Affine algebraische Mengen

Katharina Wächter, Inka Berglar

02.04.2009

Im Folgenden sei k ein kommutativer Ring mit 1, $1 \neq 0$.

Zur Schreibweise: Sei $x = (x_1, \ldots, x_n)$ ein Punkt im affinen Raum k^n, $n \in \mathbb{N}$ und $P(X_1, \ldots, X_n)$ ein Polynom in $k[X_1, \ldots, X_n]$, so schreibe $P(x)$ für $P(x_1, \ldots, x_n)$.

1 Affine algebraische Mengen und die Zariski-Topologie

Definition 1.1. *Sei $S \subseteq k[X_1, ..., X_n]$ eine beliebige Menge von Polynomen.*
*$V(S) = \{x \in k^n | P(x) = 0 \forall P \in S\}$ ist die gemeinsame Nullstellenmenge der Polynome in S und heißt **affine algebraische Menge** definiert durch S.*

Schreibweise: Ist $S = \{F_1, \ldots, F_r\}$ endlich, so schreibe $V(S) = V(F_1, \ldots, F_r)$

Beispiel 1.2.

1. *Die leere Menge und der ganze Raum k^n sind affine algebraische Mengen:*
   Sei $S = \{1\} \Rightarrow V(S) = \emptyset$.
   Sei $S = \{0\} \Rightarrow V(S) = k^n$.

2. *Sei $n = 1$, also $S \subseteq k[X]$, und sei $S \neq \emptyset$*
   $\Rightarrow$ Die Menge $V(S) = \{x \in k | P(x) = 0 \forall P \in S\}$ ist endlich.
   Die affinen algebraischen Teilmengen einer Geraden sind die Gerade selbst und die endlichen Mengen.

3. *Sei $n = 2$, also $S \subseteq k[X, Y]$*
   Die affinen algebraischen Mengen neben der Ebene k^2 und der leeren Menge sind die Kurven der Form $V(F)$ und die endlichen Mengen von Punkten, z.B. $V(X, Y) = \{(0,0)\}$, $V(X(X-1), Y) = \{(0,0), (1,0)\}$, ...

Bemerkung 1.3.

1. *Die Zuordnung V ist monoton fallend:*
   $S \subseteq S' \Rightarrow V(S') \subseteq V(S)$

   Beweis. $x \in V(S') \Rightarrow f(x) = 0 \forall f \in S' \Rightarrow f(x) = 0 \forall f \in S \Rightarrow x \in V(S)$ $\square$

2. *Bei affinen algebraischen Mengen kann man den Fall betrachten, dass S ein Ideal oder die Menge der Erzeuger des Ideals ist:*
   Sei $S \subseteq k[X_1, ..., X_n]$ und $\langle S \rangle$ das von S erzeugte Ideal.
   Dann gilt: $V(S) = V(\langle S \rangle)$

   Beweis. Das Ideal $\langle S \rangle$ wird erzeugt von den Polynomen f der Form $f = \sum_{i=1}^{r} a_i f_i$, $f_i \in S, a_i \in k[X_1, ..., X_n]$
   $\subseteq$: $x \in V(S) \Rightarrow f_i(x) = 0 \Rightarrow f(x) = 0$
   $\supseteq$: $S \subseteq \langle S \rangle \Rightarrow V(\langle S \rangle) \subseteq V(S)$ □

3. *Jede affine algebraische Menge ist ein Schnitt endlich vieler Hyperflächen:*
   Da $k[X_1, \ldots, X_n]$ noethersch ist, ist jedes Ideal endlich erzeugt: $I = \langle f_1, ...f_r \rangle$. Also ist jede affine algebraische Menge durch endlich viele Gleichungen festgelegt:
   $V(I) = V(f_1, ..., f_r) = V(f_1) \cap ... \cap V(f_r)$
   Die Mengen der Form $V(f)$ heißen ***Hyperflächen****. (Genauer ist dies definiert für f nicht-konstant und k algebraisch abgeschlossen. Vgl. dazu Kapitel IV / Vortrag 9?.)*

   Definition 1.4. *Ein kommutativer Ring R heißt* ***noethersch****, wenn jedes Ideal I in R endlich erzeugt ist. Für R einen komm. Ring ist äquivalent:*

   a) R ist noethersch.
   b) Jede aufsteigende Kette von Idealen wird stationär.
   c) Jede nichtleere Teilmenge S von Idealen besitzt ein maximales Element.

