

(i) \Rightarrow (ii): Angenommen, (i) ist erfüllt.

Wir lösen die Variable y ein und erhalten

dass ideal $\mathcal{J} = \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq \mathbb{C}(x_1, \dots, x_n, y)$

Es gilt: $V(\mathcal{J}) = V(f_1, \dots, f_s, 1 - yf) = \emptyset$:

Angenommen $(a, b) \in \mathbb{C}^n \times \mathbb{C}$ mit $f(a)$

$\in V(f_1, \dots, f_s, 1 - yf)$, d.h.

$$f_1(a) = \dots = f_s(a) = 0 = 1 - b \cdot f(a)$$

WGL (i) vgl. (i) ist wegen $f_1(a) = \dots = f_s(a) = 0$

und $f(a) = 0 \Rightarrow$

$$0 = 1 - b \cdot f(a) = 1 - b \cdot 0 = 1$$

$$\Rightarrow 0 = 1 - \underbrace{\dots}_{\text{S.}}$$

Nach dem schwachen Nullstellensatz ist

$$1 \in \mathcal{J} = \langle f_1, \dots, f_s, 1-y^p \rangle, \text{ d.h.}$$

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

gilt für gewisse $p_1, \dots, p_s, q \in \mathbb{C}[x_1, \dots, x_n, y]$.

Sei $m \in \mathbb{Z}_{>0}$ eine obere Schranke an die

Grade der Polynome p_1, \dots, p_s an

Polynome in y mit Koeffizienten in $\mathbb{C}(x_1, \dots, x_n)$.

[$f \neq 0$, dann sonst ist (i) \Rightarrow (ii) trivial].

Wir schaue für y die rationale Funktion

$\frac{1}{f} \in \mathbb{C}(x_1, \dots, x_n)$ ein und erhalten.

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

$$\Rightarrow f^m = \sum_{i=1}^s f^m p_i(x_1, \dots, x_n, \frac{1}{f}) \cdot f_i(x_1, \dots, x_n)$$

" "
 A_i gehört zu $\{f(x_1, \dots, x_n)\}$
nach der Wahl von m .

$$\Rightarrow f^m = \sum_{i=1}^s A_i f_i \in \langle f_1, \dots, f_s \rangle.$$

□

4.3.2. Bemerkung: Sätze mit den Voraussetzungen

des sogenannten stetigen Nullstellen Satzes
gibt man auch in anderen Theorien (z.B. in
der linearen Optimierung)

Algebra

starken Nullstellensatz

$$\forall (f_1, \dots, f_s) = \emptyset \Leftrightarrow \exists \in \langle f_1, \dots, f_s \rangle \text{ aus } \begin{cases} Ax = b \\ x \geq 0 \end{cases} \text{ hat L\ddot{o}sung}$$

$$\Leftrightarrow \exists y: yA \geq 0 \\ yb < 0.$$

starke Nullstellen \Leftrightarrow

aus Dualit\ddot{a}tsraum
die Lineare
Aufgaben.

4.3.3 Theorem (der starke Nullstellensatz, Formulierung 2).

Sei $I \subseteq (\{x_1, \dots, x_n\})$ Ideal. Dann gilt f\ddot{u}r
 $f \in (\{x_1, \dots, x_n\})$ die folgenden Bedingungen \ddot{a}quivalent:

(i) $f \in I \cap V(I)$

(ii) $f^m \in I$ f\ddot{u}r ein $m \in \mathbb{N}$.

Beweis: Nach dem Hilbertschen Basisatz gilt

$I = \langle f_1, \dots, f_s \rangle$ für gewisse $f_1, \dots, f_s \in \mathbb{C}[x_1, \dots, x_n]$.

Die Behauptung folgt nun aus der Formulierung

1.

□

4.3.4. Definition. Das Radikal eines Ideals

$I \subseteq k[x_1, \dots, x_n]$ ist die Menge

$$\sqrt{I} = \{ f \in k[x_1, \dots, x_n] : f^m \in I \text{ für } \text{ein } m \in \mathbb{Z}_{>0} \}$$

Man sagt, dass das Ideal I radikal ist, wenn $I = \sqrt{I}$ gilt. Ideale, die radikal sind, nennt man Radikalideale.

4.3.5 Beispiel. Sei $I = \langle x^5(x-1)^4 \rangle \subseteq \mathbb{C}[x]$

Wodurch ist \sqrt{I} erzeugt?

Einfachere Frage: ist $I = \sqrt{I}$?

