

TEIL 1. ALGORITHMISCHE ALGEBRA

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) $\mathbf{V}(x^2 + y^2 - 1)$ ist ein Kreis.

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

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

4) $\mathbf{V}(x^2 - y^2z^2 + z^3)$.

5) $\mathbf{V}(y - x^2, z - x^3)$.

6) $\mathbf{V}(xz, yz)$ 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

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

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 $g \neq \mathbf{0}$ 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 $\mathbf{V}(x^2 - y^2 z^2 + z^3)$ 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 $V = \mathbf{V}(f_1, \dots, f_s)$ 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 $\mathbf{V}(f_1, \dots, f_s) = \mathbf{V}(g_1, \dots, g_s)$. Also, jedes Ideal definiert eindeutig eine algebraische Menge.

Lemma–Definition. 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* .

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

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

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

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) $U = W \Leftrightarrow \mathbf{I}(U) = \mathbf{I}(W)$.

Beweis. Wir beweisen nur die Implikation \Leftarrow in 1). Nehmen wir an $\mathbf{I}(W) \subseteq \mathbf{I}(U)$. Sei $W = \mathbf{V}(\mathcal{F})$. Dann gilt $\mathcal{F} \in \mathbf{I}(W) \subseteq \mathbf{I}(U)$. Deshalb annulliert \mathcal{F} die Menge U . Aus $W = \mathbf{V}(\mathcal{F})$ folgt, dass W die größte Menge ist, die von \mathcal{F} annulliert ist. Deshalb ist $U \subseteq W$.

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 $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ 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 \succcurlyeq 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 $m_1 \succcurlyeq m_2$ oder $m_2 \succcurlyeq m_1$ gilt.
2. $m \succcurlyeq m$.
3. $(m_1 \succcurlyeq m_2 \ \& \ m_2 \succcurlyeq m_1) \Rightarrow (m_1 = m_2)$.
4. $(m_1 \succcurlyeq m_2 \ \& \ m_2 \succcurlyeq m_3) \Rightarrow (m_1 \succcurlyeq m_3)$.
5. $m_1 \succcurlyeq m_2 \Rightarrow m_1 m \succcurlyeq m_2 m$ für alle $m \in \mathcal{M}$.
6. $m \succcurlyeq 1$ für alle $m \in \mathcal{M}$.
7. Für jede Untermenge $S \subseteq \mathcal{M}$ existiert ein Monom $\tilde{m} \in S$, so dass $m \succcurlyeq \tilde{m}$ für alle $m \in S$ ist.

Wir werden schreiben $m_1 \succ m_2$, wenn $m_1 \succcurlyeq m_2$ 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 nichtnullsche 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:*

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

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* . Man schreibt $r = \text{Rest}_F(f)$.

Beispiel 1. Seien $f = x^2 y + x y^2 + y^2$, $F = (f_1, f_2)$, $f_1 = x y - 1$, $f_2 = y^2 - 1$. Wir werden lexikographische Ordnung auf der Menge \mathcal{M} aller Monome aus $k[x, y]$ benutzen, wobei $x \underset{\text{lex}}{\succ} y$ 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:

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

Daraus folgt

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

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:

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

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

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 $X \subseteq k[x_1, \dots, x_m]$ 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. Beweisen wir die Einzigkeit. Nehmen wir an, dass $f = h_1 + r_1 = h_2 + r_2$ mit $r_1 \neq r_2$ 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. Also ist $\text{LM}(r_1 - r_2) \subseteq (\text{Monome von } r_1) \cup (\text{Monome von } r_2)$. Ein Widerspruch.

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 $\text{LM}(S(f, g)) \prec x^\gamma$.
 2) Das Polynom $S(f, g)$ liegt in dem Ideal $\langle f, g \rangle$.

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

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

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 leitendes Monom x^δ haben. Wenn $\text{LM}(\sum_{i=1}^s f_i) \prec x^\delta$ ist, dann ist $\sum_{i=1}^s f_i$ eine lineare Kombination von $S(f_i, f_j)$ mit Koeffizienten aus k . Außerdem ist $\text{LM}(S(f_i, f_j)) \prec x^\delta$.

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

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

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 $m(i) = \text{LM}(h_i g_i)$ und $m = \max m(i)$. Dann ist es klar, dass $\text{LM}(f) \preceq m$ ist.

Fall 1: $\text{LM}(f) = m$. Dann existiert i_0 , so dass $\text{LM}(f) = \text{LM}(h_{i_0} g_{i_0})$ 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.

Fall 2: $\text{LM}(f) \prec m$. 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 $\text{LM}(h'_i g_i) \prec m$ gilt ($i = 1, \dots, s$).

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

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

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

Weiterhin sind folgende Punkte wichtig.

- Das leitende Monom von $S(\text{LMG}(h_i)g_i, \text{LMG}(h_j)g_j)$ ist kleiner als m (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 leitenden Monome von $p_k g_k$ nicht größer sind als die leitenden Monome 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 die leitende Monome von $r_k g_k$ kleiner sind als m . Wie wir schon bemerkt haben, sind die leitenden Monome aller Mitglieder in den letzten zwei Summen kleiner als m .

