4.1.2. Beispiel

Die Rest-gleich-Null-Bedingung für $S(f_i, f_j)$ (für gegebene i, j) ist i.A. nicht äquivalent zur Bedingung aus dem vorigen Theorem.

$$f_1 = xz + 1$$

$$f_2 = yz + 1$$

$$f_3 = xz - x + y + 1$$

Lex-Ordnung.

$$S(f_1, f_2) = yf_1 - xf_2 = y - x$$

Beim Teilen von $S(f_1, f_2)$ durch (f_1, f_2, f_3) kommen y ~~und~~ $-x$ in den Rest.

$$y - x = (-1)\cdot f_1 + 0\cdot f_2 + 1\cdot f_3$$

$$\operatorname{mdeg}((-1)\cdot f_1) = (1,0,1) \lessgtr (1,1,1) = \operatorname{mdeg}(f_1) \vee \operatorname{mdeg}(f_2) = (1,0,1) \vee (0,1,1)$$

$$\operatorname{mdeg}(0\cdot f_2) = -\infty \lessgtr (1,1,1)$$

$$\operatorname{mdeg}(1\cdot f_3) = (1,0,1) \lessgtr (1,1,1).$$

4.2. Der schwache Nullstellensatz.

$f_1 = \ldots = f_s = 0$ lösbar in $\mathbb{C}^n$ $\iff$

$V(I) \neq \emptyset$ für $I = \langle f_1, \ldots, f_s \rangle$.

Im Fall $n = 1$ haben eine Antwort zur

Frage: $V(I) \neq \emptyset$?

Im klassischen Fall gilt:

$$V(I) = V(\langle f_1, \dots, f_s \rangle) = V(\langle \operatorname{ggT}(f_1, \dots, f_s) \rangle)$$
$$= V(\underbrace{\operatorname{ggT}(f_1, \dots, f_s)}_{\underset{g}{\shortparallel}}).$$

Ist g keine Nichtnullkonstante ($g \notin \mathbb{C} \setminus \{0\}$), dann besitzt g eine Nullstelle in $\mathbb{C}$. Diese Nullstelle liegt in $V(I)$.

Ist $g \in \mathbb{C} \setminus \{0\}$, dann können wir $g = 1$ setzen, dann heißt es

$$1 = h_1 f_1 + \dots + h_s f_s$$ gilt

für gewisse $h_1, \dots, h_s \in \mathbb{C}[x]$.

Das bedeutet $V(I) = V(1) = \emptyset$.

Die Antwort im univariaten Fall:
Für ein Ideal $I \subseteq \mathbb{C}[x]$ gilt:

$$V(I) = \emptyset \iff 1 \notin I \iff I = \mathbb{C}[x].$$

Erstaunlicherweise gelten diese Äquivalenzen genauso im multivariaten Fall.
Das ist der schwache Nullstellensatz.

4.2.1. Lemma Sei $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ Ideal mit $1 \notin I$. Dann existiert ein $a \in \mathbb{C}$ mit

$$1 \notin I(x_1, \ldots, x_{n-1}, a).$$

Beweis: $\underline{x} := (x_1, \ldots, x_{n-1})$.

Fall 1: $I \cap \mathbb{C}[x_n] \neq \{0\}$, das bedeutet, das Ideal I enthält ein Nichtnullpolynom, das nur von x_n abhängig ist. Sei $f \in (I \cap \mathbb{C}[x_n]) \setminus \{0\}$ ein solches Polynom. OBdA sei der Leitkoeffizient von f gleich 1. Wegen $1 \notin I$ ist $f \neq 1$. Das heißt, f ist Polynom vom Grad mindestens 1. Nach dem Fundamentalen Satz von Algebra lässt sich f als

$$f = (x_n - b_1)^{m_1} \cdot \ldots \cdot (x_n - b_r)^{m_r}$$

faktorisieren, mit $b_1, \ldots, b_r \in \mathbb{C}$ und $m_1, \ldots, m_r \in \mathbb{N}$. Damit $1 \notin I(\underline{x}, a)$ erfüllt ist, <u>müssen</u> wir $a = b_i$ für ein $i = 1, \ldots, r$ festlegen. Denn für $a \in \mathbb{C} \setminus \{b_1, \ldots, b_r\}$ ist $f(a) \in \mathbb{C} \setminus \{0\}$, sodass $1 \in I(\underline{x}, a)$ hat.

