = (ac + y^5bd) + x(ad + bc).$$

Betrachten wir folgende Abbildungen zwischen den algebraischen Mengen V und W :

$$\alpha : V \rightarrow W, \quad (x, y) \mapsto x/y^2$$

und

$$\beta : W \rightarrow V, \quad z \mapsto (z^5, z^2).$$

Die Abbildungen induzieren folgende Abbildungen zwischen ihren Körpern rationaler
Funktionen $\mathbb{R}(V)$ und $\mathbb{R}(W)$:

$$\alpha^* : \mathbb{R}(W) \rightarrow \mathbb{R}(V), \quad f(z) \mapsto f(x/y^2)$$

und

$$\beta^* : \mathbb{R}(V) \rightarrow \mathbb{R}(W), \quad g(x, y) \mapsto g(z^5, z^2).$$

Man kann nachprüfen, dass $\alpha^* \circ \beta^*$ und $\beta^* \circ \alpha^*$ identische Abbildungen sind. Deshalb
sind die Körper $\mathbb{R}(V)$ und $\mathbb{R}(W)$ isomorph.

Vorlesung 21

Birationale Äquivalenz von algebraischen Mengen

Definition 1. Seien $V \subseteq k^m$ und $W \subseteq k^n$ zwei irreduzible algebraische Mengen. Eine *rationale Abbildung* von V nach W ist eine Abbildung der Form

$$\phi(x_1, \dots, x_m) = \left(\frac{f_1(x_1, \dots, x_m)}{g_1(x_1, \dots, x_m)}, \dots, \frac{f_r(x_1, \dots, x_m)}{g_r(x_1, \dots, x_m)} \right),$$

wobei $f_i/g_i \in k(x_1, \dots, x_m)$ ist und folgende Bedingungen gelten:

- (1) ϕ ist mindestens in einem Punkt von V definiert;
- (2) Wenn ϕ in einem Punkt (a_1, \dots, a_m) von V definiert ist, dann liegt $\phi(a_1, \dots, a_m)$ in W

Definition 2. Zwei irreduzible algebraische Mengen $V \subseteq k^m$ und $W \subseteq k^n$ heißen *birational-äquivalent*, wenn rationale Abbildungen $\phi : V \rightarrow W$ und $\psi : W \rightarrow V$ existieren, so dass

- (1) es existiert eine echte algebraische Untermenge $W' \subseteq W$, so dass $\phi \circ \psi$ identisch auf $W \setminus W'$ ist;
- (2) es existiert eine echte algebraische Untermenge $V' \subseteq V$, so dass $\psi \circ \phi$ identisch auf $V \setminus V'$ ist.

Beispiel. 1) Die algebraischen Mengen $V = \mathbf{V}(y^5 - x^2) \subseteq \mathbb{R}^2$ und $W = \mathbb{R}^1 = \mathbf{V}(\{0\}) \subseteq \mathbb{R}^1$ sind birational-äquivalent.

2) Die algebraischen Mengen $\mathbf{V}(x^2 + y^2 - z^2 - 1) \subseteq \mathbb{R}^3$ und $W = \mathbb{R}^2 \subseteq \mathbb{R}^2$ sind birational-äquivalent.

Satz³ 1. Zwei irreduzible algebraische Mengen V und W sind birational-äquivalent nur dann, wenn ein Isomorphismus $\alpha : k(V) \rightarrow k(W)$ existiert, so dass $\alpha|_k = id$ ist.

³Der Satz ist ohne Beweis gegeben.

Vorlesung 22

Invarianten-Theorie

Definition 1. Sei G eine endliche Untergruppe von $\mathrm{GL}_n(k)$. Ein Polynom $f \in k[x_1, \dots, x_n]$ heißt G -invariant, wenn $f(X) = f(AX)$ für alle $A \in G$ ist. Alle G -invariante Polynome bilden einen Unterring in $k[x_1, \dots, x_n]$. Der Unterring wird als $k[x_1, \dots, x_n]^G$ bezeichnet.

Beispiel. Sei $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Dann hat die Gruppe $G = \langle A \rangle$ die Ordnung 4. Es ist leicht zu beweisen, dass die Polynome $f_1 = x^2 + y^2$, $f_2 = x^3y - xy^3$ und $f_3 = x^2y^2$ G -invariant sind. Und es ist schwer zu beweisen, dass $k[x, y]^G = k[f_1, f_2, f_3]$ ist.

Definition 2. Sei G eine endliche Untergruppe von $\mathrm{GL}_n(k)$. *Reynolds-Operator* $R_G : k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]$ definiert man mit der Formel

$$R_G(f)(X) = \frac{1}{|G|} \sum_{A \in G} f(AX).$$

Lemma. Sei G eine endliche Untergruppe von $\mathrm{GL}_n(k)$. Dann gelten:

- 1) R_G ist linear.
- 2) Für alle $f \in k[x_1, \dots, x_n]$ gilt $R_G(f) \in k[x_1, \dots, x_n]^G$.
- 3) Für alle $f \in k[x_1, \dots, x_n]^G$ gilt $R_G(f) = f$.