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

Vorlesungen 5

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 angehalten 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 $m \neq \text{LM}(p)$ 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) $g'_1 \in I$.
- 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 $g - \tilde{g} = 0$.

Vorlesung 6

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

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 $I \cap J$.

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

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

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 $\mathbf{Res}(f, g; x) = y^4 - 4y^2 + 1$,

$$-(yx + 1)f + y^2g = \mathbf{Res}(f, g; x).$$

Lemma 6. Seien $f, g \in k[x_1, \dots, x_n] \setminus k$. Die folgenden Aussagen sind äquivalent.

- (1) f, g haben einen gemeinsamen Faktor in $k[x_1, \dots, x_n]$, und der Faktor enthält x_1 .
- (2) f, g haben einen gemeinsamen Faktor in $k(x_1, \dots, x_{n-1})[x_n]$, und der Faktor enthält x_1 .

Satz 7. 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) $\mathbf{Res}(f, g; x_1) = 0$.

Vorlesung 8

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

Satz 1 (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 2. 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.

Satz 3 (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 4 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 4. Sei $I = \langle f_1, f_2, \dots, f_s \rangle$ ein Ideal in $k[x_1, \dots, x_n]$. Dann liegen alle verallgemeinerten Resultanten von f_1, f_2, \dots, f_n in dem ersten Eliminationsideal I_1 .

Satz 5 (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

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

Eine Skizze des Beweises. Setzen wir $c = (c_1, \dots, c_n)$. Wir suchen eine gemeinsame Nullstelle c_1 von $f_1(x_1, c), \dots, f_s(x_1, c)$. Der Satz ist trivial $s = 1$ und wir haben ihn für $s = 2$ bewiesen. Also, sei $s \geq 3$. O.B.d.A. können wir annehmen, dass $g_1(c) \neq 0$ ist. Schreiben wir auf

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

Nach Lemma 2 ist $h_{\alpha} \in I_1$ für alle α . Da $(c_2, \dots, c_n) \in \mathbf{V}(I_1)$ ist, haben wir $h_{\alpha}(c_2, \dots, c_n) = 0$ für alle α , und so haben wir

$$\mathbf{Res}(f_1, u_2 f_2 + \dots + u_s f_s; x_1) \Big|_{\substack{(x_2, \dots, x_n) \\ = (c_2, \dots, c_n)}} = 0.$$

Jetzt können wir annehmen, dass $g_2(c) \neq 0$ ist und $\text{Grad}_{x_1}(f_2) > \text{Grad}_{x_1}(f_i)$ für $i \geq 3$ ist. Dann ist $\text{Grad}_{x_1}(u_2 f_2 + \dots + u_s f_s) = \text{Grad}_{x_1}(u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c))$.

Da $g_1(c) \neq 0$ ist, ist auch $\text{Grad}_{x_1}(f_1) = \text{Grad}_{x_1}(f_1(x_1, c))$. Deswegen gilt

$$\mathbf{Res}(f_1, u_2 f_2 + \dots + u_s f_s; x_1) \Big|_{\substack{(x_2, \dots, x_n) \\ = (c_2, \dots, c_n)}} = \mathbf{Res}(f_1(x_1, c), u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c); x_1) = 0.$$

Nach Lemma 1 haben $f_1(x_1, c)$ und $u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c)$ einen gemeinsamen Faktor in $k[x_1, u_2, \dots, u_s]$. Es ist klar, dass der Faktor nur von x_1 abhängt. Daraus folgt, dass er ein Teiler aller $f_i(x_1, c)$ ist. Also haben f_1, \dots, f_s eine gemeinsame Nullstelle $c_1 \in k$.

Vorlesung 9

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 nichtnullsches 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 $I \subseteq k[x_1, \dots, x_n]$ 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 nichtnullschische Polynome sind. Wir können annehmen, dass f_1 keine Konstant ist, sonst ist $I = k[x_1, \dots, x_k]$ 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:

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

wobei $g(a_2, \dots, a_n)$ ein Polynom von a_2, \dots, a_n ist. Jetzt wählen wir a_2, \dots, a_n so, dass $g(a_2, \dots, a_n) \neq 0$ 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 $g(a_2, \dots, a_n) \neq 0$ 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 10

Algebraische Mengen und radikale Ideale 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) $I \subseteq \mathbf{I}(\mathbf{V}(I))$,
- (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:

$$\begin{array}{ccc} & \mathbf{I} & \\ & \xrightarrow{\quad} & \\ \text{algebraische Mengen} & & \text{radikale Ideale.} \\ & \mathbf{V} & \\ & \xleftarrow{\quad} & \end{array}$$

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 $W \subsetneq \mathbf{V}(I)$, 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 $f \in k[x_{l+1}, \dots, x_n] \subseteq k[x_1, \dots, x_n]$ und $f(c_1, \dots, c_n) = 0$ für alle $(c_1, \dots, c_n) \in \mathbf{V}(I)$ ist.

Die letzte Bedingungen schreiben wir als $f \in k[x_{l+1}, \dots, x_n]$ und $f \in \mathbf{I}(\mathbf{V}(I))$ auf.

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 11

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:

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

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:

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

Zerlegung von algebraischen Mengen in irreduzible algebraische Mengen.