Wir führen ein Widerspruchsbeweis.

Angenommen, kein b_i wäre als ein mögliches Wert für a geeignet. Das heißt: $f \in I(\underline{x}, b_i)$ für alle $i = 1, \dots, r$.

Das bedeutet $1 = B_i(\underline{x}, b_i)$ für ein $B_i \in I$ ($i = 1, \dots, r$). Wir schreiben die 1 als

$$1 = B_i(\underline{x}, b_i) = \underbrace{B_i(\underline{x}, b_i) - B_i(\underline{x}, x_n)} + B_i$$

Die Differenz $B_i(\underline{x}, b_i) - B_i(\underline{x}, x_n)$ ist $\mathbb{C}$-Linearkombination der Polynome

$$\underline{x}^\alpha b_i^m - \underline{x}^\alpha x_n^m = \begin{cases} 0, & \text{für } m = 0 \\ \underline{x}^\alpha (b_i - x_n) \sum_{t=1}^{m-1} b_i^t x_n^{m-1-t}, & \text{für } m > 0 \end{cases}$$

$$\boxed{b^4 - a^4 = (b-a)(b^3 + b^2 a + b a^2 + a^3)}$$

Das bedeutet $B_i(\underline{x}, b_i) - B_i(\underline{x}, x_n) = (x_n - b_i) \cdot A_i$

für ein $A_i \in \mathbb{C}[x_1, \ldots, x_n]$. $\Longrightarrow$

$$f = \prod_{i=1}^{r} B_i(\underline{x}, b_i)^{m_i} = \underbrace{\prod_{i=1}^{r} \big((x_n - b_i) \cdot A_i + \underbrace{B_i}_{\in I} \big)^{m_i}}_{\text{Wir multiplizieren dieses Produkt aus.}}$$

Wir erhalten $2^{m_1 + \ldots + m_r}$ Terme

All die Terme, die eines der B_i's als Faktor enthalten, gehören zu I, denn $B_i \in I$. Der Term, der noch übrig bleibt, ist

$$\prod_{i=1}^{r} \big((x_n - b_i) \cdot A_i \big)^{m_i} = \left(\prod_{i=1}^{r} A_i^{m_i} \right) \prod_{i=1}^{r} (x_n - b_i)^{m_i}$$

Weil $\prod_{i=1}^{r} (x_n - b_i)^{m_i} = f \in I$ gilt,

gehört auch dieser Term zu I.

$\Rightarrow 1 \notin I$, $\lightning$ zu den Voraussetzungen.

Dieser Widerspruch zeigt, dass

$1 \notin I(\underline{x}, b_i)$ für ein $i = 1, \dots, r$

erfüllt ist.

Fall 2: $I \cap \mathbb{C}[x_n] = \{0\}$. Sei $G = \{g_1, \dots, g_t\}$

Gröbnerbasis von I bzgl. der Lex-Ordnung.

Sei $c_i \in \mathbb{C}[x_n] \setminus \{0\}$ der Leitterm (bzgl.

der Lex-Ordnung) von g_i als Polynom

in $\underline{x} = (x_1, \dots, x_{n-1})$ und sei $d_i \in \mathbb{Z}_{\geq 0}^{n-1}$

der entsprechende Multigrad von g_i also Polynom in $\underline{x}$

Da jedes c_i nur endlich viele Nullstellen besitzt, gibt es ein $a \in \mathbb{C}$ mit $c_i(a) \neq 0$ für alle $i = 1, \dots, t$.