Nachhöhere Fragen:

$$x(1-x) \in I ?$$

nein; jedoch

Polynom aus I
ist durch x^5

teilbar,

$x(1-x)$ aber nicht.

$$x(1-x) \in \sqrt{I} ?$$

ja, dann gilt S. Bknt

$$(x(1-x))^5$$

$$= x^5 (1-x)^5$$

$$= x^5 \cdot \underbrace{(1-x)^4}_{\text{teilbar}} \cdot (1-x)$$



$$I \neq \sqrt{I}.$$

Wir zeigen $\sqrt{I} = \langle x(1-x) \rangle$

Ein beliebiges Polynom aus $\langle x(1-x) \rangle$ hat die

form $x(1-x)g$ mit $g \in C([x])$. Die 5-te
Potenz davon ist

$$x^5(1-x)^5 \cdot g^5 = \underbrace{x^5(1-x)^4}_{\text{Erzeuger von } I} \cdot x \cdot g^5 \in I.$$

Erzeuger von I

Das zeigt: $\sqrt{I} \supseteq \langle x(1-x) \rangle$.

Wie kann man $\sqrt{I} \subseteq \langle x(1-x) \rangle$ zeigen?

Sei $f \in \sqrt{I}$, d.h. $f^m \in I$ für ein $m \in \mathbb{Z}_{>0}$,

$\Rightarrow f^m = x^5(1-x)^4 \cdot g$ für ein $m \in \mathbb{Z}_{>0}$ und $g \in C([x])$

$$\Rightarrow f(0)^m = 0^5 \cdot (1-0)^4 \cdot g(0) = 0$$

$$f(1)^m = 1^5 \cdot (1-1)^4 \cdot g(1) = 0$$

$\Rightarrow f(0) = f(1) = 0 \Rightarrow f$ hat 0 nur 1
als Nullstelle

$\Rightarrow f$ ist durch $x(1-x)$ teilerbar

$\Rightarrow f \in \langle x(1-x) \rangle.$

Zusammenfassend.

$$\sqrt{\langle x^5(1-x)^4 \rangle} = \langle x(1-x) \rangle.$$

4.3.6. Proposition. Für jedes Ideal $I \subseteq k(x_1, x_n)$

ist das Radikal \sqrt{I} ebenfalls ein Ideal.

Beweis: ① $0 \in \sqrt{I}$ weil $0 \in I$.

② Seien $f, g \in \sqrt{I}$, d.h. $f^{m'}, g^{m''} \in I$

für gewisse $m', m'' \in \mathbb{Z}_{>0}$. Zu zeigen: $f+g \in \sqrt{I}$.

Es gilt, $f^m, g^m \in I$ für $m = \max\{m', m''\}$.

$$\Rightarrow (f+g)^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} f^i g^{2m-i} \text{ liegt}$$

Binomischer
Lehrsatz

in I , weil für jedes $i = 0, \dots, 2m$ $i \geq m$ oder
 $2m - i \geq m$ erfüllt ist, was somit
 $f^i \in I$ oder $g^{2m-i} \in I$ gilt.

③ Hier $f \in \sqrt{I}$ und $h \in k(x_1, \dots, x_n)$,
d.h. $f^m \in I$ für ein $m \in \mathbb{Z}_{>0}$.

Zu zeigen: $f \cdot h \in \sqrt{I}$.

Man hat $(f \cdot h)^m = \underbrace{f^m}_{\substack{\cap \\ I}} \cdot h^m \in I$

$\Rightarrow f \cdot h \in \sqrt{I}$. □

4.3.7. Theorem (Der starke Nullstellen Satz,
formalizierung 3). Sei $I \subseteq \mathbb{C}(x_1, \dots, x_n)$

Ideal. Dann gilt:

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

Beweis: Direkte Folgerung aus der formalizierung 2.

□

4.3.8. Bemerkung. Es ist klar, dass

$$\sqrt{\sqrt{I}} = \sqrt{I} \text{ ist (für jedes Ideal } I).$$

Das heißt: $I(V(I))$ ist ein Radikal ideal.