Zerlegung von radikalen Idealen in Primideale

Lemma. Sei $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ eine wachsende Kette von Idealen in $k[x_1, \dots, x_n]$. Dann existiert eine natürliche N , so dass gilt $I_N = I_{N+1} = \dots$.

Lemma. 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 existiert eine Zerlegung von V in irreduzible Mengen:

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

so dass $V_i \not\subseteq V_j$ für $i \neq j$ gilt. Die Menge solcher irreduziblen Mengen ist einzig.

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.

TEIL 2. ALGORITHMISCHE GRUPPENTHEORIE

Vorlesung 12

Eine Konstruktion der freien Gruppe

12.1. Definition. Eine Gruppe F heißt *frei*, wenn sie eine Teilmenge X hat, so dass jedes Element $f \in F$ auf genau eine Weise in der Form $f = x_1 x_2 \dots x_n$ geschrieben werden kann, wobei $x_i \in X^\pm$ und $x_i x_{i+1} \neq 1$ für alle i ist. Diese Form heißt *irreduzibel*. Die Menge X heißt *Basis* von F .

Die *Länge* von $f \in F$ bezüglich X ist n und wird als $|f|$ bezeichnet.

12.2. Satz. Für jede Menge X existiert eine freie Gruppe mit der Basis X . Alle freien Gruppen mit der Basis X sind isomorph. (Wir bezeichnen eine als $F(X)$.)

12.3. Satz. Eine Gruppe F ist frei mit der Basis X nur dann, wenn für jede Gruppe G und jede Abbildung $X \xrightarrow{\phi} G$ ein einziges Homomorphismus $F \xrightarrow{\phi^*} G$ mit $\phi^*|_X = \phi$ existiert.

12.4. Satz. Alle Basen einer freien Gruppe haben dieselbe Kapazität.

Diese Kapazität heißt *Rang* der freien Gruppe.

12.5. Behauptung. Sei (u, v) eine Basis der freien Gruppe F . Dann gelten:

- 1) (u, vu^ε) und $(u, u^\varepsilon v)$, $\varepsilon = \pm 1$, die Basen von F sind,
- 2) (v, u) ist eine Basis von F ,
- 3) (u, v^{-1}) ist eine Basis von F .

12.6. Frage. Wie kann man algorithmisch erkennen, ob eine Untermenge U von freien Gruppe $F(X)$ eine Basis von $F(X)$ ist?

Vorlesung 13

Nielsen-Methode

13.1. Sei $U = (u_1, \dots, u_m)$ ein Tupel der Elemente aus einer freien Gruppe $F(X)$.

Nielsen-Transformationen sind:

- (T1) ein u_i nach u_i^{-1} ersetzen,
- (T2) ein u_i nach $u_i u_j$ ersetzen, wobei $i \neq j$ ist,
- (T3) u_i ausstreichen, wenn $u_i = 1$ ist.

U heißt *Nielsen-irreduzibel*, wenn für alle $v_1, v_2, v_3 \in U^\pm$ gilt

- (N1) $v_1 \neq 1$,
- (N2) aus $v_1 v_2 \neq 1$ folgt $|v_1 v_2| \geq |v_1|, |v_2|$,
- (N3) aus $v_1 v_2 \neq 1$ und $v_2 v_3 \neq 1$ folgt $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

13.2. Behauptung. Transformieren wir ein Tupel U an ein anderes Tupel U' . Dann gilt $\langle U \rangle = \langle U' \rangle$.

13.3. Behauptung. Sei $U_{Nirr} = (u_1, \dots, u_m)$ ein Nielsen-irreduzibles Tupel in $F(X)$. Sei $v = v_1 v_2 \dots v_k$ ein Produkt, wobei $k \geq 0$, $v_i \in U_{Nirr}^\pm$ und $v_i v_{i+1} \neq 1$ ist. Dann ist $|v| \geq k$. Insbesondere, ist $\langle U_{Nirr} \rangle$ eine freie Gruppe mit der Basis U_{Nirr} .

13.4. Satz. Man kann jedes Tupel $U = (u_1, \dots, u_m)$ der Elemente einer freien Gruppe F nach ein Nielsen-irreduzibles Tupel U_{Nirr} mit Hilfe der Nielsen-Transformationen transformieren.

13.5. Folgerung. Die Gruppe $\langle U \rangle$ ist frei mit der Basis $\langle U_{Nirr} \rangle$. Insbesondere, jede endlich erzeugte Untergruppe einer freien Gruppe ist frei.

13.6. Folgerung. Ein Tupel $U \subseteq F(X)$ ist eine Basis von $F(X)$ nur dann, wenn $U_{Nirr} = X$ bis Inversionen in X .

Vorlesung 14

Fundamentale Gruppe eines Graphes. Stallings-Faltungen

14.1. Sei Γ ein zusammengehängender Graph. Seine Eckpunkte bezeichnen wir als Γ^0 , seine Kanten als Γ^1 . Der Anfang einer Kante e wird als $\alpha(e)$ bezeichnet, und das Ende als $\omega(e)$. Ein *Weg* in Γ ist eine endliche Folge der Kanten: $p = e_1 e_2 \dots p_k$, so dass $\alpha(e_{i+1}) = \omega(e_i)$ ist. Der Weg heißt *irreduzibel*, wenn $e_{i+1} \neq \bar{e}_i$ für alle i ist.