Da $g_1, \dots, g_t$ das Ideal I erzeugen, erzeugen die Polynom $\underline{g_i} = g_i(\underline{x}, a)$ das Ideal $I(\underline{x}, a)$. Nach der Wahl von a ist $c_i(a)\underline{x}^{d_i}$ der Leitterm von $\underline{g_i}$.

Des Weiteren ist $\underline{g_i} \notin \mathbb{C}$, denn sonst wäre $g_i(x_1, \dots, x_n) = c_i(x_n)$. Dann wäre aber $c_i = g_i \in I \cap \mathbb{C}[x_n]$, $\lightning$ zur Voraussetzung im Fall 2.

<u>Hilfsbehauptung.</u> $\{\underline{g_1}, \dots, \underline{g_t}\}$ ist Gröbnerbasis von $I(\underline{x}, a)$ bzgl. der lex-Ordnung

<u>Beweis der Hilfsbehauptung:</u> Wir betrachten für $1 \le i < j \le t$ das Polynom

$$S := c_j(x_n)\frac{\underline{x}^{d_i \vee d_j}}{\underline{x}^{d_i}}\, g_i \;-\; c_i(x_n)\frac{\underline{x}^{d_i \vee d_j}}{\underline{x}^{d_j}}\, g_j .$$

Also Polynom in $\underline{x} = (x_1, \dots, x_{n-1})$ mit Koeffizienten in $\mathbb{C}[x_n]$ hat S den Multigrad $\preceq d_i \vee d_j$ bzgl. der Lex-Ordnung. Weil aber in der Differenz die Leitterme kompensiert sind, ist der Multigrad sogar $\prec d_i \vee d_j$ bzgl. der Lex-Ordnung.

Für die Lex-Ordnung Ordnung bzgl. $(x_1, \dots, x_n)$ gilt sowieso

$$\operatorname{mdeg}(S) < (d_i \vee d_j, 0).$$

Nach der Konstruktion liegt S in I und hat somit die Standarddarstellung

$$S = \sum_{\ell=1}^{t} A_\ell g_\ell .$$

Die Spezialisierung von S für $x_n = a$ ergibt

$$\underline{S} := S(\underline{x}, a) = c_j(a) \frac{\underline{x}^{d_i \vee d_j}}{\underline{x}^{d_i}} \underline{g_i} - c_i(a) \frac{\underline{x}^{d_i \vee d_j}}{\underline{x}^{d_j}} \underline{g_j}$$

Andererseits gilt

$$\underline{S} = \sum_{\ell=1}^{t} \underline{A_\ell}\, \underline{g_\ell} \quad \text{mit} \quad \underline{A_\ell} = A_\ell(\underline{x}, a).$$

$\underline{S}$ ist bis auf eine Konstante das S-Polynom von $\underline{g_i}$ und $\underline{g_j}$: $\underline{S} = c_i(a)\, c_j(a)\, S(\underline{g_i}, \underline{g_j})$

Wir haben also

$$(d_i \vee d_j, 0) \leq \mathrm{mdeg}(S) \lneq \mathrm{mdeg}(A_\ell g_\ell)$$

Daraus folgt

$$d_i \vee d_j \leq \mathrm{mdeg}(\underline{A}_\ell \underline{g}_\ell).$$

D.h., die Bedingung des modifizierten Schreyer-Kriteriums ist erfüllt (Theorem 4.1.1)

$\Longrightarrow \{\underline{g}_1, \dots, \underline{g}_t\}$ Gröbnerbasis von $I(\underline{x}, a)$. ◆

$\underline{g}_1, \dots, \underline{g}_t$ bilden Gröbnerbasis von $I(\underline{x}, a)$.
Um die Bedingung $1 \in I(\underline{x}, a)$ zu entscheiden, reicht es aus 1 durch $\{\underline{g}_1, \dots, \underline{g}_t\}$ mit Rest zu teilen. Oben haben wir festgestellt, dass $\underline{g}_1, \dots, \underline{g}_t$ keine Konstanten sind.

