Dr. Fritz Hörmann

Vorlesungsskript:

Kommutative Algebra
und Einführung in die algebraische Geometrie

Universität Freiburg — SS 2014

1 Grundlagen

1.1 Literatur

[E] D. Eisenbud. *Commutative Algebra with a view towards Algebraic Geometry.*, Springer 1995.

[AM] M.F. Atiyah und I.G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley 1969.

[M] D. Mumford. *The red book of varieties and schemes.* Lecture Notes in Mathematics 1358. Springer 1988.

[S] I.R. Shafarevich. *Basic algebraic geometry.* Springer 1994.

[H] R. Hartshorne. *Algebraic Geometry.* Graduate Texts in Mathematics. Springer 1977.

[Z] Zariski, Samuel, *Commutative algebra*, Vol 1 und 2.

1.2 Einführung

Die **algebraische Geometrie** beschäftigt sich mit dem Studium von Varietäten, also Teilmengen eines endlich-dimensionalen Raumes über einem Körper, welche durch polynomiale Gleichungen beschrieben werden können. Genauer: Sei $\{f_1, f_2, f_3, \dots\}$ eine Teilmenge des Polynomrings $k[x_1, \dots, x_n]$ in n Variablen. Dann ist

$$V = V(f_1, f_2, \dots) := \{\lambda \in k^n \mid f_1(\lambda) = f_2(\lambda) = \cdots = 0\} \tag{1}$$

die zugehörige (affine) Varietät. Sie besteht also aus denjenigen n-Tupeln, die simultane Nullstelle aller Polynome f_i sind. Die übliche Methode besteht darin, geometrische Eigenschaften einer solchen Varietät V, die untersucht werden sollen, in Eigenschaften von rein algebraischen Objekten zu übersetzen. Dies führt auf die Theorie der **kommutativen Algebra**. Z.B. können alle *wesentlichen* geometrischen Eigenschaften der affinen Varietät (1) an dem kommutativen Ring

$$k[x_1, \dots, x_n]/I(V)$$

abgelesen werden. Hierbei ist $I(V) = \{f \in k[x_1, \dots, x_n] \mid f(X) = 0 \text{ für alle } X \in V\}$[1].
Keine der beiden Theorien/Aspekte hat jedoch den alleinigen Anspruch darauf, die grundlegendere oder interessantere zu sein. Viele grundlegende Fragen der (kommutativen) Algebra gelangen erst dadurch zu einem tieferen Verständnis, indem man sie in geometrische Problemstellungen übersetzt, und umgekehrt sind viele Fragestellungen der Algebra nur deshalb interessant, weil sie Übersetzungen offensichtlicher geometrischer Fragen sind. Dieses Wechselspiel, das bei uns in der Vorlesung von Anfang an im Mittelpunkt stehen soll, ist nicht nur für sich ein ästhetisches Teilgebiet der Mathematik, sondern hat die Algebra und auch die Zahlentheorie als Ganzes ungemein beflügelt. Spätestens seit Grothendieck assoziiert man zu *jedem* kommutativen Ring, also auch solchen aus der Zahlentheorie, wie $\mathbb{Z}$, oder $\mathbb{Z}[\sqrt{-5}]$, oder $\mathbb{Z}[X]$, ein geometrisches Objekt, um die Fruchtbarkeit des obigen Wechselspiels auch hier ausnutzen zu können.
Zu den einfachsten Varitäten gehören die sogenannten ebenen Kurven. Sie werden durch *ein* Polynom $f \in k[x, y]$ in zwei Variablen beschrieben. In den Abbildungen 1–8 finden Sie Beispiele. Abbildung 9 zeigt ein Beispiel einer algebraischen Fläche. (Wir schreiben $\mathbb{A}^n$ für k^n aufgefasst als Varietät.)

[1] In vielen Fällen ist $I(V)$ das von der Menge $\{f_1, f_2, f_3, \dots\}$ erzeugte Ideal, siehe Hilbertscher Nullstellensatz.

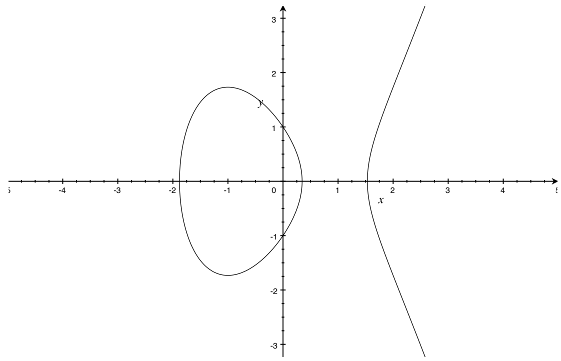

Abbildung 1: Die affine Varietät $V_1 := \{[x, y] \in \mathbb{A}^2 \mid y^2 = x^3 - 3x + 1\}$

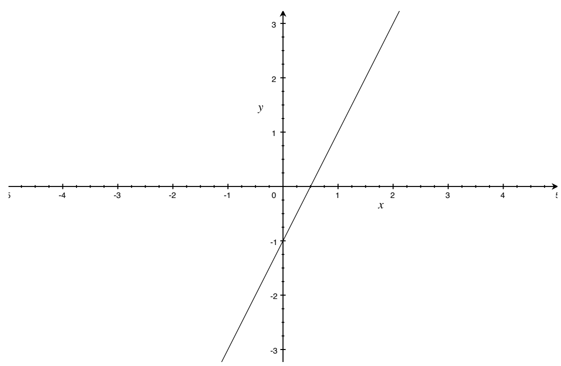

Abbildung 2: Die affine Varietät $V_2 := \{[x, y] \in \mathbb{A}^2 \mid y = 2x - 1\}$

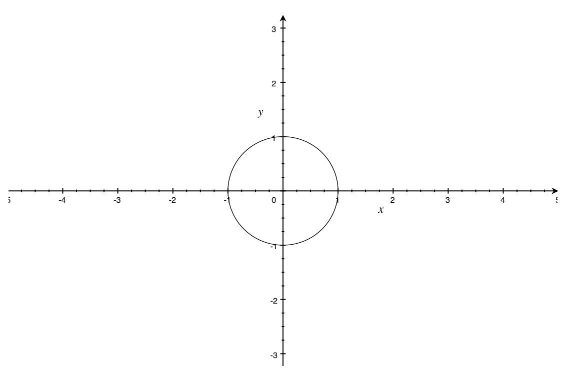

Abbildung 3: Die affine Varietät $V_3 := \{[x, y] \in \mathbb{A}^2 \mid x^2 + y^2 = 1\}$

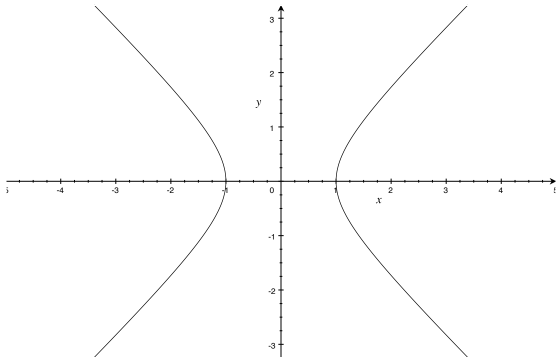

Abbildung 4: Die affine Varietät $V_4 := \{[x,y] \in \mathbb{A}^2 \mid x^2 - y^2 = 1\}$

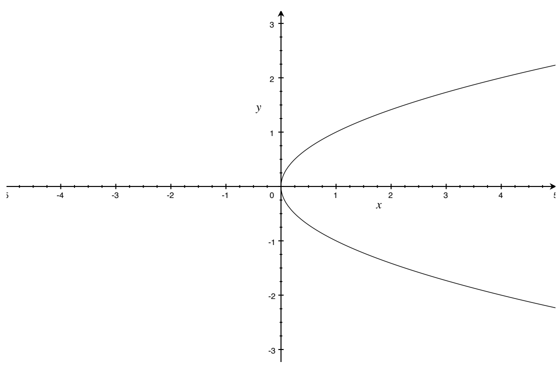

Abbildung 5: Die affine Varietät $V_5 := \{[x,y] \in \mathbb{A}^2 \mid y^2 = x\}$

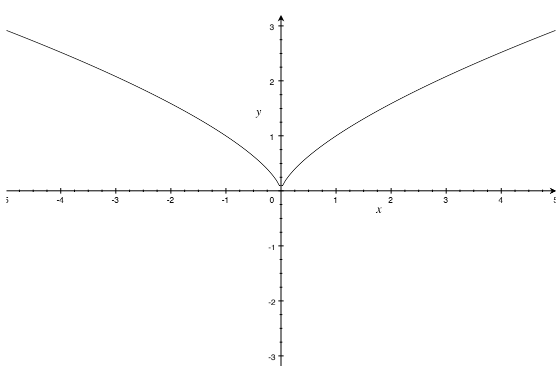

Abbildung 6: Die affine Varietät $V_6 := \{[x,y] \in \mathbb{A}^2 \mid x^2 = y^3\}$

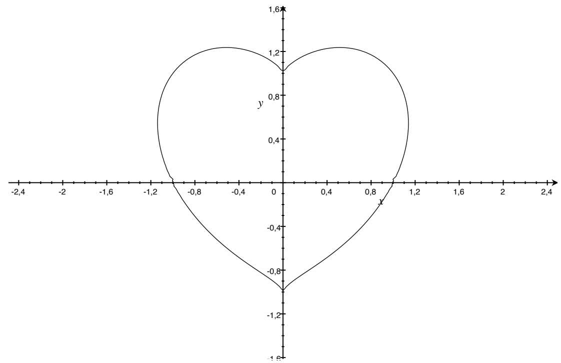

Abbildung 7: Die affine Varietät $\{[x, y] \in \mathbb{A}^2 \mid \left(x^2 + y^2 - 1\right)^3 = x^2 y^3\}$

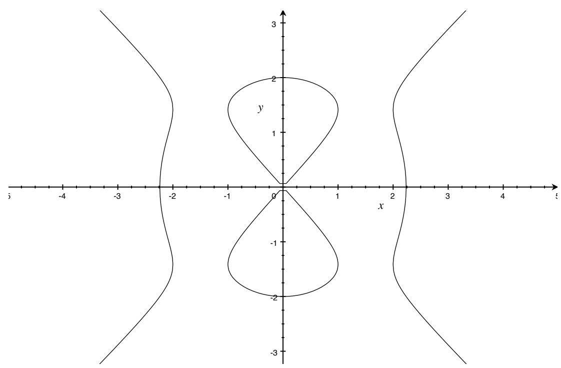

Abbildung 8: Die affine Varietät $\{[x, y] \in \mathbb{A}^2 \mid y^4 - 4y^2 = x^4 - 5x^2\}$

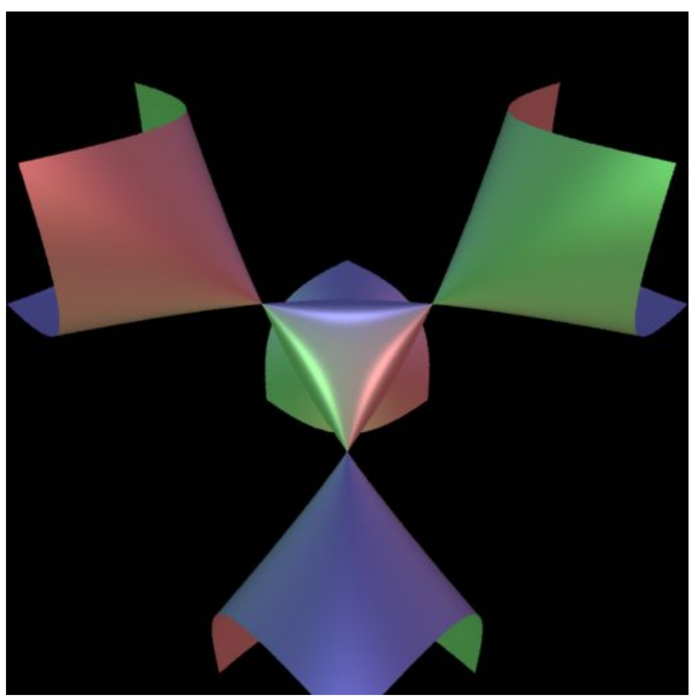

Abbildung 9: Die affine Varietät $\{[x, y, z] \in \mathbb{A}^3 \mid -5(x^2(y+z) + y^2(x+z) + z^2(x+y)) + 2(xy + yx + xz) = 0\}$

Wir haben in den Abbildungen das *reelle* Bild gezeichnet, d.h. implizit angenommen, dass der Körper $k = \mathbb{R}$ ist. Dies ist für unsere algebraische Zielsetzung nicht hilfreich. Man kann dies zwar tun, sollte dann statt mit affinen Varietäten mit sogenannten affinen Schemata arbeiten. Dies werden wir in dieser Vorlesung nicht machen, da dieser Allgemeinheitsgrad die grundlegenden Verhaltensweisen der algebraischen Geometrie verschleiert.

Beispiel 1.2.1. *Die* reellen *Varietäten $V = V(x, y)$ und $W = V(x^2 + y^2)$ in $\mathbb{A}^2$ bestehen beide nur aus dem Nullpunkt. Dennoch erwarten wir, dass W eine Kurve ist, da sie durch* eine *Gleichung beschrieben wird. In der Tat liegen auf ihr die unendlich vielen* komplexen *Punkte $[x = \lambda, y = i\lambda], \lambda \in \mathbb{C}$.*

Beispiel 1.2.2. *Sei $f \in k[x]$ ein Polynom. Die dadurch beschriebene Varietät $V(f) \subset \mathbb{A}^1$ ist gerade durch die Nullstellen von f gegeben. Falls k nicht algebraisch abgeschlossen ist, muss f keine Nullstellen besitzen. Also können wir im allgemeinen aus der Kenntnis der Nullstellen wenig über f aussagen. Ist k hingegen algebraisch abgeschlossen, so können wir f bis auf einen Faktor aus k^* aus seinen Nullstellen rekonstruieren, sofern wir wissen, dass f keine doppelten Nullstellen hatte. Dies ist der einfachste (und triviale) Fall des sogenannten* Hilbertschen Nullstellensatzes*.*

Beispiel 1.2.3. *Die beiden Varietäten V_3 (Kreis aus Abbildung 3) und V_4 (Hyperbel aus Abbildung 4) gehen durch die invertierbare Koordinatentransformation*

$$y \mapsto iy \qquad x \mapsto x$$

auseinander hervor. Trotz des völlig unterschiedlichen reellen Bildes handelt es sich also um ein und dasselbe geometrische Objekt über den komplexen Zahlen.

Diese Beispiele verdeutlichen, dass sich die Geometrie der Varietäten vereinfacht, wenn wir annehmen, dass der Körper k algebraisch abgeschlossen ist. Dies werden wir in dieser Vorlesung tun. Es ist aber — und dies kennen Sie aus der linearen Algebra — meistens nicht nötig, explizit $k = \mathbb{C}$ anzunehmen. Es gibt auch z.B. Körper der Charakteristik p, die algebraisch abgeschlossen sind, und über denen wir mit den gleichen Methoden algebraische Geometrie betreiben können. Manche Unterschiede ergeben sich jedoch, und manchmal werden wir daher zumindest auch annehmen, dass k von der Charakteristik 0 sein soll.
Ausser den Varietäten selber werden wir auch Abbildungen zwischen diesen betrachten, die ihrerseits durch Polynome beschrieben werden können (sogenannte Morphismen von Varietäten):

Beispiel 1.2.4. *Wir haben bereits gesehen, dass die Transformation*

$$y \mapsto iy \qquad x \mapsto x$$

die beiden Varietäten V_3 (Kreis, Abbildung 3) und V_4 (Hyperbel, Abbildung 4) ineinander überführt. Auch das Inverse dieser Transformation existiert und ist durch Polynome gegeben. Wir sagen daher auch, dass V_3 und V_4 isomorph *sind.*

Beispiel 1.2.5. *Wir können eine Abbildung angeben von der Standardgeraden $\mathbb{A}^1$ auf die Parabel V_5 (Abbildung 5) durch*

$$\begin{array}{rcl} \mathbb{A}^1 & \to & V_5 \\ [t] & \mapsto & [t^2, t] \end{array}$$

und umgekehrt durch

$$\begin{array}{rcl} V_5 & \to & \mathbb{A}^1 \\ [x, y] & \mapsto & [y] \end{array}$$

Wir sehen, dass diese Abbildungen zueinander invers sind und beide durch Polynome beschrieben werden. Auch V_5 und $\mathbb{A}^1$ sind also isomorph (Die Parabel ist eine "ohne Verlust" gebogene Gerade).

Beispiel 1.2.6. *Betrachte die Abbildung*

$$\begin{array}{rcl} \varphi : \mathbb{A}^1 & \to & V_6 \\ [t] & \mapsto & [t^3, t^2] \end{array}$$

(siehe Abbildung 6). Sie ist sinnvoll definiert, denn der Punkt $[x = t^3, y = t^2]$ *erfüllt offensichtlich die Gleichung* $x^2 = y^3$. *Die Abbildung*

$$\begin{array}{rcl} V_6 & \to & \mathbb{A}^1 \\ [x, y] & \mapsto & \begin{cases} 0 & y = 0, \\ \frac{x}{y} & \textit{sonst.} \end{cases} \end{array}$$

ist ihr Inverses, φ *ist also* bijektiv*; allerdings ist die Umkehrabbildung* φ^{-1} nicht *durch Polynome gegeben* ($\frac{x}{y}$ *ist eine rationale Funktion und im Nullpunkt unbestimmt). Die Kurve* V_6 *hat auch eine sogenannte* **Singularität** *im Nullpunkt, während* $\mathbb{A}^1$ *keine Singularitäten besitzt. Wir werden später sehen, dass dies a priori impliziert, dass* $\mathbb{A}^1$ *und* V_6 *nicht isomorph sein können. Später werden wir einen etwas allgemeineren Varietätsbegriff einführen und zu der Aussage gelangen, dass die Einschränkung von* φ*:*

$$\mathbb{A}^1 \setminus \{[0]\} \to V_6 \setminus \{[0, 0]\}$$

ein Isomorphismus von Varietäten ist. Im Augenblick ergibt diese Aussage für uns noch keinen Sinn, da offensichtlich $\mathbb{A}^1 \setminus \{[0]\}$ *nicht die Nullstellenmenge eines Polynoms ist.*

Beispiel 1.2.7. *Wir definieren eine Abbildung*

$$\varphi : \mathbb{A}^1 \to V_3$$

(V_3 ist ein Kreis, siehe Abbildung 3) wie folgt: Wir fassen $\mathbb{A}^1$ *als die y-Achse auf, und betrachten für einen Punkt [t,0] auf dieser, die Verbindungsgerade mit dem Punkt* $[0, 1]$ *auf* V_3. *Diese hat die Gleichung:*

$$x + ty - t = 0.$$

Der Schnitt dieser Geraden mit dem Kreis ergibt die folgende Gleichung:

$$x^2 = \frac{2x}{t} - \frac{x^2}{t^2}$$

mit den Lösungen also $x = 0$ *(dies führt auf den Punkt* $[0, 1]$*) oder* $x = \frac{2t}{t^2+1}$ *(dies führt zum Punkt* $[\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}]$*). Wir bekommen also ausser dem offensichtlichen Schnittpunkt* genau einen *weiteren Punkt. Die Abbildung werde nun durch*

$$[t] \mapsto [\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}]$$

definiert. Sie ist nicht *durch Polynome gegeben, sondern wiederum nur durch rationale Funktionen, welche aber ausserhalb von* $t = i$ *oder* $t = -i$ *für alle komplexen Zahlen definiert sind. Später werden wir sehen, dass die Abbildung einen Isomorphismus von Varietäten*

$$\mathbb{A}^1 \setminus \{[i], [-i]\} \to V_3 \setminus \{[0, 1]\}$$

definiert. Auch $\mathbb{A}^1$ *und* V_3 *(Kreis) sind also isomorph, wenn man gewisse Punkte herausnimmt. Dies wird eine weiterreichende anschauliche Erklärung finden, wenn wir* projektive *Varietäten betrachten. Im gewissem Sinne sind* $\mathbb{A}^1$ *und* V_3 *zwei affine Bilder ein und desselben projektiven Objektes, nämlich der projektiven Geraden* $\mathbb{P}^1$.

Soweit haben wir hauptsächlich ebene Kurven als Beispiele betrachtet. Im höherdimensionalen stellen sich 3 grundlegende Fragen. Sei $S \subseteq k[x_1, \ldots, x_n]$ eine Menge von Polynomen.

1. Kann man *endlich viele* Funktionen $f_1, \ldots, f_n \in S$ so finden, dass $V(S) = V(f_1, \ldots, f_n)$? Mit anderen Worten, reichen endlich viele Polynomgleichungen, um eine Varietät zu definieren?
2. Wie lautet das algebraische Kriterium dafür, dass $V(S) \neq \emptyset$? Verwandte Frage: Inwiefern kann ich die Menge S aus $V(S)$ rekonstruieren?
3. Wie definiere ich *algebraisch*, welche Dimension $V(S)$ hat? Wann ist $V(S)$ eine Kurve, Fläche, etc.?

Anmerkungen: Dass alle 3 Fragen schwierig sind, liegt u. a. an dem folgenden Problem: Sei $V(f_1, \ldots, f_n)$ eine Varietät und f_{n+1} ein Polynom. Unsere naive Vorstellung sagt uns vielleicht zunächst, dass die Varietät

$$V(f_1, \ldots, f_n, f_{n+1})$$

eine *um eins* kleinere Dimension haben sollte. Dies muss aber natürlich nicht so sein; f_{n+1} könnte gleich einem der vorhergehenden f_i sein. Aber falls sie dieselbe Dimension hat, kann sie kleiner werden? Um die Subtilität dieser Frage zu verdeutlichen, schaue man sich die folgenden Varietäten an (alle im $\mathbb{A}^2$):

$$V(x, y), \quad V(x, x+1), \quad V(xy + x^2, xy + y^2).$$

In jedem Fall ist die Dimension unterschiedlich (nämlich 0, 'leer' und 1) und es passiert etwas anderes beim Hinzunehmen des jeweils zweiten Polynoms. Trotz dieser Subtilität lassen sich alle 3 Fragen zufriedenstellend lösen, auch wenn die Lösungen nicht immer ganz einfach sind. Dies wird das erste Ziel der Vorlesung sein. Frage 1 wird durch den Hilbertschen Basissatz beantwortet. Frage 2 durch den Hilbertschen Nullstellensatz und Frage 3 durch die Dimensionstheorie.

1.3 Affine Varietäten und Hilbertscher Nullstellensatz

Sei k ein algebraisch abgeschlossener Körper. Wie schon in der Einleitung erwähnt, sind die wichtigsten Objekte, die in der algebraischen Geometrie studiert werden sollen, die folgenden:

Definition 1.3.1. *Sei $S \subset k[x_1, \ldots, x_n]$ (also eine beliebige Menge von Polynomen in n Variablen). Wir nennen*

$$V(S) := \{\lambda \in k^n \mid f(\lambda) = 0 \text{ für alle } f \in S\}$$

die **affine Varietät***, welche durch S beschrieben wird.*

Falls $S = \emptyset$ bekommen wir aus der Definition $V(S) = k^n$. Diese affine Varietät wird in der algebraischen Geometrie mit $\mathbb{A}^n$ bezeichnet. Das Adjektiv *affin* wird eingeführt, um diese Objekte von den *projektiven* Varietäten abzugrenzen, die später eingeführt werden.
Wir wenden uns nun der fundamentalen Frage zu, inwieweit die Menge S durch $V = V(S)$ rekonstruiert werden kann. Sicher haben die Elemente von S nach Definition von $V(S)$ die Eigenschaft:

$$S \subset \{f \in k[x_1, \ldots, x_n] \mid f(\lambda) = 0 \text{ für alle } \lambda \in V\}.$$

Die Menge von Polynomen auf der rechten Seite ergibt auch für eine beliebige Teilmenge $Z \subset \mathbb{A}^n$ statt V Sinn. Wir definieren:

Definition 1.3.2. *Sei $Z \subset \mathbb{A}^n$ eine Teilmenge.*

$$I(Z) = \{f \in k[x_1, \ldots, x_n] \mid f(\lambda) = 0 \text{ für alle } \lambda \in Z\}$$

ist ein Ideal von $k[x_1, \ldots, x_n]$ und heisst das **Verschwindungsideal** *von Z.*

Erinnere (siehe 1.5.1): eine Teilmenge $I \subset R$ eines kommutativen Ringes heisst *Ideal*, wenn 1. I eine additive Untergruppe von R bzgl. der Addition ist, und 2. für alle $r \in R$ und $i \in I$ ist auch $ri \in I$.

Beweis der Idealeingenschaft. Falls $f(\lambda) = 0$ und $g(\lambda) = 0$ für alle $\lambda \in Z$ so gilt auch $(f+g)(\lambda) = f(\lambda) + g(\lambda) = 0$ für alle $\lambda \in Z$; die Menge ist also unter Addition abgeschlossen. Genauso ist $(-f)(\lambda) = -f(\lambda) = 0$ für alle $\lambda \in Z$ und $0(\lambda) = 0$ für alle $\lambda \in Z$. Eigenschaft 1 eines Ideals ist also erfüllt.
Genauso ist für ein Polynom $p \in k[x_1, \ldots, x_n]$ $(pf)(\lambda) = p(\lambda)f(\lambda) = 0$ für alle $\lambda \in Z$. Eigenschaft 2 ist somit auch erfüllt. $\square$

Beispiel 1.3.3. *Sei $Z = \{[\lambda_1, \dots, \lambda_n]\}, \lambda_i \in k$ ein Punkt. Offensichtlich liegen die Funktionen*

$$x_1 - \lambda_1, \dots, x_n - \lambda_n$$

in $I(Z)$. Überlegen Sie sich als Übung, dass tatsächlich sogar $I(Z) = (x_1 - \lambda_1, \dots, x_n - \lambda_n)$ (das von diesen Funktionen erzeugte Ideal) ist. Wir werden dass in 1.5.9 wieder aufgreifen.

Sei R ein kommutativer Ring und $S \subset R$ eine Teilmenge. Wir schreiben (S) für das **von S erzeugte Ideal**. (S) ist die Menge aller Elemente von R, die sich als endliche Summe der Form

$$\alpha_1 s_1 + \dots + \alpha_n s_n$$

schreiben lassen, wobei $\alpha_i \in R$ und $s_i \in S$ für alle i. Es ist klar, dass dies ein Ideal ist. Es ist ausserdem das *kleinste* Ideal von R, welches S enthält. Beachte, dass diese Aussage sinnvoll ist, denn falls I, J zwei Ideale sind, welche S enthalten, dann ist $I \cap J$ wieder ein Ideal, welches S enthält. Falls $S = \{f_1, \dots, f_n\}$ eine endliche Menge ist, dann schreiben wir auch

$$(S) = (f_1, \dots, f_n).$$

Ideale dieser Form heissen **endlich erzeugt**. Im Abschnitt 1.5 werden wir sehen, dass *alle* Ideale im Polynomring $k[x_1, \dots, x_n]$ endlich erzeugt sind.

Proposition 1.3.4. *Die beiden Assoziationen $S \mapsto V(S)$ und $Z \mapsto I(Z)$ erfüllen die folgenden Eigenschaften*

1. *$I(\emptyset) = k[x_1, \dots, x_n]$, $I(\mathbb{A}^n) = (0)$.*
2. *$V(0) = \mathbb{A}^n$, $V(k[x_1, \dots, x_n]) = \emptyset$.*
3. *$S \subset I(V(S))$, $Z \subset V(I(Z))$.*
4. *$V(S) = V((S)) = V(I(V(S)))$, $I(Z) = I(V(I(Z)))$.*
5. *aber i.a. gilt $I \neq I(V(I))$.*

Die (relativ triviale) Beobachtung aus 4. $V(S) = V((S))$ zeigt, dass wir uns nicht weiter einschränkt hätten, wenn wir in der Definition der affinen Varietät gefordert hätten, dass S ein Ideal ist.

Beweis. Die erste Aussage aus 1. ist trivial; die ebenfalls offensichtlich aussehende Aussage $I(\mathbb{A}^n) = (0)$ bedeutet, dass das Nullpolynom das einzige Polynom ist, welches auf allen Punkten des k^n verschwindet. Dies benutzt jedoch, dass k unendlich viele Elemente enthält[2]! Wir verwenden Induktion nach n: Für $n = 1$ folgt die Aussage, da ein Polynom (ungleich 0) in einer Variablen über einem Körper nur endlich viele Nullstellen haben kann. Nimm nun an, dass die Aussage für n richtig ist, betrachte ein Polynom f in $n + 1$ Variablen als Polynom in x_{n+1}:

$$f = \alpha_k (x_{n+1})^k + \dots + \alpha_0$$

wobei $\alpha_i \in k[x_1, \dots, x_n]$. Wiederum ist dieses Polynom für alle eingesetzten Werte von $x_1, \dots, x_n$ Null. Die α_i verschwinden also auf $\mathbb{A}^n$ und sind daher 0 nach Induktionsvoraussetzung.
Die Aussagen 2. und 3. sind trivial.
4. ist eine einfache Übung: Die Inklusion $\subset$ folgt aus 3. Die Inklusion $\supset$: Sei $\lambda \in V(I(V(S)))$, d.h. $f(\lambda) = 0$ für alle $f \in I(V(S))$. Da $S \subset I(V(S))$ gilt dies insbesondere für die Elemente in $f \in S$. D.h. aber $\lambda \in V(S)$. Genauso für die andere Aussage: Die Inklusion $\supset$: Sei $f \in I(V(I(Z)))$, d.h. $f(\lambda) = 0$ für alle $\lambda \in V(I(Z))$. Da $Z \subset V(I(Z))$ gilt dies insbesondere für die Elemente in $\lambda \in Z$. D.h. aber $f \in I(Z)$.
5. Schon für $n = 1$ gilt z.B. $\{[0]\} = V(x) = V(x^2)$. I ist also durch $V(I)$ nicht eindeutig bestimmt. $\square$

Zusammenfassend kann man sagen, dass die beiden Assoziationen eine Bijektion herstellen zwischen Varietäten und Idealen der Form $I(V(I))$ für ein Ideal I. Die Frage bleibt: Welche Ideale sind von dieser Form? Unter welchen Umständen ist $I(V(I)) = I$?
Zunächst beobachten wir, dass falls $f^n \in I(Z)$ auch $f \in I(Z)$ gilt. Diese Eigenschaft eines Ideals ist besonders:

[2]Ein endlicher Körper ist niemals algebraisch abgeschlossen.

Definition 1.3.5. *Ein Ideal I eines kommutativen Ringes R heisst* **Radikalideal***, falls gilt*

$$f^n \in I \Rightarrow f \in I$$

für alle $f \in R$ und $n \in \mathbb{N}$.

