Leitfaden

Sei k ein Körper. Eine *k-Algebra* $A = (A, +, \mu, \sigma)$ ist eine Menge A mit zwei Abbildungen $+, \mu\colon A \times A \to A$ und einer Abbildung $\sigma\colon k \times A \to A$, so daß $(A, +, \mu)$ ein Ring, und $(A, +, \sigma)$ ein k-Vektorraum ist, wobei zusätzlich gelten soll: $c(a_1a_2) = (ca_1)a_2 = a_1(ca_2)$, für $c \in k$ und $a_1, a_2 \in A$; dabei schreibt man sowohl die Multiplikation μ als auch die Skalarmultiplikation σ wie üblich ohne Verwendung eines Rechenzeichens, manchmal verwendet man auch einen Multiplikationspunkt $\cdot$ zur Verdeutlichung. Zur Erinnerung: Entsprechend unserer Definition hat A (wie jeder Ring) ein Einselement $1 = 1_A$.

Beispiele: k selbst ist eine k-Algebra, dabei stimmen Multiplikation und Skalar-Multiplikation überein. Ist A eine k-Algebra, so ist auch der Polynomring $k[X]$ in einer Variablen X eine k-Algebra; insbesondere ist also $k[X]$ eine k-Algebra. Allgemeiner: der Polynomring $k[X_1, \dots, X_n]$ in n Variablen und alle seine Faktorringe sind k-Algebren.

Sind k-Algebren A, B gegeben, so nennt man eine Abbildung $\phi\colon A \to B$ einen Algebren-Homomorphismus, wenn ϕ sowohl ein Ring-Homomorphismus als auch ein Homomorphismus von k-Vektorräumen (also k-linear) ist.

Sei A eine k-Algebra. Die Zuordnung $c \mapsto c \cdot 1_A$ für $c \in k$ liefert einen Ring-Homomorphismus $k \to A$ (dies ist sogar ein Algebren-Homomorphismus). Da k ein Körper ist, gibt es nur folgende beide Möglichkeiten: Der triviale Fall: der Kern von ϕ ist ganz k, dann ist ϕ die Null-Abbildung, es ist $1_A = 0$ und demnach $A = 0$. Andernfalls ist der Kern von ϕ das Nullideal, also ϕ injektiv: unter ϕ wird k mit einem Unterring von A identifiziert, und zwar mit einem Unterring des Zentrums von A (eine von Null verschiedene k-Algebra ist also nichts anderes als ein Ring, in dessen Zentrum ein zu k isomorpher Unterring fixiert ist, genauer: fixiert ist ein derartiger Isomorphismus).

Sei A eine kommutative k-Algebra. Seien Elemente $a_1, \dots a_n$ gegeben. Es gibt genau einen k-Algebren-Homomorphismus

$$\phi = \phi_{a_1,\dots,a_n}\colon k[X_1, \dots, X_n] \to A \quad \text{mit} \quad \phi(X_i) = a_i,$$

nämlich die Auswertungsabbildung $f = f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n)$. Ist dieser Homomorphimus surjektiv, so ist also A isomorph zu einem Faktorring von $k[X_1, \dots, X_n]$. Eine kommutative k-Algebra A heißt *endlich erzeugt*, wenn es Elemente $a_1, \dots, a_n$ gibt, so daß die Abbildung $\phi_{a_1,\dots,a_n}$ surjektiv ist. (Im ersten Teil dieser Vorlesung werden wir uns vor allem mit endlich erzeugten, kommutativen k-Algebren beschäftigen.) Ist die Abbildung $\phi_{a_1,\dots,a_n}$ injektiv, so heißen die Elemente $a_1, \dots, a_n$ *algebraisch unabhängig* (also genau dann, wenn es kein Polynom $f \neq 0$ gibt mit $f(a_1, \dots, a_n) = 0$); andernfalls heißen sie *algebraisch abhängig.*

I. Einige Grundbegriffe der kommutativen Algebra und der algebraischen Geometrie

Wir wenden uns dem Studium der endlich erzeugten, kommutativen k-Algebren zu, dabei ist k ein Körper; dies sind also die Faktorringe der Polynomringe $k[X_1, \ldots, X_n]$. Herausgearbeitet werden soll der Zusammenhang zwischen Eigenschaften derartiger Ringe einerseits und Eigenschaften geometrischer Objekte andererseits: die geometrischen Objekte, mit denen wir es zu tun haben werden, sind die sogenannten 'algebraischen Mengen', dies sind gewisse Teilmengen des affinen Raums k^n, die durch algebraische Gleichungen beschrieben werden (wie algebraische Kurven oder Flächen).

1. Ganze Elemente, ganze Erweiterungen

Sei S ein kommutativer Ring, sei R ein Unterring. Ein Element $s \in S$ heißt *ganz über* R (oder *ganz-algebraisch* über R) falls es ein **normiertes** Polynom $f \in R[X]$ mit $f(s) = 0$ gibt. Ist jedes Element $s \in S$ ganz über R, so heißt S *ganz über* R.

Bemerkung. Ist $s \in S$ ganz über R, so auch 'algebraisch' (also Nullstelle eines von Null verschiedenen Polynoms mit Koeffizienten in R). Zum Beispiel: $\frac{1}{2}$ ist algebraisch über $\mathbb{Z}$, denn es ist Nullstelle des Polynoms $2X - 1$, aber $\frac{1}{2}$ ist nicht ganz über $\mathbb{Z}$. Dagegen ist $\sqrt{2}$ ganz über $\mathbb{Z}$, nämlich Nullstelle von $X^2 - 2$. In $\mathbb{Q}[\sqrt{2}]$ sind die einzigen über $\mathbb{Z}$ ganzen Elemente diejenigen im Unterring $\mathbb{Z} + \mathbb{Z}\sqrt{2}$. Die entsprechende Aussage gilt in $\mathbb{Q}[\sqrt{5}]$ nicht: natürlich sind alle Elemente aus $\mathbb{Z} + \mathbb{Z}\sqrt{5}$ ganz über $\mathbb{Z}$, aber zusätzlich ist zum Beispiel auch $a = \frac{1}{2}(1 + \sqrt{5})$ ganz über $\mathbb{Z}$, denn es ist Nullstelle von $X^2 - X - 1$ (genauer gilt: In $\mathbb{Q}[\sqrt{2}]$ bilden die über $\mathbb{Z}$ ganzen Elemente den Unterring $\mathbb{Z} + \mathbb{Z}a$).

Einschub: Erinnerung über Determinanten. Sei R ein kommutativer Ring, sei $C = (c_{ij})_{ij}$ eine $(n \times n)$-Matrix mit Koeffizienten c_{ij} in R. Die Determinante $\det C$ von C ist folgendermaßen definiert:

$$\det C = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) c_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)}$$

(hier ist S_n die symmetrische Gruppe vom Grad n). Die Matrix C_{ij} entstehe aus C durch Streichen der i-ten Zeile und der j-ten Spalte. Die *klassische Adjunkte* $\widetilde{C}$ von C hat als Koeffizienten $\widetilde{C}_{ij} = (-1)^{i+j} \det C_{ji}$. Dann gilt: $C\widetilde{C} = \widetilde{C}C$ ist eine Skalarmatrix, und zwar $\det C \cdot I_n$, dabei ist I_n die $(n \times n)$-Einheitsmatrix.

Sei S kommutativer Ring, sei R ein Unterring. Man sagt, daß S *endlich über* R ist, falls es Elemente $s_1, \ldots, s_n \in S$ gibt mit $S = \sum_i Rs_i$ (man sagt auch, S ist ein *endlich erzeugter* R*-Modul*). (Im Fall einer Körpererweiterung ist dies der alte Endlichkeitsbegriff!)

Lemma 1. *Sei S kommutativer Ring, sei R ein Unterring. Ist S endlich über R, so ist S ganz über R.*

Beweis: Seien also Elemente $s_1, \ldots, s_n \in S$ gegeben mit $S = \sum_i Rs_i$. Wir können annehmen, $s_1 = 1$ (sonst füge man 1 noch zu den Elementen s_i hinzu). Sei s in S.

Schreibe $ss_i = \sum r_{ij}s_j$ mit Koeffizienten $r_{ij} \in R$. Man erhält eine $(n \times n)$-Matrix $(r_{ij})_{ij}$. Sei $c_{ij} = s\delta_{ij} - r_{ij}$ (dabei sei $(\delta_{ij})_{ij}$ die Einheitsmatrix), wir erhalten als $C = (c_{ij})_{ij}$ eine $(n \times n)$-Matrix mit Koeffizienten in S.

Wir zeigen, daß gilt: $\det C = 0$. Es ist $\sum_j c_{ij}s_j = 0$, für $1 \le i \le n$. Der Einschub über Determinanten besagt, daß gilt $\det C \cdot \delta_{1j} = \sum_{i=1}^n \tilde{c}_{1i}c_{ij}$, für $1 \le j \le n$. Also sehen wir:

$$\det C = \det C \cdot s_1 = \sum_{j=1}^n \det C \cdot \delta_{1j} \cdot s_j = \sum_{j=1}^n \sum_{i=1}^n \tilde{c}_{1i}c_{ij} \cdot s_j = \sum_{i=1}^n \tilde{c}_{1i} \sum_{j=1}^n c_{ij}s_j = 0.$$

Also gilt: s ist Nullstelle des Polynoms $\det\left((X\delta_{ij} - r_{ij})_{ij}\right)$. Dies ist aber ein normiertes Polynom mit Koeffizienten in R.

Folgerung. *Sei S kommutativer Ring, sei R ein Unterring. Sei $s \in S$. Dann sind äquivalent:*
(i) *s ist ganz über R,*
(ii) *Der Unterring $R[s]$ von S ist endlich über R.*
(iii) *Es gibt einen Unterring S' mit $R \subseteq S' \subseteq S$, der endlich über R ist, mit $s \in S'$.*

Beweis: (i) $\Longrightarrow$ (ii): Sei $f = X^n + \sum_{i=0}^{n-1} r_iX^i$ mit $f(s) = 0$. Dann ist $\sum_{i=0}^{n-1} Rs^i$ ein Unterring von S, der R und s enthält und dies ist sicher der kleinste derartige Unterring, also gleich $R[s]$.

(ii) $\Longrightarrow$ (iii): trivial.

(iii) $\Longrightarrow$ (i): Dies ist gerade die Aussage von Lemma 1.

Lemma 2. *Sei T ein kommutativer Ring, seien $R \subseteq S \subseteq T$ Unterringe. Ist S endlich über R und T endlich über S, so ist T endlich über R.* Beweis: Ist $S = \sum_{i=1}^n Rs_i$ und $T = \sum_{j=1}^m St_j$, so ist $T = \sum_{i,j} Rs_it_j$.

Lemma 3. *Sei T ein kommutativer Ring, sei $R \subseteq T$ ein Unterring. Die Menge der Elemente aus T, die ganz über R sind, bildet einen Unterring.* Man nennt ihn den *ganzen Abschluß von R in T.*

Beweis: Zu zeigen ist folgendes: sind $a, b \in T$ ganz über R, so sind alle Elemente aus $R[a, b]$ ganz über R. Es ist aber $R \subseteq R[a]$ eine endliche Erweiterung, und ebenso ist $R[a] \subseteq R[a, b]$ eine endliche Erweiterung (jeweils verwenden wir (i) $\Longrightarrow$ (ii)). Also ist auch $R \subseteq R[a, b]$ eine endliche Erweiterung. Verwende nun (iii) $\Longrightarrow$ (i).

Es ist wichtig zu wissen, daß Summe und Produkt zweiter über R ganzer Elemente a,b, wieder ganz sind. Kennt man Minimalpolynome für a,b, so ist es allerdings oft gar nicht so einfach, Minimalpolynome für $a+b$ und ab hinzuschreiben. Notfalls bleibt nichts anderes übrig, als das Verfahren im Beweis von Lemma 1 durchzuführen.

Lemma 4. *Sei S ein kommutativer Ring, R ein Unterring von S. Sei r in R. Ist r in S invertierbar und ist r^{-1} ganz über R, so gehört r^{-1} zu R.*

Beweis: Sei r^{-1} Nullstelle des Polynoms $X^n + \sum_{i=0}^{n-1} r_iX^i$ mit $r_i \in R$. Also $r^{-n} + \sum_{i=0}^{n-1} r_ir^{-i} = 0$. Multipliziere mit r^{n-1}. Wir erhalten $r^{-1} = -\sum_{i=0}^{n-1} r_ir^{n-1-i} \in R$.

Folgerung. *Sei $R \subseteq S$ eine ganze Erweiterung. Ist S ein Körper, so ist auch R ein Körper.*

2. Der Noether'sche Normalisierungssatz.

Noether'scher Normalisierungssatz. *Sei k ein Körper und $A = k[a_1, \dots, a_n]$ eine endlich erzeugte, kommutative k-Algebra. Dann gibt es Elemente $b_1, \dots, b_m$ in A mit $0 \le m \le n$, so daß gilt:*
(a) *Die Elemente $b_1, \dots, b_m$ sind algebraisch unabhängig.*
(b) *Der Ring A ist endlich über $k[b_1, \dots, b_m]$.*

Beispiele: Sei $A = k[X_1, X_2]/I$, dabei sei $I = \langle f \rangle$ ein Hauptideal. Sei $a_i = X_i + I \in A$. Ist $f = X_1^2 + X_2^2 - 1$, so nimm zum Beispiel $b_1 = a_2$. Ist $f = X_1 X_2$, so nimm $b_1 = a_1 + a_2$, denn es gilt $a_1^2 - (a_1 + a_2)a_1 = 0$.

Beweis: Induktion nach n. Der Fall $n = 1$ ist klar: entweder a_1 ist algebraisch, dann sei $m = 0$, andernfalls nimm $b_1 = a_1$.

Sei nun $n \ge 2$. Sind die Elemente $a_1, \dots, a_n$ algebraisch unabhängig, so nimm $m = n$ und $b_i = a_i$. Es gebe also $0 \ne f(X_1, \dots, X_n)$ mit $f(a_1, \dots, a_n) = 0$. Wir konstruieren Elemente $a_2', \dots, a_n'$ in A, so daß A endlich über $A' = k[a_2', \dots, a_n']$ ist. (Nach Induktion gibt es dann in A' algebraisch unabhängige Elemente $b_1, \dots, b_m$ mit $m \le n-1$, so daß A' endlich über $B = k[b_1, \dots, b_m]$ ist. Also ist auch A endlich über B, wegen Lemma 2.)

Die Elemente a_i' werden in der Form $a_i - a_1^{\mu_i}$ gewählt. Dann wird aber A durch a_1 und die Elemente $a_2', \dots, a_n'$ erzeugt. Es ist demnach nur sicherzustellen, daß a_1 ganz über $A' = k[a_2', \dots, a_n']$ ist. Zu wählen sind also geeignete Exponenten $\mu_2, \dots, \mu_n$. Gegeben ist das Polynom f, durch Einsetzen von $a_i = a_i' + a_1^{\mu_i}$ geht dies über in einen Term, in dem neben Koeffizienten aus k die Elemente a_1 und $a_2', \dots, a_n'$ vorkommen, wir wollen, daß dies eine 'Ganzheitsgleichung' für a_1 über A' wird.

Schreibe $f = \sum_\tau c_\tau X_1^{\tau_1} \cdots, X_n^{\tau_n}$ mit Koeffizienten $c_\tau \in k$. Definieren wir $Y_i = X_i - X_1^{\mu_i}$, für $2 \le i \le n$, so ist umgekehrt $X_i = Y_i + X_1^{\mu_i}$. Setzen wir diese X_i in ein Monom $X_1^{\tau_1} \cdots, X_n^{\tau_n}$ ein, so erhalten wir $X_1^{\sum_i \tau_i \mu_i} + g_\tau(X_1, Y_2, \dots, Y_m)$, und der Grad von g_τ in der Variablen X_1 ist echt kleiner als $\sum_i \tau_i \mu_i$. Es ist also:

$$
\begin{aligned}
f(X_1, \dots, X_n) &= \sum_\tau c_\tau X_1^{\tau_1} \cdots, X_n^{\tau_n} \\
&= \sum_\tau c_\tau X_1^{\sum_i \tau_i \mu_i} + \sum_\tau c_\tau g_\tau(X_1, Y_2, \dots, Y_m).
\end{aligned}
$$

Wenn nun die Exponenten $\sum_i \tau_i \mu_i$ paarweise verschieden sind (für paarweise verschiende τ), so daß es in der ersten Summe zu keinen Kürzungen kommen kann, so ist der betrachte Term (bis auf einen skalaren Faktor in k) ein normiertes Polynom in X_1 mit Koeffizienten in $k[Y_2, \dots, Y_n]$. Ersetzen wir die Y_i durch die Elemente a_i', so erhalten wir entsprechend ein normiertes Polynom in der Variablen X_1 mit Koeffizienten in A'. Setzen wir für X_1 das Element a_1 ein, so erhalten wir Null.

Also: gegeben sind endlich viele Folgen $\tau = (\tau_1, \dots, \tau_n)$ in $\mathbb{N}_0^n$. Gesucht sind natürliche Zahlen $1 = \mu_1, \mu_2, \dots, \mu_n$, so daß die Zahlen $\sum_i \tau_i \mu_i$ paarweise verschieden sind. Wähle $\mu_i = p^{i-1}$, wobei $p > \tau_i$ für alle gegebenen τ und alle i ist. Denn es gilt: *Seien natürliche Zahlen $q < p$ gegeben. Die Abbildung γ: $\{0, 1, \dots, q\}^n \to \mathbb{Z}$ mit $\gamma(\tau_1, \dots, \tau_n) = \sum \tau_i p^{i-1}$ für $0 \le \tau_i \le q$ ist injektiv.*

Als Folgerung erhalten wir:

Hilbert'scher Nullstellensatz (Erste Fassung). *Sei L ein Körper, sei k ein Unterkörper. Ist L eine endlich erzeugte k-Algebra, so ist $k \subseteq L$ eine endliche Körpererweiterung.*

Beweis: Nach dem Noether'schen Normalisierungssatz gibt es algebraisch unabhängige Elemente $b_1, \dots, b_m$ in K, so daß L endlich über dem Unterring $B = k[b_1, \dots, b_m]$ ist. Da L endlich über B ist, ist mit L auch B ein Körper. Daraus folgt aber sofort $m = 0$, also $B = k$ (denn die einzigen invertierbaren Elemente in einem Polynomring sind die von Null verschiedenen Konstanten).