Fixieren wir ein Eckpunkt v in Γ . Sei $P(\Gamma, v)$ die Menge aller Wege in Γ mit Anfang und Ende v . Zwei Wege p_1 und p_2 heißen *homotop*, wenn man p_2 aus p_1 mit Hilfe der elementaren Transformationen bekommen kann, wobei eine elementare Transformation eine Einfügung oder eine Kürzung von $e\bar{e}$ ist. Die Homotopieklasse des Weges p wird als $[p]$ bezeichnet.

14.2. Lemma. In jede Homotopieklasse existiert genau ein irreduzibler Weg.

14.3. Satz-Definition. Die Menge $\pi_1(\Gamma, v) = \{[p] \mid p \in P(\Gamma, v)\}$ ist eine Gruppe bezüglich der Multiplikation $[p_1][p_2] = [p_1 p_2]$. Diese Gruppe heißt *fundamentale Gruppe* von Γ bezüglich v .

Sei v_1 ein anderer Eckpunkt von Γ . Dann sind die Gruppen $\pi_1(\Gamma, v)$ und $\pi_1(\Gamma, v_1)$ isomorph. In der Tat, sei q ein Weg in Γ von v nach v_1 . Dann ist die Abbildung $[p] \mapsto [q^{-1} p q]$ der gewünschte Isomorphismus.

Sei T ein maximaler Baum in Γ . Insbesondere $T^0 = \Gamma^0$. Orientieren wir $\Gamma^1 \setminus T^1$ und bezeichnen wir die Menge der orientierten Kanten als $(\Gamma^1 \setminus T^1)^+$.

Für jeden Eckpunkt $v \in \Gamma^0$ sei p_v ein irreduzibler Weg in T von x zu v . Für jede Kante $e \in \Gamma^1$ sei $p_e = p_{\alpha(e)} e p_{\omega(e)}^{-1}$.

14.4. Satz. Die fundamentale Gruppe eines zusammenhängenden Graphes Γ ist frei. Mit der oberen Bezeichnungen ist die Basis von $\pi_1(\Gamma, v)$

$$\{[p_{\alpha(e)} e p_{\omega(e)}^{-1}] \mid e \in (\Gamma^1 \setminus T^1)^+\}.$$

14.5. Definition. Sei Γ ein zusammenhängender Graph und sei X eine Untermenge einer Gruppe G . Eine X -Markierung von Γ ist eine Abbildung $\varphi : \Gamma^1 \rightarrow X^\pm$, so dass $\varphi(e^{-1}) = \varphi(e)^{-1}$ für alle $e \in \Gamma^1$ ist. Der Graph Γ mit der X -Markierung heißt X -Graph.

Für einen Weg $p = e_1 e_2 \dots e_m$ in Γ definieren wir seine Markierung $\varphi(p)$ mit der Formel $\varphi(p) = \varphi(e_1)\varphi(e_2)\dots\varphi(e_m)$. Dann ist die Abbildung

$$\phi_* : \pi_1(\Gamma, v) \rightarrow G,$$

$$[p] \mapsto \varphi(p)$$

ein Homomorphismus.

14.6. Definition. Sei Γ ein X -Graph. Wenn zwei verschiedene Kanten e_1, e_2 einen gleichen Anfang und eine gleiche Markierung x haben, falten wir die zwei Kanten in eine neue Kante e mit der Markierung x . Den neuen X -Graph bezeichnen wir als Γ' und sagen, dass Γ nach Γ' gefaltet ist.

14.7. Satz. Sei Γ ein X -Graph, wobei X eine Untermenge einer Gruppe G ist.

(1) Wenn Γ nach Γ' gefaltet ist, dann sind die Bilder von ϕ_* und ϕ'_* gleich.

(2) Wenn Γ nicht weiter gefaltet werden kann, dann ist $\phi_* : \pi_1(\Gamma, v) \rightarrow F(X)$ ein Monomorphismus.

14.8. Satz-Folgerung. Sei $U = (u_1, \dots, u_m)$ ein Tupel der Elemente in der freien Gruppe $F(X)$.

(1) Es existiert ein X -Graph Γ (eine Rose), so dass das Bild von ϕ_* gleich $\langle U \rangle$ ist.

(2) Sei $\Gamma \succ \Gamma_1 \succ \Gamma_2 \succ \dots \succ \Gamma_n$ eine Faltungs-Reihe und Γ_n kann nicht weiter gefaltet werden. Dann ist $(\phi_n)_* : \pi_1(\Gamma_n, v) \rightarrow \langle U \rangle$ ein Isomorphismus.

Insbesondere ist die Gruppe $\langle U \rangle$ frei mit der Basis $(\phi_n)_*(S)$, wobei S eine Basis von $\pi_1(\Gamma_n, v)$ ist.

Vorlesung 15

Präsentationen der Gruppen. Tietze-Transformationen

Sei $R \subseteq F(X)$ eine Untermenge. Ein *normaler Abschluss* von R in $F(X)$ ist die Menge

$$R^{F(X)} = \left\{ \prod_{i=1}^k f_i^{-1} r_i^{\varepsilon_i} f_i \mid f_i \in F(X), r_i \in R, \varepsilon_i = \pm 1, k = 0, 1, \dots \right\}.$$

Es ist leicht zu verstehen, dass $R^{F(X)}$ eine normale Untergruppe von $F(X)$ ist. Außerdem ist $R^{F(X)}$ die kleinste normale Untergruppe von $F(X)$, die R enthält.