4.4. Beziehung zwischen Radikalidealen und Varietäten.

4.4.1 Theorem. Die Abbildung $V \mapsto I(V)$ ist
ein bijektiver \leftrightarrow -operator

$$\mathcal{VR} := \{ V \subseteq \mathbb{C}^n : V \text{ Varietät} \}$$

nach

$$\mathcal{RI} := \{ I \subseteq \mathbb{C}[x_1, \dots, x_n] : I \text{ Radikalideal} \}$$

Die Abbildung $I \mapsto V(I)$ ist die Umkehr-
abbildung zu $I : \mathcal{VR} \rightarrow \mathcal{RI}$. Des Weiteren
gilt folgendes:

$$V \subseteq W \iff I(V) \supseteq I(W) \quad (\forall V, W \in \mathcal{VR})$$

$$V(I) \subseteq V(J) \iff I \supseteq J \quad (I, J \in \mathcal{RI})$$

Beweis: Eine Abbildung ist bijektiv \Leftrightarrow die Abbildung von links nach rechts invertierbar. Das heißt, hier der ersten Teil des Lemmas muss es Folgendes zu zeigen:

- $I(V)$ ist Radikalideal und $V(I(V)) = V$.
- $I(V(I)) = I$, wenn I ein Radikalideal ist.

$I(V)$ ist Radikalideal: $f \in \overline{I(V)} \Leftrightarrow f(a)^m = 0$

für alle $a \in V$ für ein gewisses $m \in \mathbb{Z} > 0$

$\Leftrightarrow f(a) = 0$ für alle $a \in V \Leftrightarrow f \in I(V)$.

Die Gleichung $V(I(V)) = V$. In Proposition 14.9 wurde gezeigt, dass das Ideal einer Varietät die Varietät eindeutig bestimmt.

Es reicht also $I(V(I(V))) = I(V)$,

d.h. $I(V(J)) = J$ für $J = I(V)$.

Nach dem starken Nullstellensatz

gilt $I(V(J)) = \sqrt{J}$. Da $\sqrt{J} = I(V)$

Radikalideal ist, gilt $\sqrt{J} = J$.

$\Rightarrow I(V(J)) = J$.

$I(V(I)) = I$, wenn I Radikalideal ist.

Nach dem starken Nullstellensatz gilt

$I(V(I)) = \sqrt{I}$. Da I Radikalideal ist,

gilt $\sqrt{I} = I$. $\Rightarrow I(V(I)) = I$.

□

4.5. Die Zariski-Topologie.

4.5.1. Definition. (Ausgewählte Begriffe aus der Mengentheoretischen Topologie).

Eine Menge X , die mit einer Familie \mathcal{U} von Teilmengen von X ausgestattet ist, heißt topologischer Raum mit dem System der offenen Mengen \mathcal{U} , wenn Folgendes gilt:

(a) $\emptyset, X \in \mathcal{U}$

(b) Für endlich viele $U_1, \dots, U_r \in \mathcal{U}$ ist $U_1 \cap \dots \cap U_r \in \mathcal{U}$.

(c) Für beliebige Familie $\{U_i : i \in R^3\}$ von Mengen $U_i \in \mathcal{U}$ ist $\bigcup_{i \in R^3} U_i \in \mathcal{U}$.

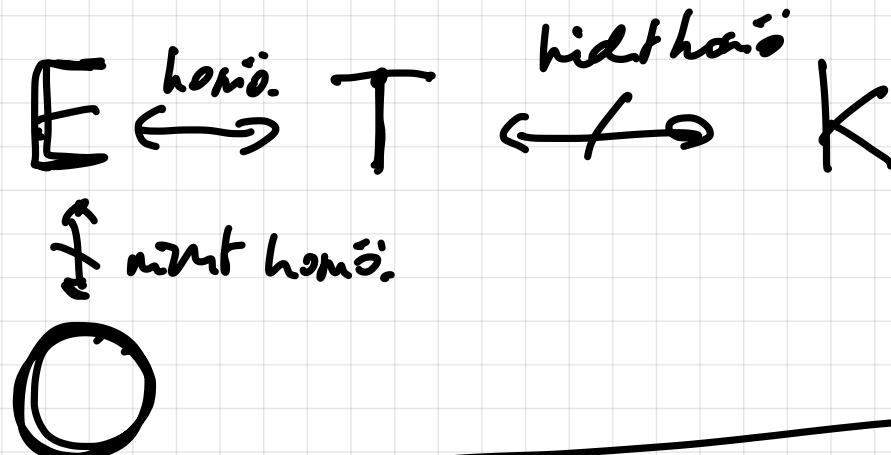
- Die Menge $X \setminus U$ mit $U \in \mathcal{U}$ nennt man abgeschlossen.
- Der topologische Abschluss \overline{M} einer Menge $M \subseteq X$ ist der Durchschnitt aller abgeschlossenen Mengen C mit $C \supseteq M$.
- Eine Abbildung $f: X \rightarrow Y$ topologischer Räume (X, \mathcal{U}) und (Y, \mathcal{V}) nennt man stetig, wenn $f^{-1}(V) := \{a \in X : f(a) \in V\} \in \mathcal{U}$ für alle $V \in \mathcal{V}$ gilt.

