Elementare Algebraische Geometrie

Ilia Pirashvili

SS 2023
Universität Augsburg

Inhaltsverzeichnis

1 Affine Geometrie **5**

1.1 Affine Räume . . . 5

1.1.1 Der Koordinatenring eines affinen Raumes . . . 5

1.1.2 Die Zuordnung $\mathrm{V}(-)$ . . . 8

1.1.3 Die Zuordnung $\mathrm{I}(-)$ . . . 11

1.1.4 Der algebraische Abschluss und $\mathrm{V}(\mathrm{I}(-))$ . . . 13

1.2 Hilberts Nullstellensatz und $\mathrm{I}(\mathrm{V}(-))$ . . . 15

1.2.1 Noethersche Ringe und der Hilbertsche Basissatz . . . 15

1.2.2 Radikale Ideale . . . 17

1.2.3 Lokalisierungen und der Quotientenkörper . . . 21

1.2.4 Hilberts Nullstellensatz . . . 26

1.2.5 Primideale und Irreduzible Varietäten . . . 33

1.3 Affine Varietäten und deren Koordinatenringe . . . 35

1.3.1 Der Koordinatenring $K[\mathrm{V}]$ einer Varietät . . . 35

1.3.2 Die Ideale von $K[\mathrm{V}]$ . . . 36

1.3.3 Morphismen zwischen Varietäten . . . 38

1.4 Komplemente von affinen Varietäten und Lokalisierungen . . . 46

1.4.1 Rationale Abbildungen . . . 46

1.5 Punkte, Halme und lokale Ringe . . . 51

1.5.1 Lokalisierung an Prim-/Maximalidealen . . . 51

1.5.2 Der Halm $\mathcal{O}_a$ . . . 54

1.5.3 Der Halm $\mathcal{O}_a(\mathrm{V})$ auf einer Varietät . . . 56

2 Planare affine Kurven und die Schnittzahl **60**

2.1 Klassifikation algebraischer Teilmengen von $\mathbb{A}^2$ . . . 60

2.2 Vielfachheit und Tangenten . . . 63

2.3 Multiplizität und diskrete Bewertungsringe . . . 70

2.3.1 Relativ Maximale Ideale . . . 72

2.3.2 Exakte Sequenzen und K-Vektorräume . . . 78

2.3.3 Multiplizität eines Polynoms an einem Punkt . . . 84

2.3.4 Diskrete Bewertungsringe . . . 87

2.4 Die Schnittzahl . . . 91

3 Projektive Geometrie **104**

3.1 Die projektive Fläche $\mathbb{P}^2$ . . . 104

3.1.1 Homogene Koordinaten . . . 106

3.1.2 Projektive Varietäten . . . 108

3.1.3 Homogene Primideale und irreduzible Varietäten . . . 112
3.1.4 Hauptproblem von projektiven Varietäten - Grenzen der Koordinatenringe . . . 115
3.1.5 Projektive Koordinatentransformationen . . . 117
3.2 Die affine Überdeckung . . . 119
3.2.1 Homogenisierung und Dehomogenisierung von Polynomen . . . 119
3.2.2 Homogenisierung und Dehomogenisierung von Idealen und Varietäten . 121
3.2.3 Dehomogenisierung von Elementen des Koordinatenrings . . . 125

4 Planare projektive Kurven **128**
4.1 Lokale Eigenschaftgen und die projektive Schnittzahl . . . 128
4.1.1 Definitionen und Notationen von lokalen Eigenschaften . . . 128
4.1.2 Die projektive Schnittzahl . . . 130
4.2 Der Satz von Bézout . . . 133
4.3 Divisoren . . . 139
4.4 (Max) Noetherscher Fundamentalsatz . . . 143
4.5 Der Satz von Pappos . . . 147
4.6 Die Picardgruppe . . . 149
4.6.1 Die Picardgruppe von Kurven mit Grad ≤ 2 . . . 149
4.6.2 Die Picardgruppe von Kurven mit Grad ≥ 3 . . . 150
4.7 Elliptische Kurven . . . 152
4.7.1 Die Verknüpfung durch die Geometrie . . . 152
4.7.2 Die Verknüpfung durch die Picardgruppe . . . 154
4.8 Der Satz von Riemann-Roch - Nicht mehr Teil des Kurses! . . . 157

5 Appendix **169**
5.1 Das Lemma von Gauß . . . 169
5.1.1 Primitive Polynome . . . 169

Danksagung

Ein großen Dank and Lukas Stoll, der das Skript überarbeitet und viele Korrekturen vorgenommen hat.

1 Affine Geometrie

1.1 Affine Räume

1.1.1 Der Koordinatenring eines affinen Raumes

Definition 1.1.1. *Sei K ein Körper. Wir definieren den* affinen Raum *der Dimension n über K als*

$$\mathbb{A}^n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in K\}.$$

Wenn wir den Grundkörper spezifizieren wollen, schreiben wir $\mathbb{A}^n_K$. Es ist direkt ersichtlich, dass dies als Menge dem n-fachen Produkt K^n von K mit sich selbst entspricht. Wir benutzen eine distinkte Notation, weil wir die beiden Objekte mit verschieden Strukturen versehen wollen. Zum Beispiel ist K^n in natürlicher Weise ein K-Vektorraum (sogar eine K-Algebra), wohingegen wir $\mathbb{A}^n$ eher geometrisch auffassen.

Polynomielle Abbildungen vs. Polynome Sei $f \in K[x_1, \ldots, x_n]$ ein Polynom in n Variablen. Dies definiert eine Abbildung

$$f : \mathbb{A}^n \to K, \quad \text{gegeben durch} \quad (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n). \tag{1}$$

Man könnte nun meinen, dass man durch diese Abbildung das Polynom wieder zurückerhält. Dies ist jedoch nicht der Fall, wie man am folgendem Beispiel sieht (oder siehe auch Beispiel 1.1.5):

Beispiel 1.1.2. Sei $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ der Körper mit 2 Elementen. Das Polynom $f \in \mathbb{F}_2[x]$, gegeben durch $f(x) = x$ induziert die Abbildung

$$\mathbb{A}^1 \to \mathbb{F}_2, \quad \text{gegeben durch} \quad (a) \mapsto a.$$

Das Problem ist, dass $g(x) = x^2$, welches die Abbildung $a \mapsto a^2$ definiert, damit übereinstimmt, denn $f(0) = 0$, $g(0) = 0$ und $f(1) = 1$ und $g(1) = 1$. In $\mathbb{A}^1$ haben wir aber keine weiteren Elemente. Damit stimmen $f, g : \mathbb{A}^1 \to \mathbb{F}_2$ miteinander an jedem Punkt überein. Als solches sind es die selben Abbildungen.

Man erinnere sich an die folgende Definition:

Definition 1.1.3. *Ein Ring R wird* Integritätsbereich *genannt, wenn für all $a, b \in R$, aus $ab = 0$ folgt $a = 0$ oder $b = 0$.*

Es ist wohlbekannt (man überprüfe es selbst), dass jeder Körper ein Integritätsbereich ist. Ebenso ist der Polynomring $R[x_1, \ldots, x_n]$ in n Variablen über einem Integritätsbereich selbst wieder ein Integritätsbereich.

Obwohl dieser Kurs sich nur über Körpern abspielen wird, werden wir das folgende Lemma für Integritätsbereiche formulieren, da dies den Beweis vereinfacht.

Lemma 1.1.4. *Sei K ein Integritätsbereich mit $|K| = \infty$ und $f \in K[x_1, \ldots, x_n]$ ein Polynom, sodass $f : \mathbb{A}^n \to K$ die konstante Nullfunktion ist. Dann ist $f = 0$ das Nullpolynom.*

Beweis. Dies ist einfach per Induktion über den Grad m des Polynoms $f(x)$ und der Anzahl n der Variablen zu zeigen. Der Fall $m = 0$ ist klar, da ein konstantes Polynom genau dann Null ist, wenn es Null ist.

Seien $m > 0$, $n = 1$ (sprich $f \in K[x]$ mit $\mathsf{grad}(f) \geq 1$) und $a_1 \in K$. Per Annahme gilt $f(a_1) = 0$ und daher ist $(x - a_1)$ ein Teiler von $f(x)$ (siehe ??). Wir erhalten $f(x) = (x - a_1)f'(x)$ für irgendein $f'(x) \in K[x_1, \ldots, x_n]$ mit $\mathsf{grad}(f') < \mathsf{grad}(f)$. Wir machen weiter indem wir ein weiteres $a_2 \in K$ nehmen und $f'(x) = (x - a_2)f''(x)$ schreiben, was zu $f(x) = (x - a_1)(x - a_2)f''(x)$ führt. Da der Grad streng monoton abnimmt und K unendlich viele Elemente hat, wird f irgendwann in Linearfaktoren zerlegt sein, also

$$f(x) = (x - a_1)\cdots(x - a_m).$$

Man wähle ein $b \neq a_i$, $1 \leq i \leq m$, welches von allen a_i verschieden ist. Dies ist möglich, da K unendlich viele Elemente hat. Da auch $f(b) = 0$ ist, gilt $(b - a_1)\cdots(b - a_m) = 0$. In einem Integritätsbereich impliziert dies $(b - a_i) = 0$ für irgendeine der Komponenten. Dies führt zum Widerspruch, da bei unserer Wahl $b \neq a_i$ für alle i ist. Somit muss $m = 0$ gelten, also der Grad von f gleich Null sein. Dies wiederum impliziert, dass f das Nullpolynom ist.

Sei nun $f \in K[x_1, \ldots, x_n]$ mit $n > 1$. Fixiere x_n und betrachte f als Polynom in einer Variable über x_n, mit Koeffizienten im Ring $R = K[x_1, \ldots, x_{n-1}]$. Wir haben

$$f(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1}) + f_1(x_1, \ldots, x_{n-1})x_n + \cdots + f_m(x_1, \ldots, x_{n-1})x_n^m.$$

Da K ein Integritätsbereich war, ist auch R ein Integritätsbereich, womit sich das obige Argument anwenden lässt. Es folgt, dass $m = 0$ und somit $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1})$ ist. Wir haben damit die Anzahl der Variablen verringert und es folgt per Induktion, dass f das Nullpolynom ist. □

Wir brauchen tatsächlich, dass K unendlich viele Elemente hat, wie man am folgendem Beispiel sieht:

Beispiel 1.1.5. Sei $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ und $h(x) = x^2 - x \in K[x]$. Es ist $0 \neq h(x)$ in $K[x]$, aber $h(0) = 0$ und $h(1) = 0$, womit h die Nullfunktion darstellt. Man bemerke, dass unser $h(x) = f(x) - g(x)$, wobei f, g die Polynome vom Beispiel 1.1.2 sind.

Lemma 1.1.6. *Die Abbildung (1) definiert das Polynom eindeutig genau dann, wenn K unendlich viele Elemente hat.*

Beweis. Sei $|K| = \infty$ unendlich und seien $f, g \in K[x_1, \ldots, x_n]$ Polynome in n Variablen, sodass $f(a) = g(a)$ für alle $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ gilt. Betrachte $h(x) := f(x) - g(x)$, wobei $x = (x_1, \ldots, x_n)$. Dann ist $h(a) = f(a) - g(a) = 0$ für alle Elemente von K. Lemma 1.1.4 gibt nun den Beweis.

Auf der anderen Seite, sei K endlich mit m Elementen. Da es genau m^m Abbildungen von K nach K gibt, es aber mehr als m^m verschiedene Polynome (der Grad ist unbegrenzt), müssen verschiedene Polynome zwangsweise dieselbe Abbildung definieren. □

Man könnte dies auch wie folgt ausdrücken: Die Abbildung $K[x_1, \ldots, x_n] \to \mathsf{Abb}(\mathbb{A}^n, K)$, gegeben durch $f \mapsto f(a_1, \ldots, a_n)$, ist injektiv genau dann, wenn K unendlich ist. Ironischerweise braucht man das K endlich ist, damit diese Abbildung surjektiv ist.

Im Hauptteil des Kurses werden wir uns auf algebraisch abgeschlossene Körper beschränken. Da diese immer unendlich viele Elemente haben (siehe **??**), betten Polynome injektiv in Abbildungen ein. Somit können wir Polynome mit den von ihnen definierten Abbildungen gleichsetzen.

Nullstellen Das Ziel der algebraischen Geometrie ist es, die Nullstellen von Polynomen in mehreren Variablen zu studieren.

Definition 1.1.7. *Ein Punkt $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ heißt* Nullstelle *von f falls $f(a) = 0$.*

Im Gegensatz zu Polynomen in einer Variable hat ein Polynom in mehreren Variablen im Allgemeinen unendlich viele Nullstellen. Als Beispiel betrachte man die klassische Parabel (über $\mathbb{R}$). Wir haben sogar folgendes Resultat:

Lemma 1.1.8. *Sei K algebraisch abgeschlossen und $c \neq f \in K[x_1, \ldots, x_n]$ mit $n \geq 2$ ein nichtkonstantes Polynom. Dann hat f unendlich viele Nullstellen.*

Beweis. Sei $n = 2$. Da $f \in K[x, y] = K[x][y]$, können wir

$$f(x, y) = f_0(x) + f_1(x)y + \cdots + f_m(x)y^m,$$

schreiben, wobei $m \in \mathbb{N}$ die größte natürliche Zahl mit $f_m(x) \neq 0$ ist. Wenn $m = 0$, dann folgt $f(x, y) = f_0(x)$. Da f nicht konstant ist, hat $f_0(x)$ mindestens eine Nullstelle $a \in K$ (K ist algebraisch abgeschlossen). Daher ist (a, y) eine Nullstelle für jedes $y \in K$.

Sei $m \neq 0$. Da $f_m(x) \in K[x]$ nur endlich viele Nullstellen hat, gibt es unendlich viele $a_\alpha \in K$ mit $f_m(a_\alpha) \neq 0$. Für jedes dieser a_α ist nun $f(a_\alpha, y)$ ein Polynom vom Grad $m \geq 1$ in $K[y]$ und da K algebraisch abgeschlossen ist, hat es mindestens eine Nullstelle b_α. Somit ist (a_α, b_α) eine Nullstelle von $f(x, y)$. All diese Nullstellen sind paarweise verschieden, da schon die a_α paarweise verschieden sind. Insgesamt haben wir also unendlich viele Nullstellen (a_α, b_α) gefunden.

Sei nun $n \geq 2$ und $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$. Betrachte das Polynom $g(x_1, x_2) = f(x_1, x_2, 1, \ldots, 1) \in K[x_1, x_2]$. Jede Nullstelle (a_1, a_2) von g liefert dann eine Nullstelle $(a_1, a_2, 1, \ldots, 1)$ von f. Nach obiger Betrachtung hat g unendlich viele Nullstellen, also gilt dies auch für f. □

Bemerkung 1.1.9. Ein weiterer Unterschied zum Fall mit einer Variablen ist, dass die Existenz von Nullstellen eines Polynoms nicht mehr dessen Reduzierbarkeit impliziert: Aus $f(a) = 0$ folgt $f(x) = (x-a)f'$, aber aus $f(a, b) = 0$ folgt nicht, dass $f(x, y) = (x-a)(y-b)g(x, y)$ (oder eine andere Faktorisierung). Zum Beispiel ist $(0, 0)$ eine Nullstelle der Parabel $f(x, y) = y - x^2$, aber $f(x, y) \neq xy \cdot g(x, y)$. Ebenso wenig lässt sich (a, b) auf eine andere Art und Weise "ausklammern", da $f(x, y) = y - x^2$ irreduzibel ist.

1.1.2 Die Zuordnung $\mathrm{V}(-)$

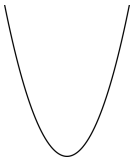
Von nun an sei K ein Körper mit unendlich vielen Elementen, solange wir nicht explizit etwas anderes fordern.

Das Nullstellengebilde

Definition 1.1.10. *Das* Nullstellengebilde $\mathrm{V}(f)$ *eines Polynoms* $f \in K[x_1, \ldots, x_n]$ *ist definiert als die Menge der Nullstellen von* f*. Mit anderen Worten ist*

$$\mathrm{V}(f) \coloneqq \{a \in \mathbb{A}^n \mid f(a) = 0\} \subseteq \mathbb{A}^n.$$

Beispiel 1.1.11. Sei $K = \mathbb{R}, n = 2$ und $f(x, y) = y - x^2$. Dann ist $\mathrm{V}(f)$ eine klassische Parabel:



Die Konstruktion lässt sich verallgemeinern:

Definition 1.1.12. *Das Nullstellengebilde* $\mathrm{V}(T)$ *einer Teilmenge* $T \subseteq K[x_1, \ldots, x_n]$ *ist definiert als*

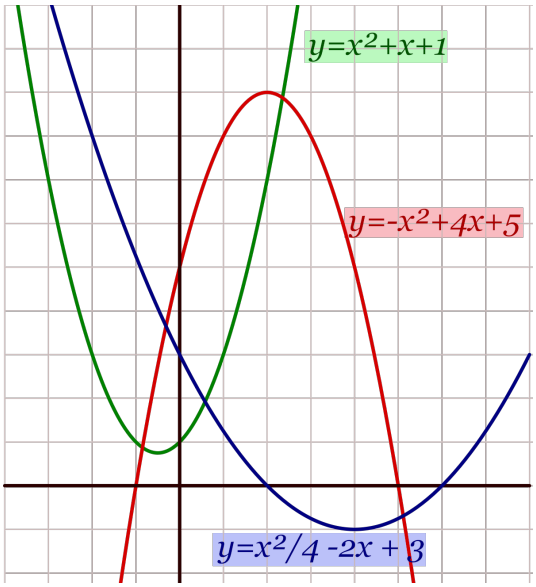
$$\mathrm{V}(T) \coloneqq \{a \in \mathbb{A}^n \mid f(a) = 0 \text{ für alle } f \in T\}.$$

Mit anderen Worten ist

$$\mathrm{V}(T) = \bigcap_{f \in T} \mathrm{V}(f).$$

Beispiel 1.1.13. Seien $f = y - x^2 - x - 1$, $g = y + x^2 - 4x - 5$ und $h = y - \frac{x^2}{4} + 2x - 3$. Dann ist $\mathrm{V}(f)$ die grüne Parabel, $\mathrm{V}(g)$ die rote, $\mathrm{V}(h)$ die blaue, die Mengen $\mathrm{V}(f, g)$, $\mathrm{V}(f, h)$ und

$V(g,h)$ jeweils die 2 Schnittpunkte und $V(f,g,h)$ ist die leere Menge.



Derartige Mengen, welche sich als Nullstellengebilde von Polynomen ausdrücken lassen, werden *algebraisch* genannt.

Algebraische Mengen

Definition 1.1.14. *Eine* algebraische Menge *oder* algebraische Varietät *ist eine Teilmenge* $X \subseteq \mathbb{A}^n$ *für die eine Menge von Polynomen* $T \subseteq K[x_1,\dots,x_n]$ *existiert, sodass* $X = V(T)$.

Wir wollen nun eine Topologie (man erinnere sich an die Definition) auf $\mathbb{A}^n$ definieren, deren abgeschlossene Mengen die algebraischen Mengen werden sollen. Dafür müssen wir die Abbildung

$$V(-) : \{\text{Teilmengen von } K[x_1,\dots,x_n]\} \to \{\text{Teilmengen von } \mathbb{A}^n\}$$

etwas genauer studieren.

Lemma 1.1.15. *Sei* $T \subseteq S \subseteq K[x_1,\dots,x_n]$. *Es gilt* $V(S) \subseteq V(T)$.

Beweis. Sei $a \in V(S)$, sprich $f(a) = 0$ für alle $f \in S$. Da $T \subseteq S$, gilt auch $f(a) = 0$ für alle $f \in T$ und damit ist $a \in V(T)$. □

Lemma 1.1.16. *Es gilt* $V(T) = V(J)$, *wobei* $J = (T) \subseteq K[x_1,\dots,x_n]$ *das von* T *erzeugte Ideal ist.*

Beweis. Die Inklusion $V(J) \subseteq V(T)$ folgt direkt aus Lemma 1.1.15. Für die andere Inklusion sei $g \in J$. Per Definition gibt es $h_1,\dots,h_l \in T$ und $q_1,\dots,q_l \in K[x_1,\dots,x_n]$, sodass

$$g = h_1 q_1 + \cdots + h_l q_l.$$

Sei nun $a \in V(T)$. Daher, $h_1(a) = \cdots = h_l(a) = 0$, was $g(a) = 0$ also $a \in V(J)$ impliziert. □

Lemma 1.1.17. *Seien $I, J, J_\lambda \subseteq K[x_1, \ldots, x_n]$ Ideale. Es gelten folgende Eigenschaften:*

(i) $\mathrm{V}(0) = \mathbb{A}^n$,

(ii) $\mathrm{V}(K[x_1, \ldots, x_n]) = \varnothing$,

(iii) $\mathrm{V}(I) \cup \mathrm{V}(J) = \mathrm{V}(IJ)$,

(iv) $\bigcap_{\lambda \in \Lambda} \mathrm{V}(J_\lambda) = \mathrm{V}\left(\sum_{\lambda \in \Lambda} J_\lambda\right)$.

Zur Erinnerung, das Ideal $\sum_{\lambda \in \Lambda} J_\lambda$ kann auch als $\left(\bigcup_{\lambda \in \Lambda} J_\lambda\right)$ geschrieben werden. Es ist das Ideal erzeugt mit der Vereinigung aller Ideale J_λ.

Beweis.

(i) Jeder Punkt ist Nullstelle des Nullpolynoms.

(ii) Kein Punkt ist Nullstelle des konstanten Polynoms 1. Man beachte, dass $1 \neq 0$ in K.

(iii) Da $IJ \subseteq I \cap J \subseteq I$, wissen wir von Lemma 1.1.15, dass $\mathrm{V}(I) \subseteq \mathrm{V}(IJ)$ folgt. Ebenso gilt auch $\mathrm{V}(J) \subseteq \mathrm{V}(IJ)$, womit $\mathrm{V}(I) \cup \mathrm{V}(J) \subseteq \mathrm{V}(IJ)$ bewiesen ist.

Sei $a \in \mathrm{V}(IJ)$. Wenn $a \notin \mathrm{V}(I)$, gibt es ein $f \in I$ mit $f(a) \neq 0$. Sei $g \in J$ beliebig. Da $fg \in IJ$, ist $(fg)(a) = f(a)g(a) = 0$. Da $K[x_1, \ldots, x_n]$ ein Integritätsbereich ist, impliziert dies $g(a) = 0$. Es folgt, dass $a \in \mathrm{V}(J)$, und damit $a \in \mathrm{V}(I) \cup \mathrm{V}(J)$.

(iv) Da $J_\lambda \subseteq \sum_{\lambda \in \Lambda} J_\lambda$, besagt Lemma 1.1.15, dass $\mathrm{V}\left(\sum_{\lambda \in \Lambda} J_\lambda\right) \subseteq \mathrm{V}(J_\lambda)$. Dies gilt für jedes $\lambda \in \Lambda$ und daher ist $\mathrm{V}\left(\sum_{\lambda \in \Lambda} J_\lambda\right) \subseteq \bigcap_{\lambda \in \Lambda} \mathrm{V}(J_\lambda)$.

Auf der anderen Seite, sei $a \in \bigcap_{\lambda \in \Lambda} \mathrm{V}(J_\lambda)$, also $f(a) = 0$ für alle $f \in J_\lambda$ für jedes λ. Es folgt $f(a) = 0$ für alle $f \in \bigcup_{\lambda \in \Lambda} J_\lambda$, was $a \in \mathrm{V}\left(\bigcup_{\lambda \in \Lambda} J_\lambda\right)$ impliziert. Lemma 1.1.16 liefert nun die gewünschte Aussage, da wir

$$\mathrm{V}\left(\bigcup_{\lambda \in \Lambda} J_\lambda\right) = \mathrm{V}\left(\left(\bigcup_{\lambda \in \Lambda} J_\lambda\right)\right) = \mathrm{V}\left(\sum_{\lambda \in \Lambda} J_\lambda\right)$$

haben. (In der Mitte meinen wir das Ideal erzeugt von der Vereinigung der Ideale, was im Allgemeinen kein Ideal ist). □

Nun können wir die Topologie einführen.

Die Zariski-Topologie

Definition/Lemma 1.1.18. *Wir definieren eine Topologie auf $\mathbb{A}^n$, genannt die* Zariski-Topologie*, indem wir genau die algebraische Mengen als abgeschlossen bezeichnen.*

Beweis. Die Eigenschaften einer Topologie werden in Lemma 1.1.17 nachgewiesen. □

Bemerkung 1.1.19. Von nun an werden wir $\mathbb{A}^n$ immer als topologischen Raum auffassen (mit der Zariski-Topologie). Es sollte erwähnt werden, dass sich diese Topologie deutlich von der gewohnten Topologie auf $\mathbb{R}^n$ unterscheidet. Zum Beispiel ist sie nicht Hausdorffsch, die offenen Mengen sind "riesig". Auch von "Lokalheit" kann man nicht ohne Weiteres in einer sinnvollen Art und Weise reden, siehe auch Bemerkung 1.5.8. Im Abschnitt 1.5 werden wir den Begriff des Halms einführen um "lokale" Eigenschaften auszudrücken.

1.1.3 Die Zuordnung $\mathrm{I}(-)$

Wir haben jeder Menge von Polynomen $T \subseteq K[x_1, \ldots, x_n]$ ihre Verschwindungsmenge $V(T) \subseteq \mathbb{A}^n$. In die umgekehrte Richtung lässt sich aber auch gehen.

Das Verschwindungsideal

Definition 1.1.20. *Sei $X \subseteq \mathbb{A}^n$ eine Teilmenge. Wir definieren*

$$\mathrm{I}(X) := \{f \in K[x_1, \cdots, x_n] \mid f(a) = 0 \text{ für alle } a \in \mathbb{A}^n\}$$

und nennen die so definierte Teilmenge das Verschwindungsideal *von X.*

Lemma 1.1.21. *Für jede Teilmenge $X \subseteq \mathbb{A}^n$ ist $\mathrm{I}(X)$ ein Ideal von $K[x_1, \ldots, x_n]$.*

Beweis. Die Eigenschaften sind einfach zu überprüfen. Da $0(a) = 0$ ist $0 \in \mathrm{I}(X)$. Seien $f, g \in \mathrm{I}(X)$ und $h \in K[x_1, \ldots, x_n]$. Dann ist $f + g \in \mathrm{I}(X)$ und $fh \in \mathrm{I}(X)$, da $f(a) + g(a) = 0 + 0$ für alle $a \in X$ und $f(a)h(a) = 0h(a) = 0$. □

Analog zu den Lemmas 1.1.17 und 1.1.15 haben wir folgende Resultate für $\mathrm{I}(-)$:

Lemma 1.1.22. *Sei $X \subseteq Y$. Dann ist $\mathrm{I}(Y) \subseteq \mathrm{I}(X)$.*

Beweis. Sei $f \in \mathrm{I}(Y)$, daher $f(a) = 0$ für alle $a \in Y$. Damit ist auch $f(a) = 0$ für alle $a \in X \subseteq Y$ und $f \in \mathrm{I}(X)$. □

Lemma 1.1.23. *Sei $(X_\lambda)_{\lambda \in \Lambda}$ eine Familie von Teilmengen von $\mathbb{A}^n$.*

(i) $\mathrm{I}(\varnothing) = K[x_1, \ldots, x_n]$,

(ii) $\mathrm{I}(\mathbb{A}^n) = 0$,

(iii) $\sum\limits_{\lambda\in\Lambda} \mathrm{I}(X_\lambda) \subseteq \mathrm{I}\left(\bigcap\limits_{\lambda\in\Lambda} X_\lambda\right)$,

(iv) $\bigcap\limits_{\lambda\in\Lambda} \mathrm{I}(X_\lambda) = \mathrm{I}\left(\bigcup\limits_{\lambda\in\Lambda} X_\lambda\right)$.