15.1. Lemma. Sei $r \in R$. Dann gilt $urv \in R^{F(X)} \Leftrightarrow uv \in R^{F(X)}$.

15.2. Definition. Sei G eine Gruppe. Dann existiert eine freie Gruppe $F(X)$ und ein Epimorphismus $\varphi : F(X) \rightarrow G$. Sei R eine beliebige Untermenge von $F(X)$, mit $R^{F(X)} = \text{Ker } \varphi$. Dann heißt $\langle X \mid R \rangle$ eine *Präsentation* von G . Diese Präsentation heißt *endlich*, wenn X und R endlich sind.

15.3. Beispiele. 1) S_3 hat die Präsentation $\langle x, y \mid x^2, y^2, (xy)^3 \rangle$.

2) \mathbb{Z}_3 hat folgende Präsentationen: $\langle x \mid x^3 \rangle$ und $\langle x, y \mid x^{-5}y^2, x^6y^{-3} \rangle$.

3) Sei G eine Untergruppe von $GL_2(\mathbb{Q})$, wobei $A = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ist. Dann hat G die Präsentation $\langle a, b \mid a^{-1}ba = b^n \rangle$.

4) Die Gruppe S_n hat die Präsentation

$$\langle t_1, t_2, \dots, t_{n-1} \mid t_i^2, t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}, t_i t_j = t_j t_i (|i - j| > 1) \rangle.$$

Eine Gruppe kann verschiedene Präsentationen haben. Aber von einer Präsentation zur anderen kann man mit Hilfe von Tietze – Transformationen gehen.

15.4. Definition.

(1) Tietze – Transformation der Type 1:

$$\langle X \mid R \rangle \rightarrow \langle X \mid R, r \rangle,$$

wobei $r \in R^{F(X)}$ ist.

(2) Tietze – Transformation der Type 2:

$$\langle X \mid R \rangle \rightarrow \langle X, y \mid R, y^{-1}w \rangle,$$

wobei $y \notin X^\pm$ und $w \in F(X)$ ist.

15.5. Satz. Seien $\langle X_1 \mid R_1 \rangle$ und $\langle X_2 \mid R_2 \rangle$ zwei endliche Präsentationen einer Gruppe G . Dann kann man die zweite Präsentation aus der ersten mit Hilfe endlicher Anwendungen der Tietze – Transformationen (1) und (2) und ihrer Inversen bekommen.

15.6. Beispiel.

1) $\langle x, y \mid xyx = yxy \rangle$ und $\langle a, b \mid a^2 = b^3 \rangle$ präsentieren dieselbe Gruppe.

2) $\langle a, b \mid a^{-1}b^2a = b^3, b^{-1}a^2b = a^3 \rangle$ und $\langle a, b \mid a, b \rangle$ sind zwei Präsentationen der trivialen Gruppe $\{1\}$.

Vorlesung 16

Schreier-Transversal. Reidemeister–Schreier–Methode

16.1. Definition. Sei H eine Untergruppe einer freien Gruppe $F(X)$. Eine Untergruppe $T \subseteq F(X)$ heißt *rechtes Schreier-Transversal* für H in $F(X)$, wenn

1) in jeder rechten Nebenklasse Hg genau ein Element aus T liegt;

in H das Element $1 \in T$ liegt;

2) für jedes $t = x_1 x_2 \dots x_m \in T$ Elemente $x_1 x_2 \dots x_i$ auch in T liegen, $i = 1, 2, \dots, m$.

Für $g \in F(X)$ bezeichnen wir als \bar{g} ein Element aus T mit $Hg = H\bar{g}$.

Für $t \in T$ und $x \in X \cup X^{-1}$ setzen wir $\gamma(t, x) = tx \cdot \overline{tx}^{-1}$.

16.2. Behauptung. Sei H eine Untergruppe einer freien Gruppe $F(X)$.

- 1) Es existiert ein rechtes Schreier-Transversal für H in $F(X)$.
- 2) Es gilt $\gamma(t, x) \in H$.
- 3) Es gilt $\gamma(t, x^{-1}) = \gamma(\overline{tx^{-1}}, x)^{-1}$.
- 4) Sei $w = x_1x_2 \dots x_n \in H$. Dann gilt

$$w = \gamma(1, x_1) \cdot \gamma(\overline{x_1}, x_2) \cdot \gamma(\overline{x_1x_2}, x_3) \cdot \dots \cdot \gamma(\overline{x_1x_2 \dots x_{n-1}}, x_n). \quad (1)$$

16.3. Satz. Die Gruppe H ist frei mit der Basis $Y = \{\gamma(t, x) \mid t \in T, x \in X\}$.

Sei $\tau(w)$ das Aufschreiben der Elemente $w \in H$ in der Basis Y (siehe die Formel (1)).

