# Varietäten und Gröbnerbasen

Thomas Markwig

keilen@mathematik.uni-kl.de

Technische Universität Kaiserslautern

# 1. Einstiegsbeispiel

Gegeben eine Sequenz:

CTCACGTGATGAGAGCATTCTCAGACCGTAGACGCGTGTAGCAGCGGC

# 1. Einstiegsbeispiel

Gegeben eine Sequenz:

CTCACGTGATGAGAGCATTCTCAGACCGTAGACGCGTGTAGCAGCGGC

Modell: Sequenz entstand folgendermaßen:

1. Wähle sukzessive einen von drei Tetraederwürfeln $W_1$, $W_2$, $W_3$ mit Seiten $A$, $C$, $G$, $T$.
2. Würfele und notiere das Ergebnis.

# 1. Einstiegsbeispiel

Idee:

- Wahrscheinlichkeitsverteilung der $W_i$ bekannt,

| | $P_{W_i}(A)$ | $P_{W_i}(C)$ | $P_{W_i}(G)$ | $P_{W_i}(T)$ |
|---|---|---|---|---|
| $i = 1$ | $0.15$ | $0.33$ | $0.36$ | $0.16$ |
| $i = 2$ | $0.27$ | $0.24$ | $0.23$ | $0.26$ |
| $i = 3$ | $0.25$ | $0.25$ | $0.25$ | $0.25$ |

# 1. Einstiegsbeispiel

Idee:

- Wahrscheinlichkeitsverteilung der $W_i$ bekannt,

| | $P_{W_i}(A)$ | $P_{W_i}(C)$ | $P_{W_i}(G)$ | $P_{W_i}(T)$ |
|---|---|---|---|---|
| $i=1$ | $0.15$ | $0.33$ | $0.36$ | $0.16$ |
| $i=2$ | $0.27$ | $0.24$ | $0.23$ | $0.26$ |
| $i=3$ | $0.25$ | $0.25$ | $0.25$ | $0.25$ |

- Wahrscheinlichkeit $\theta_i$, $W_i$ zu wählen, unbekannt.

# 1. Einstiegsbeispiel

| | $P_{W_i}(A)$ | $P_{W_i}(C)$ | $P_{W_i}(G)$ | $P_{W_i}(T)$ |
|---|---|---|---|---|
| $i=1$ | 0.15 | 0.33 | 0.36 | 0.16 |
| $i=2$ | 0.27 | 0.24 | 0.23 | 0.26 |
| $i=3$ | 0.25 | 0.25 | 0.25 | 0.25 |

Dann ergibt sich als Wahrscheinlichkeit für $A$, $C$, $G$, $T$:

$$\begin{aligned} p_A &= 0.15 \cdot \theta_1 + 0.27 \cdot \theta_2 + 0.25 \cdot (1 - \theta_1 - \theta_2) \\ p_C &= 0.33 \cdot \theta_1 + 0.24 \cdot \theta_2 + 0.25 \cdot (1 - \theta_1 - \theta_2) \\ p_G &= 0.36 \cdot \theta_1 + 0.23 \cdot \theta_2 + 0.25 \cdot (1 - \theta_1 - \theta_2) \\ p_T &= 0.16 \cdot \theta_1 + 0.26 \cdot \theta_2 + 0.25 \cdot (1 - \theta_1 - \theta_2) \end{aligned}$$

# 1. Einstiegsbeispiel

Dann ergibt sich als Wahrscheinlichkeit für $A$, $C$, $G$, $T$:

$$\begin{aligned}
p_A(\theta_1,\theta_2) &= 0.15\cdot\theta_1 + 0.27\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)\\
p_C(\theta_1,\theta_2) &= 0.33\cdot\theta_1 + 0.24\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)\\
p_G(\theta_1,\theta_2) &= 0.36\cdot\theta_1 + 0.23\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)\\
p_T(\theta_1,\theta_2) &= 0.16\cdot\theta_1 + 0.26\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)
\end{aligned}$$

# 1. Einstiegsbeispiel

Dann ergibt sich als Wahrscheinlichkeit für $A$, $C$, $G$, $T$:

$$\begin{aligned}
p_A(\theta_1,\theta_2) &= 0.15\cdot\theta_1 + 0.27\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)\\
p_C(\theta_1,\theta_2) &= 0.33\cdot\theta_1 + 0.24\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)\\
p_G(\theta_1,\theta_2) &= 0.36\cdot\theta_1 + 0.23\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)\\
p_T(\theta_1,\theta_2) &= 0.16\cdot\theta_1 + 0.26\cdot\theta_2 + 0.25\cdot(1-\theta_1-\theta_2)
\end{aligned}$$

und mithin als Wahrscheinlichkeit für die Sequenz:

$$L(\theta_1,\theta_2) = p_A^{10}\cdot p_C^{14}\cdot p_G^{15}\cdot p_T^{10}.$$

# 1. Einstiegsbeispiel

Wahrscheinlichkeit für die Sequenz:

$$L(\theta_1, \theta_2) = p_A^{10} \cdot p_C^{14} \cdot p_G^{15} \cdot p_T^{10}.$$

Ziel: Wähle $0 < \theta_1, \theta_2 < 1$ so, daß $L(\theta_1, \theta_2)$ maximal.

# 1. Einstiegsbeispiel

Wahrscheinlichkeit für die Sequenz:

$$L(\theta_1, \theta_2) = p_A^{10} \cdot p_C^{14} \cdot p_G^{15} \cdot p_T^{10}.$$

Ziel: Wähle $0 < \theta_1, \theta_2 < 1$ so, daß $L(\theta_1, \theta_2)$ maximal.

Alternativ: maximiere $l(\theta_1, \theta_2) = \log\big(L(\theta_1, \theta_2)\big)$, wobei

$$l(\theta_1, \theta_2) = 10 \cdot \log(p_A) + 14 \cdot \log(p_C) + 15 \cdot \log(p_G) + 10 \cdot \log(p_T).$$

# 1. Einstiegsbeispiel

Alternativ: maximiere $l(\theta_1, \theta_2) = \log\left(L(\theta_1, \theta_2)\right)$, wobei

$$l(\theta_1, \theta_2) = 10 \cdot \log(p_A) + 14 \cdot \log(p_C) + 15 \cdot \log(p_G) + 10 \cdot \log(p_T).$$

“Maximieren” heißt: kritische Punkte betrachten:

$$\begin{aligned} \frac{\partial l(\theta_1,\theta_2)}{\partial \theta_1} &= 0 \\ \frac{\partial l(\theta_1,\theta_2)}{\partial \theta_2} &= 0 \end{aligned}$$

# 1. Einstiegsbeispiel

Alternativ: maximiere $l(\theta_1, \theta_2) = \log\left(L(\theta_1, \theta_2)\right)$, wobei

$$l(\theta_1, \theta_2) = 10 \cdot \log(p_A) + 14 \cdot \log(p_C) + 15 \cdot \log(p_G) + 10 \cdot \log(p_T).$$

“Maximieren” heißt: kritische Punkte betrachten:

$$\frac{\partial l(\theta_1,\theta_2)}{\partial \theta_1} = \frac{10}{p_A} \cdot \frac{\partial p_A}{\partial \theta_1} + \frac{14}{p_C} \cdot \frac{\partial p_C}{\partial \theta_1} + \frac{15}{p_G} \cdot \frac{\partial p_G}{\partial \theta_1} + \frac{10}{p_T} \cdot \frac{\partial p_T}{\partial \theta_1} = 0$$

$$\frac{\partial l(\theta_1,\theta_2)}{\partial \theta_2} = \frac{10}{p_A} \cdot \frac{\partial p_A}{\partial \theta_2} + \frac{14}{p_C} \cdot \frac{\partial p_C}{\partial \theta_2} + \frac{15}{p_G} \cdot \frac{\partial p_G}{\partial \theta_2} + \frac{10}{p_T} \cdot \frac{\partial p_T}{\partial \theta_2} = 0$$

# 1. Einstiegsbeispiel

Alternativ: maximiere $l(\theta_1, \theta_2) = \log\left(L(\theta_1, \theta_2)\right)$, wobei

$$l(\theta_1, \theta_2) = 10 \cdot \log(p_A) + 14 \cdot \log(p_C) + 15 \cdot \log(p_G) + 10 \cdot \log(p_T).$$

“Maximieren” heißt: kritische Punkte betrachten:

$$\frac{\partial l(\theta_1,\theta_2)}{\partial \theta_1} = \frac{f_1(\theta_1,\theta_2)}{g_1(\theta_1,\theta_2)} = 0$$

$$\frac{\partial l(\theta_1,\theta_2)}{\partial \theta_2} = \frac{f_2(\theta_1,\theta_2)}{g_2(\theta_1,\theta_2)} = 0$$

mit $f_1, f_2, g_1, g_2 \in \mathbb{Q}[\theta_1, \theta_2]$.