Bemerkung 1.1.24. Aufgepasst, bei (*iii*) ist hier keine Gleichung mehr. Siehe Beispiel 1.1.25.

Beweis. (i) Dies mag etwas seltsam erscheinen. Wir betrachten die Menge der Polynome $f(x)$, sodass $f(a) = 0$ für alle $a \in \varnothing$. Daher haben wir also keine Bedingung auf f und somit sind alle erlaubt.

(ii) Dies ist die Aussage von Lemma 1.1.4.

(iii) Da $\bigcap\limits_{\lambda\in\Lambda} X_\lambda \subseteq X_\lambda$, besagt Lemma 1.1.22, dass $\mathrm{I}(X_\lambda) \subseteq \mathrm{I}\left(\bigcap\limits_{\lambda\in\Lambda} X_\lambda\right)$. Da dies für jedes $\lambda \in \Lambda$ gilt, ist

$$\sum_{\lambda\in\Lambda} \mathrm{I}(X_\lambda) = \left(\bigcup_{\lambda\in\Lambda} \mathrm{I}(X_\lambda)\right) \subseteq \mathrm{I}\left(\bigcap_{\lambda\in\Lambda} X_\lambda\right).$$

Hier haben wir die Tatsache verwendet, dass für jedes Ideal J und jede Teilmenge $T \subseteq J$ schon $(T) \subseteq J$ gilt.

(iv) Aus $X_\lambda \subseteq \bigcup\limits_{\lambda\in\Lambda} X_\lambda$ folgt mit Lemma 1.1.22, dass $\mathrm{I}\left(\bigcup\limits_{\lambda\in\Lambda} X_\lambda\right) \subseteq \mathrm{I}(X_\lambda)$. Da dies für jedes $\lambda \in \Lambda$ gilt, folgt $\mathrm{I}\left(\bigcup\limits_{\lambda\in\Lambda} X_\lambda\right) \subseteq \bigcap\limits_{\lambda\in\Lambda} \mathrm{I}(X_\lambda)$.

Auf der anderen Seite sei $f \in \bigcap\limits_{\lambda\in\Lambda} \mathrm{I}(X_\lambda)$, also $f(a) = 0$ für alle $a \in X_\lambda$ und für jedes $\lambda \in \Lambda$. Das bedeutet, dass $f(a) = 0$ für alle $a \in \bigcup\limits_{\lambda\in\Lambda} X_\lambda$, womit $f \in \mathrm{I}\left(\bigcup\limits_{\lambda\in\Lambda} X_\lambda\right)$ ist.

□

Beispiel 1.1.25. Seien $X = \mathrm{V}(x)$ und $Y = \mathrm{V}(x^2 - y^2)$ Teilmengen von $\mathbb{A}^2$. Beachte, dass $X \cap Y = \{(0,0)\}$, also $\mathrm{I}(X \cap Y) = (x, y)$. Wir wollen nun zeigen, dass $\mathrm{I}(X) + \mathrm{I}(Y)$ ein strikt kleineres Ideal ist, was die Ungleichung in Lemma 1.1.23 (iii) rechtfertigt.

Zunächst kann man sich davon überzeugen, dass $\mathrm{I}(X) = \mathrm{I}(\mathrm{V}(x)) = (x)$ (dafür werden wir bald explizite Formeln haben). Andererseits ist

$$Y = \mathrm{V}\left(x^2 - y^2\right) = \mathrm{V}\left((x-y)(x+y)\right) = \mathrm{V}(x-y) \cup \mathrm{V}(x+y),$$

wobei die letzte Gleichung aus Lemma 1.1.17 (iii) folgt. Dies impliziert

$$\mathrm{I}(Y) = \mathrm{I}\left(\mathrm{V}\left(x^2 - y^2\right)\right) = \mathrm{I}\left(\mathrm{V}(x-y) \cup \mathrm{V}(x+y)\right).$$

Anwendung von Lemma 1.1.23 (iv) liefert, dass dies gleich

$$\mathrm{I}(V(x-y)) \cap \mathrm{I}(\mathrm{V}(x+y)) = (x-y) \cap (x+y)$$

ist. Unter Vorgriff auf Lemma 2.3.9 haben wir $(x-y)\cap(x+y) = (x^2-y^2)$, was zusammengefasst

$$\mathrm{I}(\mathrm{V}(x^2-y^2)) = (x^2-y^2)$$

ergibt. Damit gilt

$$\mathrm{I}(X) + \mathrm{I}(Y) = \left(x, x^2-y^2\right) = \left(x, y^2\right) \subsetneq (x,y) = \mathrm{I}(X \cap Y).$$

Zwischen Idealen und algebraischen Mengen Wir haben zwei entgegengesetzte Abbildungen

$$\{ \text{ Teilmengen von } K[x_1,\ldots,x_n] \} \underset{\mathrm{I}}{\overset{\mathrm{V}}{\rightleftarrows}} \{ \text{ Teilmengen von } \mathbb{A}^n \}$$

definiert. Die erste Frage, die direkt aufkommt, ist, wie I und V miteinander interagieren. Es ist klar, dass $X \subseteq \mathrm{V}(\mathrm{I}(X))$ und $T \subseteq \mathrm{I}(\mathrm{V}(T))$. Man könnte nun vermuten, dass sogar Gleichheiten $\mathrm{I}(\mathrm{V}(T)) = T$ und $\mathrm{V}(\mathrm{I}(X)) = X$ gälten. Von Lemma 1.1.21 wissen wir jedoch direkt, dass $\mathrm{I}(\mathrm{V}(T))$ im allgemeinen nicht T sein kann, wenn T kein Ideal gewesen ist. Auf der anderen Seite ist $\mathrm{V}(T)$ per Definition immer eine algebraische Menge und daher per Definition abgeschlossen in $\mathbb{A}^n$ bezüglich der Zariski-Topologie. Wir können unsere Zuordnungen also wie folgt etwas verfeinern:

$$\{ \text{ Ideale von } K[x_1,\ldots,x_n] \} \underset{\mathrm{I}}{\overset{\mathrm{V}}{\rightleftarrows}} \{ \text{ Zariski-abgeschlossene Teilmengen von } \mathbb{A}^n \}.$$

Unter dieser Einschränkung ist $\mathrm{V}(\mathrm{I}(-))$ die Identität ist und allgemeiner haben wir den nachfolgenden Satz:

1.1.4 Der algebraische Abschluss und $\mathrm{V}(\mathrm{I}(-))$

Satz 1.1.26. *Sei $X \subseteq \mathbb{A}^n$ eine Teilmenge. Dann gilt*

$$\mathrm{V}(\mathrm{I}(X)) = \overline{X},$$

wobei $\overline{X}$ den Abschluss von X in der Zariski-Topologie bezeichnet.

Beweis. Es gilt zu zeigen, dass $\mathrm{V}(\mathrm{I}(X))$ unter allen abgeschlossenen Mengen, welche X enthalten, die kleinste ist, das heißt jede andere abgeschlossene Menge, welche X enthält, soll bereits $\mathrm{V}(\mathrm{I}(X))$ enthalten.

Zunächst ist klar, dass $X \subseteq \mathrm{V}(\mathrm{I}(X))$ und dass $\mathrm{V}(\mathrm{I}(X))$ abgeschlossen ist. Sei also Y eine beliebige abgeschlossene Teilmenge von $\mathbb{A}^n$ mit $X \subseteq Y$. Per Definition der Zariski-Topologie (in Kombination mit Lemma 1.1.16) ist $Y = V(J)$ für irgendein Ideal $J \subseteq K[x_1,\ldots,x_n]$. Damit aber X in $V(J)$ liegen kann, muss per Definition $f(X) = 0$ für alle $f \in J$ gelten. Daher ist $J \subseteq \mathrm{I}(X)$. Lemma 1.1.15 besagt nun, dass $\mathrm{V}(\mathrm{I}(X)) \subseteq \mathrm{V}(J) = Y$ gilt, was die Aussage beweist. □

Korollar 1.1.27. *Seien X, Y algebraische Mengen. Dann gilt*

(i) $\mathrm{V}(\mathrm{I}(X)) = X$ *und*

(ii) aus $\mathrm{I}(X) = \mathrm{I}(Y)$ *folgt* $X = Y$.

Beweis. Dies ist ein direktes Korollar von Satz 1.1.26. Für Teil (i) reicht es aus sich zu erinnern, dass "algebraisch" gleichbedeutend mit "abgeschlossen" ist und dass für eine abgeschlossene Menge X schon $X = \overline{X}$ gilt. Für Teil (ii) nehme man an, dass $X \neq Y$. Es gilt $\mathrm{V}(\mathrm{I}(X)) = X \neq Y = \mathrm{V}(\mathrm{I}(Y))$. Daher muss auch $\mathrm{I}(X) \neq \mathrm{I}(Y)$ sein, da V ja gleiche Ideale auf gleiche Mengen schicken würde. □

1.2 Hilberts Nullstellensatz und $\mathrm{I}(\mathrm{V}(-))$

Die umgekehrte Richtung ist deutlich komplizierter. Sei $J \subseteq K[x_1, \ldots, x_n]$ ein Ideal. Die Gleichung $J = \mathrm{I}(\mathrm{V}(J))$ muss *nicht* mehr gelten, wie das folgende Beispiel zeigt.

Beispiel 1.2.1. Sei $J = (x^2) \subseteq K[x]$ ein Ideal. Es gilt:

$$\begin{aligned}
J &= \left(x^2\right) \\
&\downarrow \\
\mathrm{V}(J) &= \{a \in \mathbb{A}^1 \mid \forall f \in J : f(a) = 0\} \\
&= \{a \in \mathbb{A}^1 \mid \forall g \in K[x] : a^2 \cdot g(a) = 0\} \\
&= \{a \in \mathbb{A}^1 \mid a^2 = 0\} \cup \{a \in \mathbb{A}^1 \mid \forall g \in K[x] : g(a) = 0\} \\
&= \{a \in \mathbb{A}^1 \mid a^2 = 0\} \quad \text{(Teil (ii) von Lemma 1.1.17)} \\
&= \{0\} \\
&\downarrow \\
\mathrm{I}(\mathrm{V}(J)) &= \mathrm{I}(\{0\}) = \{f \in K[x] \mid f(0) = 0\} \\
&= (x).
\end{aligned}$$

Wir müssen daher einen Exkurs zu Noetherschen Ringe einschieben.

1.2.1 Noethersche Ringe und der Hilbertsche Basissatz

Definition 1.2.2. *Ein Ring heißt* noethersch *falls jede aufsteigende Folge von Idealen*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

stabilisiert. Sprich, es gibt ein $N \in \mathbb{N}$, so dass für alle $n \geq N$ gilt $I_n = I_{n+1}$.

Satz 1.2.3. *Die folgenden Aussagen sind äquivalent:*

i) Der Ring R ist noethersch.

ii) Jede nichtleere Menge von Idealen hat ein maximales Element.

iii) Jedes Ideal von R ist endlich erzeugt.

Zur Erinnerung, ein Element m einer teilweise geordneten Menge wird *maximal* genannt, wenn für jedes Element x aus $m \leq x$ schon $m = x$ folgt. Beachte, dass dies nicht bedeutet, dass m das größte Element ist, sondern nur, dass es kein echt größeres gibt. Es kann durchaus nicht vergleichbare andere maximale Elemente geben. Ordnen wir etwa die Menge $\{a, 1\}$ diskret an (das heißt es gelte nur $a \leq a$ und $1 \leq 1$ ohne dass a und 1 vergleichbar seien) so ist sowohl a wie auch 1 maximal, ein größtes Element existiert aber nicht. Die Ordnung, auf welche wir uns in obigem Satz beziehen, ist die Teilmengenrelation auf der Potenzmenge des Rings, eingeschränkt auf eine Menge von Idealen.

Beweis. i) $\Rightarrow$ ii). Wir beweisen dies durch Widerspruch. Sei ii) falsch. Es gibt daher eine nichtleere Menge T von Idealen, welche kein maximales Element besitzt. Sei I_0 ein beliebiges Element von T. Da es nicht das maximale Element ist, gibt es ein $I_1 \in T$, so dass $I_0 \subsetneq I_1$. Da auch I_1 nicht maximal ist, können wir ein Ideal I_2 finden, so dass $I_0 \subsetneq I_1 \subsetneq I_2$. Das Spiel kann man endlos fortsetzen und wir erhalten eine aufsteigende Folge von Idealen, welche nicht stabilisiert. Dies widerspricht der Annahme, dass R noethersch ist.

ii) $\Rightarrow$ iii). Sei $I \subseteq R$ ein Ideal und Σ_I die Menge aller endlich erzeugten Unterideale von I. Es ist klar, dass Σ_I nicht leer ist, da $(0) \subseteq I$. Nach Annahme hat Σ_I ein maximales Element I_m. Wenn $I_m \neq I$ gilt, dann gibt es ein $x \in I \setminus I_m$ und somit wäre $I_m \subsetneq I_m + (x) \subseteq I$, was der Maximalheit von I_m widerspricht. Wir haben daher $I = I_m$, was per Konstruktion endlich erzeugt ist.

iii) $\Rightarrow$ i). Sei $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Menge von Idealen. In solch einem Fall ist die Vereinigung $J = \bigcup_i I_i$ ein Ideal. Nach Annahme muss J endlich erzeugt sein. Es ist klar, dass diese endlich vielen Erzeuger in gewissen I_i's liegen. Es existiert daher ein $N \in \mathbb{N}$, sodass alle Erzeuger von J in I_N liegen, womit $J = \bigcup_{i=0}^{N} I_i$ ist. Es folgt, dass die Folge der aufsteigenden Ideale ab Index N stabilisiert. □

Für ein Polynom $f \in R[X]$, sei $\mathfrak{L}(f)$ der Leitkoeffizient von f. Gleichermaßen benutzen wir die Notation

$$\mathfrak{L}(T) := \{\mathfrak{L}(f) \mid f \in T\}$$

für eine beliebige Teilmenge $T \subseteq R[X]$.

Lemma 1.2.4. *Sei $I \subseteq R[X]$ ein Ideal. Die Menge der Leitkoeffizienten $\mathfrak{L}(P_N) \subseteq R$ der Polynome von I, welche Grad N und geriger haben, formen ein Ideal von R. Hier kann $N = \infty$ sein.*

Beweis. Alle Idealaxiome außer der Summe kann man direkt sehen. Bei der Summe geht man wie folgt vor: Seien $f(x) = ax^n + \cdots$ und $g(x) = bx^m + \cdots$ im Ideal I. Man nehme o. B. d. A. an, dass $m \leq n$, also $k = n - m \geq 0$. Dann ist $a + b$ der Leitkoeffizient von $f(x) + g(x) \cdot x^k \in I$ und wir sind fertig. □

Satz 1.2.5 (Hilbertscher Basissatz)**.** *Sei R ein noetherscher Ring. Der Polynomring $R[X]$ ist noethersch.*

Beweis. Sei $I \subseteq R[X]$ ein Ideal und $P_N \subseteq I$ die Menge der Polynome von I vom Grad N und geringer. Die Menge $\mathfrak{L}(P_N)$ der Leitkoeffizienten der Polynome von P_N, ist ein Ideal von R laut 1.2.4. Dies ist endlich erzeugt wegen Satz 1.2.3, sprich $\mathfrak{L}(P_N) = (\mathfrak{L}(f_1), \ldots, \mathfrak{L}(f_{n_N}))$.

Wir schreiben hier den doppelten Index n_N, da die Anzahl der Erzeuger von N abhängt. Wir können aber immer annehmen, dass $n_N \leq n_{N+1}$ indem wir die Polynome f_i, welche wir für N benutzt haben beibehalten und gegebenenfalls neue Polynome für $N + 1$ hinzufügen.

Wir beweisen nun per Induktion, dass $P_N \subseteq (f_1, \ldots, f_{n_N})$. Für $N = 0$ ist dies klar, da $P_0 = R$. Gelte die Aussage also für $N - 1$ und sei $f \in P_N$. Wir können annehmen, dass

$f \notin P_{N-1}$, weil wir sonst im Fall $N-1$ wären. Da $\mathfrak{L}(P_N) = (\mathfrak{L}(f_1), \ldots, \mathfrak{L}(f_{n_N}))$, können wir

$$\mathfrak{L}(f) = \sum_{j=1}^{n} u_j \mathfrak{L}(f_j)$$

schreiben, wobei $u_j \in R$. Definiere

$$g := \sum_{j=1}^{n} u_j f_j x^{(\mathsf{grad}(f)-\mathsf{grad}(f_j))}.$$

Dies ist wohldefiniert, da $\mathsf{grad}(f) = N \geq \mathsf{grad}(f_j)$. Wir haben $\mathfrak{L}(f) = \mathfrak{L}(g)$ und $\mathsf{grad}(f) = \mathsf{grad}(g)$. Als solches ist $\mathsf{grad}(f-g) \leq N-1$ und per Induktion ist $f - g \in (f_1, \ldots, f_{n_{N-1}}) \subseteq (f_1, \ldots, f_{n_N})$. Da $g \in (f_1, \ldots, f_{n_N})$, folgt $f \in (f_1, \ldots, f_{n_N})$ und wir sind fertig.

Um den Beweis abzuschließen, bemerken wir, dass R Noethersch ist und daher die Kette

$$\mathfrak{L}(P_0) \subseteq \mathfrak{L}(P_1) \subseteq \cdots \subseteq \mathfrak{L}(P_N) \subseteq \cdots$$

stabilisiert. Es folgt, dass auch die Kette

$$(f_0 \cdots f_{n_0}) \subseteq (f_0 \cdots f_{n_1}) \subseteq \cdots \subseteq (f_0 \cdots f_{n_N}) \subseteq \cdots$$

stabilisiert, womit wir den Satz bewiesen haben. □

Korollar 1.2.6. *Für einen Körper K ist der Ring $K[x_1, \ldots, x_n]$ noethersch.*

Bemerkung 1.2.7. Da $K[x_1, \ldots, x_n]$ noethersch ist (siehe Definition 1.2.2 und Korollar 1.2.6), gibt es für jede Teilmenge $T \subseteq K[x_1, \ldots, x_n]$ eine endliche Menge von Polynomen $f_1, \ldots, f_m$, sodass $(T) = (f_1, \ldots, f_m)$ (Satz 1.2.3). Daher können wir laut Lemma 1.1.16 annehmen, dass algebraische Mengen immer durch endlich viele Polynome bestimmt sind:

$$\mathrm{V}(J) = \mathrm{V}(f_1, \ldots, f_m) = \bigcap_{i=1}^{m} \mathrm{V}(f_i).$$

Dies ist vor allem beim Rechnen und Beweisen hilfreich. Für allgemeine Aussagen werden wir aber trotzdem öfter mit Idealen arbeiten.

1.2.2 Radikale Ideale

Man erinnere sich an Beispiel 1.2.1. Da $I = (x)$ und $J = (x^2)$ dieselben Nullstellen haben, sprich $\mathrm{V}(-)$ diese nicht unterscheiden kann, ist es unmöglich für die Komposition $\mathrm{I}(\mathrm{V}(-))$ die Ideale zu rekonstruieren. Das Problem besteht allgemeiner für jedes Polynom und jede (positive) Potenz: $f(x_1, \ldots, x_n)$ und $f(x_1, \ldots, x_n)^m$, $m \geq 1$ haben dieselben Nullstellen. Obwohl dies nicht das einzige ist, was der Gleichung im Wege steht, wie man in Beispiel 1.2.18 sehen wird, ist dies eines der Haupthindernisse. Wir kommen daher zur folgenden Definition:

Definition 1.2.8. *Sei $I \subseteq R$ ein Ideal eines kommutativen Ringes R. Wir definieren das* Radikal $\sqrt{I}$ *von I als*

$$\sqrt{I} := \{a \in R \mid a^n \in I \text{ für irgendein } n \in \mathbb{N}\}.$$

Mit anderen Worten ergibt sich $\sqrt{I}$ aus dem Ideal I durch Hinzufügen aller n-ten Wurzeln seiner Elemente für jede positive natürliche Zahl n. Es ist direkt ersichtlich, dass $I \subseteq \sqrt{I}$.

Beispiel 1.2.9. Sei $R = \mathbb{Z}$. Es gilt

- $\sqrt{(4)} = \{n \in \mathbb{Z} \mid \exists\ k \in \mathbb{N}, m \in \mathbb{Z}, \text{ so dass } n^k = 4m\} = (2)$;
- $\sqrt{(125)} = \{n \in \mathbb{Z} \mid \exists\ k \in \mathbb{N}, m \in \mathbb{Z}, \text{ so dass } n^k = 125m\} = (5)$.

Sei $R = \mathbb{R}[x, y]$. Wir haben

- $\sqrt{(x^2)} = \{f(x,y) \in K[x,y] \mid \exists\ k \in \mathbb{N}, g \in K[x,y] \text{ so dass } f^k = x^2 \cdot g(x)\} = (x)$;
- $\sqrt{(x^2, y^2)} = (x, y)$;
- $\sqrt{(x^2 + y^2)} = (x^2 + y^2)$, denn aus $f^k \in (x^2 + y^2)$ folgt $x^2 + y^2 \mid f^k$. Man überzeugt sich leicht, etwa durch direkte Rechnung, dass $x^2 + y^2$ irreduzibel ist. In einem faktoriellen Ring wie $K[x, y]$ ist jedes irreduzible Element prim, daher gilt schon $x^2 + y^2 \mid f$, also $f \in (x^2 + y^2)$. Dies gilt auch für allgemeineres K der Charakteristik ungleich 2, etwa für $K = \mathbb{C}$, aber der Beweis ist etwas anders.

Definition 1.2.10. *Ein Ideal I wird* radikal *genannt, wenn $\sqrt{I} = I$.*

Lemma 1.2.11.

(i) Das Radikal eines Ideals ist wieder ein Ideal.

(ii) Es gilt $\sqrt{\sqrt{I}} = \sqrt{I}$.

Beweis. (i) Seien $I \subseteq R$ ein Ideal und $a, b \in \sqrt{I}$, also $\exists m, n \in \mathbb{N}$, so dass $a^n, b^m \in I$. Für beliebige $r \in R$ gilt $(ar)^n \in I$. Für die Summe, sei o. B. d. A. $n \geq m$. Die binomische Formel besagt

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

Sei $x_i := \max\{i, 2n-i\}$. Es ist klar, dass $x_i \geq n$ für alle $0 \leq i \leq 2n$. Da aber sowohl a^n als auch b^n im Ideal I liegen, liegen alle Summanden in I, also gilt dies auch für die gesamte Summe.

(ii) $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ gilt immer. Sei umgekehrt $f \in \sqrt{\sqrt{I}}$, also $\exists n \in \mathbb{N}$, sodass $f^n \in \sqrt{I}$. Daraus wiederum folgt die Existenz von einem $m \in \mathbb{N}$, sodass $(f^n)^m = f^{n+m} \in I$, also $f \in \sqrt{I}$. □

Lemma 1.2.12. *Das Urbild eines Radikalideals unter einem Ringhomomorphismus ist radikal.*

Beweis. Sei $f : R \to S$ ein Homomorphismus von Ringen und $I \subseteq S$ ein radikales Ideal. Ist $r \in R$ mit $r^n \in f^{-1}(I)$ für ein $n \in \mathbb{N}$, so ist $f(r)^n = f(r^n) \in I$. Da I ein Radikalideal ist, folgt $f(r) \in I$, also $r \in f^{-1}(I)$. □

Lemma 1.2.13. *Es gilt $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. Insbesondere ist der Schnitt von Radikalidealen wieder radikal.*

Beweis. Per Definition des Radikals eines Ideals gilt

$$\sqrt{I \cap J} = \left\{a \mid \exists\ k, \quad \text{mit} \quad a^k \in I, a^k \in J\right\}$$

und

$$\sqrt{I} \cap \sqrt{J} = \left\{a \mid \exists\ n, m, \quad \text{mit} \quad a^n \in I, a^m \in J\right\}.$$

Für die Inklusion $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$ setze $m = n = k$. Für die andere Seite sei $k = \max\{m, n\}$. Für den letzten Teil, seien $I = \sqrt{I}$ und $J = \sqrt{J}$ radikal. Es gilt $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = I \cap J$. □

Lemma 1.2.14. *Sei $I \subseteq \sqrt{J} \subseteq K[x_1, \ldots, x_n]$. Es gibt ein $d \geq 1$, so dass*

$$I^d \subseteq J.$$

Beweis. Da $K[x_1, \ldots, x_n]$ ein noetherscher Ring ist, ist jedes Ideal endlich erzeugt (Satz 1.2.3, iii). Sei $I = (r_1, \ldots, r_k)$. Da $I \subseteq \sqrt{J}$ gibt es $d_1, \ldots, d_k$, so dass $r_i^{d_i} \in J$. Man wähle $d' = \max\{d_1, \ldots, d_k\}$. Dann ist $r_i^{d'} \in J$ für jedes $1 \leq i \leq k$.

Betrachte nun ein beliebiges Element $r \in I$. Es ist von der Form $\sum_{i=1}^{k} a_i r_i$ für gewisse $a_i \in R$. Wenn wir $r^k = \left(\sum_{i=1}^{k} a_i r_i\right)^k$ ausmultiplizieren, ist $\prod_{i=1}^{k} a_i r_i$ der Summand, für welchen das Maximum über alle Potenzen der r_i's am kleinsten ist. Setzen wir also $d := kd'$, so enthält jeder Summand von r^d (nach Ausmultiplizieren) mindestens eines der r_i's mit Potenz $\geq d'$. Damit ist r in J und wir haben bewiesen, dass $I^d \subseteq J$. □

Beispiel 1.2.15. Sei $J = (x^3, y^3)$ und $I = (x^2, y^2)$. Dann gilt $I \subseteq \sqrt{J} = (x, y)$, aber weder $I \notin J$ noch $I^2 = (x^4, x^2y^2, y^4) \notin J$. Für $d = 3$ allerdings haben wir $I^3 = (x^6, x^4y^2, x^2y^4, y^6) \subseteq (x^3, y^3)$.

Korollar 1.2.16. *Es gilt*

(i) $\sqrt{1} = (1)$ *und*

(ii) aus $\sqrt{I} = (1)$ *folgt* $I = (1)$.

Beweis. (i) Dies ist direkt klar, da jedes Ideal in (1) liegt (also insbesondere $\sqrt{(1)} \subseteq (1)$) und weil per Definition des Radikals $I \subseteq \sqrt{I}$ gilt, also auch $(1) \subseteq \sqrt{(1)}$.

(ii) Dies ist ein Korollar von Lemma 1.2.14, da es die Existenz eines $d \geq 1$ besagt, mit $(1)^d = I$. Aber für alle $i \geq 1$ gilt $(1)^d = (1)$ und das Resultat folgt. □

Lemma 1.2.17. *Sei* J *ein Ideal von* $K[x_1, \ldots, x_n]$. *Es gilt*

$$\mathrm{V}(J) = \mathrm{V}\left(\sqrt{J}\right).$$

Des Weiteren ist $\sqrt{J} \subseteq \mathrm{I}(\mathrm{V}(J))$.