16.4. Satz. Sei G eine Gruppe mit der Präsentation $\langle X \mid R \rangle$ und sei G_1 eine Untergruppe von G . Sei $\varphi : F(X) \rightarrow G$ der kanonische Epimorphismus, sei $H = \varphi^{-1}(G_1)$ und T ein rechtes Schreier-Transversal für H in $F(X)$. Dann hat G_1 die Präsentation

$$\langle Y \mid \tau(trt^{-1}), t \in T, r \in R \rangle,$$

wobei Y und $\tau(w)$ in 16.3 definiert sind.

16.5. Beispiel. Definieren wir einen Homomorphismus $G = \langle a, b \mid a^2 = b^3 \rangle \xrightarrow{\theta} S_3$ mit der Regel $a \mapsto (12), b \mapsto (123)$. Dann hat $\text{Ker}(\theta)$ die Präsentation $\langle x, y, z \mid yz = zy, xz = zx \rangle$ und so ist $\text{Ker}(\theta) \cong F_2 \times \mathbb{Z}$.

Vorlesung 17

Todd–Coxeter–Methode

Sei G eine Gruppe mit der Präsentation $\langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$, sei G_1 eine Untergruppe von G , und seien $w_1(x_1, \dots, x_n), \dots, w_k(x_1, \dots, x_n)$ Erzeugende von G_1 . Wenn der Index $|G : G_1|$ endlich ist, dann kann man folgende Datei mit Hilfe der Todd–Coxeter–Methode berechnen:

- 1) Index von G_1 in G ;
- 2) Cayley-Graph von G bezüglich G_1 ;
- 3) Schreier-Transversal für G_1 in G .

17.1. Beispiel. 1) Seien $G = \langle x, y \mid x^4, y^3, (xy)^2 \rangle$ und $G_1 = \langle x \rangle \leq G$. Daraus kann man konsequent die folgende Information bekommen: $|G : G_1| = 6$, $|x| = 4$, $|G| = 24$, $G \cong S_4$.

2) Seien $F(2, 5) = \langle x, a, b, c, d \mid xa = b, ab = c, bc = d, cd = x, dx = a \rangle$ und $G_1 = \langle x \rangle \leq G$. Dann ist $|G : G_1| = 1$ und $F(2, 5) \cong \mathbb{Z}_{11}$.

Vorlesung 18

Fox-Calculus

18.1. Definition. Sei G eine Gruppe. Betrachten wir die Menge aller endlichen formalen Summen $\sum'_{g \in G} n_g g$, wobei $n_g \in \mathbb{Z}$ ist. Die Endlichkeit bedeutet, dass alle Koeffizienten n_g ausser einer endlichen Anzahl gleich 0 sind.

Man kann zwei solche Summen addieren und multiplizieren. Daraus entsteht ein Ring, der *Gruppenring* von G heißt. Der Ring wird als $\mathbb{Z}G$ bezeichnet.

18.2. Definition. Sei $F = F(X)$ eine freie Gruppe mit der Basis X und sei $\mathbb{Z}F$ der *Gruppenring* von F . Für jedes $x \in X$ definieren wir eine Fox-Ableitung

$$\frac{\partial}{\partial x} : F \rightarrow \mathbb{Z}F$$

nach der folgenden Regel:

$$\frac{\partial w}{\partial x} = u_1 + \dots + u_k - x^{-1}v_1 - \dots - x^{-1}v_s,$$

wobei u_1, \dots, u_k die Endsegmente von w sind, die nach Auftreten von x in w stehen, und v_1, \dots, v_s die Endsegmente von w sind, die nach Auftreten von x^{-1} in w stehen.

18.3. Beispiel.

1) $\frac{\partial}{\partial x}(x^{-1}y^{-1}xy) = y - x^{-1}y^{-1}xy,$

2) $\frac{\partial}{\partial y}(x^{-1}y^{-1}xy) = e - y^{-1}xy,$

3) $\frac{\partial}{\partial x}(x^n) = e + x + \dots + x^{n-1}.$

18.4. Behauptung. Seien $x, y \in X$ und $u, v \in F$. Dann gelten die Formeln

1)

$$\frac{\partial y}{\partial x} = \begin{cases} 1, & \text{wenn } x = y \text{ ist,} \\ 0, & \text{wenn } x \neq y \text{ ist,} \end{cases}$$

2)

$$\frac{\partial}{\partial x}(x^{-1}) = -x^{-1},$$

3)

$$\frac{\partial}{\partial x}(uv) = \frac{\partial u}{\partial x}v + \frac{\partial v}{\partial x}.$$

18.5. Satz (Kettenregel). Seien $v_1, \dots, v_k \in F(X)$ und $w = w(v_1, \dots, v_k)$. Dann gilt

$$\frac{\partial w}{\partial x} = \sum_{i=1}^k \frac{\partial v_i}{\partial x} \cdot \frac{\partial w}{\partial v_i}$$

für alle $x \in X$.