3. Der Hilbert'sche Nullstellensatz.

Erinnerung. Ein Körper k heißt *algebraisch abgeschlossen*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:
(i) Jedes nicht-konstante Polynom mit Koeffizienten in k besitzt eine Nullstelle.
(i') Jedes irreduzible Polynom mit Koeffizienten in k ist linear.
(ii) Ist $k \subseteq L$ eine algebraische Körpererweiterung, so ist $k = L$.
(ii') Ist $k \subseteq L$ eine endliche Körpererweiterung, so ist $k = L$.

Wir setzen jetzt voraus, daß k ein algebraisch abgeschlossener Körper ist. Der Hilbert'sche Nullstellensatz läßt sich in diesem Spezialfall folgendermaßen formulieren:

Hilbert'scher Nullstellensatz (Zweite Fassung). *Sei k algebraisch abgeschlossener Körper, sei I ein maximales Ideal von $k[X_1, \dots, X_n]$. Dann gilt $k[X_1, \dots, X_n] = k \oplus I$.* (Dabei bezeichnet $k \oplus I$ die direkte Summe des Unterraums k der konstanten Polynome und des Unterraums I; ein Ideal ist ja ein Unterraum.)

Beweis: Sei $L = k[X_1, \dots, X_n]/I$. Natürlich gilt $k \cap I = 0$, denn das einzige Ideal, das invertierbare Elemente eines Rings enthält, ist der Ring selbst (maximale Ideale sind aber echte Ideale). Insbesondere bilden die Restklassen (modulo I) der konstanten Polynome einen zu k isomorphen Unterkörper von L (den wir wieder mit k bezeichnen). Die Restklassen (modulo I) der Variablen $X_1, \dots, X_n$ bilden ein Erzeugendensystem von L als k-Algebra. Die erste Fassung des Nullstellensatzes zeigt, daß L eine endliche Körpererweiterung von k ist, daß also $k = L$ ist. Dies bedeutet aber gerade, daß unter der kanonischen Abbildung $k[X_1, \dots, X_n] \to k[X_1, \dots, X_n]/I = L$ die Menge k der konstanten Polynome surjektiv auf L abgebildet wird. Demnach ist $k + I = k[X_1, \dots, X_n]$.

Ist k ein beliebiger (nicht notwendig algebraisch abgeschlossener) Körper und ist $a = (a_1, \dots, a_n) \in k^n$ gegeben, so ist die Auswertungsabbildung

$$\phi_a\colon\ k[X_1, \dots, X_n] \to A \quad \text{mit} \quad \phi_a(X_i) = a_i,$$

ein surjektiver Ring-Homomorphismus

$$\phi_a\colon\ k[X_1, \dots, X_n] \to k,$$

dessen Kern wir mit I_a bezeichnen wollen; wir nennen ihn ein *Auswertungsideal.* Da wir vorausgesetzt haben, daß k ein Körper ist, ist jedes derartige Auswertungsideal I_a

ein maximales Ideal und es gilt für dieses Ideal $k \oplus I_a = k[X_1, \ldots, X_n]$ (gleicher Beweis wie oben).

Wir können diese Auswertungsideale auch anders beschreiben. Sind $r_1, \ldots, r_n$ Elemente eines kommutativen Rings, so sei $\langle r_1, \ldots, r_n \rangle$ das von diesen Elementen erzeugte Ideal, also $\langle r_1, \ldots, r_n \rangle = \sum_{i=1}^n Rr_i$. Entsprechend sei $\langle P \rangle = \sum_{p \in P} Rp$ das von der Teilmenge $P \subseteq R$ erzeugte Ideal. Es gilt:

$$I_a = \langle X_1 - a_1, \ldots, X_n - a_n \rangle.$$

Beweis: Einerseits gilt trivialerweise $\phi_a(X_i - a_i) = 0$, also die Inklusion "$\supseteq$". Andererseits zeigen wir:

$$k + \langle X_1 - a_1, \ldots, X_n - a_n \rangle = k[X_1, \ldots, X_n],$$

(daraus folgt, daß $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ Codimension höchstens 1 hat; zusammen mit der Inklusion "$\supseteq$" folgt daraus die Behauptung). Um zu sehen, daß jedes Monom zu $U = k + \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ gehört, verwenden wir Induktion: Sei also ein Monom gegeben, wir schreiben es als $X_i \cdot f$, dabei sei f ein Monom kleineren Grades. Es ist $X_i \cdot f = (X_i - a_i)f + a_i f$. Der erste Term $(X_i - a_i)f$ gehört zu $\langle X_i - a_i \rangle$, also zu $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$; nach Induktion gehört f, also auch $a_i f$ zu U; also gehört auch $X_i \cdot f$ zu U.

Hilbert'scher Nullstellensatz (Zweite Fassung, umgeschrieben). *Sei k algebraisch abgeschlossener Körper, sei I ein maximales Ideal von $k[X_1, \ldots, X_n]$. Dann gibt es ein Element $a \in k^n$ mit $I = I_a$.* Die maximalen Ideale von $k[X_1, \ldots, X_n]$ sind also gerade die Auswertungsideale I_a.

Beweis: Sei I ein maximales Ideal von $k[X_1, \ldots, X_n]$. Wie wir wissen, gilt $k \oplus I = k[X_1, \ldots, X_n]$. Jedes Element von $k[X_1, \ldots, X_n]$ läßt sich also in der Form $c + g$ mit $c \in k$ und $g \in I$ schreiben: insbesondere gilt dies für X_i. Schreibe $X_i = a_i + g_i$ mit $a_i \in k, g_i \in I$. Anders gelesen: $g_i = X_i - a_i$ und dies ist ein Element aus I. Wir sehen also: es gilt $\langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq I$. Wir setzen $a = (a_1, \ldots, a_n)$. Da, wie wir wissen, $\langle X_1 - a_1, \ldots, X_n - a_n \rangle = I_a$ ein maximales Ideal ist, folgt die Gleichheit.

Ist P eine Teilmenge von $k[X_1, \ldots, X_n]$, so setzen wir

$$V(P) = \{a \in k^n \mid f(a) = 0 \quad \text{für alle} \quad f \in P\},$$

und nennen dies die *gemeinsame Nullstellenmenge* der Polynome in P; Mengen der Form $V(P)$ nennen wir *algebraische Mengen* (oder genauer *algebraische k-Mengen*; die algebraischen k-Mengen sind also (gewisse) Teilmengen eines affinen Raums $\mathbb{A}^n = k^n$.

Es ist einfach zu sehen, daß $V(P) = V(\langle P \rangle)$ gilt, jede algebraische Menge ist also die gemeinsame Nullstellenmenge eines Ideals.

Hilbert'scher Nullstellensatz (Zweite Fassung, noch einmal umgeschrieben). *Sei k algebraisch abgeschlossener Körper, sei I ein echtes Ideal von $k[X_1, \ldots, X_n]$. Dann ist $V(I) \neq \emptyset$.*

Beweis: Jedes echte Ideal ist in einem maximalen Ideal enthalten (um dies zu sehen, verwendet man bei beliebigen Ringen das Auswahlaxiom; der Polynomring

$k[X_1,\ldots,X_n]$ ist, wie wir sehen werden "noethersch", man braucht daher das Auswahlaxiom nicht). Also gilt $I \subseteq I_a$ für gewisse Elemente $a \in k$. Dies besagt aber gerade $f(a) = 0$ für alle $f \in I$, also $a \in V(I)$.

Hilbert'scher Nullstellensatz (Dritte Fassung). *Sei k algebraisch abgeschlossener Körper. Sei I ein Ideal in $k[X_1,\ldots,X_n]$, sei $f \in k[X_1,\ldots,X_n]$. Gilt $f(a) = 0$ für alle $a \in V(I)$, so gibt es $m \in \mathbb{N}$ mit $f^m \in I$.*

Dies ist natürliche eine Verschärfung der zweiten Fassung: Ist I ein maximales Ideal, aber kein Auswertungsideal, so ist $V(I) = \emptyset$, und demnach ist die Bedingung '$f(a) = 0$ für alle $a \in V(I)$' trivialerweise für alle f erfüllt, insbesondere auch für das Einselement. Aber keine Potenz des Einselements liegt in I.

Beweis ("Trick von Rabinowitsch"): Wir können $f \neq 0$ voraussetzen. Wir fassen $k[X_1,\ldots,X_n]$ als Unterring von $B = k[X_1,\ldots,X_{n+1}]$ auf. Sei J das von I und dem Element $X_{n+1}f - 1$ erzeugte Ideal von B. Angenommen, $J \neq B$. Dann gibt es nach der letzten Fassung des Nullstellensatzes ein $b = (b_1,\ldots,b_{n+1}) \in V(J)$. Für jedes $g \in I$ gilt demnach $g(b_1,\ldots,b_n) = 0$ (die letzte Variable X_{n+1} kommt ja in den Polynomen in I nicht vor), und es ist $b_{n+1}f(b_1,\ldots,b_n) = 1$. Wir sehen also, daß $(b_1,\ldots,b_n)$ zu $V(I)$ gehört, nach Voraussetzung muß demnach $f(b_1,\ldots,b_n) = 0$ sein, dies widerspricht aber der Existenz des Elements b_{n+1} mit $b_{n+1}f(b_1,\ldots,b_n) = 1$.

Also gilt $B = J$, das heißt, das Einselement 1_B gehört zu J. Es gilt demnach Elemente $g_1,\ldots,g_t$ in I und $h_1,\ldots,h_{t+1} \in B$ mit

$$1 = \sum_{i=1}^{t} g_i h_i + (X_{n+1}f - 1) \cdot h_{t+1}.$$

Dies ist eine Gleichheit in $k[X_1,\ldots,X_{n+1}]$. Wir verwenden nun die Auswertungsabbildung

$$\phi\colon\ k[X_1,\ldots,X_{n+1}] \longrightarrow k(X_1,\ldots,X_n)$$

mit $\phi(X_i) = X_i$ für $1 \leq i \leq n$ und $\phi(X_{i+1}) = \frac{1}{f}$. Der letzte Summand geht auf 0, wir erhalten also

$$1 = \sum_{i=1}^{t} g_i(X_1,\ldots,X_n) h_i(X_1,\ldots,X_n,\tfrac{1}{f}).$$

Durch Multiplikation mit einer geeigneten Potenz von f wird erreicht, daß rechts keine Nenner auftreten: sei etwa $f^m h_i(X_1,\ldots,X_n,\frac{1}{f}) \in k[X_1,\ldots,X_n]$, für alle $1 \leq i \leq t$. Bezeichnen wir diese Polynome mit $\tilde{h}_i(X_1,\ldots,X_n) = f^m h_i(X_1,\ldots,X_n,\frac{1}{f})$, so gilt

$$f^m = \sum_{i=1}^{t} g_i(X_1,\ldots,X_n)\tilde{h}_i(X_1,\ldots,X_n),$$

also ist $f^m \in I$.

Ist I ein Ideal in einem kommutativen Ring R, so nennen wir die Menge der Elemente $r \in R$, für die es eine natürliche Zahl $t = t(r)$ mit $r^t \in I$ gibt, den *Radikalabschluß von I*, dies ist wieder ein Ideal. Den Radikalabschluß des Nullideals (also die Menge der nilpotenten Elemente von R) nennt man das *Radikal* (oder auch das

Nilradikal) von R. Ein kommutativer Ring R heißt *reduziert* (oder eben *nullteilerfrei*), falls er (außer Null) keine nilpotenten Elemente besitzt, wenn also das Nilradikal von R Null ist. Ist R ein beliebiger kommutativer Ring, und bezeichnen wir mit $N(R)$ sein Nilradikal, so ist $R/N(R)$ ein reduzierter Ring. (Die meisten Texte nennen den Radikalabschluß eines Ideals I einfach das 'Radikal' des Ideals, so daß sich die eher merkwürdige Setzung ergibt: das Radikal eines Rings ist das 'Radikal' des Nullideals).

Ist S eine Teilmenge von k^n, so sei $I(S)$ die Menge der Polynome $f \in k[X_1, \ldots, X_n]$ mit $f(a) = 0$ für alle $a \in S$. Dies ist natürlich ein Ideal von $k[X_1, \ldots, X_n]$.

Hilbert'scher Nullstellensatz (Dritte Fassung, umgeschrieben): *Sei k algebraisch abgeschlossener Körper. Sei J ein Ideal in $k[X_1, \ldots, X_n]$, sei $f \in k[X_1, \ldots, X_n]$. Es ist $I(V(J))$ gerade der Radikalabschluß von J.*

Beweis: Die vorangegangene dritte Fassung besagt, daß $I(V(J))$ im Radikalabschluß von J enthalten ist. Die Umkehrung gilt trivialerweise: Sei $f \in k[X_1, \ldots, X_n]$ gegeben. Gibt es eine natürliche Zahl t mit $f^t \in J$, so gilt für $a \in V(J)$ natürlich $f^t(a) = 0$. Aber $f^t(a) = (f(a))^t$ ist ein Element des Körpers k und k besitzt keine Nullteiler: es folgt also $f(a) = 0$, also $f \in I(V(J))$.

Hilbert'scher Nullstellensatz (Dritte Fassung, noch einmal umgeschrieben): *Sei k algebraisch abgeschlossener Körper. Sei J ein Ideal in $k[X_1, \ldots, X_n]$. Der Radikalabschluß von J ist Durchschnitt von Auswertungsidealen.* Insbesondere gilt also: Der Radikalabschluß von J ist der Durchschnitt aller maximalen Ideale, die J enthalten.

Beweis: Der Radikalabschluß von J ist $I(V(J))$. Für jede Teilmenge $S \subseteq k^n$ ist $I(S) = \bigcap_{a \in S} I(\{a\})$, aber $I(\{a\})$ ist gerade das Auswertungsideal I_a.

Bemerkung 1. In den vorangegangenen Sätzen ist die Voraussetzung, daß k ein algebraisch abgeschlossener Grundkörper ist, wesentlich. Gibt es nämlich ein irreduzibles Polynom $f \in k[X]$ mit Grad $d \geq 2$, so betrachte das von f erzeugte Hauptideal $J = \langle f \rangle$. Die Kodimension von J in $k[X]$ ist d, also ist $k \oplus J$ ein echter Unterraum von $k[X]$, und demnach kann J kein Auswertungsideal sein. Da f keine Nullstelle in k besitzt, ist $V(f) = \emptyset$. Das Ideal J ist sein eigener Radikalabschluß (denn $k[X]/J$ ist ein Körper, also nullteilerfrei), dagegen ist $I(V(J)) = I(\emptyset) = k[X]$.

Ist f ein nilpotentes Element im kommutativen Ring R, so liegt R in jedem maximalen Ideal I (denn R/I ist ein Körper, also nullteilerfrei). Demnach ist das Nilradikal $N(R)$ im Durchschnitt aller maximalen Ideale enthalten.

Folgerung. *Sei k algebraisch abgeschlossener Körper. Sei A eine endlich erzeugte, kommutative k-Algebra. Dann ist das Nilradikal von A der Durchschnitt aller maximalen Ideale.*

Beweis: Da A endlich erzeugte, kommutative k-Algebra ist, gibt es einen surjektiven Algebren-Homomorphismus ϕ: $k[X_1, \ldots, k_n] \to A$, sei J sein Kern. Unter ϕ wird der Radikalabschluß von J auf das Nilradikal $N(A)$ von A abgebildet. Da J Durchschnitt von maximalen Idealen ist, ist $N(A)$ Durchschnitt von maximalen Idealen. Da $N(A)$ im Durchschnitt D aller maximalen Ideale enthalten ist, gilt $N(A) = D$.

Bemerkung 2. Beispiel einer kommutativen k-Algebra A mit Nilradikal 0, die ein einziges maximales Ideal I besitzt, wobei $I \neq 0$ gilt: Betrachte den Körper $K = k(X)$ der rationalen Funktionen in einer Variablen X. Die Menge der Elemente der Form $\frac{f}{g}$ mit $f, g \in k[X]$ und $g(0) \neq 0$ bildet einen Unterring $A = k[X]_{(X)}$, der ein einziges maximales Ideal I enthält, nämlich das von X erzeugte Hauptideal $\langle X \rangle = \{\frac{f}{g} \mid f, g \in k[X] \quad \text{mit} \quad f(0) = 0, g(0) \neq 0\}$. Andererseits ist A sicher reduziert, da A Unterring eines Körpers ist: es ist also $N(A) = 0$.

4. Primideale und Durchschnitte von Primidealen in kommutativen Ringen

Sei R ein Ring. Die folgenden Überlegungen beschäftigen sich mit Idealen in R. Eine Menge $\mathcal{I}$ von Idealen heißt *Kette,* wenn je zwei Ideale I, I' aus $\mathcal{I}$ vergleichbar sind (also $I \subseteq I'$ oder $I' \subseteq I$ gilt). Ist $\mathcal{I}$ eine endliche Kette von Idealen, so können wir die Ideale in $\mathcal{I} = \{I_0, I_1, \dots, I_t\}$ so durchnumerieren, daß gilt

$$I_0 \subset I_1 \subset \cdots \subset I_t,$$

man nennt t die *Länge* dieser Kette (ist t die Länge der Kette $\mathcal{I}$, so hat $\mathcal{I}$ gerade die Kardinalität $t+1$). Ist $\mathcal{I}$ eine Kette von Idealen, so ist natürlich auch jede Teilmenge $\mathcal{I}'$ von $\mathcal{I}$ eine Kette und man nennt $\mathcal{I}$ eine *Verfeinerung* der Kette $\mathcal{I}'$. (Entsprechende Formulierungen verwendet man bei 'Ketten von Untergruppen' einer Gruppe, usw.)