Beweis. Aus $J \subseteq \sqrt{J}$ folgt $\mathrm{V}\left(\sqrt{J}\right) \subseteq \mathrm{V}(J)$ (Lemma 1.1.15). Auf der anderen Seite, sei $a \in \mathrm{V}(J)$. Es gilt zu zeigen, dass $f(a) = 0$ für alle $f \in \sqrt{J}$. Sei $f \in \sqrt{J}$, also $\exists n \geq 1$ mit $f^n \in J$. Daher ist $0 = f^n(a) = (f(a))^n = 0$ und da wir über einem Körper sind, muss $f(a) = 0$ gelten.

Da $T \subseteq \mathrm{I}(\mathrm{V}(T))$ immer stimmt, folgt für $T = \sqrt{J}$, dass $\sqrt{J} \subseteq \mathrm{I}(\mathrm{V}(\sqrt{J})) = \mathrm{I}(\mathrm{V}(J))$. □

Im Kombination mit Lemma 1.1.16 besagt dies, dass es ausreichend ist, sich die Nullstellen der Erzeuger des Radikals eines Ideals anzusehen.

Wir wollen nun eine ähnliche Aussage zu Satz 1.1.26 erarbeiten, nun aber die umgekehrte Komposition $\mathrm{I}(\mathrm{V}(-))$ betrachten. Dies ist nicht ohne Weiteres möglich, wie das folgende Beispiel zeigt:

Beispiel 1.2.18. Sei $\mathfrak{m} = (x^2 + 1) \subseteq \mathbb{R}$. Da $x^2 + 1$ irreduzibel über $\mathbb{R}$ ist, muss $\mathfrak{m} \subseteq \mathbb{R}$ ein Primideal sein. Mehr als das, $\mathfrak{m}$ ist ein Maximalideal, da $\mathbb{R}[x]$ ein Polynomring über einen Körper ist (und daher von Krulldimension 1 ist). Wir sehen direkt, dass $\mathrm{V}(\mathfrak{m}) = \varnothing \subseteq \mathbb{A}^n$, weil $x^2 + 1$ keine Lösungen über $\mathbb{R}$ hat. Da aber auch $\mathrm{V}(1) = \varnothing$, kann $\mathrm{I}(\mathrm{V}(-))$ diese zwei Ideale unmöglich unterscheiden.

Das Problem in diesem Beispiel ist, dass $\mathbb{R}$ nicht algebraisch abgeschlossen ist. Daher werden wir uns auf algebraisch abgeschlossene Körper konzentrieren. Hilberts Nullstellensatz wird uns dann die Beziehung $\mathrm{I}(\mathrm{V}(J)) = \sqrt{J}$ liefern. Für ein analoges Resultat im allgemeineren Kontext von nicht algebraisch abgeschlossenen Körpern oder gar Ringen R, muss man statt des affinen Raumes über R das (maximale) Spektrum von $R[x_1, \ldots, x_n]$ betrachten, siehe auch die kurze Besprechung nach Hilberts Nullstellensatz.

1.2.3 Lokalisierungen und der Quotientenkörper

Ehe wir zu Hilberts Nullstellensatz kommen, machen wir einen kleinen Umweg und führen den Begriff der Lokalisierung ein, eine der wichtigen Konstruktionen der algebraischen Geometrie.

Definition 1.2.19. *Eine Teilmenge $S \subseteq R$, welche 1 enthält und unter Produkten abgeschlossen ist, sprich $a, b \in S$ impliziert $ab \in S$, wird* multiplikativ *genannt.*

Die Elemente einer multiplikativen Teilmenge eines Ringes lassen sich durch Übergang zu einem Ring von Brüchen invertierbar machen. Diese Konstruktion funktioniert wie folgt:

Konstruktion 1.2.20. *Sei $S \subseteq R$ eine multiplikative Teilmenge. Definiere die* Lokalisierung *$S^{-1}R$ von R nach S durch*

$$S^{-1}R := (R \times S)/\sim,$$

$$\text{wobei} \quad (r,s) \sim (r',s') \quad \text{genau dann wenn} \quad \exists t \in S, \quad \text{so dass} \quad trs' = tr's.$$

Wenn R ein Integritätsbereich ist können wir $t = 1$ annehmen.

Proposition 1.2.21. *Die Lokalisierung $S^{-1}R$ trägt auf natürliche Weise die Struktur einer R-Algebra. Hierbei ist die Addition durch*

$$(r,s) + (r',s') := (rs' + r's, ss')$$

und die Multiplikation durch

$$(r,s) \cdot (r',s') := (rr', ss')$$

gegeben.

Beweis. Hausaufgabe (mündlich). □

Zur Erinnerung, eine R-Algebrenstruktur auf $S^{-1}R$ ist ein Ringhomomorphismus $R \to S^{-1}R$. Wir werden diesen Ringhomomorphismus mit γ bezeichnen.

Diese Konstruktion kann man allgemeiner machen: Sei $I \subseteq R$ ein Ideal und $S \subseteq R$ eine multiplikative Teilmenge. Wir können $S^{-1}I$ genau wie oben definieren. Wenn $I = (1)$ erhalten wir daher genau die gewünschte Lokalisierung. Es gilt folgendes:

Lemma 1.2.22. *Die Lokalisierung $S^{-1}I$ ist ein Ideal von $S^{-1}R$.*

Beweis. Hausaufgabe (mündlich). □

Bemerkung 1.2.23. Für diejenigen denen Moduln und das Tensorprodukt vertraut sind, sei gesagt, dass die Lokalisierung eines R-Moduls M auf die selbe Art und Weise definiert ist und $S^{-1}M$ ein $S^{-1}R$-Modul wird. Zudem gilt $S^{-1}M \simeq M \otimes_R S^{-1}R$.

Wir betrachten nun einige wichtige Spezialfälle von Lokalisierungen von Ringen. Dem Leser/der Leserin sei empfohlen, die Aussagen und Beweise für Ideale zu übersetzen.

Lokalisierung nach einer Untergruppe Als erstes wollen wir beweisen, dass sich nichts ändert, wenn wir invertierbare Elemente invertieren.

Lemma 1.2.24. *Für einen Ring R und eine multiplikative Untergruppe $G \subseteq R$ gilt $G^{-1}R \simeq R$.*

Beweis. Sei $g \in G \subseteq M$. Da G eine Untergruppe ist, existiert die Inverse $g^{-1} \in G \subseteq M$, so dass $gg^{-1} = g^{-1}g = 1$. Wir definieren die Umkehrabbildung

$$\gamma^{-1} : G^{-1}M \to M$$

durch

$$\frac{r}{g} \mapsto rg^{-1}.$$

Wohldefiniertheit: Sei $\frac{r}{g} \sim \frac{r'}{g'} \in G^{-1}M$, sprich $trg' = tr'g$ für irgendein $t \in G$. Da G eine Untergruppe ist, folgt $t^{-1}trg' = t^{-1}tr'g \Leftrightarrow rg' = r'g$. Multipliziere beide Seiten mit $(g'g)^{-1}$ und erhalte $rg^{-1} = r'(g')^{-1}$. Die Abbildung ist also wohldefiniert.
γ^{-1} ist ein Ringhomomorphismus: Es gilt

$$\gamma^{-1}\left(\frac{0}{g}\right) = 0g^{-1} = 0,$$

$$\gamma^{-1}\left(\frac{r}{g}\right)\gamma^{-1}\left(\frac{r'}{g'}\right) = rg^{-1}r'\left(g'\right)^{-1} = rr'g^{-1}\left(g'\right)^{-1} = rr'\left(g'g\right)^{-1} = \left(rr'\right)\left(gg'\right)^{-1} = \gamma^{-1}\left(\frac{rr'}{gg'}\right)$$

und wir haben

$$\gamma^{-1}\left(\frac{r}{g}\right) + \gamma^{-1}\left(\frac{r'}{g'}\right) = rg^{-1} + r'\left(g'\right)^{-1}$$

$$\gamma^{-1}\left(\frac{rg' + r'g}{gg'}\right) = \left(rg' + r'g\right)\left(gg'\right)^{-1} = \left(rg' + r'g\right)\left(g'\right)^{-1}g^{-1} = rg^{-1} + r'\left(g'\right)^{-1}.$$

γ^{-1} ist invers zu γ: Es gilt

$$\gamma^{-1}\left(\gamma\right)\left(r\right) = \gamma^{-1}\left(\frac{r}{1}\right) = r1^{-1} = r1 = r,$$

daher $\gamma^{-1}\gamma = \mathsf{Id}$. Auf der anderen Seite ist

$$\gamma\gamma^{-1}\left(\frac{r}{g}\right) = \gamma\left(rg^{-1}\right) = \frac{rg^{-1}}{1}.$$

Es bleibt zu folgern, dass $\frac{rg^{-1}}{1} \simeq \frac{r}{g}$. Doch dies ist klar, da $rg^{-1}g = r1$. □

Bemerkung 1.2.25. Man braucht eigentlich nicht zeigen, dass das Inverse γ^{-1} ein Ringhomomorphismus ist. Für algebraische Strukture ist dies nämlich immer der Fall. Wir zeigen es trotzdem, falls das allgemeine Argument nicht bekannt ist.

Lemma 1.2.26. *Es gilt*

$$\gamma(S) \subseteq (S^{-1}R)^*,$$

wobei $(S^{-1}R)^*$ *die invertierbaren Elemente von* $S^{-1}R$ *bezeichnet.*

Beweis. Für $s \in S$ ist $\gamma(s) = \frac{s}{1}$ und somit ist

$$\gamma(s) \cdot \frac{1}{s} = \frac{s}{1}\frac{1}{s} = \frac{s}{s} = \frac{1}{1}.$$

□

Lokalisierung nach einem Element Sei $f \in R$ ein Element. Für S wählen wir die Menge aller Potenzen von f, sprich $S = \{1, f, \ldots\}$. Offenbar ist S multiplikativ abgeschlossen, es ist sogar die kleinste multiplikativ abgeschlossene Menge, welche f enthält. Natürlich muss S nicht unendlich viele Elemente haben, beispielsweise könnte bereits $f^2 = f$ gelten, etwa wenn $f = 0$. Die Lokalisierung nach S notieren wir in diesem Fall mit

$$R_f := S^{-1}R.$$

Dies ist eine einfache, aber sehr wichtige Klasse von Lokalisierungen für uns, deren Wichtigkeit uns spätestens im Abschnitt **??** bewusst wird. Eine erste Anwendung sehen wir aber schon in Kürze.

Lokalisierungen nach einzelnen Elementen sind besonders einfach. Es gilt:

Proposition 1.2.27. *Ist* $f \in R$*, so ist*

$$R_f \simeq R[x]/(xf - 1).$$

Beweis. Wir definieren die Abbildung

$$R_f \to R[x]/(xf - 1),$$

als

$$\frac{r}{f^n} \mapsto rx^n.$$

Als erstes zeigen wir, dass dies wohldefiniert ist. Sei $\frac{r}{f^n} \sim \frac{s}{f^m}$. Daher gibt es ein $t \in \{1, f, f^2, \ldots\}$, so dass $trf^m = tsf^n$. Also ein $k \geq 0$, so dass $rf^{k+m} = sf^{k+n}$. Das Bild von $\frac{r}{f^n}$ ist rx^n. Es gilt

$$rx^n = rx^n \cdot 1 = rx^n(f^{k+m}x^{k+m}) = (rf^{k+m})x^{k+n+m} = (sf^{k+n})x^{k+n+m} = sx^m,$$

was natürlich das Bild von $\frac{s}{f^m}$ ist. Hier haben wir $xf = 1$ benutzt, was per Definition von $R[x]/(xf - 1)$ gilt. Daher ist unsere Abbildung wohldefiniert. Es ist auch recht klar, dass sie ein Ringhomomorphismus ist. Nur Addition benötigt etwas Arbeit:

$$\frac{r}{f^n} + \frac{s}{f^m} = \frac{f^m r + f^n s}{f^m + f^n} \mapsto \left(f^m r + f^n s\right) x^{n+m} = x^n r + x^m s$$

Die Umkehrabbildung definieren wir als

$$a_0 + a_1 x + \cdots + a_n x^n \mapsto \frac{a_0}{1} + \frac{a_1}{f} + \cdots + \frac{a_n}{f^n}.$$

Offenbar ist

$$\frac{r}{f^n} \mapsto r x^n \mapsto \frac{r}{f^n}.$$

Andererseits gilt

$$\begin{aligned} a_0 + a_1 x + \cdots + a_n x^n &\mapsto \frac{a_0}{1} + \frac{a_1}{f} + \cdots + \frac{a_n}{f^n} = \frac{a_0 f^n + a_1 f^{n-1} + \cdots + a_{n-1} f + a_n}{f^n} \\ &\mapsto (a_0 f^n + a_1 f^{n-1} + \cdots + a_{n-1} f + a_n) x^n = a_0 + a_1 x + \cdots + a_n x^n, \end{aligned}$$

da f sich ja mit x kürzt. Wir haben also insgesamt einen bijektiven Ringhomomorphismus $R_f \to R[x]/(xf - 1)$ definiert, was die Behauptung zeigt. □

Lokalisierung nach Nullteilern

Lemma 1.2.28. *Sei $S \subseteq R$ eine multiplikative Teilmenge, welche 0 enthält. Dann ist $S^{-1}R$ der Nullring.*

Beweis. Sei $\frac{a}{b} \in S^{-1}M$. Dann ist $\frac{a}{b} \sim \frac{1}{1}$, da $t = 0 \in S$, mit $0a = 0b$. □

Wir erinnern uns, dass ein Element $a \in R$ *Nullteiler* genannt wird, wenn es ein Element $b \in R$ gibt, so dass $b \neq 0$, aber $ab = 0$. Insbesondere ist die Null somit stets ein Nullteiler (außer im Nullring).

Lemma 1.2.29. *Sei $S \subseteq R$ eine multiplikative Teilmenge, welche einen Nullteiler a von R enthält. Dann ist $\gamma(b) = 0$ in $S^{-1}R$ für jedes $b \in R$ mit $ab = 0$.*

Beweis. Sei $ab = 0$. Daher gilt auch $\frac{a}{1}\frac{b}{1} = \frac{0}{1}$, was

$$\frac{a}{1}\frac{1}{a}\frac{b}{1} = \frac{1}{a}\frac{0}{1}$$

impliziert. Die linke Seite ist aber äquivalent zu $\frac{b}{1}$ und die rechte Seite ist wieder 0. Somit haben wir also $\frac{b}{1} \sim \frac{0}{1} = 0$. □

Korollar 1.2.30. *Die kanonische Abbildung $\gamma : R \to S^{-1}R$ ist genau dann injektiv wenn S keinen Nullteiler von R enthält.*

Beweis. Sei $\gamma(m) = \frac{m}{1} = \frac{0}{1}$, also $mt = 0t = 0$ für irgendein $t \in S$. Da aber S keinen Nullteiler enthält, ist t kein Nullteiler. Es muss also $m = 0$ sein, womit γ injektiv ist. Lemma 1.2.29 zeigt die andere Richtung. □

Der Quotientenkörper Wir wollen nun "alles" invertieren. Dies ist nicht direkt sinnvoll, siehe Lemma 1.2.29. Für Integritätsbereiche können wir jedoch folgendes betrachten:

Konstruktion 1.2.31. *Für einen Integritätsbereich R ist $S = R \setminus \{0\}$ eine multiplikative Teilmenge. Die Lokalisierung*

$$\mathsf{Q}(R) \coloneqq S^{-1}R = (R \setminus \{0\})^{-1}R$$

wird der Quotientenkörper *von R genannt.*

Es folgt direkt aus Lemma 1.2.29, dass $\gamma : R \to \mathsf{Q}(R)$ injektiv ist.

Der Begriff des Quotientenkörpers sollte nicht mit dem eines Quotientenrings nach einem Ideal verwechselt werden. Quotientenkörper entstehen durch Lokalisierung (Vergrößerung des Integritätsbereichs), Quotientenringe entstehen, indem man Elemente mittels einer Äquivalenzrelation identifiziert (Verkleinerung des Rings).

Beispiel 1.2.32. Sei $R = \mathbb{Z}$. Man überzeugt sich leicht, dass $\mathsf{Q}(\mathbb{Z}) \simeq \mathbb{Q}$ ist. Daher werden wir, wie auch schon für allgemeine Lokalisierungen, die traditionelle Notation $\frac{m}{s}$ statt (m, s) benutzen.

Die Lokalisierung eines Rings R kann ein Körper sein, ohne dass R ein Integritätsbereich war. Lediglich, um auf kanonische Art und Weise einen Körper zu erhalten sollte R nullteilerfrei sein. Betrachte etwa das folgende Beispiel:

Beispiel 1.2.33. Sei $R = \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$. Die Nullteiler sind $\{2, 3, 4\}$ mit $2 \cdot 3 = 4 \cdot 3 = 0$. Daher ist $S = \{1, 5 \equiv (-1)\}$ die größte multiplikative Teilmenge von R, welche weder 0 noch einen Nullteiler enthält. Jedoch sind sowohl 1 wie auch -1 Einheiten im Ring. Nach Lemma 1.2.24 stimmt die Lokalisierung von R nach S mit dem Ring R überein und ist inbesondere kein Körper. Betrachten wir aber $S_1 = \{1, 2, 4\}$ oder $S_2 = \{1, 3\}$, so erhalten wir

$$S_1^{-1}R \simeq \mathbb{Z}/3\mathbb{Z} \quad \text{und} \quad S_2^{-1}R \simeq \mathbb{Z}/2\mathbb{Z},$$

beide Lokalisierungen sind also Körper. Jedoch gibt es keinen Grund dem einen Vorzug vor dem anderen zu gewähren. Sie enthalten zwar unterschiedlich viele Elemente, dies muss im Allgemeinen aber nicht der Fall sein.

Bemerkung 1.2.34. An diesen Beispielen sieht man auch, dass der Ring beim Lokalisieren nicht notwendigerweise "größer" werden muss. Sprich, $\gamma : R \to S^{-1}R$ muss nicht zwingend injektiv sein.

Es gibt eine weitere besonders wichtige Klasse von Lokalisierungen, welche sich aus Komplementen von Primidealen ergeben. Diese werden wir jedoch erst später im Abschnitt 1.5.1 ansprechen.

Lemma 1.2.35. *Sei K ein Körper und $f : R \to K$ ein Ringhomomorphismus. Es existiert genau ein Körperhomomorphismus $f_* : \mathsf{Q}(R) \to K$, welcher f fortsetzt, also $f_* \circ \gamma = f$ erfüllt.*

Beweis. Definiere die Fortsetzung durch $f_*\left(\frac{r}{s}\right) := f(r)f(s)^{-1}$. Es ist ein einfaches sich zu überzeugen, dass dies einen wohldefinierten Ringhomomorphismus zwischen Körpern, also einen Körperhomomorphismus, definiert.

Ist $g : \mathsf{Q}(R) \to K$ ein weiterer Körperhomomorphismus, welcher f fortsetzt, so muss für beliebige $r \in R$ und $s \in R \setminus \{0\}$ gelten:

$$g\left(\frac{r}{s}\right) = g(\gamma(r) \cdot \gamma(s)^{-1}) = g(\gamma(r)) \cdot g(\gamma(s))^{-1} = f(r) \cdot f(s)^{-1} = f_*\left(\frac{r}{s}\right)$$

Also gilt schon $g = f_*$, womit f_* die eindeutige Fortsetzung von f ist. □

Beachte, dass Körperhomomorphismen immer injektiv sind, da Kerne von Ringhomomorphismen Ideale sind. Körper besitzen aber nur genau zwei Ideale, das Nullideal und das Einsideal. Letzteres kann nicht als Kern eines Körperhomormophismus g auftreteten, da $g(1) = 1 \neq 0$. Insbesondere ist damit $f_* : \mathsf{Q}(R) \to K$ injektiv, K ist also eine Körpererweiterung von $\mathsf{Q}(R)$.

1.2.4 Hilberts Nullstellensatz

Zariskis Lemma Zur Erinnerung, ein Integritätsbereich R wird *Hauptidealbereich* genannt, falls jedes Ideal I von R ein Hauptideal ist. Sprich, falls für jeden $I \subseteq R$ es ein $a \in R$ gibt, so dass $I = (a)$. Ein Beispiel für einen Hauptidealbereich ist $\mathbb{Z}$.

Beispiel 1.2.36. Sei K ein Körper. Der Ring $K[x]$ der Polynome in einer Variablen ist ein Hauptidealbereich. Dies lässt sich mittels des Euklidischen Algorithmus beweisen.

Definition 1.2.37. *Sei $A \subseteq B$ ein Unterring. Ein Element $b \in B$ wird* ganz *genannt falls es $a_0, \ldots, a_{n-1} \in A$ gibt, sodass*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0. \tag{2}$$

Falls jedes Element von B ganz über A ist, sagen wir, dass B ganz *über A ist und $A \subseteq B$ eine* ganze Erweiterung *ist.*

Mit anderen Worten heißt $b \in B$ ganz, falls ein *normiertes* Polynom (also ein Polynom mit Leitkoeffizient 1) $f(x) \in A[X] \subseteq B[X]$ existiert, sodass $f(b) = 0$. Vergleiche dies mit der Definition eines algebraischen Elements: Wir erinnern uns daran, dass $b \in B$ *algebraisch* über A genannt wird, wenn es ein *beliebiges* Polynom $f(x) \in A[X] \subseteq B[X]$ gibt, sodass $f(b) = 0$.

Lemma 1.2.38. *Sei $A \subseteq B$ ein Unterring. Die Menge der Elemente von B welche ganz über A sind bilden einen Ring $A \subseteq C \subseteq B$. Insbesondere gilt für über A ganze Elemente $\alpha_1, \ldots, \alpha_n \in B$: Der von den α_i erzeugte Unterring $A[\alpha_1, \ldots, \alpha_n] \subseteq B$ ist eine ganze Erweiterung von A.*

Beweisskizze. Die einzige Schwierigkeit hier ist die Abgeschlossenheit unter der Summe zu beweisen. Dies geht sehr einfach mit Modultheorie. Ein Modul ist einfach ein "Vektorraum über einen Ring". Ähnliche Argumente sind vielleicht schon von der linearen Algebra

bekannt. Die Beweisskizze ist wie folgt: Ein Element $\gamma \in B$ ist genau dann ganz über A, wenn $A[\gamma]$ endlich erzeugt ist als ein A-Modul. (Der Grund ist, dass wir γ^n als eine Linearkombination der γ^i's mit $1 \leq i \leq n-1$ ausdrücken können, siehe (2).) Seien $\alpha, \beta \in B$ ganz über A, sprich $A[\alpha]$, $A[\beta]$ sind endlich erzeugte A-Moduln. Da $[A[\alpha,\beta] : A[\alpha]] < \infty$, besagt der Körperturmsatz (für freie Moduln), dass auch $A[\alpha : \beta]$ endlich erzeugt ist als A-Modul. Da $\alpha + \beta \in A[\alpha, \beta]$ sind wir dann fertig. □

Lemma 1.2.39. *Sei D ein Integritätsbereich und K ein Körper, so dass $\mathrm{D} \subseteq K$ eine ganze Erweiterung ist. Dann ist D selbst ein Körper, sprich $D \simeq \mathsf{Q}(D)$.*

Beweis. Sei $0 \neq d \in D$. Nach Voraussetzung ist d^{-1} ganz über D, weshalb wir

$$\left(\frac{1}{d}\right)^n + a_{n-1}\left(\frac{1}{d}\right)^{n-1} + \cdots + a_1\left(\frac{1}{d}\right) + a_0 = 0$$

schreiben können, mit $a_0, \ldots, a_{n-1} \in D$. Indem wir beide Seiten mit d^{n-1} multiplizieren, erhalten wir

$$\frac{1}{d} = -a_{n-1} - \cdots - a_1 d^{n-2} - a_0 d^{n-1} \in D.$$

Es folgt, dass D schon ein Körper war, womit $D \setminus \{0\}$ eine Untergruppe von D ist. Lemma 1.2.24 liefert nun die gewünschte Aussage. □

Zur Erinnerung, ein Element $r \in R$ eines Ringes R heißt *irreduzibel*, falls aus einer Zerlegung $r = st$ folgt, dass $s \in R^*$ oder $t \in R^*$. Wir sagen, dass zwei irreduzible Elemente $r, r' \in R$ *äquivalent* sind, wenn es eine Einheit $u \in R$ gibt, sodass $r = ur'$.

Lemma 1.2.40. *Sei D ein Hauptidealbereich, welcher unendlich viele nicht-äquivalente irreduzible Elemente hat. Dann ist $\mathsf{Q}(D)$ nicht endlich erzeugt als D-Algebra.*

Beweis. Man nehme an, dass $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ den Körper $\mathsf{Q}(D)$ als D-Algebra erzeugen. Die Elemente $b_i, 1 \leq i \leq n$ sind dabei ungleich Null. Da D als Hauptidealbereich insbesondere ein faktorieller Ring ist, besitzt jedes b_i eine bis auf Äquivalenz eindeutige Zerlegung in endlich viele irreduzible Faktoren. Nach Voraussetzung existieren unendlich viele nicht-äquivalente irreduzible Elemente in D, insbesondere gibt es ein irreduzibles $p \in D$, welches keines der b_i teilt. Wir können nun $p^{-1} \in \mathsf{Q}(D)$ als Polynom in den $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ ausdrücken, das heißt, es existiert ein Polynom $\Phi(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$, sodass

$$\frac{1}{p} = \Phi\left(\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\right).$$

Indem wir nun beide Seiten mit $(b_1 \cdots b_n)^N$, für eine genügend große Zahl N, multiplizieren, erhalten wir $\frac{(b_1 \cdots b_n)^N}{p} \in D$. Dies impliziert aber, dass p ein irreduzibler Faktor des Produkts $(b_1 \cdots b_n)^N$ ist, insbesondere wäre p dann ein irreduzibler Faktor mindestens eines der b_i. Ein Widerspruch zur Definition von p. □

Proposition 1.2.41 (Zariskis Lemma)**.** *Sei K ein Körper und E eine endlich erzeugte K-Algebra, welche selbst ein Körper ist. Dann ist E endlich erzeugt als K-Vektorraum. Insbesondere ist $E \simeq K$, wenn K algebraisch abgeschlossen ist.*

Beweis. Jede endlich erzeuge K-Algebra ist von der Form $E = K[x_1, \dots, x_n]/I$ für ein Ideal I. Bezeichnen wir mit $\alpha_i := x_i + I$ die Restklasse von x_i im Quotientenring, so gilt es zu zeigen, dass die α_i's algebraisch über K sind. Wir beweisen dies per Induktion.

Sei $n = 1$ und $E = K[\alpha]$ ein Körper. Wenn $\alpha = 0$ sind wir fertig. Andernfalls ist $\alpha^{-1} \in E$. Da per Definition jedes Element $a \in R$ als polynomiale Kombination der Erzeuger (in diesem Fall nur α) dargestellt werden kann, gilt

$$\alpha^{-1} = k_0 + k_1\alpha + \cdots + k_m\alpha^m$$

für irgendwelche $k_0, \dots, k_m \in K$. Indem wir beide Seiten mit α multiplizieren, sehen wir, dass α Nullstelle eines Polynoms vom Grad $m+1$ und damit algebraisch ist.