4. *Verschiedene Polynome können die gleiche affine algebraische Menge festlegen.*
   Bsp: In k^2 gilt $V(X) = V(X^2)$

5. *Ein Punkt ist eine affine algebraische Menge:*
   $a = (a_1, ..., a_n) \Rightarrow \{a\} = V(X_1 - a_1, ..., X_n - a_n)$

6. *Der Schnitt affiner algebraischer Mengen ist eine affine algebraische Menge:*
   $\bigcap_i V(S_i) = V(\bigcup_i S_i)$

   Beweis. $x \in \bigcap_i V(S_i) \Leftrightarrow x$ Nullstelle aller Polynome in $S_i \Leftrightarrow x \in V(\bigcup_i S_i)$ □

7. *Die endliche Vereinigung affiner algebraischer Mengen ist eine affine algebraische Menge:*
   $\bigcup_i V(S_i) = V(\bigcap_i S_i)$

   Beweis. Es genügt (siehe Bem.1.3.2), dies für die durch die Ideale I, J festgelegten Mengen zu zeigen: $V(I) \cup V(J) = V(IJ)$
   $\subseteq$: $IJ \subseteq I, IJ \subseteq J \Rightarrow V(I) \cup V(I) \subseteq V(IJ)$
   $\supseteq$: Sei $x \in V(IJ), x \neq V(I) \Rightarrow \exists P \in I : P(x) \neq 0 \; \forall \; Q \in J : PQ \in IJ \Rightarrow (PQ)(x) = 0 \Rightarrow Q(x) = 0 \Rightarrow x \in V(J)$
   Analog zeigt man: $V(I) \cup V(J) = V(I \cap J)$

   □

8. *Jede endliche Menge ist eine affine algebraische Menge, denn sie ist eine endliche Vereinigung von Punkten. (Nach 5. und 7.)*

Definition 1.5 (Die Zariski-Topologie)**.** *Ein **topologischer Raum** ist ein Paar (X, O) bestehend aus einer Menge X und einer Menge O (genannt **Topologie**) von Teilmengen (genannt offenen Mengen) von X, so dass gilt:*

1. *Die Vereinigungen von offenen Mengen ist offen.*

2. *Der endliche Durchschnitt von offenen Mengen ist offen.*

3. *X und $\emptyset$ sind offen.*

Eine Teilmenge A heißt abgeschlossen, wenn ihr Komplement $X \backslash A$ offen ist. Ein topolgischer Raum heißt hausdorff'sch, wenn man zu je zwei Punkten disjunkte Umgebungen finden kann.
*Nach 6. und 7. sind die affinen algebraischen Mengen $V(I)$ die abgeschlossenen Mengen einer Topologie - diese heißt **Zariski-Topologie**.*

Bemerkung: *Jede Teilmenge $X \subseteq k^n$ hat eine induzierte Zariski-Topologie. Ihre abgeschlossenen Mengen sind die Mengen der Form $X \cap V(I)$. Insbesondere gilt: Ist X eine affine algebraische Menge, so sind die abgeschlossenen Mengen in X gerade die affinen algebraischen Mengen, die in X enthalten sind.*
Die Zariski-Topologie ist i.A. nicht hausdorffsch. Die abgeschlossenen Mengen der Topologie sind sehr klein, die offenen Mengen sehr groß.