Nebenmerkung zur Algebraischen Topologie.

Zwei topologische Räume X und Y

heißen homöomorph, wenn eine Bijektion

$f: X \rightarrow Y$ existiert, die zusammen mit
der inversen Abbildung f^{-1} stetig ist
(f , f^{-1} sind beide stetig).



4.5.2. Theorem. Der Raum k^n , ausgeschlossen nur
der Familie $\mathcal{U}_2 := \{ k^n \setminus V : V \subseteq k^n \text{ Varietät} \}$,

ist ein topologischer Raum. Die Familie \mathcal{U}_2 wird
die Zariski-Topologie auf k^n genannt, die
Menge $U \in \mathcal{U}_2$ heut nach Zariski offen.

Darüber hinaus ist für jedes Polynom $f \in k[x_1, \dots, x_n]$
die Abbildung $f: k^n \rightarrow k$ stetig bzgl.

der Zariski-Topologie von k^n und k^1 .

Beweis: $\emptyset, k^n \in \mathcal{U}_2$ gilt weil k^n und \emptyset

Varietäten sind. Sei $U_i = k^n \setminus V_i$ für eine

Varietät $V_i \subseteq k^n$ ($i = 1, \dots, r$). Dann ist

$$U_1 \cap \dots \cap U_r = k^n \setminus (V_1 \cup \dots \cup V_r).$$

Wen wir wissen ist $V_1 \cup \dots \cup V_r$ eine Varietät.

$\Rightarrow U_1 \cap \dots \cap U_r \in \mathcal{U}_2$.

Sei $U_i = k^n \setminus V_i$ mit $V_i = V(F_i)$

für eine endliche Menge $F_i \subseteq k(x_1, \dots, x_n)$

($i \in R$, R beliebig).

Dann ist

$$\bigcup_{i \in R} U_i = k^n \setminus \bigcap_{i \in R} V_i = k^n \setminus V\left(\bigcup_{i \in R} F_i\right) \underset{\substack{\text{ist Varietät} \\ \text{nach Prop. 2.4.5}}}{\in} \mathcal{U}_2.$$

$\Rightarrow \mathcal{U}_2$ M-Topologie auf k^n .

Wir zeigen, dass für $f \in K(x_1, \dots, x_n)$

die Abbildung $f: k^n \rightarrow k$ bzgl. der Zariski-Topologie stetig ist.

für U zunächst-offene Teilmenge von k.

Dann ist U leer oder das Komplement einer endlichen Menge.

Ist U = ∅, dann ist $f^{-1}(U) = f^{-1}(\emptyset) = \emptyset$.

Ist U ≠ ∅, so gelte $U = k^n \setminus \{z_1, \dots, z_r\}$

für $r \in \mathbb{Z}_{\geq 0}$. \Rightarrow

$$f^{-1}(U) = \{a \in k^n : f(a) \in U\}$$

$$= \{a \in k^n : f(a) \neq z_i \text{ für jedes } i = 1, \dots, r\}$$

$$= k^n \setminus (\underbrace{V(f - z_1) \cup \dots \cup V(f - z_r)}_{\text{eine Varietät}}).$$

$$\in \mathcal{U}_2.$$

4.5.3 Bemerkung. Man erhält aus der Analogie der sogenannte euklidische Topologie \mathcal{U}_E auf k^n für $k = \mathbb{R}$ und für $k = \mathbb{C}$.

Nach der Definition: $U \in \mathcal{U}_E$ genau dann

wenn für jedes $a \in U$ ein $\varepsilon > 0$ existiert,
für welches jeder Punkt $p \in k^n$ mit $\|p-a\| < \varepsilon$
zu U gehört.

Wie hängen \mathcal{U}_E und \mathcal{U}_Z zusammen?

$\mathcal{U}_E \supseteq \mathcal{U}_Z$ (die euklidische Topologie ist feiner).