Sei nun $n \geq 2$ und gelte der Satz für $n-1$ Erzeuger. Sei $L = K(\alpha_1) = \mathsf{Q}(K[\alpha_1])$. Wir haben einen Körperturm $K \subseteq L \subseteq E$, wobei $E = K[\alpha_1, \dots, \alpha_n] = L[\alpha_2, \dots, \alpha_n]$, da E ein Körper ist. Laut Induktionsannahme sind $\alpha_2, \dots, \alpha_n$ algebraisch über L, nach dem Körperturmsatz genügt es daher zu zeigen, dass α_1 algebraisch über K ist. Angenommen α_1 wäre transzendent über K, also $K[\alpha_1] \simeq K[x]$. Dann besäße $K[\alpha_1]$ unendlich viele nicht-äquivalente irreduzible Elemente, nach Lemma 1.2.40 wäre $\mathsf{Q}(K[\alpha_1]) = L$ also nicht endlich erzeugt als $K[\alpha_1]$-Algebra. Dies wollen wir nun zum Widerspruch führen:

Beachte, dass es ein $m \in \mathbb{N}$ und gewisse $h_k \in L$ für $k = 0, \dots, m-1$ gibt, sodass

$$\alpha_2^m = \sum_{k=0}^{m-1} h_k \alpha_2^k,$$

denn α_2 war algebraisch über L. Da $L = K(\alpha_1)$ können wir $h_k = \frac{p_k(\alpha_1)}{q_k(\alpha_1)}$ schreiben, mit $p_k, q_k \in K[x]$, für $k = 0, \dots, m-1$. Setzen wir nun

$$g_2(\alpha_1) := \prod_{k=0}^{m-1} q_k(\alpha_1) \in K[\alpha_1],$$

dann ist $h_k \in K[\alpha_1][\frac{1}{g_2(\alpha_1)}]$. Obige Gleichung zeigt daher, dass α_2 ganz über $K[\alpha_1][\frac{1}{g_2(\alpha_1)}]$ ist. Indem wir dieses Argument für $\alpha_3, \dots, \alpha_n$ wiederholen, erhalten wir Elemente $g_3(\alpha_1), \dots, g_n(\alpha_1) \in K[\alpha_1]$, sodass $\alpha_2, \dots, \alpha_n$ ganze Elemente über

$$A := K[\alpha_1][\frac{1}{g_2(\alpha_1)}, \dots, \frac{1}{g_n(\alpha_1)}]$$

sind. Da per Definition von A auch α_1 ganz über A ist, kann jedes Element von $E = K[\alpha_1, \dots, \alpha_n]$ als polynomielle Kombination von ganzen Elementen dargestellt werden. Lemma

1.2.38 besagt dann, dass alle Elemente von E ganz über A sind und Lemma 1.2.39 liefert, dass A auch ein Körper ist. Wir haben nun eine Inklusionsbeziehung

$$K[\alpha_1] \subseteq A \subseteq K(\alpha_1).$$

Da $K(\alpha_1)$ aber als Quotientenkörper von $K[\alpha_1]$ der *kleinste* Körper ist, welcher $K[\alpha_1]$ enthält, vergleiche Lemma 1.2.35, muss schon $A = K(\alpha_1)$ gelten. Per Definition ist A aber endlich erzeugt als $K[\alpha_1]$-Algebra, was den gewünschten Widerspruch liefert.

Zuletzt nehmen wir an, dass K algebraisch abgeschlossen ist, jede algebraische Erweiterung von K ist also bereits isomorph zu K. Da jede endliche Erweiterung, wie etwa E nach dem oben gezeigten, schon algebraisch ist, folgt die Behauptung. □

Hilberts Nullstellensatz Wir erinnern an den zweiten Isomorphiesatz:

Proposition 1.2.42. *Sei R ein Ring und $I \subseteq J \subseteq R$ Ideale von R. Es gilt*

$$R/J = (R/I)/(J/I).$$

Beweis. Hausaufgabe. □

Satz 1.2.43 (Hilberts Nullstellensatz)**.** *Sei K ein algebraisch abgeschlossener Körper.*

(i) Die maximalen Ideale von $K[x_1, \ldots, x_n]$ sind genau von der Form

$$(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) = \mathrm{I}(a),$$

mit $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$.

(ii) Für jedes Ideal J gilt: $\mathrm{V}(J) = \varnothing \Leftrightarrow J = (1) = K[x_1, \ldots, x_n]$.

(iii) Für jedes Ideal J gilt: $\mathrm{I}(\mathrm{V}(J)) = \sqrt{J}$.

Beweis. (i) Ist $a \in \mathbb{A}^n$, so ist das Ideal $(x_1 - a_1, \ldots, x_n - a_n) \subseteq K[x_1, \ldots, x_n]$ im Kern $\mathrm{I}(a)$ des Auswertungshomomorphismus

$$K[x_1, \ldots, x_n] \to K, f \mapsto f(a)$$

enthalten. Umgekehrt lässt sich durch "Taylorentwicklung" im Punkt a leicht einsehen, dass jedes Polynom in $\mathrm{I}(a)$ eine polynomielle Kombination der $x_i - a_i$ ist. Damit ist $(x_1 - a_1, \ldots, x_n - a_n) = \mathrm{I}(a)$ maximal, da der Auswertungshomomorphismus einen Isomorphismus $K[x_1, \ldots, x_n]/\mathrm{I}(a) \simeq K$ induziert.

Sei nun $\mathfrak{m} \subseteq K[x_1, \ldots, x_n]$ ein beliebiges maximales Ideal. Dann ist

$$K' := K[x_1, \ldots, x_n]/\mathfrak{m}$$

ein Körper und zugleich endlich erzeugt als K-Algebra. Laut Proposition 1.2.41 ist dann schon $K' \simeq K$, womit auch die Komposition

$$\varphi : K \subseteq K[x_1, \ldots, x_n] \xrightarrow{\pi} K[x_1, \ldots, x_n]/\mathfrak{m} = K'$$

ein Isomorphismus ist. Sei $b_i := \pi(x_i) = x_i + \mathfrak{m} \in K'$ und $a_i := \varphi^{-1}(b_i) \in K$. Identifizieren wir a_i als konstantes Polynom in $K[x_1, \ldots, x_n]$ vermöge der kanonischen Einbettung, so gilt

$$x_i - a_i \in \mathsf{Ker}(\pi) = \mathfrak{m}.$$

Dies zeigt, dass $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}$. Wie wir bereits gesehen haben, ist das linke Ideal ebenfalls maximal, woraus Gleichheit der beiden Ideale folgen muss.

(ii) Dies ist eine direkte Konsequenz von Teil (i). Ist $J \subsetneq K[x_1, \ldots, x_n]$ ein echtes Ideal, so existiert ein maximales Ideal $\mathfrak{m}$ mit $J \subseteq \mathfrak{m}$. Nach Teil (i) ist $\mathfrak{m}$ von der Form $\mathrm{I}(a)$ und mit Lemma 1.1.15 folgt $\mathrm{V}(\mathrm{I}(a)) = \mathrm{V}(\mathfrak{m}) \subseteq \mathrm{V}(J)$. Da aber für eine beliebige Teilmenge $X \subseteq \mathbb{A}^n$ immer $X \subseteq \mathrm{V}(\mathrm{I}(X))$ gilt, haben wir $a \in \mathrm{V}(\mathrm{I}(a)) \subseteq \mathrm{V}(J)$.

Die Implikation $J = (1) \Rightarrow \mathrm{V}(J) = \varnothing$ ist Teil (ii) von Lemma 1.1.17.

(iii) Dies wiederum basiert auf Teil (ii). Sei $J \subseteq K[x_1, \ldots, x_n]$ ein Ideal. Lemma 1.2.17 besagt $\sqrt{J} \subseteq \mathrm{I}(\mathrm{V}(J))$. Es bleibt also zu zeigen, dass $\mathrm{I}(\mathrm{V}(J)) \subseteq \sqrt{J}$ gilt. Sei dafür $f \in \mathrm{I}(\mathrm{V}(J))$. Wir müssen beweisen, dass es ein $N \in \mathbb{N}$ gibt, sodass $f^N \in J$. Dazu verwenden wir den sogenannten "Trick von Rabinowitsch", präsentiert in modernem Gewand unter Verwendung von Quotientenringen und Lokalisierungen.

Man führe eine neue Variable t ein und betrachte das Ideal

$$J' := (J, tf - 1) \subseteq K[x_1, \ldots, x_n, t].$$

Lemma 1.1.17, Teil iv) besagt, dass $\mathrm{V}(J') = \mathrm{V}(J) \cap \mathrm{V}(ft - 1)$. Ist $a \in \mathrm{V}(J)$, so gilt nach Voraussetzung, dass $f(a) = 0$. Insbesondere kann $f(a)t = 1$ nicht erfüllt sein, womit $\mathrm{V}(J') = \varnothing$. Teil (ii) des Nullstellensatzes impliziert nun, dass $J' = K[x_1, \ldots, x_n, t]$, also $K[x_1, \ldots, x_n, t]/J' = 0$. Mit dem zweiten Isomorphiesatz 1.2.42 sowie Proposition 1.2.27 folgt:

$$\begin{aligned} 0 &\simeq K[x_1, \ldots, x_n, t]/J' \\ &= K[x_1, \ldots, x_n, t]/(J, tf - 1) \\ &\simeq [K[x_1, \ldots, x_n, t]/(tf - 1)] \,/\, [(J, tf - 1)/(tf - 1)] \\ &\simeq K[x_1, \ldots, x_n]_f/J_f, \end{aligned}$$

wobei J_f die Lokalisierung des Ideals J ist. Das bedeutet, dass $J_f = K[x_1, \ldots, x_n]$, sprich $1 \in J_f$. Es existiert also ein $a \in J$ sowie ein $n \geq 0$, sodass $\frac{1}{1} \sim \frac{a}{f^n}$, also $f^n = a \in J$. □

Seinem Namen wird der Nullstellensatz aufgrund von Teil (ii) gerecht. Dieser liefert nämlich, dass jedes nichtkonstante Polynom, oder allgemeiner jede Menge nicht koprimer Polynome, mindestens eine (gemeinsame) Nullstelle besitzt.

Die anderen Teile sind aber auch sehr wichtig. So besagt Teil (i), dass Punkte in $\mathbb{A}^n$ über algebraisch abgeschlossenen Körpern, etwa den komplexen Zahlen $\mathbb{C}$, zu maximalen Idealen in $K[x_1, \ldots, x_n]$ korrespondieren, was sich als der Anfang der modernen algebraischen Geometrie ansehen lässt. Dort wird allgemeiner die Menge $\mathsf{Spec}(K[x_1, \ldots, x_n])$ der Primideale von $K[x_1, \ldots, x_n]$ (oder $\mathsf{Spec}(R)$ für beliebige Ringe R) betrachtet, welche sich ganz analog mit einer Topologie versehen lässt, die man ebenfalls Zariski-Topologie nennt.

Schließlich folgt aus Teil (iii), dass ein für ein Radikalideal $J = \sqrt{J}$ die Gleichung $\mathrm{V}(\mathrm{I}(J)) = J$ gilt. Diesen Teil werden wir am meisten benutzen, etwa zum Beweis der folgenden Aussage:

Korollar 1.2.44. *Sei K ein algebraisch abgeschlossener Körper. Seien $f, g \in K[x_1, \ldots, x_n]$, sodass für alle $a \in \mathbb{A}^n$ aus $f(a) = 0$ schon $g(a) = 0$ folgt. Dann gibt es ein Polynom $h \in K[x_1, \ldots, x_n]$ und eine natürliche Zahl $m \geq 1$, so dass*

$$g^m = f \cdot h.$$

Beweis. Etwas formeller aufgeschrieben ist unsere Voraussetzung, dass $\mathrm{V}(f) \subseteq \mathrm{V}(g)$. Lemma 1.1.22 besagt nun, dass $\mathrm{I}(\mathrm{V}(g)) \subseteq \mathrm{I}(\mathrm{V}(f))$. Da $g \in (g) \subseteq \mathrm{I}(\mathrm{V}(g)) \subseteq \mathrm{I}(\mathrm{V}(f))$ und $\mathrm{I}(\mathrm{V}(f)) = \sqrt{(f)}$ laut Hilberts Nullstellensatz (1.2.43), haben wir also $g \in \sqrt{(f)}$. Dies jedoch heißt nichts anderes als dass es ein $m \geq 1$ gibt, so dass $g^m \in (f)$, also $g^m = fh$ für irgendein $h \in K[x_1, \ldots, x_n]$. □

Es ist hierbeit zwingend notwendig, dass K algebraisch abgeschlossen ist. Betrachte etwa $f = x^2 + 1$ und $g = 1$ in $\mathbb{R}[x]$. Dann ist $\mathrm{V}(f) = \mathrm{V}(g) = \varnothing$, doch für alle $m \geq 0$ ist $g^m = 1 \notin (f)$.

Endliche Punktmengen Für das folgende Korollar, brauchen wir zuerst ein kleines Lemma, welches wir ab und zu benutzen werden.

Lemma 1.2.45. *Seien $a, b_1, \ldots, b_k \in \mathbb{A}^n$ Punkte mit $a \neq b_i$, $1 \leq i \leq k$. Es gibt ein Polynom f, so dass $f(a) \neq 0$, aber $f(b_i) = 0$ für alle $1 \leq i \leq k$.*

Beweis. Der Beweis ist elementar und bedarf keiner vorherigen Resultate. Schreibe $a = (a_1, \ldots, a_n)$ und $b_i = (b_{i1}, \ldots, b_{in})$. Sei I_1 die Menge all jener Indizes $i \in \{1, \ldots, k\}$ für die sich die erste Koordinate von b_i von a_1 unterscheidet, also

$$I_1 = \{i \mid b_{i1} \neq a_1\}.$$

Wir definieren $f_1 := \prod_{i \in I_1}(x_1 - b_{i1})$. Dies wiederholen wir analog mit den zweiten Koordinaten, um $f_2 := \prod_{i \in I_2}(x_2 - b_{i2})$ zu erhalten, und so weiter. Schließlich ist $f = \prod_{i=1}^{n} f_i$ sicherlich ein Polynom, welches auf allen b_i verschwindet (andernfalls gäbe es ein i, welches in keinem der I_r liegt, womit für das zugehörige b_i dann $b_i = a$ gelten müsste), aber a nicht als Nullstelle hat. □

Beispiel 1.2.46. Da die Hauptschwierigkeit von Lemma 1.2.45 in der Notation besteht, wollen wir das Ganze im Fall von $n = 2$ an einem konkreten Beispiel verdeutlichen. Sei etwa $a = (0,1)$ und $b_1 = (0,2), b_2 = (0,0), b_3 = (1,0), b_4 = (2,1)$ und $b_5 = (2,3)$. Dann ist $\{b_{i1} \mid i \in I_1\} = \{1,2,2\}$ und folglich $f_1 = (x-1)(x-2)^2$. Weiter ist $\{b_{i2} \mid i \in I_2\} = \{2,0,0,3\}$, also $f_2 = (y-2)y^2(y-3)$. Insgesamt ergibt sich dann $f = (x-1)(x-2)^2(y-2)y^2(y-3)$ und wir sehen sofort, dass $f(b_i) = 0$ für alle i, aber $f(a) \neq 0$. Das Polynom f ist natürlich nicht minimal mit dieser Eigenschaft, aber das war auch nicht verlangt.

Korollar 1.2.47. *Sei $J \subseteq K[x_1, \ldots, x_n]$ ein Ideal. Genau dann ist $\mathrm{V}(J)$ eine endliche Menge wenn $K[x_1, \ldots, x_n]/J$ ein endlich dimensionaler K-Vektorraum ist. Es gilt zudem*

$$|\mathrm{V}(J)| \leq \dim_K \left(K[x_1, \ldots, x_n]/J\right).$$

Beweis. Sei $\dim_K \left(K[x_1, \ldots, x_n]\right)/J$ endlich und seien $a_1, \ldots, a_r \in \mathrm{V}(J)$ paarweise verschieden. Wir wollen beweisen, dass r kleiner als die Dimension sein muss. Da die endlich und distinkt Laut Lemma 1.2.45 existieren Polynome $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$, sodass

$$f_i(a_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

Behauptung: Die Polynome sind K-linear unabhängig. Wir benutzen die Notation $\overline{f}_i = f_i \mod J$. Es gilt

$$\sum_{i=1}^{r} \lambda_i \overline{f}_i = 0 \quad \text{in} \quad K[x_1, \ldots x_n]/J \iff \sum_{i=1}^{r} \lambda_i f_i \in J \iff \left(\sum_{i=1}^{r} \lambda_i f_i\right)(a) = 0 \quad \forall a \in \mathrm{V}(J).$$

Per Definition der f_i's gilt $\lambda_j = \sum_{i=1}^{r} \lambda_i f_i(a_j)$ für alle $1 \leq j \leq r$. Es folgt

$$\lambda_j = \sum_{i=1}^{r} \lambda_i f_i(a_j) = 0$$

für alle $1 \leq j \leq r$ und die Behauptung folgt. Insbesondere also auch $r \leq \dim_K \left(K[x_1, \ldots, x_n]/J\right)$.

Umgekehrt, sei $\{a_1, \ldots, a_r\} = \mathrm{V}(J)$ endlich, mit $a_i = (a_{i1}, \ldots, a_{in})$. Wir definieren

$$f_j \coloneqq \prod_{i=1}^{r} (x_j - a_{ij}), \quad 1 \leq j \leq n.$$

Für jedes j wird einer der Faktoren von f_j für jeden der Punkte in $\mathrm{V}(J)$ Null. Anders gesagt, $f_j \in \mathrm{I}(\mathrm{V}(J))$ für jedes $1 \leq j \leq r$. Teil (iii) von Hilberts Nullstellensatz 1.2.43 besagt, dass es ein $N_j \in \mathbb{N}$ gibt, so dass $f_j^{N_j} \in J$. Indem man $N \coloneqq \max\{N_j\}_{i=1}^{r}$ setzt, gilt also $f_j^N \in J$ für alle j's.

Für $\overline{f}_j^N \coloneqq f_j^N \mod J$ gilt $\overline{f}_j^N = 0$ in $K[x_1, \ldots, x_n]/J$. Per Definition der Polynome f_j können wir $\overline{x}_j^{rN}$, für jedes j, als eine K-lineare Kombination der $1, \overline{x}_j, \overline{x}_j^2, \ldots, \overline{x}_j^{rN-1}$ darstellen. Es folgt, dass die endliche Menge $\left\{\overline{x}_1^{k_1}, \ldots, \overline{x}_n^{k_n} \mid k_i \leq rN\right\}$ ein Erzeugendensystem von $K[x_1, \ldots, x_n]/J$ ist. □

1.2.5 Primideale und Irreduzible Varietäten

Von Hilberts Nullstellensatz wissen wir, dass Maximalideale zu Punkten und Radikalideale zu abgeschlossenen Mengen korrespondieren. Wir wollen nun verstehen, wie Primideale in dieses Bild passen.

Lemma 1.2.48. *Jedes Primideal ist radikal.*

Beweis. Ist $\mathfrak{p}$ prim, so folgt aus $a^n \in \mathfrak{p}$ schon $a \in \mathfrak{p}$. □

Definition 1.2.49. *Ein nichtleerer topologischer Raum X heißt* irreduzibel*, , wenn er sich nicht als Vereinigung echter abgeschlossener Teilmengen schreiben lässt. Das heißt, für alle abgeschlossenen Teilmengen X_1, X_2 folgt aus $X = X_1 \cup X_2$ schon $X_1 = X$ oder $X_2 = X$. Eine* irreduzible Teilmenge *eines topologischen Raumes X, ist eine Teilmenge $Y \subseteq X$, welche bezüglich der Teilraumtopologie irreduzibel ist.*

Offenbar sind einpunktige Teilmengen irreduzibel. Versehen wir $\mathbb{C}^n$ oder $\mathbb{R}^n$ mit der klassischen metrischen Topologie, sind dies sogar die einzigen irreduziblen Teilmengen. Dies gilt allgemeiner für beliebige Hausdorffsche Räume und lässt sich sehr leicht mit der äquivalenten Charakterisierung von Irreduzibilität über offene Mengen einsehen. In der Zariski-Topologie dagegen gibt es sehr viel mehr irreduzible Teilmengen, siehe folgenden Satz, weshalb das Konzept der Irreduzibilität erst in der algebraischen Geometrie wirklich Früchte trägt.

Satz 1.2.50. *Sei K ein Körper, $X \subseteq \mathbb{A}^n_K$ eine Varietät und $J \subseteq K[x_1, \ldots, x_n]$ ein Radikalideal.*

(i) Es ist X genau dann irreduzibel, wenn $\mathrm{I}(X)$ prim ist.

(ii) Ist K algebraisch abgeschlossen, so ist J genau dann prim, wenn $\mathrm{V}(J)$ irreduzibel ist.

Beweis. (i) Sei X irreduzibel, insbesondere ist $X \neq \varnothing$, also $\mathrm{I}(X) \neq (1)$, nach Korollar 1.1.27. Um zu zeigen, dass $\mathrm{I}(X)$ prim ist, seien Polynome f und g gegeben, sodass $fg \in \mathrm{I}(X)$. Mit Lemma 1.1.17 folgt, dass $\mathrm{V}(f) \cup \mathrm{V}(g) = \mathrm{V}(f \cdot g) \supseteq \mathrm{V}(\mathrm{I}(X)) = X$. Da X irreduzibel ist, muss schon $X \subseteq \mathrm{V}(f)$ oder $X \subseteq \mathrm{V}(g)$ gelten. Ohne Einschränkung sei $X \subseteq \mathrm{V}(f)$, sodass also $f(x) = 0$ für alle $x \in X$ ist. Dann gilt aber gerade $f \in \mathrm{I}(X)$.

Sei nun umgekehrt X reduzibel, es existieren also Varietäten $Y, Z \subsetneq X$ mit $X = Y \cup Z$. Nach Korollar 1.1.27 ist dann $\mathrm{I}(Y) \supsetneq \mathrm{I}(X)$ und $\mathrm{I}(Z) \supsetneq \mathrm{I}(X)$, wir finden also Polynome

$$f \in \mathrm{I}(Y) \setminus \mathrm{I}(X) \text{ und } g \in \mathrm{I}(Z) \setminus \mathrm{I}(X).$$

Da $X = Y \cup Z$ ist nun aber $f \cdot g \in I(X)$. Zugleich liegen aber weder f noch g in $\mathrm{I}(X)$, womit $\mathrm{I}(X)$ nicht prim sein kann.

(ii) Sei nun K algebraisch abgeschlossen und J ein Radikalideal. Nach Teil (iii) des Hilbertschen Nullstellensatzes 1.2.43 ist dann $\mathrm{I}(\mathrm{V}(J)) = \sqrt{J} = J$. Aus (i) folgt daher, dass $X = \mathrm{V}(J)$ genau dann irreduzibel ist, wenn $\mathrm{I}(X) = J$ prim ist. □

Die Korrespondenz zwischen Idealen und Varietäten

Korollar 1.2.51. *Sei K algebraisch abgeschlossen. Die ordnungsumkehrenden Abbildungen*

$$\{ \text{ Teilmengen von } K[x_1, \ldots, x_n] \} \underset{\mathrm{I}}{\overset{\mathrm{V}}{\rightleftarrows}} \{ \text{ Teilmengen von } \mathbb{A}^n \}$$

schränken zu folgenden Bijektionen ein:

$$(i) \qquad \{\text{Radikalideale in } K[x_1, \ldots, x_n]\} \quad \overset{\simeq}{\longleftrightarrow} \quad \{ \text{ Varietäten in } \mathbb{A}^n\}$$

$$(ii) \qquad \{ \text{ Primideale in } K[x_1, \ldots, x_n]\} \quad \overset{\simeq}{\longleftrightarrow} \quad \{ \text{ irreduzible Varietäten in } \mathbb{A}^n\}$$

$$(iii) \qquad \{ \text{ Maximalideale in } K[x_1, \ldots, x_n]\} \quad \overset{\simeq}{\longleftrightarrow} \quad \{ \text{ Punkte in } \mathbb{A}^n\}.$$

Beweis. Für jedes Ideal $J \subseteq K[x_1, \ldots, x_n]$ ist $\mathrm{V}(J)$ per Definition eine Varietät. Ist J überdies prim, so ist $\mathrm{V}(J)$ irreduzibel nach Satz 1.2.50 Teil (ii). Ist J sogar maximal, so ist $\mathrm{V}(J)$ offensichtlich ein Punkt.

Umgekehrt ist für jede algebraische Varietät $X \subseteq \mathbb{A}^n$, das Verschwindungsideal radikal nach dem dritten Teil des Hilbertschen Nullstellensatzes. Denn ist $X = \mathrm{V}(J)$ für ein Ideal $J \subseteq K[x_1, \ldots, x_n]$, so ist

$$\sqrt{I(X)} = \sqrt{\mathrm{I}(\mathrm{V}(J))} = \sqrt{\sqrt{J}} = \sqrt{J} = \mathrm{I}(\mathrm{V}(J)) = \mathrm{I}(X).$$

Ist X irreduzibel, so ist $\mathrm{I}(X)$ prim nach Satz 1.2.50 (i). Und schließlich ist $\mathrm{I}(X)$ maximal, wenn X ein Punkt ist, nach dem ersten Teil des Hilbertschen Nullstellensatzes 1.2.43.

Damit ist gezeigt, dass sowohl V als auch I auf die oben genannten Teilmengen einschränken. Es bleibt zu beweisen, dass sie auf diesen Teilmengen Bijektionen definieren, also dass $\mathrm{V}(\mathrm{I}(-)) = \mathsf{Id}$ und $\mathrm{I}(\mathrm{V}(-)) = \mathsf{Id}$. Die erste Gleichung folgt aus der Tatsache, dass $\mathrm{V}(\mathrm{I}(-))$ nach Satz 1.1.26 den Zariski-Abschluss einer Teilmenge bildet und Varietäten per Definition bereits abgeschlossen sind. Für die zweite Gleichung benötigen wir den dritten Teil des Hilbertschen Nullstellensatzes 1.2.43, welcher besagt, dass $\mathrm{I}(\mathrm{V}(-))$ das Radikal eines Ideals bildet. Da maximale Ideale, Primideale und natürlich radikale Ideale gleich ihrem eigenen Radikal sind, folgt auch die zweite Gleichung. □

1.3 Affine Varietäten und deren Koordinatenringe

In den vorherigen Abschnitten haben wir algebraische Varietäten als abgeschlossene Teilmengen des affinen Raums $\mathbb{A}^n$ über einem algebraisch abgeschlossenen Körper K definiert. Diese geometrischen Objekte haben wir, nicht zuletzt mithilfe des Hilbertschen Nullstellensatzes, mit algebraischen Objekten, nämlich den Idealen im Polynomring $K[x_1, \ldots, x_n]$, in Verbindung gebracht. Dabei haben wir den Polynomring als Koordinatenring, also als Ring von Funktionen auf dem affinen Raum aufgefasst. Im Folgenden wollen wir allgemeiner Koordinatenringe beliebiger algebraischer Varietäten studieren. Da der affine Raum natürlich selbst eine algebraische Varietät ist, kann man dies als echte Verallgemeinerung des letzten Abschnitts ansehen.