# 1. Einstiegsbeispiel

Alternativ: maximiere $l(\theta_1, \theta_2) = \log\big(L(\theta_1, \theta_2)\big)$, wobei

$$l(\theta_1, \theta_2) = 10 \cdot \log(p_A) + 14 \cdot \log(p_C) + 15 \cdot \log(p_G) + 10 \cdot \log(p_T).$$

"Maximieren" heißt: kritische Punkte betrachten:

$$\frac{\partial l(\theta_1,\theta_2)}{\partial \theta_1} = 0 \iff f_1(\theta_1, \theta_2) = 0$$

$$\frac{\partial l(\theta_1,\theta_2)}{\partial \theta_2} = 0 \iff f_2(\theta_1, \theta_2) = 0$$

mit $f_1, f_2 \in \mathbb{Q}[\theta_1, \theta_2]$ geeignet.

# 1. Einstiegsbeispiel

Problemstellung:

Finde $0 < \theta_1, \theta_2 < 1$ so, daß die Wahrscheinlichkeit für die beobachtete Sequenz maximal wird.

# 1. Einstiegsbeispiel

Problemstellung:

Finde $0 < \theta_1, \theta_2 < 1$ so, daß die Wahrscheinlichkeit für die beobachtete Sequenz maximal wird.

Gleichwertig zu:

Finde $(\theta_1, \theta_2) \in (0,1) \times (0,1) \subset \mathbb{R}^2$ so, daß

$$f_1(\theta_1, \theta_2) = 0, \qquad f_2(\theta_1, \theta_2) = 0,$$

für geeignete Polynome $f_1, f_2 \in \mathbb{Q}[\theta_1, \theta_2]$.

# 2. Notation

- $x = (x_1, \ldots, x_n)$, Variablen,
- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, Multiindex,
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, Monom,
- $|\alpha| = \alpha_1 + \ldots + \alpha_n$,

# 2. Notation

- $x = (x_1, \ldots, x_n)$, Variablen,
- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, Multiindex,
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, Monom,
- $|\alpha| = \alpha_1 + \ldots + \alpha_n$,
- $\mathrm{Mon}_x = \left\{ x^\alpha \mid \alpha \in \mathbb{N}^n \right\}$, Menge der Monome in $x$,

# 2. Notation

- $x = (x_1, \ldots, x_n)$, Variablen,
- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, Multiindex,
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, Monom,
- $|\alpha| = \alpha_1 + \ldots + \alpha_n$,
- $\mathrm{Mon}_x = \left\{ x^\alpha \mid \alpha \in \mathbb{N}^n \right\}$, Menge der Monome in $x$,
- $R = \mathbb{Q}[x_1, \ldots, x_n] = \left\{ \sum_{|\alpha|=0}^{d} a_\alpha x^\alpha \;\middle|\; a_\alpha \in \mathbb{Q}, d \geq 0 \right\}$, der Polynomring in $x$.

# 2. Notation

- $x = (x_1, \ldots, x_n)$, Variablen,
- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, Multiindex,
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, Monom,
- $|\alpha| = \alpha_1 + \ldots + \alpha_n$,
- $\mathrm{Mon}_x = \left\{ x^\alpha \mid \alpha \in \mathbb{N}^n \right\}$, Menge der Monome in $x$,
- $R = \mathbb{Q}[x_1, \ldots, x_n] = \left\{ \sum_{|\alpha|=0}^{d} a_\alpha x^\alpha \;\middle|\; a_\alpha \in \mathbb{Q}, d \geq 0 \right\}$, der Polynomring in $x$.
- Manchmal: $(x_1, \ldots, x_n) = (\theta_1, \ldots, \theta_n)$, oder

# 2. Notation

- $x = (x_1, \ldots, x_n)$, Variablen,
- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, Multiindex,
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, Monom,
- $|\alpha| = \alpha_1 + \ldots + \alpha_n$,
- $\mathrm{Mon}_x = \left\{ x^\alpha \mid \alpha \in \mathbb{N}^n \right\}$, Menge der Monome in $x$,
- $R = \mathbb{Q}[x_1, \ldots, x_n] = \left\{ \sum_{|\alpha|=0}^{d} a_\alpha x^\alpha \;\middle|\; a_\alpha \in \mathbb{Q}, d \geq 0 \right\}$, der Polynomring in $x$.
- Manchmal: $(x_1, \ldots, x_{n \cdot m}) = (p_{11}, \ldots, p_{nm})$, oder

# 2. Notation

- $x = (x_1, \ldots, x_n)$, Variablen,
- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, Multiindex,
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, Monom,
- $|\alpha| = \alpha_1 + \ldots + \alpha_n$,
- $\mathrm{Mon}_x = \left\{ x^\alpha \mid \alpha \in \mathbb{N}^n \right\}$, Menge der Monome in $x$,
- $R = \mathbb{Q}[x_1, \ldots, x_n] = \left\{ \sum_{|\alpha|=0}^{d} a_\alpha x^\alpha \;\middle|\; a_\alpha \in \mathbb{Q}, d \geq 0 \right\}$, der Polynomring in $x$.
- Manchmal: $(x_1, \ldots, x_{16}) = (p_{AA}, p_{AC}, \ldots, p_{TT})$.

# 3. Varietäten

Ziel: Gegeben $f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$, löse

$$f_1(x) = 0 \qquad f_2(x) = 0 \qquad \ldots \qquad f_k(x) = 0.$$

# 3. Varietäten

Ziel: Gegeben $f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$, löse

$$f_1(x) = 0 \quad f_2(x) = 0 \quad \ldots \quad f_k(x) = 0.$$

Definition: $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \mathbb{Q}[x_1, \ldots, x_n]$, dann heißt

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f_1(a) = \ldots = f_k(a) = 0\}$$

die durch $\mathcal{F}$ definierte Varietät.

# 3. Varietäten

Definition: $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \mathbb{Q}[x_1, \ldots, x_n]$, dann heißt

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f_1(a) = \ldots = f_k(a) = 0\}$$

die durch $\mathcal{F}$ definierte Varietät.

1. Frage: Wieso $\mathbb{C}^n$? Wir suchen $a \in (0,1)^n \subset \mathbb{R}^n$!

# 3. Varietäten

1. Frage: Wieso $\mathbb{C}^n$? Wir suchen $a \in (0,1)^n \subset \mathbb{R}^n$!

Antwort: Fundamentalsatz der Algebra

$f \in \mathbb{Q}[x_1]$ dann hat $f$ in $\mathbb{C}$ "genau" $\deg(f)$ Nullstellen.

# 3. Varietäten

1. Frage: Wieso $\mathbb{C}^n$? Wir suchen $a \in (0,1)^n \subset \mathbb{R}^n$!

Antwort: Fundamentalsatz der Algebra

$f \in \mathbb{Q}[x_1]$ dann hat $f$ in $\mathbb{C}$ "genau" $\deg(f)$ Nullstellen.