18.6. Satz (Taylor-Formel). Für alle $w \in F(x_1, \dots, x_n)$ gilt

$$w - e = \sum_{i=1}^n (x_i - e) \cdot \frac{\partial w}{\partial x_i}.$$

Vorlesung 19

Alexander-Matrix und elementare Ideale

19.1. Definition. Sei G eine Gruppe mit einer endlichen Präsentation $\mathcal{P} = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$. Wir betrachten folgende Homomorphismen:

$$F \xrightarrow{\varphi} G \xrightarrow{Ab} G/G',$$

wobei F die freie Gruppe mit der Basis $X = \{x_1, \dots, x_n\}$ ist, $\varphi : F \rightarrow G$ der kanonische Epimorphismus ist und Ab der Abelianisierungshomomorphismus $G \rightarrow G/G'$ ist. Wir erweitern die Homomorphismen der Gruppen bis Homomorphismen ihren Gruppenringe:

$$\mathbb{Z}F \xrightarrow{\varphi} \mathbb{Z}G \xrightarrow{Ab} \mathbb{Z}(G/G').$$

Die *Alexander-Matrix* der Präsentation \mathcal{P} ist

$$Ab \begin{pmatrix} \varphi\left(\frac{\partial r_1}{\partial x_1}\right) & \dots & \varphi\left(\frac{\partial r_1}{\partial x_n}\right) \\ \vdots & & \vdots \\ \varphi\left(\frac{\partial r_m}{\partial x_1}\right) & \dots & \varphi\left(\frac{\partial r_m}{\partial x_n}\right) \end{pmatrix}.$$

Wir definieren *elementare Ideale* $E_i(\mathcal{P})$, $i = 1, 2, \dots$ in dem Gruppenring $\mathbb{Z}(G/G')$ nach der folgenden Regel:

$E_1(\mathcal{P})$ ist von Determinanten aller Minoren der Größe $l = \min(n, m)$ erzeugt.

$E_2(\mathcal{P})$ ist von Determinanten aller Minoren der Größe $l - 1$ erzeugt.

...

$E_l(\mathcal{P})$ ist von Determinanten aller Minoren der Größe 1 erzeugt.

$E_s(\mathcal{P}) = \mathbb{Z}(G/G')$ für $s \geq l + 1$.

Falls $G/G' \cong \mathbb{Z}$ ist, definiert man auch *Alexander-Polynom* von \mathcal{P} als ggT aller Elemente der Alexander-Matrix.

19.2. Satz. Seien $\mathcal{P}_1 = \langle X_1 \mid R_1 \rangle$ und $\mathcal{P}_2 = \langle X_2 \mid R_2 \rangle$ zwei endliche Präsentationen einer Gruppe G . Dann sind die elementaren Ideale von \mathcal{P}_1 und \mathcal{P}_2 gleich.

Falls $G/G' \cong \mathbb{Z}$ ist, sind die Alexander-Polynome von \mathcal{P}_1 und \mathcal{P}_2 gleich.

Vorlesung 20

Anwendungen zur Knoten-Theorie

Ein Knoten in \mathbb{R}^3 ist eine injektive und stetige Abbildung von dem Kreis

$$\{e^{i\varphi} \mid 0 \leq \varphi \leq 2\pi\}$$

in \mathbb{R}^3 . Wir betrachten nur die Knoten, die unendlich differenzierbar sind.

Man muss

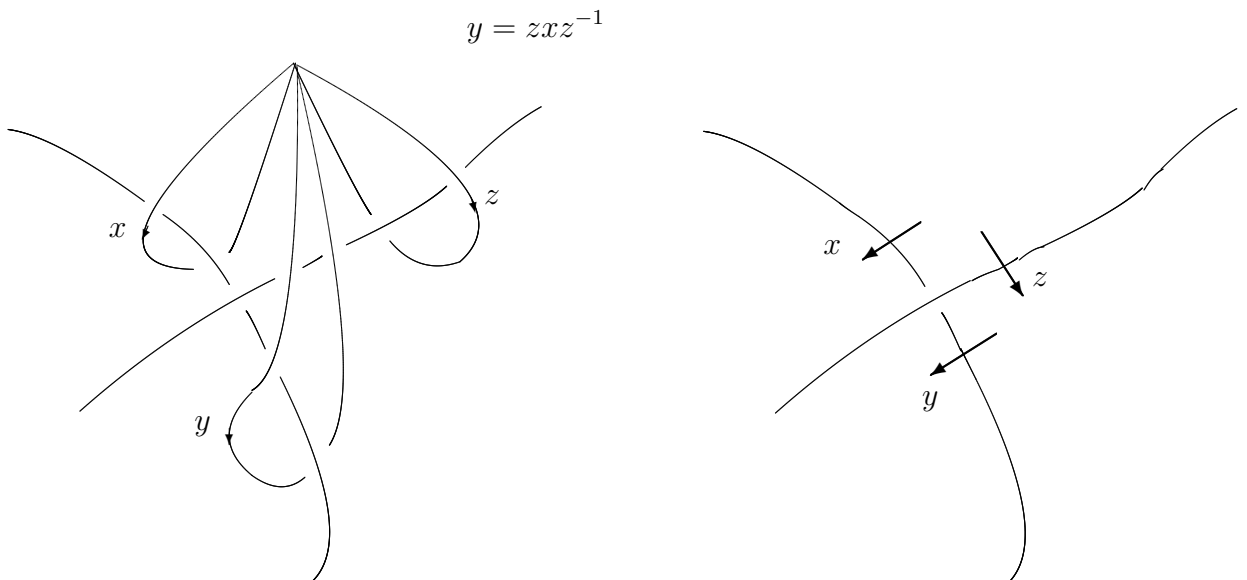
- 1) die Definition der fundamentalen Gruppe eines Knotens kennen;
- 2) die Wirtinger-Präsentation dieser Gruppe aufschreiben können;
- 3) verstehen, warum die Abelianisierung dieser Gruppe isomorph \mathbb{Z} ist;

4) die Alexander-Matrix, die elementaren Ideale und das Alexander-Polynom der Präsentation berechnen.