1.3.1 Der Koordinatenring $K[\mathrm{V}]$ einer Varietät

Im Folgenden wird $\mathrm{V} \subseteq \mathbb{A}^n$ durchgehend eine Varietät bezeichnen. Wenn $f \in R$ Element eines Rings R und $I \subseteq R$ ein Ideal ist, werden wir mit $\overline{f}$ dessen Projektion in R/I notieren. Umgekehrt, wenn $f \in R/I$, so bezeichne $\hat{f}$ eine (beliebige) Hochhebung von f in R. Es ist also $\overline{\left(\hat{f}\right)} = f$ und $f - \left(\hat{\overline{f}}\right) \in I$.

Polynomfunktionen Man erinnere sich an Lemma 1.1.4, wo wir gesehen haben, dass sich der Polynomring $K[x_1, \ldots, x_n]$ injektiv in den Ring der Funktionen $\mathbb{A}^n \to K$ einbetten lässt (zumindest falls K unendlich viele Elemente hat, was aber immer der Fall ist, wenn K algebraisch abgeschlossen ist). Eine beliebige Funktion $\mathbb{A}^n \to K$ nennen wir daher *Polynomfunktion*, wenn sie im Bild dieser Einbettung liegt. Allgemeiner definieren wir:

Definition 1.3.1. *Eine Abbildung $f : \mathrm{V} \to K$ heißt* Polynomfunktion auf V*, falls es ein Polynom $\hat{f} \in K[x_1, \ldots, x_n]$ gibt, sodass $\hat{f}_{|\mathrm{V}} = f$, also falls $f(a) = \hat{f}(a)$ für jedes $a \in \mathrm{V}$.*

In obiger Definition identifizieren wir $\hat{f}$ mit der von $\hat{f}$ induzierten Polynomfunktion $\mathbb{A}^n \to K$. Weiter bezeichnet $\hat{f}_{|\mathrm{V}}$ die Einschränkung von $\hat{f}$ auf V.

Man beachte, dass das Polynom $\hat{f}$, welches zu einer Polynomfunktion $f : \mathrm{V} \to K$ assoziiert ist, nicht unbedingt eindeutig bestimmt sein muss. Dies steht im Gegensatz zum globalen Fall $\mathrm{V} = \mathbb{A}^n$, wo Lemma 1.1.6 uns Eindeutigkeit garantiert. Man betrachte etwa $\mathrm{V} = \varnothing$ oder folgendes etwas instruktiveres Beispiel:

Beispiel 1.3.2. Sei $\mathrm{V} = \mathrm{V}(x - y)$. Betrachte $f(x, y) = 2x - y$ und $g(x, y) = x$. Da $\mathrm{V}(x - y) = \{(a, b) \mid a = b\}$, gilt $f_{\mathrm{V}} = 2x - x = x = g_{\mathrm{V}}$.

Wir können aber genau charakterisieren, wann zwei Polynome dieselbe Polynomfunktion auf einer Varietät V definieren, was uns dann zur Definition des Koordinatenrings von V führen wird.

Proposition 1.3.3. *Zwei Polynome $f, g \in K[x_1, \ldots, x_n]$ definieren die selbe Polynomfunktion $\mathrm{V} \to K$ genau dann, wenn $f - g \in \mathrm{I}(\mathrm{V})$.*

Beweis. Es gilt $f_{|\mathrm{V}} = g_{|\mathrm{V}} \Leftrightarrow f_{|\mathrm{V}} - g_{|\mathrm{V}} = 0_{|\mathrm{V}} \Leftrightarrow \ \forall a \in \mathrm{V}$ gilt $(f - g)(a) = 0 \Leftrightarrow f - g \in \mathrm{I}(\mathrm{V})$. □

Quotientenringe und der Koordinatenring $K[\mathrm{V}]$ einer Varietät

Definition 1.3.4. *Der* Koordinatenring *von* V *ist definiert als der Quotientenring*

$$K[\mathrm{V}] \coloneqq K[x_1, \ldots, x_n]/\mathrm{I}(\mathrm{V}).$$

Eine alternative Notation für $K[\mathrm{V}]$ ist $\Gamma(\mathrm{V})$. Obige Proposition 1.3.3 besagt, dass die Abbildung, welche einem Polynom seine zugehörige Polynomfunktion $\mathrm{V} \to K$ zuordnet, einen Isomorphismus zwischen dem Koordinatenring $K[\mathrm{V}]$ und dem Ring der Polynomfunktionen $\mathrm{V} \to K$ induziert. Explizit lässt sich eine Polynomfunktion $\mathrm{V} \to K$ als eine Äquivalenzklasse von Polynomen in n Variablen über K beschreiben, welche genau dann äquivalent sind, wenn sie auf V übereinstimmen.

Bemerkung 1.3.5. Der Koordinatenring $K[\mathrm{V}]$ einer Varietät ist im Allgemeinen kein faktorieller Ring. Mit anderen Worten gibt es normalerweise keine eindeutige Zerlegung in irreduzible Elemente. Daher ergibt es auch keinen Sinn von einer irreduziblen Darstellung zu reden. Dies ist im allgemeinen nicht einmal in einer Variablen richtig. Die algebraische Zahlentheorie setzt sich intensiv mit dieser Frage auseinander.

Bemerkung 1.3.6. Unter der Identifizierung zwischen dem Koordinatenring $K[x_1, \ldots, x_n]/\mathrm{I}(V)$ einer Varietät V und dem Ring der Polynomfunktionen $\mathrm{V} \to K$ werden die Erzeuger x_i als Projektionen $x_i : \mathrm{V} \subseteq \mathbb{A}^n = K^n \to K$ auf die i-te Koordinate aufgefasst. Das heißt $(a_1, \ldots, a_n) \in \mathrm{V}$ wird von x_i auf a_i abgebildet.

Der Fall $\mathrm{V} = \mathbb{A}^n$ ist natürlich ein besonderer Spezialfall. In diesem Fall gilt $K[\mathrm{V}] = K[x_1, \ldots, x_n]$.

Proposition 1.3.7. *Eine Varietät ist genau dann irreduzibel, wenn ihr Koordinatenring ein Integritätsbereich ist.*

Beweis. Dies ist eine direkte Konsequenz von Satz 1.2.50 und der Tatsache, dass ein Quotientenring R/I genau dann ein Integritätsbereich ist, wenn I ein Primideal ist. □

Bemerkung 1.3.8. Man nehme zwei irreduzible Polynome $f, g \in K[x_1, \ldots, x_n]$ und betrachte $K[\mathrm{V}(fg)] = K[x_1, \ldots, x_n]/(fg)$. Dann ist $\overline{f}, \overline{g} \neq 0$ in $K[\mathrm{V}(fg)]$, aber ihr Produkt $\overline{f}\overline{g}$ ist per Konstruktion Null. Daher ist $K[\mathrm{V}(fg)]$ kein Integritätsbereich.

1.3.2 Die Ideale von $K[\mathrm{V}]$

Wir wollen nun die Ideale von $K[\mathrm{V}]$ studieren. Dazu untersuchen wir allgemeiner Ideale beliebiger Quotientenringe.

Bilder von Idealen in Quotientenringen Zur Erinnerung, das Urbild eines Primideals unter einem Ringhomomorphismus ist wieder ein Primideal. Das Urbild eines maximalen Ideals ist jedoch im Allgemeinen nicht mehr maximal, sondern lediglich prim.

Das Bild eines Ideals unter einem Ringhomomorphismus muss nicht einmal mehr ein Ideal sein. Selbst wenn man das vom Bild erzeugte Ideal (das entlang des Morphismus "vorgedrückte" Ideal) betrachtet, wird weder Primalität noch Maximalität erhalten. Ist der Ringhomomorphismus jedoch surjektiv, haben wir folgendes Resultat:

Proposition 1.3.9. *Sei R ein Ring, $I \subseteq J \subseteq R$ Ideale und $\pi : R \to R/I$ die kanonische Projektion. Wir haben folgende Resultate:*

(i) Das Bild $\pi(J)$ ist ein Ideal von R/I (hier braucht man $I \subseteq J$ nicht).

(ii) Sei J ein Radikalideal. Dann ist $\pi(J)$ ein Radikalideal.

(iii) Sei $J = \mathfrak{p}$ prim. Dann ist $\pi(\mathfrak{p})$ ein Primideal.

(iv) Sei $J' \subseteq R/I$ ein Ideal. Es gilt

(a) $I \subseteq \pi^{-1}(J')$,
(b) $\pi(\pi^{-1}(J')) = J'$ und
(c) $\pi^{-1}(\pi(J)) = J$.

(v) Es gilt $I \subseteq J \subseteq J' \subseteq R$ genau dann, wenn $\pi(J) \subseteq \pi(J') \subseteq R/I$ mit Gleichheiten in R, genau dann, wenn wir Gleichheiten in R/I haben.

(vi) Sei $J = \mathfrak{m}$ ein Maximalideal. Dann ist $\pi(\mathfrak{m})$ ein Maximalideal.

Beweis. Hausaufgabe. □

Statt $\pi(\mathfrak{m})$ schreibt man auch $\mathfrak{m}/I$, da dies genau der Gruppenquotient $\mathfrak{m}/(I \cap \mathfrak{m})$ ist.

Bemerkung 1.3.10. Ein Wort zu Teil (vi). Laut Hilberts Nullstellensatz 1.2.43 entsprechen maximale Ideale von $K[x_1, \ldots, x_n]$ genau den Punkten von $\mathbb{A}^n$. Sei nun $V \subseteq \mathbb{A}^n$ eine Varietät. Auf der geometrischen Seite können wir einen Punkt $a \in V$ natürlich trivialerweise als einen Punkt $a \in \mathbb{A}^n$ vermöge der kanonischen Injektion $V \subseteq \mathbb{A}^n$ auffassen.

Teil (vi) von obiger Proposition 1.3.9 besagt nun, dass dies auch auf der algebraischen Seite möglich ist. Genauer setzen wir $R = K[x_1, \ldots, x_n]$, $I = \mathrm{I}(V)$ und $J = \mathrm{I}(a)$, dann bildet die kanonische Projektion $R \to K[V]$ das maximale Ideal $J = \mathrm{I}(a)$ auf ein maximales Ideal in $K[V]$ ab.

Teil (iii) ist die schematheoretische Verallgemeinerung davon, wo statt den maximalen Idealen allgemeiner Primideale von Ringen untersucht werden.

(Beachte, dass hier eine Injektion $V \to \mathbb{A}^n$ zu einer Surjektion $K[\mathbb{A}^n] \to K[V]$ auf Koordinatenringen in die entgegengesetzte Richtung geführt hat. Dieses Umdrehen der Pfeile und Eigenschaften ist ein fundamentales Phänomen der Dualität zwischen Geometrie und Algebra, welches wir durchgehend beobachten können.)

Wir fassen unsere Diskussion hier zusammen:

Korollar 1.3.11. *Es gibt eine ordnungserhaltende bijektive Beziehung zwischen den Idealen von $K[x_1, \ldots, x_n]$, welche $\mathrm{I}(\mathrm{V})$ enthalten und den Idealen von $K[\mathrm{V}]$. Unter dieser Zuordnung werden Radikalideale auf Radikalideale abgebildet, Primideale auf Primideale und Maximalideale auf Maximalideale.*

Beweis. Nach Proposition 1.3.9 bleibt nur noch zu beweisen, dass die Urbilder alle Eigenschaften erhalten. Für Radikalideale haben wir es in Lemma 1.2.12 gezeigt. Für Prim- und Maximalideale ist es wohlbekannt (und einfach zum überprüfen). □

Definition 1.3.12. *Eine Varietät $\mathrm{W} \subseteq \mathbb{A}^n$ wird eine* Untervarietät *von V genant, falls $\mathrm{W} \subseteq \mathrm{V}$. Dies ist äquivalent zu sagen, dass es ein Ideal $J \subseteq K[\mathrm{V}]$ gibt, sodass $\mathrm{W} = \mathrm{V}(\pi^{-1}(J))$.*

Verhältnis zwischen Unteridealen und Untervarietäten

Satz 1.3.13. *Es gibt eine bijektive Beziehung zwischen den Untervarietäten von V und den Idealen von $K[\mathrm{V}]$. Unter dieser Korrespondenz sind folgende Teilmengen bijektiv zueinander:*

(i)	{ Radikalideale in $K[\mathrm{V}]$}	$\overset{\simeq}{\longleftrightarrow}$	{ Untervarietäten in V}
(ii)	{ Primideale in $K[\mathrm{V}]$}	$\overset{\simeq}{\longleftrightarrow}$	{ irreduzible Untervarietäten in V}
(iii)	{ Maximalideale in $K[\mathrm{V}]$}	$\overset{\simeq}{\longleftrightarrow}$	{ Punkte von V}.

Beweis. Dies folgt aus Korollar 1.3.11 und Korollar 1.2.51. □

1.3.3 Morphismen zwischen Varietäten

Wir haben bisher nur Varietäten betrachtet. Wie aber in so ziemlich allen algebraischen Bereichen, ist dies nur die Hälfte der Geschichte. Die andere Hälfte sind Morphismen zwischen zwei Varietäten. Beachte, dass die Varietäten in affinen Räumen verschiedener Dimension liegen können. Wir nehmen aber stets an, dass der Grundkörper derselbe ist.

Polynomielle Abbildungen

Definition 1.3.14. *Sein $\mathrm{V} \subseteq \mathbb{A}^n_K$ und $\mathrm{W} \subseteq \mathbb{A}^m_K$ Varietäten. Eine Abbildung $f : \mathrm{V} \to \mathrm{W}$ heißt* polynomiell*, falls es Polynome $\hat{f}_1, \ldots, \hat{f}_m \in K[x_1, \ldots, x_n]$ gibt, sodass*

$$f(a) = \left(\hat{f}_1(a), \ldots, \hat{f}_m(a)\right) \in \mathrm{W}$$

für alle $a \in \mathrm{V}$. Eine polynomielle Abbildung wird auch Morphismus von Varietäten *genannt.*

Lemma 1.3.15. *Eine Abbildung $f : \mathrm{V} \to \mathrm{W}$ ist genau dann eine polynomielle Abbildung, wenn es Polynomfunktionen $f_j : \mathrm{V} \to K$, $1 \leq j \leq m$ (also $f_j \in K[\mathrm{V}]$) gibt, sodass für alle $a \in \mathrm{V}$, $f(a) = (f_1(a), \ldots, f_m(a))$.*

Beweis. Diese f_j sollen natürlich die Äquivalenzklassen der $\hat{f}_j$ in der Definition 1.3.14 sein. Sei $f = \left(\hat{f}_1, \ldots, \hat{f}_m\right) : \mathrm{V} \to \mathrm{W}$ eine polynomielle Abbildung, wobei $\hat{f}_i \in K[x_1, \ldots, x_n]$. Durch die natürliche Projektion $\pi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]/\mathrm{I}(\mathrm{V}) = K[\mathrm{V}]$ definieren wir $f_j := \pi\left(\hat{f}_j\right)$. Da per Definition $f_j(a) = \hat{f}_j(a)$ für alle $a \in \mathrm{V}$ gilt, ist

$$(f_1(a), \ldots, f_m(a)) = \left(\hat{f}_1(a), \ldots, \hat{f}_m(a)\right) = f(a),$$

wie gewünscht.

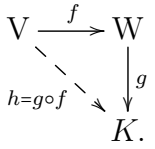
Seien andererseits $f_j \in K[\mathrm{V}]$ Polynomfunktionen. Man nehme einen Repräsentanten $\hat{f}_j$ in $\pi^{-1}(f_j)$. Per Definition stimmen $\hat{f}_j$ und f_j auf V miteinander überein. Daher folgt

$$f(a) = (f_1(a), \ldots, f_m(a)) = \left(\hat{f}_1(a), \ldots, \hat{f}_m(a)\right),$$

wobei die $\hat{f}_j$'s in $K[x_1, \ldots, x_n]$ liegen und wir für alle $a \in \mathrm{V}$ in W landen. □

Die Präkomposition

Lemma 1.3.16. *Sei $f : \mathrm{V} \to \mathrm{W}$ eine polynomielle Abbildung und $g : \mathrm{W} \to K$ eine Polynomfunktion auf* W. *Dann ist $h := g \circ f : \mathrm{V} \to K$ eine Polynomfunktion auf* V.



Beweis. Da $g : \mathrm{W} \to K$ eine Polynomfunktion ist, gibt es ein $\hat{g} \in K[x_1, \ldots, x_m]$, sodass $\hat{g}(b) = g(b)$ für alle $b \in \mathrm{W}$. Per Definition gibt es auch Polynome $\hat{f}_1, \ldots, \hat{f}_m \in K[x_1, \ldots, x_n]$, sodass $f(a) = \left(\hat{f}_1(a), \ldots, \hat{f}_m(a)\right) \in \mathrm{W}$ für alle $a \in \mathrm{V}$. Dann ist

$$\hat{h} := \hat{g}(\hat{f}_1(x_1, \ldots, x_n), \ldots, \hat{f}_m(x_1, \ldots, x_n)) \in K[x_1, \ldots, x_n]$$

und es gilt $\hat{h}(a) = \hat{g}(\hat{f}_1(a), \ldots, \hat{f}_m(a)) = g(f(a)) = h(a)$ für alle $a \in \mathrm{V}$. Damit ist h eine Polynomfunktion. □

Beispiel 1.3.17. Sei $\mathrm{V} = \mathrm{V}(y - x^2) \subseteq K[x, y]$, $\mathrm{W} = \mathrm{V}(yz - x^2) \subseteq K[x, y, z]$, $f : \mathrm{V} \to \mathrm{W}$ gegeben durch $(a, b) \mapsto (a, b, 1)$ und $g : \mathrm{W} \to K$ gegeben durch $(a, b, c) \mapsto a + b + c$. Dann ist $h = g \circ f : \mathrm{V} \to K$ gegeben durch $h(a, b) = g(f(a, b)) = g(a, b, 1) = a + b + 1$.

Definition 1.3.18. *Seien X, Y topologische Räume. Man erinnere sich, dass eine Abbildung $f : X \to Y$* stetig *ist, wenn für alle $V \subseteq Y$ offen, $f^{-1}(V) \subseteq X$ offen ist. Alternativ: wenn für jede abgeschlossene Teilmenge $\mathrm{Z} \subseteq Y$, das Urbild $f^{-1}(\mathrm{Z}) \subseteq X$ abgeschlossen ist.*

In $\mathbb{R}^n$ ist dies äquivalent zu der klassischen ε-δ-Definition von Stetigkeit. Das folgende kann man auch aus Proposition 1.3.9 schlussfolgern:

Lemma 1.3.19. *Eine polynomielle Abbildung $f : \mathrm{V} \to \mathrm{W}$ ist stetig bezüglich der Zariski-Topologie (genauer, in der von der Zariski-Topologie induzierten Teilraumtopologie).*

Beweis. Sei $\mathrm{Z} = \mathrm{V}(J) \subseteq \mathrm{W}$ abgeschlossen. Wir müssen zeigen, dass $f^{-1}(\mathrm{Z}) \subseteq \mathrm{V}$ abgeschlossen ist. Sei $J = (h_1, \ldots, h_k)$ das Ideal erzeugt von den h_i's. Wie in Lemma 1.3.16 argumentiert, sind $h_i \circ f \in K[\mathrm{V}]$ (da Polynomfunktionen von V nach K, genau den Elementen von $K[\mathrm{V}]$ entsprechen, siehe Proposition 1.3.3 bzw. Definition 1.3.4). Somit ist $f^{-1}(\mathrm{Z}) = \mathrm{V}(h_1 \circ f, \ldots, h_k \circ f)$, was per Definition abgeschlossen ist. □

Lemma 1.3.20. *Seien $\mathrm{U} \subseteq \mathbb{A}^k, \mathrm{V} \subseteq \mathbb{A}^n, \mathrm{W} \subseteq \mathbb{A}^m$ Varietäten und $\mathrm{U} \xrightarrow{f} \mathrm{V} \xrightarrow{g} \mathrm{W}$ polynomielle Abbildungen. Dann ist $g \circ f : \mathrm{U} \to \mathrm{W}$ eine polynomielle Abbildung.*

Beweis. Dies wird genauso bewiesen wie die obigen Lemmas. Man wählt sich Repräsentanten $\hat{f}$ und $\hat{g}$ und komponiert diese. Da eine Komposition von Polynomen wider ein Polynom ist, bleibt hier nichts zu zeigen. □

Sei $f : \mathrm{V} \to \mathrm{W}$ eine polynomielle Abbildung. Von Lemma 1.3.16 wissen wir, dass wir für jede Polynomfunktion $g : \mathrm{W} \to K$ eine Polynomfunktion $g \circ f : \mathrm{V} \to K$ erhalten. Wir erhalten eine Abbildung

$$\begin{aligned} f^* : K[\mathrm{W}] &\to K[\mathrm{V}], \\ g &\mapsto f^*(g) := g \circ f. \end{aligned}$$

die *Präkomposition* mit f.

Aufgepasst, hier hat sich die Richtung geändert. (Dies ist auch der Grund, warum das Sternchen oben ist. Ware die Richtung gleich geblieben, wäre das Sternchen unten. Dies ist eine etablierte Notation, welche ursprünglich aus der homologischen Algebra stammt).

Äquivalenz zwischen Varietäten und Koordinatenringen

Proposition 1.3.21. *Sei $f : \mathrm{V} \to \mathrm{W}$ eine polynomielle Abbildung. Die induzierte Abbildung $f^* : K[\mathrm{W}] \to K[\mathrm{V}]$ ist ein Homomorphismus von K-Algebren.*

Beweis. Seien $g, h \in K[\mathrm{W}]$ und $c \in K$. Es gilt

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

und

$$f^*(gh) = (gh) \circ f = (g \circ f)(h \circ f) = f^*(g) \cdot f^*(h),$$

wobei die ersten und letzten Gleichungen Definitionen sind und die Mittleren eine allgemeine Kompositionseigenschaft für Punktweise Addition (bzw. Multiplikation) ist. Was wir damit

meinen ist, dass die Addition $g+h$ und Multiplikation gh punktweise auf K definiert sind, daher $(g+h)(x) \coloneqq g(x)+h(x)$ und $(gh)(x) \coloneqq g(x)h(x)$.

Die Einheit $1_{K[\mathrm{W}]}$ ist die Abbildung $\mathrm{W} \to K$, welches jedes Element $b \in \mathrm{W}$ auf die Einheit in K abbildet. Wohin auch immer f ein Element $a \in V$ abbilden sollte, es muss ein Element in W sein. Nach der Komposition mit f wird diese also auf die Einheit in K gehen. Dies beweist, dass f^* ein Ringhomomorphismus ist.

Für jede konstante Abbildung $k : \mathrm{W} \to K$, (wo jedes $b \in \mathrm{W}$ stets zu $k \in K$ geht) ist $f^*(k) = k \circ f$ wider die konstante Abbildung $k : \mathrm{V} \to K$. Daher ist also $f^*(k) = k$ was f^* zu einem K-Algebrahomomorphismus macht. (Denn es folgt, dass $f^*(kg) = f^*(k)f^*(g) = kf^*(g)$). □

Wir haben gezeigt, dass polynomielle Abbildungen von V nach W, Homomorphismen von K-Algebren zwischen den assoziierten Koordinatenringen $K[\mathrm{W}]$ und $K[\mathrm{V}]$ induzieren. Nun wollen wir die Umkehrung dieser Aussage beweisen. Zuvor aber eine kurze Bemerkung zur Interaktion zwischen Polynomen und Homomorphismen von K-Algebren.

Bemerkung 1.3.22. Sei $\varphi : K[y_1, \ldots, y_m] \to K[x_1, \ldots, x_n]$ ein K-Algebrahomomorphismus und $g \in K[y_1, \ldots, y_m]$. Dann gilt

$$\varphi(g) = g(\varphi(y_1), \ldots, \varphi(y_m)).$$

Falls es nicht klar ist, mache man es sich am Beispiel klar: Sei $\varphi : K[y_1, y_2] \to K[x]$, gegeben durch $\varphi(y_1) = x^3$ und $\varphi(y_2) = x^2$. Sei $g = 2y_1y_2 + y_1^2 + 3y_2$. Dann gilt

$$\varphi(g) = \varphi(2y_1y_2 + y_1^2 + 3y_2) = 2\varphi(y_1)\varphi(y_2) + \varphi(y_1)^2 + 3\varphi(y_2) = g(\varphi(y_1), \varphi(y_2)).$$

Proposition 1.3.23. *Sei $\varphi : K[\mathrm{W}] \to K[\mathrm{V}]$ ein Homomorphismus von K-Algebren. Es gibt genau eine polynomielle Abbildung $f : \mathrm{V} \to \mathrm{W}$, sodass $\varphi = f^*$.*

Beweis. Als erstes konstruieren wir eine Abbildung $f : \mathrm{V} \to \mathrm{W}$, dann zeigen wir, dass dies eine polynomielle Abbildung ist und schließlich beweisen wir, dass $f^* = \varphi$.

Sei $\mathrm{W} \subseteq \mathbb{A}^m$, mit $K[\mathrm{W}] = K[x_1, \ldots, x_m]/\mathrm{I}(W)$. Wir bezeichnen mit $\overline{x}_j \in K[\mathrm{W}]$ die Klasse von $x_j \in K[x_1, \ldots, x_m]$ in $K[\mathrm{W}]$. Es ist $\varphi(\overline{x}_j) \in K[\mathrm{V}]$ was einer Abbildung $\varphi(\overline{x}_j) : \mathrm{V} \to K$ entspricht. Definiere

$$f \coloneqq (\varphi(\overline{x}_1), \ldots, \varphi(\overline{x}_m)).$$

Um zu überprüfen, dass dies eine polynomielle Abbildung ist, können wir direkt Lemma 1.3.15 (für $f_j = \varphi(\overline{x}_j)$) anwenden, sofern wir sicherstellen, dass f wirklich eine Abbildung von V nach W ist. A priori ist es nur eine Abbildung $\mathrm{V} \to \mathbb{A}^m$. Wir wollen nun beweisen, dass $f(\mathrm{V}) \subseteq \mathrm{W}$.

Sei $a \in \mathrm{V}$. Laut Korollar 1.1.27 gilt $\mathrm{V}(\mathrm{I}(\mathrm{W})) = \mathrm{W}$. Um zu zeigen, dass $f(a) \in \mathrm{W}$, müssen wir also beweisen, dass für alle Polynome $\mathrm{I}(\mathrm{W}) \ni \hat{g} : \mathbb{A}^m \to K$ gilt, dass $\hat{g}(f(a)) = 0$. Da aber $\hat{g}$ ein Polynom in den Variablen $x_1, \ldots x_m$ ist und φ ein K-Algebrahomomorphismus, kommutieren $\hat{g}$ und φ, wie in Bemerkung 1.3.22. Wir erhalten also

$$\hat{g}(f(a)) = \hat{g}(\varphi(\overline{x}_1)(a), \ldots, \varphi(\overline{x}_m)(a)) = \left(\varphi\left(\overline{\hat{g}}\right)\right)(a) = \varphi(0)(a) = 0(a) = 0$$

Hier benutzen wir noch die Tatsache, dass $\hat{g} \in \mathrm{I}(\mathrm{W})$ und daher das Bild konstant Null in $K[W]$ ist.