Definition 1.6 (Offene Standard-Mengen)**.** *Sei $f \in k[X_1, ..., X_n]$ und $V(f)$ die Hyperfläche definiert durch f.*
*Die Menge $D(f) = k^n \backslash V(f)$ ist eine Zariski-offene Menge von k^n und heißt offene **Standard-Menge**.*
Die Standard-Mengen bilden eine Basis der Zariski-Topologie: Jede offene Menge U ist eine endliche Vereinigung von Standard-Mengen: $U = \bigcap_i D(f_i)$ (Vgl. 1.3.3)

2 Ideal einer affinen algebraischen Menge

Definition 2.1. *Sei $V \subseteq k^n$ eine beliebige Menge von Punkten. Die Menge $I(V) = \{f \in k[X_1, ..., X_n] \,|\, f(x) = 0 \forall x \in V\}$ ist die Menge von polynomialen Funktionen, die auf V verschwinden, und heißt **Ideal** von V.*

Bemerkung: *Um zu zeigen, dass $I(V)$ ein Ideal (nach der bisherigen Definition) ist, betrachten wir den Ringhomomorphismus $r : k[X_1, ..., X_n] \to F(V, k), P \mapsto P|_V$.*
*$F(V, k) = \{f : V \to k, f \text{ polynomial}\}$ ist der Ring der k-wertigen, polynomialen Funktionen auf V. Ein Polynom wird auf die Einschränkung der assoziierten polynomialen Funktion auf V abgebildet. $I(V)$ ist der Kern von r, also ein Ideal. Das Bild von r ist der Ring $\Gamma(V) \cong k[X_1, ..., X_n] / I(V)$, genannt **affiner Koordinatenring*** von V.

Bemerkung 2.2. *1. Die Zuordnung I ist monoton fallend:*
$V \subseteq V' \Rightarrow I(V') \subseteq I(V)$

Beweis. $f \in I(V') \Rightarrow f(x) = 0 \forall x \in V' \Rightarrow f(x) = 0 \forall x \in V \Rightarrow f \in I(V)$ □

2. *Sei V eine affine algebraische Menge, dann gilt: $V(I(V)) = V$*

Beweis. $\subseteq$: Sei V die affine algebraische Menge $V = V(I)$. $\Rightarrow I \subseteq I(V) \Rightarrow V(I(V)) \subseteq V(I) = V$
$\supseteq$: $V \subseteq V(I(V))$ klar.

□

3. *Die Zuordnung $V \mapsto I(V)$ ist injektiv (folgt aus 2.):*
$V \subset W, V \neq W \Rightarrow I(W) \subset I(V), I(W) \neq I(V)$, das heißt, es gibt ein Polynom, das auf V verschwindet, aber nicht auf W.

4. *$I \subseteq I(V(I))$ (klar)*
Im Allgemeinen gilt keine Gleichheit. Es gibt zwei Einschränkungen:

   a) *Ist der Körper k nicht algebraisch abgeschlossen, kann $V(I)$ sehr klein sein.*
   Bsp: $k = \mathbb{R}, I = \left(X^2 + Y^2 + 1\right) \Rightarrow V(I) = \emptyset \Rightarrow I(V(I)) = k[X_1, ..., X_n] \neq I$

   b) *Die Operation I verliert Potenzen.*
   Bsp: $n = 2, I = \left(X^2\right) \Rightarrow V(I) = \{(0,t), t \in k\}$ ist die y-Achse $\Rightarrow I(V(I)) = (X) \neq I$

Beispiel 2.3. *1. $I(\emptyset) = k[X_1, ..., X_n]$*

2. *$I(k^n) = ...$*
Dazu:

Satz 2.4. *Sei k unendlich. Dann gilt: $I(k^n) = 0$.*
(M.a.W.: Verschwindet eine Polynomialfunktion auf ganz k^n, so ist das Polynom das Null-Polynom.)