Definition/Lemma 1.3.6. *Sei R ein kommutativer Ring und ein I ein Ideal von R. Wir definieren*

$$\sqrt{I} := \{f \in R \mid \exists n \in \mathbb{N} : f^n \in I\}.$$

Dies ist das kleinste Radikalideal, welches I enthält, und heisst das **Radikal** *von I.*

Beweis. Eigenschaft 2. eines Ideals ist sicher erfüllt, denn sei $f \in \sqrt{I}$ und $p \in R$. D.h es existiert ein n mit $f^n \in I$, dann gilt auch $(pf)^n = p^n f^n \in I$, d.h. $pf \in \sqrt{I}$. Eigenschaft 1.: Seien $f, g \in \sqrt{I}$. Sicher existiert dann ein gemeinsames n so, dass $f^n \in I$ und $g^n \in I$. Betrachte

$$(f+g)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} f^i g^{2n-i}.$$

Es ist entweder $i \geq n$ oder $2n - i \geq n$. Daher ist entweder $f^i \in I$ oder $g^{2n-i} \in I$. Insgesamt ist also $(f+g)^{2n} \in I$, d.h. also auch (nach Definition) $(f+g) \in \sqrt{I}$. Dass es sich um das kleinste Radikalideal handelt, welches I enthält, ist klar. □

Unsere obige Diskussion können wir also so zusammenfassen: $\sqrt{I} \subseteq I(V(I))$. Es gilt nun

Satz 1.3.7 (Hilbertscher Nullstellensatz)**.** *Sei k ein algebraisch abgeschlossener Körper und $I \subseteq k[x_1, \dots, x_n]$ ein Ideal. Dann gilt:*

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

Korollar 1.3.8. *Sei k ein algebraisch abgeschlossener Körper. Die Assoziationen $I \mapsto V(I)$, $V \mapsto I(V)$ sind zueinander inverse inklusionsumkehrende Bijektionen zwischen der Menge der affinen Varietäten im $\mathbb{A}^n$ und der Menge der Radikalideale von $k[x_1, \dots, x_n]$.*

Insbesondere wird durch den Hilbertschen Nullstellensatz die in der Einleitung aufgeworfene Frage nach einem algebraischen Kriterium dafür, wann $V(I) = \emptyset$ ist, beantwortet. Nämlich (durch Anwenden von I auf beiden Seiten) genau dann, wenn $\sqrt{I} = I(\emptyset) = k[x_1, \dots, x_n]$ ist. Dies ist genau dann der Fall, wenn $I = k[x_1, \dots, x_n]$. Insbesondere folgt für den Fall endlich vieler Polynome:

Korollar 1.3.9. *Sei k ein algebraisch abgeschlossener Körper. Seien $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. Dann gilt entweder*

1. *Es existieren $g_1, \dots, g_m \in k[x_1, \dots, x_n]$ so, dass*

$$g_1 f_1 + \dots + g_m f_m = 1,$$

   oder

2. *$V(f_1, \dots, f_m) \neq \emptyset$.*

Dies ist das versprochene algebraische Kriterium.
Der Hilbertsche Nullstellensatz ist nicht leicht zu beweisen. Wir werden dies nach einigen Vorbereitungen in Kapitel 3 tun.

1.4 Morphismen von affinen Varietäten

Wir möchten ein Werkzeug haben, um mehrere Varietäten miteinander vergleichen zu können. Z.B. möchten wir Varietäten, die sich nur um eine Koordinatentransformation voneinander unterscheiden, nicht als "verschieden" ansehen. Ähnliche Situationen finden wir in der Mathematik bei der Definition einer Gruppe, eines Ringes, eines Vektorraumes, eines Körpers... Jedesmal haben wir hier den Begriff der *Isomorphie*. Der Schlüssel liegt jedesmal darin, geeignete Abbildungen zwischen den Objekten auszuzeichnen, welche alle zu untersuchenden Strukturen erhalten. Existieren Abbildungen $f : X \to Y$ und $f^{-1} : Y \to X$ zwischen zwei Objekten, so dass f und f^{-1} zu dieser ausgezeichneten Klasse gehören und so dass

$$f \circ f^{-1} = \mathrm{id}_Y \qquad f^{-1} \circ f = \mathrm{id}_X,$$

dann nennen wir f einen *Isomorphismus*, X und Y heissen *isomorph*. Dies definiert auf mathematisch präzise Weise, wann wir zwei Objekte als "verschieden" oder "gleich" ansehen sollen. Die "ausgezeichneten Abbildungen" sind natürlich in den Beispielen oben die Gruppenhomomorphismen (Gruppen), Ringhomomorphismen (Ringe), lineare Abbildungen (Vektorräume) und Körperhomomorphismen.
In der algebraischen Geometrie ist es naheliegend, nur solche Abbildungen $V \to W$ zuzulassen, welche ihrerseits durch Polynome beschrieben werden können.

Definition 1.4.1. *Seien $V \subset \mathbb{A}^n$ und $W \subset \mathbb{A}^m$ affine Varietäten. Eine Abbildung $\varphi : V \to W$ heisst polynomiale Funktion oder* **Morphismus von Varietäten***, falls Polynome $p_1, \dots, p_m \in k[x_1, \dots, x_n]$ existieren, so dass*

$$\varphi(\lambda) = [p_1(\lambda), p_2(\lambda), \dots, p_m(\lambda)]$$

für alle $\lambda \in V$.

Beachte: Die Polynome $p_1, \dots, p_m$ sind nicht notwendigerweise eindeutig bestimmt (wir können beliebige Polynome in $I(V)$ hinzuaddieren ohne φ zu ändern). Eine rein algebraische Beschreibung der Menge der Morphismen $V \to W$ ergibt sich durch Proposition 1.4.4 unten.
Eine Sonderrolle spielen die polynomialen Funktionen nach $k = \mathbb{A}^1$:

Definition/Lemma 1.4.2. *Die Menge der Funktionen $V \to \mathbb{A}^1$, die "Morphismen von Varietäten" sind, also die Menge der polynomialen k-wertigen Funktionen auf V bildet einen kommutativen Ring (sogar eine k-Algebra) bzgl. Addition und Multiplikation von Funktionen. Er wird mit $\mathcal{O}(V)$ bezeichnet.*

Beweis. Die Verifikation der Ringaxiome lassen wir als Übung. □

Es gibt einen offensichtlichen k-Algebrenhomomorphismus:

$$\psi : k[x_1, \dots, x_n] \to \mathcal{O}(V), \tag{2}$$

der ein Polynom f auf die durch es dargestellte polynomiale Funktion $\lambda \mapsto f(\lambda)$ abbildet. ψ ist surjektiv (nach Definition von polynomialer Funktion) und der Kern von ψ ist gerade $I(V)$. Diese Aussage lässt sich nutzen, um den Ring $\mathcal{O}(V)$ als den Quotientenring $k[x_1, \dots, x_n]/I(V)$ zu konstruieren (siehe dazu im nächsten Abschnitt den Homomorphiesatz 1.5.3).

Beispiel 1.4.3. *Z.B. ist $\mathcal{O}(\mathbb{A}^n) = k[x_1, \dots, x_n]$.* Beweis: *Der Kern von ψ ist $I(\mathbb{A}^n)$. Dies ist* (0) *nach Proposition 1.3.4, 1. Der k-Algebrenhomomorphismus oben ist daher ein Isomorphismus.*

Ein erstes Beispiel für eine (recht triviale) Übersetzung von geometrischen Begriffen in algebraische ist die

Proposition 1.4.4. *Seien V, W affine Varietäten. Es gibt eine natürliche Bijektion zwischen der Menge der Morphismen von affinen Varietäten $V \to W$ und der Menge der k-Algebrenhomomorphismen $\mathcal{O}(W) \to \mathcal{O}(V)$.*

Beweis. Sei $\varphi : V \to W$ ein Morphismus von Varietäten. Wir ordnen diesem den folgenden k-Algebrenhomorphismus

$$\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$$

zu. Eine polynomiale Funktion $p : W \to \mathbb{A}^1$ wird auf die Funktion $\Phi(p) := p \circ \varphi$ abgebildet, d.h. auf diejenige Funktion, welche zuerst φ ausführt und dann p. Man überprüft leicht, dass auch $\Phi(p)$ durch Polynome gegeben ist.
Beachten Sie, dass sich die Richtung ändert. Man sagt daher auch, dass $\Phi(p)$ der **Rückzug** der Funktion p entlang φ ist.
Umgekehrt, sei ein k-Algebrenhomomorphismus $\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$ gegeben. Wir können ihn auffassen als Algebrenhomomorphismus (in dem wir mit dem Algebrenhomomorphismus ψ komponieren): $\widetilde{\Phi} = \Phi \circ \psi : k[x_1, \ldots, x_m] \to \mathcal{O}(V)$. Wir definieren nun eine Abbildung $V \to W$ durch

$$\varphi : \lambda \mapsto [\widetilde{\Phi}(x_1)(\lambda), \ldots, \widetilde{\Phi}(x_m)(\lambda)].$$

Man überprüft, dass dies wohldefiniert ist, und dass diese beiden Assoziationen invers zueinander sind. $\square$

Bemerkung: Die Proposition (und der Hilbertsche Nullstellensatz) gibt uns insbesondere eine natürliche Bijektion zwischen den Isomorphieklassen affiner Varietäten und den Isomorphieklassen von k-Algebren der Form $k[x_1, \ldots, x_n]/I$, wobei I ein Radikalideal ist. Diese heissen endlich erzeugte reduzierte k-Algebren (siehe nächster Abschnitt).

Beispiel 1.4.5. *Wir wollen hier den Fall $n = 1$ behandeln und $V(f)$ für ein $f \in k[x]$, $f \neq 0$ untersuchen. Da k algebraisch abgeschlossen ist, können wir*

$$f = \alpha \prod_{i=1}^{m} (x - \alpha_i)^{n_i}$$

mit $\alpha \in k^*$ und $\alpha_i \in k$ (paarweise verschieden) schreiben. Wir haben also

$$V(f) = \{\alpha_1, \ldots, \alpha_m\}$$

und offensichtlich

$$I(V(f)) = (\prod_{i=1}^{m} (x - \alpha_i)) = \sqrt{(f)}$$

Dies ist der Hilbertsche Nullstellensatz in diesem Fall.
Der Ring $k(V)$ aller *Funktionen*

$$V(f) \to k$$

ist isomorph zu k^m, wobei ein Vektor $[\beta_1, \ldots, \beta_n]$ der Funktion:

$$\alpha_i \mapsto \beta_i \text{ für alle } i$$

entsprechen soll. Wir behaupten, dass in diesem Fall die Abbildung (siehe (2) oben)

$$\psi : k[x] \to k(V) = k^m$$

surjektiv ist und daher

$$\mathcal{O}(V) = k(V)$$

ist. Beweis: *Die Basisabbildung $e_j := (0, \ldots, 0, 1, 0 \ldots, 1)$ (wobei die 1 an der j-ten Stelle steht) wird gerade durch das Polynom*

$$f_j = \prod_{i \neq j} \frac{x - \alpha_i}{\alpha_j - \alpha_i}$$

beschrieben.

1.5 Kommutative Ringe

Wir wollen einige elementare Definitionen über kommutative Ringe nachtragen.

Definition 1.5.1. *Sei R ein kommutativer Ring*[3]*. Eine Teilmenge $I \subset R$ heisst* **Ideal***, falls gilt:*

1. *I ist eine Untergruppe der additiven Gruppe von R.*
2. *$ri \in I$ für alle $r \in R$ und $i \in I$.*

Lemma 1.5.2. *Der Kern eines Ringhomorphismus*[4] *ist ein Ideal.*

Beweis. Einfache Übung □

Satz 1.5.3 (Homomorphiesatz)**.** *Sei R ein kommuativer Ring und $I \subset R$ ein Ideal. Es gibt einen Ring R/I und einen surjektiven Homomorphismus $p : R \to R/I$ mit $\ker(p) = I$ und folgender universeller Eigenschaft: Für jeden Ringhomomorphismus $\varphi : R \to S$ so, dass $\varphi(I) = 0$ ist, gibt es einen eindeutigen Ringhomomorphismus $\widetilde{\varphi} : R/I \to S$, so dass*

$$\varphi = \widetilde{\varphi} \circ p.$$

Falls φ surjektiv ist mit $\ker(\varphi) = I$, so ist $\widetilde{\varphi}$ ein Isomorphismus.

Beweisskizze (siehe beliebiges Algebrabuch für Details). Der Ring R/I (Ring der Nebenklassen von I) wird durch die Definition der folgenden Äquivalenzrelation auf R definiert:

$$x \sim y \Leftrightarrow x - y \in I.$$

Dies ist eine Äquivalenzrelation, da I eine additive Untergruppe ist. Die Äquivalenzklasse eines Elementes x bezeichnen wir mit $x + I$. Wir definieren nun auf der Menge der Äquivalenzklassen eine Addition und Multiplikation durch

$$(x + I) + (y + I) := (x + y + I)$$
$$(x + I) \cdot (y + I) := (xy + I)$$

Man muss nachrechnen, dass diese Definitionen nicht von der Wahl der Vertreter x und y abhängen und dass die Ringaxiome erfüllt sind. Als Beipiel zeigen wir hier nur, dass in der Definition der Multiplikation $(xy+I)$ wohldefiniert ist: Falls $x' = x + i$ und $y' = y + j$ zwei andere Vertreter sind, so gilt $x'y' = xy + iy + xj + ij$. Da aber $iy + xj + ij \in I$ ist $xy + I = x'y' + I$. Beachte, hier wurde Eigenschaft 2 eines Ideales verwendet.
Wir können nun einen surjektiven Ringhomomorphismus $p : R \to R/I$ durch $x \mapsto x + I$ definieren. Wir behaupten, dass er die universelle Eigenschaft erfüllt. Falls $\varphi : R \to S$ ein Ringhomomorphismus mit $\varphi(I) = 0$ ist, so können wir $\widetilde{\varphi}(x + I) = \varphi(x)$ definieren. Aus $\varphi(I) = 0$ folgt sofort, dass dies wohldefiniert ist. Die Gleichung $\varphi = \widetilde{\varphi} \circ p$ zwingt uns darüberhinaus $\widetilde{\varphi}$ so zu definieren. Er ist daher eindeutig bestimmt.
Die letzte Aussage ergibt sich daraus, dass $\ker(\widetilde{\varphi}) = p(\ker(\varphi))$ ist. Falls $\ker(\varphi) = I$ ist dies 0. □

Beachte: Die Aussage des Satzes impliziert, dass R/I bis auf Isomorphie eindeutig bestimmt ist. Ein Ring der Form R/I heisst auch **Quotient** oder **homomorphes Bild** von R.

Beispiel 1.5.4. *Der Ringhomomorphismus $\psi : k[x_1, \ldots, x_n] \to \mathcal{O}(V)$, welcher ein Polynom auf die darstellende Funktion abbildet, ist surjektiv und erfüllt $\ker(\psi) = I(V)$. Es gilt daher nach dem Homomorphiesatz*

$$\mathcal{O}(V) \cong k[x_1, \ldots, x_n]/I(V).$$

Proposition 1.5.5. *Betrachte den Ringhomomorphismus $p : R \to R/I$ aus dem Homomorphiesatz. Die Abbildung $J \mapsto p^{-1}(J)$ definiert eine Bijektion zwischen der Menge der Ideale von R/I und der Menge der Ideale $\widetilde{J}$ von R, welche $I \subset \widetilde{J} \subset R$ erfüllen.*

[3] Wir verstehen unter einem Ring einen "Ring mit 1".
[4] Wir fordern, dass ein Ringhomomorphismus 1 auf 1 abbildet.

Beweis. Es ist klar, dass $p^{-1}(J)$ ein Ideal von R ist (dies gilt analog für jeden Ringhomomorphismus). Ausserdem enthält $p^{-1}(J)$ den Kern von p, welcher I ist. $J \mapsto p^{-1}(J)$ ist also eine Abbildung zwischen den angegebenen Mengen. Umgekehrt, sei $\widetilde{J}$ ein Ideal von R, welches I enthält. Wir definieren das Ideal von R/I:

$$\widetilde{J}/I = p(\widetilde{J}) = \{(j+I) \in R/I \mid j \in \widetilde{J}\}.$$

(Beachte, dass die rechte Menge nur sinnvoll definiert ist, da $I \subset \widetilde{J}$.) Man überprüft leicht, dass diese Assoziation zur vorigen invers ist. ☐

Weitere wichtige Eigenschaften von Idealen:

Definition 1.5.6. *Sei R ein kommutativer Ring und $I \subset R$ ein Ideal.*

1. *I heisst* **echtes** *Ideal, falls $I \neq R$ ist.*
2. *Ein echtes Ideal I heisst* **prim**, *falls gilt*
$$pq \in I \Rightarrow p \in I \text{ oder } q \in I.$$
3. *I heisst* **maximal**, *falls es maximal ist bzgl. der Teilordnung auf den echten Idealen, welche durch Inklusion gegeben ist. Mit anderen Worten: I ist echt und falls J ein Ideal ist mit $I \subset J \subsetneq R$, dann gilt $I = J$.*
4. *I heisst* **Radikalideal**, *falls gilt*
$$f^n \in I \Rightarrow f \in I.$$

Es gibt die folgenden Implikationen: I maximal $\Rightarrow$ I prim. I prim $\Rightarrow$ I Radikalideal. Ausserdem ist das triviale Ideal $I = R$ ein Radikalideal aber nicht prim.

Definition 1.5.7. *Sei R ein kommutativer Ring.*

1. *R heisst* **Nullring**, *falls $R = \{0\}$*[5].
2. *R, welcher nicht der Nullring ist, heisst* **nullteilerfrei**, *falls gilt:*
$$pq = 0 \Rightarrow p = 0 \text{ oder } q = 0,$$
für alle $p, q \in R$.
3. *R, welcher nicht der Nullring ist, heisst* **Körper**, *falls jedes von Null verschiedene Element in R multiplikativ invertierbar (d.h. eine Einheit) ist.*
4. *R heisst* **reduziert**, *falls R keine* **nilpotenten** *Elemente enthält, d.h.*
$$f^n = 0 \Rightarrow f = 0,$$
für alle $f \in R$.

Diese Begriffe entsprechen denen der vorigen Definition wie folgt:

Proposition 1.5.8. *Sei R ein kommutativer Ring und I ein Ideal von R. Wir haben*

$$\begin{aligned} I \text{ echt} &\Leftrightarrow R/I \text{ ist nicht der Nullring} && (3)\\ I \text{ prim} &\Leftrightarrow R/I \text{ nullteilerfrei} && (4)\\ I \text{ maximal} &\Leftrightarrow R/I \text{ Körper} && (5)\\ I \text{ Radikalideal} &\Leftrightarrow R/I \text{ reduziert} && (6)\end{aligned}$$

[5] Dies ist gleichbedeutend zur Gleichung $0 = 1$.

Den Beweis lassen wir als Übung. Verwende 1.5.5 für die Entsprechung (5). Beachte: Ein kommutativer Ring R ist ein Körper, genau dann wenn er genau 2 Ideale besitzt (R und (0)). Hieraus ergibt sich auch sofort die oben behauptete Implikation: I maximal $\Rightarrow$ I prim.
Wir werden im Abschnitt 1.7 sehen, was es für eine affine Varietät geometrisch bedeutet, dass $\mathcal{O}(V)$ eine dieser Eigenschaften besitzt.

Beispiel 1.5.9. *Sei $Z = \{[\lambda_1, \ldots, \lambda_n]\}$ ein Punkt. Wir sind noch die Begründung schuldig, dass*

$$I(Z) = (x_1 - \lambda_1, \ldots, x_n - \lambda_n).$$

Es gilt aber $(x_1 - \lambda_1, \ldots, x_n - \lambda_n) \subset I(Z)$, daher ist $I(Z)$ wegen Proposition 1.5.5 gleich $p^{-1}J$ für ein Ideal von $k[x_1, \ldots, x_n]/(x_1 - \lambda_1, \ldots, x_n - \lambda_n)$. Nun ist aber klar, dass

$$k[x_1, \ldots, x_n]/(x_1 - \lambda_1, \ldots, x_n - \lambda_n) = k,$$

denn alle x_i werden zu Konstanten gemacht! Daher ist $I(Z) = p^{-1}(0) = (x_1 - \lambda_1, \ldots, x_n - \lambda_n)$. Q.E.D.
Der Hilbertsche Nullstellensatz impliziert, dass umgekehrt jedes maximale Ideal von dieser Form ist. Wir werden darauf noch zurückkommen.

Definition 1.5.10. *Sei R ein kommutativer Ring und k ein Körper.*

1. *Falls ein Ringhomomorphismus $\iota : k \to R$ gegeben ist, so heisst (R, ι) eine k-**Algebra**.*
2. *Ein k-Algebrenhomomorphismus von einer k-Algebra (R, ι) in eine k-Algebra (S, ι') ist ein Ringhomomorphismus $\varphi : R \to S$ so, dass $\iota' = \varphi \circ \iota$.*
3. *Eine k-Algebra (R, ι) heisst **endlich erzeugt**, falls es $\xi_1, \ldots, \xi_n$ in R gibt, so dass jedes $x \in R$ eine polynomiale Darstellung der Form*

   $$x = \sum_{i=1}^{N} \iota(\alpha_i)(\xi_1)^{m_{i,1}} \cdots (\xi_n)^{m_{i,n}}$$

   mit $\alpha_i \in k$ und $m_{i,j} \in \mathbb{N}_0$ besitzt.

Üblicherweise lassen wir ι in der Bezeichnung einer k-Algebra weg, wenn klar ist, was ι sein soll. Dies ist insbesondere für die Polynomringe $k[x_1, \ldots, x_n]$ und ihre Quotienten der Fall. Wir identifizieren k dann mit seinem Bild in $k[x_1, \ldots, x_n]$ (konstante Polynome).
Man überlege sich, dass eine k-Algebra R genau dann endlich erzeugt ist, wenn es $n \in \mathbb{N}$ und einen surjektiven k-Algebrenhomomorphismus $k[x_1, \ldots, x_n] \to R$ gibt.

1.6 Noethersche Ringe

Es zeigt sich, dass in den Ringen der algebraischen Geometrie, also Ringen der Form $\mathcal{O}(V)$ *alle* Ideale endlich erzeugt sind. Dies bedeutet insbesondere, dass alle affinen Varietäten durch *endlich viele* Polynome beschrieben werden können. Diese Eigenschaft ist sehr wichtig, darum definieren wir:

Definition 1.6.1. *Ein kommutativer Ring R heisst **noethersch**, wenn jedes Ideal $I \subset R$ endlich erzeugt ist.*

Es ist manchmal praktisch, diese Bedingung anders zu formulieren:

Proposition 1.6.2. *Ein kommutativer Ring R ist genau dann noethersch, wenn jede unendliche aufsteigende Kette von Idealen von R*

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

stationär wird, d. h. es gibt ein $n \in N$ so, dass

$$I_n = I_{n+1} = I_{n+2} = \ldots.$$

Beweis. Sei R noethersch und

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

eine unendliche aufsteigende Kette von Idealen. Betrachte die Vereinigung:

$$I := \bigcup_i I_i.$$

Dies ist wieder ein Ideal. Da R noethersch ist, gilt $I = (f_1, \dots, f_n)$. Nun gilt nach Definition von I, dass die f_j jeweils in einem der Ideale I_i liegen. Daher gibt es ein n, so dass alle $f_j \in I_n$. Es gilt also $I = I_n = I_{n+1} = I_{n+2} = \dots$.
Umgekehrt, sei R ein kommutativer Ring, welcher die Idealkettenbedingung erfüllt. Beweis der Noethereigenschaft durch Widerspruch. Sei I ein Ideal, welches nicht endlich erzeugt werden kann. Wir konstruieren induktiv eine Kette von endlich erzeugten Idealen $I_i \subset I$: Wir setzen $I_1 := 0$. Sei nun I_n konstruiert. Da I_n endlich erzeugt ist, gilt $I_n \subsetneq I$. Es gibt also ein $x \in I \setminus I_n$. Definiere $I_{n+1} := (I_n, x)$. Nach Konstruktion wird dies eine *strikt* aufsteigende Kette von Idealen. Widerspruch. □

Die einfachsten noetherschen Ringe sind die **Hauptidealringe**, wie z.B. $\mathbb{Z}$ oder $k[x]$, in denen jedes Ideal von nur einem Element erzeugt wird. Schon in $k[x, y]$ gibt es jedoch keine obere Schranke für die Anzahl der nötigen Erzeuger eines Ideals mehr (Übung). Aber wie wir werden gleich sehen werden, ist jedes Ideal zumindest endlich erzeugt.
Es gilt zunächst der

Satz 1.6.3 (Hilbertscher Basissatz)**.** *Sei R ein kommutativer noetherscher Ring. Dann ist auch $R[x]$ noethersch.*

Beweis. Es ist lehrreich, sich an den Fall $R = k$ zu erinnern. In diesem Fall ist sogar jedes Ideal von $R[x]$ von nur einem Element erzeugt. *Beweis:* Sei $I \subset k[x]$ ein Ideal und $0 \neq f \in I$ ein Element von minimalem Grad. Sei g nun ein beliebiges Element von I. Durch Polynomdivision können wir schreiben $g = pf + q$ wobei $q = 0$ oder Grad $q <$ Grad f. Da f minimalen Grad in I hatte, und $q = g - pf \in I$, folgt $q = 0$, also $g \in (f)$.
Warum funktioniert dieser Beweis nicht für $R[x]$? Das Problem ist, dass die Polynomdivision nur noch funktioniert, falls der führende Koeffizient von f eine Einheit ist! Die Idee des Beweises ist nun, die führenden Koeffizienten der Polynome in I zu betrachten und auszunutzen, dass sie nach Voraussetzung in einem noetherschen Ring liegen. Definiere

$$J_i = \{a_i \in R \mid \text{Es gibt } f = a_i x^i + a_{i-1} x^{i-1} + \dots + a_0 \in I\}.$$

($a_i = 0$ ist erlaubt.) Dies ist offensichtlich ein Ideal von R. Es gilt ausserdem $J_i \subset J_{i+1}$, denn sei $a_i \in J_i$, d.h. es gibt $f = a_i x^i + \dots + a_0 \in I$. Dann ist $fx = a_i x^{i+1} + \dots + a_0 x \in I$ und daher $a_i \in J_{i+1}$. Nach der Proposition gibt es also ein n mit

$$J_n = J_{n+1} = J_{n+2} = \dots$$

Ausserdem ist jedes J_i endlich erzeugt:

$$J_i = (a_{1,i}, \dots, a_{r_i,i}).$$

Nach Definition ist jedes der $a_{j,i}$ der führende Koeffizient eines Polynoms $f_{j,i} = a_{j,i} x^i + \cdots$.
Behauptung:

$$I = (f_{1,0}, \dots, f_{r_0,0}, \dots, f_{1,n}, \dots, f_{r_n,n}).$$

Beweis der Behauptung: Sei $\widetilde{I}$ das Ideal auf der rechten Seite. Sei f ein Element in $I \setminus \widetilde{I}$ von minimalem Grad. Schreibe $f = a_i x^i + \dots + a_0$ mit $a_i \neq 0$.
Falls $i \leq n$, dann gilt $a_i = \alpha_1 a_{1,i} + \dots + \alpha_{r_i} a_{r_i,i}$ für gewisse $\alpha_j \in R$ und daher hat

$$f - \alpha_1 f_{1,i} - \dots - \alpha_{r_i} f_{r_i,i} \in I \setminus \widetilde{I}$$

kleineren Grad als f. Widerspruch.
Falls $i > n$, dann gilt $a_i = \alpha_1 a_{1,n} + \dots + \alpha_{r_n} a_{r_n,n}$ für gewisse $\alpha_j \in R$ und daher hat

$$f - \alpha_1 x^{i-n} f_{1,n} - \dots - \alpha_{r_n} x^{i-n} f_{r_n,n} \in I \setminus \widetilde{I}$$

kleineren Grad als f. Widerspruch. □

Lemma 1.6.4. *Falls R noethersch ist, so ist auch R/I noethersch für alle Ideale I von R.*

Beweis. Dies folgt sofort aus der Umformulierung in Proposition 1.6.2 und Proposition 1.5.5. $\square$

Korollar 1.6.5. *Alle Ringe der Form $k[x_1, \dots, x_n]/I$ sind noethersch. Insbesondere sind die Ringe $\mathcal{O}(V)$, wobei V eine affine Varietät ist, noethersch.*

Beweis. Induktion über n unter Verwendung von Satz 1.6.3 beweist, dass $k[x_1, \dots, x_n]$ noethersch ist. Lemma 1.6.4 zeigt dann das gewünschte. $\square$

1.7 Zariski-Topologie

In der Analysis ist es sehr praktisch, von stetigen Funktionen sprechen zu können und diese auf einfach struktuierte offene Teilmengen, wie Kreisscheiben, einschränken zu können. Wir möchten gerne die sich daraus ergebende Begrifflichkeit in die algebraische Geometrie übernehmen. Das Problem ist, dass wir mit rein algebraischen Begriffen auskommen müssen. Wie haben nicht, so wie etwa in der Analysis, eine Abstandsfunktion auf den Werten von k zur Verfügung. Wir können aber folgende Beobachtung machen: In jeder sinnvollen Definition einer "Topologie" auf dem Raum $\mathbb{A}^n$ sollten affine Varietäten *abgeschlossen* sein und also ihre Komplemente *offen*. Es zeigt sich, dass allein dadurch, dass wir *ausschliesslich* diese Mengen als offen bzw. abgeschlossen bezeichnen, bereits eine sinnvolle Theorie ergibt. Dafür müssen wir uns an die abstrakte Definition einer Topologie erinnern:

Definition 1.7.1. *Sei M eine Menge. Eine Menge $\mathcal{T}$ von Teilmengen von M (die offen heissen sollen) heisst Topologie, falls*

1. *$M \in \mathcal{T}$ und $\emptyset \in \mathcal{T}$.*
2. *Falls $U, V \in \mathcal{T}$, dann ist auch $U \cap V \in \mathcal{T}$.*
3. *Falls $\{U_i\}_{i \in I}$ eine Familie von Mengen $U_i \in \mathcal{T}$ ist, so ist auch*
$$\bigcup_{i \in I} U_i \in \mathcal{T}.$$

Definition/Proposition 1.7.2. *Wir definieren nun* **Zariski-Topologie** *$\mathcal{T}^{Zar}$ auf $\mathbb{A}^n$, indem die Komplemente der affinen Varietäten $V(S)$ zu offenen Mengen erklärt werden. Also: $U \in \mathcal{T}^{Zar}$ genau dann, wenn es ein Ideal $I \subset k[x_1, \dots, x_n]$ so gibt, dass $U = \mathbb{A}^n \setminus V(I)$. Dies definiert eine Topologie.*

Beweis. Wir müssen nachrechnen, dass dies die Axiome einer Topologie erfüllt. Dies folgt aus den folgenden einfachen Relationen

$$V(I_1) \cap V(I_2) = V(I_1 + I_2), \tag{7}$$
$$V(I_1) \cup V(I_2) = V(I_1 \cap I_2). \tag{8}$$

Die Gleichung (7) verallgemeinert sich auf unendliche Schnitte:

$$\bigcap_{i \in I} V(I_i) = V((I_i)_{i \in I}).$$

Hierbei ist $(I_i)_{i \in I}$ das Ideal, welches von allen I_i erzeugt wird. Achtung: Gleichung (8) lässt sich *nicht* auf unendliche Vereinigungen verallgemeinern! $\square$

Genauso definiert dies durch Einschränkung eine Topologie auf allen affinen Varietäten $V(I)$.

1.7.3. Die abgeschlossenen Mengen $W \subset V(I)$ sind gerade die affinen Varietäten, die sich als $V(J)$ schreiben lassen, wobei J ein Ideal von $k[x_1, \dots, x_n]$ ist mit $I \subset J$. Diese entsprechen nach 1.5.5 den Idealen von $k[x_1, \dots, x_n]/I \cong \mathcal{O}(V)$. Wir benutzen daher auch die Notation $V(f_1, \dots, f_m) \subset V(I)$ für ein Ideal $(f_1, \dots, f_m)$ von $\mathcal{O}(V)$ mit $f_i \in \mathcal{O}(V)$. Die Definition

$$V(f_1, \dots, f_m) = \{\lambda \in V \mid f_1(\lambda) = \dots = f_m(\lambda) = 0\}$$

bleibt ebenfalls richtig.