Da die Elemente $\overline{x}_j$ die K-Algebra $K[\mathrm{W}]$ erzeugen, genügt es zu zeigen, dass

$$\varphi(\overline{x}_j) = f^*(\overline{x}_j),$$

um zu zeigen, dass $\varphi = f^*$. Doch dies gilt per Konstruktion von unserem f, denn $\varphi(\overline{x}_j)$ ist die j'te Komponente unserer Funktion f, siehe Bemerkung 1.3.6. Auf der anderen Seite ist $f^*(\overline{x}_j)$ per Definition die Komposition $\overline{x}_j \circ f$, wobei wir $\overline{x}_j$ hier mit der natürlichen Projektion auf die j-Koordinate gleichsetzen. Damit folgt auch die Eindeutigkeit. □

Wir bezeichnen das oben konstruierte f auch mit $\varphi^!$.

Korollar 1.3.24. *Es gibt eine natürliche Bijektion*

$$(-)^* : \left\{\textit{polynomielle Abb. } \mathrm{V} \to \mathrm{W}\right\} \xleftrightarrow{\simeq} \left\{K\textit{-Algebrenhom. } K[\mathrm{W}] \to K[\mathrm{V}]\right\} : (-)^!$$

Beweis. Die Abbildungen werden in Propositionen 1.3.21 und 1.3.23 definiert. Es gilt noch zu zeigen, dass die Kompositionen Identitäten sind.

Sei $\varphi : K[\mathrm{W}] \to K[\mathrm{V}]$. Dann ist $\varphi^! : \mathrm{V} \to \mathrm{W}$ durch

$$a \mapsto (\varphi(\overline{x_1})(a), \ldots, \varphi(\overline{x_m})(a)) \tag{3}$$

gegeben. Des weiteren ist $(\varphi^!)^*$ durch

$$g \mapsto g \circ \varphi^! = g(\varphi(\overline{x_1}), \ldots, \varphi(\overline{x_m})) = \varphi(g)$$

aufgrund von Bemerkung 1.3.22 gegeben. Es folgt, dass $(\varphi^!)^* = \varphi$.

Sei $f : \mathrm{V} \to \mathrm{W}$. Die Abbildung $f^* : K[\mathrm{W}] \to K[\mathrm{V}]$ ist durch $g \mapsto g \circ f$ gegeben und somit ist $(f^*)^! : \mathrm{V} \to \mathrm{W}$ definiert als

$$\begin{aligned} a &\mapsto (f^*(\overline{x_1})(a), \ldots, f^*(\overline{x_m})(a)) \\ &= ((\overline{x_1} \circ f^*)(a), \ldots, (\overline{x_m} \circ f^*)(a)) \\ &= (\overline{x_1}(f^*(a)), \ldots, \overline{x_m}(f^*(a))) \\ &= (f^*(a)_1, \ldots, f^*(a)_m) = f^*(a). \end{aligned}$$

Hier haben wir Bemerkung 1.3.6 benutzt. □

Lemma 1.3.25. *Seien* V, W, X *Varietäten.*

(i) Sind $\mathrm{V} \xrightarrow{f} \mathrm{W} \xrightarrow{g} X$ *polynomielle Abbildungen, so ist*

$$(g \circ f)^* = f^* \circ g^* \quad \textit{und} \quad (\mathsf{Id}_{\mathrm{V}})^* = \mathsf{Id}_{K[\mathrm{V}]}.$$

(ii) Sind $K[\mathrm{V}] \xrightarrow{\varphi} K[\mathrm{W}] \xrightarrow{\psi} K[X]$ *Homomorphismen von* K*-Algebren, so ist*

$$(\psi \circ \varphi)^! = \varphi^! \circ \psi^! \quad \textit{und} \quad (\mathsf{Id}_{K[\mathrm{V}]})^! = \mathsf{Id}_{\mathrm{V}}.$$

Beweis. Ist $\alpha \in K[X]$ eine polynomielle Funktion $X \to K$, so ist

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

Des Weiteren ist $(\mathsf{Id}_X)^*(\alpha) = \alpha \circ \mathsf{Id}_X = \alpha = \mathsf{Id}_{K[X]}(\alpha)$.

Der zweite Teil folgt direkt von Korollar 1.3.24 und dem ersten Teil. Wendet man nämlich $(-)^*$ auf beiden Seiten an, so erhält man

$$\left((\psi \circ \varphi)^!\right)^* = \psi \circ \varphi = ((\psi)^!)^* \circ ((\varphi)^!)^* = \left(\psi^! \circ \varphi^!\right)^*,$$

was uns

$$(\psi \circ \varphi)^! = \left(\left((\psi \circ \varphi)^!\right)^*\right)^! = \left(\left(\psi^! \circ \varphi^!\right)^*\right)^! = \psi^! \circ \varphi^!$$

liefert. Ebenso erhält man $(\mathsf{Id}_K[\mathrm{V}])^! = ((\mathsf{Id}_{\mathrm{V}})^*)^! = \mathsf{Id}_V$. □

Bemerkung 1.3.26. Wir erinnern uns an Bemerkung 1.2.25. Auch hier brauchte man die Rückrichtung eigentlich nicht zeigen.

In diesem letzten Schritt haben wir die sogenannte Funktorialität der Zuordnungen $(-)^*$ und $(-)^!$ bewiesen. Ohne näher darauf einzugehen sei gesagt, dass 1.3.25 und 1.3.24 gemeinsam eine kategorielle Äquivalenz zeigen.

Definition 1.3.27. *Eine polynomielle Abbildung* $f : \mathrm{V} \to \mathrm{W}$ *ist ein* Isomorphismus von Varietäten*, falls es eine polynomielle Abbildung* $g : \mathrm{W} \to \mathrm{V}$ *gibt, sodass* $f \circ g = \mathsf{Id}_{\mathrm{W}}$ *und* $g \circ f = \mathsf{Id}_{\mathrm{V}}$.

Korollar 1.3.28. *Eine polynomielle Abbildung* $f : \mathrm{V} \to \mathrm{W}$ *ist genau dann ein Isomorphismus von Varietäten, wenn* $f^* : K[\mathrm{W}] \to K[\mathrm{V}]$ *ein Isomorphismus von* K*-Algebren ist.*

Beweis. Die Hinrichtung ist direkte Konsequenz von Lemma 1.3.25. Ist etwa $f : \mathrm{V} \to \mathrm{W}$ ein Isomorphismus, so existiert ein $g : \mathrm{W} \to \mathrm{V}$, sodass $g \circ f = \mathsf{Id}_{\mathrm{V}}$ und $f \circ g = \mathsf{Id}_{\mathrm{W}}$. Es folgt, dass $f^* \circ g^* = (f \circ g)^* = \mathsf{Id}_{\mathrm{W}}^* = \mathsf{Id}_{K[\mathrm{W}]}$ und $g^* \circ f^* = (g \circ f)^* = \mathsf{Id}_{\mathrm{V}}^* = \mathsf{Id}_{K[\mathrm{V}]}$. Damit ist f^* ein Isomorphismus von K-Algebren.

Für die Rückrichtung benötigen wir zusätzlich Korollar 1.3.24. Sei nämlich $f^* : K[\mathrm{V}] \to K[\mathrm{W}]$ ein Isomorphismus von K-Algebren. Es existiert also ein $\psi : K[\mathrm{W}] \to K[\mathrm{V}]$, sodass $f^* \circ \psi = \mathsf{Id}_{K[\mathrm{W}]}$ und $\psi \circ f^* = \mathsf{Id}_{K[\mathrm{V}]}$. Nun sagt uns Korollar 1.3.24, das ψ von der Form g^* für eine polynomielle Abbildung $g : \mathrm{W} \to \mathrm{V}$ ist. Wir erhalten daher

$$g \circ f = (g^*)^! \circ (f^*)^! = (f^* \circ g^*)^! = (f^* \circ \psi)^! = (\mathsf{Id}_{K[\mathrm{W}]})^! = \mathsf{Id}_{\mathrm{W}}$$

und ebenso $f \circ g = \mathsf{Id}_{\mathrm{V}}$, womit f ein Isomorphismus von Varietäten ist. □

Bemerkung 1.3.29. Die Hinrichtung des obigen Korollars 1.3.28, dass also Isomorphismen auf Isomorphismen abgebildet werden, folgte direkt aus der Funktorialität. Eine kategorielle Äquivalenz war dafür nicht notwendig. Man vergleiche dies mit der Aussage, dass Homomorphismen von Gruppen oder Ringen, Einheiten immer auf Einheiten abbilden. Die Umkehrung, dass ein Element eine Einheit ist, wenn sein Bild unter einem Homomorphismus es ist, ist im Allgemeinen falsch und benötigt, dass der Homomorphismus ein Isomorphismus ist.

Wir können nun also Varietäten durch Koordinatenringe studieren. Im Gegensatz zu den geometrischen Varietäten, sind die Koordinatenringe algebraische Objekte, was uns erlaubt viele algebraische Methoden zum Einsatz zu bringen.

Beispiel 1.3.30. Betrachte die Parabel $f(x,y) = y - x^2 \in K[x,y]$. Es ist $y - x^2$ irreduzibel, insbesondere ist $(y-x^2)$ radikal, womit $K[\mathrm{V}(f)] = K[x,y]/(y-x^2)$ gilt. Wir erhalten einen wohldefinierten Morphismus $\alpha : K[\mathrm{V}(f)] \to K[t]$ von K-Algebren durch die Zuordnung $\alpha(x) := t$ und $\alpha(y) := t^2$, welcher bijektiv mit Umkehrung $t \mapsto x$ ist (es gilt in $K[x,y]/(y-x^2)$ die Gleichung $y = x^2$, die Variable y ist daher sozusagen überflüssig und kann "weggeworfen" werden). Die Koordinatenringe $K[\mathrm{V}(f)]$ und $K[t] = K[\mathbb{A}^1]$ sind also vermöge α isomorph. Wir erhalten daher einen Isomorphismus von Varietäten

$$\alpha^! : \mathbb{A}^1 \longrightarrow \mathrm{V}(f), \quad a \longmapsto \big(\alpha(x)(a), \alpha(y)(a)\big) = (a, a^2)$$

deren Umkehrungabbildung genau durch Einschränkung der Projektion $\mathbb{A}^2 \to \mathbb{A}^1$ auf die erste Koordinate gegeben ist, also $(a,b) \mapsto a$.

Natürlich wäre es in diesem Fall auch nicht besonders schwer gewesen obigen Isomorphismus von Varietäten direkt zu sehen, das Vorgehen über die Koordinatenringe ist aber vielleicht etwas "kanonischer".

Eine bijektive polynomielle Abbildung $\mathbb{A}^n \to \mathrm{V}$ aus einem affinen Raum in eine Varietät hinein, nennt man auch ein *Parametrisierung* der Varietät. Etwa war die Abbildung $a \mapsto (a, a^2)$ in obigem Beispiel eine Parametrisierung der Parabel durch die affine Gerade. Beachte aber, dass eine solche Parametrisierung *kein* Isomorphismus sein muss! Dies werden wir im folgenden Abschnitt besprechen.

Die Unzulänglichkeit von Bijektionen In Definition 1.3.27 hatten wir einen Isomorphismus von Varietäten als einen invertierbaren Morphismus von Varietäten definiert (wie in der Kategorientheorie üblich). Natürlich ist ein Isomorphismus insbesondere eine Bijektion, in der Algebra gilt aber oft schon die Umkehrung. Homomorphismen von Gruppen, Ringen, Moduln und von allen anderen "algebraischen Strukturen" sind schon dann Isomorphismen, wenn sie bijektiv sind, vergleiche auch die Bemerkung 1.2.25. Man könnte nun, vor allem in Anbetracht der Resultate 1.3.24 und 1.3.25, denken, dass dieses Prinzip auch für Varietäten gilt. Dies ist aber nicht der Fall, Varietäten sind *keine* algebraische Struktur! Folgendes Beispiel zeigt eine bijektive polynomielle Abbildung, welche kein Isomorphismus ist.

Beispiel 1.3.31. Betrachte die Neilsche Parabel $f(x,y) = y^2 - x^3 \in K[x,y]$. Wir haben eine polynomielle Abbildung

$$\begin{aligned} \varphi : \mathbb{A}^1 &\longrightarrow \mathrm{V}(f) \\ t &\longmapsto (t^2, t^3). \end{aligned}$$

Eine Umkehrungabbildung ist gegeben durch die Zuordnung

$$\begin{aligned} \psi : \mathrm{V}(f) &\longrightarrow \mathbb{A}^1 \\ (x,y) &\longmapsto \begin{cases} \frac{y}{x}, & \text{falls } (x,y) \neq (0,0) \\ 0, & \text{falls } (x,y) = (0,0) \end{cases}. \end{aligned}$$

Dies zeigt zwar, dass φ eine Parametrisierung der Neilschen Parabel ist, jedoch ist φ kein Isomorphismus von Varietäten. Die eindeutig bestimmte Umkehrabbildung ψ ist nämlich *nicht* polynomiell.

Dass φ kein Isomorphismus sein kann, lässt sich auch an dem zu φ assoziierten Homomorphismus von K-Algebren erkennen:

$$\begin{aligned} \varphi^* : K[\mathrm{V}] &\longrightarrow K[t] \\ x &\longmapsto t^2 \\ y &\longmapsto t^3 \end{aligned}$$

Offenbar ist φ^* nicht surjektiv, etwa wir t nicht "getroffen", insbesondere ist φ^* kein Isomorphismus und damit auch φ nicht, nach Korollar 1.3.28.

Beachte, dass dies noch nicht zeigt, dass $\mathbb{A}^1$ und $\mathrm{V}(f)$ nicht isomorph sein *können*. Um dies einzusehen, betrachtet am besten wieder die assoziierten Koordinatenringe. Intuitiv ist klar, dass sich $K[\mathrm{V}(f)] = K[x,y]/y^2 - x^3$ nicht auf eine Variable reduzieren lässt. Nämlich lässt sich zwar y^2 im Sinne von x ausdrücken, y aber nicht. Dies explizit zu beweisen ist ein kleines bisschen schwerer. In solchen Fällen ist es eine der besten Methoden, eine Invariante zu finden, der die beiden K-Algebren unterscheidet. Dies ist Hausaufgabe der letzten Woche.

Bemerkung 1.3.32. Nützliche Invarianten sind etwa: Dimension (Krull-, als K-Vektorraum, als $K[x]$-Modul (oder $K[x,y]$-Modul etc.)), Einheiten, invariante Eigenschaften (Hauptidealbereich, Faktorring, Integritätsbereich, etc.) und noch vieles mehr. Im Grunde kann jede Eigenschaft, welche unter Isomorphien erhalten wird (was nichts anderes bedeutet als zu sagen, dass es eine "Eigenschaft von Ringen" ist) dazu dienen. Zum Beispiel die Ordnung von Elementen oder Untergruppen sein. Quotientenkörper und andere Lokalisierungen (z. B., Halme, was wir in kürze kennenlernen werden) sind ebenfalls Invarianten.

Später werden wir auch die Picardgruppe kennenlernen, welche ein spezieller Fall von Kohomologie ist. Kohomologiegruppen sind eine gewaltige Klasse von Invarianten, welches wir aber nicht weiter studieren werden. Mehr dazu kann man in Vorlesungen zu Schematheorie lernen oder, allgemeiner, zu algebraischer Topologie oder homologischer Algebra.

1.4 Komplemente von affinen Varietäten und Lokalisierungen

Im letzten Abschnitt haben wir abgeschlossene Mengen studiert. Nun wollen wir deren Komplemente, also die offenen Mengen untersuchen. Rein geometrisch scheinen diese weniger spannend zu sein, da wir ja das Komplement von dem studieren, was wir "interessant finden". In der modernen algebraischen Geometrie jedoch, sind diese Mengen "wichtiger", da man Garben auf offenen Mengen definiert.

Wir werden uns auf Komplemente von Varietäten der Form $\mathrm{V}(f)$ konzentrieren, welche von Hauptidealen (f) ausgeschnitten werden. Dazu definieren wir

$$\mathrm{D}(f) \coloneqq \mathbb{A}^n \setminus \mathrm{V}(f).$$

So wie wir den Koordinatenring $K[\mathrm{V}]$ zu einer Varietät V assoziiert haben, wollen wir nun auch einen Ring zu $D(f)$ assoziieren. Der naive Ansatz wäre, sich wieder Abbildungen $D(f) \to K$ anzusehen, welche durch Einschränken von Polynomfunktionen $\mathbb{A}^n \to K$ entstehen. Das Problem ist, dass diese Funktionen für nichtleere Mengen immer die selben Ringe definieren. Denn nichtleere offene Mengen des $\mathbb{A}^n$ liegen bezüglich der Zariski-Topologie immer dicht! Im Detail haben wir folgende Aussage:

Lemma 1.4.1. *Seien $f, g, h \in K[x_1, \dots, x_n]$. Fassen wir g und h als Polynomfunktionen $\mathbb{A}^n \to K$ auf, so impliziert die Gleichung $g_{|_{D(f)}} = h_{|_{D(f)}}$ schon $g = h$.*

Beweis. Hausaufgabe. □

Eine analoge Aussage zu Korollar 1.3.24 zu erhalten scheint nun unmöglich, zumindest, wenn wir versuchen Polynomfunktionen wie in $K[\mathrm{V}]$ zu betrachten. Wenn wir aber statt zu "kleineren" Quotientenringen zu "größeren" Lokalisierungen übergehen, können wir einen zu Korollar 1.3.24 ähnlichen Satz beweisen.

1.4.1 Rationale Abbildungen

Im Folgenden sei stets $f \in K[x_1, \dots, x_n]$ ein festes Polynom und $D(f) = \mathbb{A}^n \setminus V(f)$ die offene Menge der Punkte an denen f nicht verschwindet. Wir nehmen an, dass $f \neq 0$, sodass $D(f) \neq \varnothing$.

Definition 1.4.2. *Eine* rationale Funktion *über $\mathbb{A}^n$ ist ein Element des Quotientenkörpers $K(\mathbb{A}^n) \coloneqq \mathsf{Q}(K[x_1, \dots, x_n])$ des Koordinatenrings von $\mathbb{A}^n$.*

Eine rationale Funktion über $\mathbb{A}^n$ ist also von der Form $\frac{g}{h}$ für zwei Polynome $g, h \in K[x_1, \dots, x_n]$, wobei h nicht konstant Null sein darf. Das Polynom h darf aber sehr wohl Nullstellen besitzen, was nun aber zur Folge hat, dass die Zuordnung $a \mapsto \frac{g(a)}{h(a)}$ keine Funktion auf ganz $\mathbb{A}^n$ definiert, sondern nur auf dem Teil, wo $h(a) \neq 0$, also auf $D(h)$. Diese Beobachtung motiviert die folgende Definition.

$\Gamma(D(f))$ - Ring der Rationalen Abbildungen

Definition 1.4.3. *Eine Abbildung $\gamma : D(f) \to K$ heißt* rational *, falls es eine rationale Funktion $\frac{g}{h} \in K(\mathbb{A}^n)$ gibt, so dass für alle $a \in D(f)$, $\gamma(a) = \frac{g(a)}{h(a)}$ und $h(a) \neq 0$. Den Ring der rationalen Abbildungen auf $D(f)$ bezeichnen wir mit $\Gamma(D(f))$.*

Die Tatsache, dass dies wirklich ein Ring ist (sogar eine K-Algebra) ist einfach zu überprüfen. Addition und Multiplikation sind dabei komponentenweise definiert.

Lemma 1.4.4. *Die K-Algebra der rationalen Funktionen $\Gamma(D(f))$ ist isomorph zu folgender Unteralgebra von $K(\mathbb{A}^n)$:*

$$\left\{ \frac{g}{h} \,\middle|\, \forall a \in D(f) : h(a) \neq 0 \right\}.$$

Beweis. Per Definition gibt es für $\gamma : D(f) \to K$ ein $\frac{g}{h}$ von der gewünschten Form und wir bilden dies genau darauf ab. Für die Wohldefiniertheit seien $\frac{g}{h}$ und $\frac{g'}{h'}$ zwei solche Elemente, welche dieselbe rationale Abbildung $\gamma : D(f) \to K$ definieren. Mit anderen Worten, für alle $a \in D(f)$ gilt $\frac{g(a)}{h(a)} = \frac{g'(a)}{h'(a)}$. Dies ist äquivalent dazu, dass $g(a)h'(a) = g'(a)h(a)$ für alle $a \in D(f)$. Da $f \neq 0$ (unsere Generalvoraussetzung) besagt Lemma 1.4.1, dass $gh' = g'h$ und damit $\frac{g}{h} \sim \frac{g'}{h'}$.

Surjektivität folgt direkt aus der Definition rationaler Abbildungen. Für die Injektivität, seien $\gamma, \phi : D(f) \to K$ zwei Abbildungen, so dass diese äquivalente Elemente $\frac{g}{h}$ und $\frac{g'}{h'}$ definieren. Daher $gh' = g'h$. Da diese eine Gleichung von Polynomen ist, ist auch deren Auswertung $g(a)h'(a) = g'(a)h(a)$ für jeden $a \in A^n$ gleich, spezifisch auch für $a \in D(f)$ und daher waren also $\gamma(a) = \phi(a)$ für alle $a \in D(f)$ und somit dieselbe rationale Abbildung.

Dass dieser Isomorphismus die K-Algebrenstruktur erhält, ist einfach zu überprüfen. □

Bemerkung 1.4.5. Damit es nicht zu Verwirrung führt, erinnern wir uns dass die "Brüche", sprich $\frac{g}{h}$ Äquivalenzklassen sind. Sprich, zu sagen, dass $h(a) \neq 0$ bedeutet, dass für irgendeinen Repräsentanten des Bruches, der Nenner ungleich Null ist. In Formeln ausgedrückt bedeutet dies, dass es eine Äquivalenz $\frac{g}{h} \sim \frac{g'}{h'}$ gibt, mit $h'(a) \neq 0$ für alle $a \in D(f)$

Von nun an werden wir diese zwei Mengen miteinander (durch die gegebene Isomorphie) identifizieren. Wir haben folgenden wichtigen Satz (man erinnere sich, dass $f \neq 0$ war):

Satz 1.4.6. *Für alle $f \in K[x_1, \ldots, x_n]$ gilt*

$$\Gamma(D(f)) \simeq K[x_1, \ldots, x_n]_f.$$

Beweis. Zur Erinnerung, mit $K[x_1, \ldots, x_n]_f$ meinen wir die Lokalisierung von $K[x_1, \ldots, x_n]$

nach $\langle f\rangle = \{1, f, f^2, \ldots\}$. Es gilt

$$\begin{aligned}
\Gamma(D(f)) &= \left\{ \frac{g}{h} \,\middle|\, \forall a \in D(f) : h(a) \neq 0 \right\} \\
&= \left\{ \frac{g}{h} \,\middle|\, h(a) = 0 \Rightarrow a \in \mathrm{V}(f) \right\} \\
&= \left\{ \frac{g}{h} \,\middle|\, h(a) = 0 \Rightarrow f(a) = 0 \right\} \\
\text{Proposition 1.2.44} &= \left\{ \frac{g}{h} \,\middle|\, \exists\ n \geq 1, f' \in K[x_1, \ldots, x_n],\ \text{sodass } f^n = hf'. \right\}
\end{aligned}$$

Es ist nun klar, dass dies isomorph zu

$$K[x_1, \ldots, x_n]_f \simeq \left\{ \frac{g}{f^n} \mid n \in \mathbb{N} \right\}$$

ist. Tatsächlich, sei $\frac{g}{h}$ in der linken Seite (wie in der letzten Zeile). Da $f(a) \neq 0$ für $a \in D(f)$ (Definition von $D(f)$ muss $f'(a) \neq 0$ für alle $a \in D(f)$ sein und somit können wir

$$\frac{g}{h} \sim \frac{gf'}{hf'} = \frac{gf'}{f^n}$$

schreiben.

Auf der anderen Seite kann $\frac{a(x)}{f^n(x)} \in K[x_1, \ldots, x_n]_f$ direkt als Element von $\Gamma(D(f))$ aufgefasst werden, da $f^n(a) \neq 0$ für alle $a \in \mathrm{D}(f)$ (Integritätsbereich).

Das hin-und-zurück Identitäten sind und alle Abbildungen Ringhomomorphismen kann ohne Weiteres überprüft werden. □

Korollar 1.4.7. *Es gilt* $\Gamma(D(1)) = K[\mathbb{A}^n] = K[x_1, \ldots, x_n]$.

Bemerkung 1.4.8. Wir erwähnen folgendes ohne Beweis oder Anwendung. Seien $U_1, U_2 \subseteq \mathbb{A}^n$ offen und $U_{12} := U_1 \cap U_2$ sowie $W := U_1 \cup U_2$. Für alle $f \in K(U_1)$, $g \in K(U_2)$ welche auf U_{12} übereinstimmen (also $f_{|_{U_{12}}} = g_{|_{U_{12}}}$), gibt es genau einen $h \in K(W)$ (in anderen Worten, so ein h existiert und es ist eindeutig), mit $h_{|_{U_1}} = f$ und $h_{|_{U_2}} = g$. Dies wird die *Verklebungseigenschaft* bzw. *Garbeneigenschaft* genannt und ist sehr wichtig in moderner algebraischer Geometrie. Lemma 1.4.1 ist dann ein Spezialfall, wenn $U_1 = \mathbb{A}^n$ und $U_2 = U$.

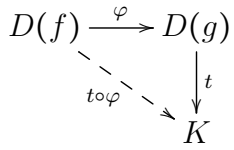
Dies gilt sogar für allgemeine kommutative Ringe, nicht nur algebraisch abgeschlossene Körper. Jedoch muss man dann $\mathsf{Spec}(R)$ anstatt $\mathbb{A}^n_K$ nehmen.

$\mathsf{Hom}(D(f), D(g))$ vs $\mathsf{Hom}(\Gamma(D(g)), \Gamma(D(f)))$

Definition 1.4.9. *Sei* $f \in K[x_1, \ldots, x_n]$ *und* $g \in K[y_1, \ldots, y_m]$ *. Eine Abbildung* $\varphi : \mathrm{D}(f) \to D(g)$ *heißt* rational *wenn es* m *rationale Abbildungen* $\varphi_1, \ldots, \varphi_m : D(f) \to K$ *gibt, sodass*

$$\varphi(a) = (\varphi_1(a), \ldots, \varphi_m(a)).$$

Ist $\varphi : D(f) \to D(g)$ eine rationale Abbildung, so können wir für jede rationale Abbildung $t : D(g) \to K$ die Präkomposition



betrachten. Es wird $t \in \Gamma(D(g))$ repräsentiert von einer rationalen Funktion $\frac{r}{s} \in K(\mathbb{A}^n)$, wobei $s(b) \neq 0$ für alle $b \in D(g)$. Da $\varphi(D(f)) \subseteq D(g)$, ist $(s \circ \varphi)(a) \neq 0$ für alle $a \in D(f)$. Damit ist $(t \circ \varphi)(a) = \frac{(r \circ \varphi)(a)}{(s \circ \varphi)(a)}$, also ist $t \circ \varphi$ eine rationale Abbildung $D(f) \to K$, dargestellt durch die rationale Funktion $\frac{r \circ \varphi}{s \circ \varphi}$. Dies beweist, dass die Präkomposition in der folgenden Proposition wohldefiniert ist.