Ein Ideal I eines kommutativen Rings R heißt *Primideal,* wenn R/I ein Integritätsbereich ist. Offensichtlich gilt: Ein Ideal I von R ist genau dann ein Primideal, wenn einerseits $I \neq R$ gilt, und wenn andererseits für Elemente $r_1, r_2 \in R$ aus $r_1 r_2 \in I$ folgt, daß mindestens eines der beiden Elemente r_1, r_2 zu I gehört.

Beispiele: Sei R kommutativer Ring. *Alle maximalen Ideale von R sind Primideale* (denn ist I maximales Ideal, so ist R/I ein Körper, also ein Integritätsbereich). *Ist $r \in R$ Primelement, so ist $\langle r \rangle$ ein Primideal.*

Für Primideale gilt: *Sei P ein Primideal in R, seien I, J Ideale in R. Ist $IJ \subseteq P$, so gilt $I \subseteq P$ oder $J \subseteq P$. Ist $I \cap J \subseteq P$, so gilt $I \subseteq P$ oder $J \subseteq P$.* Beweis: Es ist $IJ \subseteq I \cap J$, daher ist nur die erste Aussage zu zeigen. Wir nehmen an, daß I nicht in P enthalten ist, also gibt es ein $x \in I$ mit $x \notin P$. Ist $y \in J$, so ist $xy \in IJ \subseteq P$. Da P Primideal ist und wir vorausgesetzt haben, daß $x \notin P$ gilt, sehen wir: $y \in P$, also $J \subseteq P$.

Eine Teilmenge M eines Rings R heißt *multiplikativ abgeschlossen*, wenn das Produkt zweier Elemente aus M wieder zu M gehört und zusätzlich auch $1_R \in M$ gilt. *Ein Ideal I des kommutativen Rings R ist genau dann ein Primideal, wenn $R \setminus I$ multiplikativ abgeschlossen ist.* Ist I ein Ideal des Rings R, so ist natürlich 0 nicht in $R \setminus I$ enthalten.

Man kann nun multiplikativ abgeschlossene Teilmengen M eines kommutativen Rings mit $0 \notin M$ verwenden, um Primideale zu konstruieren: Nach dem Zorn'schen Lemma gibt es zu M ein Ideal I_0, das maximal mit der Eigenschaft $I_0 \cap M = \emptyset$ ist (d.h.: einerseits gilt $I_0 \cap M = \emptyset$, andererseits gilt $I' \cap M \neq \emptyset$ für jedes Ideal I' von R mit $I_0 \subset I'$). (Hinweis: um das Zorn'sche Lemma anwenden zu können, muß man wissen, daß es überhaupt Ideale I mit $I \cap M = \emptyset$ gibt: die Voraussetzung $0 \notin M$ garantiert, daß das Nullideal diese Eigenschaft hat; andererseits ist festzuhalten, daß gilt: Ist $\mathcal{I}$ eine Kette von Idealen mit $I \cap M = \emptyset$ für alle $I \in \mathcal{I}$, so erfüllt auch $I' = \bigcup_{I \in \mathcal{I}} I$ die Bedingung $I' \cap M = \emptyset$.) Es gilt nun:

Primideallemma. *Sei M eine multiplikative Menge in R, die 0 nicht enthält. Sei P ein Ideal in R, das maximal ist mit der Eigenschaft $P \cap M = \emptyset$. Dann ist P ein Primideal.*

Beweis: Seien y_1, y_2 Elemente aus R, die nicht zu P gehören: zu zeigen ist, daß auch y_1y_2 nicht zu P gehört. Die Maximalität von P zeigt, daß $(P + Ry_i) \cap M \neq \emptyset$ für $i = 1, 2$ gilt. Also gibt es $p_i \in P, r_i \in R$ mit $p_1 + r_1y_1, p_2 + r_2y_2 \in M$. Das Produkt

$$(p_1 + r_1y_1)(p_2 + r_2y_2) = (p_1 + r_1y_1)p_2 + p_1r_2y_2 + r_1r_2y_1y_2$$

gehört zu M, da M multiplikativ abgeschlossen ist. Wäre $y_1y_2 \in P$, so läge dieses Produkt auch in P, unmöglich.

Lemma 2. *Das Nilradikal $N(R)$ ist der Durchschnitt aller Primideale von R.*

Beweis: Ist $x \in R$ nilpotent, und P ein Primideal, so folgt aus $x^t = 0 \in P$, daß $x \in P$. Sei D der Durchschnitt aller Primideale. Wir sehen: $N(R) \subseteq D$.

Umgekehrt: Sei $x \in R$ nicht nilpotent. Sei $M = \{x^t \mid t \in \mathbb{N}_0\}$. Dies ist eine multiplikative Menge, die das Element 0 nicht enthält. Sei P ein Ideal mit $P \cap M = \emptyset$, und maximal mit dieser Eigenschaft. Dann ist P ein Primideal. Zu jedem nicht nilpotenten Element $x \in R$ haben wir also ein Primideal P_x von R gefunden mit $x \notin P_x$. Also ist $D \subseteq N(R)$.

Ein Ideal I im kommutativen Ring R heißt *reduziert,* wenn R/I reduzierter Ring ist.

Folgerung. *Die reduzierten Ideale sind gerade die Ideale, die sich als Durchschnitte von Primidealen schreiben lassen.*

Lemma 3. *Ist I ein reduziertes Ideal, aber kein Primideal, so gibt es reduzierte Ideale I_1, I_2, die beide I echt enthalten, mit $I = I_1 \cap I_2$.*

Beweis: Sei I reduziertes Ideal von R, aber kein Primideal. Dann gibt es Elemente $x_1, x_2 \in R \setminus I$ mit $x_1x_2 \in R$. Sei I_i der Radikalabschluß von $I + Rx_i$. Es ist natürlich $I \subset I + Rx_i \subseteq I_i$. Sei $\mathcal{P}$ die Menge der Primideale P mit $I \subseteq P$. Da I reduziertes Ideal ist, ist $I = \bigcap_{P \in \mathcal{P}} P$. Wir zeigen, daß für jedes $P \in \mathcal{P}$ gilt: $I_1 \cap I_2 \subseteq P$. Es ist $x_1x_2 \in I \subseteq P$, also $x_1 \in P$ oder $x_2 \in P$. Ist $x_1 \in P$, so ist $I + Rx_1 \subseteq P$, also $I_1 \subseteq P$, und demnach $I_1 \cap I_2 \subseteq P$. Entsprechendes gilt für $x_2 \in P$. Aus $I \subseteq I_1 \cap I_2 \subseteq \bigcap_{P \in \mathcal{P}} P = I$ folgt nun $I = I_1 \cap I_2$.

Sei I ein Ideal. Wir sagen, daß ein Primideal P *minimal über I* ist, wenn einerseits $I \subseteq P$ gilt und wenn es andererseits kein Primideal P' mit $I \subseteq P' \subset P$ gibt.

Lemma 4. *Sei I Durchschnitt von endlich vielen Primidealen $P_1, \ldots, P_n$. Die Ideale P_i seien paarweise unvergleichbar. Dann sind diese Ideale P_i gerade die minimalen Primideale über I.* Insbesondere ist die Menge $\{P_1, \ldots, P_n\}$ durch I eindeutig bestimmt.

Beweis: Sei P ein Primideal mit $I \subseteq P$. Aus $\bigcap_{i=1}^n P_n \subseteq P$ folgt $P_i \subseteq P$ für mindestens ein i. Ist also P minimales Primideal über I, so gilt $P_i = P$. Andererseits sehen wir auch, daß die Ideale P_i minimale Primideale über I sind.

Einschub über den Transzendenzgrad einer Körper-Erweiterung.

Sei $k \subseteq K$ eine Körpererweiterung.

Eine Teilmenge T von K heißt *Transzendenzbasis* von K über k, wenn gilt:

(a) Die Elemente von T sind algebraisch unabhängig (über k).

(b) Ist K' der von k und T erzeugte Unterkörper von K, so ist K algebraisch über K'.

(1) *Jede über k algebraisch unabhängige Teilmenge von K läßt sich zu einer Transzendenzbasis von K über k vervollständigen.*

(2) *Ist S eine Teilmenge von K, so daß K algebraisch über dem von k und S erzeugten Unterkörper ist, so gibt es eine Teilmenge von S, die eine Transzendenzbasis ist.*

(3) *Je zwei Transzendenzbasen von K über k haben die gleiche Kardinalität.* Man nennt diese Kardinalität den *Transzendenzgrad von K über k* und schreibt.

(4) *Sind Körpererweiterungen $k_0 \subseteq k_1 \subseteq k_2$ gegeben, und ist T_1 eine Transzendenzbasis von k_1 über k_0 und ist T_2 eine Transzendenzbasis von k_2 über k_1, so ist die Vereinigung von T_1, T_2 eine Transzendenzbasis von k_2 über k_0* (und die Mengen T_1, T_2 sind natürlich disjunkt); der Transzendenzgrad von k_2 über k_0 ist also die Summe der Transzendenzgrade von k_1 über k_0 und von k_2 über k_1.

Die Beweise sind ähnlich zu den entsprechenden Sätzen über Basen, linear unabhängige Teilmengen und Erzeugendensysteme von Vektorräumen. Sie beruhen wie dort auf einem 'Austausch-Lemma'.

(5) Sei A eine kommutative k-Algebra ohne Nullteiler (also ein Integritätsbereich), so können wir den Quotientenkörper K von A bilden: wir erhalten eine Körper-Erweiterung $k \subseteq K$. Es gilt nun: *Ist A eine endlich erzeugte, kommutative k-Algebra ohne Nullteiler, und ist t der Transzendenzgrad des Quotientenkörpers von A über k, so gibt es in A algebraisch unabhängige Elemente $b_1, \ldots, b_t$ so daß A endlich über $k[b_1, \ldots, b_t]$ ist.* Der Noether'sche Normalisierungssatz liefert algebraisch unabhängige Elemente $b_1, \ldots, b_m$ von A, so daß A endlich über $k[b_1, \ldots, b_m]$ ist. Die Menge der Elemente $b_1, \ldots, b_m$ ist offensichtlich eine Transzendenzbasis von K, es ist also $m = t$.

Beispiel: *Ist $0 \neq f \in A = k[X_1, \ldots, X_n]$ ein irreduzibles Polynom, so ist $A/\langle f \rangle$ eine endlich erzeugte, kommutative k-Algebra ohne Nullteiler, und der Transzendenzgrad des Quotientenkörpers von $A/\langle f \rangle$ über k ist $n-1$.* Die k-Algebra $A/\langle f \rangle$ wird erzeugt von den Restklassen der Elemente $X_1, \ldots, X_n$, und das Polynom f zeigt, daß diese Restklassen algebraisch abhängig sind. Also ist der Transzendenzgrad des Quotientenkörpers K von $A/\langle f \rangle$ über k höchstens $n-1$. Wir können annehmen, daß die Variable X_n wirklich in f vorkommt (ansonsten Umnumerierung der Variablen), daher sind die Restklassen der Elemente $X_1, \ldots, X_{n-1}$ modulo $\langle f \rangle$ algebraisch unabhängig. Dies zeigt, daß der Transzendenzgrad von K über k mindestens $n-1$ ist.

5. Primidealketten im Polynomring $k[X_1, \ldots, X_n]$

Eine *Primidealkette* ist eine Idealkette, deren Glieder Primideale sind. Das Supremum der Längen aller Primidealketten in R nennt man die *Krull-Dimension* des Rings R.

Satz. *Ist P ein Primideal in A, so ist die Krull-Dimension von A/P gerade der Transzendenzgrad des Quotientenkörpers von A/P über k.* Insbesondere ist die Krull-Dimension von $k[X_1, \ldots, X_n]$ gerade n.

Für den Beweis werden einige Vorüberlegungen benötigt.

Lemma 0. *Sei S ein kommutativer Ring, sei $R \subseteq S$ ein Unterring. Ist Q ein Primideal von S, so ist $Q \cap R$ ein Primideal von R.*

Beweis: Die Hintereinanderschaltung $R \subseteq S \to S/Q$ der Inklusion $R \subseteq S$ und der kanonischen Projektion $S \to S/Q$ has als Kern $R/(Q \cap R)$. Das Bild dieser Hintereinanderschaltung ist ein Unterring des Integritätsbereichs S/Q, also selbst ein Integritätsbereich.

Lemma 1. *Sei S ein kommutativer Ring, sei R ein Unterring. Sei P ein Primideal in R. Sei Q ein Ideal in S, das maximal mit der Eigenschaft $Q \cap R \subseteq P$ ist. Dann ist Q ein Primideal von S. Ist S ganz über R, so gilt $Q \cap R = P$.*

Beweis: Sei $M = R \setminus P$, dies ist eine multiplikative Menge in S, die 0 nicht enthält. Die Eigenschaft $Q \cap R \subseteq P$ sagt aber gerade $Q \cap M = \emptyset$. Also folgt die erste Behauptung aus dem Primideallemma.

Sei nun S ganz über R, und sei p ein Element von P. Angenommen, es liegt nicht in $Q \cap R$, also nicht in Q. Die Maximalität von Q liefert $q \in Q, s \in S$, so daß $x = q + sp$ zu R, aber nicht zu P gehört. Da s ganz über R ist, gibt es eine Gleichung

$$s^n + \sum_{i=0}^{n-1} r_i s^i = 0$$

mit Koeffizienten $r_i \in R$. Multiplikation mit p^n liefert

$$(sp)^n + \sum_{i=0}^{n-1} r_i p^{n-i} (sp)^i = 0.$$

Es ist $sp = x - q$ mit $q \in Q$, also gilt $sp \equiv x \pmod{Q}$, und demnach ist

$$x^n + \sum_{i=0}^{n-1} r_i p^{n-i} x^i \equiv 0 \pmod{Q}.$$

Die linke Seite bezeichnet ein Element aus R, also aus $Q \cap R \subseteq P$. Die Summanden $r_i p^{n-i} x^i$ gehören zu P, also liegt auch x^n in P. Da P ein Primideal ist, folgt $x \in P$, ein Widerspruch.

Folgerung ("Going up"). *Sei S ein kommutativer Ring, sei R ein Unterring und sei S ganz über R. Seien $P_0 \subset P_1$ Primideale von R. Ist Q_0 ein Primideal in S mit $Q_0 \cap R = P_0$, so gibt es ein Primideal Q_1 in S mit $Q_0 \subset Q_1$ und $Q_1 \cap R = P_1$.*

Die (übliche) Bezeichnung dieser Aussage als "Going up" bezieht sich darauf, daß man dabei ist, eine *aufsteigende* Primidealkette zu konstruieren: Zu Q_0 wird Q_1 mit $Q_0 \subset Q_1$ konstruiert (es gibt entsprechende "Going down" Sätze: hier wird zu einem Primideal Q ein Primideal Q' mit $Q'{\subset}Q$ gesucht). In beiden Fällen ist eine Ring-Erweiterung $R{\subset}S$ und eine Primidealkette im Ring R gegeben, gesucht ist jeweils eine zugehörige Primidealkette in S. Bezüglich der Ringe geht man also in beiden Fällen vom kleineren zum größeren Ring über; der umgekehrte Prozess des Übergangs vom größeren zum kleineren Ring ist unproblematisch, siehe Lemma 0.

Beweis: Wähle als Q_1 ein Ideal von S, das Q_0 enthält, und das maximal mit der Eigenschaft $Q_1{\cap}R \subseteq P_1$ ist (das Zorn'schen Lemma liefert die Existenz eines derartigen Ideals). Lemma 1 besagt nun, daß Q_1 ein Primideal ist und daß $Q_1 \cap R = P_1$ gilt.

Lemma 2. *Sei S ein kommutativer Ring, sei R ein Unterring und sei S ganz über R. Sind $Q_0 \subset Q_1$ Primideale in S, so ist $Q_0 \cap R \subset Q_1 \cap R$.*

Beweis: Angenommen, $Q_0{\cap}R = Q_1{\cap}R$. Sei $y \in Q_1 \backslash Q_0$. Da y ganz über R ist, gibt es ein normiertes Polynom f in $R[X]$ mit $f(y) = 0$, also gibt es normierte Polynome g in $R[X]$ mit $g(y) \in Q_0$. Wähle ein derartiges Polynom g mit kleinstmöglichem Grad, etwa

$$g(y) = y^n + r_{n-1}y^{n-1} + \cdots + r_1y + r_0 \in Q_0,$$

mit Koeffizienten $r_i \in R$. Da y zu Q_1 gehört, und $Q_0 \subset Q_1$ gilt, gehört auch r_0 zu Q_1, also zu $Q_1 \cap R = Q_0 \cap R \subseteq Q_0$, also sehen wir:

$$y(y^{n-1} + r_{n-1}y^{n-2} + \cdots + r_1) \in Q_0.$$

Für $n = 1$ folgt $y \in Q_0$, ein Widerspruch. Für $n \geq 2$ folgt wegen $y \notin Q_0$, daß die Klammer zu Q_0 gehört (denn Q_0 ist ein Primideal. Dies widerspricht aber der Minimalität des Grads von g.

Folgerung. *Sei S ein kommutativer Ring, sei R ein Unterring und sei S ganz über R. Ist*

$$Q_0 \subset Q_1 \subset \cdots \subset Q_d$$

eine Primidealkette in S der Länge d, so ist

$$Q_0 \cap R \subset Q_1 \cap R \subset \cdots \subset Q_d \cap R$$

eine Primidealkette in R der Länge d, und man erhält auf diese Weise alle Primidealketten von R der Länge d.

Insbesondere gilt: *Ist $R \subseteq S$ eine ganze Erweiterung kommutativer Ringe, so haben R und S die gleiche Krull-Dimension.*

Lemma 3. *Sei k ein Körper. Sei P ein Primideal von $A = k[X_1, \ldots, X_n]$. Dann gibt es ein irreduzibles Polynom $f \in k[X_1, \ldots, X_n]$ mit $\langle f \rangle \subseteq P$.*

Beweis: Sei $0 \neq g \in P$. Wir können $g = g_1g_2 \cdots g_t$ mit irreduziblen Faktoren g_i schreiben, denn A ist faktorieller Ring. Da P Primideal ist, liegt mindestens ein g_i in P, also ist $\langle g_i \rangle \subseteq P$.