Die erste Beobachtung, die wir machen können, ist:

Proposition 1.7.4. *Ein Morphismus von affinen Varietäten ist stetig bzgl. der Zariski-Topologie.*

Beweis. Erinnere, dass Stetigkeit nach Definition heisst, dass Urbilder von abgeschlossenen Mengen abgeschlossen sind. Sei $f : V \to W$ ein Morphismus von Varietäten.
Sei $Z \subset W$ eine abgeschlossene Menge. Wir haben gesehen (1.7.3), dass dann $Z = V(f_1, \dots, f_m)$ für gewisse $f_1, \dots, f_m \in \mathcal{O}(W)$. Es gilt dann

$$\varphi^{-1} V(f_1, \dots, f_m) = V(f_1 \circ \varphi, \dots, f_m \circ \varphi).$$

Die $f_j \circ \varphi$ sind gerade die Rückzüge der f_j unter φ. Sie sind als Komposition polynomialer Funktionen wieder polynomial, und daher ist $V(f_1 \circ \varphi, \dots, f_m \circ \varphi)$ eine affine Varietät. $\square$

Beispiel 1.7.5. *Umgekehrt kann man mit der Information, dass eine gegebene Funktion stetig ist bzgl. der Zariski-Topologie nicht besonders viel anfangen. Man überlege sich z.B., dass* jede *bijektive Funktion $\mathbb{A}^1 \to \mathbb{A}^1$ stetig ist.*

Die Zariski-Topologie ist dennoch sehr verschieden von der reellen Topologie, die uns aus der Analysis vertraut ist. Z.B. sind Varietäten im allgemeinen nicht Hausdorffsch, d.h. zu zwei verschiedenen Punkten p_1, p_2 finden wir keine offenen Umgebungen $U_1 \ni p_1$, $U_2 \ni p_2$, mit $U_1 \cap U_2 = \emptyset$. Dies bringt jedoch auch Vorteile. Zum Beispiel ist die folgende Definition hier sinnvoll:

Definition 1.7.6. *Eine nicht-leere abgeschlossene Menge Z eines topologischen Raumes heisst* **irreduzibel***, wenn aus $Z = Z_1 \cup Z_2$ mit Z_1, Z_2 abgeschlossen, folgt, dass $Z = Z_1$ oder $Z = Z_2$.*

Definition 1.7.7. *Ein topologischer Raum heisst* **noethersch***, falls jede absteigende Kette abgeschlossener Teilmengen*

$$Z_1 \supset Z_2 \supset Z_3 \supset Z_4 \supset \dots$$

stationär wird, d.h. es gibt $n \in \mathbb{N}$ so, dass $Z_n = Z_{n+1} = Z_{n+2} = \dots$.

Diese beiden Begriffe sind für die reelle Topologie unsinnig: Die einzigen irreduziblen Mengen sind die Punkte, und natürlich gibt es Ketten abgeschlossener Teilmengen, die nicht stationär werden. Aber in der Zariski-Topologie sind diese Begriffe sinnvoll:

Proposition 1.7.8. *Eine affine Varietät V, versehen mit der Zariski-Topologie, ist ein noetherscher topologischer Raum. Sie ist irreduzibel, genau dann wenn $I(V)$ prim ist.*

Beweis. Der erste Teil folgt durch Anwenden von I (Verschwindungsideal) sofort aus Proposition 1.6.2 und Korollar 1.6.5.
$I(V)$ prim $\Rightarrow$ V irreduzibel: Falls $V = V_1 \cup V_2$ ist wobei V_j affine Varietäten sind, so folgt $I(V) = I(V_1) \cap I(V_2)$. Falls $I(V_1) \not\subset I(V_2)$, dann gibt es f, welches in $I(V_1)$, aber nicht in $I(V)$ liegt. Genauso, falls $I(V_2) \not\subset I(V_1)$ gibt es g welches in $I(V_2)$, aber nicht in $I(V)$ liegt. fg liegt aber in $I(V_1)$ und $I(V_2)$, d.h. $fg \in I(V)$. Falls I prim ist, kann dies nicht sein, es gilt daher $I(V_1) \subset I(V_2)$ oder umgekehrt. Daher gilt $V_1 \subset V_2$ oder umgekehrt. V ist also irreduzibel.
V irreduzibel $\Rightarrow$ $I(V)$ prim: Sei $fg \in I(V)$, dann ist $V = (V \cap V(f)) \cup (V \cap V(g))$. Wenn V irreduzibel ist folgt entweder $(V \cap V(f)) = V$, d.h. $f \in I(V)$ oder $(V \cap V(g)) = V$, d.h. $g \in I(V)$. D.h. $I(V)$ ist prim. $\square$

Wir können nun die rein topologische Sprache verwenden, um etwas über die Relation von beliebigen echten Radikalidealen und Primidealen auszusagen:

Proposition 1.7.9. *In jedem noetherschen topologischen Raum ist jede nicht-leere abgeschlossene Teilmenge Z eine Vereinigung von endlich vielen irreduziblen abgeschlossenen Teilmengen:*

$$Z = Z_1 \cup Z_2 \cup \dots \cup Z_m.$$

Dabei können wir annehmen, dass $Z_i \not\subset Z_j$ für $i \neq j$. Die Z_i sind dann (bis auf Umnummerierung) eindeutig bestimmt und heissen **irreduzible Komponenten** *von Z.*

Beweis. Sei M die Menge der nicht-leeren abgeschlossenen Teilmengen, welche nicht als Vereinigung von irreduziblen abgeschlossenen Teilmengen geschrieben werden kann. Dann muss M ein minimales Element enthalten, da der Raum noethersch ist, sagen wir Y. Dann ist Y nicht irreduzibel (sonst wäre es die Vereinigung von *einer* irreduziblen abgeschlossenen Menge). Daher gibt es also Y_1, Y_2 abgeschlossen mit $Y = Y_1 \cup Y_2$ und $Y_1 \neq Y$ und $Y_2 \neq Y$. Wegen der Minmalität von Y in M haben nun aber Y_1 und Y_2 Zerlegungen in irreduzible abgeschlossene Teilmengen. Dann hat aber auch Y so eine Zerlegung. Widerspruch! Daher muss M die leere Menge sein und die Existenz der Zerlegung ist bewiesen. Nehmen wir nun an die Zerlegung erfüllt die Zusatzbedingung $Z_i \not\subset Z_j$ für $i \neq j$. (Dies können wir immer erreichen, indem wir in einer gegebenen Zerlegung Elemente weglassen). Sei

$$Z = Z_1' \cup Z_2' \cup \cdots \cup Z_k'$$

eine zweite solche Zerlegung. Dann folgt durch Schneiden der ersten Zerlegung mit Z_1':

$$Z_1' = (Z_1 \cap Z_1') \cup \cdots \cup (Z_m \cap Z_1')$$

Nun ist aber Z_1' irreduzibel, daher $Z_1' \subset Z_i$ für ein i. Durch Umnummerieren können wir annehmen $Z_1' \subset Z_1$. Umgekehrt folgt $Z_1 \subset Z_j'$ für irgendein j, also

$$Z_1' \subset Z_1 \subset Z_j'.$$

Wegen der Zusatzbedingung folgt $j = 1$, also $Z_1 = Z_1'$. Genauso macht man weiter für Z_2', Z_3' etc. □

Beispiel 1.7.10. *Wir wollen die Varietät $V(x^2 + y^2 - z^2, x)$ in irreduzible Komponenten zerlegen. Zunächst gilt:*

$$(x^2 + y^2 - z^2, x) = ((y + z)(y - z), x) = (y + z, x) \cap (y - z, x).$$

Daher ist

$$V(x^2 + y^2 - z^2, x) = V(y + z, x) \cup V(y - z, x). \tag{9}$$

Die beiden Varietäten auf der rechten Seite sind Geraden, die verschieden sind. Ausserdem ist $k[x, y, z]/(y + z, x) \cong k[y]$, das Ideal $(y + z, x)$ ist also prim (da $k[y]$ nullteilerfrei ist). Genauso ist $(y - z, x)$ prim. Daraus schliessen wir, dass die Zerlegung (9) die Zerlegung in irreduzible Komponenten ist.

Durch Übersetzung mittels des Hilbertschen Nullstellensatzes folgt für ein echtes *Radikal*ideal $I \subset k[x_1, \ldots, x_n]$, dass endlich viele Primideale P_i existieren, so dass

$$I = P_1 \cap P_2 \cap \cdots \cap P_k;$$

eine Aussage, die keineswegs offensichtlich ist.
Wir können den Hilbertschen Nullstellensatz dahingehend verfeinern, dass die Abbildungen $I \mapsto V(I)$ und $V \mapsto I(V)$ Bijektionen der folgenden Mengen induzieren:

affine Varietäten	reduzierte Ideale
irreduzible affine Varietäten	Primideale
Punkte	maximale Ideale

Ein Begriff, der sowohl für die Zariski-Topologie, als auch für die reelle Topologie sinnvoll ist, ist der der Kompaktheit. In Abwesenheit der Hausdorffbedingung ist die Kompaktheit schwächer, deshalb wird hier üblicherweise der Begriff "quasi-kompakt" verwendet:

Definition 1.7.11. *Ein topologischer Raum X heisst* **quasi-kompakt***, falls für jede Überdeckung:*

$$X = \bigcup_{i \in I} U_i$$

wobei $U_i \subset X$ offen, eine endliche Teilüberdeckung

$$X = U_{i_1} \cup \cdots \cup U_{i_k}$$

($i_j \in I$) ausgewählt werden kann.

Proposition 1.7.12. *Ein noetherscher topologischer Raum ist quasi-kompakt.*

Beweis. Übung! □

Nun zurück zur algebraischen Geometrie:

Definition/Proposition 1.7.13. *Sei V eine affine Varietät und $f \in \mathcal{O}(V)$. Offene Mengen der Form*

$$U_f = V \setminus V(f)$$

heissen **standard-offen**. *Jede beliebige offene Menge ist eine Vereinigung von endlich vielen standard-offenen Mengen.*

Beweis. Eine beliebige offene Menge ist von der Form

$$V \setminus V(f_1, \ldots, f_n)$$

für gewisse $f_i \in \mathcal{O}(V)$, da $\mathcal{O}(V)$ noethersch ist. Nun gilt offenbar

$$V \setminus V(f_1, \ldots, f_n) = \bigcup_i (V \setminus V(f_i)).$$

Alternativer Beweis: Es gilt offenbar

$$V \setminus V(I) = \bigcup_{f \in I} (V \setminus V(f)),$$

wähle nun eine endliche Teilüberdeckung aus. □

In vielen Rechnungen kann man sich auf standard-offene Umgebungen zurückziehen. Diese sind besonders einfach. Wir werden in einem noch zu präzisierenden Sinn feststellen, dass sie selber affine Varietäten sind.

1.8 Projektive Varietäten

Wir haben gesehen, dass affine Varietäten einfacher strukturiert sind, wenn wir über einem algebraisch abgeschlossenen Körper k arbeiten. Dennoch bleiben einige Unregelmässigkeiten, wenn wir mit affinen Varietäten arbeiten.

Beispiel 1.8.1. *Zwei* verschiedene *Geraden*

$$V(a_1x + a_2y + a_3) \quad V(b_1x + b_2y + b_3)$$

(hier $[a_1, a_2] \neq [0, 0]$ und $[b_1, b_2] \neq [0, 0]$) schneiden sich immer in einem Punkt, ausser im Falle, dass sie parallel sind, also wenn

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = 0.$$

In diesem Fall gibt es keinen Schnittpunkt. Im reellen *Bild ergibt sich anschaulich für ein sich bewegendes Geradenpaar mit*

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \to 0,$$

dass der Schnittpunkt im Unendlichen *verschwindet.*

Beispiel 1.8.2. *Die Varietät $V_4 = V(x^2 - y^2 - 1)$ aus der Einführung (Hyperbel) schneidet jede Gerade durch den Ursprung in 2 Punkten, ausser die beiden Geraden $V(x - y)$ und $V(x + y)$, welche gerade den beiden Asymptoten der Hyperbel entsprechen. Auch hier liegt der zu erwartende Schnittpunkt* “im Unendlichen”.

Es gibt nun eine fundamentale Konstruktion, um diese *fehlenden Punkte* ins Bild zurückzuholen. Wir betten die Ebene $\mathbb{A}^2$ in den $\mathbb{A}^3$ ein, indem wir die z-Koordinate auf 1 setzen:

$$\begin{array}{ccc} \mathbb{A}^2 & \hookrightarrow & \mathbb{A}^3 \\ [x,y] & \mapsto & [x,y,1] \end{array}$$

Wir bezeichnen das Bild dieser Abbildung mit E.
Eine affine Varietät V (zum Beispiel eine der beiden Geraden aus Beispiel 1.8.1), die wir uns als Teilmenge von E eingebettet denken, kann man nun zu einer Varietät im $\mathbb{A}^3$ erweitern, indem man zu jedem Punkt $[x,y,1] \in E$ mit $[x,y] \in V$ die Verbindungsgerade dieses Punktes mit dem Nullpunkt $[0,0,0]$ hinzunimmt. Alle diese Verbindungsgeraden zusammengenommen ergeben ein kegelartiges Gebilde, das so aussieht, als würden wir die Varietät V aus dem Nullpunkt auf die Ebene E *projizieren*.
Starten wir mit den beiden Geraden aus Beispiel 1.8.1, so ergeben sich auf diese Weise Ebenen im Raum, bei denen jedoch die Geraden fehlen, die in der Ebene $[x,y,0]$ liegen (denn diese schneiden E nicht). Waren die ursprünglichen Geraden parallel, so schneiden sich die zugehörigen Ebenen gerade in der Ebene $[x,y,0]$ also in zusätzlichen Punkten "im Unendlichen", die im affinen Bild fehlen.
Dies ist das allgemeine Bild. Durch obige Konstruktion wird aus einer Varietät $V \subsetneq E$ ein kegelartiges Gebilde, bei dem einzelne Geraden, nämlich diejenigen in der Ebene $[x,y,0]$ fehlen. Fügen wir sie hinzu (durch Bildung des topologischen Abschlusses), ergibt sich eine affine Varietät P im $\mathbb{A}^3$, die die Eigenschaft hat, dass mit jedem Punkt auch die gesamte Verbindungsgerade mit dem Ursprung in P liegt.
Wir möchten dies nun mathematisch präzisieren.
Dazu müssen wir untersuchen, was es heisst für eine Varietät im $\mathbb{A}^3$ oder allgemeiner im $\mathbb{A}^{n+1}$, dass sie "mit jedem Punkt auch die gesamte Verbindungsgerade mit dem Ursprung" enthält. Dazu müssen wir etwas ausholen:

Definition 1.8.3. *Ein kommutativer Ring R, zusammen mit einer Zerlegung*

$$R = \bigoplus_{i \in \mathbb{Z}} R_i$$

als abelsche Gruppen heisst **graduierter Ring***, falls gilt*

$$R_i \cdot R_j \subset R_{i+j}.$$

Genauso für eine k-Algebra (R,ι). Hierbei wird zusätzlich gefordert, dass $\iota(k) \subset R_0$, die R_i sind daher k-Vektorräume.

Zunächst beobachten wir, dass der Polynomring eine **graduierte k-Algebra** ist:

$$k[x_1,\ldots,x_n] = \bigoplus_i (k[x_1,\ldots,x_n])_i. \tag{10}$$

Hierbei ist $(k[x_1,\ldots,x_n])_i$ die Menge der Polynome in denen jedes vorkommende Monom den genauen Grad i hat. Die Gleichung (10) bedeutet, dass sich jedes Polynom auf eindeutige Weise in eine endliche Summe von Bestandteilen verschiedener Grade zerlegt. Die Polynome in den k-Vektorräumen $(k[x_1,\ldots,x_n])_i$, d.h. solche, in denen jedes vorkommende Monom denselben Grad i hat, heissen **homogen**. Allgemeiner heissen in einem beliebigen graduierten Ring die Elemente der R_i homogen.
Ein homogenes Polynom f hat die Eigenschaft, dass $V(f)$ kegelartig ist, d.h. mit jedem Punkt auch alle Vielfachen enthält. Dies folgt aus der Gleichung

$$f(\alpha\lambda) = \alpha^{\deg(f)} f(\lambda),$$

die für ein homogenes Polynom gilt. Daraus folgt für $\alpha \in k, \alpha \neq 0$ die Äquivalenz

$$f(\alpha\lambda) = 0 \Leftrightarrow f(\lambda) = 0.$$

In gewisser Weise gilt auch die Umkehrung, wie wir sehen werden. Um allgemeine Varietäten, also solche, die durch mehrere Polynome beschrieben werden, behanden zu können, benötigen wir den Begriff des homogenen Ideals, den wir für beliebige graduierte Ringe einführen:

Definition/Proposition 1.8.4. *Sei $R = \bigoplus_i R_i$ ein graduierter noetherscher Ring. Ein Ideal I von R heisst* **homogen***, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

1. *$I = \bigoplus_i (I \cap R_i)$,*

2. *I wird durch homogene Elemente erzeugt.*

Falls I ein homogenes Ideal ist, dann definiert

$$(R/I)_i := R_i/(I \cap R_i) \tag{11}$$

eine Graduierung auf R/I.

Beweis. 1. $\Rightarrow$ 2.: Falls 1. erfüllt ist und $I = (f_1, \ldots, f_n)$, dann gilt, dass jedes $f_j = \sum_i f_{j,i}$ für $f_{j,i} \in I \cap R_i$ von denen nur endlich viele von 0 verschieden sind. Die $f_{j,i}$ erzeugen also auch I und sind homogen.
2. $\Rightarrow$ 1.: Falls 1. für zwei Ideale I und J gilt, so gilt es offensichtlich auch für die Summe $I + J$. Daher genügt es, 1. für ein Ideal der Form (f) zu zeigen, wobei f homogen vom Grad d ist (d.h. in R_d liegt). Es gilt aber

$$(f) = f \cdot \bigoplus_i R_i = \bigoplus_i (f \cdot R_i),$$

und da f homogen ist, gilt $f \cdot R_i = (f) \cap R_{i+d}$.
Die Aussage, dass (11) eine Graduierung definiert, folgt sofort aus 1. □

Proposition 1.8.5. *Eine Varietät $V \subseteq \mathbb{A}^{n+1}$ erfüllt die Eigenschaft:*

(*) V enthält mit jedem Punkt auch die gesamte Verbindungsgerade mit dem Ursprung[6]

genau dann, wenn $I(V)$ homogen ist.

Beweis. Wir zeigen zunächst: Falls $I(V)$ homogen ist, so erfüllt die Varietät die Eigenschaft (*). Seien $f_1, \ldots, f_n$ die homogenen Erzeuger von $I = I(V)$ (da $k[X_0, \ldots, X_n]$ noethersch ist, reichen endlich viele). Dann ist $V = V(I) = V(f_1) \cap \cdots \cap V(f_n)$. Es genügt daher die Behauptung (*) für jedes der $V(f_i)$ zu beweisen. Dies haben wir schon gesehen: Ein homogenes Polynom f vom Grad i erfüllt die Eigenschaft $f(\alpha\lambda) = \alpha^i f(\lambda)$. Daher: Falls $V(f)$ einen Punkt enthält, enthält es auch alle Vielfachen dieses Punktes.
Den Beweis, dass die Eigenschaft (*) impliziert, dass $I(V)$ homogen ist, verschieben wir auf das Ende des Abschnittes (siehe 1.8.15). □

Lemma 1.8.6. *Summe, Produkt und Schnitt von homogenen Idealen sind homogen. Das Radikal eines homogenen Ideals ist homogen.*

Beweis. Übung! □

Definition 1.8.7. *Die Menge der Geraden durch den Ursprung im $\mathbb{A}^{n+1}$ heisst n-dimensionaler* **projektiver Raum** *$\mathbb{P}^n$. Um einen Punkt $P \in \mathbb{P}^n$ im projektiven Raum anzugeben, reicht es, einen Punkt auf der entsprechenden Geraden P zu nennen, welcher nicht 0 ist:*

$$[\lambda_0, \ldots, \lambda_n] \in P \subset \mathbb{A}^{n+1}.$$

Diese heissen die **homogenen Koordinaten** *von P und sind nur bis auf simultane Multiplikation mit einer Konstanten in k^* bestimmt.*
Für jedes homogene Ideal $I \subset k[X_0, \ldots, X_n]$, bezeichnen wir mit $PV(I) \subset \mathbb{P}^n$ die Menge der *Geraden, welche in $V(I) \subset \mathbb{A}^{n+1}$ liegen. Eine Menge der Form $PV(I) \subset \mathbb{P}^n$ heisst* **projektive Varietät***.*

[6] mit anderen Worten: V ist kegelartig

$\mathbb{P}^n$ kann auch als der Quotient von $\mathbb{A}^{n+1} \setminus \{[0, \ldots, 0]\}$ bzgl. der Äquivalenzrelation

$$[\lambda_0, \ldots, \lambda_n] \sim [\lambda'_0, \ldots, \lambda'_n] \Leftrightarrow \exists \alpha \in k^* : \lambda'_i = \alpha\lambda_i \text{ für alle } i$$

aufgefasst werden.
Eine andere Definition einer projektiven Varietät P wäre die folgende gewesen: Sei $I \subseteq k[X_0, \ldots, X_n]$ ein Radikalideal, so dass die affine Varietät $V' = V(I) \subset \mathbb{A}^{n+1}$ die Eigenschaft (*) aus der Proposition 1.8.5 hat (d.h. eine die kegelartig ist) und definiere $P \subset \mathbb{P}^n$ als die Menge der Geraden in V'. Aber Proposition 1.8.5 sagt uns, dass dann $I = I(V)$ homogen ist und natürlich ist dann $P = PV(I)$. Insofern ist diese Definition nicht allgemeiner, als die, die wir gegeben haben. Hier wird allerdings die Beweisrichtung von 1.8.5 verwendet, die wir noch zeigen müssen (siehe 1.8.15 weiter unten).

1.8.8. Wiederum definieren wir die Zariski-Topologie auf $\mathbb{P}^n$, indem wir die projektiven Varietäten $PV(I)$ zu abgeschlossenen Teilmengen erklären (und ihre Komplemente zu offenen). Die folgenden Eigenschaften werden analog zu Abschnitt 1.7 bewiesen (Sie sollten sich das als Übung klarmachen!):

1. Die Menge der Zariski-offenen Mengen bildet eine Topologie. Durch Einschränkung bekommen wir eine Topologie auf allen projektiven Varietäten.

2. Alle projektiven Varietäten sind noethersche topologische Räume. Insbesondere sind sie quasi-kompakt und wir haben eine kanonische Zerlegung in irreduzible Komponenten.

3. Sei I ein homogenes Radikalideal. Mengen der Form $U_F := PV(I) \setminus PV(F)$ für ein homogenes Polynom F heissen standard-offen in $PV(I)$. Dabei muss F nur modulo I bestimmt sein, kann also ein Element aus $k[X_0, \ldots, X_n]/I$ sein. Wiederum ist jede offene Menge in $PV(I)$ die Vereinigung von endlich vielen standard-offenen Mengen.

1.8.9. Wir möchten nun die zu Beginn dieses Abschnittes beschriebene Prozedur formalisieren. Zunächst beobachten wir, dass wir $n + 1$ verschiedene Einbettungen

$$\begin{array}{rcl} \varphi_i : \mathbb{A}^n & \hookrightarrow & \mathbb{P}^n \\ [\lambda_1, \ldots, \lambda_n] & \mapsto & [\lambda_1, \ldots, \lambda_i, 1, \lambda_{i+1}, \ldots, \lambda_n] \end{array}$$

haben. Es wird also an der Stelle i eine 1 eingefügt. Das Bild von φ_i ist gerade die Menge

$$U_i := \mathbb{P}^n \setminus PV(X_i)$$

also eine Zariski-offene Menge. Ferner definieren die U_i eine Überdeckung:

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i.$$

U_i ist nun mit der induzierten Topologie ein topologischer Raum und es gilt:

Proposition 1.8.10. *Die Abbildungen φ_i sind Homöomorphismen*[7] $\mathbb{A}^n \to U_i$.

Beweis. Da φ_i offensichtlich bijektiv ist, müssen wir nur zeigen:

1. Für jede Varietät $V(I) \subset \mathbb{A}^n$ existiert eine projektive Varietät $PV(J) \subset \mathbb{P}^n$ mit

$$\varphi_i(V(I)) = U_i \cap PV(J)$$

2. Für jede projektive Varietät $PV(J) \subset \mathbb{P}^n$ ist auch $PV(J) \cap U_i = \varphi_i(V(I))$ für eine affine Varietät $V(I)$.

[7] d.h. Bijektionen so, dass die Abbildung und ihr Inverses stetig sind.

Wir zeigen zunächst 2. Sei $J = (F_1, \dots, F_m)$ wobei die F_i homogen sind. Wir können φ_i als Abbildung $\widetilde{\varphi}_i : \mathbb{A}^n \to \mathbb{A}^{n+1}$ auffassen und es ist klar, dass

$$V(F_1 \circ \widetilde{\varphi}_i, \dots, F_n \circ \widetilde{\varphi}_i) = \widetilde{\varphi}_i^{-1}(V(F_1, \dots, F_m)) = \varphi_i^{-1}(PV(J)).$$

Daher ist das Urbild von $PV(J)$ eine affine Varietät.
1. In umgekehrter Richtung sei $V(I)$ eine affine Varietät und $I = (f_1, \dots, f_n)$. Wir substituieren $x_j, j \leq i$ mit $\frac{X_{j-1}}{X_i}$ und $x_j, j > i$ mit $\frac{X_j}{X_i}$ und erhalten rationale Funktionen $F_i \in k(X_0, \dots, X_n)$. Durch Multiplikation mit einer gewissen Potenz X_i^k bekommen wir Polynome $X_i^k F_j \in k[X_0, \dots, X_n]$. Sei $J := (X_i^k F_1, \dots, X_i^k F_m)$. Die $X_i^k F_1$ sind offenbar alle homogen, daher ist J ein homogenes Ideal. Behauptung:

$$V(I) = \varphi_i^{-1}(PV(J))$$

Dies ist aber klar nach dem Beweis von 2. oben, denn wir erhalten die f_j durch Substitution der 1 für X_i in den $X_i^k F_j$ zurück. □

1.8.11. Wir möchten nochmals explizit das Verfahren beschreiben, welches im Beweis oben verwendet wurde: Sei $J = (F_1, \dots, F_m)$. Um aus der projektiven Varietät $PV(J)$ die affine Varietät $\varphi_i^{-1}(PV(J))$ zu bestimmen, werden also in den F_j die homogenen Koordinaten $X_0, \dots, X_n$ durch $x_1, \dots, x_i, 1, x_{i+1}, \dots, x_n$ (in dieser Reihenfolge) substituiert. Wir erhalten die Polynome $f_j := F_j \circ \widetilde{\varphi}_i$. Die gesuchte affine Varietät ist dann einfach $V(f_1, \dots, f_n)$.
Beispiel: Das homogene Polynom

$$F := X_1^2 X_0 - X_2^3 + X_2 X_0^2 + X_0^3$$

führt auf die affine Varietät $\varphi_0^{-1}(PV(F)) = V(f)$, wobei

$$f = x_1^2 - x_2^3 + x_2 + 1.$$

Umgekehrt, falls $I = (f_1, \dots, f_n)$ eine affine Varietät, so substituieren wir $x_1, \dots, x_n$ mit $\frac{X_0}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i}$ (in dieser Reihenfolge), erhalten rationale Funktionen $F_i \in k(X_0, \dots, X_n)$ und multiplizieren anschliessend mit einer genügend hohen Potenz von X_i um *Polynome* zu erhalten. Diese sind automatisch homogen. Die Potenz von X_i ist hierbei beliebig; mindestens müssen wir jedoch mit $X_i^{\deg(f_i)}$ multiplizieren. Wir wir gleich sehen werden, hat es eine besondere Bedeutung, hier mit der kleinsten Potenz zu multiplizieren. Für ein Polynom $f \in k[x_1, \dots, x_n]$ bezeichnen wir daher $\beta_i(f) := X_i^{\deg(f)} F$ wobei F die rationale Funktion ist, welches aus f durch die obige Substitution entsteht. $\beta_i(f)$ heisst auch **die Homogenisierung** von f.
Beispiel: Das Polynom

$$f := x_1^2 + x_2^2 - 1$$

führt nach Substitution (bzgl. $i = 0$) zunächst auf die rationale Funktion

$$(\frac{X_1}{X_0})^2 + (\frac{X_2}{X_0})^2 - 1$$

und nach Multiplikation mit X_0^2 auf das homogene Polynom:

$$\beta_0(f) = X_1^2 + X_2^2 - X_0^2.$$

In diesem Fall ist sogar $\overline{\varphi_0(V(f))} = PV(\beta_0(f))$ (projektiver Abschluss; siehe weiter unten).

1.8.12. *Achtung:* Die Entsprechungen $I \leftrightarrow J$ zwischen Idealen in $k[x_1, \dots, x_n]$ und homogenen Idealen $k[X_0, \dots, X_n]$ (welche wie oben durch φ_i induziert sind) sind nicht bijektiv, selbst wenn wir uns auf Radikalideale beschränken. z.B. ist natürlich $\varphi_i^{-1}(PV(X_i)) = V(1) = \emptyset$. Dies spiegelt sich auf der algebraischen Seite dadurch, dass wir die F_i mit einer *beliebigen* Potenz von X_i multiplizieren können (sogar die einzelnen F_i jeweils mit unterschiedlichen).

Es gibt jedoch eine *kanonische* Wahl einer Zuordnung, um aus einer affinen Varietät $V(I)$ eine projektive Varietät zu machen, nämlich den **projektiven Abschluss**

$$V(I) \mapsto \overline{\varphi_i(V(I))}.$$

Erinnere, dass für einen topologischen Raum M und eine Teilmenge $Y \subset M$ der Abschluss von Y wie folgt definiert ist:

$$\overline{Y} = \bigcap_{\substack{Z \text{ abgeschlossen} \\ Y \subset Z}} Z.$$

Es handelt sich also um die kleinste abgeschlossene Menge, die Y enthält. Wir haben den folgenden Satz:

Proposition 1.8.13. *Sei I ein Radikalideal von $k[x_1, \dots, x_n]$. Sei $J \subset k[X_0, \dots, X_n]$ das Ideal, welchen von allen $\beta_i(f), f \in I$ erzeugt wird. Dann gilt:*

$$\overline{\varphi_i(V(I))} = PV(J).$$

Insbesondere, falls $I = (f)$ ein Hauptideal ist, gilt:

$$\overline{\varphi_i(V(f))} = PV(\beta_i(f)).$$

Mit anderen Worten, wenn wir bei der Konstruktion des homogenen Ideales vorsichtig sind, und überall mit der *kleinsten möglichen* Potenz von X_i multiplizieren, die uns erlaubt, ein Polynom zu erhalten, dann bekommen wir die Elemente des Ideals des projektiven Abschlusses. *Achtung:* Falls I kein Hauptideal ist, reicht es u.U. nicht, dies für die Erzeuger von I zu tun (siehe Beispiel 1.8.14).