Proposition 1.4.10. *Sei $\varphi : D(f) \to D(g)$ eine rationale Abbildung. Dann definiert*

$$\varphi^* : \Gamma(D(g)) \to \Gamma(D(f)),$$

gegeben durch

$$\frac{r}{s} \mapsto \frac{r \circ \varphi}{s \circ \varphi},$$

einen Morphismus von K-Algebren.

Beweis. Es gilt:

$$\varphi^*\left(\frac{r}{s}\frac{r'}{s'}\right) = \varphi^*\left(\frac{rr'}{ss'}\right) = \frac{rr' \circ \varphi}{ss' \circ \varphi} = \frac{(r \circ \varphi)(r' \circ \varphi)}{(s \circ \varphi)(s' \circ \varphi)} = \varphi^*\left(\frac{r}{s}\right)\varphi^*\left(\frac{r'}{s'}\right).$$

Ebenso gilt:

$$\varphi^*\left(\frac{r}{s} + \frac{r'}{s'}\right) = \varphi^*\left(\frac{rs' + rs'}{ss'}\right) = \frac{(rs' + r's) \circ \varphi}{ss' \circ \varphi} = \frac{(ss' \circ \varphi) + (r's \circ \varphi)}{(s \circ \varphi)(s' \circ \varphi)}$$

und

$$\varphi^*\left(\frac{r}{s}\right) + \varphi^*\left(\frac{r'}{s'}\right) = \frac{r \circ \varphi}{s \circ \varphi} + \frac{r' \circ \varphi}{s' \circ \varphi} = \frac{(r \circ \varphi)(s' \circ \varphi) + (r' \circ \varphi)(s \circ \varphi)}{(s \circ \varphi)(s' \circ \varphi)} = \frac{(rs' \circ \varphi) + (r's \circ \varphi)}{(s \circ \varphi)(s' \circ \varphi)}.$$

Die Gleichungen $rr' \circ \varphi = (r \circ \varphi)(r' \circ \varphi)$ und $(r + r') \circ \varphi = (r \circ \varphi)(r' \circ \varphi)$ stimmen allgemein für Kompositionen mit punktweise definierter Verknüpfungen, rein von der Definition. Wenn nun $k \in K$ als eine konstante Abbildung $k : D(g) \to K$ aufgefasst, dann ist $k \circ \varphi : D(f) \to K$ natürlich auf die konstante Abbildung, die jedes Element von $D(f)$ auf k abbildet. Insgesamt ist φ^* daher ein Morphismus von K-Algebren. □

Proposition 1.4.11. *Seien $f \in K[x_1, \ldots, x_n]$ und $g \in K[y_1, \ldots, y_m]$. Für jeden Morphismus*

$$\alpha : \Gamma(D(g)) \to \Gamma(D(f))$$

von K-Algebren gibt es eine eindeutige rationale Abbildung

$$\varphi : D(f) \to D(g),$$

so dass $\varphi^* = \alpha$.

Beweis. Dies ist analog zu Proposition 1.3.23. Man nehme die Variablen $y_1, \ldots, y_m \in K[y_1, \ldots, y_m]$ und betrachte deren Bilder $\frac{y_1}{1}, \ldots, \frac{y_m}{1}$ unter der natürlichen (Lokalisierungs-) Einbettung

$$K[y_1, \ldots, y_m] \to K[y_1, \ldots, y_m]_g.$$

Wir definieren

$$\varphi := \left(\alpha\left(\frac{y_1}{1}\right), \ldots, \alpha\left(\frac{y_m}{1}\right)\right).$$

Daher, für einen $a = (a_1, \ldots, a_n) \in D(f)$ setzen wir $\varphi(a) = \left(\alpha\left(\frac{y_1}{1}\right)(a), \ldots, \alpha\left(\frac{y_m}{1}\right)(a)\right)$. Dies macht Sinn, da $\alpha\left(\frac{y_1}{1}\right) \in \Gamma(D(f))$ und daher, eine Abbildung in n Variablen ist. Als nächstes müssen wir zeigen, dass wir in $D(g)$ landen. Daher, dass aus $f(a) \neq 0$ folgt $g(\varphi(a)) \neq 0$. Man bemerke aber, dass $g \in K[x_1, \ldots, x_n]$ ein Element ist, welches mit den Erzeugern $y_1, \ldots, y_m$ ausgerückt werden kann. Es gilt also

$$g(\varphi(a)) = g\left(\alpha\left(\frac{y_1}{1}\right)(a), \ldots, \alpha\left(\frac{y_m}{1}\right)(a)\right) = \alpha(g)(a),$$

wobei die letzte Gleichung Bemerkung 1.3.22 ist. Da aber g eine Einheit in $K[y_1, \ldots, y_m]_g$ ist, muss dessen Bild unter α auch eine Einheit sein, also $\alpha(g) \in K[x_1, \ldots, x_n]_g^*$. Es gibt also ein v, so dass $\alpha(g)v = 1$. Also ist $\alpha(g)(a)v(a) = 1(a) = 1$, was besagt, dass $\alpha(g)(a)$ eine Einheit ist. Daher ist es nicht Null, wie gewollt.

Eindeutigkeit folgt von der Konstruktion, da α von dessen Werten auf den Erzeugern definiert wird. □

Korollar 1.4.12. *Für $f \in K[x_1, \ldots, x_n]$, $g \in K[y_1, \ldots, y_m]$ gibt es eine bijektive Zuordnung*

$$\{\text{Rationale Abb. zw. } D(F) \text{ und } D(g)\} \xleftrightarrow{\simeq} \{K\text{-Alg. Hom. zw. } \Gamma(D(g)) \text{ und } \Gamma(D(f))\}.$$

Das hin und zurück werden wir wieder mit $(-)^*$ und $(-)^!$ bezeichnen. Sprich, für $\alpha : D(f) : D(g)$ bezeichnen wir den induzierten K-Algebrahomomorphismus als $\alpha^* : \Gamma(D(g)) \to \Gamma(D(f))$ und umgekehrt wird zu $\varphi : \Gamma(D(g)) \to \Gamma(D(f))$ die stetige Abbildung $\varphi^! : D(f) \to D(g)$ zugeordnet.

Der Beweis geht analog zu Proposition 1.3.24. Ebenso haben wir die Gegenstücke zu Lemma 1.3.25 und Korollar 1.3.28, was wir wie folgt formulieren:

Proposition 1.4.13. *Die Zuordnungen $(-)^*$ und $(-)^!$ respektieren Kompositionen und Identitäten und bilden rationale Abbildungen, welche sogar Homöomorphismen von offenen Mengen $D(f)$ sind, genau auf Isomorphismen von K-Algebren ab.*

Beweise für beide Aussagen sind Hausaufgaben.

1.5 Punkte, Halme und lokale Ringe

1.5.1 Lokalisierung an Prim-/Maximalidealen

Wir haben schon einige Klassen von Lokalisierungen eingeführt. Es gibt aber noch einen weiteren wichtigen Typ den wir besprechen wollen. Zuerst ein kleines Lemma, welches sich mit Abbildungen beschäftigt. Es wird erst später Anwendung haben, wird aber hier erwähnt, um den ringtheoretischen Teil über Lokalisierungen abschließen zu können.

Homomorphismen und die Lokalisierung Beachte, dass sowohl Bild als auch Urbild einer multiplikativen Teilmenge unter einem Ringhomomorphismus wieder eine multiplikative Teilmenge ist. Wir erhalten induzierte Abbildungen zwischen den entsprechenden Lokalisierungen, wie folgendes Lemma zeigt.

Lemma 1.5.1. *Sei $g : R \to S$ ein Ringhomomorphismus.*

(i) Sei $A \subseteq R$ eine multiplikative Teilmenge. Es existiert ein kanonischer Ringhomomorphismus

$$g_A : A^{-1}R \to g(A)^{-1}S.$$

Es ist $(\mathsf{Id}_R)_A = \mathsf{Id}_{A^{-1}R}$ und für jeden weiteren Ringhomomorphismus $h : S \to T$ gilt $(h \circ g)_A = h_A \circ f_A$.

(ii) Sei $B \subseteq S$ eine multiplikative Teilmenge. Es existiert ein kanonischer Ringhomomorphismus

$$g_B : \left(g^{-1}(B)\right)^{-1} R \to B^{-1}S.$$

Es ist $(\mathsf{Id}_S)_B = \mathsf{Id}_{B^{-1}R}$ und für jeden weiteren Ringhomomorphismus $f : Q \to R$ gilt $(g \circ f)_B = g_B \circ f_B$.

Zur Vereinfachung der Notation schreiben wir oft auch einfach $A^{-1}S$ statt $g(A)^{-1}S$ beziehungsweise $B^{-1}R$ statt $(g^{-1}(B))^{-1} R$.

Beweis. Wir behandeln nur den zweiten Fall, der erste folgt ganz analog. Wir definieren die Abbildung f_B durch die Zuordnung $\frac{r}{b} \mapsto \frac{f(r)}{f(b)}$ für $r \in R$ und $b \in f^{-1}(B)$. Beachte zum Einen, dass $f(b) \in B$, der Ausdruck $\frac{f(r)}{f(b)}$ also Sinn ergibt. Zum anderen folgt aus $\frac{r}{b} = \frac{r'}{b'}$ die Existenz von einem $a \in f^{-1}(B)$ mit $arb' = ar'b$. Daher ist $f(a)f(r)f(b') = f(a)f(r')f(b)$ und da $f(a) \in S$, folgt $\frac{f(r)}{f(b)} = \frac{f(r')}{f(b')}$. Die Abbildung ist somit wohldefiniert.

Offenbar ist f_B verträglich mit der Multiplikation. Für die Addition gilt

$$\frac{r}{b} + \frac{r'}{b'} = \frac{rb' + r'b}{bb'} \mapsto \frac{f(rb' + r'b)}{f(bb')} = \frac{f(r)f(b') + f(r')f(b)}{f(b)f(b')} = \frac{f(r)}{f(b)} + \frac{f(r')}{f(b')},$$

wie gewünscht. Schließlich gilt für die Komposition

$$(g_S \circ f_S)\left(\frac{b}{s}\right) = g_S\left(\frac{f(b)}{g(s)}\right) = \frac{(g \circ f)(b)}{(g \circ f)(s)} = (g \circ f)_S\left(\frac{b}{s}\right). \qquad \square$$

Lokale Ringe

Definition 1.5.2. *Ein Ring heißt* lokal*, falls er genau ein maximales Ideal hat.*

Lemma 1.5.3. *Ein Ring R ist genau dann lokal, wenn die Nichteinheiten $R \setminus R^*$ ein Ideal in R bilden.*

Beweis. Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m} \subseteq R$. Sind $a, b \in R \setminus R^*$, so ist $(a) \neq (1)$ und $(b) \neq (1)$. Da jedes echte Ideal in einem maximalen Ideal enthalten ist (Zornsches Lemma), folgt $(a), (b) \subseteq \mathfrak{m}$, also $a, b \in \mathfrak{m}$. Dann ist auch $a + b \in \mathfrak{m} \neq (1)$, also ist $a + b$ keine Einheit. Ist nun außerdem $c \in R$, so muss $ac \notin R^*$ sein, wäre nämlich $x \in R$ invers zu ac, so wäre cx invers zu $a \notin R^*$, ein Widerspruch. Schließlich ist Null keine Einheit, weil ansonsten R der Nullring wäre und kein Ideal $\mathfrak{m}$ ungleich (1) existieren würde.

Sei nun umgekehrt $R \setminus R^*$ ein Ideal. Ist $I \neq (1)$ ein beliebiges echtes Ideal, so kann I keine Einheiten $u \in R$ enthalten, andernfalls wäre $1 = u^{-1}u \in I$, ein Widerspruch. Insbesondere gilt $I \subseteq R \setminus R^*$. Ist nun $I = \mathfrak{m}$ ein beliebiges maximales Ideal, so folgt aus dieser Teilmengenbeziehung bereits $\mathfrak{m} = R \setminus R^*$, denn das Ideal $R \setminus R^*$ enthält sicherlich nicht 1. Andererseits ist R nicht der Nullring, andernfalls wäre $R \setminus R^*$ kein Ideal (0 ist invertierbar im Nullring), mindestens ein maximales Ideal muss R also besitzen (Zornsches Lemma). Damit haben wir gezeigt, dass R genau ein maximales Ideal besitzt, also lokal ist. □

Korollar 1.5.4. *Sei R ein lokaler Ring und sei $\mathfrak{m}$ sein eindeutiges maximales Ideal. Dann gilt $R \setminus \mathfrak{m} = R^*$ oder äquivalenterweise $\mathfrak{m} = R \setminus R^*$.*

Beweis. Laut Lemma 1.5.3 formt $R \setminus R^*$ ein Ideal. Es ist maximal, denn jedes Ideal J mit $R \setminus R^* \subsetneq J \subseteq R$ enthält bereits eine Einheit u, weshalb schon $J = R$ gilt. Da R lokal ist muss daher $\mathfrak{m} = R \setminus R^*$ sein. Übergang zum Komplement liefert $R \setminus \mathfrak{m} = R^*$. □

Von ganz besonderer Bedeutung ist die Lokalisierung mit multiplikativen Teilmengen der folgenden Art:

Lokalisierung an Primidealen

Lemma 1.5.5. *Sei $\mathfrak{p} \subseteq R$ ein Primideal und $S_\mathfrak{p} := R \setminus \mathfrak{p}$ sein Komplement. Dann ist $S_\mathfrak{p} \subseteq R$ eine multiplikative Teilmenge von R.*

Beweis. Dies ist quasi die Definition eines Primideals. Seien $a, b \in S_\mathfrak{p}$. Wenn ab nicht in $S_\mathfrak{p}$ wäre, dann würde $ab \in \mathfrak{p}$ und gleichzeitig $a \notin \mathfrak{p}$ und $b \notin \mathfrak{p}$ gelten, was ein Widerspruch ist. □

Definition 1.5.6. *Sei $\mathfrak{p} \subseteq R$ ein Primideal. Die Lokalisierung*

$$R_\mathfrak{p} := S_\mathfrak{p}^{-1} R$$

nennen wir die Lokalisierung von R an $\mathfrak{p}$ *. Ebenso schreiben wir*

$$I_\mathfrak{p} := I R_\mathfrak{p} = \left\{ \frac{x}{a} \mid x \in I, a \in S_\mathfrak{p} \right\}$$

für die Lokalisierung eines Ideals I von R an $\mathfrak{p}$.

Die Lokalisierung eines Ideals I an $\mathfrak{p}$ kann auch als das vom Bild $\gamma(I)$ unter der kanonischen Abbildung $\gamma : R \to S^{-1}R$ erzeugte Ideal aufgefasst werden. Dies ist Gegenstand des folgenden Lemmas, welches analog auch für allgemeine Lokalisierungen gilt.

Lemma 1.5.7. *Die Teilmenge $I_\mathfrak{p} \subseteq R_\mathfrak{p}$ ist ein Ideal von $R_\mathfrak{p}$.*

Beweis. Es gilt $0 \in I$ und $1 \in S_\mathfrak{p}$, daher $\frac{0}{1} \in I_\mathfrak{p}$. Seien $\frac{x}{a}, \frac{y}{b} \in I_\mathfrak{p}$. Dann ist

$$\frac{x}{a} + \frac{y}{b} = \frac{ay + bx}{ab} \in I_\mathfrak{p},$$

da $ay + bx \in I$ $(x, y \in I)$ und aus $a, b \notin \mathfrak{p}$, $ab \notin \mathfrak{p}$ folgt. Sei nun $\frac{r}{c} \in R_\mathfrak{p}$, daher $r \in R$ und $c \notin \mathfrak{p}$. Dann ist auch

$$\frac{x}{a}\frac{r}{c} = \frac{xr}{ac} \in \mathrm{I}_\mathfrak{p},$$

denn wie schon gesagt, aus $a, c \notin \mathfrak{p}$ folgt $ac \notin \mathfrak{p}$ und $xr \in I$. □

Bemerkung 1.5.8. Die Bezeichnung "Lokalisierung *an* einem Primideal" kommt von folgender (algebraisch) geometrischen Intuition: Wir hatten bereits erwähnt, dass in der modernen algebraische Geometrie (in der Schematheorie) statt der Menge der maximalen Ideale eines Ringes R (wie es der Hilbertsche Nullstellensatz vermuten ließe) die Menge $\mathsf{Spec}(R)$ der Primideale studiert wird. Die "Punkte" des Raumes $\mathsf{Spec}(R)$ entsprechen also genau den Primidealen $\mathfrak{p}$ von R. Ein Element $f \in R$ stellt man sich dann wie eine "Funktion" auf $\mathsf{Spec}(R)$ vor, die genau dann bei einem Punkt $\mathfrak{p}$ verschwindet, wenn $f \in p$ (wenn $R = K[\mathbb{A}^n]$ und $\mathfrak{p} = \mathfrak{m}_a$ das maximale Ideal eines Punktes a, so entspricht dies gerade der gewohnten Definition). In der Lokalisierung $R_\mathfrak{p}$ sind dann alle Funktionen die an $\mathfrak{p}$ nicht verschwinden bereits invertierbar, daher können wir uns $R_\mathfrak{p}$ als den Koordinatenring einer "kleinen offenen Umgebung" um $\mathfrak{p}$ vorstellen. Mit anderen Worten befinden wir uns "lokal am Punkt $\mathfrak{p}$", wenn wir in der Lokalisierung $R_\mathfrak{p}$ von R an einem Primideal $\mathfrak{p}$ arbeiten. Vergleiche auch die Diskussion über Halme später in diesem Abschnitt.

Die Ideale von Lokalisierungen

Proposition 1.5.9. *Sei $\mathfrak{p} \subseteq R$ ein Primideal. Es gibt eine ordnungserhaltende Bijektion zwischen den Primidealen von $R_\mathfrak{p}$ und den Primidealen von R unter $\mathfrak{p}$, also den Primidealen $\mathfrak{q}$ mit $\mathfrak{q} \subseteq \mathfrak{p}$.*

Beweis. Seien $I, J \subseteq \mathfrak{p}$ Primideale von R mit $I \neq J$. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass es ein $x \in I$ gibt, sodass $x \notin Y$. Wir behaupten, dass es keinen Elementen $\frac{y}{a} \in J_\mathfrak{p}$ gibt, mit $\frac{x}{1} \sim \frac{y}{a}$. Dies folgt, da die Äquivalenz die Existenz eines $t \in R \setminus \mathfrak{p}$ impliziert, mit $txa = ty$. Da $ty \in J$, folgt $txa \in J$. Aber $a, t \notin \mathfrak{p} \supset J$ und $x \notin J$ bei Annahme. Da J prim ist, ist dies ein Widerspruch. Es folgt, dass die Zuordnung $I \mapsto I_\mathfrak{p}$ injektiv ist.

Wir erinnern uns, dass das Urbild eines Primideals immer Prim ist. Man nehme daher $\gamma^{-1}(A) \subseteq R$. Aus mengentheoretischen Argumenten folgt, dass $\gamma(\gamma^{-1}(A)) = A$ und damit haben wir auch Surjektivität.

Sei nun $I \subseteq J$. Dann ist bei Definition $I_\mathfrak{p} \subseteq J_\mathfrak{p}$. Aus Bijektivität folgt nun auch, dass $I_\mathfrak{p} \subseteq J_\mathfrak{p}$ $I \subseteq J$ impliziert. □

Man vergleiche dies mit Proposition 1.3.9, wo wir die Ideale vom Quotienten $R/\mathfrak{p}$ studiert haben.

Korollar 1.5.10. *Die Lokalisierung $R_\mathfrak{p}$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{p}_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$.*

Beweis. Dies folgt direkt aus Proposition 1.5.9, da $\mathfrak{p}$ natürlich das eindeutige größte Primideal unter $\mathfrak{p}$ ist. □

Korollar 1.5.11. *Sei R ein Integritätsbereich. Dann ist $R_\mathfrak{o}$ ein Körper, wobei $\mathfrak{o} = (0)$, und die natürliche Abbildung*

$$R \to R_\mathfrak{o}$$

ist injektiv.

Proposition 1.5.12. *Sei R ein Integritätsbereich, $\mathfrak{p} \subseteq R$ ein Primideal und $I \subseteq R$ ein Ideal. Dann gibt es eine kanonische Abbildung $\alpha : R/I \to R_\mathfrak{p}/I_\mathfrak{p}$.*

Beweis. Wir betrachten das folgende Diagramm:

$$\begin{array}{ccc} R & \xrightarrow{\iota} & R_\mathfrak{p} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_I} \\ R/I & \xrightarrow{\alpha} & R_\mathfrak{p}/I_\mathfrak{p} \end{array} .$$

Hier ist ι die kanonische Einbettung in die Lokalisierung, welche r auf $\frac{r}{1}$ abbildet und π, π_I sind die kanonischen Projektionen, welche ein Element auf seine Restklasse schicken. Wir definieren α wie folgt: Man hebe ein Element $\overline{r} \in R/I$ zu einem Repräsentanten $r \in R$ hoch und bilde es auf $\pi_I(\iota(r))$ ab.

Seien $r, r' \in R$, so dass $\overline{r} = \overline{r'}$. Dann ist $r - r' \in I$, also $\frac{r-r'}{1} = \frac{r}{1} - \frac{r'}{1} \in I_\mathfrak{p} \subseteq R_\mathfrak{p}$. Daher ist $\overline{\left(\frac{r}{1}\right)} = \overline{\left(\frac{r'}{1}\right)}$ in $R_\mathfrak{p}/I_\mathfrak{p}$ und somit ist α wohldefiniert.

□

1.5.2 Der Halm $\mathcal{O}_a$

Nach unserem Studium abgeschlossener Mengen $\mathrm{V}(J)$ und standardoffener Mengen $D(f)$ über ihre Koordinatenringe, wollen wir nun Punkte genauer untersuchen. Natürlich ist jeder Punkt $a = (a_1, \ldots, a_n)$ eine abgeschlossene Menge, es ist $\{a\} = \mathrm{V}(x_1 - a_1, \ldots, x_n - a_n)$ (der Schnitt aller Hyperebenen der Form $x_i - a_i$, welche a enthalten). Der assoziierte Koordinatenring $K[\{a\}]$ ist aber "zu klein", es ist nämlich

$$K[\{a\}] = K[x_1, \ldots, x_n]/\mathrm{I}(\{a\}) \simeq K \tag{4}$$

vermöge des Isomorphismus $x_i \mapsto a_i$. Beachte, dass $K[\{a\}] \simeq K[\{b\}]$ für je zwei Punkte a, b. Um lokale Eigenschaften besser einzufangen benötigen wir eine andere Konstruktion.

Definition 1.5.13. *Sei $a \in \mathbb{A}^n$. Wir definieren den* Halm *am Punkt a als*

$$\mathcal{O}_a := \left\{ \frac{f}{g} \in K(\mathbb{A}^n) \mid g(a) \neq 0 \right\}.$$

Mit anderen Worten, enthält der Halm an einem Punkt a genau die rationalen Funktionen auf $\mathbb{A}^n$, welche am Punkt a definiert sind. Beachte, dass auch hier wieder gilt $\mathcal{O}_a \simeq \mathcal{O}_b$ für alle Punkte $a, b \in \mathrm{V}$.

Die Definition des Halms ähnelt stark der Beschreibung der Koordinatenringe standard-offener Mengen $D(f)$ als gewisse rationale Funktionen auf $\mathbb{A}^n$:

$$\Gamma(D(f)) = \left\{ \frac{g}{h} \in K(\mathbb{A}^n) \mid \forall a \in D(f) : h(a) \neq 0 \right\}$$

Im Allgemeinen ist $\mathbb{A}^n \setminus \{a\}$ aber nicht von der Form $D(f)$ für ein $f \in K[\mathbb{A}^n]$ (wann wäre das der Fall?), wir können also nicht einfach $\mathcal{O}_a = \Gamma(\mathbb{A}^n \setminus \{a\})$ schreiben. Dennoch gibt es eine Beschreibung des Halmes $\mathcal{O}_a$ als Lokalisierung von $K[x_1, \ldots, x_n]$, analog zu Satz 1.4.6 für $\Gamma(D(f))$. Dazu sei $\mathfrak{m}_a$ das zu a laut Korollar 1.2.51 korrespondierende maximale Ideal von $K[x_1, \ldots, x_n]$. Anstatt den Quotienten nach $\mathfrak{m}_a$ zu bilden (dies haben wir in 4 getan, denn $\mathfrak{m}_a = \mathrm{I}(a) = (x_1 - a_1, \ldots, x_n - a_n)$), können wir auch an $\mathfrak{m}_a$ lokalisieren, denn $\mathfrak{m}_a$ ist als maximales Ideal insbesondere prim (vergleiche Korollar 1.5.10). Wir haben dann folgendes Ergebnis, welches wir aber an anderer Stelle in etwas allgemeinerer Form beweisen werden.

Proposition 1.5.14. *Es gibt eine Isomorphie*

$$\mathcal{O}_a \simeq K[x_1, \ldots, x_n]_{\mathfrak{m}_a}.$$

Insbesondere ist $\mathcal{O}_a$ ein lokaler Ring.

Beweis. Siehe Satz 1.5.20 für den Fall $\mathrm{V} = \mathbb{A}^n$ und Proposition 1.5.10. □

Wir können diesen Ring auch etwas anders beschreiben:

Proposition 1.5.15. *Wir haben eine Isomorphie*

$$\mathcal{O}_a \simeq \bigcup_{a \in D(f)} \Gamma(D(f)).$$

Beweis. Sei $\psi = \frac{g}{h} \in \mathcal{O}_a$. Dann ist $h(a) \neq 0$. Also ist $a \notin h$ und somit $a \in D(h) = \mathbb{A}^n \setminus \mathrm{V}(h)$. Daher liegt ψ in $\Gamma(D(h))$, also auch in der Vereinigung auf der rechten Seite.

Auf der anderen Seite, sei $\varphi = \frac{g}{f^k} \in \Gamma(D(f))$ für irgendein $f \in K[x_1, \ldots, x_n]$. Da $a \in D(f) = \mathbb{A}^n \setminus \mathrm{V}(f)$, folgt, dass $f^k(a) \neq 0$ und daher ist $\varphi \in \mathcal{O}_a$. □

Es genügt in obiger Proposition die Vereinigung nur über alle irreduziblen f zu indizieren.

1.5.3 Der Halm $\mathcal{O}_a(\mathrm{V})$ auf einer Varietät

Nachdem wir im letzten Abschnitt den Halm eines Punktes im affinen Raum eingeführt haben, wollen wir diese Konstruktion nun für Punkte auf beliebigen Varietäten verallgemeinern. Dazu genügt es den Begriff der rationalen Funktion zu verallgemeinern, die Definition des Halmes lässt sich dann direkt übertragen.

Zur Erinnerung, je zwei Halme an Punkten im affinen Raum sind isomorph (dies ist wenig überraschend, für je zwei Punkte gibt es einen Isomorphismus des affinen Raums, welcher den einen in den anderen überführt und umgekehrt). Für beliebige Varietäten wird dies im Allgemeinen nicht mehr der Fall sein. Stattdessen geben uns Halme Aufschluss über unterschiedliche lokale Phänomene einer Varietät. So lassen sich etwa Singularitäten an Punkten der Varietät durch Eigenschaften der zugehörigen lokalen Ringe ablesen.