Problem in $\mathbb{R}$: $f = x^2 + 1$ hat keine Nullstelle in $\mathbb{R}$!

# 3. Varietäten

1. Frage: Wieso $\mathbb{C}^n$? Wir suchen $a \in (0,1)^n \subset \mathbb{R}^n$!

Antwort: Fundamentalsatz der Algebra

$f \in \mathbb{Q}[x_1]$ dann hat $f$ in $\mathbb{C}$ "genau" $\deg(f)$ Nullstellen.

Problem in $\mathbb{R}$: $f = x^2 + 1$ hat keine Nullstelle in $\mathbb{R}$!

Quintessenz: Theorie über $\mathbb{C}$ schöner, also löse zunächst über $\mathbb{C}$.

# 3. Varietäten

1. Frage: Wieso $\mathbb{C}^n$? Wir suchen $a \in (0,1)^n \subset \mathbb{R}^n$!

Antwort: Fundamentalsatz der Algebra

$f \in \mathbb{Q}[x_1]$ dann hat $f$ in $\mathbb{C}$ "genau" $\deg(f)$ Nullstellen.

Problem in $\mathbb{R}$: $f = x^2 + 1$ hat keine Nullstelle in $\mathbb{R}$!

Quintessenz: Theorie über $\mathbb{C}$ schöner, also löse zunächst über $\mathbb{C}$.

Definition: $S \subset \mathbb{C}^n$ dann $V_S(\mathcal{F}) = S \cap V(\mathcal{F})$.

# 3. Varietäten

Definition: $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \mathbb{Q}[x_1, \ldots, x_n]$, dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f_1(a) = \ldots = f_k(a) = 0\}.$$

2. Frage: Muß $\mathcal{F}$ endlich sein?

# 3. Varietäten

Definition: $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \mathbb{Q}[x_1, \ldots, x_n]$, dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f_1(a) = \ldots = f_k(a) = 0\}.$$

2. Frage: Muß $\mathcal{F}$ endlich sein?

Wenn $f = g_1 \cdot f_1 + \ldots + g_k \cdot f_k$ mit $g_i \in R$ dann

$f(a) = g_1(a) \cdot f_1(a) + \ldots + g_k(a) \cdot f_k(a) = 0$ für alle $a \in V($

# 3. Varietäten

Definition: $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \mathbb{Q}[x_1, \ldots, x_n]$, dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f_1(a) = \ldots = f_k(a) = 0\}.$$

2. Frage: Muß $\mathcal{F}$ endlich sein?

Setzen wir $\langle \mathcal{F} \rangle = \{g_1 \cdot f_1 + \ldots + g_k \cdot f_k \mid g_i \in R\}$ dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f(a) = 0 \ \ \forall\ f \in \langle \mathcal{F} \rangle\},$$

Nullstellenmenge von unendlich vielen Polynomen.

# 3. Varietäten

Definition: $\mathcal{F} \subset \mathbb{Q}[x_1, \ldots, x_n]$ beliebig, dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f(a) = 0 \quad \forall\, f \in \mathcal{F}\}.$$

2. Frage: Muß $\mathcal{F}$ endlich sein?

Für $\langle \mathcal{F} \rangle = \{g_1 \cdot f_1 + \ldots + g_k \cdot f_k \mid g_i \in R, f_i \in \mathcal{F}\}$ dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f(a) = 0 \ \ \forall\, f \in \langle \mathcal{F} \rangle\}.$$

# 3. Varietäten

Definition: $\mathcal{F} \subset \mathbb{Q}[x_1, \ldots, x_n]$ beliebig, dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f(a) = 0 \quad \forall\, f \in \mathcal{F}\}.$$

2. Frage: Muß $\mathcal{F}$ endlich sein?

Für $\langle \mathcal{F} \rangle = \{g_1 \cdot f_1 + \ldots + g_k \cdot f_k \mid g_i \in R, f_i \in \mathcal{F}\}$ dann ist

$$V(\mathcal{F}) = \{a \in \mathbb{C}^n \mid f(a) = 0 \;\; \forall\, f \in \langle \mathcal{F} \rangle\}.$$

3. Frage: Kommt man immer mit endlich vielen $f_i$ aus?

# 3. Varietäten

3. Frage: Kommt man immer mit endlich vielen $f_i$ aus?

Antwort: Hilberts Basissatz.

Ist $\mathcal{F} \subset R$ beliebig, dann gibt es $f_1, \ldots, f_k \in \mathcal{F}$ so, daß

$$\langle \mathcal{F} \rangle = \langle f_1, \ldots, f_k \rangle.$$

Insbesondere:

$$V(\mathcal{F}) = V(f_1, \ldots, f_k).$$

# 3. Varietäten

3. Frage: Kommt man immer mit endlich vielen $f_i$ aus?

Antwort: Hilberts Basissatz.

Ist $\mathcal{F} \subset R$ beliebig, dann gibt es $f_1, \ldots, f_k \in \mathcal{F}$ so, daß

$$\langle \mathcal{F} \rangle = \langle f_1, \ldots, f_k \rangle.$$

Insbesondere:

$$V(\mathcal{F}) = V(f_1, \ldots, f_k).$$

Quintessenz: Jede Varietät ist Nullstellenmenge von endlich vielen Polynomen.

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Hoffnung: $\#V(f_1, \ldots, f_k) < \infty$.

Dann: “löse” = “finde alle Punkte in $V(f_1, \ldots, f_k)$”.

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Hoffnung: $\#V(f_1, \ldots, f_k) < \infty$.

Dann: "löse" = "finde alle Punkte in $V(f_1, \ldots, f_k)$".

Wie macht man das?

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Hoffnung: $\#V(f_1, \ldots, f_k) < \infty$.

Dann: "löse" = "finde alle Punkte in $V(f_1, \ldots, f_k)$".

Wie macht man das?

Einfachster Fall:

$$\begin{array}{lllllllllll} f_1 & = & a_{11}x_1 & + & a_{12}x_2 & + & \ldots & a_{1n}x_n & + & b_1 & = & 0 \\ f_2 & = & a_{21}x_1 & + & a_{22}x_2 & + & \ldots & a_{2n}x_n & + & b_2 & = & 0 \\ \vdots & & & & & & \vdots & & & & & \\ f_n & = & a_{n1}x_1 & + & a_{n2}x_2 & + & \ldots & a_{nn}x_n & + & b_n & = & 0 \end{array}$$

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Hoffnung: $\#V(f_1, \ldots, f_k) < \infty$.

Dann: "löse" = "finde alle Punkte in $V(f_1, \ldots, f_k)$".

Wie macht man das?

Einfachster Fall: Gaußalgorithmus $\longrightarrow$ Zeilenstufenform

$$\begin{array}{lcccccccccc}
f_1' & = & a_{11}'x_1 & + & a_{12}'x_2 & + & \ldots & a_{1n}'x_n & + & b_1' & = & 0 \\
f_2' & = & & & a_{22}'x_2 & + & \ldots & a_{2n}'x_n & + & b_2' & = & 0 \\
\vdots & & & & & & & \vdots & & & & \\
f_n' & = & & & & & & a_{nn}'x_n & + & b_n' & = & 0
\end{array}$$

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Hoffnung: $\#V(f_1, \ldots, f_k) < \infty$.

Dann: "löse" = "finde alle Punkte in $V(f_1, \ldots, f_k)$".

Einfachster Fall: $V(f_1, \ldots, f_n) = V(f'_1, \ldots, f'_n)$

$$\begin{array}{lcccccccccc}
f'_1 & = & a'_{11}x_1 & + & a'_{12}x_2 & + & \ldots & a'_{1n}x_n & + & b'_1 & = & 0 \\
f'_2 & = & & & a'_{22}x_2 & + & \ldots & a'_{2n}x_n & + & b'_2 & = & 0 \\
\vdots & & & & & & & \vdots & & & & \\
f'_n & = & & & & & & a'_{nn}x_n & + & b'_n & = & 0
\end{array}$$

Rückeinsetzen liefert die (hier eindeutige) Lösung.