Beweis. Es folgt aus dem Beweis von Proposition 1.8.10, dass $\overline{\varphi_i(V(I))} \subset PV(J)$. Sei also $p \in PV(J)$. Es genügt zu zeigen (Übung in elementarer Topologie), dass für jede offene Umgebung $U \ni p$ gilt: $U \cap \varphi_i(V(I)) \neq \emptyset$. Es genügt daher sogar, dies für standard-offene Umgebungen $U_F = \mathbb{P}^n \setminus PV(F)$ zu zeigen.
Behauptung: Es genügt zu zeigen: Für alle $F \in k[X_0, \dots, X_n]$ gilt: $F \circ \widetilde{\varphi}_i \in I \Rightarrow F \in J$.
Beweis der Behauptung:

$$\begin{aligned} p \in PV(J) \text{ und } p \in U_F \quad &\Rightarrow \quad F \notin J \\ &\Rightarrow \quad F \circ \widetilde{\varphi}_i \notin I \qquad \text{dies ist die Umkehrung der Annahme!} \\ &\Rightarrow \quad U_{F \circ \widetilde{\varphi}_i} \cap V(I) \neq \emptyset \\ &\Rightarrow \quad U_F \cap \varphi_i(V(I)) \neq \emptyset. \end{aligned}$$

Wir müssen also noch zeigen: Für alle $F \in k[X_0, \dots, X_n]$ gilt: $F \circ \widetilde{\varphi}_i \in I \Rightarrow F \in J$. Sei also $f := F \circ \widetilde{\varphi}_i \in I$. Wir haben dann nach Definition $\beta_i(f) \in J$. Es genügt also zu zeigen $F = X_i^k \beta_i(f)$ für gewisses $k \in \mathbb{N}_0$. Sei $X_0^{k_0} \dots X_n^{k_n}$ ein Monom welches in F vorkommt. Durch die erste Substitution wird dies zum Monom

$$x_1^{k_0} \cdots x_i^{k_{i-1}} x_{i+1}^{k_{i+1}} \cdots x_n^{k_n}$$

in $f := F \circ \widetilde{\varphi}_i$. Durch die zweite Substitution zu

$$(\frac{X_0}{X_i})^{k_0} \cdots (\frac{X_{i-1}}{X_i})^{k_{i-1}} (\frac{X_{i+1}}{X_i})^{k_{i+1}} \cdots (\frac{X_n}{X_i})^{k_n}.$$

Dies wird nun mit $X_i^{\deg(f)}$ multipliziert, um ein Monom in $\beta_i(f)$ zu erhalten, also wird zu

$$X_i^{\deg(f) - \deg(F)} X_0^{k_0} \cdots X_n^{k_n}.$$

Beachte: $\deg(f) - \deg(F) \geq -k_i$, daher steht hier ein Monom (ohne negative Potenzen von X_i). Wir bekommen also:

$$F = X_i^{\deg(F) - \deg(f)} \beta_i(f)$$

und daher das gewünschte, da $\deg(F) - \deg(f) \geq 0$. □

Beispiel 1.8.14. *Sei $V = V(x_1^2+x_2, x_1^2+x_3)$. Betrachte das Bild von V unter $\varphi_0 : \mathbb{A}^2 \to \mathbb{P}^2$. Die Rechnung $(x_1^2+x_2, x_1^2+x_3) = (x_1^2+x_2, x_2-x_3)$ zeigt, dass es sich um eine Parabel handelt, welche in sich in der $x_2 = x_3$-Ebene befindet. Wir erwarten, dass der projektive Abschluss aus der Vereinigung von V mit einzelnen Punkten besteht. Berechnen wir die Homogenisierungen:*

$$\beta_0(x_1^2+x_2) = X_1^2 + X_2X_0,$$

$$\beta_0(x_1^2+x_3) = X_1^2 + X_3X_0,$$

$$\beta_0(x_2-x_3) = X_2 - X_3.$$

Würden wir nur die Erzeuger homogenisieren, bekämen wir die projektive Varietät $PV(X_1^2 + X_2X_0, X_1^2 + X_3X_0)$. Dies ist nicht *der projektive Abschluss von V, da das Polynom $X_2 - X_3$ (oder eine Potenz davon) nicht im homogenen Ideal $(X_1^2 + X_2X_0, X_1^2 + X_3X_0)$ liegt. In der Tat liegt die ganze projektive Gerade mit homogenen Koordinaten $[0, 0, \alpha, \beta] \in PV(X_1^2 + X_2X_0, X_1^2 + X_3X_0)$ aber bis auf einen einzigen Punkt nicht in $PV(X_2 - X_3)$! Man überlege sich, dass aber gilt:*

$$\overline{\varphi_0(V)} = PV(X_1^2 + X_2X_0, X_2 - X_3).$$

1.8.15. Wir sind noch die Begründung schuldig, dass in Proposition 1.8.5, (*) impliziert, dass I homogen ist. Sei also I ein Radikalideal so, dass $V(I)$ eine Varietät in $\mathbb{A}^{n+1}$ mit der Eigenschaft (*) ist (also kegelartig). Sie induziert eine Menge $P \subset \mathbb{P}^n$ (die Menge der Geraden, die in $V(I)$ enthalten sind), von der wir zunächst zeigen wollen, dass sie abgeschlossen ist. $\widetilde{\varphi_i}^{-1}(V(I))$ ist eine Varietät $V(I_i)$ in $\mathbb{A}^n$. Wir bilden den Abschluss: $\overline{\varphi_i(V(I_i))} = PV(J_i)$ wobei J_i ein zugehöriges Ideal ist, welches wir als homogenes Radikalideal annehmen können.
Daher gilt nach Proposition 1.8.10, dass $PV(J_i) \cap U_i = \varphi_i(V(I_i))$. Wegen der Eigenschaft (*) gilt: $\varphi_i(V(I_i)) = P \cap U_i$. M.a.W. für jede der Mengen U_i in der offenen Überdeckung

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$$

ist der Schnitt $P \cap U_i$ abgeschlossen in U_i. Es folgt, dass P abgeschlossen ist (Übung in elementarer Topologie). In der Tat gilt hier:

$$P = PV(J_0) \cup \cdots \cup PV(J_n).$$

Falls $V(I) \neq \{[0,\ldots,0]\}$ gilt daher $V(I) = V(J_0 \cap \cdots \cap J_n)$ und daher $I = J_0 \cap \cdots \cap J_n$ (beide Seiten sind bereits Radikalideale). $I = I(V(I))$ ist also homogen.
Falls $V(I) = \{[0,\ldots,0]\}$ ist $I = (X_0,\ldots,X_n)$. Dieses Ideal ist ebenfalls homogen. Da es durch P nicht von (1) (falls $V(I) = \emptyset$) unterschieden werden kann, betrachtet man es üblicherweise nicht. Es heisst auch in der Literatur das *irrelevante Ideal*.

Wir haben bisher nicht über Funktionen auf projektiven Varietäten gesprochen. Zunächst können wir wie im affinen definieren:

Definition/Lemma 1.8.16. *Sei $V \subset \mathbb{P}^n$ eine projektive Varietät, dann sei $I(V)$ das Ideal, welches von allen $f \in k[X_0,\ldots,X_n]$* homogen *mit $f(P) = 0$ für alle $P \in V$ erzeugt wird. Es heisst das* **homogene Verschwindungsideal** *von V. Der Quotientenring $k[X_0,\ldots,X_n]/I(V)$ heisst der* **homogene Koordinatenring** *von V. Er ist ebenfalls in natürlicher Weise ein graduierter Ring. Falls $V' \subset \mathbb{A}^{n+1}$ die entsprechende Vereinigung von Geraden bezeichnet so gilt: $I(V) = I(V')$.*

Beachte, dass die Bedingung $f(P) = 0$ für alle $P \in V$ sinnvoll ist, da sie nicht von der Wahl der homogenen Koordinaten für P abhängt. Hierfür ist entscheidend, dass f homogen ist.
Der homogene Koordinatenring $k[X_0,\ldots,X_n]/I(V)$ kann *nicht* mehr als Menge von Funktionen auf $PV(I)$ aufgefasst werden. Allerdings gibt jedes homogene Ideal bzgl. der Graduierung (siehe 1.8.4) auf diesem Quotientenring $J \subset k[X_0,\ldots,X_n]/I(V)$ eine wohldefinierte projektive Varietät $PV(J) \subset PV(I)$. Wie wir dennoch Funktionen und insbesondere Morphismen zwischen projektiven Varietäten definieren können, werden wir im Abschnitt 1.10 sehen.
Der Hilbertsche Nullstellensatz gibt uns nun:

Korollar 1.8.17 (Projektiver Hilbertscher Nullstellensatz)**.** *Die Abbildungen $I \mapsto PV(I)$ und $V \mapsto I(V)$ (aus 1.8.7 und 1.8.16) definieren eine inklusionsumkehrende Bijektion zwischen homogenen Radikalidealen in $k[X_0, \ldots, X_n]$ (welche nicht das irrelevante Ideal sind) und projektiven Varietäten im $\mathbb{P}^n$.*

Beweis. Aus dem affinen Hilbertschen Nullstellensatz 1.3.7 und Proposition 1.8.5 folgt, dass die Abbildungen $I \mapsto V(I)$ und $V \mapsto I(V)$ (affine Variante) eine Bijektion zwischen Varietäten im $\mathbb{A}^{n+1}$, welche (*) von 1.8.5 erfüllen (d.h. kegelartig sind) und homogenen Radikalidealen gibt. Nun ist aber $PV(I)$ gerade die Menge der Geraden in $V(I)$ und umgekehrt ist $V(I)$ die Vereinigung der Geraden in $PV(I)$, falls I nicht das irrelevante Ideal ist. Ferner gilt $I(V(I)) = I(PV(I))$, falls I nicht das irrelevante Ideal ist. □

Beispiel 1.8.18. *Zum Ende des Abschnittes wollen wir den Bogen spannen und noch einmal auf Beispiel 1.8.1 zurückkommen. Zwei verschiedene Geraden im $\mathbb{A}^2$*

$$V(a_1x_1 + a_2x_2 + a_3) \qquad V(b_1x_1 + b_2x_2 + b_3)$$

(mit $[a_1, a_2] \neq [0, 0]$ und $[b_1, b_2] \neq [0, 0]$) können wir mit der Abbildung

$$\varphi_0 : [\lambda_1, \lambda_2] \mapsto [1, \lambda_1, \lambda_2]$$

in den $\mathbb{P}^2$ einbetten. Wir haben gesehen: Die projektiven Abschlüsse werden gerade durch die Homogenisierungen

$$PV(a_1X_1 + a_2X_2 + a_3X_0) \qquad PV(b_1X_1 + b_2X_2 + b_3X_0)$$

beschrieben. Die Punkte "im unendlichen", also in $\mathbb{P}^2 \setminus \varphi_0(\mathbb{A}^2) = V(X_0)$, welche auf den Geraden liegen, sind gerade die Punkte

$$PV(a_1X_1 + a_2X_2 + a_3X_0, X_0) \qquad PV(b_1X_1 + b_2X_2 + b_3X_0, X_0)$$

also

$$PV(a_1X_1 + a_2X_2, X_0) \qquad PV(b_1X_1 + b_2X_2, X_0)$$

Dies ist jeweils ein einzelner Punkt mit homogenen Koordinaten

$$[a_2, -a_1, 0] \qquad [b_2, -b_1, 0].$$

Diese Punkte sind gleich, genau dann wenn ihre homogenen Koordinaten Vielfache voneinander sind. Dies ist genau dann der Fall, wenn

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = 0,$$

also genau dann, wenn die beiden ursprünglichen affinen Geraden parallel waren. Zwei verschiedene Geraden schneiden sich nun also immer *in genau einem Punkt. Wir bekommen darüberhinaus zusätzlich die Gerade*

$$PV(0X_1 + 0X_2 + X_0)$$

welche keine *affine Entsprechung hat. Sie ist, wie gesagt, genau das Komplement von $\varphi_0(\mathbb{A}^2)$ und wird auch unendlich ferne Gerade genannt.*

1.9 Lokalisierung von Ringen

Eine der fundamentalen Beobachtungen über affine Varietäten war, dass man abstrakt konstruierte Ringe wie $k[x_1, \ldots, x_n]/I$ (wobei I ein Radikalideal ist) als Ringe von polynomialen Funktionen auf einer geeigneten solchen Varietät auffassen konnte. Für projektive Varietäten haben wir bisher eine solche Beschreibung nicht. Wir wissen überhaupt noch nicht, wie wir geeignete Abbildungen zwischen projektiven Varietäten definieren sollen. Insbesondere fehlt bisher ein Begriff der Isomorphie von projektiven Varietäten. Homogene Polynome definieren keine wohldefinierten Funktionen auf einer projektiven Varietät. Anders sieht es mit einer Funktion aus, welche durch den Quotienten zweier homogener Polynome $F, G \in (k[X_0, \ldots, X_n])_i$ (d.h. vom selben Grad) gegeben wird:

$$\frac{F}{G} : \lambda \mapsto \frac{F(\lambda)}{G(\lambda)}$$

Die Rechnung

$$\frac{F}{G}(\alpha\lambda) = \frac{F(\alpha\lambda)}{G(\alpha\lambda)} = \frac{\alpha^i F(\lambda)}{\alpha^i G(\lambda)} = \frac{F}{G}(\lambda)$$

zeigt, dass dies eine wohldefinierte Funktion ist (also nicht von der Wahl homogener Koordinaten abhängt). Es gibt allerdings einen fundamentalen Unterschied: Die Funktion $\frac{F}{G}$ ist nicht überall definiert, sondern nur auf der Zariski-offenen Menge $U_G = \mathbb{P}^n \setminus PV(G)$. Ein ähnliches Problem haben wir noch aus der Einleitung in Erinnerung. Auch dort, bei affinen Varietäten, waren manchmal natürlich gegebene Funktionen nicht durch Polynome, sondern durch rationale Funktionen gegeben, wiederum mit dem Unterschied, dass sie nur auf einer Zariski-offenen Menge definiert waren.
Es ist daher geschickt, das folgende zu definieren:

Definition 1.9.1. *1. Sei U eine Zariski-offene Menge in einer* affinen *Varietät $V \subset \mathbb{A}^n$. Eine Funktion $\varphi : U \to \mathbb{A}^1$ heisst* **regulär** *an einem Punkt $p \in U$ falls eine Zariski-offene Menge $U' \subset U$ mit $p \in U'$ und Polynome $f, g \in k[x_1, \ldots, x_n]$ existieren, so dass*

$$\varphi(\lambda) = \frac{f(\lambda)}{g(\lambda)}$$

für alle $\lambda \in U'$. φ heisst regulär, wenn sie an allen Punkten regulär ist.

2. *Sei U eine Zariski-offene Menge in einer* projektiven *Varietät $V \subset \mathbb{P}^n$. Eine Funktion $\varphi : U \to \mathbb{A}^1$ heisst* **regulär** *an einem Punkt $p \in U$ falls eine Zariski-offene Menge $U' \subset U$ mit $p \in U'$ und homogene Polynome $F, G \in (k[X_0, \ldots, X_n])_i$ existieren, so dass*

$$\varphi(\lambda) = \frac{F(\lambda)}{G(\lambda)}$$

für alle $\lambda \in U'$. φ heisst regulär, wenn sie an allen Punkten regulär ist.

Offenbar bilden reguläre Funktionen auf einer Zariski-offenen Menge U einen Ring. Wir werden diesen später mit $\mathcal{O}(U)$ bezeichnen. Dies gibt zu diesem Zeitpunkt aber ein Problem, da wir ja $\mathcal{O}(V)$ für eine affine Varietät (V ist insbesondere auch eine Zariski-offene Menge in V) bereits definiert haben. Wir werden später sehen (Proposition 1.10.1), dass dies keinen Unterschied macht, aber erst dann diese Bezeichnung verwenden.
Sie werden sich möglicherweise wundern, warum wir nicht einfach die Existenz von Polynomen f und g (bzw. F und G) für ganz U gefordert haben. Dies ergibt jedoch in einigen Fällen eine Einschränkung, ausserdem ist unsere Definition flexibler.
So wie wir unsere polynomialen Funktionen als abstrakte Elemente eines Ringes auffassen konnten, so können wir auch reguläre Funktionen (also solche die "lokal" durch rationale Funktionen gegeben sind) als Elemente von abstrakt konstruierten Ringen auffassen. Diese heissen *Lokalisierungen.* Ihre Konstruktion ist ganz ähnlich zu der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ durch das Kalkül von Brüchen.
Wir stellen uns dazu folgendes abstraktes Problem. Sei R ein kommutativer Ring und S eine Teilmenge von R. Wir möchten einen Ring $R[S^{-1}]$ konstruieren, in den R abbildet, und in dem alle Elemente von S zu Einheiten werden. Zunächst gilt natürlich $s \in R$ Einheit und $t \in R$ Einheit $\Rightarrow st$ Einheit. Daher ändert sich das Problem nicht, wenn wir fordern, dass S multiplikativ abgeschlossen ist:

Definition 1.9.2. *Sei R ein kommutativer Ring. Eine Teilmenge $S \subset R$ heisst* **multiplikativ abgeschlossen**, *falls $1 \in S$, $0 \notin S$, und $s, t \in S \Rightarrow st \in S$.*

Die Bedingung $0 \notin S$ haben wir hinzugefügt, da es offensichtlich nicht möglich ist, einen Ring (ausser vielleicht dem Nullring) zu konstruieren, in dem 0 eine Einheit wird.

Beispiel 1.9.3. *Die folgenden Mengen sind multiplikativ abgeschlossen:*

1. *$S_f = \{1, f, f^2, f^3, \ldots\}$, wobei $f \in R$ nicht nilpotent.*
2. *$S_\wp = R \setminus \wp$, wobei $\wp$ ein Primideal ist.*
3. *S die Menge aller Elemente von R die keine Nullteiler sind. Falls R nullteilerfrei ist, so ist $S = R \setminus \{0\}$.*

Unser Problem wird durch die folgende Proposition gelöst:

Proposition 1.9.4. *Sei R ein kommutativer Ring und $S \subset R$ eine multiplikativ abgeschlossene Teilmenge. Dann existiert ein Ringhomomorphismus $\iota : R \to R[S^{-1}]$ so, dass $\iota(s)$ für alle $s \in S$ invertierbar ist, mit folgender universeller Eigenschaft: Für jeden Ringhomomorphimus $\varphi : R \to Q$ so, dass $\varphi(s)$ für alle $s \in S$ invertierbar ist, gibt es einen eindeutigen Ringhomomorphismus $\widetilde{\varphi} : R[S^{-1}] \to Q$ so, dass $\varphi = \widetilde{\varphi} \circ \iota$.*
Falls S nullteilerfrei ist, so ist $R \to R[S^{-1}]$ injektiv.

Beachte: Wiederum ist $R[S^{-1}]$ (bis auf Isomorphie) eindeutig durch diese universelle Eigenschaft bestimmt. Der Ring $R[S^{-1}]$ heisst die **Lokalisierung** von R bei S.

Beweis. Die Konstruktion ist, wie gesagt, ganz analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$. Wir definieren $R[S^{-1}]$ als die Menge

$$R \times S = \left\{ \frac{f}{g} \middle| f \in R, g \in S \right\}$$

(hier ist $\frac{f}{g}$ zunächst als abstraktes Symbol zu verstehen) modulo der Äquivalenzrelation

$$\frac{f}{g} \sim \frac{f'}{g'} \Leftrightarrow \exists s \in S : s(fg' - f'g) = 0.$$

Falls S keine Nullteiler enthält, vereinfacht sich die Bedingung zu der gewohnten: $\frac{f}{g} \sim \frac{f'}{g'} \Leftrightarrow fg' = f'g$. Die etwas verschärfte Bedingung ist nötig, um auch im allgemeinen eine *transtitive* Relation zu erhalten: Zunächst sind Symmetrie und Reflexivität der Relation offensichtlich. Beweis der Transitivität: Seien:

$$\frac{f}{g} \sim \frac{f'}{g'} \text{ und } \frac{f'}{g'} \sim \frac{f''}{g''},$$

d.h.

$$\begin{aligned} \exists s \in S &: \quad s(fg' - f'g) = 0 \\ \exists t \in S &: \quad t(f'g'' - f''g') = 0. \end{aligned}$$

dann gilt:

$$\begin{aligned} stg'(fg'' - f''g) &= stg'fg'' - stg'f''g = stg'fg'' - stg''f'g + stg''f'g - stg'f''g \\ &= tg''(s(fg' - f'g)) + sg(t(f'g'' - f''g')) = 0. \end{aligned}$$

d.h. $\frac{f}{g} \sim \frac{f''}{g''}$. Die Relation ist also transitiv. Die Äquivalenzklasse eines Bruches in $R[S^{-1}]$ bezeichnen wir wieder mit $\frac{f}{g}$ und schreiben daher $\frac{f}{g} = \frac{f'}{g'}$ statt $\frac{f}{g} \sim \frac{f'}{g'}$.
Wir definieren nun eine Ringstruktur auf $R[S^{-1}]$ durch die bekannten Formeln:

$$\begin{aligned} \frac{f}{g} + \frac{f'}{g'} &:= \frac{fg' + f'g}{gg'} \\ \frac{f}{g} \cdot \frac{f'}{g'} &:= \frac{ff'}{gg'}. \end{aligned}$$

Man rechnet nach, dass dies wohldefiniert ist, d.h. nicht von der Wahl der Vertreter abhängt. Die Überprüfung der Ringaxiome lassen wir als Übung. Die neutralen Elemente bzgl. Addition und Multiplikation sind $\frac{0}{1}$ bzw. $\frac{1}{1}$. Definiere den Ringhomomorphismus:

$$\begin{aligned} \iota : R &\to R[S^{-1}] \\ f &\mapsto \frac{f}{1} \end{aligned}$$

Er ist injektiv, falls S keine Nullteiler enthält, denn dann folgt aus $\exists s \in S : s(f \cdot 1 - 0 \cdot 1) = 0$, dass $f = 0$.
Wir wollen noch beweisen, dass $\iota : R \to R[S^{-1}]$ die universelle Eigenschaft erfüllt: Sei also $\varphi : S \to Q$ ein Ringhomomorphismus mit der Eigenschaft: $\varphi(s)$ Einheit für alls $s \in S$. Wir definieren dann

$$\begin{array}{rcl} \widetilde{\varphi} : R[S^{-1}] & \to & Q \\ \dfrac{f}{g} & \mapsto & \varphi(g)^{-1} \cdot \varphi(f). \end{array}$$

Dann gilt offensichtlich die Gleichung $\varphi = \widetilde{\varphi} \circ \iota$. Ausserdem zwingt diese uns, $\widetilde{\varphi}$ so zu definieren. $\widetilde{\varphi}$ ist also eindeutig bestimmt. Wir haben noch zu überprüfen, dass $\widetilde{\varphi}$ wohldefiniert ist, d.h. der Ausdruck $\varphi(g)^{-1} \cdot \varphi(f)$ nicht von der Wahl der Vertreter f, g abhängt. Sei also $\frac{f}{g} = \frac{f'}{g'}$. Es gibt dann $s \in S$ so, dass $s(fg' - f'g) = 0$.
Anwenden von φ gibt:

$$\varphi(s)(\varphi(f)\varphi(g') - \varphi(f')\varphi(g)) = 0.$$

Nun sind aber nach Voraussetzung $\varphi(s), \varphi(g)$ und $\varphi(g')$ Einheiten, d.h. wir bekommen

$$\varphi(g)^{-1}\varphi(f) = \varphi(g')^{-1}\varphi(f').$$

□

Die multiplikativ abgeschlossenen Mengen in Beispiel 1.9.3 sind die häufigsten, an denen wir Ringe lokalisieren werden:

Definition 1.9.5. *1. Für $S_f = \{1, f, f^2, f^3, \dots\}$, wobei $f \in R$ nicht nilpotent, bezeichnen wir $R[f^{-1}] := R[S_f^{-1}]$. Zeigen Sie als Übung (z.B. indem Sie die universelle Eigenschaft überprüfen), dass $R[f^{-1}] \cong R[x]/(fx - 1)$.*

2. Für $S_\wp = R \setminus \wp$, wobei $\wp$ ein Primideal ist, bezeichnen wir $R_\wp := R[S_\wp^{-1}]$. Er heisst die Lokalisierung von R bei $\wp$ und ist ein lokaler Ring, *d.h. hat genau ein maximales Ideal, wie wir gleich sehen werden.*

3. Falls R nullteilerfrei ist, und $S = R \setminus \{0\}$, dann ist $R[S^{-1}]$ ein Körper, welcher R enthält. Er heisst **Quotientenkörper** *von R und wird mit* $\mathrm{Quot}(R)$ *bezeichnet.*

Für jedes Ideal I von R definiert

$$I[S^{-1}] = \left\{ \frac{f}{g} \in R[S^{-1}] \middle| f \in I, g \in S \right\}$$

ein Ideal von $R[S^{-1}]$. Die Aussage $f \in I$ ist u. U. abhängig von der Wahl des Vertreters. In diesem Fall ist die Definition so zu verstehen, dass ein Vertreter existiert, so dass $f \in I$.

Proposition 1.9.6. *Sei $\iota : R \to R[S^{-1}]$ wie in Proposition 1.9.4. Die Zuordnung $J \mapsto \iota^{-1}(J)$ und $I \mapsto I[S^{-1}]$ sind zueinander inverse Bijektionen zwischen der Menge der Primideale von $R[S^{-1}]$ und der Menge der Primideale I von R mit der Eigenschaft $I \cap S = \emptyset$.*

Beweis. Übung. □

Überlegen Sie sich, dass die Aussage der Proposition falsch wird, falls "Primideal" durch "Ideal" oder "maximales Ideal" ersetzt wird.

Definition 1.9.7. *Ein kommutativer Ring R heisst* **lokal**, *falls er genau ein maximales Ideal enthält.*

Ein Ring R ist genau dann lokal, wenn die nicht-Einheiten von R ein Ideal bilden. Insbesondere gilt in einem lokalen Ring R mit maximalem Ideal $\mathfrak{m}$, dass alle Elemente in $R \setminus \mathfrak{m}$ invertierbar sind.
Für einen lokalen Ring R ist der Quotient von $R/\mathfrak{m}$ ein Körper (da $\mathfrak{m}$ maximal ist). Er ist wegen der Lokalität von R der einzige Körper, der als Quotient von R auftauchen kann. Er heisst der **Restklassenkörper** von R.

Beispiel 1.9.8. *Ein Körper ist ein lokaler Ring; das maximale Ideal ist hier das Ideal* (0).

Beispiel 1.9.9. *Ringe der Form $R_\wp$ für ein Primideal $\wp \subset R$ sind lokal.*
In der Tat sind maximale Ideale prim und Primideale von $R_\wp$ entsprechen nach der Proposition Primidealen J von R welche $(R \setminus \wp) \cap J = \emptyset$, also $J \subset \wp$ erfüllen. In der Menge der Primideale mit dieser Eigenschaft gibt es offensichtlich genau ein maximales Element, nämlich $\wp$ selbst.

Proposition 1.9.10. *Sei R ein graduierter Ring und S eine Menge von* homogenen *Elementen. Dann definiert*

$$R[S^{-1}]_i := \left\{ \frac{f}{g} \mid f \text{ homogen und } \deg(f) - \deg(g) = i \right\}$$

eine Graduierung auf $R[S^{-1}]$. Hier schreiben wir: $\deg(f) = i :\Leftrightarrow f \in R_i$.

Beweis. Übung. □

1.10 Quasi-projektive Varietäten

Wir wollen nun die Konstruktion des letzten Abschnittes mit algebraischer Geometrie in Verbindung bringen. Sei U_g eine standard-offene Menge in einer affinen Varietät V. Jedes Element $\frac{f}{g^m}$ in $\mathcal{O}(V)[g^{-1}]$ definiert eine reguläre Funktion (siehe Definition 1.9.1) auf U_g:

$$\begin{aligned} U_g &\to \mathbb{A}^1 \\ \lambda &\mapsto \frac{f(\lambda)}{g^m(\lambda)} \end{aligned}$$

(Überlegen Sie sich die Wohldefiniertheit!).

Proposition 1.10.1. *Wir haben (vermöge der obigen Abbildung):*

$$\mathcal{O}(V)[g^{-1}] \cong \{\textit{reguläre Funktionen auf } U_g\}.$$

Beweis. Wir zeigen zunächst die Injektivität der obigen Abbildung. Sei $\frac{f}{g^m} \in \mathcal{O}(V)[g^{-1}]$ so, dass dies die Nullfunktion auf U definiert. Das heisst aber, dass $f(\lambda) = 0$ für alle $\lambda \in U_g$. Daraus folgt, dass $f \cdot g$ in $\mathcal{O}(V)$ Null ist. Daher $\frac{f}{g^m} = \frac{fg}{g^{m+1}} = 0$.
Surjektivität: Sei $\varphi : U_g \to \mathbb{A}^1$ eine reguläre Funktion. Nach Definition existiert also zu jedem $p \in U_g$ eine offene Menge U_p mit $p \in U_p \subset U_g$ und Polynome $f_p, g_p \in k[x_1, \ldots, x_n]$ mit $\varphi(\lambda) = \frac{f_p(\lambda)}{g_p(\lambda)}$ für alle $\lambda \in U_p$. Offensichtlich dürfen wir die U_ps so verkleinern, dass sie alle standard-offen werden. Da $U_g = \bigcup_{p \in U_g} U_p$ und U_g quasi-kompakt ist, reichen endlich viele U_ps, um U_g zu überdecken.
Also:

$$U_g = (U_{h_1} \cup \cdots \cup U_{h_m}) \cap V \tag{12}$$

wobei die $h_i \in k[x_1, \ldots, x_n]$ liegen, und für alle i existieren $f_i, g_i \in k[x_1, \ldots, x_n]$, so dass $\varphi(\lambda) = \frac{f_i(\lambda)}{g_i(\lambda)}$ für alle $\lambda \in U_{h_i} \cap V$.
Daraus folgt insbesondere $V(g_i) \cap V \subset V(h_i)$, d.h. $h_i \in I(V(g_i) \cap V) = \sqrt{(g_i) + I(V)}$, d.h. es existieren $l \in \mathbb{N}$ und $b \in k[x_1, \ldots, x_n]$ so, dass $bg_i - h_i^l \in I(V)$. Daher gilt auch $\frac{f_i(\lambda)}{g_i(\lambda)} = \frac{f_i(\lambda)b(\lambda)}{g_i(\lambda)b(\lambda)} = \frac{f_i(\lambda)b(\lambda)}{h_i(\lambda)^l}$ für alle $\lambda \in U_{h_i}$.
Wir können also f_i, g_i, h_i durch $f_i b, h_i^l, h_i^l$ ersetzen und o.B.d.A. annehmen, dass $g_i = h_i$.
Betrachten wir zunächst ein Paar offener Mengen U_{h_i}, U_{h_j}. Wir haben

$$U_{h_i} \cap U_{h_j} = U_{h_i h_j}$$

und auf $U_{h_i h_j} \cap V$ gilt also $\frac{f_i(\lambda)}{h_i(\lambda)} = \frac{f_j(\lambda)}{h_j(\lambda)}$ oder $f_i(\lambda)h_j(\lambda) = f_j(\lambda)h_i(\lambda)$. Daher gilt

$$h_i h_j^2 f_i - h_i^2 h_j f_j \in I(V).$$

Indem wir nochmals erweitern, und f_i, h_i durch $f_i h_i, h_i^2$ ersetzen können wir also annehmen, dass

$$h_j f_i - h_i f_j \in I(V). \tag{13}$$

Die Gleichung (12) bedeutet

$$V(g) = V(h_1) \cap \cdots \cap V(h_m) \cap V = V(h_1, \ldots, h_m) \cap V$$

und daher nach dem Hilbertschen Nullstellensatz $g \in \sqrt{(h_1, \ldots, h_m) + I(V)}$, also existiert $l \in \mathbb{N}$ und $a_i \in k[x_1, \ldots, x_n]$ so, dass

$$g^l - a_1 h_1 - \cdots - a_m h_m \in I(V)$$

Definiere

$$\widetilde{\varphi} = \frac{a_1 f_1 + \cdots + a_m f_m}{g^l} \in \mathcal{O}(V)[g^{-1}].$$

Behauptung: $\widetilde{\varphi}$ repräsentiert φ. Wir rechnen das auf U_{h_i} nach. Hier dürfen wir mit h_i erweitern, d.h. es gilt:

$$\widetilde{\varphi}(\lambda) = \frac{h_i(a_1 f_1 + \cdots + a_m f_m)}{h_i g^l}(\lambda) = \frac{h_i(a_1 f_1 + \cdots + a_m f_m)}{h_i(a_1 h_1 + \cdots + a_m h_m)}(\lambda)$$

$$= \frac{f_i(a_1 h_1 + \cdots + a_m h_m)}{h_i(a_1 h_1 + \cdots + a_m h_m)}(\lambda) = \frac{f_i}{h_i}(\lambda)$$

für alle $\lambda \in U_{h_i}$ (hier wurde Gleichung (13) verwendet). □

Insbesondere erhalten wir für eine affine Varietät $V = U_1$ (hier ist $g = 1$), dass $\mathcal{O}(V)$ mit dem Ring der regulären Funktionen auf V übereinstimmt. Es ist daher sinnvoll, für *alle* Zariski-offenen Mengen zu definieren:

Definition 1.10.2. *Sei U eine Zariski-offene Menge in einer affinen (bzw. projektiven) Varietät. U heisst eine* **quasi-affine (bzw. quasi-projektive) Varietät.** *Wir bezeichnen mit $\mathcal{O}(U)$ den Ring der regulären Funktionen auf U (siehe Definition 1.9.1).*

Bemerkung 1.10.3. *Eine Zuordnung $U \mapsto \mathcal{O}(U)$, wie wir sie gerade definiert haben, ist in der Mathematik allgegenwärtig. Wir wollen das kurz diskutieren:*
Sei X ein topologischer Raum. Eine Zuordnung

$$\begin{array}{rcl} \{\textit{offene Mengen } \subset X\} & \to & \{k-\textit{Algebren}\} \\ U & \mapsto & \mathcal{O}(U) \end{array}$$

zusammen mit Einschränkungsabbildungen (k-Algebrenhomomorphismen)

$$r_{U,U'} : \mathcal{O}(U) \to \mathcal{O}(U')$$

für $U' \subset U$ heisst **Garbe** *(von k-Algebren), falls die folgenden Eigenschaften erfüllt sind:*

1. *$r_{U,U} = \mathrm{id}_{\mathcal{O}(U)}$ und $r_{U',U''} \circ r_{U,U'} = r_{U,U''}$.*
2. *Falls $U = \bigcup_{i \in I} U_i$ eine offene Überdeckung ist, so gilt für $f \in \mathcal{O}(U)$, dass*
$$r_{U,U_i}(f) = 0 \textit{ für alle } i \in I \;\Rightarrow\; f = 0.$$
3. *Falls $U = \bigcup_{i \in I} U_i$ eine offene Überdeckung ist und $f_i \in \mathcal{O}(U_i)$ gegeben mit*
$$r_{U_i, U_i \cap U_j}(f_i) = r_{U_j, U_i \cap U_j}(f_j) \qquad \textit{für alle } i, j \in I\ ,$$
so gibt es ein $f \in \mathcal{O}(U)$ mit $r_{U,U_i}(f) = f_i$ für alle i.