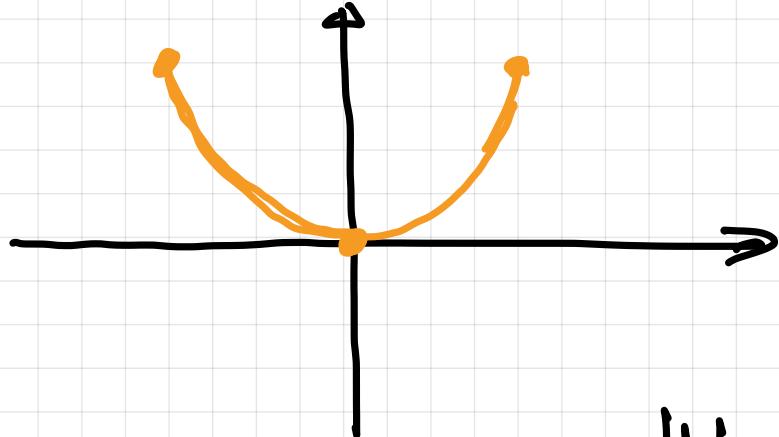
Bsp.
 $k = \mathbb{R}$

$$[0,1]^2$$

der euklidische Abschluss davon
ist $[0,1]^2$ (ist also abgeschlossen
in der euklidischen Topologie)

Weg ist der Abschluss von $[0,1]^2$ in der Zariski-Topologie? Dass in \mathbb{K}^2 (außer \mathbb{K}^2 gibt es keine Varietät $V \subseteq \mathbb{K}^2$, die $[0,1]^2$ als Teilmenge enthält).

Bsp. $M = \{(a,b) : f = a^2, -1 \leq a \leq 1\}$ ($\mathbb{K} = \mathbb{R}$)



Der euklidische Abschluss von M ist M (denn M ist Euklidisch abgeschlossen).

Was ist der Zariski-Abschluss?

Der zariski-Abschluss von M ist $V_{\mathbb{R}}(y - x^2)$ (die gesamte Parabel).

4.5.9. Theorem. Der Zariski-Abschluss (Abschluss in der Zariski-Topologie) von $S \subseteq \mathbb{C}^n$ ist $V(I(S))$
 [Die Menge aller Punkte, auf denen alle Polynome gleich 0 sind, die auf S offen 0 sind]

Beweis: Der Zariski-Abschluss von S ist der Durchschnitt aller Varietäten, die S enthalten.
 Somit ist das die inklusiv minimale Varietät, die S enthält. Sei W Varietät mit $W \supseteq S$.
 $\Rightarrow I(W) \subseteq I(S) \Rightarrow V(I(W)) \supseteq V(I(S))$.

Nach Theorem 4.4.1 ist $V(I(W)) = W$.

Das zeigt $W \supseteq \underbrace{V(I(S))}$. Also ist $V(I(S))$ die inklusiv minimale Varietät, die S enthält.



4.6. Der Abschluss-Satz.

4.6.1. Theorem (der schwache Abschluss-Satz).

Sei $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ Ideal, $a_i : i = 1, \dots, n$.

Man betrachte die Projektion $\pi_l : \mathbb{C}^n \rightarrow \mathbb{C}^{n-l}$,

$\pi_l(a_1, \dots, a_n) = (a_{l+1}, \dots, a_n)$ und das l -te

Eliminationsideal $I_l = I \cap \mathbb{C}[x_{l+1}, \dots, x_n]$.

Dann ist der Zariski-Abschluss von

$\pi_l(V(I))$ gleich $V(I_l)$.

Beweis: Es gilt $\pi_l(V(I)) \subseteq V(I_l)$,

denn $\pi_l(V(I))$ ist die Menge aller Punkte (a_{l+1}, \dots, a_n) für $(a_1, \dots, a_n) \in \mathbb{C}^n$ mit der Eigenschaft

dass $f(a_1, \dots, a_n) = 0$ für alle $f \in I$

I_ℓ besteht aus Polynomen in I , die von x_1, \dots, x_ℓ unabhängig sind. Diese Polynome sind auf $(a_{\ell+1}, \dots, a_n)$ gleich 0.

Somit ist $(a_{\ell+1}, \dots, a_n) \in V(I_\ell)$.

Das heißt, für den Zariski-Abschluss $\overline{J_\ell(V(I))}$ von $J_\ell(V(I))$ gilt: $\overline{J_\ell(V(I))} \subseteq V(I_\ell)$.

Wir zeigen die Umkehrung $V(I_\ell) \subseteq \overline{J_\ell(V(I))}$.

Nach Theorem 4.5.9 gilt $\overline{J_\ell(V(I))} = V(I(J_\ell(V(I)))$

Wie zeigen also $V(I_\ell) \subseteq V(I(J_\ell(V(I))))$.