Die Leitkoeffizienten von $\underline{g}_1, \dots, \underline{g}_t$ sind keine Konstanten. D.h. Beim Teilen von 1 durch $\{\underline{g}_1, \dots, \underline{g}_t\}$ kommt 1 direkt in den Rest.

D.h. Bedeutet $1 \notin I(\underline{x}, \underline{a})$. $\square$

4.2.2. Theorem (Der schwache Nullstellensatz)

Für jedes Ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ sind die folgenden Bedingungen äquivalent

(i) $V(I) = \emptyset$

(ii) $I = \mathbb{C}[x_1, \dots, x_n]$

(iii) $1 \in I$

<u>Beweis:</u> (ii) $\Leftrightarrow$ (iii) ist klar.

(iii) $\Rightarrow$ (i) ist auch klar.

Um (i) $\Rightarrow$ (iii) zu zeigen, zeigen wir nicht (iii) $\Rightarrow$ nicht (i).

Sei $1 \notin I$. Wir können mit Hilfe von Lemma 4.2.1 für $x_n, \dots, x_1$ iterativ Werte $a_n, \dots, a_1$ fixieren, so dass in der $i$ten Iteration $1 \notin I(x_1, \dots, x_i, a_{i+1}, \dots, a_n)$.

In der letzten Iteration gilt

$$1 \notin I(a_1, \dots, a_n) \subseteq \mathbb{C}.$$

$$\Rightarrow \quad I(a_1, \dots, a_n) = \{0\}$$

$$\Longleftrightarrow \quad f(a_1, \dots, a_n) = 0 \text{ für alle } f \in I.$$

$$\Longleftrightarrow \quad (a_1, \dots, a_n) \in V(I).$$

$\square$

4.2.3. Bemerkung.

Aus dem schwachen Nullstellensatz folgt, dass man $V(f_1, \dots, f_s) = \emptyset$ im Fall $k = \mathbb{C}$ mit Gröbner-Basen entscheiden kann. Man bestimmt die Gröbner-Basis $g_1, \dots, g_t$ von $\langle f_1, \dots, f_s \rangle$ und testet anschließend mit Hilfe des Teilens, ob $1 \in \langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_s \rangle$ gilt.

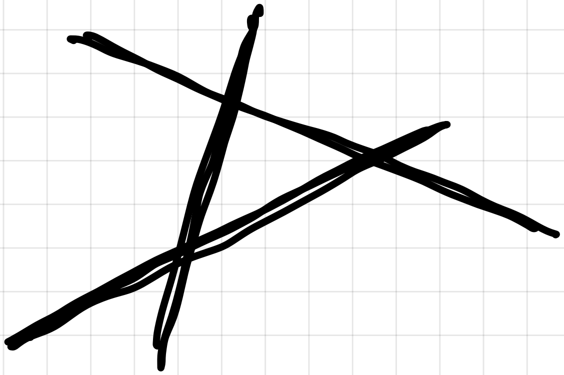
Sogar einfacher:

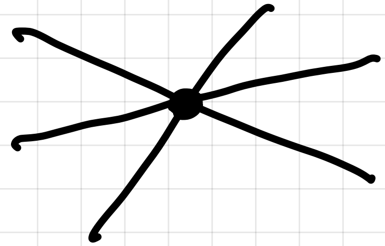
$1 \in I \iff$ die Gröbner-Basis von I enthält 1

$\iff$ Die reduzierte Gröbner-Basis ist $\{1\}$.