Beweis. durch Induktion über n
Induktionsanfang: Für $n = 1$: $I(k) = \{0\}$ klar (Vgl. 1.2.2: $S \neq \{0\} \Rightarrow V(S)$ *endl.*)
Induktionsvoraussetzung: $I\left(k^{n-1}\right) = \{0\}$
Induktionsschritt: Annahme: $P \in I(k^n), P \neq 0$, nicht-konstant. Stelle P dar als $P = \sum_{i=0}^{r} a_i(X_1, ..., X_{n-1}) X_n^i$, $r \geq 1$, $a_r \neq 0$. Da $a_r \notin \{0\} = I\left(k^{n-1}\right)$, existiert nach Ind.vor. $(x_1, ... x_{n-1}) \in k^{n-1}$ mit $a_r(x_1, ... x_{n-1}) \neq 0$. $P(x_1, ..., x_{n-1}, X_n)$ hat höchstens r Nullstellen, d.h. P ist nicht Null für alle $x \in k^n$. $\lightning \Rightarrow P = 0$ □

Bemerkung: Diese Aussage ist falsch für k endlich.
Bsp: Betrachte das Polynom $X^p - X$ auf $\mathbb{F}_p$.

3. $I(\{a_1, ...a_n\}) = (X_1 - a_1, ..., X_n - a_n)$

Beweis. $\subseteq$: Sei $P \in I(\{a_1, ...a_n\})$, also $P(a_1, ...a_n) = 0$. Teile P sukzessive durch die Terme $X_i - a_i$: $P = (X_1 - a_1) Q_1 + ... + (X_n - a_n) Q_n + c$, $c \in k$ Es gilt: $c = P(a_1, ...a_n) = 0$. Also $P \in (X_1 - a_1, ..., X_n - a_n)$.
$\supseteq$: Es ist klar: $(X_1 - a_1, ..., X_n - a_n) \subseteq I(\{a_1, ...a_n\})$

□

4. *Sei k unendlich. Berechne das Ideal $I(V)$ mit $V = V(Y^2 - X^3)$ in $k[X, Y]$.*
Es gilt: $I(V) = (Y^2 - X^3)$

Beweis. $\subseteq$: Jeder Punkt in V ist von der Form (t^2, t^3), $t \in k$.
Sei $P(X, Y) \in I(V)$. Teile P durch $Y^2 - X^3$ bzgl. der Variablen Y: $P(X, Y) = (Y^2 - X^3) Q(X, Y) + a(X) Y + b(X)$.
Für alle $t \in k$ gilt: $P(t^2, t^3) = a(t^2) t^3 + b(t^2) = 0$. Da k unendlich ist, gilt in $k[T]$: $a(T^2) T^3 + b(T^2) = 0$. Durch Koeffizientenvergleich ergibt sich: $a(T^2) = b(T^2) = 0$. Also gilt: $I(V) \subseteq (Y^2 - X^3)$
$\supseteq$: Es ist klar: $I(V) \supseteq (Y^2 - X^3)$

□

3 Irreduzibilität

Wir betrachten die affine algebraische Menge im k^2 , definiert durch $XY = 0$.
Diese Menge ist die Vereinigung von zwei Koordinatenachsen, welche selbst affine algebraische Mengen und daher Zariski-abgeschlossene Untermengen sind. In solchen Fällen ist es möglich sich mit jeder separat zu beschäftigen.

Prop.-Definition 3.1. *Sei X ein nicht-leerer topologischer Raum. Dann sind folgende Aussagen äquivalent:*

i) Lässt sich X schreiben als $X = F \cup G$, wobei F und G abgeschlossene Mengen von X sind. Dann gilt $X = F \vee X = G$.

ii) Sind U,V zwei offene Mengen von X und $U \cap V = \emptyset$. Dann gilt $U = \emptyset \vee V = \emptyset$.

iii) Jede nicht-leere offene Menge von X ist dicht in X.

Erfüllt X eine der drei Bedingungen, so heißt X irreduzibel.