Beweis des Satzes durch Induktion nach n, mit Induktionsanfang $n = 0$. Sei $n \geq 1$. Sei eine Primidealkette

$$(*) \qquad 0 = P_0 \subset P_1 \subset \cdots \subset P_d$$

in $A = k[X_1, \ldots, X_n]$ gegeben. Wegen Lemma 3 können wir annehmen, daß $P_1 = \langle f \rangle$ gilt, dabei ist $f \in A$ ein irreduzibles Polynom. Es gibt keine Primideale P mit $0 \subset P \subset \langle f \rangle$, die Primidealketten in A, die mit 0 und $\langle f \rangle$ beginnen, entsprechen bijektiv den Primidealketten im Faktorring $A/\langle f\rangle$ (dabei wird der Primidealkette $(*)$ in A die Primidealkette

$$(**) \qquad 0 = \langle f\rangle/\langle f\rangle \subset P_2/\langle f\rangle \subset \cdots \subset P_d/\langle f\rangle$$

zugeordnet). Wie wir wissen, gibt es algebraisch unabhängige Elemente $b_1, \ldots, b_{n-1}$ in $A/\langle f\rangle$, so daß $A/\langle f\rangle$ endlich über $B = k[b_1, \ldots, b_{n-1}]$ ist. Die Primidealkette $(**)$ liefert durch Schnitt mit B eine Primidealkette in B der Länge $d-1$ (Lemma 2). Nach Induktion ist $d-1 \leq n-1$, also $d \leq n$. Die Ideale der Form $I_i = \langle X_1, \ldots, X_i\rangle$ bilden eine Primidealkette in A der Länge n.

Sei nun P ein beliebiges Primideal in A und A/P habe Transzendenzgrad t. Dann gibt es in A/P algebraisch unabhängige Elemente $b_1, \ldots, b_t$, so daß A/P endlich über $B = k[b_1, \ldots, b_t]$ ist. Die Folgerung zu Lemma 2 besagt, daß A/P und B gleiche Krull-Dimension haben. Also ist die Krull-Dimension von A/P gleich t.

Bemerkung. Üblicherweise haben nicht alle maximalen Primidealketten eines kommutativen Rings gleiche Länge. Betrachte etwa im Körper $k(X)$ der rationalen Funktionen in einer Variablen X den Unterring $A = k[X]_{(X)}$ aller Elemente $\frac{f}{g}$ mit $f, g \in k[X]$ und $g(0) \neq 0$. *Im Polynomring $k[Y]$ gibt es maximale Primidealketten der Länge 1 wie der Länge 2.* Der Ring-Homomorphismus ϕ: $k[Y] \to k(X)$, der die Elemente aus A auf sich und Y auf $\frac{1}{X}$ schickt, hat als Kern das Haupideal $I = \langle XY-1\rangle$. Da ϕ surjektiv ist, ist I ein maximales Ideal. Die Kette

$$0 \subset \langle XY - 1\rangle$$

ist eine maximale Primidealkette (und hat Länge 1). Andererseits haben wir auch die (maximale) Primidealkette

$$0 \subset \langle Y\rangle \subset \langle X, Y\rangle.$$

6. Minimale Primideale in Faktorringen von $k[X_1, \ldots, X_n]$

Wir wollen zeigen:

Satz. *Sei k Körper. Jede endlich erzeugte, kommutative k-Algebra besitzt nur endlich viele minimale Primideale.*

Dazu brauchen wir eine Eigenschaft dieser endlich erzeugten, kommutativen k-Algebren, die auch an vielen anderen Stellen von Bedeutung sein wird: sie sind 'noethersch'. Diese Begriffsbildung soll auch für nicht notwendig kommutative Ringe vorgestellt werden.

Ist R ein (nicht notwendig kommutativer) Ring, so nennt man eine nicht-leere Teilmenge L von R ein *Linksideal*, falls die folgenden beiden Eigenschaften gelten:

(1) (Abgeschlossenheit unter der Addition): Sind $x_1, x_2 \in I$, so ist auch $x_1 + x_2 \in I$.

(2) Ist $x \in I$ und $r \in R$, so gehört auch rx zu I.

Ist L ein Linksideal, so ist L eine Untergruppe von $(R, +)$, denn mit x gehört wegen der Bedingung (2) auch $-x = (-1)x$ zu L.

Eine Kette $\mathcal{I}$ von Linksidealen heißt *aufsteigend*, wenn es zu jedem $I \in \mathcal{I}$ nur endlich viele Ideale $I' \in \mathcal{I}$ mit $I' \subset I$ gibt.

Lemma. *Sei R ein Ring. Die folgenden Aussagen sind äquivalent:*

(i) *Jedes Linksideal von R ist endlich erzeugt.*

(ii) *Ist $\mathcal{I}$ eine nicht-leere Menge von Linksidealen von R, so gibt es in $\mathcal{I}$ ein maximales Element.*
(iii) *Jede aufsteigende Kette von Linksidealen von R ist endlich.*

Wenn diese Bedingungen erfüllt sind, so heißt R *links-noethersch*; man sagt in diesem Fall auch, daß *jede aufsteigende Kette abbricht,* und nennt dies die *aufsteigende Kettenbedingung.* (Ist R kommutativ und erfüllt diese Bedingungen, so nennt man ihn *noethersch*).

Beweis der Äquivalenz: (i) $\implies$ (iii): Angenommen es gibt eine aufsteigende Kette von Linksidealen, die nicht abbricht:

$$L_0 \subset L_1 \subset \cdots \subset L_s \subset L_{s+1} \subset \ldots$$

Sei $L = \bigoplus_{j\in\mathbb{N}_0} L_j$. Dies ist ein Linksideal, also endlich erzeugt. Sei etwa $L = \sum_{i=1}^t Rx_i$ mit $x_i \in L$. Jedes dieser Elemente x_i gehört zu L, also zu einem $L_{j(i)}$ mit $j(i) \in \mathbb{N}_0$. Ist s das Maximum von $j(1), \ldots, j(t)$, so liegen alle x_i in L_s, es ist also $L \subseteq L_s$. Dies widerspricht aber der Tatsache, daß L_s eine echte Teilmenge von $L_{s+1} \subseteq L$ ist.

(iii) $\implies$ (ii): Offensichtlich.

(ii) $\implies$ (ii): Sei L ein Linksideal von R. Sei $\mathcal{I}$ die Menge der endlich erzeugten Linksideale $L' \subseteq L$ von R. Wegen (ii) besitzt $\mathcal{I}$ ein maximales Element, etwa L_0. Ist nun $x \in L$, so ist auch L_0+Rx endlich erzeugtes Linksideal von R. Wegen $L_0 \subseteq L_0+Rx$ und der Maximalität von L_0 folgt $x \in L_0$. Wir sehen also: $L_0 = L$.

Hilbert'scher Basissatz. *Ist R links-noetherscher Ring, so ist auch $R[X]$ links-noetherscher Ring.*

Beweis: Sei L ein Linksideal von $R[X]$, das nicht endlich erzeugt ist. Sei f_1 ein Polynom kleinsten Grades in $L \setminus 0$. Induktiv wähle als f_{m+1} ein Polynom kleinsten Grades in $L \setminus \sum_{i=0}^m R[X]f_i$. Sei n_m der Grad von f_m, sei r_m der höchste Koeffizient von f_m. Es ist $n_1 \le n_2 \le \ldots$. Betrachte die Kette von Linksidealen $Ra_1 \subseteq Ra_1+Ra_2 \subseteq \ldots$. Behauptung: dies ist eine echt aufsteigende Kette. Wäre nämlich $a_{m+1} \in \sum_{i=1}^m Ra_i$, also $a_{m+1} = \sum_{i=1}^m r_i a_i$, mit $r_i \in R$, so ist

$$g = f_{m+1} - \sum_{i=1}^m r_i X^{n_{m+1}-n_i} f_i \quad \in \quad L \setminus \sum_{i=0}^m R[X]f_i$$

ein Polynom kleineren Grads als f_{m+1}, im Widerspruch zur Auswahl von f_{m+1}.

Lemma. *Sei R ein kommutativer noetherscher Ring. Jedes reduzierte Ideal von R ist Durchschnitt endlich vieler Primideale.*

Beweis: Sei $\mathcal{I}$ die Menge der reduzierten Ideale, die sich nicht als Durchschnitt endlich vieler Primideale schreiben lassen. Angenommen, die Menge $\mathcal{I}$ ist nicht leer. Da R noethersch ist, können wir ein maximales Element I in $\mathcal{I}$ wählen. Weil I zu $\mathcal{I}$ gehört, ist I kein Primideal.

Ein reduziertes Ideal, das kein Primideal ist, ist Durchschnitt $I_1 \cap I_2$ mit reduzierten Idealen $I_1 \supset I$, $I_2 \supset I$ (siehe Lemma 3 im Abschnitt 4).

Die Maximimalität von I zeigt, daß sich die Ideale I_1, I_2 beide als Durchschnitt endlich vieler Primideale schreiben lassen, also gilt dies auch für I.

Beweis des Satzes: Ist I Durchschnitt von endlich vielen Primidealen $P_1, \ldots, P_n$, so können wir annehmen, daß diese Ideale paarweise unvergleichbar sind, daß also $P_i \subseteq P_j$ nur für $i = j$ gilt (ist nämlich $i \neq j$ und $P_i \subseteq P_j$, so verzichten wir auf P_j).

7. Die Relation "ist Nullstelle von".

Sei k ein Körper, und n eine natürliche Zahl. Einerseits betrachten wir den n-dimensionalen affinen Raum k^n, andererseits den Polynomring $k[X_1, \dots, X_n]$ in n Variablen mit Koeffizienten in k.

Wir haben oben folgende Zuordnungen eingeführt: Ist P eine Teilmenge von $k[X_1, \dots, X_n]$, so setzen wir

$$V(P) = \{a \in k^n \mid f(a) = 0 \quad \text{für alle} \quad f \in P\},$$

und nennen dies die *gemeinsame Nullstellenmenge* der Polynome in P; Mengen der Form $V(P)$ haben wir *algebraische Mengen* genannt.

Ist S eine Teilmenge von k^n, so ist

$$I(S) = \{f \in k[X_1, \dots, X_n] \mid f(a) = 0 \quad \text{für alle} \quad a \in S\},$$

und dies ist ein Ideal von $k[X_1, \dots, X_n]$.

(i) *Es ist $P \subseteq I(V(P))$ für jedes $P \subseteq k[X_1, \dots, X_n]$.*
(i*) *Es ist $S \subseteq V(I(S))$ für jedes $S \subseteq k^n$.*
(ii) *Aus $P \subseteq P' \subseteq k[X_1, \dots, X_n]$ folgt $V(P) \supseteq V(P')$.*
(ii*) *Aus $S \subseteq S' \subseteq k^n$ folgt $I(S) \supseteq I(S')$.*
(iii) *Es ist $V(P) = V(I(V(P)))$ für jedes $P \subseteq k[X_1, \dots, X_n]$.*
(iii*) *Es ist $I(S) = I(V(I(S)))$ für jedes $S \subseteq k^n$.*

Die Aussagen (i), (i*), (ii), (ii*) sollten offensichtlich sein. Daraus folgen aber die beiden weiteren Aussagen unmittelbar: so liefert (i) die Inklusion $P \subseteq I(V(P))$, daraus folgt nach (ii) aber $V(P) \supseteq V(I(V(P))$, während (ii*), angewandt auf $S = V(P)$ die umgekehrte Inklusion liefert; dies der Beweis von (iii), entsprechend beweist man (iii*).

(iv) *Sei k algebraisch abgeschlossener Körper. Die Zuordnungen*

$$V(-) : \{P \mid P \subseteq k[X_1, \dots, X_n]\} \longrightarrow \{S \mid S \subseteq k^n\}$$
$$I(-) : \{S \mid S \subseteq k^n\} \longrightarrow \{P \mid P \subseteq k[X_1, \dots, X_n]\}$$

liefern zueinander inverse Bijektionen zwischen der Menge der reduzierten Ideale in $k[X_1, \dots, X_n]$ und der Menge der algebraischen Teilmengen des k^n.

Sind Zuordnungen wie $V(-)$ und $I(-)$ gegeben, die die Bedingungen der Form (i), (i*), (ii), (ii*) erfüllen, so spricht man von einer *Galois-Korrespondenz.* In einem derartigen Fall richtet sich das Interesse auf die Teilmengen der Form $V(P)$ und $I(S)$, da immer eine Bijektivitätsaussage wie in (iv) gilt. In unserem Fall haben wir die Mengen der Form $V(P)$ als die "algebraischen" Teilmengen **definiert,** dagegen erforderte es recht viel Aufwand, die Mengen der Form $I(S)$ als die "reduzierten Ideale" zu **charakterisieren.**

Algebraische Teilmengen sind immer durch endlich viele Polynome definierbar. Dies folgt unmittelbar aus der Tatsache, daß der Polynomring $k[X_1,\dots,X_n]$ noethersch ist: denn ist $V = V(P)$, so ist das von P erzeugte Ideal $\langle P\rangle$ endlich erzeugt; genauer gilt: es gibt eine endliche Teilmenge von P, die das Ideal $\langle P\rangle$ erzeugt, also gilt: *Zu jeder Teilmenge P von $k[X_1,\dots,X_n]$ gibt es eine endliche Teilmenge $P' \subseteq P$ mit $V(P') = V(P)$.*

Die aufsteigende Kettenbedingung für Ideale impliziert die absteigende Kettenbedingung für algebraische Mengen: *Jede absteigende Kette algebraischer Mengen bricht ab.* Ist eine Kette algebraischer Mengen

$$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_i \supseteq V_{i+1} \supseteq \dots$$

gegeben, so gibt es ein s mit $V_i = V_j$ für alle $i, j \geq s$. Entsprechend gilt: *Jede nicht leere Menge algebraischer Mengen besitzt ein minimales Element.*

Beliebige Durchschnitte algebraischer Mengen sind wieder algebraische Mengen: Seien algebraische Mengen $V(P_i)$ mit $i \in I$ (eine Indexmenge) gegeben, dabei sei P_i eine Teilmenge von $k[X_1,\dots,X_n]$. Dann gilt

$$\bigcap_{i\in I} V(P_i) = V(\bigcup_{i\in I} P_i).$$

Allerdings gilt auch: Jeder derartige Durchschnitt ist schon Durchschnitt über endlich viele dieser Mengen (wegen der absteigenden Kettenbedingung)!

Endliche Vereinigungen algebraischer Mengen im k^n sind wieder algebraische Mengen: Sind $P_1, P_2 \subseteq k[X_1,\dots,X_n]$ gegeben, so gilt

$$V_1 \cup V_2 = V(\{p_1p_2 \mid p_1 \in P_1, p_2 \in P_2\}).$$

Warnung: Beliebige Vereinigungen algebraischer Mengen brauchen natürlich keinesfalls algebraische Mengen zu sein. Denn jede einelementige Teilmenge des k^n (jeder Punkt) ist algebraische Menge. Ist aber $n \geq 1$ und k unendlich, so gibt es Teilmengen des k^n, die nicht algebraisch sind. (Für $n = 1$ gilt: Eine echte Teilmenge $S \subset k^1$ ist algebraisch genau dann, wenn S endlich ist.)

Eine algebraische Teilmenge $V \subseteq k^n$ heißt *irreduzibel*, wenn es keine algebraischen Teilmengen $V_1 \subset V$ und $V_2 \subset V$ mit $V = V_1 \cup V_2$ gibt. Irreduzible algebraische Mengen nennt man oft "affine Varietäten".

Sei $V \subseteq k^n$ eine algebraische Menge. Genau dann ist V irreduzibel, wenn $I(V)$ ein Primideal ist.

Beweis: Zuerst nehmen wir an, daß $I(V)$ kein Primideal ist. Seien $f_1, f_2 \in mit f_1f_2 \in I(V)$. Ist f_i nicht in $I(V)$, so ist $V_i = V(I(V) + Af_i)$ eine echte Teilmenge von V, und natürlich eine algebraische Menge. Wegen $f_1f_2 \in U(V)$ ist $V_1 \cup V_2 = V$ (denn ist $v \in V$, so ist $f_1(v)f_2(v) = (f_1f_2)(v) = 0$, also $f_1(v) = 0$ oder $f_2(v) = 0$). Dies zeigt, daß V nicht irreduzibel sein kann.

Sei nun V nicht irreduzibel, also $V = V_1 \cup V_2$ mit algebraischen Teilmengen V_i, die echt in V enthalten sind. Sei etwa $w_i \in V \setminus V_i$. Da V_i algebraische Teilmenge ist, gibt es ein $f_i \in I(V_i)$ mit $f_i(w_i) \neq 0$. Insbesondere gehört weder f_1 noch f_2 zu $I(V)$. Wegen $V = V_1 \cup V_2$ ist $(f_1f_2)(v) = 0$ für alle $v \in V$, also f_1f_2 gehört zu $I(V)$. Wir sehen, daß $I(V)$ kein Primideal sein kann.

Folgerung. *Sei k algebraisch abgeschlossener Körper. Die Zuordnungen $V(-)$ und $I(-)$ liefern zueinander inverse Bijektionen zwischen der Menge der Primideale in $k[X_1, \ldots, X_n]$ und der Menge der irreduziblen algebraischen Teilmengen des k^n.*

Sei V eine algebraische Teilmenge von k^n. Eine irreduzible algebraische Menge $V' \subseteq V$ heißt *irreduzible Komponente von V*, wenn es keine irreduzible algebraische Menge V'' mit $V' \subset V'' \subseteq V$ gibt.