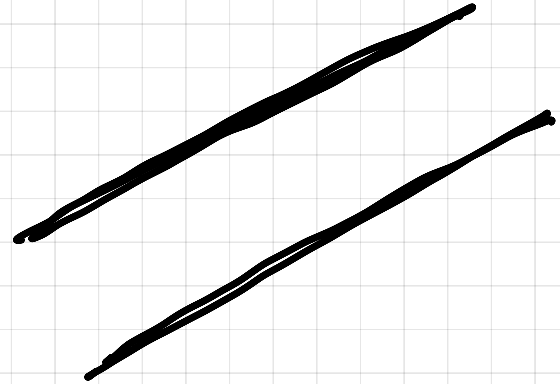
4.2.4 Beispiel.

(i)





(ii)



$$\boxed{\begin{aligned} f &= 2x^2 + 3y - 7 \\ g &= x^2 + y^4 - 10 \\ h &= 2x^2 + 4y^3 - 1 \end{aligned}}$$

```
I = R.ideal((f, g, h)).
```

```
I.groebner_basis()
```

```
R(1).lift([f, g, h])
```

4.2.5 Bemerkung. Nach dem schwachen Nullstellensatz hat ein System $f_1 = \ldots = f_s = 0$ ($f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$), das über $\mathbb{C}^n$ nicht lösbar ist, einen Nachweis der Unlösbarkeit in der Form

$$h_1 f_1 + \ldots + h_s f_s = 1$$

für gewisse $h_1, \ldots, h_s \in \mathbb{C}[x_1, \ldots, x_n]$.

Die Polynome $h_1, \ldots, h_s$ können im Rahmen des Buchberger-Algorithmus ausgerechnet werden, wenn im Buchberger-Algorithmus während des Teilens die Quotienten aufgehoben werden.

$$f_1, f_2, f_3, f_4$$

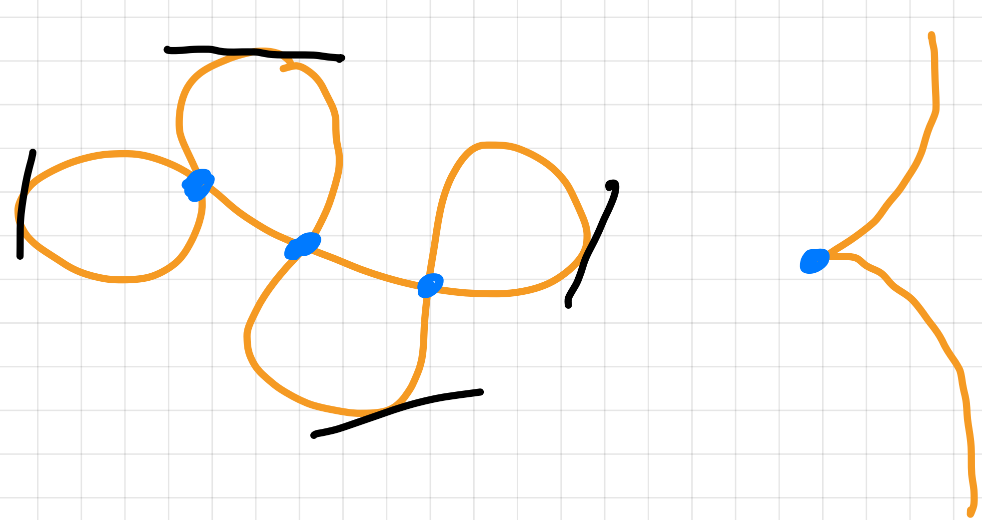
$$\mathrm{Rem}(S(f_1, f_2); f_1, f_2, f_3, f_4) =: f_5$$

$$\underbrace{a_1 f_1 + a_2 f_2}_{= S(f_1, f_2)} = q_1 f_1 + q_2 f_2 + q_3 f_3 + q_4 f_4 + f_5$$

$$\Longrightarrow \quad f_5 = b_1 f_1 + b_2 f_2 + b_3 f_3 + b_4 f_4$$

Aber in SageMath steht dafür die lift-Methode zur Verfügung.