Diese Definition mag technisch erscheinen, ist aber fundamental. In unserem Fall sind die $\mathcal{O}(U)$ durch Funktionen *auf U gegeben und die Abbildungen $r_{U,U'} : \mathcal{O}(U) \to \mathcal{O}(U')$ sind durch die* Einschränkung von Funktionen *gegeben. Die Eigenschaften 1. und 2. sind dann trivial! Die Eigenschaften 2. und 3. übersetzen sich in:*

2. Falls die Einschränkung einer Funktion auf alle offenen Mengen einer Überdeckung von U null ist, so ist die Funktion null auf U.
3. Falls Funktionen auf allen Mengen einer offenen Überdeckung von U gegeben sind, die auf Schnitten übereinstimmen, so verkleben sie zu einer Funktion auf U.
Die Eigenschaft 3. ist die entscheidende. Sie wird das **Garbenaxiom** *genannt. Für unsere Definition von regulärer Funktion folgt es aus der lokalen Natur der Definition! Analog zu Garben von k-Algebren kann man auch Garben (abelscher) Gruppen, von Ringen, Moduln, etc. betrachten.*
Unsere Garbe $U \mapsto \mathcal{O}(U)$ auf einer Varietät heisst auch die **Strukturgarbe**. *Sie allein bestimmt welche Abbildungen als Morphismen von Varietäten zugelassen sind (siehe Definition 1.10.4).*

Wir möchten insbesondere auch quasi-affine oder affine Varietäten mit quasi-projektiven oder projektiven vergleichen können. Erinnere aus 1.8.9 die Abbildungen

$$\varphi_i : \mathbb{A}^n \to U_i \subset \mathbb{P}^n.$$

Wir wissen bereits, dass sie Homoömorphismen sind. Es stellt sich heraus, dass die folgende einfache Definition eines Morphismus zwischen Varietäten V, W, die sowohl (quasi-)affin als auch (quasi-)projektiv sein dürfen, φ_i zu Isomorphismen von Varietäten macht (siehe Proposition 1.10.7).

Definition 1.10.4. *Wir nennen eine quasi-affine, affine, quasi-projektive oder projektive Varietät V einfach eine* **Varietät.** *Ein* **Morphismus** *$\varphi : V \to W$ zwischen zwei Varietäten ist eine stetige Abbildung so, dass für alle $p \in W$, offene Umgebungen $U \ni p$ und $f : U \to \mathbb{A}^1$ regulär (siehe 1.9.1), die Funktion $f \circ \varphi$ (der Rückzug von f) wieder regulär ist.*

Bemerkung 1.10.5. Achtung: *Wir hatten bereits den Begriff eines Morphismus von affinen Varietäten $V \to W$ definiert (1.4.1). Wir müssen überprüfen, dass die neue Definition in diesem Spezialfall mit der alten übereinstimmt. Seien also V und W affine Varietäten. Es ist klar, dass eine polynomiale Funktion (also ein Morphismus von affinen Varietäten nach der alten Definition) $\varphi : V \to W$ nach der neuen Definition ein Morphismus von Varietäten ist. In der Tat ist φ stetig (1.7.4) und der Rückzug von regulären Funktionen ist regulär. Sei umgekehrt $\varphi : V \to W$ ein Morphismus von Varietäten nach der neuen Definition, wobei V und W affin sind. Sei $W \subset \mathbb{A}^n$. Es gilt dann für die Funktionen $x_i : W \to \mathbb{A}^1$, dass*

$$\varphi(\lambda) = [(x_1 \circ \varphi)(\lambda), \ldots, (x_n \circ \varphi)(\lambda)].$$

Da nach Definition die Funktionen $x_i \circ \varphi$ regulär auf V sind, und nach Proposition 1.10.1 also Polynome, folgt, dass φ eine polynomiale Funktion ist.

Bemerkung 1.10.6. *Insbesondere bekommen wir durch Definition 1.10.4 einen Begriff von der Isomorphie zweier projektiver Varietäten.* Achtung: *Wenn $V \subset \mathbb{P}^n, W \subset \mathbb{P}^n$ zwei* isomorphe *projektive Varietäten sind, so ist i.A.*

$$k[X_0, \ldots, X_n]/I(V) \ncong k[X_0, \ldots, X_n]/I(W).$$

Mit anderen Worten: Der homogene Koordnatenring einer projektiven Varietät ist keine Isomorphie-Invariante!

Proposition 1.10.7. *Der Morphismus*

$$\varphi_i : \mathbb{A}^n \to U_i \subset \mathbb{P}^n$$

wobei $U_i = \mathbb{P}^n \setminus PV(X_i)$, ist ein Isomorphismus von Varietäten.

Wir wissen bereits, dass φ_i und die Umkehrung stetig bzgl. der Zariski-Topologie sind. Mit anderen Worten bedeutet die Aussage der Proposition also nur, dass die Definition von regulärer Funktion im affinen mit der Definition von regulärer Funktion im projektiven kompatibel ist (siehe 1.9.1 für diese Definitionen)!

Beweis. Wir müssen noch beweisen, dass der Rückzug unter φ_i und φ_i^{-1} von regulären Funktionen regulär ist. Für den Fall von φ_i genügt es, das folgende zu zeigen. Seien F, G homogene Polynome vom selben Grad, dann ist

$$\mu \mapsto \frac{F(\varphi_i(\mu))}{G(\varphi_i(\mu))}$$

eine reguläre Funktion auf der offenen Menge $\varphi_i^{-1}U_G$, wobei der Ausdruck bedeutet, dass im Zähler und Nenner dieselben homogenen Koordinaten gewählt werden müssen. Dann ist der Ausdruck wohldefiniert, d.h. nicht von dieser Wahl der homogenen Koordinaten abhängig.
Wir haben aber $\varphi_i^{-1}U_G = U_{G\circ\widetilde{\varphi}_i}$ und

$$\frac{F(\varphi_i(\mu))}{G(\varphi_i(\mu))} = \frac{F\circ\widetilde{\varphi}_i(\mu)}{G\circ\widetilde{\varphi}_i(\mu)}$$

(da wir beliebige homogene Koordinaten wählen dürfen, sind insbesondere die mit $\mu_i = 1$ in Ordnung). $F\circ\widetilde{\varphi}_i$ und $G\circ\widetilde{\varphi}_i$ sind aber Polynome.
Umgekehrt sei

$$\psi : \lambda \mapsto \frac{f(\lambda)}{g(\lambda)}$$

eine reguläre Funktion auf $U_g \subset \mathbb{A}^n$. Behauptung $\psi = \widetilde{\psi}\circ\varphi_i$, wobei

$$\widetilde{\psi} : \mu \mapsto \frac{(X_i^k f(\frac{X_0}{X_i},\ldots,\frac{X_{i-1}}{X_i},\frac{X_{i+1}}{X_i},\ldots,\frac{X_n}{X_i}))(\mu)}{(X_i^k g(\frac{X_0}{X_i},\ldots,\frac{X_{i-1}}{X_i},\frac{X_{i+1}}{X_i},\ldots,\frac{X_n}{X_i}))(\mu)}.$$

Hierbei ist X_i^k eine geeignete Potenz, welche dafür sorgt, dass beide Funktionen Polynome sind. Dies ist aber klar, denn

$$(X_i^k f(\frac{X_0}{X_i},\ldots,\frac{X_{i-1}}{X_i},\frac{X_{i+1}}{X_i},\ldots,\frac{X_n}{X_i}))\circ\widetilde{\varphi}_i = f$$

und

$$(X_i^k g(\frac{X_0}{X_i},\ldots,\frac{X_{i-1}}{X_i},\frac{X_{i+1}}{X_i},\ldots,\frac{X_n}{X_i}))\circ\widetilde{\varphi}_i = g.$$

Die Gleichung $\psi = \widetilde{\psi}\circ\varphi_i$ zeigt, dass die Funktion ψ auf $\varphi_i(U_g)$ durch die reguläre Funktion $\widetilde{\psi}$ gegeben ist. □

Korollar 1.10.8. *Sei $V \subset \mathbb{P}^n$ eine projektive Varietät. Dann existiert eine offene Überdeckung $V = \bigcup_{i=0}^n V_i$ so, dass alle V_i isomorph zu affinen Varietäten sind.*

Beweis. Dies folgt aus der Proposition. Die gesuchten V_i sind einfach die $U_i \cap V$. Beachte, dass $U_i \cap V$ in U_i abgeschlossen ist. □

Die Proposition 1.10.7 ist der Spezialfall $V = \mathbb{P}^n, G = X_i$ einer viel weitergehenden Aussage:
Sei U_G eine standard-offene Menge in einer *irreduziblen* projektiven Varietät V.
Jedes Element $\frac{F}{G^m} \in (k[X_0,\ldots,X_n]/I(V))[G^{-1}]$ vom Grad 0 (bzgl. der Graduierung aus 1.9.10), also wobei $F, G^m \in (k[X_0,\ldots,X_n]/I(V))_i$ für dasselbe i, definiert eine reguläre Funktion auf U_G:

$$\lambda \mapsto \frac{F(\lambda)}{G^m(\lambda)}$$

(Überlegen Sie sich die Wohldefiniertheit!).

Proposition 1.10.9. *Sei $V \subset \mathbb{P}^n$ eine* irreduzible *projektive Varietät und $G \in k[X_0,\ldots,X_n]/I(V)$ ein* nicht konstantes *homogenes Element. Dann ist U_G isomorph zu einer affinen Varietät V'. Wir haben (vermöge der Assoziation oben)*

$$\mathcal{O}(U_G) = \mathcal{O}(V') \cong (k[X_0,\ldots,X_n]/I(V))[G^{-1}]_0$$

(Elemente vom Grad 0).

Beweisskizze (für Interessierte). Es genügt, dies für $V = \mathbb{P}^n$ zu zeigen. Begründung: Sei $\widetilde{G} \in k[X_0,\ldots,X_n]$ ein (homogener) Lift von G. Wir haben $U_G = V \cap U_{\widetilde{G}}$ und dies ist abgeschlossen in $U_{\widetilde{G}}$. Falls $U_{\widetilde{G}}$ affin ist, so ist also auch U_G affin. Falls wir ferner annehmen, dass $U_{\widetilde{G}} \cong k[X_0,\ldots,X_n,\widetilde{G}^{-1}]_0$, so gilt auch $\mathcal{O}(U_G) \cong (k[X_0,\ldots,X_n]/I(V))[G^{-1}]_0$, denn

$$k[X_0,\ldots,X_n,\widetilde{G}^{-1}]_0/(I(V)[\widetilde{G}^{-1}]_0) = (k[X_0,\ldots,X_n]/I(V))[G^{-1}]_0$$

(Übung).
Es fehlt also die Aussage für $V = \mathbb{P}^n$ zu zeigen. Sei d der Grad von G. Sei $N = \binom{n+d}{n} - 1$. Seien $M_0, \ldots, M_N$ alle Monome vom Grad d in $k[X_0, \ldots, X_n]$. Betrachte die Abbildung (die sogenannte **Veronese Einbettung**)

$$v_d : \mathbb{P}^n \to \mathbb{P}^N$$

$$\lambda \mapsto [M_0(\lambda), \ldots, M_N(\lambda)]$$

Beweise als Übung, dass $v_d(\mathbb{P}^n)$ abgeschlossen ist, und $v_d : \mathbb{P}^n \to v_d(\mathbb{P}^n)$ ein Isomorphismus. In diesem Fall ist die Abbildung durch einen Morphismus der graduierten homogenen Koordinatenringe (der allerdings die Graduierung mit d multipliziert)

$$\begin{aligned} \Phi_d : k[Y_0, \ldots, Y_N] &\to k[X_0, \ldots, X_n] \\ Y_i &\mapsto M_i \end{aligned}$$

gegeben. Da $G = \sum_i \alpha_i M_i$ für gewisse $\alpha_i \in k$, folgt $v_d(U_G) = v_d(\mathbb{P}^n) \cap U_{G'}$ für $G' = \sum_i \alpha_i Y_i$!
Wiederum lassen wir als Übung, dass Φ_d einen Isomorphismus

$$k[Y_0, \ldots, Y_N]/I(v(\mathbb{P}^n))[G'^{-1}]_0 \cong k[X_0, \ldots, X_n, G^{-1}]_0$$

induziert.
Indem wir wieder die Behauptung vom Anfang des Beweises verwenden, genügt es also die Aussage für $\mathbb{P}^n$ und ein G' vom Grad 1 zu beweisen. Durch Koordinatenwechsel können wir annehmen, dass $G' = X_i$. Dann ist aber $U_G = \varphi_i(\mathbb{A}^n)$ und wir haben die Aussage in 1.10.7 gezeigt. Ausserdem ist

$$k[x_1, \ldots, x_n] \cong k[X_0, \ldots, X_n, X_i^{-1}]_0$$

vermöge der Abbildung

$$x_j \mapsto \frac{X_j}{X_i}.$$

$\square$

Bemerkung 1.10.10. *Im affinen gilt dieselbe Aussage. Eine standard-offene Menge $U_g \subset V$ in einer affinen Varietät ist wieder isomorph zu einer affinen Varietät. Falls $V = V(f_1, \ldots, f_m) \subset \mathbb{A}^n$ so gilt $U_g \cong V(f_1, \ldots, f_m, gx_{n+1} - 1) \subset \mathbb{A}^{n+1}$ und — dies ist ja schon die Aussage der Proposition 1.10.1 — $\mathcal{O}(U_g) = \mathcal{O}(V)[g^{-1}] = k[x_1, \ldots, x_n, x_{n+1}]/(f_1, \ldots, f_m, gx_{n+1} - 1)$. Den Beweis lassen wir als Übung (direkter Beweis unter Benutzung von 1.10.1, oder als Korollar von 1.10.9 für $G = X_0 G'$, wobei G' eine Homogenisierung von g ist).*
Das allereinfachste Beispiel ist die Isomorphie von quasi-affinen Varietäten:

$$\mathbb{A}^1 \setminus \{[0]\} \cong V(xy - 1) \subset \mathbb{A}^2.$$

Überlegen Sie sich, wie hier die Abbildungen aussehen!

Im Kontrast zur vorigen Proposition gilt aber für eine *irreduzible* projektive Varietät V:

Proposition 1.10.11. *Für eine* irreduzible *projektive Varietät V gilt*

$$\mathcal{O}(V) = k.$$

Beweis. Sei ψ eine reguläre Funktion auf V. Proposition 1.10.1 zeigt: $\psi \circ \varphi_i = f_i$, wobei $f_i \in k[x_1, \ldots, x_n]/I(\varphi_i^{-1}(V))$.
Es gilt also für $\mu \in U_i$, dass

$$\psi(\mu) = (\frac{F_i}{X_i^{d_i}})(\mu),$$

wobei $F_i = \beta_i(f_i)$ und $d_i \in \mathbb{N}$. Für $\mu \in U_i \cap U_j$ gilt:

$$(\frac{F_i}{X_i^{d_i}})(\mu) = (\frac{F_j}{X_j^{d_j}})(\mu)$$

daher gilt:

$$X_i X_j (F_i X_j^{d_j} - F_j X_i^{d_i}) \in I(V)$$

Da V nach Voraussetzung irreduzibel und daher nach Proposition 1.7.8 $I(V)$ prim und natürlich o.B.d.A. $X_i, X_j \notin I(V)$ gilt:

$$F_i X_j^{d_j} - F_j X_i^{d_i} \in I(V)$$

Daraus folgt, dass das Element vom Grad 0

$$h = \frac{F_i}{X_i^{d_i}}$$

im Quotientenkörper $\mathrm{Quot}(k[X_0, \dots, X_n]/I(V))$ unabhängig von i ist. Wir müssen zeigen, dass es eine Konstante ist. Bezeichne $A := (k[X_0, \dots, X_n]/I(V))$. Es ist ein graduierter Ring, indem alle A_i endlich dimensionale k-Vektorräume sind. Behauptung: $hA_D \subset A_D$ wobei $D = \sum_i d_i$. Beweis: Jedes Monom $X_0^{a_0} \cdots X_n^{a_n}$ in A_D hat die Eigenschaft, dass mindestens für ein i gilt: $a_i \geq d_i$ und also daher das Monom durch $X_i^{d_i}$ teilbar ist. Da A_D ein endlich-dimensionaler Vektorraum ist, gibt es nach Cayley-Hamilton $a_i \in k$, so dass

$$(h^d + a_{d-1} h^{d-1} + \cdots + a_0) A_D = 0$$

Da $\mathrm{Quot}(A)$ nullteilerfrei ist, gilt $h^d + a_{d-1}h^{d-1} + \cdots + a_0 = 0$ und da k algebraisch abgeschlossen (und da $\mathrm{Quot}(A)$ ein Körper ist) gilt $h \in k$. □

Korollar 1.10.12. *Jeder Morphismus von Varietäten $V \to W$, wobei V projektiv und irreduzibel ist und W affin, ist konstant.*

Beweis. Übung, dies aus der vorigen Proposition abzuleiten. □

1.10.13. Sei V eine affine *irreduzible* Varietät und $\wp$ ein Primideal von $\mathcal{O}(V)$. Auch die *Lokalisierung* $\mathcal{O}(V)_\wp$ (siehe Definition 1.9.5) und der *Quotientenkörper* $\mathrm{Quot}(\mathcal{O}(V))$ haben eine geometrische Bedeutung:
$W := V(\wp) \subset V$ ist nach Proposition 1.7.8 eine nicht-leere irreduzible abgeschlossene Menge. Betrachte die Menge der Paare (U, f) aus einer offenen Menge U, so dass $W \cap U \neq \emptyset$ und $f : U \to \mathbb{A}^1$ eine reguläre Funktion ist. Wir nennen (U, f) und (U', f') äquivalent, falls $U'' \subset U \cap U'$ offen mit $W \cap U'' \neq \emptyset$ existiert, so dass f und f' auf U'' übereinstimmen. Überlegen Sie sich, dass dies eine Äquivalenzrelation definiert. Bezeichne die Menge der Äquivalenzklassen mit $\mathcal{O}(V)_W$. Multiplikation und Addition von Funktionen ergibt eine Ringstruktur auf dieser Menge.
Es gilt nun:

$$\mathcal{O}(V)_W \cong \mathcal{O}(V)_\wp$$

wobei $\mathcal{O}(V)_\wp$ die Lokalisierung von $\mathcal{O}(V)$ bei $\wp$ ist (siehe Definition 1.9.5). Insbesondere bekommen wir für $\wp = (0)$ dass $\mathcal{O}(V)_V = \mathrm{Quot}(\mathcal{O}(V))$ ein Körper ist.
Diese Tatsache erklärt schliesslich die Terminologie "lokal" bzw. "Lokalisierung": Elemente des lokalen Rings $\mathcal{O}(V)_\wp$, also der Lokalisierung von $\mathcal{O}(V)$ bei $\wp$, können als Funktionen aufgefasst werden, welche *lokal* in einer offenen Umgebung "um W" in obigem Sinne definiert sind.

Beweis. Wir geben die Abbildung von rechts nach links an: Ein Bruch $\frac{f}{g} \in \mathcal{O}(V)_\wp$, d.h. wobei $g \notin \wp$, wird auf die Äquivalenzklasse von $(U_g, \lambda \mapsto \frac{f(\lambda)}{g(\lambda)})$ abgebildet. Beachte, da $g \notin \wp$ folgt $W \cap U_g \neq \emptyset$. Da jede offene Menge durch solche standard-offenen Mengen überdeckt wird, folgt die Surjektivität der Abbildung. Die Injektivität und Wohldefiniertheit zu überprüfen, lassen wir als Übung. □

2 Moduln

2.1 Definition

Der Begriff “Modul” ist die Verallgemeinerung des Begriffes “Vektorraum” über Ringen.

Definition 2.1.1. *Sei R ein kommutativer Ring. Ein* R**-Modul** M *ist eine abelsche Gruppe, zusammen mit einer Abbildung*

$$\begin{aligned} R \times M &\to M \\ r, m &\mapsto r \cdot m \end{aligned}$$

so, dass die folgenden Eigenschaften erfüllt sind:

1. $1 \cdot m = m$,
2. $r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m$,
3. $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$,
4. $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$,

für alle $r, r_1, r_2 \in R$ und alle $m, m_1, m_2 \in M$.
Ein Modulhomomorphismus (lineare Abbildung) $\varphi : M_1 \to M_2$ zwischen zwei Moduln ist ein Gruppenhomomorphismus, welcher die Multiplikation respektiert, d.h. $\varphi(r \cdot m) = r \cdot \varphi(m)$ für alle $r \in R$ und $m \in M$.

Beobachte, dass dies genau dieselben Axiome sind, wie die des Vektorraumes, mit dem Unterschied, dass k (der Grundkörper) durch einen beliebigen Ring R ersetzt wurde. Da man in einem Ring nicht invertieren kann, gelten viele der grundlegenden Tatsachen über Vektorräume *nicht* mehr für beliebige Moduln. Z.B. besitzt ein Modul im allgemeinen keine Basis!
Wir lassen oft den Punkt “$\cdot$” bei der Multiplikation mit Elementen aus R weg, und wegen Gesetz 2. des Moduls schreiben wir auch einfach $r_1 r_2 m$ für $r_1 \cdot (r_2 \cdot m)$.
Genau wie für Vektorräume definieren wir die folgenden Begriffe:

Definition 2.1.2. *Eine Teilmenge $E \subset M$ heisst* **Erzeugendensystem**, *falls jedes Element $m \in M$ eine Darstellung*

$$m = \alpha_1 e_1 + \cdots + \alpha_l e_l$$

für gewisse $e_i \in E$ und $\alpha_i \in R$ besitzt. Ein Erzeugendensystem heisst **Basis**, *falls diese Darstellung für alle m* eindeutig *ist. Ein Modul, welcher ein* endliches *Erzeugendensystem besitzt heisst* **endlich erzeugt**. *Ein Modul, welcher eine Basis besitzt, heisst* **frei**.

Beispiel 2.1.3. *Das einfachste Beispiel eines Moduls ist der Modul der Spaltenvektoren R^n. Er besteht aus n-Tupeln*

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

mit $\alpha_i \in R$. Spaltenvektoren werden genauso addiert und mit Elementen aus R multipliziert, wie man das von Vektoren mit Einträgen in einem Körper gewohnt ist. Moduln dieser Bauart sind endlich erzeugt *und* frei *(siehe Definition 2.1.2). Umgekehrt ist (wie bei Vektorräumen) jeder endlich erzeugte, freie Modul isomorph zu einem R^n.*

Wie für Vektorräume gilt:

Lemma 2.1.4. *Sei R ein kommutativer Ring, welcher nicht der Nullring ist. Falls $\varphi : R^n \to R^m$ ein Isomorphismus von R-Moduln ist, so folgt $m = n$.*

Beweisskizze. O.B.d.A. können wir annehmen, dass $m \leq n$. Wie in der linearen Algebra können wir φ und φ^{-1} durch $m \times n-$ bzw. $n \times m-$Matrizen A und B mit Einträgen in R ausdrücken. Es gilt dann offensichtlich $AB = E_m$ und $BA = E_n$. In der Gleichung $BA = E_n$ können wir die Matrizen durch Auffüllen von Nullen zu quadratischen Matrizen machen, so dass sich das Produkt nicht ändert:

$$\begin{pmatrix} B & 0_{n \times (n-m)} \end{pmatrix} \begin{pmatrix} A \\ 0_{(n-m) \times n} \end{pmatrix} = E_n.$$

Nun gilt aber beliebige quadratische $n \times n$-Matrizen P und Q die Gleichung $\det(P)\det(Q) = \det(PQ)$. (Für deren Beweis wird lediglich verwendet, dass die Matrixeinträge aus einem kommutativen Ring stammen — ansonsten wäre es noch nicht einmal möglich $\det(P)$ sinnvoll zu definieren.) Falls $m < n$ haben aber unsere beiden mit Nullen aufgefüllten Matrizen die Determinante 0 und die Matrix auf der rechten Seite hat Determinante $1 \neq 0$. Daraus folgt, dass $m = n$ sein muss. □

Dieses Lemma zeigt, dass die folgende Definition sinnvoll ist.

Definition 2.1.5. *Wir nennen M einen freien R-Modul* **vom Rang** *n, falls $M \cong R^n$, oder äquivalent, falls er eine Basis der Kardinalität n besitzt.*

Es hat historische Gründe, dass man bei Moduln hier vom "Rang" und nicht von der "Dimension" spricht. *Bemerkung:* Für die Gültigkeit des Lemmas ist entscheidend, dass R kommutativ ist. Es gibt tatsächlich nicht-kommutative Ringe R so, dass $R^1 \cong R^2 \cong R^3 \cong \cdots$!

2.2 Weitere Beispiele

Beispiel 2.2.1. *Für zwei R-Moduln M_1 und M_2 ist die direkte Summe*

$$M_1 \oplus M_2$$

(definiert wie für Vektorräume) wieder ein R-Modul.

Beispiel 2.2.2. *Falls $R = k$ ein Körper ist, dann ist ein k-Modul einfach dasselbe wie ein k-Vektorraum.*

Beispiel 2.2.3. *Falls $R = \mathbb{Z}$, so ist ein R-Modul dasselbe wie eine abelsche Gruppe. Mit anderen Worten: Für jede abelsche Gruppe M gibt es genau eine Möglichkeit, eine Abbildung $\mathbb{Z} \times M \to M$ so zu definieren, dass die Axiome 1.–4. erfüllt sind. Aus diesen folgt nämlich für $n \in \mathbb{N}$:*

$$n \cdot m = (\underbrace{1 + \cdots + 1}_{n\text{-mal}}) \cdot m = \underbrace{1 \cdot m + \cdots + 1 \cdot m}_{n\text{-mal}} = \underbrace{m + \cdots + m}_{n\text{-mal}}.$$

Genauso folgt:

$$(-n) \cdot m = ((-1) \cdot n) \cdot m = (-1) \cdot (\underbrace{m + \cdots + m}_{n\text{-mal}}) = -(\underbrace{m + \cdots + m}_{n\text{-mal}})$$

$$0 \cdot m = (1 + (-1)) \cdot m = m + (-m) = 0$$

Es gibt also nur eine Möglichkeit die Abbildung "$\cdot$" zu definieren. Umgekehrt definieren diese Gleichungen aber auch eine Funktion, die die Eigenschaften 1.–4. hat. Wir werden dieses Beispiel noch intensiv studieren. Diese so erhaltenden Moduln sind nicht immer frei. Zum Beispiel ist eine endliche abelsche Gruppe (ausser der trivialen Gruppe) niemals ein freier $\mathbb{Z}$-Modul!

Beispiel 2.2.4. *Sei R ein kommutativer Ring und I ein Ideal. Dann ist R/I ein R-Modul vermöge:*

$$\begin{aligned} R \times R/I &\to R/I, \\ r, x + I &\mapsto rx + I. \end{aligned}$$

(Überlegen Sie sich die Wohldefiniertheit!)

Beispiel 2.2.5. *Eine Verallgemeinerung des letzten Beispieles: Sei $\psi : R \to S$ ein Ringhomomorphismus. Dann ist S ein R-Modul vermöge der Abbildung:*

$$\begin{aligned} R \times S &\to S, \\ r, s &\mapsto \psi(r)s. \end{aligned}$$

Beispiel 2.2.6. *Sei R ein kommutativer Ring und I ein Ideal. Dann ist auch I selber ein R-Modul.* Übung: *Falls I frei ist, ist I ein Hauptideal. Die Umkehrung gilt, falls R nullteilerfrei ist.*

Beispiel 2.2.7. *Sei k ein Körper. Ein $k[X]$-Modul M ist dasselbe wie ein k-Vektorraum M zusammen mit einer linearen Abbildung $\gamma : M \to M$ in folgendem Sinne: Falls M ein $k[X]$-Modul ist, dann definiert*

$$\gamma_M : m \mapsto X \cdot m$$

eine k-lineare Abbildung $M \to M$. Unter dieser Zuordnung sind Modulhomomorphismen $M_1 \to M_2$ genau diejenigen k-linearen Abbildungen $\psi : M_1 \to M_2$, welche $\psi\gamma_{M_1} = \gamma_{M_2}\psi$ erfüllen.
Umgekehrt, falls V ein k-Vektorraum ist und $\gamma : V \to V$ ein Endomorphismus, so definiert

$$\begin{aligned} k[X] \times V &\to V \\ p, v &\mapsto p(\gamma)v \end{aligned}$$

die Struktur eines $k[X]$-Moduls auf V.

Im allgemeinen sind Moduln kompliziert, aber falls R einfach strukturiert ist, ist die Theorie übersichtlicher. Wir haben das für den Fall, dass R ein Körper ist, schon gesagt: Dann hat man Vektorräume und alle Resultate der linearen Algebra gelten. Falls R ein Hauptidealring ist (z.B. $\mathbb{Z}$ und $k[X]$), dann gibt es noch immer eine einfache und schöne Theorie, die wir in Abschnitt 2.5 behandeln wollen. Dies gibt uns insbesondere Aufschluss über die Theorie des abelschen Gruppen (in Falle $R = \mathbb{Z}$) und über die Theorie der Vektorräume mit Endomorphismus (im Falle $R = k[X]$). Im letzteren Fall bekommen wir einen sehr eleganten Beweis der Existenz der Jordanschen Normalform.
Im nächsten Abschnitt werden wir sehen, dass schon eine gewisse Vereinfachung eintritt, falls der Ring R noethersch ist.
Wie für Vektorräume und Ringe, gibt es auch für Moduln den Begriff eines Quotienten. Wir formulieren dies wieder durch eine universelle Eigenschaft. Zunächst ist ein **Untermodul** $N \subset M$ eines Moduls eine Untergruppe mit der Eigenschaft $r \cdot n \in N$, für alle $r \in R$ und $n \in N$. Z.B. sind Kern und Bild eines Modulhomomophismus Untermoduln. Ein Untermodul von R ist dasselbe wie ein Ideal.