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Hoffnung: $\#V(f_1, \ldots, f_k) < \infty$.

Dann: "löse" = "finde alle Punkte in $V(f_1, \ldots, f_k)$".

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Beispiel:

- $\mathcal{F} = \{f_1 = x_1^2 - x_2^2, \quad f_2 = x_1^2 - x_2\}$,
- $\mathcal{G} = \{f_1, \quad f_2' = f_2 - f_1 = x_2^2 - x_2\}$,

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Beispiel:

- $\mathcal{F} = \{f_1 = x_1^2 - x_2^2, \quad f_2 = x_1^2 - x_2\}$,
- $\mathcal{G} = \{f_1, \quad f_2' = f_2 - f_1 = x_2^2 - x_2\}$,
- $f_2' = x_2^2 - x_2 = 0 \quad \Longrightarrow \quad x_2 = 0$ oder $x_2 = 1$

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Beispiel:

- $\mathcal{F} = \{f_1 = x_1^2 - x_2^2, \quad f_2 = x_1^2 - x_2\}$,
- $\mathcal{G} = \{f_1, \quad f_2' = f_2 - f_1 = x_2^2 - x_2\}$,
- $f_2' = x_2^2 - x_2 = 0 \quad \Longrightarrow \quad x_2 = 0$ oder $x_2 = 1$
- $f_1(x_1, 0) = 0 \quad \Longrightarrow \quad x_1 = 0.$
- $f_1(x_1, 1) = 0 \quad \Longrightarrow \quad x_1 = 1$ oder $x_1 = -1.$

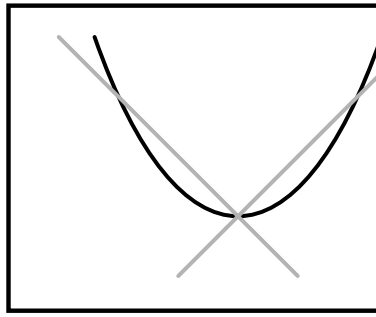
# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Beispiel:

- $\mathcal{F} = \{f_1 = x_1^2 - x_2^2, \quad f_2 = x_1^2 - x_2\}$,
- $\mathcal{G} = \{f_1, \quad f_2' = f_2 - f_1 = x_2^2 - x_2\}$,
- $f_2' = x_2^2 - x_2 = 0 \quad \Longrightarrow \quad x_2 = 0$ oder $x_2 = 1$
- $f_1(x_1, 0) = 0 \quad \Longrightarrow \quad x_1 = 0$.
- $f_1(x_1, 1) = 0 \quad \Longrightarrow \quad x_1 = 1$ oder $x_1 = -1$.
- Also: $V(\mathcal{F}) = V(\mathcal{G}) = \{(0,0), (1,1), (-1,1)\}$.



# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Quintessenz: Die Idee reduziert das Problem darauf, Nullstellen von Polynomen in einer Veränderlichen zu finden! (Numerik!)

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Quintessenz: Die Idee reduziert das Problem darauf, Nullstellen von Polynomen in einer Veränderlichen zu finden! (Numerik!)

Beispiel: $\mathcal{F} = \{f_1 = x^3 - 1, \quad f_2 = x^2 - x\} \subset \mathbb{Q}[x]$.

- Wir haben zwei Polynome, die nur von $x$ abhängen!
- Müssen wir für beide alle Nullstellen bestimmen?

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Quintessenz: Die Idee reduziert das Problem darauf, Nullstellen von Polynomen in einer Veränderlichen zu finden! (Numerik!)

Beispiel: $\mathcal{F} = \{f_1 = x^3 - 1, \quad f_2 = x^2 - x\} \subset \mathbb{Q}[x]$.

- Nein, denn $\langle f_1, f_2 \rangle = \langle \mathrm{ggT}(f_1, f_2) \rangle$!
- Also: $V(f_1, f_2) = V\big(\mathrm{ggT}(f_1, f_2)\big)$.

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Quintessenz: Die Idee reduziert das Problem darauf, Nullstellen von Polynomen in einer Veränderlichen zu finden! (Numerik!)

Beispiel: $\mathcal{F} = \{f_1 = x^3 - 1, \quad f_2 = x^2 - x\} \subset \mathbb{Q}[x]$.

- Wie berechne ich den $\mathrm{ggT}$ von $f_1$ und $f_2$?
- Antwort: Euklidischer Algorithmus!

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Beispiel: $\mathcal{F} = \{f_1 = x^3 - 1, \quad f_2 = x^2 - x\} \subset \mathbb{Q}[x]$.

Eukl.Alg. = wiederholte Division mit Rest: $r_{-1} = f_1, r_0 = f_2$

$$\begin{array}{rcccccl} r_{-1} & = & x^3 - x & = & (x+1) \cdot (x^2 - x) + (x-1) & = & q_1 \cdot r_0 + r \\ r_0 & = & x^2 - 1 & = & x \cdot (x-1) + 0 & = & q_2 \cdot r_1 + r \end{array}$$

$$r_2 = 0 \quad \Longrightarrow \quad \mathrm{ggT}(f_1, f_2) = r_1 = x - 1.$$

# 4.Was heißt löse $f_1(x) = \ldots = f_k(x) =$

Idee: Gegeben $\mathcal{F} \subset R$, finde $\mathcal{G} = \{g_1, \ldots, g_l\} \subset R$ so, daß

$\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$ und $g_i$ "hängt nur von $x_i, \ldots, x_n$ ab".

Beispiel: $\mathcal{F} = \{f_1 = x^3 - 1, \quad f_2 = x^2 - x\} \subset \mathbb{Q}[x]$.

Also:

$$V(f_1, f_2) = V(x - 1) = 1.$$

# 5. Ideensammlung

- 1. Gauß-Algorithmus – viele Veränderliche

  Grundidee: Man entledige sich sukzessive der einzelnen Variablen.

  Wichtig: Dazu muß man die Variablen angeordnet haben

# 5. Ideensammlung

- 1. Gauß-Algorithmus – viele Veränderliche

  Grundidee: Man entledige sich sukzessive der einzelnen Variablen.

  Wichtig: Dazu muß man die Variablen angeordnet haben

- 2. Euklidischer Algorithmus – eine Veränderliche

  Grundidee: Führe Division mit Rest durch und erniedrige dabei sukzessive den Grad.

  Wichtig: Monome sortiert nach Grad und Division mit Re

# 5. Ideensammlung

- 1. Gauß-Algorithmus – viele Veränderliche

  Wichtig: Dazu muß man die Variablen angeordnet haben

- 2. Euklidischer Algorithmus – eine Veränderliche

  Wichtig: Monome sortiert nach Grad und Division mit Re

- 3. Quintessenz:
  - Ordne die Monome vernünftig!
  - Verallgemeinere Division mit Rest!

# 6. Lexikographische Monomordnung

**Definition:** Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

# 6. Lexikographische Monomordnung

Definition: Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Offensichtlich gilt:

- $>$ ist eine Totalordnung auf $\mathrm{Mon}_x$.

# 6. Lexikographische Monomordnung

Definition: Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Offensichtlich gilt:

- $>$ ist eine Totalordnung auf $\mathrm{Mon}_x$.
- $x^\alpha > x^\beta \quad \Longrightarrow \quad x^\alpha \cdot x^\gamma = x^{\alpha+\gamma} > x^{\alpha+\gamma} = x^\beta \cdot x^\gamma$.

# 6. Lexikographische Monomordnung

Definition: Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Offensichtlich gilt:

- $>$ ist eine Wohlordnung auf $\mathrm{Mon}_x$.
- $x^\alpha > x^\beta \quad \Longrightarrow \quad x^\alpha \cdot x^\gamma = x^{\alpha+\gamma} > x^{\alpha+\gamma} = x^\beta \cdot x^\gamma$.
- $1 = x^{(0,\ldots,0)} \leq x^\alpha$ für alle $\alpha$.