Jede nicht leere algebraische Teilmenge $V \subseteq k^n$ besitzt endlich viele irreduzible Komponenten $V_1, \ldots, V_t$. Jedes Element von V liegt in mindestens einer dieser Mengen V_i, und zu jedem Index i gibt es Elemente von V, die zu V_i, aber zu keiner anderen Menge V_j gehören. Es ist also einerseits

$$V = \bigcup_{i=1}^{t} V_i,$$

und andererseits

$$V_1 \cup \cdots \cup V_{i-1} \cup V_{i+1} \cup \ldots V_t \ \subset \ V,$$

für jedes $1 \leq i \leq t$. Dies folgt unmittelbar aus der Tatsache, daß sich jedes reduzierte Ideal in $k[X_1, \ldots, X_n]$ als Durchschnitt endlich vieler paarweise unvergleichbarer Primideale $P_1, \ldots, P_t$ schreiben läßt.

Wir haben gesehen, daß jede Primidealkette im Polynomring $k[X_1, \ldots, X_n]$ Länge höchstens n hat. Dies liefert: *Jede Kette von irreduziblen algebraischen Mengen in k^n hat Länge höchstens n.*

Man definiert als *Dimension* einer algebraischen Menge V die Länge t der längsten Kette

$$V_0 \subset V_1 \subset \cdots \subset V_t \subseteq V$$

mit irreduziblen algebraischen Mengen $V_0, \ldots, V_t$. Es gilt: *Die Dimension einer algebraischen Menge V ist das Maximum der Dimension der irreduziblen Komponenten von V. Die Dimension einer irreduziblen algebraischen Teilmenge $V \subseteq k^n$ ist gerade der Transzendenzgrad des Quotientenkörpers von $k[X_1, \ldots, X_n]/I(V)$.*

Sei nun n fixiert. Sei $A = k[X_1, \ldots, X_n]$.

Dimension 0. Die irreduziblen algebraischen Mengen der Dimension 0 sind gerade die Punkte. Sie entsprechen bijektiv den Auswertungsidealen I_a, also den maximalen Idealen I von A mit $A/I = k$. Ist k algebraisch abgeschlossen, so entsprechen die Punkte des k^n bijektiv den maximalen Idealen.

Dimension 1. Die irreduziblen algebraischen Mengen der Dimension 1 nennt man *irreduzible Kurven.*

Dimension 2. Die irreduziblen algebraischen Mengen der Dimension 2 nennt man *irreduzible Flächen.*

Sei nun k algebraisch abgeschlossen.

Dimension n. Die einzige algebraische Teilmenge des k^n der Dimension n ist k^n selbst. Es ist $I(k^n)$ das Nullideal, dies ist ein Primideal, also ist k^n irreduzibel.

Dimension $n-1$. Die irreduziblen algebraischen Mengen der Dimension 1 nennt man irreduzible Hyperflächen, sie sind von der Form $V(f)$, dabei ist f ein irreduzibles Polynom in A. Natürlich ist umgekehrt $I(V(f)) = \langle f \rangle$.

Erinnerung. Eine Menge S zusammen mit einer Menge $\mathcal{U}$ von Teilmengen $U{\subseteq}S$ nennt man einen topologischen Raum, falls die folgenden Bedingungen erfüllt sind:

(i) Die Menge S selbst und die leere Menge gehören zu $\mathcal{U}$.

(ii) Die Menge U ist abgeschlossen unter endlichen Durchschnitten und beliebigen Vereinigungen.

Ist $(S,\mathcal{U})$ ein topologischer Raum, so nennt man die Mengen in U *offene Mengen*; eine Teilmenge $A{\subseteq}S$ heißt *abgeschlossen,* falls $S\backslash A$ offen ist. Ein topologischer Raum $(S,\mathcal{U})$ ist ein *Hausdorff-Raum,* falls es zu je zwei Elementen $s_1{\neq}s_2$ in S offene Mengen U_1,U_2 mit $u_1{\in}U_1$, $u_2{\in}U_2$ und $U_1{\cap}U_2{=}\emptyset$ gibt.

Ist V eine algebraische Menge, so bildet V zusammen mit den Komplementen der algebraischen Mengen einen topologischen Raum. Man nennt diese Topologie die *Zariski-Topologie.* Dieser topologische Raum ist nur dann ein Hausdorff-Raum, wenn V null-dimensional (also eine endliche Menge) ist.

8. Nicht verfeinerbare Primidealketten

Satz. *Sei k ein Körper. Sei A eine endlich erzeugte k-Algebra; sei A Integritätsbereich der Krull-Dimension t. Dann gilt: Jede Primidealkette in A, die nicht verfeinert werden kann, hat Länge t.*

Beweis: Wir werden zeigen: Ist $P \neq 0$ ein Primideal von A, und gibt es kein Primideal P' mit $0 \subset P' \subset P$, so ist die Krull-Dimension von A/P gerade $t-1$. Daraus folgt dann die Behauptung mit Induktion.

Wie früher verwenden wir wieder eine Noether'sche Normalisierung B, also eine Unteralgebra $B = k[b_1, \ldots, b_t]$ mit algebraisch unabhängigen Elementen $b_1, \ldots, b_t$, so daß A endlich über B ist. Sei also $P \neq 0$ ein Primideal von A, und es gebe kein Primideal P' mit $0 \subset P' \subset P$. Es ist $P \cap B$ ein Primideal von B, und wegen Lemma 2 im Abschnitt 5 ist $P \cap B \neq 0$. Lemma 3 im gleichen Abschnitt liefert ein irreduzibles Element $f \in P \cap B$, also eine Primidealinklusion $Bf \subseteq P \cap B$ in B. Wir können annehmen, daß f nicht zu $k[b_1, \ldots, b_{t-1}]$ gehört (ansonsten ändere die Numerierung der Elemente b_i). Wir werden ein Going-down-Lemma beweisen, aus dem unmittelbar folgt, daß $Bf = P \cap B$ gelten muß. Wenn aber $Bf = P \cap B$ gilt, so ist $P \cap k[b_1, \ldots, b_{t-1}] = 0$, also sind die Restklassen der Elemente $b_1, \ldots, b_{t-1}$ in A/P über k algebraisch unabhängig. Dies zeigt, daß der Transzendenzgrad, und damit die Krull-Dimension von A/P mindestens $t-1$ ist. Andererseits ist die Krull-Dimension von A/P echt kleiner als die von A.

Lemma ("Going down"). *Sei S Integritätsbereich, sei $R \subseteq S$ ein Unterring. Wir setzen voraus, daß R faktoriell ist und daß S endlich über R ist. Seien $P_0 \subset P_1$ Primideale von R. Ist Q_1 ein Primideal in S mit $Q_1 \cap R = P_1$, so gibt es ein Primideal Q_0 in S mit $Q_0 \subset Q_1$ und $Q_0 \cap R = P_0$.*

Beweis: Wir setzen zuerst nur voraus, daß $R \subseteq S$ eine endliche Erweiterung kommutativer Ringe ist.

(1) *Sei I ein Ideal in R. Ist $y \in IS$, so gibt es ein Polynom $f(X) = X^n + \sum_{i=0}^{n-1} r_i X^i$ mit Koeffizienten $r_i \in I$ für $0 \leq i < n$ und $f(y) = 0$.*

Beweis wie der von Lemma 1 im Abschnitt 1: Sei $S = \sum_i Rs_i$ mit Elementen $s_i \in S$ und $s_1 = 1$. Da ys_i zu $IS = \sum_i Is_i$ gehört, hat das dort konstruierte normierte Polynom die gewünschten Eigenschaften.

Sei nun zusätzlich S ein Integritätsbereich, sei R faktoriell mit Quotientenkörper K, und sei P ein Primideal in R.

(2) *Ist* $y \in PS$ *und ist* $g(X) = X^n + \sum_{i=0}^{n-1} c_i X^i$ *das Minimalpolynom von* y *über* K*, so gehören alle Koeffizienten* c_i *von* $g(X)$ *mit* $0 \leq i \leq n-1$ *zu* P.

Beweis: Sei $f(X)$ zu $P = I$ wie in (1) konstruiert. Da $g(X)$ das Minimalpolynom von y über K ist, gibt es ein Polynom $h(X) = X^m + \sum_{j=0}^{m-1} c'_j X^j$ mit Koeffizienten c'_j in K, so daß gilt $f(X) = g(X)h(X)$. Das Gauß-Lemma besagt, daß alle Koeffizienten c_i, c'_j von $g(X)$ und $h(X)$ zu R gehören. Die entsprechende Argumentation wie beim Beweis vom Gauß-Lemma zeigt, daß die Koeffizienten r'_i mit $0 \leq i \leq n-1$ sogar zu zu P gehören: Um dies zu zeigen, nehmen wir an, daß es $0 \leq a < n$ gibt mit $c_a \notin P$ und wir wählen das minimale derartige a. Wir setzen $c'_m = 1$, und wählen $0 \leq b \leq m$ minimal, so daß gilt $c'_b \notin P$ (wegen $c'_m = 1 \notin P$ gibt es derartige Koeffizienten). Der Koeffizient von $f(X)$ mit Index $a+b$ ist

$$\left(c_0 c'_{a+b} + \cdots + c_{a-1} c'_{b+1}\right) + c_a c'_b + \left(c_{a+1} c'_{b-1} + \cdots + c_{a+b} c'_0\right).$$

Wegen $a + b < n + m$ gehört dieser Koeffizient zu P. Die beiden Klammern sind jeweils Elemente von P, wegen der Minimalität von a, beziwhungsweise b. Also ist auch $c_a c'_b \in P$. Da P Primideal ist, muß dann aber auch einer der beiden Faktoren zu P gehören, ein Widerspruch. Also sehen wir, daß $g(X)$ die gewünschte Eigenschaft hat.

(3) *Sei* P_0 *ein Primideal von* R*, sei* Q_1 *ein Primideal von* S*, sei* $P_0 \subseteq Q_1$*. Dann gilt*

$$P_0 S (S \setminus Q_1)^{-1} \cap R = P_0.$$

(Wir betrachten hier Teilmengen des Quotientenkörpers L von S.)

Beweis: Sei $y \in P_0 S$, sei $s \in S \setminus Q_1$, sei $z = ys^{-1} \in R$. Angenommen z gehört nicht zu P_0. Sei $g(X) = X^n + \sum_{i=0}^{n-1} c_i X^i$ das normierte Minimalpolynom von y über K. Wegen (2) wissen wir, daß die Koeffizienten c_i zu P_0 gehören. Es ist $s = yz^{-1}$, und $0 \neq z^{-1} \in K$, also hat das Minimalpolynom von s ebenfalls Grad n. Multiplizieren wir

$$0 = g(y) = y^n + \sum_{i=0}^{n-1} c_i y^i$$

mit z^{-n}, so erhalten wir

$$0 = (yz^{-1})^n + \sum_{i=0}^{n-1} c_i z^{-n+i} (yz^{-1})^i,$$

demnach ist $X^n + \sum_{i=0}^{n-1} d_i X^i$ mit $d_i = c_i z^{-n+i}$ das Minimalpolynom von s über K. Da s ganz über R und R faktoriell ist, gehören alle diese Koeffizienten d_i zu R. Es ist $c_i = d_i z^{n-i}$. Da wir annehmen, daß z nicht zu P_0 gehört, und da $c_i \in P_0$, sehen wir: es ist $d_i \in P_0$ für $1 \leq i < n$. Also ist $s^n \in P_0 \subseteq Q_1$, also $s \in Q_1$, ein Widerspruch.

(4) Nun also der Beweis des Satzes: Beachte: $S' = S(S \setminus Q_1)^{-1}$ ist ein Unterring des Quotientenkörpers L von S, und es ist $R \subseteq S \subseteq S' \subseteq L$. Die Menge $P_0 S (S \setminus Q_1)^{-1}$ ist ein Ideal in diesem Ring S'. Wir sehen also, daß es in S' Ideale I gibt mit $I \cap R = P_0$. Sei I ein Ideal von S', das maximal ist mit $I \cap R = P_0$. Ein derartiges Ideal ist maximal mit der Eigenschaft $I \cap (R \setminus P_0) = \emptyset$, also ist es (nach dem Primideallemma) ein Primideal. Wir haben $R \subseteq S \subseteq S'$. Setzen wir $Q_0 = I \cap S$, so ist auch Q_0 ein Primideal (Lemma 0 im Abschnitt 5), und es gilt $Q_0 \cap R = P_0$. Es bleibt zu zeigen, daß $Q_0 \subseteq Q_1$ gilt. Angenommen, es gibt $s \in Q_0 \setminus Q_1$. In S' ist s invertierbar, also ist $1 = ss^{-1}$ ein Element im Ideal I des Rings S'. Als Primideal ist aber I ein echtes Ideal.

9. Die Algebra der polynomialen Funktionen $\mathcal{A}(V)$.

Jeder algebraischen Menge $V \subseteq k^n$ kann man als wichtigste Invariante die *Algebra der polynomialen Funktionen*

$$\mathcal{A}(V) = k[X_1, \ldots, X_n]/I(V)$$

zuordnen; man nennt $\mathcal{A}(V)$ manchmal auch die 'Koordinatenalgebra' von V (und man schreibt oft $k[V]$ statt $\mathcal{A}(V)$). Wir bezeichnen mit $\mathrm{Abb}(V,k)$ die k-Algebra der (mengentheoretischen) Abbildungen $V \to k$ mit punktweisen Operationen (Addition, Multiplikation, Skalar-Multiplikation).

Sind also f_1, f_2: $V \to k$ Abbildungen, und ist $c \in k$, so sind die Abbildungen $f_1 + f_2$, $f_2 \cdot f_2$, cf_1 durch $(f_1+f_2)(v) = f_1(v) + f_2(v)$, $(f_1 \cdot f_2)(v) = f_1(v) \cdot f_2(v)$, und $(cf_1)(v) = c(f_1(v))$ definiert.

Ordnen wir einem Polynom $f \in k[X_1, \ldots, X_n]$ die Abbildung $\eta_V(f)$: $V \to k$, mit $\eta_V(f)(a) = f(a)$ für $a \in k^n$ zu, so erhalten wir einen Algebren-Homomorphismus

$$\eta_V\colon\ k[X_1, \ldots, X_n] \longrightarrow \mathrm{Abb}(V, k).$$

Die Elemente im Bild von η_V sind gerade die 'polynomialen Abbildungen' oder 'polynomialen Funktionen' $V \to k$ (also diejenigen Abbildungen, die durch die Auswertung eines Polynoms beschrieben werden können), wir verwenden daher folgende Bezeichnung $\mathrm{Pol}(V,k) = \mathrm{Im}\, \eta_V$. Eigentlich ist es die k-Algebra $\mathrm{Pol}(V,k)$, die man die 'Algebra der polynomialen Funktionen' nennen sollte. Nun ist η_V ein k-Algebren-Homomorphismus mit Kern $I(V)$, also induziert η_V nach dem 'Ersten Isomorphiesatz' einen k-Algebren-Isomorphismus

$$\mathcal{A}(V) \longrightarrow \mathrm{Pol}(V, k).$$

Auf diese Weise können wir $\mathrm{Pol}(V,k)$ mit $\mathcal{A}(V)$ identifizieren.

Die k-Algebra $k[X_1, \ldots, X_n]$ wird durch die Polynome $X_1, \ldots, X_n$ erzeugt, also wird $\mathrm{Pol}(V,k)$ durch die Elemente $\eta_V(X_1), \ldots, \eta_V(X_n)$ erzeugt. Es ist $\eta_V(X_i)$ die Projektion von V auf die i-te Koordinatenachse: für $a = (a_1, \ldots, a_n) \in V$ ist $\eta_V(X_i)(a) = a_i$, jedem n-Tupel a in V wird also seine i-te Koordinate zugeordnet. Die Algebra $\mathrm{Pol}(V,k)$ ist die kleinste Unteralgebra von $\mathrm{Abb}(V,k)$, die diese 'Koordinatenfunktionen' enthält, daher der Name 'Koordinatenalgebra'.

Das Bild $\mathrm{Pol}(V,k)$ ist eine reduzierte, endlich erzeugte, kommutative k-Algebra (als Faktoralgebra der endlich erzeugten, kommutativen Algebra $k[X_1, \ldots, X_n]$ ist $\mathrm{Pol}(V,k)$ endlich erzeugt und kommutativ, andererseits gibt es im Ring $\mathrm{Abb}(V,k)$ keine von Null verschiedenen nilpotenten Elemente). Umgekehrt gilt:

Hilbert'scher Nullstellensatz (Vierte Fassung). *Ist k ein algebraisch abgeschlossener Körper k, so ist jede reduzierte, endlich erzeugte, kommutative k-Algebra isomorph zur Algebra der polynomialen Funktionen einer algebraischen k-Menge.*

Beweis: Sei k algebraisch abgeschlossener Grundkörper und sei A eine reduzierte, kommutative k-Algebra, die als k-Algebra von den Elementen $a_1, \ldots, a_n$ erzeugt wird. Die Auswertungsabbildung

$$\phi = \phi_{a_1,\ldots,a_n}\colon\ k[X_1, \ldots, X_n] \longrightarrow A \quad \text{mit} \quad \phi(X_i) = a_i$$

hat als Kern ein reduziertes Ideal, sagen wir I und natürlich induziert ϕ einen Isomorphismus

$$k[X_1, \ldots, X_n]/I \longrightarrow A.$$

Andererseits ist $I = I(V(I))$, da I reduziert und k algebraisch abgeschlossen ist. Also ist $k[X_1,\ldots,X_n]/I = \mathcal{A}(V)$ mit $V = V(I)$.

Schauen wir uns dies noch genauer an: wir arbeiten mit den beiden surjektiven Algebren-Homomorphismen

$$\begin{tikzcd} & k[X_1,\ldots,X_n] \arrow[dl, "\eta_V"'] \arrow[dr, "\phi"] & \\ \mathrm{Pol}(V,k) & & A \end{tikzcd}$$

die beide den Kern I haben. Also gibt es einen k-Algebren-Isomorphismus ω: $\mathcal{A}(V) \to A$ gibt, der die Restklasse von X_i (modulo I), also die i-te Koordinatenfunktion auf der algebraischen Menge V, auf das Element $a_i \in A$ schickt. Wir erhalten das folgende kommutative Diagramm

$$\begin{tikzcd} & k[X_1,\ldots,X_n] \arrow[dl, "\eta_V"'] \arrow[dr, "\phi"] & \\ \mathrm{Pol}(V,k) \arrow[rr, "\omega"] & & A \end{tikzcd}$$

(Die 'Kommutativität' des Diagramms bedeutet, daß $\phi = \omega\circ\eta_V$ gilt.)