Proposition 2.2.8 (Homomorphiesatz)**.** *Sei R ein kommutativer Ring, M ein R-Modul und $N \subset M$ ein Untermodul. Dann existiert ein Modulhomomorphismus $p : M \to M/N$ mit $\ker(p) = N$ mit der folgenden universellen Eigenschaft: Für jeden Modul M' und Modulhomomorphismus $\varphi : M \to M'$ mit $\varphi(N) = 0$ existiert ein eindeutiger Modulhomomorphismus $\widetilde{\varphi} : M/N \to M'$ so, dass $\widetilde{\varphi} \circ p = \varphi$.*
Falls φ surjektiv ist, mit $\ker(\varphi) = N$, so ist $\widetilde{\varphi}$ ein Isomorphismus.

Beweis. Der Beweis ist ähnlich dem für Vektorräume, Gruppen oder Ringe. □

2.2.9. Manchmal ist es praktisch, die Tatsache, dass $M' \cong M/N$ (mit den Bezeichnungen der Proposition) anders zu formulieren: Eine Sequenz

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} M_4 \xrightarrow{\varphi_4} M_5$$

von Modulhomomorphismen soll **exakt** heissen, falls jeweils $\ker(\varphi_{i+1}) = \mathrm{im}(\varphi_i)$, also falls der Kern eines Modulhomomorphismus in der Sequenz gleich dem Bild des vorigen ist. Insbesondere ist $\varphi_{i+1} \circ \varphi_i = 0$, aber dies ist nicht hinreichend.
Betrachte nun die Sequenz

$$0 \xrightarrow{\varphi_1} N \xrightarrow{\varphi_2} M \xrightarrow{\varphi_3} M' \xrightarrow{\varphi_4} 0 \tag{14}$$

wobei 0 der Nullmodul ist und φ_1, φ_4 die Nullabbildungen, φ_2 die Inklusion $N \hookrightarrow M$ und φ_3 irgendeine Abbildung $M \to M'$, wie in der Proposition.
Behauptung: Es gilt: $M' \cong M/N$ genau dann, wenn die Sequenz (14) exakt ist.
Beweis: Die Aussage $\mathrm{im}(\varphi_1) = \ker(\varphi_2)$ bedeutet gerade, dass φ_2 injektiv ist, also gerade, dass N ein Untermodul von M ist (bzw. genauer: durch φ_2 mit einem Untermodul von M identifiziert wird).
Die Aussage $\mathrm{im}(\varphi_2) = \ker(\varphi_3)$ bedeutet gerade, dass $\ker(\varphi_3) = N$ und die Aussage $\mathrm{im}(\varphi_3) = \ker(\varphi_4)$ bedeutet gerade, dass φ_3 surjektiv ist. Die Proposition gibt uns dann $M' \cong M/N$.

2.3 Noethersche Moduln

Definition 2.3.1. *Sei R ein kommutativer Ring. Ein Modul M heisst* **noethersch***, falls jeder Untermodul $N \subset M$ endlich erzeugt ist.*

Wie für Ideale gilt:

Proposition 2.3.2. *M ist noethersch, genau dann wenn jede unendliche aufsteigende Kette von Untermoduln*

$$N_1 \subset N_2 \subset N_3 \subset N_4 \subset \cdots$$

stationär wird.

Beweis. Der Beweis ist der gleiche wie für Ideale: siehe 1.6.2. □

Die Eigenschaft noethersch zu sein überträgt sich auf Untermoduln und Quotientenmoduln (und umgekehrt, wenn beide noethersch sind). Wir können das im Hinblick auf 2.2.9 wie folgt formulieren:

Proposition 2.3.3. *Sei*

$$0 \longrightarrow M_1 \longrightarrow M \xrightarrow{p} M_2 \longrightarrow 0$$

eine exakte Sequenz von R-Moduln. Dann ist M genau dann noethersch, wenn M_1 und M_2 noethersch sind.

Beweis. Wir beweisen zunächst die Richtung M noethersch $\Rightarrow M_1$ und M_2 noethersch. Sei

$$N_1 \subset N_2 \subset N_3 \subset N_4 \subset \cdots$$

eine aufsteigende Kette von Untermoduln von M_1. Da M_1 ein Untermodul von M ist, sind die N_i insbesondere auch Untermoduln von M. Die Kette wird daher stationär, da M noethersch ist. Sei

$$N_1 \subset N_2 \subset N_3 \subset N_4 \subset \cdots$$

eine aufsteigende Kette von Untermoduln von M_2. Dann bilden auch die Urbilder unter $p : M \to M_2$ eine aufsteigende Kette von Untermoduln von M:

$$p^{-1}(N_1) \subset p^{-1}(N_2) \subset p^{-1}(N_3) \subset p^{-1}(N_4) \subset \cdots$$

Die Kette wird stationär, da M noethersch ist. Es gilt trivialerweise $p(p^{-1}(m)) = m$ für alle $m \in M_2$, durch Anwenden von p erhalten wir also die ursprüngliche Sequenz zurück. Sie wird also auch stationär.
Wir zeigen nun die Richtung: M_1 und M_2 noethersch $\Rightarrow M$ noethersch. Sei N ein Untermodul von M. Wir müssen zeigen, dass N endlich erzeugt ist. Es ist klar, dass wir eine exakte Sequenz

$$0 \longrightarrow M_1 \cap N \longrightarrow N \xrightarrow{p} p(N) \longrightarrow 0$$

haben. Nun sind $p(N)$ als Untermodul von M_2 und $M_1 \cap N$ als Untermodul von M_1 nach Voraussetzung endlich erzeugt, d.h.

$$p(N) = Re_1 + \cdots + Re_l, \qquad M_1 \cap N = Rf_1 + \cdots + Rf_k.$$

Wähle für alle i ein Urbild $\widetilde{e}_i \in N$ von e_i unter p.

Behauptung:

$$N = Rf_1 + \cdots + Rf_k + R\widetilde{e}_1 + \cdots + R\widetilde{e}_l.$$

Beweis: Sei $n \in N$ gegeben. Dann gibt es $\alpha_i \in R$ so, dass $p(n) = \alpha_1 e_1 + \cdots \alpha_l e_l$. Nun ist

$$p(n - \alpha_1\widetilde{e}_1 - \cdots - \alpha_l\widetilde{e}_l) = p(n) - \alpha_1 e_1 - \cdots - \alpha_l e_l = 0.$$

Daher ist $(n - \alpha_1\widetilde{e}_1 - \cdots - \alpha_l\widetilde{e}_l) \in N \cap M_1$ und daher eine Linearkombination der f_i. □

Proposition 2.3.4. *Falls R noethersch ist, dann gilt*

$$M \text{ noethersch } \Leftrightarrow M \text{ endlich erzeugt.}$$

Beweis. Falls M noethersch ist, ist M per Definition endlich erzeugt. Falls M endlich erzeugt ist (durch n Elemente), gibt es nach Definition eine exakte Sequenz

$$0 \longrightarrow \ker(\psi) \longrightarrow R^n \xrightarrow{\psi} M \longrightarrow 0$$

Es genügt also nach Proposition 2.3.3 zu zeigen, dass R^n noethersch ist. Betrachte die exakte Sequenz

$$0 \longrightarrow R \longrightarrow R^n \longrightarrow R^{n-1} \longrightarrow 0$$

wobei die beiden Abbildungen die Einbettung des ersten Eintrages und die Projektion auf die letzten $n-1$ Einträge sind. Induktion über n und Proposition 2.3.3 zeigen uns also, dass es reicht, zu beweisen, dass R noethersch ist (als R-Modul). Nun sind aber die Untermoduln von R als R-Modul genau die Ideale. Sie sind endlich erzeugt, da R ein noetherscher Ring ist. □

2.4 Lokalisierung von Moduln

Sei S eine multiplikativ abgeschlossene Teilmenge von R und M ein R-Modul, dann definieren wir auf

$$S \times M = \{\frac{m}{g} \mid m \in M, g \in S\}$$

wiederum die Äquivalenzrelation:

$$\frac{m_1}{g_1} \sim \frac{m_2}{g_2} \Leftrightarrow \exists s \in S : s(g_2 m_1 - g_1 m_2) = 0.$$

Man rechnet nach, dass die Menge der Äquivalenzklassen einen $R[S^{-1}]$-Modul bildet (siehe 1.9.4). Wir bezeichnen ihn mit $M[S^{-1}]$, bzw. falls $S = R \setminus \wp$ auch mit $M_\wp$.

Proposition 2.4.1. *Für einen R-Modul M sind die folgenden Aussagen äquivalent:*

1. $M = 0$,
2. $M_\wp = 0$ *für alle Primideale* $\wp \subset R$,
3. $M_\mathfrak{m} = 0$ *für alle maximalen Ideale* $\mathfrak{m} \subset R$.

Beweis. Übung. □

Dies ist oft praktisch, da lokale Ringe viel einfacher zu verstehen sind.

Proposition 2.4.2. *Sei*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

eine exakte Sequenz von R-Moduln und S eine multiplikativ abgeschlossene Teilmenge von R. Dann ist auch

$$0 \longrightarrow M_1[S^{-1}] \longrightarrow M[S^{-1}] \longrightarrow M_2[S^{-1}] \longrightarrow 0$$

exakt.

Beweis. Übung. □

2.5 Moduln über Hauptidealringen

Wir möchten in diesem Abschnitt endlich erzeugte Moduln über Hauptidealringen klassifizieren. Erinnere:

Definition 2.5.1. *Ein kommutativer Ring R heisst* **Hauptidealring***, wenn er nullteilerfrei ist und jedes Ideal ein Hauptideal ist, also von einem Element erzeugt wird.*

Z.B. ist $\mathbb{Z}$ ein Hauptidealring, Polynomringe $k[x]$ in einer Variablen über einem Körper sind Hauptidealringe, oder allgemeiner Ringe, in denen man eine "Division mit Rest" durchführen kann, sogenannte euklidische Ringe.
Zunächst haben wir den folgende Satz:

Satz 2.5.2 (Elementarteilersatz)**.** *Sei R ein Hauptidealring und A eine $m \times n$-Matrix mit Einträgen in R. Es gibt dann eine* invertierbare *$m \times m$-Matrix P und eine* invertierbare *$n \times n$-Matrix Q so, dass QAP^{-1} die Gestalt*

$$\begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_k & & \\ & & & 0 & \\ & & & & \vdots \end{pmatrix}$$

hat. Dabei gilt $(d_1) \supset (d_2) \supset (d_3) \supset \cdots \supset (d_k)$.
k und die Ideale (d_i) sind dadurch eindeutig bestimmt. Die (d_k) heissen die **Elementarteiler** *von A.*

Wir benötigen zunächst ein Lemma

Lemma 2.5.3. *Sei R ein Hauptidealring und $(a, b) = (x)$. Dann gibt es eine invertierbare $2 \times 2-$Matrix P so, dass*

$$P \begin{pmatrix} a & * \\ b & * \end{pmatrix} = \begin{pmatrix} x & * \\ * & * \end{pmatrix}$$

oder auch

$$\begin{pmatrix} a & b \\ * & * \end{pmatrix} {}^tP = \begin{pmatrix} x & * \\ * & * \end{pmatrix}$$

Beweis. Wegen der Idealgleichung gibt es $\lambda, \mu \in R$ mit

$$\lambda a + \mu b = x.$$

Ausserdem gilt:

$$a = \alpha x, \qquad b = \beta x,$$

für gewisse $\alpha, \beta \in R$, da a und b im Ideal (x) liegen. Da R nullteilerfrei ist, dürfen wir x kürzen: $\lambda\alpha + \mu\beta = 1$. Es gilt dann

$$\begin{pmatrix} \lambda & \mu \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} a & * \\ b & * \end{pmatrix} = \begin{pmatrix} x & * \\ * & * \end{pmatrix}$$

und die linke Matrix ist invertierbar. Die andere Gleichung folgt durch Transposition. □

Beweis des Satzes. Die Strategie besteht darin, A durch Multiplikation mit invertierbaren Matrizen der folgenden Typen von rechts bzw. links zu multiplizieren, bis sie die gewünschte Gestalt hat:

1. Für zwei Indizes i, j, Matrizen in denen höchstens die folgenden Einträge von Null verschieden sind: $a_{kk} = 1$ für $k \neq i, j$ und $a_{ii}, a_{ij}, a_{ji}, a_{jj}$ beliebig, so dass

$$\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix}$$

invertierbar ist.

2. Permutationsmatrizen zu einer Transposition.

Die gesuchten Matrizen P^{-1} und Q sind dann einfach die Produkte der entsprechenden Matrizen.
Falls $A = 0$ ist die Aussage trivial. Durch Vertauschen von Zeilen oder Spalten (d.h. Multiplikation mit Matrizen vom Typ 2 von links oder rechts) können wir also zunächst annehmen, dass a_{11} nicht 0 ist. Wir möchten erreichen, dass A die Blockgestalt:

$$\begin{pmatrix} a_{11} & 0 \\ 0 & B \end{pmatrix}$$

hat, wobei a_{11} jeden Eintrag von B teilt. Die Aussage des Satzes folgt dann durch Induktion. Wir unterscheiden dazu die folgenden Fälle:

1. Es gibt einen Eintrag a_{1j} oder a_{i1} welcher nicht durch a_{11} teilbar ist. Wir haben dann im ersten Fall: $(a_{11}, a_{1j}) = (x)$ für ein $x \in R$, da R ein Hauptidealring ist. Beachte, dass $(a_{11}) \subsetneq (x)$! D.h., dass wir durch Multiplikation mit einer geeigneten Matrix vom Typ 1 von links erreichen können, dass der obere linke Eintrag x wird (Lemma!). Genauso im zweiten Fall durch Multiplikation von rechts. Wir beginnen von vorn.

2. Alle Einträge a_{1j} oder a_{i1} (für $j \neq 1$ bzw. $i \neq 1$) sind durch a_{11} teilbar aber nicht alle 0. Durch Abziehen der entsprechenden Vielfachen der ersten Spalte bzw. Zeile von der i-ten Spalte bzw. j-ten Zeile sind wir im nächsten Fall. Beachte, dass die entsprechende Operation ebenfalls durch Multiplikation mit einer Matrix vom Typ 1 bewerkstelligt werden kann.

3. Alle Einträge a_{1j} oder a_{i1} (für $j \neq 1$ bzw. $i \neq 1$) sind Null, aber ein Eintrag a_{ij} ist nicht durch a_{11} teilbar. Wir addieren dann die i-te Spalte zur 1. Spalte und gehen zu Fall 1.

4. Alle Einträge a_{1j} oder a_{i1} (für $j \neq 1$ bzw. $i \neq 1$) sind Null und a_{11} teilt alle anderen Einträge der Matrix. Wir haben dann unser Ziel erreicht.

Beachte, dass dieser Algorithmus zum Ende kommt, da wir entweder zum jeweils nächsten Fall übergehen, oder das Ideal (a_{11}) durch ein Ideal (a'_{11}) mit $(a_{11}) \subsetneq (a'_{11})$ ersetzt wird. Würde der Algorithmus nicht stoppen, bekämen wir also eine unendliche strikt aufsteigende Kette von Idealen, was nicht sein kann, da R noethersch ist.
Die Eindeutigkeit der (d_i) werden wir nicht zeigen. □

Korollar 2.5.4. *Sei R ein Hauptidealring und M ein endlich erzeugter freier Modul vom Rang m. Dann ist jeder Untermodul von M frei vom Rang $\leq m$.*

Beweis. Sei N ein Untermodul von R^m. Da N endlich erzeugt ist (Proposition 2.3.3) gibt es einen Modulhomorphismus $\iota : R^n \to R^m$, deren Bild N ist. Nach dem Satz gibt es daher Basen von R^n und R^m so, dass ι durch die Matix

$$\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \\ & & & \vdots \end{pmatrix}$$

gegeben wird. N ist also bzgl. dieser Basis auf R^m gleich dem Untermodul $Rd_1e_1 + \cdots + Rd_ke_k$. Dieser ist frei, da R Nullteilerfrei ist. Ausserdem ist $k \leq m$. □

Korollar 2.5.5 (Struktursatz für endlich erzeugte Moduln über Hauptidealringen)**.** *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es $k, l \in \mathbb{N}_0$ und*

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_k) \oplus R^l,$$

wobei $(d_1) \supset \cdots \supset (d_k)$. Die (d_i) sind eindeutig durch diese Bedingung bestimmt.

Beweis. Wir haben eine Surjektion $p : R^m \to M$, da M endlich erzeugt ist. Das vorige Korollar impliziert, dass $\ker(p)$ frei ist. Es gibt daher eine exakte Sequenz

$$0 \longrightarrow R^k \xrightarrow{A} R^m \xrightarrow{p} M \longrightarrow 0$$

wobei A eine $k \times m$-Matrix mit Einträgen in R ist. Nach Satz 2.5.2 gibt es invertierbare Matrizen P und Q so dass QAP^{-1} die Gestalt

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_k \\ \hline & 0 & \end{pmatrix}$$

hat, wobei $(d_1) \supset \cdots \supset (d_k)$. Betrachte die exakte Sequenz

$$0 \longrightarrow R^k \xrightarrow{D} R^m \xrightarrow{p'} M' \longrightarrow 0$$

wobei M' der Quotient ist. Hier gilt offensichtlich

$$M' \cong R/(d_1) \oplus \cdots \oplus R/(d_k) \oplus R^{m-k}.$$

Wir behaupten, dass $M \cong M'$ ist (dies ist gerade die Aussage des Korollars). Betrachte das Diagramm von Modulhomomorphismen

$$\begin{tikzcd} 0 \arrow[r] & R^k \arrow[r, "A"] \arrow[d, "P"] & R^m \arrow[r, "p"] \arrow[d, "Q"] & M \arrow[r] \arrow[d, dotted, "\psi"] & 0 \\ 0 \arrow[r] & R^k \arrow[r, "D"] & R^m \arrow[r, "p'"] & M' \arrow[r] & 0 \end{tikzcd}$$

Hier definieren P und Q jeweils Isomorphismen (da die Matrizen invertierbar sind). Ausserdem kommutiert das linke Quadrat, d.h. es gilt: $QA = DP$. Wir behaupten, dass wir auf genau eine Weise eine Abbildung ψ definieren können, so dass auch das rechte Quadrat kommutiert, d.h. $\psi p = p'Q$. Wir können ψ explizit konstruieren, durch $\psi(x + AR^k) := Qx + DR^k$ (man überlege sich die Wohldefiniertheit). Genauso können wir eine Abbildung in die andere Richtung konstruieren und sehen leicht, dass beide zueinander invers sind. Eine andere Möglichkeit ist, die universelle Eigenschaft des Quotientenmoduls zu verwenden: Die Abbildung $p'Q$ erfüllt $\ker(p'Q) = Q^{-1}\ker(p') = Q^{-1}DR^k = AP^{-1}R^k = AR^k$. Daher induziert sie einen *Isomorphismus* $\psi : M = R^m/AR^k \to M'$ so, dass $\psi p = p'Q$.
Die Eindeutigkeit der (d_i) kann man aus der Eindeutigkeit der (d_i) im Satz folgern. Wir lassen dies als Übung. □

Korollar 2.5.6 (Struktursatz für endlich erzeugte abelsche Gruppen)**.** *Sei M ein endlich erzeugte abelsche Gruppe. Dann gilt:*

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^l$$

wobei $d_1 | \cdots | d_k$. Die d_i können positiv gewählt werden und sind dann eindeutig durch die Teilerbedingung bestimmt.

Beweis. Dies ist der Spezialfall $R = \mathbb{Z}$ des vorigen Korollars. □

2.5.7. Wir wollen kurz erläutern, wie sich der Satz über die Jordanzerlegung einer Matrix mit Einträgen in einem algebraisch abgeschlossenen Körper k aus dem Struktursatz 2.5.5 ergibt. Sei V ein endlich dimensionaler k-Vektorraum und φ ein Endomorphismus von V. Wir können V wie in Beispiel 2.2.7 als $k[x]$-Modul auffassen, in dem Multiplikation mit x durch Anwenden von φ erfolgt. Korollar 2.5.5 gibt uns die Zerlegung

$$V \cong k[x]/(p_1) \oplus \cdots \oplus k[x]/(p_k).$$

Beachte, dass kein freier Anteil auftritt, da $k[x]$ als k-Vektorraum unendliche Dimension hat. Da k algebraisch abgeschlossen ist, gilt $p_i = \prod (x-\alpha_j)^{n_j}$ und daher nach dem chinesischen Restsatz

$$k[x]/(p_i) = \bigoplus_j k[x]/(x-\alpha_j)^{n_j}.$$

Die Existenz einer Jordanschen Normalform ist also darauf zurückgeführt, dies für die Multiplikation mit x in einem Vektorraum der Gestalt

$$k[x]/(x-\alpha)^n$$

zu zeigen. *Behauptung:* Bzgl. der Basis bestehend aus den Restklassen von $(x-\alpha)^{n-1}, \ldots, (x-\alpha)^2, (x-\alpha), 1$ hat die Multiplikation mit x in diesem Vektorraum Jordankästchengestalt. Dies folgt sofort aus

$$x(x-\alpha)^j \equiv \alpha(x-\alpha)^j + (x-\alpha)^{j+1} \quad \text{modulo } (x-\alpha)^n$$

für $j < n-1$ bzw.

$$x(x-\alpha)^{n-1} \equiv \alpha(x-\alpha)^{n-1} \quad \text{modulo } (x-\alpha)^n.$$

Anmerkung: Die freie Präsentation von V, wie im Beweis von Satz 2.5.5, können wir in diesem Fall ganz explizit angeben: Wähle eine Basis von V, d.h. einen Isomorphismus $V \cong k^n$, so dass φ durch eine Matrix S gegeben wird. Überlegen Sie sich, dass es exakte Sequenz von $k[x]$-Moduln der folgenden Form gibt (wobei x auf k^n durch S wirkt):

$$0 \longrightarrow k[x]^n \xrightarrow{xE_n - S} k[x]^n \xrightarrow{p} k^n \longrightarrow 0$$

Um herauszufinden, welche Jordankästchen wir bekommen, genügt es also die Elementarteiler von $xE_n - S$ mit dem Verfahren aus Satz 2.5.2 zu bestimmen!

2.6 Ganzheit

Eine besondere Bedeutung kommt solchen Ringhomomorphismen $\psi : R \to S$ zu, mit der Eigenschaft, dass *S als R-Modul* endlich erzeugt ist (siehe auch Beispiel 2.2.5). Beachten Sie, dass dies sehr viel stärker ist, als als R-Algebra endlich erzeugt zu sein.

Definition 2.6.1. *1. Ein Ringhomomorphismus $\psi : R \to S$ so, dass S als R-Modul endlich erzeugt ist, heisst* **endliche** *Ringerweiterung.*

2. Ein Ringhomomorphismus $\psi : R \to S$ so, dass jedes $s \in S$ eine normierte *Gleichung der Form*

$$s^n + \psi(\alpha_{n-1})s^{n-1} + \cdots + \psi(\alpha_0) = 0$$

erfüllt, heisst **ganze** *Ringerweiterung.*

3. Ein Ringhomomorphismus $\psi : R \to S$ heisst **endlich erzeugte** *Ringerweiterung (bzw. S heisst endlich erzeugte R-Algebra), falls es $\xi_1, \ldots, \xi_n$ in S gibt, so dass jedes $x \in S$ eine polynomiale Darstellung der Form*

$$x = \sum_{i=1}^{N} \psi(\alpha_i)(\xi_1)^{m_{i,1}} \cdots (\xi_n)^{m_{i,n}}$$

mit $\alpha_i \in R$ und $m_{i,j} \in \mathbb{N}_0$ besitzt (vergleiche 1.5.10).

Falls R und S Körper sind, so ist eine endliche Ringerweiterung dasselbe, wie eine endliche Körpererweiterung. Genau wie für k-Algebren gilt, dass eine Ringerweiterung $\psi : R \to S$ genau dann endlich erzeugt ist, wenn es einen surjektiven Ringhomomorphismus $\widetilde{\psi} : R[x_1, \ldots, x_n] \to S$ gibt so dass $\widetilde{\psi} \circ \iota = \psi$ ist, wobei ι die Einbettung $R \to R[x_1, \ldots, x_n]$ ist.

Proposition 2.6.2. *1. Falls $\psi : R \to S$ und $\phi : S \to T$ endliche Ringerweiterungen sind, so ist auch $\phi \circ \psi : R \to T$ eine endliche Ringerweiterung.*

2. Für eine Ringerweiterung $\psi : R \to S$ gilt:

$$\textit{endlich erzeugt + ganz} \Leftrightarrow \textit{endlich.}$$

Beweis. 1. Dies ist derselbe Beweis, wie für Körpererweiterungen. Falls S als $\psi(R)$-Modul durch $\alpha_1, \ldots, \alpha_r$ erzeugt ist und T als $\phi(S)$-Modul durch $\beta_1, \ldots, \beta_l$, so erzeugen die Produkte $\phi(\alpha_1)\beta_1, \ldots, \phi(\alpha_r)\beta_l$ den $\phi(\psi(R))$-Modul T.
2. Wir können o.B.d.A. annehmen, dass ψ injektiv ist (indem wir ggfl. R durch $\psi(R)$ ersetzen). Wir zeigen zunächst die Richtung endlich-erzeugt + ganz $\Rightarrow$ endlich. Wegen 1. und Induktion nach der Anzahl der Erzeuger genügt es, dies für eine Ringerweiterung, welche (als R-Algebra) durch ein Element s erzeugt wird, zu zeigen. Nach Voraussetzung erfüllt s eine normierte Gleichung mit Koeffizienten in R. Der Ring S ist also ein Quotient von

$$R[s]/(s^n + \alpha_{n-1}s^{n-1} + \cdots + \alpha_0).$$

Diese Erweiterung wird aber als R-Modul durch die Elemente $1, s, s^2, \ldots, s^{n-1}$ erzeugt, da wir in einem beliebigen Polynom in s sukzessive Potenzen von s mit Exponent grösser oder gleich n mittels der Relation $s^n = -\alpha_{n-1}s^{n-1} - \cdots - \alpha_0$ durch kleinere Potenzen ersetzen können. Beachte, dass dies nur funktioniert, da der Koeffizient von s^n in dieser Relation 1 ist.
Wir zeigen nun die Richtung: endlich $\Rightarrow$ endlich-erzeugt + ganz. Sei S als R-Modul erzeugt durch $\alpha_1, \ldots, \alpha_r$. Dann erzeugen diese Elemente S erst recht auch als R-Algebra. Die Ringerweiterung $\psi : R \to S$ ist also endlich erzeugt. Sei nun $s \in S$ ein beliebiges Element. Es gilt dann nach Voraussetzung:

$$s\alpha_j = \sum \gamma_{ij}\alpha_i$$

für gewisse $\gamma_{ij} \in R$. Die Matrix $\Gamma = (\gamma_{ij})$ können wir als Endomorphismus von R^r auffassen und es gibt ein kommutatives Diagram von R-Modulhomomorphismen:

$$\begin{tikzcd} R^r \arrow[r, two heads] \arrow[d, "\Gamma"'] & S \arrow[d, "s"] \\ R^r \arrow[r, two heads] & S \end{tikzcd}$$

Daher gilt: Falls Γ eine Gleichung $x^m + \beta_{m-1}x^{m-1} + \cdots + \beta_0 = 0$ mit $\beta_i \in R$ erfüllt, dann auch s. Γ ist aber nach Cayley-Hamilton Nullstelle des eigenen charakteristischen Polynoms

$$\det(xE_n - \Gamma) = x^r - \beta_{r-1}x^{r-1} + \cdots \pm \beta_0.$$

Dieses ist normiert!
Bemerkung: Für den Beweis von Cayley-Hamilton wird wiederum nur verwendet, dass die Einträge der Matrix aus einem kommutativen Ring stammen. Z.B. gilt für jeden kommutativen Ring R die Gleichung

$$A \cdot \widetilde{A} = \det(A)E_n$$

für eine Matrix A sowie ihre Adjungierte mit Einträgen in R. Also gilt insbesondere

$$(xE_n - \Gamma) \cdot (\widetilde{xE_n - \Gamma}) = \det(xE_n - \Gamma)E_n.$$

Wenn wir (wie bei Vektorräumen) R^n zu einem $R[x]$-Modul machen, indem Multiplikation mit x die Multiplikation mit Γ bedeutet, dann gilt offensichtlich für jeden Vektor $v' \in R^n$ die Gleichung[8]

$$p((xE_n - \Gamma)v') = 0,$$

wobei $p : R[x]^n \to R^n$ der eindeutig bestimmte $R[x]$-Modulhomomorphismus ist, welcher $p(f \cdot v) = f(\Gamma)v$ für alle $f \in R[x]$ und $v \in R^n$ erfüllt. Daher durch Einsetzen von $v' = (\widetilde{xE_n - S})v$ für einen beliebiges $v \in R^n$:

$$p(\det(xE_n - \Gamma)v) = \det(xE_n - \Gamma)v = 0.$$

Da dies für alle $v \in R^n$ gilt, folgt genau die Aussage. □

[8] Hier wird v' als Vektor in $R[x]^n$ aufgefasst!

2.7 Endliche Morphismen von affinen Varietäten

Der Begriff der Endlichkeit hat eine geometrische Interpretation. Dazu definieren wir zunächst:

Definition 2.7.1. *Ein Morphismus von* affinen *Varietäten $\varphi : V \to W$ heisst* **endlich***, wenn die zugehörige Abbildung (siehe 1.4.4)*

$$\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$$

eine endliche Ringerweiterung ist.