# 6. Lexikographische Monomordnung

**Definition:** Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Notationen: $f = \sum_{|\alpha|=0}^{d} a_\alpha \cdot x^\alpha \in \mathbb{Q}[x_1, \ldots, x_n]$.

- $\mathrm{Mon}(f) = \{x^\alpha \mid a_\alpha \neq 0\}$, die Monome von $f$.

# 6. Lexikographische Monomordnung

**Definition:** Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Notationen: $f = \sum_{|\alpha|=0}^{d} a_\alpha \cdot x^\alpha \in \mathbb{Q}[x_1, \ldots, x_n]$.

- $\mathrm{Mon}(f) = \{x^\alpha \mid a_\alpha \neq 0\}$, die Monome von $f$.
- $\mathrm{lm}(f) = \max \mathrm{Mon}(f)$, das Leitmonom von $f$.
- $\mathrm{lc}(f) = a_\alpha$, wenn $\mathrm{lm}(f) = x^\alpha$, der Leitkoeffizient von $f$.

# 6. Lexikographische Monomordnung

**Definition:** Für $x^\alpha, x^\beta \in \mathrm{Mon}_x$ definieren wir

$$x^\alpha > x^\beta \quad :\Longleftrightarrow \quad \exists\, i \;:\; \alpha_1{=}\beta_1, \ldots, \alpha_{i-1}{=}\beta_{i-1}, \alpha_i > \beta_i.$$

Notationen: $f = \sum_{|\alpha|=0}^{d} a_\alpha \cdot x^\alpha \in \mathbb{Q}[x_1, \ldots, x_n]$.

- $\mathrm{Mon}(f) = \{x^\alpha \mid a_\alpha \neq 0\}$, die Monome von $f$.
- $\mathrm{lm}(f) = \max \mathrm{Mon}(f)$, das Leitmonom von $f$.
- $\mathrm{lc}(f) = a_\alpha$, wenn $\mathrm{lm}(f) = x^\alpha$, der Leitkoeffizient von $f$.
- $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$, der Leitterm von $f$.
- $\mathrm{tail}(f) = f - \mathrm{lt}(f)$, der Schwanz von $f$.

# 6. Lexikographische Monomordnung

- $\mathrm{Mon}(f) = \{x^\alpha \mid a_\alpha \neq 0\}$, die Monome von $f$.
- $\mathrm{lm}(f) = \max \mathrm{Mon}(f)$, das Leitmonom von $f$.
- $\mathrm{lc}(f) = a_\alpha$, wenn $\mathrm{lm}(f) = x^\alpha$, der Leitkoeffizient von $f$.
- $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$, der Leitterm von $f$.
- $\mathrm{tail}(f) = f - \mathrm{lt}(f)$, der Schwanz von $f$.

Beispiel: $f = 2x_1x_2^2 + x_2^3x_3 - 7x_2x_3^5 + 3 \in \mathbb{Q}[x_1, x_2, x_3]$

$$\mathrm{Mon}(f) = \{x_1x_2^2,\ x_2^3x_3,\ x_2x_3^5, 1\}, \quad \mathrm{lm}(f) = x_1x_2^2, \quad \mathrm{lc}(f) = 2,$$

$$\mathrm{lt}(f) = 2x_1x_2^2, \quad \mathrm{tail}(f) = x_2^3x_3 - 7x_2x_3^5 + 3$$

# 7. Verallgemeinerte Division mit Rest

Definition: Gegeben $f, f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$.

$$f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$$

heißt Division mit Rest, wenn gilt:

# 7. Verallgemeinerte Division mit Rest

Definition: Gegeben $f, f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$.

$$f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$$

heißt Division mit Rest, wenn gilt:

**ID1**: $\mathrm{lm}(f) \geq \mathrm{lm}(q_i f_i)$ für alle $i$, und

# 7. Verallgemeinerte Division mit Rest

Definition: Gegeben $f, f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$.

$$f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$$

heißt Division mit Rest, wenn gilt:

**ID1**: $\mathrm{lm}(f) \geq \mathrm{lm}(q_i f_i)$ für alle $i$, und

**ID2**: $r = 0$ oder $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.

# 7. Verallgemeinerte Division mit Rest

**Definition:** Gegeben $f, f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$.

$$f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$$

heißt Division mit Rest, wenn gilt:

**ID1:** $\mathrm{lm}(f) \geq \mathrm{lm}(q_i f_i)$ für alle $i$, und

**ID2:** $r = 0$ oder $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.

Wir nennen $r$ den Rest der Division mit Rest oder eine Normalform von $f$ bezüglich $f_1, \ldots, f_k$.

# 7. Verallgemeinerte Division mit Rest

**Definition:** Gegeben $f, f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$.

$$f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$$

heißt Division mit Rest, wenn gilt:

**ID1:** $\mathrm{lm}(f) \geq \mathrm{lm}(q_i f_i)$ für alle $i$, und

**ID2:** $r = 0$ oder $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.

**Beispiel:** $f = xy + y^2,\ f_1 = y^2 \in \mathbb{Q}[x, y]$

$$f = q \cdot f_1 + \left(xy + (1 - q) \cdot y^2\right)$$

ist für jedes $q \in \mathbb{Q}$ eine DmR – keine Eindeutigkeit!

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Beispiel:

$f = 3x^2 + x - 4, \quad f_1 = x^2 + 3x - 4, \quad f_2 = x^3 - 5x + 4 \in \mathbb{Q}[x].$

$$f = -3 \cdot f_1 + 0 \cdot f_2 + (-8x + 8)$$

ist eine Division mit Rest $r = -8x + 8 \neq 0$, aber

$$f = x \cdot f_1 - f_2 \in \langle f_1, f_2 \rangle.$$

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Wir wissen, falls $r \neq 0$:

- Wegen ID2 gilt: $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Wir wissen, falls $r \neq 0$:

- Wegen ID2 gilt: $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.
- Falls $\mathrm{lm}(r) \notin L(I) := \langle \mathrm{lm}(g) \mid g \in I \rangle$, dann $r \notin I$.

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Wir wissen, falls $r \neq 0$:

- Wegen ID2 gilt: $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.
- Falls $\mathrm{lm}(r) \notin L(I) := \langle \mathrm{lm}(g) \mid g \in I \rangle$, dann $f \notin I$.

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Wir wissen, falls $r \neq 0$:

- Wegen ID2 gilt: $\mathrm{lm}(r) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle$.
- Falls $\mathrm{lm}(r) \notin L(I) := \langle \mathrm{lm}(g) \mid g \in I \rangle$, dann $f \notin I$.

Schön wäre wenn für das Leitideal $L(I)$ gelten würde:

$$L(I) = \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle.$$

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Schön wäre wenn für das Leitideal $L(I)$ gelten würde:

$$L(I) = \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k) \rangle.$$

Definition: Gegeben $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$.

$\mathcal{G} \subset I$ endlich heißt Gröbnerbasis von $I$, falls

$$L(I) = \langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle.$$

# 8. Gröbnerbasen

Definition: Gegeben $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$.

$\mathcal{G} \subset I$ endlich heißt Gröbnerbasis von $I$, falls

$$L(I) = \langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle.$$

Beispiel:

$f_1 = x^2 + 3x - 4, \quad f_2 = x^3 - 5x + 4, \quad r = -8x + 8 \in \mathbb{Q}[x].$

$$r = (x - 3) \cdot f_1 - f_2 \in I = \langle f_1, f_2 \rangle,$$

aber

$$x = \mathrm{lm}(r) \notin \langle x^2 \rangle = \langle \mathrm{lm}(f_1), \mathrm{lm}(f_2) \rangle.$$

Also ist $\mathcal{G} = \{f_1, f_2\}$ keine Gröbnerbasis von $I$.