4.2.6. Beispiel.



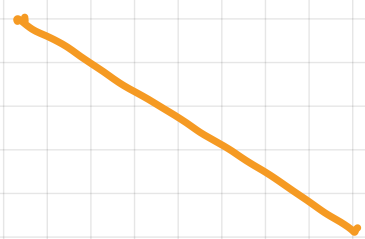
Varietäten der Form

$V(f)$ für $f \in \mathbb{C}[x_1,\dots,x_n] \setminus \mathbb{C}$, nennt man Hyperflächen (im Fall $n=3$ – Flächen, im Fall $n=2$ – ebene Kurven).

$$V\big((x-y+1)^2\big)$$

$$\shortparallel$$

$$V(x-y+1)$$



Wir nennen $f \in \mathbb{C}[x_1,\dots,x_n] \setminus \mathbb{C}$ quadratfrei, wenn f nicht durch das Quadrat eines Polynoms aus $\mathbb{C}[x_1, \dots, x_n] \setminus \mathbb{C}$ teilbar ist.

Es kann gezeigt werden, dass jede Hyperfläche durch ein quadratfreies Polynom definiert werden kann und dass so eine Darstellung bis auf Konstanten eindeutig ist.

Ist $V(f)$ eine Hyperfläche, die durch ein quadratfreies Polynom f definiert ist $\in \mathbb{C}[x_1, \dots, x_n] \setminus \mathbb{C}$,

so nennt man einen Punkt $a \in V(f)$ singulär, wenn $\nabla f(a) = \left(\frac{\partial f}{\partial x_1}(a), \dots, \frac{\partial f}{\partial x_n}(a)\right) = (0, \dots, 0)$.

$V\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)$ ist die Menge aller singulären Punkte von $V(f)$.

(i) $y^2 - x^2(1-x) = 0$

4.2.7. Aufgabe

Parametrisierte Kurve.

$$x = \frac{1-t}{2+t^2}, \quad y = \frac{1-t^3}{3+t^4}$$

Gibt's singuläre Punkte?
Ggf. wie viele?
und wo liegen sie?

SageMath kann/soll dafür benutzt werden.

Wir finden zuerst die implizite Beschreibung.

Wir haben implizitiert, kommen auf ein $f \in \mathbb{C}[x,y]$, das die Kurve als $V(f)$ beschreibt.

$$
\begin{cases}
(1) & x^2 - x + \frac{59}{84} y = 0 \\
(2) & xy - \frac{5}{14} y = 0 \\
(3) & y^2 - \frac{135}{413} y = 0
\end{cases}
$$

Das ist das System für $V\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$.