Wir sehen: *Ist A eine reduzierte, kommutative k-Algebra und ist $a_1,\ldots,a_n$ ein Erzeugendensystem von A als k-Algebra, so können wir A als die Algebra der polynomialen Funktionen auf einer algebraischen Menge $V \subseteq k^n$ auffassen; dabei sind die Elemente a_i dann gerade die Koordinatenfunktionen.* Die algebraische Menge V ist durch A und $a_1,\ldots,a_n$ eindeutig bestimmt.

Viele Eigenschaften von V lassen sich durch Eigenschaften der k-Algebra $\mathcal{A}(V)$, also "algebraisch", ausdrücken. Beispiele: Wie wir wissen, ist $\mathcal{A}(V)$ genau dann nullteilerfrei, wenn V irreduzibel ist. Die Anzahl der minimalen Primideale von $\mathcal{A}(V)$ ist gerade die Anzahl der irrduziblen Komponenten von V. Die Dimension von V wurde durch die Krull-Dimension von $\mathcal{A}(V)$ definiert. Man nennt V 'rational', wenn $\mathcal{A}(V)$ ein Polynomring ist (d.h. wenn es algebraisch unabhängige Elemente $a_1,\ldots,a_t$ mit $\mathcal{A}(V)=k[a_1,\ldots,a_t]$) gibt. Man nennt eine irreduzible algebraische Menge V 'birational', wenn der Quotientenkörper $\mathrm{Quot}\,\mathcal{A}(V)$ von $\mathcal{A}(V)$ von einer Transzendenzbasis über k erzeugt wird; man nennt V 'normal', wenn $\mathcal{A}(V)$ in seinem Quotientenkörper ganz abgeschlossen ist . . .

Genau dann ist V die disjunkte Vereinigung zweier nicht-leerer algebraischer Mengen, wenn es in $\mathcal{A}(V)$ ein Idempotent e mit $e \neq 0, e \neq 1$ gibt, wenn sich also $\mathcal{A}(V)$ als Produkt zweier von Null verschiedener Algebren schreiben läßt. (Ist e ein Idempotent, so betrachte die Nullstellenmengen von e und von $1-e$. Umgekehrt sei V die disjunkte Vereinigung von V_1 und V_2. Es ist $I(V) = I(V_1)\cap I(V_2)$. Wäre $I(V_1)+I(V_2)$ ein echtes Ideal, so gäbe es ein maximales Ideal I_a, das $I(V_1)+I(V_2)$ enthält: es wäre dann aber $a \in V_1 \cap V_2$.)

Sei $W\subseteq k^n$ eine algebraische Menge. Gehört $f\in k[X_1,\ldots,X_n]$ nicht zu $I(W)$, so ist $W\cap V(f)$ eine echte Teilmenge von W. Es sollte klar sein, daß es für viele Überlegungen der algebraischen Geometrie wichtig sein wird, aus Eigenschaften von W Eigenschaften von $W\cap V(f)$ abzuleiten: immerhin läßt sich ja **jede** algebraische Teilmenge induktiv auf diese Weise aus k^n gewinnen: es ist $W=V(g_1,\ldots,g_m)$ für geeignete Polynome $g_1,\ldots,g_m$, also $W=V(g_1)\cap V(g_2)\cap\cdots\cap V(g_m)$.

Die *Höhe* $h(P)$ eines Primideals P ist das Supremum der Längen aller Primidealketten

$$P_0 \subset P_1 \subset \cdots \subset P_d = P.$$

Ist R ein kommutativer Ring, in dem alle Primidealketten zu Primidealketten der Länge n verfeinerbar sind, so ist $\dim R = n$ und es gilt für jedes Primideal P

$$h(P) + \dim R/P = \dim R.$$

Satz (Krull'scher Hauptidealsatz). *Sei R noetherscher kommutativer Ring. Sei $f \in R$. Sei P minimales Primideal über dem Hauptideal $\langle f\rangle$. Dann ist $h(P) \le 1$.*

Zusatz. *Ist f kein Nullteiler, so ist $h(P) = 1$.*

Der Beweis des Hauptidealsatzes wird erst später (im Abschnitt über Moduln) gegeben. Beachte, daß man zusätzlich voraussetzen kann, daß f nicht invertierbar ist: denn ist f invertierbar, so ist $\langle f\rangle = R$, also gibt es keine Primideale über $\langle f\rangle$.

Beweis des Zusatzes: Wir zeigen: *Die Elemente der minimalen Primideale eines noetherschen Rings sind Nullteiler.* Wie wir wissen, gibt es nur endlich viele minimale Primideale, etwa $P_1, \dots, P_n$. Ist $n = 1$, so ist P_1 das Nilradikal des Rings R, also sind alle Elemente in P_1 nilpotent, also Nullteiler. Sei nun $n \ge 2$. Wir zeigen, daß alle Elemente $s \in P_1$ Nullteiler sind. Es ist $\bigcap_{i\ge 2} P_i \not\subseteq P_1$ (siehe Lemma 4.4), also gibt es ein Element $r \in \bigcap_{i\ge 2} P_i$, mit $r \notin P_1$. Es ist $rs \in \bigcap_i P_i$, dies ist das Nilradikal von R, also ist rs nilpotent, etwa $(rs)^t = 0$. Es ist $s^t \ne 0$, da s nicht in allen Primidealen enthalten ist. Wählen wir t' maximal mit $r^{t'} s^t \ne 0$, so sehen wir $r \cdot r^{t'} s^t = 0$.

Korollar. *Sei R noetherscher Integritätsbereich. Sei P ein Primideal, das minimal über einem von Null verschiedenen Hauptideal ist, so ist $h(P) = 1$.* In einem Integritätsbereich bedeutet $h(P) = 1$, daß es keine Primideale P' mit $0 \subset P' \subset P$ gibt.

Anwendung: Sei nun k algebraisch abgeschlossener Körper. Sei $W \subseteq k^n$ eine algebraische Menge. *Sei W irreduzibel mit Dimension d. und sei $f \in k[X_1, \dots, X_n]$ nicht in $I(W)$. Dann gilt: alle irreduziblen Komponenten von $W \cap V(f)$ haben Dimension $d-1$.* Es kann natürlich $W \cap V(f) = \emptyset$ gelten, dann gibt es keine irreduziblen Komponenten. Beweis: Der Ring $\mathcal{A}(W)$ ist ein Integritätsbereich mit Krull-Dimension d. Betrachte die Restklasse $\overline{f} = f + I(W) \ne 0$ von f. Ist V_i eine irreduzible Komponente von $W \cap V(f)$, so ist das Primideal $I(V_i)/I(W)$ minimal über dem Hauptideal $\langle\overline{f}\rangle$, hat also Höhe 1. Demnach hat der Restklassenring $\mathcal{A}(W)$ die Krull-Dimension $d-1$.

Ist $f \in I(W)$, so hat $W \cap V(f) = W$ die Dimension d. Ist W reduzibel, so betrachten wir die einzelnen irreduziblen Komponenten W_i. Wir erhalten: *Haben alle irreduziblen Komponenten von W Dimension mindestens d, und sind $f_1, \dots, f_r \in k[X_1, \dots, X_n]$, so haben alle irreduziblen Komponenten von $W \cap V(f)$ Dimension mindestens $d - r$.*

Im allgemeinen kann man nur feststellen, daß $W\cap V(f)$ entweder leer ist, oder aber die Dimension mindestens $d-r$ hat. Es gibt einen Spezialfall, wo man von Anfang an weiß, daß $W\cap V(f)$ nicht leer sein kann, nämlich wenn man mit **homogenen** Polynomen arbeitet.

Ein Polynom $f = \sum c_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ im Polynomring $k[X_1, \dots, X_n]$ (mit Koeffizienten $c_{i_1,\dots,i_n} \in k$) heißt *homogen vom Grad d*, wenn gilt: Ist $c_{i_1,\dots,i_n} \ne 0$, so ist $i_1 + \dots i_n = d$. *Ist f homogen vom Grad d, so gilt $f(\lambda a) = \lambda^d f(a)$ für alle $a \in k^n$ und $\lambda \in k$.* (Ist k unendlicher Körper, so gilt auch die Umkehrung!) Es folgt: Ist a eine Nullstelle eines homogenen Polynoms f, so ist auch λa Nullstelle von f, für jedes $\lambda \in k$.

Eine nicht-leere Teilmenge $S \subseteq k^n$ heißt *Kegel*, falls gilt: Ist $a \in S$, so ist auch $\lambda a \in S$, für jedes $\lambda \in k$, also es ist $ka \subseteq S$. *Sind $f_1, \dots, f_n$ nicht-konstante homogene Polynome in $k[X_1, \dots, X_n]$, so ist $V(f_1, \dots, f_n)$ ein Kegel* (dabei können die Polynome $f_1, \dots, f_n$ verschiedene Grade haben).

Folgerung. *Sind $g_1, \ldots, g_r$ homogene Polynome in $k[X_1, \ldots, X_n]$, so ist die Dimension von $V(g_1, \ldots, g_r)$ mindestens $n - r$.*

Man vergleiche diese Aussagen mit denjenigen, die das Lösen von **linearen** Gleichungssystemen in n Variablen betreffen.

Die Lösungsmenge eines linearen Gleichungssystems ist (leer oder) ein affiner Teilraum W von k^n. Sei d die Dimension von W. Fügen wir eine Gleichung $f{=}0$ hinzu, so kann es passieren, daß die Menge $W \cap V(f)$ leer ist. Ist $f \in I(W)$, so ist $W \cap V(f) = W$, ansonsten hat $W \cap V(f)$ Dimension $d{-}1$.

Wenn ein polynomiales Gleichungssystem gegeben ist, so gelten, wie wir gesehen haben, entsprechende Dimensionsaussagen. Natürlich ist in diesem Fall die Lösungsmenge üblicherweise kein affiner Teilraum, sondern nur noch eine algebraische Menge. Insbesondere ist die Lösungsmenge im allgemeinen nicht irreduzibel (nicht-leere affine Teilräume sind immer irreduzibel).

10. Kategorielle Formulierung des Nullstellensatzes.

Jeder algebraischen Teilmenge $V \subseteq k^n$ haben wir die k-Algebra $\mathcal{A}(V)$ der polynomialen Funktionen auf V zugeordnet und wir wissen, daß wir auf diese Weise gerade die reduzierten, kommutativen k-Algebren, die von n Elementen erzeugt werden, erhalten. Diese Zuordnung ist 'funktoriell'; um dies zu formulieren, brauchen wir einen geeigneten Morphismen-Begriff für algebraische Mengen.

Die Kategorie der algebraischen k-Mengen. Eine algebraische Menge V ist eine Teilmenge eines affinen Raums k^n, statt V werden wir jetzt besser $(V \subseteq k^n)$ schreiben. Wir betrachten die algebraischen k-Mengen als Objekte einer Kategorie. Sind zwei algebraische Mengen $V = (V \subseteq k^n)$ und $W = (W \subseteq k^m)$ gegeben, so ist ein Morphismus $f\colon V \to W$ eine mengentheoretische Abbildung $f\colon V \to W$, die von einer polynomialen Abbildung $\tilde{f}\colon k^n \to k^m$ induziert wird. Eine *polynomiale Abbildung* $k^n \to k^m$ ist natürlich (wie man das aus der Analysis II kennt) durch ein m-Tupel $\tilde{f} = (\tilde{f}_1, \ldots, \tilde{f}_m)$ von Polynomen $\tilde{f}_i$ in n Variablen gegeben. Also: $f\colon V \to W$ ist ein *Morphismus,* wenn es Polynome $\tilde{f}_1, \ldots, \tilde{f}_m \in k[X_1, \ldots, X_n]$ gibt, so daß gilt

$$f(a_1, \ldots, a_n) = \Big(\tilde{f}_1(a_1, \ldots, a_n), \ldots, \tilde{f}_m(a_1, \ldots, a_n)\Big) \quad \text{für jedes} \quad (a_1, \ldots, a_n) \in V.$$

Die Polynome $\tilde{f}_i$ sind üblicherweise durch f nicht eindeutig bestimmt (genau dann liefern die n-Tupel $(\tilde{f}_1, \ldots, \tilde{f}_m)$ und $(\tilde{g}_1, \ldots, \tilde{g}_m)$ die gleiche polynomiale Funktion auf V, wenn die Differenzen $\tilde{f}_i - \tilde{g}_i$ zu $I(V)$ gehören).

Man sieht leicht, daß die Komposition zweier Morphismen $f\colon V_1 \to V_2$, und $g\colon V_2 \to V_3$ wieder ein Morphismus ist: sei $V_1 \subseteq k^n$, $V_2 \subseteq k^m$, und $V_3 \subseteq k^r$, sei f durch $(\tilde{f}_1, \ldots, \tilde{f}_m)$ und g durch $(\tilde{g}_1, \ldots, \tilde{g}_r)$ induziert, dann ist $g \circ f$ durch

$$(\tilde{f}_1(\tilde{g}_1, \ldots, \tilde{g}_r), \ldots, \tilde{f}_m(\tilde{g}_1, \ldots, \tilde{g}_r))$$

induziert. Dies wird gebraucht, wenn man wissen will, daß es sich wirklich um eine 'Kategorie' handelt.

Die Kategorie der endlich erzeugten, reduzierten, kommutativen k-Algebren hat als Objekte die k-Algebren mit den genannten drei Eigeschaften, die Morphismen sind die k-Algebren-Homomorphismen.

Die Zuordnung $\mathcal{A}(-)$ als kontravarianter Funktor. Zuerst bemerken wir: *Ist V eine algebraische Menge, so ist $\mathcal{A}(V)$ die Menge der Morphismen $V \to k$* (denn ist $V \subseteq k^n$, so sind die Morphismen $V \to k$ gerade die Einschränkungen der polynomialen Abbildungen $k^n \to k$ auf V, oder besser: deren Restklassen modulo $I(V)$; die Menge dieser Restklassen ist aber nach Definition $\mathcal{A}(V)$).

Ist ein Morphismus $f\colon W \to V$ von algebraischen Mengen gegeben, und ist $h \in \mathcal{A}(V)$, so ist die Komposition $h \circ f$ ein Morphismus $W \to k$, also ein Element von $\mathcal{A}(W)$. Definieren wir also

$$f^*(h) = h \circ f \quad \text{für} \quad h \in \mathcal{A}(V),$$

so erhalten wir eine Abbildung

$$f^* = \mathcal{A}(f)\colon \mathcal{A}(V) \longrightarrow \mathcal{A}(W).$$

Als erstes überlegt man sich, daß f^* ein Homomorphismus von k-Algebren ist: daß also für $h, h_1, h_2 \in \mathcal{A}(V)$ und $c \in k$ gilt:

$$\begin{aligned} f^*(ch) &= (ch) \circ f = c(h \circ f) = cf^*(h) \\ f^*(h_1 + h_2) &= (h_1 + h_2) \circ f = (h_1 \circ f) + (h_2 \circ f) = f^*h_1 + f^*h_2 \\ f^*(h_1 h_2) &= (h_1 h_2) \circ f = (h_1 \circ f)(h_2 \circ f) = \big(f^*(h_1)\big)\big(f^*(h_2)\big). \end{aligned}$$

Wir sehen, daß unter $\mathcal{A}(-)$ jeder algebraischen Menge eine (reduzierte, endlich erzeugte, kommutative) k-Algebra, und jedem Morphismus algebraischer Mengen $W \to V$ ein Algebren-Homomorphismus $\mathcal{A}(V) \to \mathcal{A}(W)$ zugeordnet wird.

Wir zeigen, daß $\mathcal{A}(-)$ ein kontravarianter Funktor ist: Natürlich ist $(1_V)^* = 1_{\mathcal{A}(V)}$ für jede algebraische Menge V. Sind Morphismen $f\colon V_1 \to V_2$, und $g\colon V_2 \to V_3$ gegeben, so ist

$$(g \circ f)^* = f^* \circ g^*,$$

denn für $h \in \mathcal{A}(V_3)$ gilt

$$(f^* \circ g^*)(h) = f^*(h \circ g) = h \circ g \circ f = (g \circ f)^*(h).$$

Satz. *Sei k ein algebraisch abgeschlossener Körper. Der kontravariante Funktor $\mathcal{A}(-)$ liefert eine Anti-Äquivalenz von der Kategorie der algebraischen k-Mengen auf die Kategorie der endlich erzeugten, reduzierten, kommutativen k-Algebren.*

Beweis: Wir zeigen, daß der Funktor $\mathcal{A}(-)$ voll, treu und dicht ist. Seien $V \subseteq k^n$ und $W \subseteq k^m$ algebraische Mengen. Zu V betrachten wir die Inklusionsabbildung $\iota = \iota^V\colon V \to k^n$, gegeben sind also die Abbildungen $\iota_i = \iota_i^V\colon V \to k$, für $1 \le i \le n$, mit $\iota(v) = (\iota_1(v), \ldots, \iota_n(v))$. Bezeichnen wir mit $\pi = \pi_V\colon k[X_1, \ldots, X_n] \to \mathcal{A}(V)$ die kanonische Projektion mit Kern $I(V)$, so ist $\iota_i = \pi(X_i)$ (die Elemente ι_i sind also die sogenannten Koordinatenfunktionen).

Der Funktor $\mathcal{A}(-)$ ist treu: Seien $f, g\colon W \to V$ Morphismen algebraischer Mengen. Sei $f^* = g^*$. Für $h \in \mathcal{A}(V)$ gilt also $h \circ f = f^*(h) = g^*(h) = h \circ g$. Insbesondere können wir die Abbildungen $\iota_i^V \in \mathcal{A}(V)$ betrachten und sehen $f_i = \iota_i \circ f = \iota_i \circ g = g_i$, also ist $f = g$.