Beweis. Im Folgenden sei die Äquivalenz der drei Aussagen gezeigt:

- *i)* $\Rightarrow$ *ii)* Seien U und V offene Mengen in X und gelte $U \cap V = \emptyset \Rightarrow (U \cap V)^c = \emptyset^c = X$
  Es gilt $(U \cap V)^c = U^c \cup V^c = X \Rightarrow X = U^c \vee X = V^c$

- $ii) \Rightarrow i)$ Analog
- $ii) \Rightarrow iii)$ Sei $U \subset X$ offen, $U \neq \emptyset$
  z.z. $\overline{U} = X$
  Betrachte $\overline{U}^c = X \backslash \overline{U} \Rightarrow U \cap \overline{U}^c = \emptyset \Rightarrow U = \emptyset$ oder $\overline{U}^c = \emptyset \Rightarrow \overline{U}^c = \emptyset \Rightarrow \overline{U} = X$

$\square$

Theorem 3.2. *Sei V eine affine algebraische Menge mit Zariski-Topologie. Dann gilt:*

$$V \text{ ist irreduzibel} \Leftrightarrow I\left(V\right) \text{ prim} \Leftrightarrow \Gamma\left(V\right) \text{ nullteilerfrei}$$

Beweis. i) V irreduzibel $\Rightarrow I\left(V\right)$ prim

Sei V irreduzibel und sei $fg \in I\left(V\right)$ und $I\left(V\right) \supseteq (fg)$, V monoton fallend

$$\Rightarrow V(I(V)) \subseteq V(fg) = V \subseteq V(f) \cup V(g)$$
$$V = V(I(V)) \subseteq V(f) \cup V(g)$$
$$V = ((V(f) \cup V(g)) \cap V) = (V(f) \cap V) \cup (V(g) \cap V).$$

$\overset{V \text{ irreduzibel}}{\Rightarrow}$ oE $V(f) \cap V = V$ d.h. $V \subset V(f)$ und $f \in I(V)$

V irred. $\Leftarrow I(V) prim$
Annahme: V ist nicht irreduzibel, d.h. $V = V_1 \cup V_2$ mit V_i abgeschlossene Mengen und $V_i \neq V$ und $I(V)$ prim
$I(V) \subset I(V_i)$ und $I(V) \neq I(V_i)$
Nehme $f_i \in I(V_i) \backslash I(V)$ und nehme $f_1 f_2$ auf $V \Rightarrow f_1 f_2 = 0$ (da $f_1 \in I(V_1) \backslash I(V)$ und $f_2 \in I(V_2) \backslash I(V)$)
$f_1 f_2 \in I(V_1 \cup V_2) = I(V)$ aber $f_1 \notin I(V)$ und $f_2 \notin I(V)$ aber $I(V)$ prim $\lightning$
$I(V)$ prim $\Rightarrow V$ irreduzibel.
ii) $\Leftrightarrow$ iii)
$I(V)$ prim $\Leftrightarrow \Gamma(V)$
$I(V)$ prim $\Leftrightarrow k[x_1, ..., x_n] \; / I(V) \cong \Gamma(V)$ $\square$

Korollar 3.3. *Nehme an, dass k unendlich ist. Dann ist der affine Raum k^n irreduzibel.*

Beweis. Nach Prop 2.4 gilt $I(k^n) = (0)$ und (0) prim da $k[x_1, ..., x_n]$ nullteilerfrei und $I(k^n)$ prim $\Leftrightarrow k^n$ irreduzibel folgt die Behauptung. $\square$

Wenn k endlich ist, dann ist das Korollar falsch, da k^n dann endliche Vereinigung von abgeschlossenen Mengen (Punkten) ist und somit nicht irreduzibel.

Anwendung 3.4 (Fortsetzung algebraischer Gleichungen)**.** *Nehme an, dass k unendlich ist und V eine affine algebraische Menge $\neq k^n$ und*

$$P \in k[x_1, ..., x_n].$$

Nehme an, dass $P = 0$ außerhalb von V, dann folgt dass $P \equiv 0$.

Beweis. Sei $V \subset k^n$ Zariski-abgeschlossen $\Rightarrow V(P) \supset V^c$ ist Zariski-abgeschlossen.
Es gilt $k^n = V \cup V(P), \xrightarrow{k^n irred.} k^n = V \vee k^n = V(P) \Rightarrow k^n = V(P)$
$\Rightarrow P \equiv 0$ auf ganz k^n.