# 8. Gröbnerbasen

Beispiel:

$f_1 = x^2 + 3x - 4, \quad f_2 = x^3 - 5x + 4, \quad r = -8x + 8 \in \mathbb{Q}[x].$

$$r = (x-3) \cdot f_1 - f_2 \in I = \langle f_1, f_2 \rangle,$$

aber

$$x = \mathrm{lm}(r) \notin \langle x^2 \rangle = \langle \mathrm{lm}(f_1), \mathrm{lm}(f_2) \rangle.$$

Also ist $\mathcal{G} = \{f_1, f_2\}$ keine Gröbnerbasis von $I$.

Beachte:

$$r = \mathrm{ggT}(f_1, f_2) \quad \Longrightarrow \quad I = \langle r \rangle \quad \Longrightarrow \quad L(I) = \langle \mathrm{lm}(r) \rangle = \langle x \rangle.$$

Also ist $\mathcal{G} = \{r\}$ eine Gröbnerbasis von $I$.

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Definition: Gegeben $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$.

$\mathcal{G} \subset I$ endlich heißt Gröbnerbasis von $I$, falls

$$L(I) = \langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle.$$

# 8. Gröbnerbasen

Idee: Sei $f = q_1 \cdot f_1 + \ldots + q_k \cdot f_k + r$ eine DmR, dann

$$f \in I := \langle f_1, \ldots, f_k \rangle \iff r = 0.$$

Definition: Gegeben $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$.

$\mathcal{G} \subset I$ endlich heißt Gröbnerbasis von $I$, falls

$$L(I) = \langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle.$$

Fragen:

- Gilt eigentlich $I = \langle G \rangle$?
- Genügt eine Gröbnerbasis unserer Idee?

# 9. Satz A

Gegeben:

- $\mathcal{G} = \{g_1, \ldots, g_k\} \subset I$ Gröbnerbasis von $I$,
- $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine Division mit Rest.

Dann gilt: a. $f \in I \iff r = 0$.

b. $I = \langle \mathcal{G} \rangle$.

# 9. Satz A

Gegeben:

- $\mathcal{G} = \{g_1, \ldots, g_k\} \subset I$ Gröbnerbasis von $I$,
- $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine Division mit Rest.

Dann gilt: a. $f \in I \iff r = 0$.

b. $I = \langle \mathcal{G} \rangle$.

Beweis: a. "$\Longleftarrow$"

$$r = 0 \implies f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k \in I.$$

# 9. Satz A

Gegeben:

- $\mathcal{G} = \{g_1, \ldots, g_k\} \subset I$ Gröbnerbasis von $I$,
- $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine Division mit Rest.

Dann gilt: a. $f \in I \iff r = 0$.

b. $I = \langle \mathcal{G} \rangle$.

Beweis: a. "$\Longrightarrow$"

$$0 \neq r = f - q_1 \cdot g_1 - \ldots - q_k \cdot g_k \in I$$

$$\Longrightarrow \quad 0 \neq \mathrm{lm}(r) \in L(I) = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_r) \rangle$$

im Widerspruch zu ID2.

# 9. Satz A

Gegeben:

- $\mathcal{G} = \{g_1, \ldots, g_k\} \subset I$ Gröbnerbasis von $I$,
- $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine Division mit Rest.

Dann gilt: a. $f \in I \iff r = 0$.

b. $I = \langle \mathcal{G} \rangle$.

Beweis:

b. Sei $f \in I$ und $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine DmR.

# 9. Satz A

Gegeben:

- $\mathcal{G} = \{g_1, \ldots, g_k\} \subset I$ Gröbnerbasis von $I$,
- $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine Division mit Rest.

Dann gilt: a. $f \in I \iff r = 0$.

b. $I = \langle \mathcal{G} \rangle$.

Beweis:

b. Sei $f \in I$ und $f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$ eine DmR.

Aus a. folgt dann $r = 0$ und somit

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k \in \langle \mathcal{G} \rangle.$$

# 10. Satz B – verallgemeinert FSdA

Sei $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ mit Gröbnerbasis $\mathcal{G}$. Dann

$$\#V(f_1, \ldots, f_k) = \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/L(I) \right)$$

$$= \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/\langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle \right).$$

# 10. Satz B – verallgemeinert FSdA

Sei $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ mit Gröbnerbasis $\mathcal{G}$. Dann

$$\#V(f_1, \ldots, f_k) = \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/L(I) \right)$$

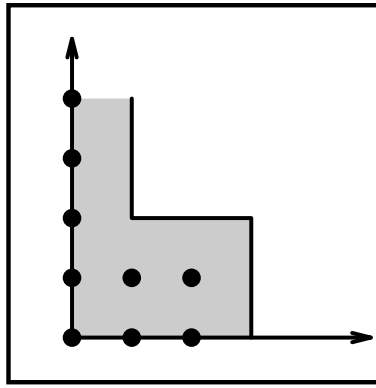
$$= \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/\langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle \right).$$

Beispiel: $f_1 = x^3 + xy, \quad f_2 = xy^2 + 2xy, \quad I = \langle f_1, f_2 \rangle.$

$\mathcal{G} = \{f_1, f_2\}$ ist Gröbnerbasis, $L(I) = \langle x^3, xy^2 \rangle$,

$\{x, x^2, xy, x^2y, y^i \mid i \in \mathbb{N}\}$ $\mathbb{Q}$-Basis von $R/L(I)$.

Also: $\#V(f_1, f_2) = \infty$ – $\{x = 0\} \subset V(f_1, f_2)$.



# 10. Satz B – verallgemeinert FSdA

Sei $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ mit Gröbnerbasis $\mathcal{G}$. Dann

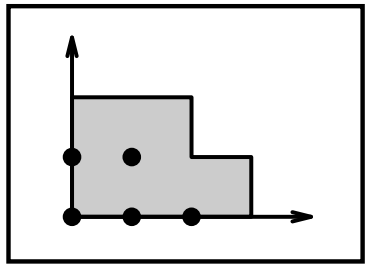
$$\#V(f_1, \ldots, f_k) = \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/L(I) \right)$$

$$= \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/\langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle \right).$$

Beispiel: $f_1 = x^3 + x^2y, \quad f_2 = x^2y + xy^4, \quad f_3 = y^2 + y.$

$\mathcal{G} = \{f_1, f_2, f_3\}$ ist Gröbnerbasis, $L(I) = \langle x^3, x^2y, y^2 \rangle$,

$\{1, x, x^2, y, xy\}$ $\mathbb{Q}$-Basis von $R/L(I)$.



Also: $\#V(f_1, f_2, f_3) = 5$ .

# 10. Satz B – verallgemeinert FSdA

Sei $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ mit Gröbnerbasis $\mathcal{G}$. Dann

$$\#V(f_1, \ldots, f_k) = \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/L(I) \right)$$

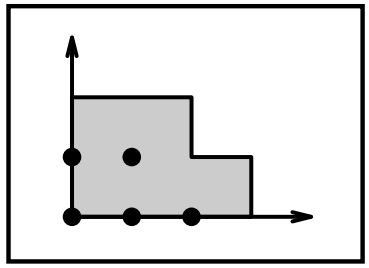
$$= \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/\langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle \right).$$

Beispiel: $f_1 = x^3 + x^2y, \quad f_2 = x^2y + xy^4, \quad f_3 = y^2 + y.$

$\mathcal{G} = \{f_1, f_2, f_3\}$ ist Gröbnerbasis, $L(I) = \langle x^3, x^2y, y^2 \rangle$,

$\{1, x, x^2, y, xy\}$ $\mathbb{Q}$-Basis von $R/L(I)$.

Also: $V(f_1, f_2, f_3) = \{(0,1), (-1,1), 3\mathsf{x}(0,0)\}$ .