Der Funktor $\mathcal{A}(-)$ ist voll: Sei $\gamma\colon \mathcal{A}(V) \to \mathcal{A}(W)$ ein Algebren-Homomorphismus. Wir müssen zeigen, daß ein Morphismus $g\colon W \to V$ existiert mit $g^* = \gamma$. Es ist sehr einfach, g zu finden: sei $g_i = \gamma(\iota_i^V)$, dies ist ein Element von $\mathcal{A}(W)$, also eine Abbildung $W \to k$. Sei $g = (g_1, \dots, g_n)$: $W \to k^n$. Zu zeigen ist, daß $g(W) \subseteq V$ gilt, denn dann können wir g als Morphismus g: $W \to V$ auffassen, und unsere Konstruktion von g^* zeigt, daß $g^* = \gamma$ gilt. Um $g(W) \subseteq V$ zu verifizieren, zeigen wir: Ist $f \in I(V)$, so ist $f \circ g = 0$. Sei also $f \in I(V)$. Die Projektionsabbildung π: $k[X_1, \dots, X_n] \to \mathcal{A}(V)$ ist ein Algebren-Homomorphismus, also ist $f(\iota_1^V, \dots, \iota_n^V) = f(\pi(X_1), \dots, \pi(X_n)) = \pi(f(X_1, \dots, X_n)) = 0$. Da γ ein Algebren-Homomorphismus ist, gilt

$$f \circ g = f(g_1, \dots, g_n) = f(\gamma(\iota_1^V), \dots, \gamma(\iota_n^V)) = \gamma(f(\iota_1^V, \dots, \iota_n^V)) = 0.$$

Dies zeigt, daß $\mathcal{A}(-)$ voll ist.

Die Tatsache, daß der Funktor $\mathcal{A}(-)$ dicht ist, wurde zu Beginn des letzten Abschnitts herausgearbeitet. Dies ist gerade die Aussage (der vierten Fassung) des Hilbert'schen Nullstellensatzes. Ein Funktor, der voll, treu und dicht ist, liefert immer eine Äquivalenz von Kategorien. Damit ist also der Beweis des Satzes abgeschlossen.

Die Menge $\mathrm{Max}_k(A)$ der Ideale von A der Codimension 1. Wir haben einen kontravarianten Funktor $\mathcal{A}(-)$ konstruiert, der voll, treu und dicht ist, also eine Anti-Äquivalenz von Kategorien liefert. Es ist oft sehr hilfreich, einen 'Umkehrfunktor' zu kennen: wie ordnet man einer reduzierten, endlich erzeugten, kommutativen Algebra A eine algebraische Menge zu? Wir haben dafür ein endliches Erzeugendensystem von A verwendet, also eine Auswahl treffen müssen. Man kann jedoch jeder k-Algebra A eindeutig eine Menge zuordnen, die im Fall einer Algebra der Form $\mathcal{A}(V)$ bijektiv der Menge V entspricht, nämlich die Menge $\mathrm{Max}_k(A)$ der Ideale I von A der Codimension 1 (dies sind natürlich maximale Ideale). Beachte: *Sind A, B k-Algebren, und ist γ: $A \to B$ ein Algebren-Homomorphismus, so ist für jedes Ideal I von B mit Codimension* 1 *das Urbild $\gamma^{-1}(I)$ ein Ideal von A mit Codimension* 1, also liefert γ^{-1} eine Abbildung $\mathrm{Max}_k(B) \to \mathrm{Max}_k(A)$.

Ist $A = \mathcal{A}(V)$, wobei $V \subseteq k^n$ eine algebraische Menge ist, so sind die Elemente von $\mathrm{Max}_k(A)$ gerade die Auswertungsideale an Punkten $a \in V$. *Ist k algebraisch abgeschlossener Körper und V eine algebraische Menge, so liefert die Zuordnung $a \mapsto I_a$ für $a \in V$ eine Bijektion zwischen den Punkten von V und den Elementen von* $\mathrm{Max}_k(\mathcal{A}(V))$. Beweis: Es wurde schon notiert, daß die Ideale in $\mathrm{Max}_k(V)$ maximale Ideale sind. Umgekehrt gilt: Ist k algebraisch abgeschlossen, und ist A eine endlich erzeugte k-Algebra, so hat jedes maximale Ideal Codimension 1; dies ist die zweite Fassung des Nullstellensatzes. Also gilt in diesem Fall: $\mathrm{Max}_k(A)$ ist die Menge **aller** maximalen Ideale.

Ist f: $W \to V$ ein Morphismus von algebraischen Mengen, so gilt für $w \in W$

$$(f^*)^{-1}(I_w) = I_{f(w)}.$$

Beweis: Zu zeigen ist die Gleichheit zweier Untermengen von $\mathcal{A}(V)$. Sei also $h \in \mathcal{A}(V)$. Dieses Element h gehört genau dann zu $(f^*)^{-1}(I_w)$, wenn $f^*(h)$ zu I_w gehört, also wenn $f^*(h)(w) = 0$ gilt. Aber $f^*(h)(w) = (h \circ f)(w) = h(f(w))$, also $f^*(h)(w) = 0$ ist gleichbedeutend mit $h(f(w)) = 0$, also mit $h \in I_{f(w)}$.

Was bedeutet diese Urbild-Bildung von maximalen Idealen? Da jeder Ring-Homomorphismus die Hintereinanderschaltung eines surjektiven Ring-Homomorphismus und einer Inklusionsabbildung ist, genügt es, die beiden Fällen zu betrachten: Ist γ: $R \to S$ ein surjektiver Ring-Homomorphismus, so entsprechen unter γ^{-1} die Ideale von S gerade den Idealen von R, die den Kern von γ enthalten, und maximale Ideale von R entsprechen den maximalen Idealen von S, die den Kern von γ enthalten. Ist R ein Unterring von S und γ: $R \to S$ die Inklusionsabbildung, so ist $\gamma^{-1}(I) = I \cap R$ für jedes Ideal I.

Warnung. Ist γ: $R \to S$ ein Ring-Homomorphismus, und ist I ein maximales Ideal von S, so wird im allgemeinen $\gamma^{-1}(I)$ zwar ein Primideal, aber kein maximales Ideal von R sein. Beispiel: sei $R = k[T], S = k(T)$ und γ die Inklusionsabbildung. In S ist das Nullideal maximales Ideal, aber $\gamma^{-1}(0) = 0$ ist in $k[X]$ kein maximales Ideal!

(0) **Isomorphismen algebraischer Mengen.** Seien $V = (V \subseteq k^n)$ und $W = (W \subseteq k^m)$ algebraische Mengen. Die Begriffsbildung in Kategorien besagt: V und W sind genau dann isomorph, wenn es Morphismen f: $W \to V$ und g: $V \to W$ gibt mit $f \circ g = 1_V$ und $g \circ f = 1_W$. Genau dann sind diese beiden Gleichungen $f \circ g = 1_V$ und $g \circ f = 1_W$ erfüllt, wenn für die Algebren-Homomorphismen f^* und g^* gilt: $g^* \circ f^* = 1_{\mathcal{A}(V)}$ und $f^* \circ g^* = 1_{\mathcal{A}(W)}$, wenn also f^* ein Algebren-Isomorphismus und g^* sein Inverses ist.

Sind f: $W \to V$ und g: $V \to W$ zueinander inverse Isomorphismen algebraischer Mengen, so sind die Algebren $\mathcal{A}(V)$ und $\mathcal{A}(W)$ zueinander isomorph. Man könnte sie also miteinander identifizieren, also mit einer festen Algebra A mit $A \simeq \mathcal{A}(V) \simeq \mathcal{A}(W)$ arbeiten. Allerdings arbeitet man, wenn man die Algebren $\mathcal{A}(V)$ und $\mathcal{A}(W)$ betrachtet, jeweils mit einem fest gewählten Erzeugendensystem dieser Algebra A. Sei etwa $V \subseteq k^n$, $W \subseteq k^m$. Erstens kann $n \neq m$ gelten, dann betrachtet man einerseits ein Erzeugendensystem von A mit genau n Elementen, andererseits ein Erzeugendensystem von A mit genau m Elementen. Zweitens wird es sich aber auch im Fall $n = m$ üblicherweise um verschiedene Untermengen des k^n handeln (allerdings um solche, die 'isomorph' sind), also um verschiedene (aber nun gleich mächtige) Erzeugendensysteme von A. Algebraisch gesehen handelt es sich also darum, daß man in der Algebra A verschiedene Erzeugendensysteme auswählt.

Warnung. Sei f: $W \to V$ ein Morphismus algebraischer Mengen. Ist f ein Isomorphismus, so entsprechen sich die Punkte von V und von W bijektiv. Allerdings kann f bijektiv sein, ohne daß f ein Isomorphismus ist. Das einfachste Beispiel ist die Abbildung f: $k \to V(Y^2 - X^3) \subset k^2$, die jedem $t \in k$ das Paar (t^2, t^3) zuordnet. Dies ist ein Morphismus, man sieht leicht, daß unter f die Punkte von k bijektiv den Punkten in $V = V(Y^2 - X^3($ entsprechen. Es ist f^*: $\mathcal{A}(V) \to k[T]$ die Einbettung der von T^2, T^3 erzeugten Unteralgebra von $k[T]$ in $k[T]$.

Wörterbuch

Was bedeutet der Anti-Äquivalenz-Satz? Er kann in zwei verschiedene Richtungen gelesen werden: Einerseits sagt er, daß Fragen über Algebren, die endlich erzeugt, reduziert und kommutativ sind, immer in geometrische Fragen übersetzt werden können. Andererseits zeigt er aber auch, daß geometrische Objekte (sofern es sich dabei um algebraische Mengen handelt) rein algebraisch beschrieben werden können. Wir wollen hier einen kleinen Ausschnitt aus dem Wörterbuch vorlegen, das beim Übersetzen gebraucht wird.

Wörterbuch: Geometrie $\mapsto$ Algebra.

(1) **Der affine Raum.** Unter der Äquivalenz wird dem affinen n-dimensionalen Raum k^n der Polynomring $\mathcal{A}(k^n) = k[X_1, \ldots, X_n]$ in n Variablen zugeordnet; insbesondere ist also $\mathcal{A}(k) = k[X]$.

(2) **Algebraische Mengen als abgeschlossene Teilmengen eines affinen**

Raums. Nach Definition ist eine algebraische Menge eine (Zariski-)abgeschlossene Teilmenge V in einem affinen Raum k^n, die als gemeinsame Nullstellenmenge einer Menge von Polynomen (in n Variablen) auftritt. Es ist $\mathcal{A}(V) = k[X_1, \ldots, X_n]/I(V)$. Der kanonische Algebren-Homomorphismus

$$\phi\colon \mathcal{A}(k^n) = k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n]/I(V) = \mathcal{A}(V)$$

bildet die Variablen $X_1, \ldots, X_n$ auf ein Erzeugendensystem $a_1 = \phi(X_1), \ldots, a_n = \phi(X_n)$ von $\mathcal{A}(V)$ ab. In (0) wurde schon herausgearbeitet, daß die Wahl eines Erzeugendensystems von $\mathcal{A}(V)$ mit m Elementen eine Einbettung von V in den affinen Raum k^m liefert. Ist nämlich $b_1, \ldots, b_m$ ein Erzeugendensystem von $\mathcal{A}(V)$, so erhält man einen surjektiven Algebren-Homomorphismus

$$\phi_{b_1,\ldots,b_m}\colon \mathcal{A}(k^m) = k[X_1, \ldots, X_m] \longrightarrow \mathcal{A}(V)$$

also einen Isomorphismus von

$$k[X_1, \ldots, X_m]/J \longrightarrow \mathcal{A}(V)$$

für ein reduziertes Ideal J. Als reduziertes Ideal ist J von der Form $J = I(V')$ für eine algebraische Menge $V' \subseteq k^m$, und der Isomorphismus

$$\mathcal{A}(V') \to \mathcal{A}(V)$$

entspricht einem Isomorphismus $V \to V'$ von algebraischen Mengen.

(3) **Die Punkte einer algebraischen Menge V.** Sei $a \in V$. Es ist also $\{a\} \subseteq V$ die Inklusion einer algebraischen Teilmenge, und wir bezeichnen mit $\iota_a\colon \{a\} \to V$ die Inklusionsabbildung. Dann ist $\iota_a^* = \phi_a$ gerade die Auswertungsabbildung an der Stelle a, die durch $\phi_a(f) = f(a)$ für $f \in \mathcal{A}(V)$ definiert ist.

(4) **Inklusionen algebraischer Mengen.** Seien $W \subseteq V \subseteq k^n$ algebraische Mengen. Die Inklusionsabbildung $\mu\colon W \to V$ liefert $\mu^*\colon \mathcal{A}(V) \to \mathcal{A}(W)$, dies ist gerade die Einschränkungsabbildung: jeder polynomialen Funktion $f\colon V \to k$ wird die Einschränkung $f|W$ zugeordnet; diese Zuordnung ist surjektiv, da jede auf W definierte polynomiale Funktion $W \to k$ durch ein Polynom $\tilde{f} \in k[X_1, \ldots, X_n]$ definiert ist, und $\tilde{f}$ natürlich auf ganz V ausgewertet werden kann. Also gilt: *Die Abbildung μ^* ist ein surjektiver Algebren-Homomorphismus* zwischen reduzierten, endlich erzeugten, kommutativen Algebren. Schreiben wir $\mathcal{A}(V) = k[X_1, \ldots, X_n]/I(V)$ so ist der Kern von μ^* gerade $I(W)/I(V)$.

Es ist durchaus bemerkenswert, daß für jede Einbettung μ der Algebren-Homomorphismus μ^* surjektiv ist, daß also jeder auf W definierter Morphismus eine Fortsetzung auf V besitzt. Dies liegt natürlich daran, daß wir hier nur (Zariski-)abgeschlossene Teilmengen $W \subseteq V$ betrachten.

Wörterbuch: Algebra $\mapsto$ Geometrie.

(5) **Die Elemente von $\mathcal{A}(V)$.** Die Elemente f von $\mathcal{A}(V)$ sind die polynomialen Abbildungen $f\colon V \to k$; jeder derartigen Abbildung $f\colon V \to k$ wird unter dem Funktor $\mathcal{A}(-)$ ein Algebren-Homomorphismus $f^*\colon \mathcal{A}(k) = k[X] \to \mathcal{A}(V)$ zugeordnet; dabei wird X gerade auf das Element f abgebildet. Die Bijektion zwischen

$$\{\text{Morphismen } V \to k\} \quad \text{und} \quad \{\text{Algebren-Homomorphismen } \mathcal{A}(k) \to \mathcal{A}(V)\}$$

ist ein Spezialfall der Tatsache, das $\mathcal{A}(-)$ voll und treu ist.

(6) **Surjektive Algebren-Homomorphismen.** Sei ein Morphismus $f\colon W \to V$ algebraischer Mengen gegeben, und f^* sei surjektiv. Der Kern von f^* ist ein reduziertes Ideal in $\mathcal{A}(V)$. Der 'Erste Isomorphiesatz' für k-Algebren besagt, daß $\mathcal{A}(W)$ zu $\mathcal{A}(V)/\operatorname{Ker} f^*$ isomorph ist. Sei V algebraische Menge im k^n. Wir haben einerseits die Projektionsabbildung $\pi\colon\ k[X_1,\dots,X_n] \to \mathcal{A}(V)$ mit Kern $I(V)$. Andererseits betrachten wir die Hintereinanderschaltung $f\circ\pi\colon\ k[X_1,\dots,X_n] \to \mathcal{A}(W)$, sei $J = \operatorname{Ker}(f\circ\pi)$. Es ist dann $I(V) \subseteq J$, und $J/I(V) = \operatorname{Ker} f$. Da J reduziertes Ideal ist, gibt es eine algebraische Menge $W' \subseteq V$ mit $J = I(W')$. Der Homomorphismus f^* liefert einen Isomorphismus $\mathcal{A}(W') \simeq \mathcal{A}(W)$, die algebraischen Mengen W, W' sind also isomorph, und W' ist eine algebraische Untermenge von V. Unter f wird also W bijektiv auf die algebraische Teilmenge W' von V abgebildet. Für die umgekehrten Überlegungen verweisen wir auf (4).

(7) **Die Einbettung einer Algebra A in den Polynomring $A[X]$.** Sei A eine reduzierte, endlich erzeugte, kommutative k-Algebra, es gibt also eine algebraische Menge $V \subseteq k^n$ mit $A = \mathcal{A}(V) = k[X_1,\dots,X_n]/I(V)$. Betrachte nun $V\times k \subseteq k^{n+1}$ und die Projektionsabbildung

$$\pi\colon\ V\times k \longrightarrow V \quad \text{mit} \quad \pi(a,c) = c \quad \text{für} \quad a\in V, c\in k.$$

Es ist $\mathcal{A}(V\times k) = A[X]$ and $\pi^* = \iota$.