□

Proposition 3.5. *Sei X ein topologischer Raum und Y ein Unterraum von X. Dann gilt:*

i) Ist Y irreduzibel, so ist auch $\overline{Y}$ irreduzibel

ii) Ist U eine offene Menge von X dann sind die Abbildungen

$$Y \longmapsto \overline{Y}$$

und

$$Z \longmapsto Z \cap U$$

die zueinander inversen Bijektionen zwischen den irreduziblen abgeschlossenen Mengen Y in U und den irreduziblen abgeschlossenen Mengen Z in X, die U schneiden.

Beweis. i) Gilt $\overline{Y} = F_1 \cup F_2$ und sind F_i abgeschlosse Mengen von $\overline{Y}$ und daher eine abgeschlossenen Menge von X, dann gilt:

$Y = (F_1 \cap Y) \cup (F_2 \cap Y)$ und da Y irrededuzibel $\Rightarrow Y = F_i \cup Y \Rightarrow Y \subseteq F_i \Rightarrow \overline{Y} \subseteq F_i$, da F_i abgeschlossen.

Aber nach Vorraussetzung gilt: $\overline{Y} = F_1 \cup F_2 \Rightarrow F_i \subseteq \overline{Y}$

$\Rightarrow \overline{Y} = F_i$

ii) z.z. $Y \mapsto \overline{Y}_{inX} \mapsto \overline{Y} \cap U = Y$

Y abgeschlossen in $U \Rightarrow \overline{Y}_{inU} = Y = \bigcap_{Y \subseteq A_{abgeschl.} \subseteq U} A$

$Y \mapsto \overline{Y}_{inX} \mapsto \overline{Y}_{inX} \cap U = \bigcap_{Y \subseteq A_{abgeschl.} \subseteq X} A \cap U = \bigcap_{Y \subseteq A_{abgeschl.} \subseteq X} (A \cap U) = \bigcap_{Y \subseteq A_{abgeschl.} \subseteq U} A = Y$

z.z. $Z \mapsto Z \cap U \mapsto \overline{Z \cap U}_{inX} = Z$

Z irred., abg. in X, $Z \cap U \neq \emptyset$

$Z \subseteq \overline{Z \cap U}_{inX}$ klar

Ann.: $\bigcap\limits_{Z \cap U \subseteq A_{abgeschl.} \subseteq X} A \subsetneq Z$ dann existiert $z \in Z \backslash (Z \cap \overline{U})_{inX}$

$\Rightarrow Z = \overline{Z \cap U}_{inX} \cup (U^c \cap Z)$ ↯(da Z irred.)

□

Theorem-Definition 3.6. *Sei V eine nicht leere affine algebraische Menge.*
Wir können V (bis auf Vertauschungen) eindeutig in der Form $V = V_1 \cup \cdots \cup V_r$ schreiben, wobei V_i irreduzible affine algebraische Mengen sind und $V_i \subsetneq V_j$ für $i \neq j$.
Die Mengen V_i heißen irreduzibel Komponenten von V.

Beweis. Existenz
Annahme: Es gibt affine algebraische Mengen, für die es keine solche Zerlegung $V = V_1 \cup \cdots \cup V_r$ gibt. Wähle eine Menge V aus diesen Mengen , deren Ideal maximal ist.
Da V nicht irreduzibel gilt
$V = F \cup G$ wobei $F, G \neq V$
Wegen der Injektivität von I folgt, dass $I(F)$, $I(G) \supset I(V)$ und $I(F)$, $I(G) \neq I(V)$.
Da $I(V)$ maximal gewählt, müssen F und G die Form $F = F_1 \cup ... \cup F_r$ und $G = G_1 \cup ... \cup G_s$ haben.
Dann ist aber auch V zerlegbar. ↯
Eindeutigkeit
Nehme an es existieren zwei Darstellungen für V:
$V = V_1 \cup ... \cup V_r = W_1 \cup ... \cup W_s$
Wir setzen $V_i = V \cap V_i = (W_1 \cap V_i) \cup ... \cup (W_s \cap V_i)$.
Da V_i irreduzibel ist, ex. ein j sodass $V_i = W_j \cap V_i \Rightarrow V_i \subset W_j$.
Genauso existiert ein k sodass $W_j \subset V_k$ und daher $V_i \subset V_k \Rightarrow V_i = W_j$ □

Bemerkung 3.7. *Wenn W eine irreduzible abgeschlossene Menge von V ist, dann ist W in einer irreduziblen Komponente enthalten.*
Es folgt, dass die irreduziblen Komponenten gerade die maximalen abgeschlossenen irreduziblen Teilmengen von V sind.