Satz (Emmy Nöther). Sei k ein Körper mit $\mathrm{char}(k) = 0$ und sei G eine endliche Untergruppe von $\mathrm{GL}_n(k)$. Dann gilt

$$k[x_1, \dots, x_n]^G = k[R_G(x^\beta) \mid |\beta| \leq |G|].$$

Satz. Seien $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ gegeben. Fixieren wir eine monomiale Ordnung, so dass $x_i \succ y_j$ für alle i, j gilt. Sei S eine Gröbner Basis von Ideal $\langle f_1 - y_1, \dots, f_m - y_m \rangle \subseteq k[x_1, \dots, x_n, y_1, \dots, y_m]$.

Dann gelten für alle Polynome $f \in k[x_1, \dots, x_n]$:

- (1) $f \in k[f_1, \dots, f_m] \iff \mathrm{Rest}_S(f) \in k[y_1, \dots, y_m]$.
- (2) Wenn $f \in k[f_1, \dots, f_m]$ ist, dann ist $f = \mathrm{Rest}_S(f)(f_1, \dots, f_m)$.

Vorlesungen 23-24

Dimension der affinen algebraischen Menge

1. Für $J \subseteq \{1, \dots, n\}$ bezeichnen wir

$$H_J = \{(p_1, \dots, p_n) \in k^n \mid p_j = 0 \text{ für alle } j \in J\}.$$

Die Menge H_J ist ein Unterraum von k^n der Dimension $n - |J|$ und heißt *Koordinaten-Unterraum* von k^n .

Satz. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal. Dann ist $\mathbf{V}(I)$ eine endliche Vereinigung der Koordinaten-Unterräume von k^n .

Definition. Sei $V \subseteq k^n$ eine algebraische Menge, die eine endliche Vereinigung einiger Unterräume von k^n ist. Die *Dimension* von V ist maximum der Dimensionen dieser Unterräume.

Folgerung. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal. Dann ist

$$\dim \mathbf{V}(I) = \max\{\dim H_J \mid H_J \subseteq \mathbf{V}(I)\}.$$

2. Für $J \subseteq \{1, \dots, n\}$ bezeichnen wir

$$M_J = \{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \mid \alpha_j = 0 \text{ für alle } j \in J\}.$$

Die Menge M_J heißt *Koordinaten-Unterraum* von $\mathbb{Z}_{\geq 0}^n$ (obwohl M_J kein Vektorraum ist). Die *Dimension* von M_J ist (nach Definition) $n - |J|$ und wird als $\dim M_J$ bezeichnet.

Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal. Bezeichnen wir

$$C(I) = \{\alpha \in \mathbb{Z}_{\geq 0}^n \mid x^\alpha \notin I\}.$$

Satz. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal und sei $J \subseteq \{1, \dots, n\}$ eine Unter-
menge. Dann sind die folgenden Bedingungen äquivalent:

- (a) Der Koordinaten-Unterraum H_J liegt in $\mathbf{V}(I)$.
- (b) Der Koordinaten-Unterraum M_J liegt in $C(I)$.

Folgerung. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal. Dann ist

$$\begin{aligned} \dim \mathbf{V}(I) &= \max\{\dim H_J \mid H_J \subseteq \mathbf{V}(I)\} \\ &= \max\{\dim M_J \mid M_J \subseteq C(I)\}. \end{aligned}$$

Satz. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal mit $\dim \mathbf{V}(I) = d$. Dann ist die Funktion $f(s) = |\{x^\alpha \notin I : |\alpha| \leq s\}|$ ein Polynom von s des Grades d für alle groß genug s .

3. Sei M eine Untermenge von $k[x_1, \dots, x_n]$. Bezeichnen wir als $M_{\leq s}$ die Menge aller Polynome von M des totalen Grades $\leq s$.

Definition. Sei $I \subseteq k[x_1, \dots, x_n]$ ein beliebiges Ideal. *Hilbertsche Funktion von I* ist die Funktion $HF_I : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$, die so definiert ist:

$$\begin{aligned} HF_I(s) &= \dim(k[x_1, \dots, x_n]_{\leq s} / I_{\leq s}) \\ &= \dim k[x_1, \dots, x_n]_{\leq s} - \dim I_{\leq s}. \end{aligned}$$

Satz. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal. Dann gilt

$$HF_I(s) = |\{x^\alpha \notin I : |\alpha| \leq s\}|$$

für alle $s \geq 0$.

Folgerung. Sei $I \subseteq k[x_1, \dots, x_n]$ ein monomiales Ideal. Dann ist $HF_I(s)$ ein Polynom von s für alle groß genug s .