(8) **Endliche Ring-Erweiterungen.** Wir betrachten einen Morphismus $f\colon W \to V$, so daß $f^*\colon\ A = \mathcal{A}(V) \to \mathcal{A}(W) = B$ injektiv und B endlich über dem Bild von f^* ist. Wir können annehmen, daß f^* eine Inklusionsabbildung ist, daß also A ein Unterring von B ist. Wir wissen: Ist Q ein Primideal von B, so ist $Q\cap A$ ein Primideal von A und man erhält auf diese Weise alle Primideale von A. Zu jedem Primideal P von A gibt es also mindestens ein Primideal Q von B mit $Q\cap A = P$, und es gibt nur endlich viele derartige Primideale Q. Genau dann ist Q maximales Ideal von B, wenn $Q\cap A$ maximales Ideal von A ist. Schauen wir uns die Zuordnung $Q \mapsto Q\cap A$ genauer an: Ist etwa $Q = I_w$ das Auswertungsideal von $\mathcal{A}(W)$ an der Stelle $w\in W$, so ist $Q\cap A = I_{f(w)}$. Dies zeigt: *Der Morphismus $f\colon W\to V$ ist surjektiv, und die Urbilder der einzelnen Punkte in V* (man nennt sie die 'Fasern' der Abbildung) *sind endliche (nicht leere) Teilmengen von V.*

(9) **Algebraische, aber nicht endliche Ring-Erweiterungen.** Wir betrachten eine Einbettung $\iota\colon\ A \to B$, wobei B algebraisch, aber nicht ganz über A ist. Wir beschränken uns auf den Fall, wo A ein Integritätsbereich ist und B die folgende spezielle Form hat: $B = A[a^{-1}] \subseteq \operatorname{Quot}(A)$, dabei sei $a\neq 0$ ein nicht-invertierbares Element von A. (Ist A "ganz abgeschlossen", wie zum Beispiel im Fall eines Polynomrings, so ist a^{-1} auf keinen Fall endlich über A. Im allgemeinen bilden die Elemente von $\operatorname{Quot}(A)$, die ganz über A sind, einen echten Unterring von $\operatorname{Quot}(A)$.) Das Element a^{-1} ist Nullstelle eines linearen Polynoms mit Koeffizienten in A, nämlich von $aT-1$.

Sei also V eine irreduzible algebraische Menge, sei $f\neq 0$ eine polynomiale Funktion auf V, die nicht invertierbar ist. Wir betrachten die Einbettung

$$\iota\colon\ \mathcal{A}(V) \to \mathcal{A}(V)[f^{-1}].$$

Es ist $\mathcal{A}(V)[f^{-1}]$ reduziert und endlich erzeugt, also von der Form $\mathcal{A}(W)$ für eine algebraische Menge W; ist $V\subseteq k^n$, so können wir W als abgeschlossene Untermenge des k^{n+1} realisieren, nämlich als Menge

$$W = \{(a,c) \mid a\in V,\ c\in k, \quad \text{mit} \quad f(a)\cdot c = 1\} \ \subseteq\ k^{n+1}.$$

Die Projektionsabbildung $f\colon W \to V$ mit $f(a,c) = a$ liefert unter dem Funktor $\mathcal{A}(-)$ gerade $f^* = \iota$. Diese Abbildung f ist injektiv und unter f wird W mit der Teilmenge $\{a \in V \mid f(a) \neq 0\} \subseteq V$ identifiziert; dies ist eine Zariski-offene Teilmenge von V, nämlich gerade das Komplement der Nullstellenmenge von f in V.

Beachte: Der 'Trick von Rabinowitsch' verwendet gerade diese Konstruktion!

(10) **Noether'sche Normalisierung.** Sei A eine reduzierte, endlich erzeugte, kommutative k-Algebra, sei B eine Noether'sche Normalisierung von A, also eine Unteralgebra, die von algebraisch unabhängigen Elementen $b_1, \dots, b_t$ erzeugt wird, so daß B endlich über A ist. Sei $A = \mathcal{A}(V)$, dabei sei $V \subseteq k^n$ eine algebraische Menge. Natürlich ist $B = \mathcal{A}(k^t)$ und die Inklusion $B \subseteq A$ ist das Bild unter $\mathcal{A}(-)$ eines Morphismus $f\colon V \to k^t$. Da A endlich über B ist, folgt, daß f surjektiv mit endlichen Fasern ist. Es gilt also: *Zu jeder algebraischen Menge V der Dimension t gibt es einen Morphismus $V \to k^t$, der surjektiv ist und endliche Fasern hat.*

Weitere Bemerkungen zu den Morphismen algebraischer Mengen

Noch einmal: Was bedeutet der Anti-Äquivalenz-Satz? Auf der geometrischen Seite ist sicher der Morphismenbegriff ungewohnt; klassisch hat sich die Geometrie eigentlich nur um geometrische Objekte und deren Unterobjekte gekümmert (also um surjektive Algebren-Homomorphismen). Die Anti-Äquivalenz von Kategorien legt es nahe, sich auch auf der geometrischen Seite für beliebige Morphismen zu interessieren. Die injektiven Algebren-Homomorphismen entsprechen dabei, wie wir gesehen haben, recht unterschiedlichen geometrischen Konstruktionen.

Die Überlegungen in (4) und (6) besagen:

Ist $f\colon W \to V$ ein Morphismus von algebraischen Mengen, so ist f^* genau dann surjektiv, wenn gilt $f = f_2 \cdot f_1$, wobei f_1 ein Isomorphismus und f_2 die Inklusion einer (Zariski-)abgeschlossen Untermenge von V ist.

Entsprechend gilt:

Ist $f\colon W \to V$ ein Morphismus von algebraischen Mengen, so ist f^* genau dann injektiv, wenn V der (Zariski-)Abschluß der Menge der Bildpunkte von f ist.

Beweis: Gegeben ist also die algebraische Menge $V \subseteq k^n$, und der Morphismus $f\colon W \to V$. Sei V' der Zariski-Abschluß der Menge $W' = \{f(w) \mid w \in W\}$, also $V' = V(I(W'))$. Ist V' eine echte Untermenge von V, so ist $I(V)$ echt in $I(V')$ enthalten, und $I(V')/I(V)$ liegt im Kern von $f^*\colon k[X_1, \dots, X_n]/I(V) \to \mathcal{A}(W)$. Dies zeigt, daß f^* nicht injektiv sein kann. Ist umgekehrt f^* nicht injektiv, so ist der Kern von f^* von der Form $J/I(V)$, wobei J ein reduziertes Ideal von $k[X_1, \dots, X_n]$ ist, das $I(V)$ echt enthält. Als reduziertes Ideal ist J von der Form $J = I(V'')$ und V'' ist eine echte Teilmenge von V, die alle Bildpunkte von f enthält. Natürlich ist V'' abgeschlossen, also ist $V' \subseteq V'' \subset V$.

Da der Funktor $\mathcal{A}(-)$ kontravariant ist, überrascht es nicht, daß surjektive Algebren-Homomorphismen injektive Morphismen algebraischer Mengen liefern. Den injektiven Algebren-Homomorphismen entsprechen dagegen eine Vielzahl möglicher geometrischer Verhaltensweisen! Wir notieren noch, daß es reicht, sich mit Algebren-Homomorphismen zu beschäftigen, die entweder surjektiv oder injektiv sind:

Seien V, W algebraische k-Mengen, sei $f\colon W \to V$ ein Morphismus. Wir betrachten den zugehörigen Algebren-Homomorphismus $f^*\colon \mathcal{A}(V) \to \mathcal{A}(W)$. Sei B das Bild von f^*, dies ist wieder eine endlich erzeugte, reduzierte, kommutative k-Algebra (endlich erzeugt, weil B zu einer Faktoralgebra von $\mathcal{A}(V)$ isomorph ist, reduziert, weil B eine Unteralgebra von $\mathcal{A}(W)$ ist), also $B = \mathcal{A}(U)$ für eine algebraische k-Menge

U. Wir erhalten eine Faktorisierung $f = f_2 \circ f_1$ mit $f_1\colon W \to U$, $f_2\colon U \to V$, dabei ist $f_2^*\colon \mathcal{A}(V) \to \mathcal{A}(U)$ surjektiv und $f_1^*\colon \mathcal{A}(U) \to \mathcal{A}(W)$ injektiv (und natürlich gilt $f^* = f_1^* \circ f_2^*$). Es genügt, die beiden Morphismen f_1, f_2 zu analysieren. Den Fall eines surjektiven Algebren-Homomorphismus haben wir vollständig behandelt, der Fall eines injektiven Algebren-Homomorphismus konnte hier nur beispielhaft behandelt werden.

Noch einmal: Der Funktor $\mathcal{A}(-)$. Sind V, W algebraische Mengen, so bezeichnen wir mit $\operatorname{Mor}(V, W)$ die Menge der Morphismen $V \to W$. Es gilt

$$\mathcal{A}(V) = \operatorname{Mor}(V, k) \quad \text{und} \quad \mathcal{A}(f) = \operatorname{Mor}(f, k)$$

für jede algebraische Menge V und jeden Morphismus f von algebraischen Mengen. Wir sehen also, daß die kontravarianten Funktoren $\mathcal{A}(-)$ und $\operatorname{Mor}(-, k)$ (als Funktoren von der Kategorie der algebraischen Mengen in die Kategorie der Mengen) übereinstimmen. Funktoren der Form $\operatorname{Mor}(-, U)$ nennt man "darstellbare" Funktoren. Wir sehen also, daß $\mathcal{A}(-)$ ein "darstellbarer" Funktor ist.

11. Ausblick

Unser Einblick in die Beziehungen zwischen kommutativer Algebra und algebraischer Geometrie betrachtete nur algebraische Mengen, und demnach nur reduzierte endlich erzeugte kommutative k-Algebren. Dabei haben wir zwei Richtungen völlig ausgespart:

A. Die lokale Theorie. Ist man an einzelnen Punkten einer algebraischen Mengen interessiert, zum Beispiel an Doppelpunkten einer Kurve oder an komplizierteren "Singularitäten", so betrachtet man den zugehörigen "lokalen" Ring: Ist etwa V eine irreduzible algebraische Menge und $v \in V$, so untersucht man den Ring $\mathcal{A}(V)_v = \{\frac{f}{g} \mid f, g \in \mathcal{A}(V), g(v) \neq 0\}$. Dieser Ring spiegelt die geometrischen Eigenschaften im Umfeld des Punkts v wider. Besitzt V nicht nur diesen einen Punkt, so ist $\mathcal{A}(V)_v$ nicht endlich erzeugt als k-Algebra, aber immerhin ein noetherscher Integritätsbereich. Den Übergang von $\mathcal{A}(V)$ zu $\mathcal{A}(V)_v$ nennt man "Lokalisieren", hier wurde an einem maximalen Ideal, nämlich dem Verschwindungsideal zum Punkt v, "lokalisiert". Man kann an beliebigen Primidealen "lokalisieren" und erhält auf diese Weise analog Aussagen über die Einbettung von irreduziblen algebraischen Teilmengen in V.

B. Projektive Varietäten. Wir haben gesehen, daß es sich manchmal lohnt, nur mit homogenen Polynomen zu arbeiten; das zugehörige geometrische Modell beim Arbeiten mit homogenen Polynomen in n Variablen nennt man den "projektiven Raum" $\mathbb{P}_{n-1}$ der Dimension $n-1$. Die Dimensionsverschiebung ist folgendermaßen begründet: Jedes Polynom $f = \sum c_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ kann man "homogenisieren", dabei nimmt man eine zusätzliche Variable X_0 und multipliziert die auftretenden Monome $X_1^{i_1} \cdots X_n^{i_n}$ mit einer geeigneten Potenz $X_0^{i_0}$, so daß man ein homogenes Polynom $\tilde{f}$ erhält (ist der Grad von f höchstens d, so kann man jeweils $i_0 = d - \sum_{j=1}^n i_j$ nehmen). Das ursprüngliche Polynom f erhält man aus $\tilde{f}$ zurück, wenn man X_0 durch 1 ersetzt. Die Nullstellenmenge von $\tilde{f}$ ist eine Teilmenge des k^{n+1}, und natürlich ein Kegel. Schneidet man diesen Kegel K mit der Hyperebene $V(X_0 - 1)$, so erhält man in dieser Hyperebene (sie ist ein affiner Unterraum der Dimension n) eine Teilmenge, die man als die algebraische Menge $V(f)$ interpretieren kann. Diejenigen Geraden im Kegel K, die die Hyperebene $V(X_0 - 1)$ nicht schneiden, liegen in der Hyperebene $V(X_0)$; die geometrische Vorstellung, mit der man hier arbeitet, interpretiert die Ursprungsgeraden in $V(X_0)$ als "uneigentliche" oder "unendlich ferne" Punkte, die zum affinen Raum $V(X_0 - 1)$ hinzugefügt werden; projektive Varietäten werden als Vervollständigungen von irreduziblen algebraischen Mengen aufgefaßt. Wie schon erwähnt, arbeitet die algebraische Entsprechung mit homogenen Polynomen, und damit mit homogenen Idealen, insbesondere natürlich mit homogenen Primidealen und damit mit "graduierten" Algebren. Hierzu gehört die sogenannte klassische Invariantentheorie, die sich mit den homogenen Polynomen festen Grades und fester Variablenanzahl beschäftigte.

"Schematische" algebraische Geometrie. Schließlich ist als Grundbegriff der modernen algebraischen Geometrie der Begriff eines "Schemas" zu erwähnen. Hier wird einerseits die volle Bandbreite kommutativer Algebren oder kommutativer Ringe als mögliche Koordinatenringe zugelassen (es darf also nilpotente Ideale geben, es müssen keine Endlichkeitsbedingungen gelten), andererseits werden durch die Verwendung von "Garben" Verklebungen derartiger Ringe betrachtet, wie sie schon in der klassischen projektiven Geometrie eine Rolle spielen.

Zum Idealbegriff. Einer der Grundbegriffe der kommutativen Ringtheorie ist der Idealbegriff. Wir haben den Ring $\mathbb{Z}$ der ganzen Zahlen und den Polynomring $k[X]$ in einer Variablen als typische einfachste Ringe vorgestellt, dies verweist darauf, daß die wichtigsten Anwendungen der kommutativen Ringtheorie in der (algebraischen) Zahlentheorie und in der (algebraischen) Geometrie zu finden sind. Arbeitet man mit einem derartigen Ring R, so ist man zuerst vor allem an seinen Elementen, also zum Beispiel eben an ganzen Zahlen oder an einzelnen Polynomen, interessiert. Es erleichtert das Rechnen, wenn man die jeweiligen Primelemente kennt, allerdings nur dann, wenn es auch genügend viele derartigen Elemente gibt: wenn R faktoriell ist. Im Rahmen der Zahlentheorie hat Kummer vorgeschlagen, in nicht-faktoriellen Ringen statt mit 'Zahlen' (also Elementen) mit 'idealen Zahlen' (also Idealen) zu arbeiten; statt mit Primelementen arbeitet man mit Primidealen. In den sogenannten Dedekind-Ringen gilt in Analogie zur Faktorialität, also zur Darstellung von Elementen als Produkt von Primzalen: Jedes von Null verschiedene Ideal ist (eindeutig) als Produkt von Primidealen schreibbar. Natürlich ist ein von Null verschiedenes Hauptideal $\langle r\rangle$ genau dann ein Primideal, wenn r ein Primelement ist. Eine gewisse Nähe zwischen Elementen einerseits und Idealen andererseits kann es allerdings nach dem Krull'schen Haupidealsatz nur in Ringen der (Krull-)Dimension höchstens 1 geben, da Primideale P mit $h(P) \geq 2$ nie Haupideale sein können. In der Zahlentheorie spielen die Ringe der 'ganzen Zahlen' in Zahlkörpern eine wichtige Rolle, diese sind eindimensional. In der algebraischen Geometrie beschreiben die eindimensionalen (reduzierten, endlich erzeugten) k-Algebren gerade die Kurven. Typische Beispiele von Primidealen in eindimensionalen Ringen, die keine Hauptideale sind:

(a) Betrachte $A = k[X,Y]/(Y^2 - X^3)$ (oder, dazu isomorph, die von T^2 und T^3 erzeugte Unteralgebra von $k[T]$): das Ideal $\langle X,Y\rangle$ (oder $\langle T^2,T^3\rangle$) ist ein Primideal (der zugehörige Faktorring ist k), aber kein Haupideal. Die Restklassen $x = \overline{X}$ und $y = \overline{Y}$ von X,Y in A sind nicht assoziierte irreduzible Elemente, aber keine Primelemente, denn es gilt ja $x^2 = y^3$.

(b) Analog ist im Ring $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/\langle X^2+5\rangle$ das Ideal $I = \langle 2, 1-\sqrt{-5}\rangle$ ein Primideal, aber kein Hauptideal (das Ideal I ist der Kern des eindeuig bestimmten Ring-Homomorphismus $\mathbb{Z}[X]/\langle X^2+5\rangle \to \mathbb{F}_2$; er schickt die Restklasse von X auf 1); hier haben wir paarweise nicht assoziierte irreduzible Elemente $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$, mit $(1+\sqrt{-5})(1-\sqrt{-5})$.

Die Ählichkeit der Theorie der ganzen algebraischen Zahlen in einem Zahlkörper und der Theorie der algebraischen Kurven wurde von Kronecker, Dedekind und Weber aufgezeigt. (Siehe z.B. Klein: *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*, p.320 ff). Die kommutative Algebra ist als Klammer zwischen der Zahlentheorie und der algebraischen Geometrie zu sehen.

12. Literatur

Hier sind einige Bücher, die zur ersten Lektüre herangezogen werden können; zuerst zwei einführende Texte zur kommutativen Ringtheorie, die höchstens andeutungsweise auf geometrische Sachverhalte eingehen:

ATIYAH, MACDONALD: Introduction to Commutative Algebra.
KAPLANSKY: Commutative Rings.

Eher geometrisch motiviert sind die Bücher:

KUNZ: Einführung in die kommutative Algebra und algebraische Geometrie.
SCHAFAREWITSCH (oder SHAFAREVICH): Grundzüge der algebraischen Geometrie / Basic Algebraic Geometry.

Sehr elementar und sehr gut lesbar sind:

REID: Undergraduate Algebraic Geometry. (Nur 125 Seiten; der Teil I lautet: Playing with plane curves. Teil II: The category of affine varieties. Im Teil III geht es um: Projective varieties. Tangent space and non-singularity. Und schließlich um die 27 Geraden auf kubischen Flächen.)
FULTON: Algebraic Curves. (Von besonderem Interesse: auf Seite 112 der Satz von Bézout über den Durchschnitt zweier ebener Kurven, und am Ende des Buchs, S.210, der Satz von Riemann-Roch.)

Als Standard-Einführungstext in die algebraische Geometrie gilt:

HARTSHORNE: Algebraic Geometry. (Dort wird gerade das, was hier entwickelt wurde, als bekannt vorausgesetzt.)