# 10. Satz B – verallgemeinert FSdA

Sei $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ mit Gröbnerbasis $\mathcal{G}$. Dann:

$$\#V(f_1, \ldots, f_k) = \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/L(I) \right)$$

$$= \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/\langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle \right).$$

Insbesondere:

$$\#V(f_1, \ldots, f_k) < \infty \iff \forall\, i = 1, \ldots, n\ \exists\, \alpha_i \ : \ x_i^{\alpha_i} \in L(I) = L(G)$$

$$\iff \forall\, i = 1, \ldots, n\ \exists\, g \in \mathcal{G} \ : \ \mathrm{lm}(g) \in \mathbb{Q}[x_i]$$

$$\iff \forall\, i\ \exists\, g_i \in \mathcal{G}$$ "nur von $x_i, \ldots, x_n$ abhängi

# 10. Satz B – verallgemeinert FSdA

Sei $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ mit Gröbnerbasis $\mathcal{G}$. Dann

$$\#V(f_1, \ldots, f_k) = \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/L(I) \right)$$

$$= \dim_{\mathbb{Q}} \left( \mathbb{Q}[x_1, \ldots, x_n]/\langle \mathrm{lm}(g) \mid g \in \mathcal{G} \rangle \right).$$

Quintessenz:

Wenn wir Gröbnerbasen berechnen können, können wir Gleichungssysteme lösen – modulo Numerik!

# 11. Wie berechnet man Gröbnerbasen

Notation:

- $\mathrm{kgV}(x^\alpha, x^\beta) = x_1^{\max\{\alpha_1,\beta_1\}} \cdots x_n^{\max\{\alpha_n,\beta_n\}}$.
- $\mathrm{spoly}(f,g) = \frac{\mathrm{kgV}\left(\mathrm{lm}(f),\mathrm{lm}(g)\right)}{\mathrm{lt}(f)} \cdot f - \frac{\mathrm{kgV}\left(\mathrm{lm}(f),\mathrm{lm}(g)\right)}{\mathrm{lt}(g)} \cdot g$.

# 11. Wie berechnet man Gröbnerbasen

Notation:

- $\mathrm{kgV}(x^\alpha, x^\beta) = x_1^{\max\{\alpha_1,\beta_1\}} \cdots x_n^{\max\{\alpha_n,\beta_n\}}$.
- $\mathrm{spoly}(f,g) = \frac{\mathrm{kgV}\left(\mathrm{lm}(f),\mathrm{lm}(g)\right)}{\mathrm{lt}(f)} \cdot f - \frac{\mathrm{kgV}\left(\mathrm{lm}(f),\mathrm{lm}(g)\right)}{\mathrm{lt}(g)} \cdot g$.

Beispiel: $f = x^3 + x^2y$, $g = x^2y + xy^4$.

$$\mathrm{spoly}(f,g) = \frac{x^3y}{x^3}\cdot(x^3+x^2y) - \frac{x^3y}{x^2y}\cdot(x^2y+xy^4) = x^2y^2 - x^2y^4.$$

# 11. Wie berechnet man Gröbnerbasen

Notation:

- $\mathrm{kgV}(x^\alpha, x^\beta) = x_1^{\max\{\alpha_1,\beta_1\}} \cdots x_n^{\max\{\alpha_n,\beta_n\}}$.
- $\mathrm{spoly}(f,g) = \frac{\mathrm{kgV}\left(\mathrm{lm}(f),\mathrm{lm}(g)\right)}{\mathrm{lt}(f)} \cdot f - \frac{\mathrm{kgV}\left(\mathrm{lm}(f),\mathrm{lm}(g)\right)}{\mathrm{lt}(g)} \cdot g$.

Buchberger-Kriterium: $\mathcal{G} = \{g_1, \ldots, g_k\}$ ist Gröbnerbasis

$\Longleftrightarrow \quad \forall\, i \neq j \;:\; \mathrm{spoly}(g_i, g_j)$ hat Rest null bei DmR bezüglich

# 12. Buchberger-Algorithmus

Input: $f_1, \ldots, f_k$.

Output: $g_1, \ldots, g_l$ Gröbnerbasis von $\langle f_1, \ldots, f_k \rangle$.

- $S = \{f_1, \ldots, f_k\}$, $P = \{(f, g) \mid f, g \in S, f \neq g\}$.
- Solange $P \neq \emptyset$:
  - Wähle $(f, g) \in P$ und setze $P = P \setminus \{(f, g)\}$.
  - Wenn $r := Rest\big(\operatorname{spoly}(f, g), S\big) \neq 0$, dann
    - $P = P \cup \{(r, f) \mid f \in S\}$
    - $S = S \cup \{r\}$
- Gib $S$ zurück.

# 13. Wie berechnet man den "Rest"?

Input: $f, f_1, \ldots, f_k$.

Output: $r$, Rest von $f$ bei DmR durch $f_1, \ldots, f_k$.

- $r = f$
- Solange $r \neq 0$ und $\exists\, i \;:\; \mathrm{lm}(f_i) \mid \mathrm{lm}(r)$
  - Wähle so ein $f_i$.
  - $r := \frac{\mathrm{spoly}(r, f_i)}{\mathrm{lc}(f_i)} = r - \frac{\mathrm{lt}(r)}{\mathrm{lt}(f_i)} \cdot f_i$.
- Gib $r$ zurück.

# 14. Verallgemeinerung von Satz B

$$\dim\big(V(I)\big) = 0 \iff \#V(I) < \infty$$

$$\iff L(I) \cap \mathbb{Q}[x_i] \neq \{0\} \ \ \forall\, i = 1, \ldots, n$$

# 14. Verallgemeinerung von Satz B

$$\dim\big(V(I)\big) = 0 \iff \#V(I) < \infty$$

$$\iff L(I) \cap \mathbb{Q}[x_i] \neq \{0\} \ \ \forall\, i = 1, \ldots, n$$

Insbesondere:

$$\max\left\{m \;\middle|\; \exists\, i_1 < \ldots < i_m \ : L(I) \cap \mathbb{Q}[x_{i_1}, \ldots, x_{i_m}] = \{0\}\right\} = 0$$

# 14. Verallgemeinerung von Satz B

Für $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ beliebig gilt

$$\dim\left(V(I)\right) = \max\left\{m \;\middle|\; \exists\, i_1 < \ldots < i_m \;:\; L(I) \cap \mathbb{Q}[x_{i_1}, \ldots, x_{i_m}] = \{0$$

Wir nennen $\{x_{i_1}, \ldots, x_{i_m}\}$ eine maximal unabhängig.

# 14. Verallgemeinerung von Satz B

Für $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$ beliebig gilt

$$\dim\big(V(I)\big) = \max\big\{m \;\big|\; \exists\, i_1 < \ldots < i_m \;:\; L(I) \cap \mathbb{Q}[x_{i_1}, \ldots, x_{i_m}] = \{0$$

Wir nennen $\{x_{i_1}, \ldots, x_{i_m}\}$ eine maximal unabhängig.

Beachte: Ist $\mathcal{G}$ eine Gröbnerbasis von $I$, dann gilt

$$L(I) \cap \mathbb{Q}[x_{i_1}, \ldots, x_{i_m}] = \{0\} \quad \Longleftrightarrow \quad \nexists\, x_{i_1}^{\alpha_1} \cdots x_{i_m}^{\alpha_m} \in \{\mathrm{lm}(g) \mid g \in G\}$$

# 15. Polynomiale Abbildungen

$f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$ definieren zwei Abbildungen:

- $\varphi : \mathbb{C}^n \to \mathbb{C}^k : a \mapsto \big(f_1(a), \ldots, f_k(a)\big)$
- $\varphi^* : \mathbb{Q}[y_1, \ldots, y_k] \to \mathbb{Q}[x_1, \ldots, x_n] : g \mapsto g(f_1, \ldots, f_k)$.

# 15. Polynomiale Abbildungen

$f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$ definieren zwei Abbildungen:

- $\varphi : \mathbb{C}^n \to \mathbb{C}^k : a \mapsto \big(f_1(a), \ldots, f_k(a)\big)$
- $\varphi^* : \mathbb{Q}[y_1, \ldots, y_k] \to \mathbb{Q}[x_1, \ldots, x_n] : g \mapsto g(f_1, \ldots, f_k)$.