4 Der Nullstellensatz (Hilbertscher Nullstellensatz)

Der Hilbertsche Nullstellensatz behandelt den Zusammenhang zwischen affinen algebraischen Mengen und Idealen. Er ermöglicht die Berechnung von $I(V(I))$.
Fortan wird k als algebraisch abgeschlossen vorausgesetzt (Dadurch wird vermieden, dass die affinen algebraischen Mengen zu klein werden).
Man kann (auch ohne den Nullstellensatz) sehen, dass wenn $F \in k[X_1, ..., X_n]$ nicht konstant ist, die Hyperfläche $V(F)$ unendlich ist (falls ≥ 2).

Theorem 4.1 (Schwacher Nullstellensatz). *Sei $I \subset k[X_1, ..., X_n]$ ein von $k[X_1, ..., X_n]$ verschiedenes Ideal.*
Dann ist $V(I)$ nicht leer.

Beweis. Der folgende Beweis gilt für k überabzählbar (z.B. $k = \mathbb{C}$).
(Für den allgemeinen Fall siehe Problem III, 4)
Man bette I in ein maximales Ideal I_{max} ein. Es reicht den Beweis für I_{max} zu führen (I_{max} existiert nach dem Lemma von Zorn). O.B.d.A. kann angenommen werden, dass $I_{max} = I$, da wegen der Monotonie von V gilt: $V(I_{max}) \neq \emptyset \Rightarrow V(I) \neq \emptyset$

Sei $K = k[X_1, ..., X_n] \mod I$ ein Restklassenkörper. Da $k[X_1, \ldots, X_n]$ ein Vektorraum von höchstens abzählbarer Dimension über k ist, gilt dies auch für K.

Lemma 4.2. *Sei k ein überabzählbarer algebraisch abgeschlossener Körper und sei K eine Erweiterung von k, deren Dimension über k höchstens abzählbar ist.*

Dann gilt:

$$K = k$$

Beweis des Lemmas. Es reicht zu zeigen, dass K algebraisch ist über k (da k bereits algebraisch abgeschlossen).
Annahme:
K enthält ein transzendentes Element. Dann enthält K einen Teilkörper isomorph zu dem rationalen Funktionenkörper in 1 Variablen $k(T)$. Aber dieser Körper besitzt eine überabzählbare Familie $\frac{1}{T-a}$, $a \in k$. Diese Familie ist ein linear unabhängiges System $\frac{1}{T-a_i}$ von $k(T)$. Es folgt also aus

$$\sum_{i=1}^{n} \frac{\lambda_i}{T - a_i} = 0$$

mit Multiplikation von $T - a_i$ und setzen von $T = a_i$ dass $\lambda_i = 0$ ↯
(Man hat zu dem Teilkörper $k(T)$ von K eine überabzählbare Basis gefunden. K ist aber nach Voraussetzung höchstens abzählbar) □

Zurück zu 4.1:
Nach Lemma 4.2 folgt:

$$K = k[X_1, ..., X_n] \mod I = k$$

Man betrachte die Bilder $a_1, ..., a_n$ der Variablen X_i in $K = k$.
Sei nun P ein Polynom in I. Nun zeigen wir, dass es ein Tupel in k^n gibt, so dass P auf diesem Tupel verschwindet, oder mit anderen Worten $V(I) \neq \emptyset$.