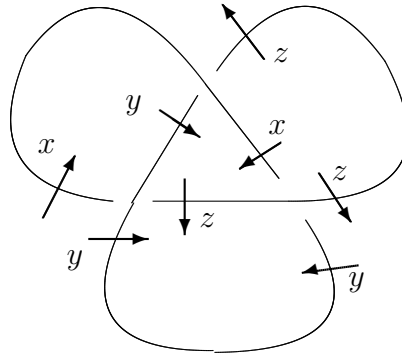
Bezeichnung.



Relation.



20.1. Beispiel. Betrachten wir den Kleeblatt-Knoten K :



Seine fundamentale Gruppe $G = \pi_1(\mathbb{R}^3 \setminus K)$ hat folgende Wirtinger-Präsentation:

$$\langle x, y, z \mid y = z x z^{-1}, y^{-1} = x z x^{-1}, z^{-1} = y x y^{-1} \rangle.$$

Man kann hier z eliminieren und vereinfachen:

$$\langle x, y \mid x y x = y x y \rangle.$$

Sei $r = x y x y^{-1} x^{-1} y^{-1}$. Dann ist

$$\begin{pmatrix} \frac{\partial r}{\partial x} \\ \frac{\partial r}{\partial y} \end{pmatrix} = \begin{pmatrix} y x y^{-1} x^{-1} y^{-1} + y^{-1} x^{-1} y^{-1} - x^{-1} y^{-1} \\ x y^{-1} x^{-1} y^{-1} - y^{-1} x^{-1} y^{-1} - y^{-1} \end{pmatrix}.$$

Es ist klar, dass G/G' eine unendliche zyklische Gruppe ist. Wir haben

$$\begin{aligned} G &\xrightarrow{Ab} G/G' = \langle t \rangle, \\ x &\mapsto t, \\ y &\mapsto t. \end{aligned}$$

Die Alexander-Matrix ist

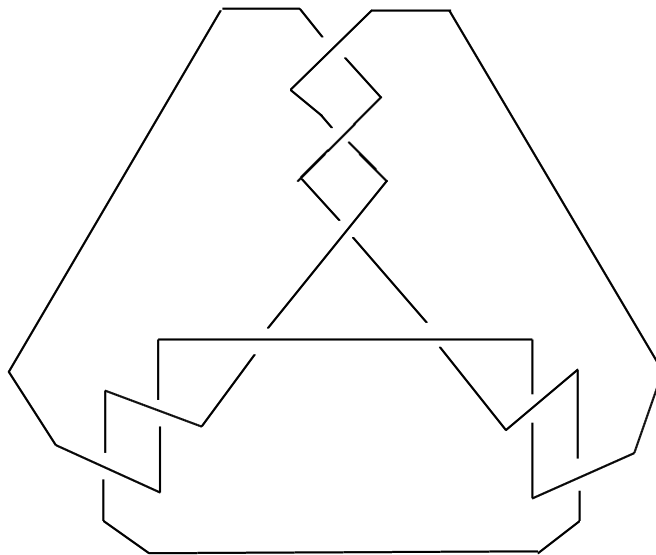
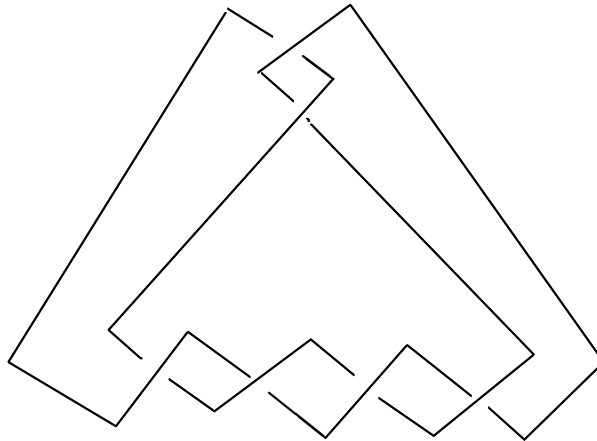
$$\begin{pmatrix} t^{-1} + t^{-3} - t^{-2} \\ t^{-2} - t^{-3} - t^{-1} \end{pmatrix}.$$

Das erste elementare Ideal ist $\langle t^2 - t + 1 \rangle \subseteq \mathbb{Z}(G/G')$.

Das Alexander-Polynom ist $t^2 - t + 1$.

20.2. Satz. Äquivalente Knoten haben isomorphe fundamentale Gruppen und isomorphe elementare Ideale. Außerdem haben sie gleiche Alexander-Polynome.

20.3. Bemerkung. Folgende Knoten sind nicht äquivalent, obwohl ihre Alexander-Polynome gleich sind:



TEIL 3. ALGORITHMISCHE ZAHLENTHEORIE