Fragen:

- Ist $\varphi\big(V(I)\big)$ wieder eine Varietät?
- Wie hängen $\varphi$ und $\varphi^*$ zusammen?

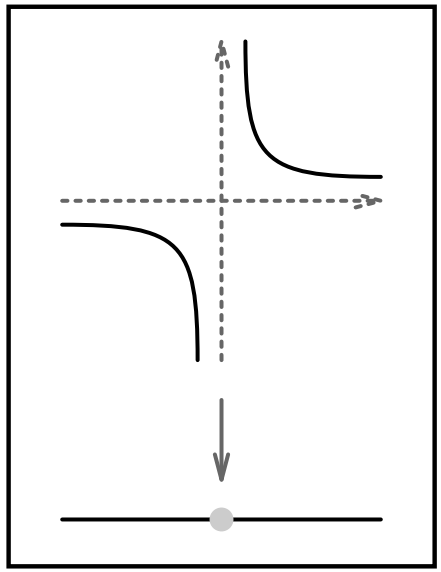
# 15. Polynomiale Abbildungen

Fragen:

- Ist $\varphi\big(V(I)\big)$ wieder eine Varietät?
- Wie hängen $\varphi$ und $\varphi^*$ zusammen?

Beispiel:

- $I = \langle xy - 1 \rangle$.
- $\varphi : \mathbb{C}^2 \to \mathbb{C} : (x, y) \mapsto x$.
- $\varphi\big(V(I)\big) = \mathbb{C} \setminus \{0\}$ ist keine Varietät.
- Wohl aber $\overline{\varphi\big(V(I)\big)} = \mathbb{C}$.



# 15. Polynomiale Abbildungen

Fragen:

- Ist $\varphi\big(V(I)\big)$ wieder eine Varietät?
- Wie hängen $\varphi$ und $\varphi^*$ zusammen?

Satz C:

Der topologische Abschluß $\overline{\varphi\big(V(I)\big)}$ ist eine Varietät und $\varphi\big(V(I)\big)$ liegt dicht darin.

Bemerkung: Für $V_{\mathbb{R}^n}(I)$ gilt das leider nicht mehr!

# 15. Polynomiale Abbildungen

Fragen:

- Ist $\varphi\big(V(I)\big)$ wieder eine Varietät?
- Wie hängen $\varphi$ und $\varphi^*$ zusammen?

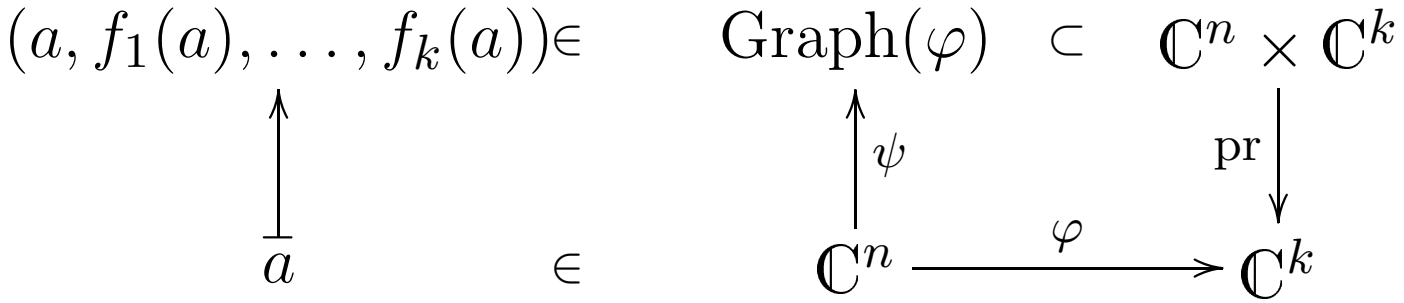
Satz C:

Der topologische Abschluß $\overline{\varphi\big(V(I)\big)}$ ist eine Varietät und $\varphi\big(V(I)\big)$ liegt dicht darin.

Beweisidee: Zeige $\overline{\varphi\big(V(I)\big)} = V\big((\varphi^*)^{-1}(I)\big)$!

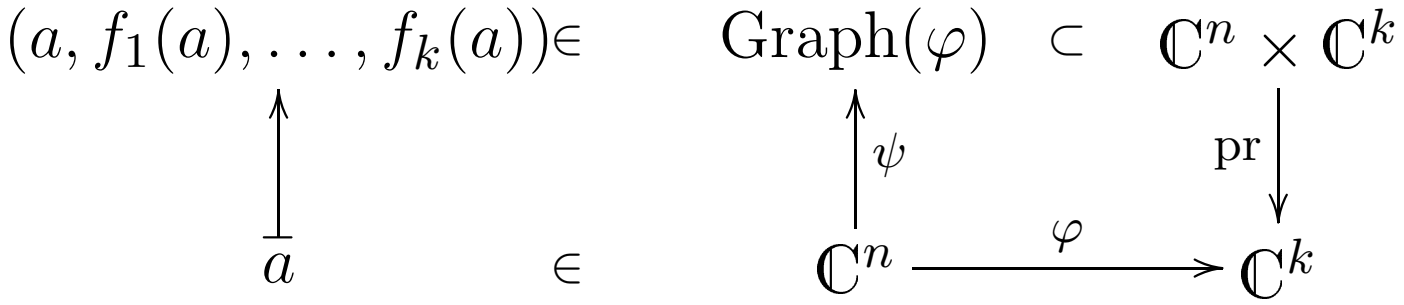
# 15. Polynomiale Abbildungen

Genauer – betrachte den Graphen von $\varphi$



# 15. Polynomiale Abbildungen

Genauer – betrachte den Graphen von $\varphi$




Dann gilt $\psi\big(V(I)\big) = V\big(I + J\big)$, wobei

$$J = \langle y_1 - f_1, \ldots, y_k - f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_k]$$

und

$$\varphi\big(V(I)\big) = \mathrm{pr}\,\big(V(I + J)\big).$$

# 15. Polynomiale Abbildungen

Dann gilt $\psi\big(V(I)\big) = V\big(I + J\big)$, wobei

$$J = \langle y_1 - f_1, \ldots, y_k - f_k \rangle \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_k]$$

und

$$\varphi\big(V(I)\big) = \mathrm{pr}\,\big(V(I + J)\big).$$

Schließlich gilt für eine Projektion:

$$\overline{\mathrm{pr}\,\big(V(I + J)\big)} = V\big((I + J) \cap \mathbb{Q}[y_1, \ldots, y_k]\big),$$

# 15. Polynomiale Abbildungen

Schließlich gilt für eine Projektion:

$$\overline{\mathrm{pr}\left(V(I+J)\right)} = V\big((I+J)\cap\mathbb{Q}[y_1,\ldots,y_k]\big),$$

das heißt, man kann $(\varphi^*)^{-1}(I) = (I+J)\cap\mathbb{Q}[y_1,\ldots,y_k]$ durch Elimination berechnen:

Berechne eine Gröbnerbasis von $I+J$ und streiche alle Polynome, die von einem $x_i$ abhängen.

# 16. Zusammenfassung

1. Gröbnerbasen + Numerik lösen $f_1 = \ldots = f_k = 0$, falls endlich.

# 16. Zusammenfassung

1. Gröbnerbasen + Numerik lösen $f_1 = \ldots = f_k = 0$, falls endlich.

2. Gröbnerbasen liefern stets die Dimension der Lösungsmenge.

# 16. Zusammenfassung

1. Gröbnerbasen + Numerik lösen $f_1 = \ldots = f_k = 0$, falls endlich.

2. Gröbnerbasen liefern stets die Dimension der Lösungsmenge.

3. Gröbnerbasen liefern Gleichungen für das Bild einer Abbildung.