Satz. Sei $I \subseteq k[x_1, \dots, x_n]$ ein beliebiges Ideal. Dann gilt

$$HF_I(s) = HF_{\langle \text{LM}(I) \rangle}(s),$$

wobei $\text{LM}(I)$ die Menge aller leitenden Monome von I bezüglich \succ_{grlex} -Ordnung ist.

Folgerung – Definition. Sei $I \subseteq k[x_1, \dots, x_n]$ ein beliebiges Ideal. Dann ist $HF_I(s)$ ein Polynom von s für alle groß genug s . Dieses Polynom heißt *Hilbertsches Polynom* von I und wird als $HP_I(s)$ bezeichnet.

4. Definition. Die *Dimension der algebraischen Menge* $V \subseteq k^n$ ist der Grad des Hilbertschen Polynoms $HP_I(s)$, wobei $I = \mathbf{I}(V)$ ist.

Satz. Sei $I \subseteq k[x_1, \dots, x_n]$ ein beliebiges Ideal. Dann haben die Hilbertschen Polynome von I und \sqrt{I} den gleichen Grad.

Dimension-Satz. Sei k ein algebraisch abgeschlossener Körper und sei $\mathbf{V}(I) \subseteq k^n$ eine algebraische Menge. Dann ist

$$\dim \mathbf{V}(I) = \text{Grad } HP_I.$$

Vorlesung 25

Dimension und algebraische Unabhängigkeit

Erst erinnern wir uns an die Definition des Koordinatenrings. Sei $V \subseteq k^n$ eine algebraische Menge. Eine Funktion $\phi : V \rightarrow k$ heißt *polynomial*, wenn ein Polynom $f \in k[x_1, \dots, x_n]$ existiert, so dass für alle $(a_1, \dots, a_n) \in V$ gilt

$$\phi(a_1, \dots, a_n) = f(a_1, \dots, a_n).$$

Bezeichnen wir als $k[V]$ die Menge aller polynomialen Funktionen $\phi : V \rightarrow k$. Natürlicherweise definiert man die Addition und die Multiplikation zweier polynomialer Funktionen. Dann ist $k[V]$ ein kommutativer Ring mit 1. Der Ring $k[V]$ heißt *Koordinatenring* von V . Nach dem Satz 1 aus der Vorlesung 18 gilt

$$k[V] \cong k[x_1, \dots, x_n]/\mathbf{I}(V), \quad (1)$$

wobei der Isomorphismus auf k identisch ist.

1. Behauptung. Für alle natürlichen Zahlen s hat der kanonische Homomorphismus $k[x_1, \dots, x_n]_{\leq s} \rightarrow k[x_1, \dots, x_n]/\mathbf{I}(V)$ den Kern $\mathbf{I}(V)_{\leq s}$, und angesichts von (1) induziert er eine Einbettung

$$k[x_1, \dots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s} \rightarrow k[V].$$

Identifizieren wir den Ring $k[x_1, \dots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s}$ mit seinem Bild in $k[V]$. Dann haben wir eine wachsende Kette der Ringe

$$k[x_1, \dots, x_n]_{\leq 1}/\mathbf{I}(V)_{\leq 1} \subseteq k[x_1, \dots, x_n]_{\leq 2}/\mathbf{I}(V)_{\leq 2} \subseteq \dots,$$

die $k[V]$ erschöpft. In diesem Sinn approximieren die Ringe $k[x_1, \dots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s}$ den Koordinatenring $k[V]$. Deshalb widerspiegelt die Dimension von $\mathbf{I}(V)$ (siehe Punkt 3 und Definition 4 der Vorlesung 24) die Geschwindigkeit des Wachstums von $k[V]$

2. Definition. Seien $\varphi_1, \dots, \varphi_r \in k[V]$. Die Funktionen $\varphi_1, \dots, \varphi_r$ sind *algebraisch unabhängig* über k , wenn $p(\varphi_1, \dots, \varphi_r) \neq 0$ in $k[V]$ für alle nichtnullischen Polynome $p \in k[y_1, \dots, y_r]$ ist.

3. Satz. Sei $V \subseteq k^n$ eine algebraische Menge. Dann ist die Dimension von V gleich der maximalen Anzahl der algebraisch unabhängigen Elemente von $k[V]$.

4. Folgerung. Seien V und V' zwei algebraischen Mengen, die isomorph (oder sogar bi-rational äquivalent) sind. Dann gilt $\dim(V) = \dim(V')$.

5. Satz. Sei $V \subseteq k^n$ eine algebraische Menge. Dann ist die Dimension von V gleich der maximalen r , so dass r Unbekannte x_{i_1}, \dots, x_{i_r} mit $\mathbf{I}(V) \cap k[x_{i_1}, \dots, x_{i_r}] = \{0\}$ existieren.

Bibliographie

1. D. Cox, J. Little, D. O'shea, *Ideals, Varieties, and Algorithms*, Springer, 1997.