Proposition 2.7.2. *Ein endlicher Morphismus $\varphi : V \to W$ ist abgeschlossen*[9] *und jeder Punkt hat höchstens endlich viele Urbilder.*

Es ist lehrreich, das folgende Beispiel zu betrachten: Sei $\varphi : V \to W$ ein Morphismus so, dass $\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$ injektiv und endlich ist und so, dass $\mathcal{O}(V)$ über $\mathcal{O}(W)$ durch ein Element s erzeugt wird und so dass gilt:

$$\mathcal{O}(V) \cong \mathcal{O}(W)[s]/(s^n + \beta_{n-1}s^{n-1} + \cdots + \beta_0).$$

Beachte: *Nicht jede* endliche injektive Ringerweiterung, welche von einem Element erzeugt wird, sieht so aus[10]!
Sei $W \subset \mathbb{A}^n$, dann ist also (wegen 1.4.4) V isomorph zur Varietät

$$V' = \{[\lambda_1, \ldots, \lambda_n, s] \in \mathbb{A}^{n+1} \mid [\lambda_1, \ldots, \lambda_n] \in W, s^n + \beta_{n-1}(\lambda_1, \ldots, \lambda_n)s^{n-1} + \cdots + \beta_0(\lambda_1, \ldots, \lambda_n) = 0\}.$$

Die Surjektivität von $\varphi : V \to W$ folgt nun einfach daraus, dass wir für alle Wahlen von $[\lambda_1, \ldots, \lambda_n] \in \mathbb{A}^n$ ein $s \in k$ so finden, dass

$$s^n + \beta_{n-1}(\lambda_1, \ldots, \lambda_n)s^{n-1} + \cdots + \beta_0(\lambda_1, \ldots, \lambda_n) = 0.$$

Hier ist entscheidend, dass k algebraisch abgeschlossen und die Gleichung normiert ist! Ausserdem gibt es für feste Wahl von $[\lambda_1, \ldots, \lambda_n] \in \mathbb{A}^n$ höchstens n verschiedene s, die diese Gleichung erfüllen.
Im allgemeinen Fall müssen wir etwas kommutative Algebra benutzen und beweisen zunächst einige Lemmata:

Lemma 2.7.3 (Nakayama)**.** *Sei R ein lokaler Ring (siehe Definition 1.9.7) mit maximalem Ideal $\mathfrak{m}$ und M ein endlich erzeugter R-Modul. Falls $\mathfrak{m}M = M$, so gilt $M = 0$.*

Beweis. Sei $m_1, \ldots, m_n$ ein minimales Erzeugendensystem von M. Nehme an, dass $M \neq 0$, d.h. $n \geq 1$. Wegen $\mathfrak{m}M = M$ gilt z.B.

$$m_n = \sum_{k=1}^{n} r_i m_i$$

für $r_i \in \mathfrak{m}$, also

$$(1 - r_n)m_n = \sum_{k=1}^{n-1} r_i m_i$$

Da R lokal ist, folgt, dass $(1-r_n)$ invertierbar ist. Daher lässt sich m_n durch die anderen Erzeuger ausdrücken. Widerspruch. □

Lemma 2.7.4. *Sei $\Phi : R \to R'$ eine injektive endliche Ringerweiterung. Dann ist für jedes maximale Ideal $\mathfrak{m}$ von R das Ideal $\Phi(\mathfrak{m})R'$ echt.*

Beweis. Auch die Erweiterung $\Phi[S^{-1}] : R[S^{-1}] \to R'[S^{-1}]$ ist endlich, wobei $S = R \setminus \mathfrak{m}$. $R[S^{-1}]$ ist lokal mit maximalem Ideal $\mathfrak{m}[S^{-1}]$. Daher gilt nach dem Nakayama Lemma mit $M = R'[S^{-1}]$, die Aussage $\Phi(\mathfrak{m}[S^{-1}]) \cdot R'[S^{-1}] \neq R'[S^{-1}]$. Daher kann auch nicht $\Phi(\mathfrak{m})R' = R'$ gelten. □

[9] dies bedeutet, dass Bilder von abgeschlossenen Mengen abgeschlossen sind
[10] Gegenbeispiel: $k[x^2, x^3] \subset k[x]$

Lemma 2.7.5. *Für einen Morphismus von affinen Varietäten $\varphi : V \to W$ so, dass die dazugehörige Abbildung $\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$ injektiv ist, gilt:*

1. *Für jeden Punkt $p \in W$ und das dazugehörige maximale Ideal $\mathfrak{m}_p = I(\{p\})$ gibt es eine Bijektion*

$$\{ \text{ maximale Ideale von } \mathcal{O}(V)/\Phi(\mathfrak{m}_p)\mathcal{O}(V) \ \} \cong \varphi^{-1}(p)$$

2. *φ ist genau dann surjektiv, wenn $\Phi(\mathfrak{m}_p)\mathcal{O}(V)$ für alle p ein echtes Ideal ist.*

Beweis. 1. Dies ist ein Korollar aus dem Hilbertschen Nullstellensatz. Nach Proposition 1.5.5 ist die linke Menge gleich der Menge der maximalen Ideale $\mathfrak{m}$ von $\mathcal{O}(V)$, die $\Phi(\mathfrak{m}_p)\mathcal{O}(V) \subset \mathfrak{m}$ erfüllen. Da Φ injektiv ist, ist dies gleich der Menge der Primideale $\mathfrak{m}$ so, dass $\mathfrak{m}_p \subset \Phi^{-1}(\mathfrak{m})$. Dies ist nach dem Hilbertschen Nullstellensatz gleich der Menge der Punkte p', die $\mathfrak{m}_p \subset \Phi^{-1}(I(\{p'\})) = I(\{\varphi(p')\})$ erfüllen. Also gleich der Menge $\varphi^{-1}(p)$.
2. folgt direkt aus 1. □

Lemma 2.7.6. *Sei k ein algebraisch abgeschlossener Köper und $k \to R$ eine endliche Ringerweiterung. Dann gilt:*

1. *Falls R reduziert ist, so gilt $R \cong \bigoplus_{j=1}^n k$ (k-Algebrenisomorphismus).*

2. *R hat nur endlich viele maximale Ideale.*

Beweis. Übung. *Beachte: Für die zweite Aussage kann man sich auf R reduziert beschränken, da die maximalen Ideale von R und $R/\sqrt{(0)}$ in Bijektion stehen.* □

Beweis von Proposition 2.7.2. Sei zunächst $\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$ injektiv (und nach Voraussetzung endlich). Dann ist nach Lemma 2.7.4 für jeden Punkt p von W und das maximale Ideal $\mathfrak{m}_p = I(\{p\})$ von $\mathcal{O}(W)$ das Ideal $\mathfrak{m}_p\mathcal{O}(V)$ echt. Daher ist φ nach Lemma 2.7.5 surjektiv und die Fasern sind in Bijektion mit der Menge der maximalen Ideale des Ringes $\mathcal{O}(V)/\Phi(\mathfrak{m}_p)\mathcal{O}(V)$. Dies ist jedoch eine *endliche* Ringerweiterung des Körpers $\mathcal{O}(W)/\mathfrak{m}_p$. Lemma 2.7.6 zeigt, dass er nur endlich viele maximale Ideale hat.
Wir müssen noch den Fall untersuchen, dass $\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$ nicht injektiv ist. Dann gibt es einen Kern $I \subset \mathcal{O}(W)$ und daher nach dem Homomorphiesatz (1.5.3) einen injektiven Ringhomomorphismus

$$\widetilde{\Phi} : \mathcal{O}(W)/I \hookrightarrow \mathcal{O}(V).$$

Daher ist I ein Radikalideal (da $\mathcal{O}(V)$ reduziert ist) und diese Gleichung bedeutet, dass φ wie folgt faktorisiert:

$$V \to V(I) \subset W.$$

Nach dem injektiven Fall ist $V \to V(I)$ surjektiv und jeder Punkt hat höchstens endlich viele Urbilder.
Wir müssen noch zeigen, jetzt wieder im allgemeinen Fall $\Phi : \mathcal{O}(W) \to \mathcal{O}(V)$ endlich, dass φ abgeschlossen ist. Dazu sei $V' \subset V$ eine Untervarietät, welche zum Ideal $I = I(V') \subset \mathcal{O}(V)$ gehört. Die Einschränkung von φ auf V' gehört zur Komposition

$$\widetilde{\Phi} : \mathcal{O}(W) \to \mathcal{O}(V) \to \mathcal{O}(V)/I \cong \mathcal{O}(V').$$

Sie ist wieder eine endliche Ringerweiterung! Somit ergibt der bereits bewiesene Teil, dass die Einschränkung von φ:

$$\varphi|_{V'} : V' \to V(\ker(\widetilde{\Phi}))$$

surjektiv ist. Das Bild von V' ist daher insbesondere abgeschlossen. □

In der algebraischen Geometrie gilt die auf den ersten Blick erstaunliche Aussage:

Satz 2.7.7. *Sei V eine nicht-leere affine Varietät. Dann gibt es einen endlichen surjektiven Morphismus*

$$V \to \mathbb{A}^l$$

für ein $l \in \mathbb{N}_0$.

Beweis. Die Aussage folgt aus dem nächsten Satz angewendet auf $R = \mathcal{O}(V)$ unter Verwendung von Proposition 1.4.4. □

Beispiel 2.7.8. *Betrachte die Varietät $V(x_1x_2-1) \subset \mathbb{A}^2$. Die beiden Projektionen $V(x_1x_2-1) \to \mathbb{A}^1$, welche einen Punkt $[\lambda_1, \lambda_2]$ auf λ_1 bzw. λ_2 abbilden sind nicht surjektiv. Daher können sie nach Proposition 2.7.2 nicht endlich sein. In der Tat ist $k[x_1,x_2]/(x_1x_2-1) = k[x_1, x_1^{-1}]$ als $k[x_1]$-Modul nicht endlich erzeugt (die unendlich vielen Potenzen $x_1^{-n}, n > 0$ können über $k[x_1]$ nicht alle durch eine endliche Anzahl von Elementen in $k[x_1, x_1^{-1}]$ erzeugt werden). Betrachte aber nun die Abbildung $\varphi : V(x_1x_2-1) \to \mathbb{A}^1$, welche einen Punkt $[\lambda_1, \lambda_2]$ auf $\lambda_1 + \lambda_2$ abbildet. Zu ihr gehört die Ringerweiterung $k[t] \to k[x_1,x_2]/(x_1x_2-1)$, welche t auf $x_1 + x_2$ abbildet. Sie wird z.B. durch x_2 erzeugt und es gilt nun $x_2^2 - x_2t + 1 = 0$. x_2 ist also ganz über $k[t]$! Daher ist diese Ringerweiterung endlich. Überlegen Sie sich, dass φ surjektiv ist.*

Satz 2.7.9 (Noethersches Normalisierungslemma)**.** *Sei k ein Köper mit unendlich vielen Elementen*[11]*. Für jede endlich erzeugte k-Algebra R gibt einen injektiven k-Algebrenhomomorphismus*

$$k[y_1, \ldots, y_l] \to R$$

so dass R über $k[y_1, \ldots, y_l]$ als Modul *endlich erzeugt ist, d.h. endlich ist.*

Beweis. Wir beweisen die Aussage durch Induktion nach der Anzahl n der Erzeuger der k-Algebra R. Seien $\xi_1, \ldots, \xi_n$ Erzeuger. Wir können (durch Umnummerieren) annehmen, dass $\xi_1, \ldots, \xi_r$ algebraisch unabhängig sind, d.h. dass die Abbildung

$$k[x_1, \ldots, x_r] \to R$$

welche x_i auf ξ_i abbildet, injektiv ist und dass jedes ξ_i für $i > r$ algebraisch über $k[\xi_1, \ldots, \xi_r]$ ist, d.h. eine polynomiale Gleichung mit Koeffizienten in $k[\xi_1, \ldots, \xi_r]$ erfüllt.
Falls $r = n$ ist, ist die Aussage trivial. Wir können also $r < n$ annehmen und $\xi_1, \ldots, \xi_n$ sind also Nullstelle eines Polynoms $f \in k[x_1, \ldots, x_n]$ in dem x_n tatsächlich vorkommt. Sei F der homogene Bestandteil höchsten Grades N in f.
Falls $n = 1$ ist, ist die Aussage mit $k = 0$ offensichtlich erfüllt. Ansonsten substituieren wir nun $x_i = x_i' + \alpha_i x_n$ für $i < n$ und zunächst beliebige $\alpha_1, \ldots, \alpha_{n-1} \in k$ und schreiben f als Polynom in x_n mit Koeffizienten in $k[x_1', \ldots, x_{n-1}']$.
Damit gilt

$$f = F(\alpha_1, \ldots, \alpha_{n-1}, 1)x_n^N + \text{ Terme von kleinerem Grad in } x_n.$$

Begründung: Jedes Monom $x_1^{i_1} \cdots x_n^{i_n}$ in f wird nach Substitution zu einer Summe von Monomen in den x_i' und x_n so, dass dasjenige in dem x_n mit dem höchsten Grad vorkommt, das Monom $\alpha_1^{i_1} \cdots \alpha_{n-1}^{i_{n-1}} (x_n)^{\sum_j i_j}$ ist.
Da k unendlich viele Elemente enthält, gibt es $\alpha_1, \ldots, \alpha_{n-1} \in k$ so, dass $F(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$. Für diese Wahl der α_i ist also f (bzw. ein Vielfaches) ein *normiertes* Polynom in x_n. Da $f(\lambda_1', \ldots, \lambda_{n-1}', \lambda_n) = 0$ (wobei $\lambda_i' = \lambda_i - \alpha_i x_n$ für die x_i' eingesetzt werden) folgt, dass λ_n eine normierte Gleichung mit Koeffizienten in $Q = k[\lambda_1', \ldots, \lambda_{n-1}'] \subset R$ erfüllt. Insbesondere ist R endlich über Q (siehe Beweis von 2.6.2, 2.). Nach Induktionsvoraussetzung gibt es einen injektiven k-Algebrenhomomorphismus

$$k[y_1, \ldots, y_l] \to Q$$

so dass Q endlich über $k[y_1, \ldots, y_n]$ ist. Daher ist nach Proposition 2.6.2, 1. auch R endlich über $k[y_1, \ldots, y_l]$. □

[11] Diese Voraussetzung kann entfallen, allerdings mit einem leicht komplizierteren Beweis.

3 Hilbertscher Nullstellensatz und Dimensionstheorie

3.1 Schwacher Nullstellensatz

Überraschenderweise folgt der Hilbertsche Nullstellensatz 1.3.7 bereits aus der folgenden schwächeren Aussage. Wir werden das im nächsten Abschnitt erklären.

Satz 3.1.1 (Schwacher Hilbertscher Nullstellensatz)**.** *Sei k ein algebraisch abgeschlossener Körper.*

1. *Sei R eine endlich erzeugte k-Algebra. Falls R ein Körper ist, so gilt $R \cong k$.*
2. *Jedes maximale Ideal $\mathfrak{m}$ von $k[x_1, \ldots, x_n]$ ist von der Form $\mathfrak{m} = (x_1 - \lambda_1, \ldots, x_n - \lambda_n)$ für $\lambda_i \in k$.*
3. *Die Abbildungen $V : I \mapsto V(I)$ und $I : V \mapsto I(V)$ induzieren Bijektionen zwischen der Menge der Punkte in $\mathbb{A}^n$ und der Menge der maximalen Ideale von $k[x_1, \ldots, x_n]$.*

Beweis. 2. folgt sofort aus der 1. Aussage, denn sei $\mathfrak{m}$ ein maximales Ideal von $k[x_1, \ldots, x_n]$. Dann ist $R = k[x_1, \ldots, x_n]/\mathfrak{m}$ endlich erzeugt (nämlich von den Restklassen der x_i) und ein Körper (da $\mathfrak{m}$ maximal ist). 1. besagt, dass $R = k$ ist. Betrachte dann die resultierende Abbildung: $p : k[x_1, \ldots, x_n] \to k$ mit $\ker(p) = \mathfrak{m}$. Sei $\lambda_i := p(x_i)$. Es gilt dann offensichtlich $(x_1 - \lambda_1, \ldots, x_n - \lambda_n) \subset \ker(p)$. Da aber das Ideal $(x_1 - \lambda_1, \ldots, x_n - \lambda_n)$ bereits maximal ist (siehe auch 1.5.9) folgt, dass Gleichheit besteht.
3. folgt sofort aus 2.
Es bleibt 1. zu zeigen: Nach dem Noetherschen Normalisierungslemma 2.7.9 gibt es einen injektiven k-Algebrenhomomorphismus $k[x_1, \ldots, x_r] \to R$ so, dass R endlich über $k[x_1, \ldots, x_r]$ ist. Aus dem folgenden Lemma 3.1.2 folgt dann, dass $k[x_1, \ldots, x_r]$ ebenfalls ein Körper ist. Daraus folgt sofort $r = 0$. Also ist R endlich über k. Daher gilt nach Lemma 2.7.6 1., dass $R \cong \bigoplus_{i=1}^{l} k$. Da aber R ein Körper ist, muss $R \cong k$ gelten. □

Lemma 3.1.2. *Sei K ein Körper und $R \to K$ eine injektive endliche Ringerweiterung. Dann ist auch R ein Körper.*

Beweis. Wir identifizieren R mit seinem Bild in K. Sei $b \in R$. Wir müssen zeigen, dass $b^{-1} \in R$ liegt. Nun gibt es aber $\beta_i \in R$ so, dass

$$b^{-n} + \beta_{n-1} b^{-n+1} + \cdots + \beta_0 = 0.$$

Durch Multiplikation mit b^{n-1} folgt

$$b^{-1} = -\beta_{n-1} - \beta_{n-2} b - \cdots - \beta_0 b^{n-1} \in R.$$

□

3.2 Starker Nullstellensatz

Wir können nun endlich den Hilbertschen Nullstellensatz beweisen.

Satz 1.3.7. *Sei k ein algebraisch abgeschlossener Körper und $I \subset k[x_1, \ldots, x_n]$ ein Ideal. Dann gilt:*

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

Beweis. Wir haben bereits gesehen, dass $\sqrt{I} \subset I(V(I))$. Sei also $g \in I(V(I))$. Wir müssen zeigen, dass ein k existiert so, dass $g^k \in I$. Sei $I = (f_1, \ldots, f_m)$. Wir betrachten die Varietät $V(J) \subset \mathbb{A}^{n+1}$, welche durch das Ideal

$$J = (f_1, \ldots, f_m, x_{n+1} g - 1)$$

definiert wird. Offensichtlich ist $V(J) = \emptyset$!

Angenommen J ist ein echtes Ideal. Dann liegt J in einem maximalen Ideal[12] $\mathfrak{m}$ und daher nach dem schwachen Nullstellensatz 3.1.1

$$\mathfrak{m} = (x_1 - \lambda_1, \dots, x_{n+1} - \lambda_{n+1}).$$

Dies bedeutet, dass der Punkt $\lambda = (\lambda_1, \dots, \lambda_{n+1})$ in $V(J)$ liegt. Widerspruch.
Wir bekommen also, dass $J = k[x_1, \dots, x_{n+1}]$. Es gibt daher $\beta_i \in k[x_1, \dots, x_{n+1}]$ so, dass

$$1 = \beta_1 f_1 + \cdots + \beta_m f_m + \beta_{m+1}(x_{n+1}g - 1).$$

In dieser Gleichung ersetzen wir x_{n+1} durch g^{-1} und erhalten

$$1 = \beta_1' f_1 + \cdots + \beta_m' f_m,$$

wobei β_i' rationale Funktionen in $k(x_1, \dots, x_n)$ sind, in deren Nenner eine Potenz von g steht. Durch Multiplikation dieser Gleichung mit einer geeigneten Potenz g^k bekommen wir eine Gleichung der Form

$$g^k = \beta_1'' f_1 + \cdots + \beta_m'' f_m,$$

wobei $\beta_i'' \in k[x_1, \dots, x_n]$. Insbesondere ist $g^k \in I$, was zu beweisen war. □

3.3 Dimension

Es gibt verschiedene Möglichkeiten in zufriedenstellender Weise einen Begriff der **Dimension** einer Varietät zu definieren. Wir werden dies zunächst für affine Varietäten erklären. Man erinnere sich an das Beispiel aus der Einleitung, wo wir die folgenden affinen Varietäten in $\mathbb{A}^2$ betrachtet haben:

$$V(x, y), \quad V(x, x+1), \quad V(xy + x^2, xy + y^2).$$

In jedem Fall ist die Dimension unterschiedlich (nämlich 0, 'leer' und 1) und es passiert etwas anderes beim Hinzunehmen des jeweils zweiten Polynoms. Die Dimension hängt also nur sehr indirekt mit der Anzahl der Gleichungen zusammen, die die Varietät beschreiben. Allerdings können wir nun, mit etwas mehr Wissen, die Probleme identifizieren, die in obigem Beispiel auftreten:

- $V(x, x+1)$ ist leer. Diese Tatsache spiegelt sich algebraisch in der Tatsache, dass das Ideal $(x, x+1) = (1)$ kein echtes Ideal und insbesondere nicht prim ist.
- $V(xy+x^2)$ ist nicht-irreduzibel! Dies ist anschaulich der Grund, weshalb die Dimension bei Hinzunahme der zweiten Gleichung nicht abnimmt, obwohl die Varietät sich verkleinert. Wieder bedeutet diese Tatsache algebraisch, dass das Ideal $(xy + x^2)$ nicht prim ist.

Dies verleitet uns zu den Vermutungen:

1. Für zwei *irreduzible* affine Varietäten $V \subset W$ gilt entweder $\dim(V) < \dim(W)$ oder $V = W$.
2. Für zwei *irreduzible* affine Varietäten $V \subsetneq W$ mit $\dim(V) \leq \dim(W) + 2$ gibt es eine irreduzible affine Varietät Z mit $V \subsetneq Z \subsetneq W$.

Die zweite Vermutung motiviert sich aus der Erfahrung, dass die Dimension in einer irreduziblen Varietät bei Hinzunahme einer zusätzlichen Gleichung genau um eins abnimmt.
Natürlich ergibt es keinen Sinn, die obigen Vermutungen zu beweisen, da wir ja den Begriff $\dim(V)$ nicht definiert haben. Umgekehrt ergibt sich aber aus diesen Vermutungen eine sinnvolle **Definition** des Begriffes der Dimension, und zwar

Definition 3.3.1. *Sei V eine irreduzible affine Varietät.* $\dim(V)$ *wird definiert als das Maximum der Längen n von Ketten*

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$$

von nicht-leeren irreduziblen *affinen Untervarietäten Z_i.*

[12] Da $k[x_1, \dots, x_{n+1}]$ noethersch ist, zeigt eine einfache Übung, dass jedes echte Ideal in einem maximalen enthalten ist. Die Aussage gilt jedoch sogar für beliebige Ringe, wenn man das Lemma von Zorn verwendet.

Unsere Vermutungen werden ihre Bestätigung darin finden, dass wir zeigen, dass Definition 3.3.1 eine sinnvolle Definition ergibt:

Satz 3.3.2. *0. Für alle irreduziblen affinen Varietäten V gilt* $\dim V < \infty$.

1. *Für zwei* irreduzible *affine Varietäten $V \subset W$ gilt* $\dim(V) < \dim(W)$ *oder* $V = W$.
2. *Für* irreduzible *affine Varietäten $V \subsetneq W$ mit* $\dim(V) \leq \dim(W) + 2$ *gibt es eine irreduzible Varietät Z mit $V \subsetneq Z \subsetneq W$.*
3. $\dim \mathbb{A}^n = n$.

Beachte, dass 1. und 2. gerade unsere Vermutungen von oben sind. Man überlege sich, dass die Aussagen dennoch nicht tautologisch sind!

Beispiel 3.3.3. *In $\mathbb{A}^n$ haben wir die Kette der Länge n von irreduziblen Varietäten:*

$$V(x_1, \ldots, x_n) \subsetneq \cdots \subsetneq V(x_1) \subsetneq \mathbb{A}^n.$$

Dies zeigt aber nur $\dim(\mathbb{A}^n) \geq n$. *Den Beweis, dass Gleichheit besteht, werden wir in den nächsten Abschnitten erbringen. Auch hier spielt das Noethersche Normalisierungslemma eine zentrale Rolle.*

Der Begriff der Dimension einer affinen Varietät V hängt nur von der Menge V versehen mit der Zariski-Topologie ab. Deshalb können wir allgemeiner definieren:

Definition 3.3.4. *Sei X ein noetherscher topologischer Raum.* $\dim(X)$ *wird definiert als das Maximum der Längen n von Ketten*

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$$

von nicht-leeren irreduziblen *abgeschlossenen Teilmengen Z_i.*

Dieser Begriff stimmt für eine affine Varietät nach Definition der Zariskitopologie und nach Definition von "irreduzibel" mit der vorigen überein. Ausserdem dehnt er die Definition der Dimension auf beliebige, nicht notwendigerweise affine, Varietäten aus. Für einen nicht-noetherschen topologischen Raum ist dieser Begriff nicht sinnvoll. Insbesondere kann man auf diese Weise nicht sinnvoll $\dim(\mathbb{R}^n)$ oder $\dim(\mathbb{C}^n)$, wobei $\mathbb{R}^n$ oder $\mathbb{C}^n$ mit der gewöhnlichen Topologie ausgestattet sind, definieren!

3.3.5. Sei V eine affine Varietät. Nach dem Hilbertschen Nullstellensatz entsprechen *irreduzible* affine Untervarietäten von V gerade den *Prim*idealen von $\mathcal{O}(V)$. Wir definieren deshalb auch:

Definition 3.3.6. *Sei R ein kommutativer Ring. Die* **Krulldimension** $\dim(R)$ *ist das Maximum der Längen n von Ketten*

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

von Primidealen P_i.

Es folgt für eine affine Varietät sofort: $\dim(V) = \dim(\mathcal{O}(V))$.

Beispiel 3.3.7. *Ein Körper hat Krulldimension 0, da* (0) *das einzige Primideal ist. Ein Hauptidealring, welcher kein Köper ist, hat Krulldimension 1 (Übung). Hieraus folgt schon einmal* $\dim(\mathbb{A}^1) = 1$.

Beispiel 3.3.8. *Die Kette von irreduziblen affinen Untervarietäten in Beispiel 3.3.3 oben korrespondiert zu der Kette der Länge n von Primidealen*

$$(x_1, \ldots, x_n) \supsetneq \cdots \supsetneq (x_1) \supsetneq (0)$$

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

3.3.9. Die naive Idee, dass die Dimension eine irreduziblen affinen Varietät V etwas mit der Anzahl der Gleichungen zu tun hat, die V definieren, müssen wir dennoch nicht aufgeben. Es zeigt sich aber, dass es dazu nötig ist, zum Quotientenkörper $K = \mathrm{Quot}(\mathcal{O}(V))$ überzugehen. Wir nennen eine Menge $f_1, \ldots, f_n$ von Elementen in einem Körper K, welcher k enthält, **algebraisch unabhängig** über k, falls kein Polynom $p \neq 0$ in $k[x_1, \ldots, x_n]$ mit $p(f_1, \ldots, f_n) = 0$ existiert. Mit anderen Worten, $f_1, \ldots, f_n$ sind algebraisch unabhängig über k, genau dann wenn der von $f_1, \ldots, f_n$ erzeugte Teilkörper $k(f_1, \ldots, f_n)$ isomorph zum rationalen Funktionenkörper $k(x_1, \ldots, x_n)$ ist (unter der offensichtlichen Abbildung). Eine algebraisch unabhängige Teilmenge $f_1, \ldots, f_n$ heisst (endliche) **Transzendenzbasis** von K über k, falls K *algebraisch* über $k(f_1, \ldots, f_n)$ ist. Wir werden zeigen, dass die Länge (Kardinalität) einer (endlichen) Transzendenzbasis wohlbestimmt ist. Diese Länge heisst der **Transzendenzgrad** $\mathrm{trdeg}(K|k)$ der Körpererweiterung $K|k$. Wir haben dann den

Satz 3.3.10. *Sei V eine irreduzible affine Varietät. Dann gilt:*

$$\dim(V) = \mathrm{trdeg}(\mathrm{Quot}(\mathcal{O}(V))|k).$$

Dieser Satz folgt aus der algebraischen Variante, Satz 3.6.2.

3.4 "Going-up" und "Going-down"

Entscheidend für das Verständnis des im letzten Abschnitt definierten Dimensionsbegriffes ist wiederum das Noethersche Normalisierungslemma. Dies setzt voraus, dass wir verstehen, dass sich die Krulldimension unter einer injektiven endlichen Ringerweiterung nicht ändert.

Satz 3.4.1. *Sei $\Phi : R \to R'$ eine endliche Ringerweiterung und $P \subsetneq Q$ zwei Primideale von R'. Dann ist auch $\Phi^{-1}(P) \subsetneq \Phi^{-1}(Q)$. Insbesondere ist $\dim(R) \geq \dim(R')$.*

Beweis. Wir lokalisieren an der Menge $S := R \setminus \Phi^{-1}(Q)$. Der Ring $R[S^{-1}]$ ist dann lokal mit maximalem Ideal $\Phi^{-1}(Q)[S^{-1}]$. Es gilt $0 \notin \Phi(S)$, da $S \cap \ker(\Phi) = \emptyset$. Wir können also R' an $\Phi(S)$ lokalisieren. und es gilt noch immer $P[\Phi(S)^{-1}] \subsetneq Q[\Phi(S)^{-1}]$ (siehe 1.9.6). Ausserdem ist auch $R[S^{-1}] \to R'[\Phi(S)^{-1}]$ wieder endlich. Wir können also o.B.d.A. annehmen, dass R lokal ist mit maximalem Ideal $\Phi^{-1}(Q)$.
In diesem Fall nehmen wir an, dass $\Phi^{-1}(P) = \Phi^{-1}(Q)$ und beweisen die Aussage durch Widerspruch. Die Ringerweiterung

$$R/\Phi^{-1}(P) \to R'/P$$

ist ebenfalls endlich. Ausserdem ist $R/\Phi^{-1}(P)$ ein Körper, da $\Phi^{-1}(P)$ maximal ist. Daher ist nach Lemma 3.4.2 unten R'/P ein Körper. Daher kann nur $P = Q$ gelten. Widerspruch.
Die Aussage $\dim(R) \geq \dim(R')$ ergibt sich wie folgt: Sei

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

eine strikt absteigende Kette von Primidealen. Anwenden von Φ^{-1} ergibt die Kette

$$\Phi^{-1}(P_0) \supsetneq \Phi^{-1}(P_1) \supsetneq \cdots \supsetneq \Phi^{-1}(P_n)$$

von Primidealen, welche wegen der soeben bewiesenen Aussage wieder *strikt* absteigend ist. □

Lemma 3.4.2. *Sei $\Phi : K \to R'$ eine endliche Ringerweiterung, wobei K ein Körper ist und R' nullteilerfrei. Dann ist auch R' ein Körper.*

Beweis. (vgl. auch Lemma 2.7.6, aus dem Aussage für K alg. abgeschlossen bereits folgt.) Da K ein Köper ist, ist Φ injektiv und wir identifizieren K mit seinem Bild in R'. Sei $s \in R' \setminus 0$. Wir wollen zeigen, dass s invertierbar ist. s ist ganz über K, erfüllt also eine Gleichung der Form

$$s^n + \beta_{n-1}s^{n-1} + \cdots + \beta_0 = 0$$

mit $\beta_i \in K$. Wir können annehmen, dass die Gleichung von minimalem Grad ist und schreiben sie als

$$s(s^{n-1} + \beta_{n-1}s^{n-2} + \cdots + \beta_1) = -\beta_0.$$

Falls $\beta_0 = 0$, folgt $s = 0$ oder $s^{n-1} + \beta_{n-1}s^{n-2} + \cdots + \beta_1 = 0$ da R' nullteilerfrei ist. Dies kann nicht sein, da die Gleichung von minimalem Grad war. Daher können wir die Gleichung mit $(-\beta_0)^{-1}$ multiplizieren und bekommen, dass s invertierbar ist. □

Es gilt auch eine Umkehrung von des vorigen Satzes, eine Verschärfung der Aussage von Lemma 2.7.4. Wir beweisen dazu zunächst das folgende

Lemma 3.4.3. *Sei $\Phi : R \to R'$ ein beliebiger Ringhomomorphismus und $\mathfrak{p}$ ein Primideal von R. Dann gibt es ein Primideal P von R' mit $\Phi^{-1}(P) = \mathfrak{p}$, genau dann wenn $\Phi^{-1}(\Phi(\mathfrak{p})R') = \mathfrak{p}$.*

Beweis. Falls ein solches Primideal existiert, gilt $\Phi(\mathfrak{p})R' \subset P$ und daher $\Phi^{-1}(\Phi(\mathfrak{p})R') \subset \mathfrak{p}$ und daher Gleichheit. Umgekehrt gelte $\Phi^{-1}(\Phi(\mathfrak{p})R') = \mathfrak{p}$ und sei $S = R \setminus \mathfrak{p}$. Wir haben $S \cap \ker(\Phi) = \emptyset$, da $\ker(\Phi) \subset \mathfrak{p}$. Daher können wir die Lokalisierung

$$R[S^{-1}] \to R'[\Phi(S)^{-1}]$$

betrachten. Das Ideal $\Phi(\mathfrak{p})R'[S^{-1}]$ ist echt, denn ansonsten wäre $1 = \frac{\Phi(p)r'}{\Phi(s)}$, also existiert $t \in S$ so dass $\Phi(t)\Phi(s) = \Phi(t)\Phi(p)r'$. Also ist $st \in \Phi^{-1}(\Phi(\mathfrak{p})R') = \mathfrak{p}$. Widerspruch. Daher existiert ein maximales Ideal $\mathfrak{m}$, welches $\Phi(\mathfrak{p})R'[S^{-1}]$ enthält. Das Urbild $\Phi^{-1}(\mathfrak{m})$ in $R[S^{-1}]$ ist prim und enthält $\mathfrak{p}[S^{-1}]$ ist also gleich $\mathfrak{p}[S^{-1}]$. Das Ideal $\mathfrak{m} \cap R'$ erfüllt das gewünschte. □

Satz 3.4.4. *Sei $\Phi : R \to R'$ eine* injektive *endliche Ringerweiterung und $\mathfrak{q}$ ein Primideal von R. Dann gibt es ein Primideal Q mit $\Phi^{-1}(Q) = \mathfrak{q}$.*
Darüberhinaus gilt die verschärfte Aussage ("Going up"): Seien $\mathfrak{p} \subsetneq \mathfrak{q}$ zwei Primideale von R. Dann gibt es für jedes Primideal P von R' mit $\Phi^{-1}(P) = \mathfrak{p}$ ein Primideal Q mit $P \subsetneq Q$ und $\Phi^{-1}(Q) = \mathfrak{q}$.
Insbesondere ist $\dim(R) = \dim(R')$.