Betrachte die kanonische Projektion $\tau : k[X_1, ..., X_n] \twoheadrightarrow k[X_1, ..., X_n] \mod I$. Es ist τ ein Ringhomomorphismus. Da $P \in I$ gilt $\tau(P) = 0$. Da τ ein Ringhomorphismus, folgt

$$\begin{aligned} \tau(P(X_1, ..., X_n)) &= P(\tau(X_1), ..., \tau(X_n)) \\ &\overset{\text{def.}}{=} P(a_1, ..., a_n), \end{aligned}$$

und letzteres ist 0, da $\tau(P) = 0$. Aufgrund des Lemmas sind $a_1, ..., a_n$ nicht nur Elemente in dem Quotientenring, sondern sogar Elemente in k. Damit ist das Tupel in k^n gefunden. □

Um den Nullstellensatz zu formulieren, wird das Radikal von einem Ideal I in k eingeführt.
Es ist das Ideal

$$rac(I) = \{x \in A \mid \exists r \in \mathbb{N}, x^r \in I\} = \sqrt{I}$$

Theorem 4.3 (Nullstellensatz)**.** *Sei I ein Ideal von $k[X_1, ..., X_n]$.*
Dann gilt:

$$I(V(I)) = rac(I)$$

Beweis. Wir setzen

$$\begin{aligned} R &= k[X_1, \ldots, X_n], \\ I &= (P_1, \ldots, P_r), \\ V &= V(I). \end{aligned}$$

Es gilt $\mathrm{rac}(I) \subset I(V(I))$, denn sei $P \in \mathrm{rac}(I)$

$$\begin{aligned} &\Rightarrow && \exists\, r \in \mathbb{N} : P^r \in I \subseteq I(V(I)) \\ &\Rightarrow && P^r(x) = 0 \ \forall\, x \in V \\ &\overset{Nullteilerfreiheit}{\Rightarrow} && P(x) = 0 \ \forall\, x \in V \\ &\Rightarrow && P \in I(V). \end{aligned}$$

Nun $\mathrm{rac}(I) \supset I(V(I))$: Nehme an $F \in I(V) = I(V(I))$.
Z.z.: $F^m \in I$ für großes m.
Hierzu bildet man den lokalisierten Ring von F, R_F. Dies ist als Menge

$$R_F = \left\{ \frac{Q_i}{F^m};\ Q_i \in R,\ m \in \mathbb{N} \right\}.$$

Zeige $IR_F = (1) = R_F$. Man kann dann 1 darstellen als:

$$1 = \sum_i \frac{P_i Q_i}{F^m},$$

d.h. $F^m = \sum_i P_i Q_i$ $(P_i Q_i \in I)$

$$\Rightarrow F^m \in I.$$

Somit ist noch zu zeigen: $IR_F = (1)$. Es gilt

$$R_F \cong k[X_1, \ldots, X_n, T] \mod (1 - TF).$$

Mit $IR_F = (1)$ kann 1 dargestellt werden als

$$1 = \sum_i P_i Q_i + A(1 - TF),$$

wobei $A,\ Q_i \in k[X_1, \ldots, X_n, T]$.
Nun definiere $J = (P_1, \ldots, P_r, 1 - TF)$ in $k[X_1, \ldots, X_n, T]$.
Es gilt $V(J) = \emptyset$ in k^{n+1}.

Beweis. Annahme: $(x_1, \ldots, x_n, t) \in V(J)$
$\Rightarrow P_i$ werden durch $x = (x_1, \ldots, x_n)$ annuliert, da P_i nicht von t abhängen.
$\Rightarrow x \in V = V(I)$, da $I = (P_1, \ldots, P_n)$.
Da $F \in I(V) = I(V(I))$, wird F von x annuliert

$$\Rightarrow 1 - TF = 1 \neq 0 \ ↯$$

$$\Rightarrow (x_1, \ldots, x_n, t) \notin V(J)$$

Dies zeigt $V(J) = \emptyset$.

Nach dem schwachen Nullstellensatz gilt

$$\begin{aligned} \Rightarrow &\quad J = (1) \\ \Rightarrow &\quad 1 = \sum_i P_i Q_i + A(1 - TF), \end{aligned}$$

wobei $P_i,\ Q_i,\ A \in J$. Da die Elemente aus J formal den Elementen aus IR_F entsprechen, gilt

$$IR_F = (1).$$

□