Nach dem Theorem 4.9.9 und den starken Nullstellensatz ist diese Inklusion äquivalent

$$\text{zu } \sqrt{I_e} \supseteq \sqrt{I(\mathfrak{J}_e(V(I)))}$$

Das Ideal einer Menge ist immer ein Radikalideal.

$$\Rightarrow \sqrt{I(\mathfrak{J}_e(V(I)))} = I(\mathfrak{J}_e(V(I))).$$

Wir wollen also

$$\sqrt{I_e} \supseteq I(\mathfrak{J}_e(V(I))) \text{ zeigen.}$$

Sei $f \in \mathbb{C}(x_{d+1}, \dots, x_n)$ ein Polynom, dass auf $\mathfrak{J}_e(V(I))$ gleich 0 ist. Das heißt

für alle $(a_1, \dots, a_n) \in V(I)$ gilt

$$f(a_{d+1}, \dots, a_n) = 0.$$

Wir können u f als Polynom in $\mathbb{C}(x_1, \dots, x_d)$

auffassen. Da wir wissen wir f auf (a_1, \dots, a_n) auswerten und es gilt $f(a_1, \dots, a_n) = f(a_{d+1}, \dots, a_n) = 0$.

D.h. als Polynom in $\mathbb{C}[x_1, \dots, x_n]$ ist f gleich 0 auf $V(I)$. Nun den ersten Nullstellenzatz ist $f^m \in I$ für ein $m \in \mathbb{N}$.

Wg $f \in \mathbb{C}[x_{\ell+1}, \dots, x_n]$ gilt $f^m \in (\mathbb{C}[x_{\ell+1}, \dots, x_n])$
 $\Rightarrow f^m \in I_\ell \Rightarrow f \in \sqrt{I_\ell}.$ □

Die Botschaft des vorigen Satzes ist ähnlich zu
 Botschaft des Projektions- und Erweiterungstheorems: $\text{St}_\ell(V(I))$ und $V(I_\ell)$ sind fast
 gleich. Aber im Gegensatz zum Projektions- und Erweiterungstheorem nimmt man im Abschluss-
 satz keinen Bezug auf die konkreten Ergebnisse von I .

4.6.3 Theorem (Der starke Abschluss-Satz).

In den Voraussetzungen des Thm. 4.6.2 gilt
Folgendes: es existiert eine affine Varietät

$$W \subseteq \mathbb{C}^n \text{ derart, dass } V(I_e) \setminus W \subseteq \mathcal{T}_e(V(t))$$

erfüllt $\mathfrak{I}(V)$ und der Zwischenabschluss
von $V(I_e) \setminus W$ gleich $V(I_e)$ ist.

Hilf ohne Beweis.

4.7. Berechnungen mit Radikalen.

Rechenprobleme hier geben $f_1, f_2, \dots, f_s \in k(x_1, \dots, x_n)$.

- Erzeuger des Radikals: man bestimme endlich viele Erzeuger von $\sqrt{\langle f_1, \dots, f_s \rangle}$.
- Radikal ideal-Test: man prüfe ob $\langle f_1, \dots, f_s \rangle$ ein Radikal-Ideal ist.

- Zur Sicherheit zum Radikal: man prüfe

$$f \in \sqrt{\langle f_1, \dots, f_s \rangle}.$$

Alle drei Aufgaben sind algorithmisch lösbar.

Die erste löst automatisch die zweite und die dritte.

Wir diskutieren die dritte Aufgabe.

4.7.1. Proposition. Für $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$

gilt: $f \in \sqrt{\langle f_1, \dots, f_s \rangle} \iff$

$$f \in \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq k(x_1, \dots, x_n, y).$$

Beweis: (\Leftarrow) findet im Beweis des starken Nullstellenatzes.

(\Rightarrow): Sei $f \in \sqrt{\langle f_1, \dots, f_s \rangle}$. Dann ist
 $f^m \in \langle f_1, \dots, f_s \rangle$ für ein $m \in \mathbb{N}$. Es folgt:

$$1 = y^m f^m + (1 - y^m f^m)$$

$$= \underbrace{y^m}_{\in \langle f_1, \dots, f_s \rangle} \underbrace{f^m}_{+ (1-y^m f^m)} + (1-y^m f^m)(1+y^1 f^1 + \dots + y^{n-1} f^{n-1})$$

$$\in \langle f_1, \dots, f_s, 1-y^m f^m \rangle.$$

□