Beweis. Die verschärfte Aussage folgt unter Verwendung von 1.5.5 sofort aus der ersten, angewendet auf die (immer noch endliche und injektive) Ringerweiterung

$$R/\mathfrak{p} \to R'/P.$$

Wir lokalisieren dann an der Menge $S = R \setminus \mathfrak{q}$ und betrachten die endliche injektive Ringerweiterung $\Phi[S^{-1}] : R[S^{-1}] \to R'[S^{-1}]$. Falls wir ein Ideal $\widetilde{Q}$ von $R'[S^{-1}]$ mit $\Phi^{-1}(\widetilde{Q}) = \mathfrak{q}[S^{-1}]$ finden, so entspricht $\widetilde{Q}$ nach 1.9.6 einem Primdeal Q von R' welches $\widetilde{Q} = Q[S^{-1}]$ erfüllt. Wir können daher o.B.d.A. anzunehmen, dass $\mathfrak{q}$ maximal und R lokal ist.
Dann wissen wir bereits nach Lemma 2.7.4, dass das Ideal $\Phi(\mathfrak{q})R'$ echt ist. Daher gilt $\Phi^{-1}(\Phi(\mathfrak{q})R') = \mathfrak{q}$ und daher gibt es nach Lemma 3.4.3 ein Primideal Q mit $\Phi^{-1}(Q) = \mathfrak{q}$.
Die Aussage über die Dimensionen ergibt sich wie folgt: Sei

$$\mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

eine strikt absteigende Kette von Primidealen von R.
Behauptung: Wir finden eine strikt absteigende Kette von Primidealen von R, so dass

$$P_0 \supsetneq \cdots \supsetneq P_n$$

Daraus folgt sofort $\dim(R) \leq \dim(R')$. Da wir wegen Satz 3.4.1 schon wissen, dass $\dim(R) \geq \dim(R')$ folgt $\dim(R) = \dim(R')$.
Beweis der Behauptung durch Induktion nach n: Für eine Kette aus einem Primideal, also für $n = 0$, haben wir genau die Aussage des Satzes. Ansonsten können wir die Kette

$$\mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

nach Induktionsvoraussetzung zu einer Kette

$$P_1 \supsetneq \cdots \supsetneq P_n$$

liften und wenden dann die verschärfte Aussage auf $P = P_1$, $\mathfrak{p} = \mathfrak{p}_1$ und $\mathfrak{q} = \mathfrak{p}_0$ an. Wir erhalten das Ideal $P_0 := Q$, welches $\varphi^{-1}(P_0) = \mathfrak{p}_0$ erfüllt und die Kette nach links fortsetzt:

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

□

Der Name "Going up" erklärt sich durch die Richtung in der wir die Primideale auf R' liften können. Es gibt auch den "Going down"-Satz, indem dies in umgekehrter Richtung erfolgt. Es ist jedoch nicht mehr in so grosser Allgemeinheit gültig. Dazu benötigen wir:

Definition 3.4.5. *Sei R ein nullteilerfreier kommutativer Ring. R heisst* **ganz abgeschlossen (oder normal)** *, falls für jede ganze Erweiterung (siehe Definition 2.6.1)*

$$R \subset R' \subset \mathrm{Quot}(R)$$

gilt: $R = R'$.

Lemma 3.4.6. *Sei R ein ganz abgeschlossener Ring und sei $P \in R[x]$ ein normiertes Polynom und $K = \mathrm{Quot}(R)$.*

1. *Sei $P = Q \cdot Q'$ eine Faktorisierung in $K[x]$. Dann sind $Q, Q' \in R[x]$. Falls die Koeffizienten von P (ausser dem führenden) in einem Primideal $\wp \subset R$ liegen, so liegen die Koeffizienten von Q und Q' in $\wp$ (ausser den führenden).*

2. *Sei $\Phi : R \to R'$ eine* injektive *endliche Ringerweiterung mit R' nullteilerfrei. Falls $P(p) = 0$ für $p \in \wp R'$, dann sind alle Koeffizienten von P (ausser dem führenden) in $\wp$.*

Beweis. 1. Sei L der Zerfällungskörper von P. Dann gilt: $P = \prod_{i=1}^{n}(x - \gamma_i)$. Jedes γ_i erfüllt die normierte Gleichung P über R, d.h. der Teilring $R' = R[\gamma_1, \ldots, \gamma_n]$ von L ist endlich über R. Da die Koeffizienten von Q und Q' Polynome in den γ_i sind, sind sie als Elemente von K ebenfalls ganz über R und liegen daher in R, da R ganz abgeschlossen ist.
Sei

$$P = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$$

und nehme an, dass $\alpha_i \in I$ für alle i. Da $P(\gamma_i) = 0$ für alle i gilt: $\gamma_i \in \sqrt{\wp R'}$ für alle i und daher sind auch alle Koeffizienten (ausser dem führenden) von Q und Q' in $\sqrt{\wp R'} \cap R$. Behauptung: $\sqrt{\wp R'} \cap R = \wp$. Dies folgt aus Lemma 3.4.3 in Verbindung mit 3.4.4 angewendet auf die Ringerweiterung $R \to R'$.
2. Betrachte die Multiplikation mit p als eine K-lineare Abbildung γ_p von $\mathrm{Quot}(R')$. Das Minimalpolynom Q von γ_p teilt dann P und ist daher nach dem 1. Teil ein Polynom mit Koeffizienten in R. Sei nun $\xi_1, \ldots, \xi_n$ ein Erzeugendensystem von R' über R. Sei $p = \sum i_k p_k$ mit $i_k \in \wp$ und $p_k \in R'$. Es gilt $p_k\xi_i = \sum_j \gamma_{ijk}\xi_j$ für gewisse $\gamma_{ijk} \in R$ und daher $p\xi_i = \sum_j(\sum_k i_k\gamma_{ijk})\xi_j$. Wie im Beweis von Proposition 2.6.2 bekommen wir, dass für das charakteristische Polynom P' der Matrix $\Gamma = (\sum_k i_k\gamma_{ijk})_{ij}$ die Gleichung $P'(p) = 0$ erfüllt ist. Daher ist Q ein Teiler von P'. Da Γ eine Matrix mit Koeffizienten in $\wp$ ist, so sind alle Koeffizienten von P' (bis auf den führenden), die Polynome in den Einträgen der Matrix sind in $\wp$. Daher sind die Koeffizienten von Q (bis auf den führenden) in $\wp$ nach dem 1. Teil dieses Lemmas. Daher sind auch die Koeffizienten von P (bis auf den führenden) in $\wp$. □

Satz 3.4.7 ("Going down")**.** *Sei $\Phi : R \to R'$ eine* injektive *endliche Ringerweiterung, R ganz abgeschlossen und R' nullteilerfrei. Seien $\mathfrak{p} \subsetneq \mathfrak{q}$ zwei Primideale von R. Dann gibt es für jedes Primideal Q von R mit $\Phi^{-1}(Q) = \mathfrak{q}$ ein Primideal P mit $P \subsetneq Q$ und $\Phi^{-1}(P) = \mathfrak{p}$.*

Beweis. Wir lokalisieren an der Menge $S = R' \setminus Q$ und betrachten die injektive Zusammensetzung $\Phi' : R \to R' \to R'[S^{-1}]$. Es genügt nach Lemma 3.4.3 zu zeigen, dass $(\mathfrak{p}R'[S^{-1}]) \cap R = \mathfrak{p}$. In diesem Fall gibt es ein Primideal P' von $R'[S^{-1}]$ mit $P' \cap R = \mathfrak{p}$. Für $P := R' \cap P'$ gilt ausserdem $P \subset Q$. Sei also ein Element $y \in (\mathfrak{p}R'[S^{-1}]) \cap R$ gegeben. Wir können schreiben $y = \frac{p}{s}$ bzw. $sy = p$, wobei $p \in \mathfrak{p}R'$. und $s \in R' \setminus Q$. Es gibt daher ein Polynom

$$P = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 \in R[x]$$

mit $P(p) = 0$. Daraus folgt nach Lemma 3.4.6, 2. $\alpha_i \in \mathfrak{p}$ für alle i.
Sei $Q = x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_0$ das Minimalpolynom von s über $\mathrm{Quot}(R)$, Nach Lemma 3.4.6, 1. hat es Koeffizienten in R. Nicht alle β_i können in $\mathfrak{p}$ liegen, denn ansonsten wäre $s^n \in \mathfrak{p}R' \subset \mathfrak{q}R' \subset Q$. Widerspruch. Das Minimalpolynom von $p = sy$ ist nun offenbar $Q' = x^n + \beta_{n-1}yx^{n-1} + \cdots + \beta_0 y^n$. Daher teilt Q' das Polynom P und daher nach Lemma 3.4.6, 1. $y^j\beta_{n-j} \in \sqrt{\mathfrak{p}} = \mathfrak{p}$ für $j = 1, \ldots, n$. Da nicht alle β_i in $\mathfrak{p}$ liegen, muss y in $\mathfrak{p}$ liegen. □

3.5 Transzendenzgrad

Für die Definitionen von "algebraisch unabhängig" und "Transzendenzbasis" gelten die folgenden Aussagen:

Proposition 3.5.1. *Sei $K|k$ eine Körpererweiterung und $f_1, \ldots, f_n$ eine Transzendenzbasis von $K|k$, sowie $e_1, \ldots, e_m$ eine Menge über k algebraisch unabhängiger Elemente von K. Dann gilt $m \leq n$ und man kann gewisse m Elemente unter den $f_1, \ldots, f_n$ durch $e_1, \ldots, e_m$ tauschen und erhält wieder eine Transzendenzbasis von $K|k$.*

Beweis. Übung. □

Korollar 3.5.2. *Sei $K|k$ eine Körpererweiterung welche eine endiche Transzendenzbasis enthält. Dann gilt:*

1. *Je zwei Transzendenzbasen haben dieselbe Anzahl Elemente.*
2. *Aus jeder Menge $f_1, \ldots, f_n \in K$ so, dass K über $k(f_1, \ldots, f_n)$ algebraisch ist, kann eine Transzendenzbasis ausgewählt werden.*
3. *Jede algebraisch unabhängige Menge kann zu einer Transzendenzbasis ergänzt werden.*

Beweis. Dies folgt sofort aus der vorigen Proposition. □

Es gibt auch den Begriff einer unendlichen Transzendenzbasis, und die obigen Aussagen gelten analog. Dieser Fall interessiert jedoch für die algebraische Geometrie nicht.
Erinnere aus der Algebra:

Definition 3.5.3. *Ein nullteilerfreier kommutativer Ring R heisst* **faktoriell***, falls jedes Element $x \in R$ eine Darstellung*

$$x = \varepsilon p_1^{n_1} \cdots p_l^{n_l}$$

hat, wobei die p_i irreduzibel sind, ε eine Einheit und $(p_i) \neq (p_j)$ für $i \neq j$, so dass die Ideale (p_i), sowie die n_i bis auf die Reihenfolge eindeutig bestimmt sind.

Proposition 3.5.4. *Sei R ein kommutativer noetherscher Ring. Die folgenden Aussagen sind äquivalent:*

1. *R ist nullteilerfrei und irreduzible Elemente sind prim.*
2. *R ist faktoriell.*

Proposition 3.5.5. *Sei R ein faktorieller Ring. Dann ist auch $R[x]$ faktoriell.*

Insbesondere ist für jeden Körper k der Polynomring $k[x_1, \ldots, x_n]$ faktoriell.

Lemma 3.5.6. *Faktoriell impliziert ganz abgeschlossen.*

Beweis. Übung. □

Lemma 3.5.7. *Für jedes Primideal I von $k[x_1, \ldots, x_n]$ gilt:*

$$\mathrm{trdeg}(\mathrm{Quot}(k[x_1, \ldots, x_n]/I)) = \begin{cases} n & \textit{falls } I = (0), \\ n-1 & \textit{falls } I = (g) \textit{ ein Hauptideal ist,} \\ \leq n-2 & \textit{sonst.} \end{cases}$$

Beweis. Sei $f \neq 0$ ein Element von I. Es induziert eine nicht-triviale Relation zwischen den Restklassen von $x_1, \dots, x_n$. Da wir unter letzteren eine Transzendenzbasis auswählen können, muss $\mathrm{trdeg}(k[x_1, \dots, x_n]/I) < n$ gelten. Sei $I = (g)$. Bezeichne $R = k[x_1, \dots, x_n]/(g)$. Beachte: R ist nullteilerfrei, da (g) prim ist. Falls $\mathrm{trdeg}(\mathrm{Quot}(R)) \leq n - 2$ wäre, hiesse dies, dass die Mengen $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$ für alle i algebraisch abhängig sind. Es gilt also für alle i ein Polynom $p_i \in k[x_1, \dots, x_n]$ mit $p_i(\overline{x_1}, \dots, \overline{x_n}) = 0$ in R und so, dass x_i in p_i nicht vorkommt. Das bedeutet gerade, dass $\overline{p_i} = 0$ in R. Daher $p_i \in (g)$. Daher ist $p_i = \lambda_i \cdot g$. Daraus folgt, dass auch x_i in g nicht vorkommt. Da i beliebig ist, kommt kein x_i in g vor, also $g = 0$. Widerspruch. Falls I kein Hauptideal ist, muss hingegen $\mathrm{trdeg}(k[x_1, \dots, x_n]) \leq n-2$ gelten. Wir werden dies nicht benutzen und lassen deshalb den Beweis als Übung. *Hinweis:* Benutze Lemma 3.6.1 unten. □

3.6 Hauptsätze der Dimensionstheorie

Der Schlüssel zum Verständnis des Begriffes der Krulldimension liegt in folgendem Lemma

Lemma 3.6.1. *Sei R eine endlich erzeugte nullteilerfreie k-Algebra. Für jedes Primideal $I \neq (0)$ von R gilt:*

$$\mathrm{trdeg}(\mathrm{Quot}(R/I)) < \mathrm{trdeg}(\mathrm{Quot}(R))$$

Beweis. Sei $\Phi : k[x_1, \dots, x_l] \to R$ der endliche Morphismus aus dem Noetherschen Normalisierungslemma. Er ist injektiv und setzt sich deshalb zu einem Morphismus $k(x_1, \dots, x_l) \to \mathrm{Quot}(R)$ fort und $\mathrm{Quot}(R)$ ist wieder endlich, also algebraisch über $k(x_1, \dots, x_l)$. Es gilt daher $\mathrm{trdeg}(R) = l$, daraus folgt, dass l wohlbestimmt ist. Betrachte die wiederum injektive endliche Abbildung $k[x_1, \dots, x_l]/\Phi^{-1}(I) \to R/I$. Sie impliziert, dass $\mathrm{trdeg}(R/I) = \mathrm{trdeg}(k[x_1, \dots, x_l]/\Phi^{-1}(I)) < l$ (Lemma 3.5.7). Beachte $\Phi^{-1}(I) \neq \Phi^{-1}((0)) = (0)$ nach Satz 3.4.1. □

Damit können wir beweisen:

Satz 3.6.2. *Sei R eine nullteilerfreie endlich erzeugte k-Algebra. Dann gilt:* $\dim(R) = \mathrm{trdeg}(\mathrm{Quot}(R))$.

Beweis. Wir zeigen zunächst $\mathrm{trdeg}(\mathrm{Quot}(R)) \geq \dim(R)$. Sei

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

eine strikt absteigende Kette von Primidealen. Wir zeigen $\mathrm{trdeg}(\mathrm{Quot}(R)) \geq n$. Daraus folgt die Aussage. Dies zeigen wir mit Induktion nach n. Für $n = 0$ ist die Aussage klar. Sei

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

eine strikt absteigende Kette von Primidealen. Dann ist

$$P_0/P_n \supsetneq P_1/P_n \supsetneq \cdots \supsetneq P_{n-1}/P_n$$

eine strikt absteigende Kette von Primidealen von R/P_n. Es gilt dann nach Induktionsvoraussetzung

$$\mathrm{trdeg}(\mathrm{Quot}(R/P_n)) \geq n - 1$$

und nach Lemma 3.6.1

$$\mathrm{trdeg}(\mathrm{Quot}(R)) - 1 \geq \mathrm{Quot}(R/P_n).$$

Sei $\Phi : k[x_1, \dots, x_l] \to R$ nun wieder der injektive endliche k-Algebrenhomomorphismus aus dem Noetherschen Normalisierungslemma. Wir haben gesehen, dass $\dim(R) = \dim(k[x_1, \dots, x_l])$ und im Beweis des letzten Lemmas $\mathrm{trdeg}(R) = l$. Es genügt also, die Aussage $\mathrm{trdeg}(\mathrm{Quot}(R)) \leq \dim(R)$ für $R = k[x_1, \dots, x_l]$ zu zeigen. Hier haben wir aber die strikt absteigende Kette von Primidealen

$$(x_1) \supsetneq (x_1, x_2) \supsetneq \cdots \supsetneq (x_1, \dots, x_l) \supsetneq (0)$$

der Länge l. □

Hieraus ergibt sich sofort die geometrische Fassung: Satz 3.3.10.
Um alle Aussagen von Satz 3.3.2 zu beweisen, insbesondere Behauptung 2., benötigen wir ein algebraisches Resultat, den *Hauptidealsatz von Krull*. Er präzisiert die Aussage, dass die Dimension einer Varietät, welche durch eine Gleichung gegeben wird eine um eins kleinere Dimension hat. Zunächst beweisen wir einige Lemmata.

Lemma 3.6.3. *Seien R und R' nullteilerfreie Ringe und $\Phi : R \to R'$ eine endliche injektive Ringerweiterung wobei R ganz abgeschlossen ist. Betrachte die zugehörige endliche Körpererweiterung*

$$\mathrm{Quot}(R') | \mathrm{Quot}(R)$$

Jedes Element x von $\mathrm{Quot}(R')$ definiert durch Multiplikation einen linearen Endomorphismus γ_x von $\mathrm{Quot}(R')$ als $\mathrm{Quot}(R)$ Vektorraum. Dann gilt

$$y \in R \Rightarrow \det(\gamma_y) \in R.$$

Wir bezeichnen $\det(\gamma_y)$ auch einfach als $\det(y)$.

Beweis. Sei $y \in R'$. Da y ganz über R ist, gibt es ein Polynom

$$P = x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_0 \in R[x]$$

mit $P(y) = 0$.
Sei Q das Minimalpolynom von γ_y. Q ist ein Teiler des Polynoms P und hat damit nach 3.4.6, 1. ebenfalls Koeffizienten in R. Das charakteristische Polynom

$$x^n - \mathrm{tr}(\gamma_x)x^{n-1} + \cdots \pm \det(\gamma_x)$$

von γ_x ist eine Potenz von Q (Körpertheorie) und hat daher ebenfalls Koeffizienten in R. Insbesondere ist $\det(\gamma_x) \in R$. □

Lemma 3.6.4. *Seien R und R' nullteilerfreie Ringe und $\Phi : R \to R'$ eine endliche injektive Ringerweiterung wobei R faktoriell ist. Sei $0 \neq g \in R'$. Dann ist $\Phi^{-1}((g))$ ein von Null verschiedenes Hauptideal.*

Beweis. Wir zeigen dass $\Phi^{-1}((g))$ nicht Null ist und in einem Hauptideal enthalten ist. Daraus folgt die Aussage, da R faktoriell ist. Behauptung $\Phi^{-1}((g)) \subset \sqrt{(\det(g))}$ (beachte $\det(g) \in R$ wegen Lemma 3.6.3. Ausserdem ist $\sqrt{(\det(g))}$ ein Hauptideal, da R faktoriell ist (Übung). Sei

$$\lambda g = h$$

mit $h \in R$, d.h. $h \in \Phi^{-1}((g))$. Es gilt dann

$$\det(\lambda)\det(g) = \det(h) = h^n,$$

wobei n der Grad der Körpererweiterung $\mathrm{Quot}(R') | \mathrm{Quot}(R)$ ist. Das heisst $h \in \sqrt{(\det(g))}$.
Ausserdem ist $\Phi^{-1}((g))$ nicht das Nullideal, da g eine normierte Gleichung der Form

$$g^n + \beta_{n-1}g^{n-1} + \cdots + \beta_0 = 0$$

erfüllt, von der wir annehmen können, dass der Grad minimal ist. Dies zeigt, dass

$$g(g^{n-1} + \beta_{n-1}g^{n-2} + \cdots + \beta_1) = \beta_0$$

Daher $\beta_0 \neq 0$, da R' nullteilerfrei ist und $g \neq 0$ und der Grad der obigen Gleichung minimal war. Ausserdem zeigt die Gleichung: $\beta_0 \in \Phi^{-1}((g))$. □

Satz 3.6.5 (Krulls Hauptidealsatz)**.** *Sei k ein algebraisch abgeschlossener Körper und sei R eine endlich erzeugte nullteilerfreie k-Algebra, $0 \neq g \in R$ und $\wp$ ein Primideal, welches minimal ist mit der Eigenschaft $g \in \wp$. Dann ist* $\mathrm{trdeg}(\mathrm{Quot}(R/\wp)) = \mathrm{trdeg}(\mathrm{Quot}(R)) - 1$.

Beweis. Beachte, dass aus den Voraussetzungen folgt $R = \mathcal{O}(V)$ für eine affine Varietät V. Wir haben daher nach Proposition 1.7.9 (algebraische Fassung), dass $\sqrt{(g)} = \wp_1 \cap \cdots \cap \wp_n$ (endlicher Schnitt). Da $\sqrt{(g)} \subset \wp$ gilt also $\wp_i \subset \wp$ für ein i da $\wp$ prim ist (Übung). Da $\wp$ minimal ist mit der Eigenschaft $g \in \wp$ folgt Gleichheit. Durch Umnummerieren sei $\wp = \wp_n$.
Zunächst gilt o.B.d.A., dass $\wp_1 \cap \cdots \cap \wp_{n-1} \not\subset \wp$, da daraus folgen würde, dass $\wp_i \subset \wp$ für ein $i < n$. Wir können also o.B.d.A. annehmen, dass ein Element $h \in \wp_1 \cap \cdots \cap \wp_{n-1}$ existiert mit $h \notin \wp$. Dann ist $\wp_n[h^{-1}]$ in $R[h^{-1}]$ prim (Proposition 1.9.6). Alle anderen $\wp_i[h^{-1}]$ sind aber gleich $R[h^{-1}]$. Daher gilt:

$$\wp[h^{-1}] = \sqrt{(g)}$$

in $R[h^{-1}]$ und ausserdem $\mathrm{Quot}(R/\wp_n) = \mathrm{Quot}(R[h^{-1}]/\wp[h^{-1}])$. Wir dürfen daher o.B.d.A. annehmen, dass $\wp = \sqrt{(g)}$.
Sei $\Phi : k[x_1, \ldots, x_l] \to R$ der injektive endliche k-Algebrenhomomorphismus aus dem Noetherschen Normalisierungslemma. Insbesondere $\mathrm{trdeg}(\mathrm{Quot}(R)) = l$. Wir wissen nach dem vorigen Lemma, dass $\Phi^{-1}((g)) = (h)$ für ein $h \in k[x_1, \ldots, x_n]$ und daher auch $\Phi^{-1}(\sqrt{(g)}) = \sqrt{(h)} = (h')$ für ein gewisses $h' \in k[x_1, \ldots, x_l]$ (Die letzte Gleichheit folgt wiederum daraus, dass der Polynomring faktoriell ist). Ausserdem ist auch

$$k[x_1, \ldots, x_l]/(h') \to R/\sqrt{(g)}$$

endlich und daher sind die Transzendenzgrade der Quotientenkörper gleich. Es gilt nun aber nach Lemma 3.5.7, $\mathrm{trdeg}(\mathrm{Quot}(k[x_1, \ldots, x_l]/(h'))) = l - 1$. □

Diesen Satz können wir geometrisch so formulieren: Sei V eine *irreduzible* affine Varietät. Für jedes $g \in \mathcal{O}(V)$ und für jede irreduzible Komponente $Z \subseteq V(g)$ gilt:

$$\dim(Z) = \dim(V) - 1.$$

Der Beweis den wir gegeben haben stammt von Mumford und benutzt geometrische Argumente (und damit insbesondere den Hilbertschen Nullstellensatz) in Form von Proposition 1.7.9. Es gibt jedoch einen sehr trickreichen und kurzen rein algebraischen Beweis (siehe z.B. das Buch von Atiyah Macdonald [AM] oder Eisenbud [E]) oder man kann "Going-down" verwendet, siehe Appendix.
Wir können nun die anvisierten Aussagen der Dimensionstheorie beweisen:

Satz 3.3.2.

0. *Für alle irreduziblen affinen Varietäten V gilt* $\dim V < \infty$.
1. *Für zwei* irreduzible *affine Varietäten $V \subset W$ gilt* $\dim(V) < \dim(W)$ *oder* $V = W$.
2. *Für* irreduzible *affine Varietäten $V \subsetneq W$ mit* $\dim(V) \leq \dim(W) + 2$ *gibt es eine irreduzible affine Varietät Z mit $V \subsetneq Z \subsetneq W$.*
3. $\dim \mathbb{A}^n = n$.

Beweis. 0. folgt aus 1. und 3.
1. folgt unter Verwendung von Satz 3.6.2 aus Lemma 3.6.1.
2. Seien $V \subsetneq W$ zwei irreduzible affine Varietäten mit $\dim(V) \leq \dim(W) - 2$ und sei $V = V(I)$ für $I = (f_1, \ldots, f_n) \subset \mathcal{O}(W)$ ein Primideal. Sei V' eine irreduzible Komponente von $V(f_1)$. Dann gilt $V \subset V' \subsetneq W$ und nach Krulls Hauptidealsatz (geometrische Fassung) ist $\dim(V') = \dim(W) - 1$. Nach 1. folgt daher

$$V \subsetneq V' \subsetneq W.$$

4. folgt aus Satz 3.6.2 angewendet auf $k[x_1, \ldots, x_n]$. □

Beachte, aus 3.3.2 folgt auch die **Äquidimensionalität** einer irreduziblen affinen Varietät, d.h. *jede* Kette von irreduziblen affinen Untervarietäten $Z_i \subset V$

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_k$$

kann zu einer Kette der Länge $n = \dim(V)$ erweitert werden (natürlich nicht notwendigerweise rechts oder links, sondern immer dort, wo die Dimension um mindestens 2 springt).

Appendix

Hier folgt noch ein Beweis von Krulls Hauptidealsatz in voller Allgemeinheit unter Verwendung von "Going down":

Satz 3.6.6 (Krulls Hauptidealsatz (beliebiger Körper))**.** *Sei k ein Körper und sei R eine endlich erzeugte nullteilerfreie k-Algebra, $0 \neq g \in R$ und $\wp$ ein Primideal, welches minimal ist mit der Eigenschaft $g \in \wp$. Dann ist* $\operatorname{trdeg}(\operatorname{Quot}(R/\wp)) = \operatorname{trdeg}(\operatorname{Quot}(R)) - 1$.

Beweis. Sei $\Phi : k[x_1, \ldots, x_l] \to R$ der injektive endliche k-Algebrenhomomorphismus aus dem Noetherschen Normalisierungslemma. Wir haben nach Lemma 3.6.4, dass $\Phi^{-1}((g)) = (h)$ und wir haben $\sqrt{(h)} = (h_1) \cap \cdots \cap (h_k)$, da $k[x_1, \ldots, x_l]$ faktoriell ist, wobei die (h_i) Primideale sind (die h_i sind einfach die irreduziblen Faktoren ohne Multiplizität von h). Wir können ein i wählen, so dass $h_i \in \wp$, da $\wp$ prim ist. Nach dem Beweis von "Going-down" gilt für die zusammengesetzte injektive Abbildung

$$\Psi : k[x_1, \ldots, x_l] \to R \to R_\wp$$

die Aussage:

$$R_\wp(h_i) \cap k[x_1, \ldots, x_l] = (h_i)$$

Daraus wurde mit Lemma 3.4.3 gefolgert, dass $(h_i) \subset k[x_1, \ldots, x_n]$ Urbild eines Primideales P' in $R_\wp$ ist. Im Beweis von Lemma 3.4.3 geschieht das, indem $R_\wp$ an der Menge $S = k[x_1, \ldots, x_l] \setminus (h_i)$ lokalisiert wird und darin ein beliebiges maximales Ideal gewählt wird, dass das Ideal $R_\wp[S^{-1}](h_i)$ enthält. Wir wählen stattdessen ein maximales Ideal $\mathfrak{m} \subset R_\wp[S^{-1}]$, welches g enthält. Dazu müssen wir zunächst überprüfen, dass g keine Einheit ist. g ist aber weder in $S_\wp$, da $g \in \wp$ noch in $k[x_1, \ldots, x_l] \setminus (h_i)$, denn wenn es in $k[x_1, \ldots, x_l]$ wäre, so wäre $(g) = (h)$ und wir haben ja $h \in (h_i)$. Sei also $\mathfrak{m}$ ein maximales Ideal von $R_\wp[S^{-1}]$ welches g enthält und sei $\mathfrak{p} = \mathfrak{m} \cap k[x_1, \ldots, x_l]$. Wir haben $\mathfrak{p} \subset (h_i)$, da $\mathfrak{m}$ keine Einheiten des Ringes $R_\wp[S^{-1}]$ enthält. Ausserdem ist $h \in \mathfrak{p}$ (denn h ist ein Vielfaches von g), $\mathfrak{p}$ ist also nicht das Nullideal. Es folgt $\mathfrak{p} = (h_i)$ (da $k[x_1, \ldots, x_l]$ faktoriell[13]). Sei $P = \mathfrak{m} \cap R$. Falls $(h_i) \subsetneq (\wp \cap k[x_1, \ldots, x_l])$ gelten würde, hätten wir auch $P \subsetneq \wp$. Da aber $g \in P$ nach Konstruktion, widerspräche dies der Minimalität von $\wp$. Es gilt also $\wp \cap k[x_1, \ldots, x_l] = (h_i)$ und daher ist die Erweiterung

$$k[x_1, \ldots, x_l]/(h_i) \to R/\wp$$

endlich und daher $\operatorname{trdeg}(\operatorname{Quot}(R/\wp)) = \operatorname{trdeg}(\operatorname{Quot}(k[x_1, \ldots, x_l]/(h_i)))$. Letzterer ist nach Lemma 3.5.7 gleich $l - 1$. □

[13] Sei $0 \neq x \in \mathfrak{p}$. Schreibe $x = (h_i)^k \alpha$, wobei $h_i \not| \alpha$ (eindeutige Primfaktorzerlegung). Wegen $x \in (h_i)$ folgt $k \geq 1$. Dann folgt, da $\mathfrak{p}$ prim ist: $h_i \in \mathfrak{p}$.

Inhaltsverzeichnis