$$(3) \Rightarrow y \in \left\{0, \frac{135}{413}\right\}$$

$y = 0$: $\quad x = 0$, $\quad x = 1$

$y = \frac{135}{413}$ $\Downarrow$ $x = \frac{5}{14}$

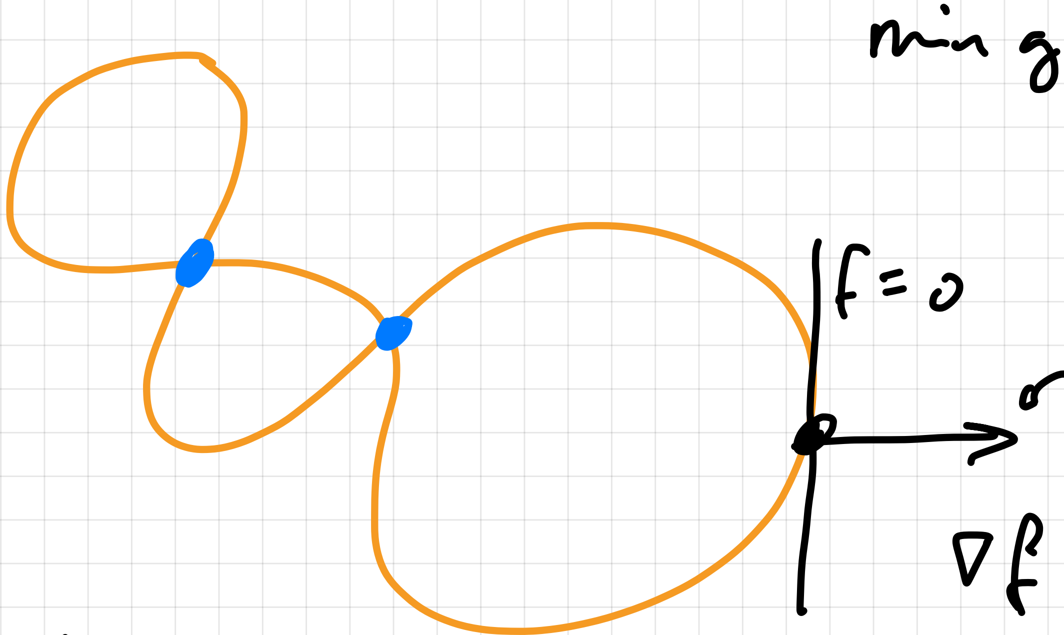
$$x(x-1) + \frac{59}{84} y \overset{?}{=} 0$$

$$\underbrace{-\frac{5}{14} \cdot \frac{9}{14}}_{\frac{45}{196}} + \underbrace{\frac{59}{84} \cdot \frac{135}{413}}_{\frac{45}{196}} \overset{?}{=} 0$$

$$(0,0), \quad (1,0), \quad \left(\frac{5}{14}, \frac{135}{413}\right).$$

Drei singuläre Punkte!

Singuläre Punkte sind Ausnahmen in den KKT-Bedingungen.



$\nabla f \neq 0$

$\Downarrow$

∇f und ∇g parallel ist notwendig für ein lokales Minimum

Durch den Hilbertschen Nullstellensatz und Gröbnerbasen können wir solche Ausnahmen abfangen.

4.3. Der starke Nullstellensatz

$$f_1 = \dots = f_s = 0 \overset{?}{\Longrightarrow} f = 0$$

__4.3.1. Theorem__ (Der starke Nullstellensatz, Formulierung 1).

Seien $f, f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$. Dann sind die folgenden Bedingungen äquivalent:

(i) $f \in \underline{I}(V(f_1, \ldots, f_s))$

(ii) $f^m \in \langle f_1, \ldots, f_s \rangle$ gilt für ein $m \in \mathbb{N}$.

Beweis:

(i) Bedeutet: $z \in \mathbb{C}^m$, $f_1(z) = \ldots = f_s(z) = 0$
$\Rightarrow f(z) = 0$.

(ii) Bedeutet: $f^m = h_1 f_1 + \ldots + h_s f_s$
gilt für ein $m \in \mathbb{N}$ und gewisse $h_1, \ldots, h_s \in \mathbb{C}[x_1, \ldots, x_n]$.

(ii) $\Rightarrow$ (i): Angenommen, für $z \in \mathbb{C}^n$

gilt $f_1(z) = \ldots = f_s(z) = 0$.

Dann gilt $f(z)^m = h_1(z) \cdot \underbrace{f_1(z)}_{\overset{\shortparallel}{0}} + \ldots + h_s(z) \cdot \underbrace{f_s(z)}_{\overset{\shortparallel}{0}}$

$$= 0$$

$\Longrightarrow f(z)^m = 0 \quad \Longrightarrow f(z) = 0$.

(i) $\Longrightarrow$ (ii): Angenommen, (i) ist erfüllt.

Wir führen eine Variable y ein und betrachten das Ideal $\mathcal{J} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \mathbb{C}[x_1, \ldots, x_n, y]$