Wir werden uns in diesem Abschnitt auf irreduzible Varietäten konzentrieren. Laut Proposition 1.3.7 sind dies genau die Varietäten deren Koordinatenring ein Integritätsbereich ist. Nach Lemma **??** und Proposition 1.5.11 können wir dann nämlich den Quotientenkörper des Koordinatenringes bilden und rationale Funktionen auf der Varietät als Elemente des Quotientenkörpers definieren, in direkter Verallgemeinerung des Falls vom affinen Raum.

Definition 1.5.16. *Sei* $\mathrm{V} =\subseteq \mathbb{A}^n$ *eine irreduzible Varietät. Dann bezeichne* $K(\mathrm{V})$ *den Quotientenkörper von* $K[\mathrm{V}]$*. Ein Element von* $K(\mathrm{V})$ *nennen wir* rationale Funktion auf V*.*

Von unserer Diskussion über Lokalisationen wissen wir schon, dass

$$K(\mathrm{V}) \coloneqq \left\{ \frac{f}{g} \mid f, g \in K[\mathrm{V}],\ g \neq 0 \right\}.$$

Zur Erinnerung, der Bruch $\frac{f}{g}$ bezeichnet eine Äquivalenzklasse von Paaren von Elementen des Rings $K[\mathrm{V}]$ bezüglich der Relation $\frac{f}{g} \sim \frac{f'}{g'}$ genau dann wenn $fg' = f'g$. Es ist nicht immer trivial zu sehen, ob ein Repräsentant einer rationalen Funktion in $K(\mathrm{V})$ liegt, siehe das folgende Beispiel.

Beispiel 1.5.17. Sei $\mathrm{V} = \mathrm{V}(y^2 - x^2(x+1))$. Da $\overline{y}^2 = \overline{x}^2(\overline{x}+1)$ in $K[\mathrm{V}]$, gilt

$$\frac{\overline{y}}{\overline{x}} = \frac{\overline{y}^2}{\overline{xy}} = \frac{\overline{x}^2(\overline{x}+1)}{\overline{xy}} = \frac{\overline{x}(\overline{x}+1)}{\overline{y}}.$$

Man betrachte nun den Punkt $a = (-1, 0)$. Es ist klar, dass die linke Seite auf a definiert ist. Die rechte Seite ist jedoch nicht ohne weiteres ersichtlich, da wir ja nur ein " $\frac{0}{0}$ " haben, wir aber nicht einfach "kürzen" können.

Mithilfe des Begriffs der rationalen Funktion auf einer irreduziblen Varietät lässt sich nun die Definition des Halmes auf beliebige irreduzible Varietäten verallgemeinern.

Definition 1.5.18. *Sei* $\mathrm{V} \subseteq \mathbb{A}^n$ *irreduzibel und* $a \in \mathrm{V}$ *ein Punkt. Wir definieren*

$$\mathcal{O}_a(\mathrm{V}) \coloneqq \left\{ \frac{f}{g} \mid f, g \in K[\mathrm{V}],\ g(a) \neq 0 \right\}$$

und nennen dies den Halm von V auf a*.*

Ebenso wie $\mathcal{O}_a \subseteq K(\mathbb{A}^n)$ einen Unterring bildet, ist dies auch für $\mathcal{O}_a(\mathrm{V}) \subseteq K(\mathrm{V})$ der Fall. Diese Ringe müssen nun aber nicht mehr für alle Punkte isomorph sein, da nicht alle Punkte von V "gleich" sind (etwa, wenn V Singularitäten oder "doppelte" Tangenten hat, siehe Beispiel 1.5.22).

$\mathcal{O}_a(\mathrm{V})$ als Lokalisierung und Quotient Wir erinnern uns an Proposition 1.3.9, bzw. Bemerkung 1.3.10, woraus sich sofort folgende Proposition ergibt:

Proposition 1.5.19. *Sei $\mathrm{V} \subseteq \mathbb{A}^n$ irreduzibel, $a \in \mathrm{V}$ ein Punkt und $\mathfrak{m}_a \subset K[x_1, \ldots, x_n]$ das zugehörige maximale Ideal. Ferner sei*

$$\pi : K[x_1, \ldots, x_n] \to K[\mathrm{V}] = K[x_1, \ldots, x_n]/\mathrm{I}(\mathrm{V})$$

die kanonische Projektion. Dann ist $\pi(\mathfrak{m}_a) \subseteq K[\mathrm{V}]$ ein maximales Ideal.

Dies erlaubt uns nun, folgende Lokalisierung zu betrachten (man erinnere sich, dass man mit einem nicht-primen Ideal nicht lokalisieren kann):

Satz 1.5.20. *Es gibt eine Isomorphie $\mathcal{O}_a(\mathrm{V}) \simeq K[\mathrm{V}]_{\pi(\mathfrak{m}_a)}$. Genauer ist $\mathcal{O}_a(\mathrm{V})$ ein lokaler Ring, dessen maximales Ideal das Bild von $\pi(\mathfrak{m}_a)$ unter der natürlichen Einbettung $K[\mathrm{V}] \to K[\mathrm{V}]_{\pi(\mathfrak{m}_a)}$ ist. Wir notieren dieses maximale Ideal mit $\mathfrak{m}_a\mathcal{O}_a(\mathrm{V})$.*

Beweis. Das folgt fast per Definition, denn es gilt

$$K[\mathrm{V}]_{\pi(\mathfrak{m}_a)} = \left\{ \frac{f}{g} \mid f, g \in K[\mathrm{V}], g \notin \pi(\mathfrak{m}_a) \right\} = \left\{ \frac{f}{g} \mid f, g \in K[\mathrm{V}], g(a) \neq 0 \right\} = \mathcal{O}_a(\mathrm{V}). \qquad \square$$

Lemma 1.5.21. *Sei V irreduzibel und $a \in \mathrm{V}$. Wir haben einen Isomorphismus*

$$\mathcal{O}_a/\mathrm{I}(\mathrm{V}) \to \mathcal{O}_a(\mathrm{V}),$$

wobei wir abkürzend $\mathrm{I}(\mathrm{V}) = \mathcal{O}_a\mathrm{I}(\mathrm{V})$ schreiben.

Beweis. Wir definieren die Abbildung als $\overline{\left(\frac{f}{g}\right)} \mapsto \frac{\overline{f}}{\overline{g}}$. Für die Wohldefiniertheit ist allein zu beweisen, dass $\overline{g}(a) \neq 0$ gilt. Angenommen nicht, also $\overline{g}(a) = 0$. Da alle Repräsentanten von $\overline{g}$ auf allen Punkten von V miteinander und mit den Werten von $\overline{g}$ übereinstimmen, muss also $g(a) = 0$ sein, was ein Widerspruch ist, da dies kein Element von $\mathcal{O}_a$ sein kann, also auch nicht in $\mathcal{O}_a/\mathrm{I}(\mathrm{V})$ ein Element definieren kann.

Es ist leicht zu sehen, dass die Abbildung ein Ringhomomorphismus ist, für die Injektivität genügt es also zu zeigen, dass ihr Kern Null ist. Sei dazu $\frac{\overline{f}}{\overline{g}} = 0 = \frac{0}{1}$. Da $K[\mathrm{V}]$ ein Integritätsbereich ist, aufgrund der Irreduzibilität von V, folgt, dass schon $\overline{f} = 0$ gelten muss. Dies wiederum impliziert, dass $f \in \mathrm{I}(\mathrm{V}) \subseteq K[x_1, \ldots, x_n]$, was dann natürlich auf $\frac{0}{1} \in \mathcal{O}_a/\mathrm{I}(\mathrm{V})$ abgebildet wird.

Für die Surjektivität sei $\frac{\overline{f}}{\overline{g}} \in \mathcal{O}_a(\mathrm{V})$. Per Definitionen haben wir Repräsentanten $f, g \in K[x_1, \ldots, x_n]$ von $\overline{f}, \overline{g} \in K[\mathrm{V}]$. Man betrachte das Bild $\frac{f}{g}$ in $\mathcal{O}_a = K[x_1, \ldots, x_n]_{\mathfrak{m}_a}$. Unter der kanonischen Projektion $\mathcal{O}_a \to \mathcal{O}_a/\mathrm{I}(\mathrm{V})$ wird $\frac{f}{g}$ auf $\overline{\left(\frac{f}{g}\right)}$ abgebildet, was per Konstruktion ein Urbild von $\frac{\overline{f}}{\overline{g}}$ ist. $\square$

Der Halm $\mathcal{O}_a(\mathrm{V})$ ist vom Punkt a abhängig. Zur Erinnerung, für den Koordinatenring eines Punktes im affinen Raum galt $K[x_1,\dots,x_n]/\mathfrak{m}_a \simeq K$. Allgemeiner ist

$$K[\mathrm{V}]/\pi(\mathfrak{m}_a) \simeq (K[x_1,\dots,x_n]/\mathfrak{m}_a)/\mathrm{I}(\mathrm{V}) \simeq K/\pi'(\mathrm{I}(\mathrm{V}))K,$$

was isomorph zu K oder zu 0 ist, denn K besitzt als Körper nur die beiden Ideale 0 und (1). Dieser Quotientenringen ist daher nicht geeignet um Punkte einer Varietät zu unterscheiden.

Im Fall des affinen Raums haben wir gesehen, dass alle Halme $\mathcal{O}_a$ ebenfalls isomorph waren. Für eine allgemeine Varietät muss dies jedoch nicht mehr der Fall sein. Nicht alle Punkte einer Varietät verhalten sich also gleich und die Untersuchung der Halme ermöglicht uns lokale Unterschiede der Varietät an verschiedenen Punkten festzustellen.

Beispiel 1.5.22. Sei $\mathrm{V} = \mathrm{V}(xy - z^2)$, $a = (0,0,0)$ und $b = (1,1,1)$. Die maximalen Ideale von a und b sind $\mathfrak{m}_a = (x,y,z)$ und $\mathfrak{m}_b = (x-1, y-1, z-1)$. Lemma 1.5.21 liefert uns

$$\mathcal{O}_a(\mathrm{V}) \simeq \mathcal{O}_a/\mathrm{I}(\mathrm{V}) \simeq \left(K[x,y,z]_{\mathfrak{m}_a}\right)/\mathrm{I}(\mathrm{V}) \simeq \left(K[x,y,z]_{\mathfrak{m}_a}\right)/xy - z^2$$

und analog $\mathcal{O}_b \simeq \left(K[x,y,z]_{\mathfrak{m}_b}\right)/xy - z^2$. Wir bemerken, dass $x,y,z \in \mathfrak{m}_a$ und daher $x,y,z \notin S_a = K[x,y,z] \setminus \mathfrak{m}_a$. Auf der anderen Seite sind $x,y,z \notin \mathfrak{m}_b$ und daher sind $x,y,z \in S_b = K[x,y,z] \setminus \mathfrak{m}_b$. Mit anderen Worten sind x,y,z invertierbar in $\mathcal{O}_b$ aber nicht in $\mathcal{O}_a$. A priori hilft uns das nicht weiter, es ist ja umgekehrt $x-1, y-1, z-1$ in $\mathcal{O}_a$ invertierbar, aber nicht in $\mathcal{O}_b$.

Erst wenn wir zum Quotienten nach der Gleichung $xy = z^2$ (nicht $(x-1)(y-1) = (z-1)^2$) übergehen, stellen wir einen Unterschied fest. Es gilt nämlich in $\mathcal{O}_b(\mathrm{V}) = \left(K[x,y,z]_{\mathfrak{m}_b}\right)/xy - z^2$ die Gleichung $y = \frac{1}{x}z^2$. Das heißt y lässt sich durch die anderen Variablen ausdrücken und wir haben $\mathcal{O}_b(\mathrm{V}) \simeq \left(K[x,z]_{\mathfrak{m}'_b}\right)$, mit $\mathfrak{m}'_b = (x-1, z-1)$. Damit ist

$$\mathcal{O}_b(\mathrm{V}) \simeq \mathcal{O}_c,$$

wobei $\mathcal{O}_c = \mathcal{O}_c(\mathbb{A}^2)$ der Halm des Punktes $c = (1,1) \in \mathbb{A}^2$ ist. Durch eine Koordinatentransformation lässt sich auch einfach $c = (x', y')$ annehmen. Mit anderen Worten ist $\mathcal{O}_b(\mathrm{V})$ isomorph zum lokalen Ring des Ursprungs in $\mathbb{A}^2$. Eine ähnliche Vereinfachung kann man mit $\mathcal{O}_a(\mathrm{V})$ nicht durchführen.

Die Ideale der Halme

Lemma 1.5.23. *Sei $\mathrm{V} \subseteq \mathbb{A}^n$ eine irreduzible Varietät und $a \in \mathrm{V}$ ein Punkt. Betrachte das Diagramm*

$$K[x_1,\dots,x_n] \xrightarrow{\pi} K[\mathrm{V}] \xrightarrow{\iota} K[\mathrm{V}]_{\mathfrak{m}_a} = \mathcal{O}_a(\mathrm{V}) \,,$$

wobei π die kanonischen Projektion, ι die Einbettung, λ deren Komposition. Ist nun $J \subseteq K[x_1,\dots,x_n]$ ein Ideal, so ist

$$J_a(\mathrm{V}) := \left\{ \frac{\overline{f}}{\overline{g}} \mid \overline{f} \in \pi(J), \overline{g} \in K[\mathrm{V}], \overline{g}(a) \neq 0 \right\} = (\lambda(J))$$

ein Ideal von $\mathcal{O}_a(\mathrm{V})$. *Insbesondere ist*

$$J_a := J_a(\mathbb{A}^n) = \left\{ \frac{f}{g} \mid f \in J, g \in K[x_1, \ldots, x_n], g(a) \neq 0 \right\}$$

ein Ideal von $\mathcal{O}_a$.

Beweis. Wir haben $0 = \frac{0}{1} \in J_a(\mathrm{V})$. Sind $\frac{\overline{f}}{\overline{g}}$ und $\frac{\overline{f'}}{\overline{g'}}$ in $J_a(\mathrm{V})$, so liegt auch die Summe $\frac{\overline{f}}{\overline{g}} + \frac{\overline{f'}}{\overline{g'}} = \frac{\overline{fg'+f'g}}{\overline{gg'}}$ darin, denn sowohl f als auch f' liegen im Ideal J, also auch $fg' + f'g$ und damit ist $\overline{fg' + f'g} = \overline{f}\overline{g'} + \overline{f'}\overline{g}$ in $\pi(J)$ und weder g noch g' verschwindet bei a, also ist auch $gg'(a) \neq 0$. Des Weiteren ist $\frac{\varphi}{\psi}\frac{\overline{f}}{\overline{g}} = \frac{\overline{\varphi f}}{\overline{\psi g}}$. Wenn also $\frac{\varphi}{\psi} \in \mathcal{O}_a(\mathrm{V})$, daher $\varphi, \psi \in K[\mathrm{V}]$ mit $\psi(a) \neq 0$, dann ist auch wieder $\varphi\overline{f} \in \pi(J)$ und $(\psi g)(a) = \psi(a)h(a) \neq 0$. Insgesamt ist $J_a(\mathrm{V})$ damit ein Ideal.

Um die Gleichheit $\mathrm{J}_a(\mathrm{V}) = (\lambda(J))$ zu zeigen, beachte zunächst, dass das Bild $\lambda(J)$ Teilmenge von $J_a(\mathrm{V})$ ist, denn für jedes $f \in J$ ist $\lambda(f) = \frac{\overline{f}}{1}$ von der gewünschten Form. Dann liegt aber auch das von $\lambda(J)$ erzeugte Ideal darin, da $J_a(\mathrm{V})$ nach obiger Betrachtung ein Ideal ist. Umgekehrt lässt sich jedes Element $\frac{\overline{f}}{\overline{g}} \in J_a(V)$ als $\frac{1}{\overline{g}} \cdot \overline{f} = \frac{1}{\overline{g}} \cdot \lambda(f)$ für ein $f \in J$ schreiben, was natürlich im von $\lambda(J)$ erzeugten Ideal liegt. □

Korollar 1.5.24. *Sei* $\mathrm{V} \subseteq \mathbb{A}^n$ *eine irreduzible Varietät,* $I = \mathrm{I}(\mathrm{V}) \subseteq K[x_1, \ldots, x_n], a \in \mathrm{V}$ *und* $I \subseteq J \subseteq K[x_1, \ldots, x_n]$ *ein Ideal, welches* I *enthält. Dann gilt*

$$\mathcal{O}_a/(\iota(J)) \simeq \mathcal{O}_a(\mathrm{V})/(\lambda(J)),$$

wobei $\iota : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]_{\mathfrak{m}_a} = \mathcal{O}_a$ *die kanonische Einbettung ist und* λ *wie in Lemma 1.5.23 oben.*

Beweis. Dies ist ein Korollar von Lemma 1.5.21 und dem zweiten Isomorphiesatz 1.2.43. □

2 Planare affine Kurven und die Schnittzahl

Nachdem wir einige allgemeine Aussagen bewiesen haben, wollen wir uns nun die Ebene etwas genauer ansehen.

2.1 Klassifikation algebraischer Teilmengen von $\mathbb{A}^2$

Teilbarkeit und Irreduzibilität

Lemma 2.1.1 (Gaußsches Lemma)**.** *Zwei Polynome $f, g \in K[x,y]$ haben genau dann einen gemeinsamen Teiler, wenn sie einen gemeinsamen Teiler in $K(x)[y]$ haben.*

Beweis. Siehe Anhang in einigen Tagen. □

Satz 2.1.2. *Seien f, g teilerfremde Polynome in $K[x,y]$. Dann gilt*

$$|\mathrm{V}(f,g)| = |\mathrm{V}(f) \cap \mathrm{V}(g)| < \infty.$$

Mit anderen Worten, teilerfremde Polynome schneiden sich nur in endlich vielen Punkten.

Beweis. Da f und g keine gemeinsamen Teiler in $K[x,y]$ haben, sind sie auch über $K(x)[y]$ teilerfremd, laut Lemma 2.1.1. Da $K(x)$ ein Körper ist, wissen wir, dass $K(x)[y]$ ein Hauptidealbereich ist. Teilerfremdheit bedeutet dann gerade $(f,g) = 1$, in $K(x)[y]$. Daher gibt es $r, s \in K(x)[y]$, so dass $1 = rf + sg$. Aus der Tatsache, dass $r, s \in K(x)[y]$, folgern wir, dass es $d_r, d_s \in K[x]$ gibt, sodass $d_r r \in K[x,y]$ und $d_s s \in K[x,y]$. Indem wir $d := d_r d_s$ setzen, können wir $1 = rf + sg$ zu

$$drf + dsg = d \in K[x] \subset K[x,y]$$

umschreiben. Sei nun (a,b) ein Schnittpunkt von f und g, also $(a,b) \in \mathrm{V}(f,g)$. Dann ist $d(a) = 0$ wegen obiger Gleichung. Da d als Polynom über x aber nur endlich viele Lösungen hat (es liegt in $K[x]$, also nur eine Variable), gibt es nur eine endliche Anzahl von Möglichkeiten für die x-Koordinate eines Punktes in $\mathrm{V}(f,g)$. Aus Symmetriegründen gilt dasselbe für die y-Koordinate eines Schnittpunktes, was insgesamt die Aussage beweist. □

Planare Kurven Wir definieren eine Relation $\sim$ auf $K[x,y]$ wie folgt: Für $f, g \in K[x,y]$ ist $f \sim g$ genau dann, wenn $\mathrm{V}(f) = \mathrm{V}(g)$.

Lemma 2.1.3. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $K[x,y]$, welche mit der Multiplikation von Polynomen verträglich ist.*

Beweis. Da die Relation durch eine Gleichheit definiert ist, ist sie eine Äquivalenzrelation. Für die Verträglichkeit mit der Multiplikation sei $f \sim g$ und $r \sim h$. Nun gilt

$$\mathrm{V}(fr) = \mathrm{V}(f) \cup \mathrm{V}(r) = \mathrm{V}(g) \cup \mathrm{V}(r) = \mathrm{V}(gr)$$

und damit $fr \sim gh$. □

Definition 2.1.4. *Eine* affine planare Kurve *ist eine Äquivalenzklasse nichtkonstanter Polynome bezüglich der in Lemma 2.1.3 eingeführten Äquivalenzrelation.*

Normalerweise werden wir einfach Kurve sagen. Des Weiteren werden wir hier etwas unpräzise sein und einfach x^2+y^2-1 als eine Kurve bezeichnen, anstatt die Klasse $[x^2+y^2-1]$ zu schreiben.

Klassifikation von irreduziblen Varietäten

Korollar 2.1.5. *Ist K ein Körper mit unendlich vielen Elementen, so ist jede irreduzible algebraische Teilmenge von $\mathbb{A}^2$ von der Form*

$$\varnothing,\ \text{Punkt},\ \text{irreduzible planare Kurve } \mathrm{V}(f) \quad \text{oder} \quad \mathbb{A}^2,$$

wobei f irreduzibel und $\mathrm{V}(f)$ unendlich ist.

Beweis. Es ist klar, dass all diese Mengen irreduzibel und abgeschlossen/algebraisch sind. Sei umgekehrt V eine irreduzible algebraische Teilmenge von $\mathbb{A}^2$. Wenn $|\mathrm{V}| < \infty$, dann ist V eine Vereinigung von Punkten (bzw. leer). Eine endliche Vereinigung von Punkten ist genau dann irreduzibel, wenn sie ein einziger Punkt ist (oder leer).

Sei nun V eine unendliche Menge und betrachte $\mathrm{I}(\mathrm{V})$. Da $\mathrm{V}(k) = \varnothing$ für alle konstanten Polynome $0 \neq k \in K$, muss entweder $\mathrm{V} = \mathrm{V}(0) = \mathbb{A}^2$ sein, oder $\mathrm{I}(\mathrm{V})$ enthält ein nichtkonstantes Polynom f. Aus Satz 1.2.50 wissen wir, dass $\mathrm{I}(\mathrm{V})$ prim ist. Daher gibt es ein irreduzibles $f' \in \mathrm{I}(\mathrm{V})$, so dass $f' | f$. Ohne Einschränkung können wir daher schon annehmen, dass f selbst irreduzibel ist.

Wir behaupten nun, dass $\mathrm{V} = \mathrm{V}(f)$. Angenommen nicht. Da nach Wahl von f sicherlich $\mathrm{V} \subseteq \mathrm{V}(f)$ gilt, muss ein $g \in \mathrm{I}(\mathrm{V})$ existieren, sodass $g \notin (f)$. Nun ist f aber irreduzibel, weshalb f und g keinen gemeinsamen Teiler besitzen können. Aus $\mathrm{V} \subseteq \mathrm{V}(f,g)$ folgt damit ein Widersprich zu Satz 2.1.2. □

Korollar 2.1.6. *Sei K algebraisch abgeschlossen und $f \in K[x,y]$ ein nicht-konstantes Polynom mit $f = f_1^{e_1} \cdots f_r^{e_r}$, wobei f_i irreduzibel und $e_i \geq 1$. Dann gilt*

$$\mathrm{V}(f) = \mathrm{V}(f_1) \cup \cdots \cup \mathrm{V}(f_r),$$

mit $\mathrm{V}(f_i)$ irreduzibel und $\mathrm{I}(\mathrm{V}(f)) = (f_1 \cdots f_r)$.

Beweis. Hausaufgabe. □

Wir wollen nun jeder affinen Kurve V einen eindeutigen Repräsentanten f mit $\mathrm{V} = \mathrm{V}(f)$ zuordnen. Dazu führen wir eine Ordnung auf den Monomen $x^n y^m \in K[x,y]$ wie folgt ein: Zunächst ordnen wir Monome nach dem Totalgrad $n+m$, etwa ist $xy^2 > x^2$. Anschließend legen wir fest, dass $x > y$ sein soll und setzen diese Ordnung lexikographisch fort. Das heißt, sind $f := x^n y^m$ und $g := x^k y^l$ vom selben Totalgrad $m+n = k+l$, so ist $f > g$ genau dann,

wenn $n > k$. Beispielsweise ist $x^4 > x^2y^2$ und $xy^2 > xy$. Nun können wir definieren, was der *Leitkoeffizient* eines Polynoms ist, nämlich der Koeffizient des bezüglich dieser Ordnung größten Monoms im Polynom. Zum Beispiel ist -1 der Leitkoeffizient des Polynoms

$$5x^2y^2 - xy^4 + 2x^3 - 3y^5.$$

Ein Polynom heißt nun *normiert*, wenn sein Leitkoeffizient 1 ist.

Bemerkung 2.1.7. Offenbar lässt sich obige Ordnung auch für Monome mit mehr als zwei Variablen einführen. Beachte aber, dass die lexikographische Ordnung etwas komplizierter zu definieren ist. In drei Variablen $x > y > z$ gilt etwa, dass $x^a y^b z^c > x^d y^e z^f$ genau dann, wenn $a > d$ oder wenn $a = d$ und $b > e$.

Es gibt noch viele weitere Monomordnungen. Welche man genau wählt, ist für unsere Zwecke nicht von Belang, wir brauchen die Ordnung nur um vom Leitkoeffizienten eines Polynoms sprechen zu können. Wichtig ist lediglich, bei der gewählten Ordnung zu bleiben.

Korollar 2.1.8. *Es gibt eine Bijektion zwischen affinen planaren Kurven und nicht-konstanten normierten Polynomen ohne multiple Faktoren.*

Beweis. Sei f ein Polynom, welches eine affine planare Kurve $\mathrm{V}(f)$ repräsentiere, insbesondere ist f nicht konstant. Ist $f = f_1^{e_1} \dots f_r^{e_r}$ eine Zerlegung in irreduzible Faktoren, so gilt nach Korollar 2.1.6, dass $\mathrm{V}(f) = \mathrm{V}(f_1 \dots f_r)$. Indem wir durch den Leitkoeffizienten von $f_1 \dots f_r$ teilen, was offenbar nicht die affine Kurve $\mathrm{V}(f)$ verändert, erhalten wir ein normiertes nicht-konstantes Polynom ohne multiple Faktoren, welches zu f äquivalent ist.

Umgekehrt sind je zwei nicht-konstante normierte Polynome ohne multiple Faktoren f, g, welche $\mathrm{V}(f) = \mathrm{V}(g)$ erfüllen, also die selbe affine planare Kurve darstellen, bereits gleich. Denn (f), (g) sind Radikalideale, was aus der Bedingung folgt, dass beide Polynome keine multiplen Faktoren besitzen, und somit gilt

$$(f) = \sqrt{(f)} = \mathrm{I}(\mathrm{V}(f)) = \mathrm{I}(\mathrm{V}(g)) = \sqrt{(g)} = (g).$$

Die Normiertheitsbedingung impliziert dann schon, dass $f = g$. □

2.2 Vielfachheit und Tangenten

Mit Korollar 2.1.8 haben wir eine Art Klassifikation planarer Kurven in $\mathbb{A}^2$. Nun wollen wir Kurven weiter studieren. Wir haben uns in dem Korollar auf normierte Polynome eingeschränkt. Tatsächlich ist es etwas praktischer, hier etwas anders ranzugehen.

Grad einer Kurve

Definition 2.2.1. *Sei $f \in K[x,y]$ eine Kurve. Der* Grad *der Kurve $[f]$ wird definiert als den Grad des Polynoms $f(x,y)$.*

Zur Erinnerung, der Grad eines multivariaten Polynoms ist definiert als der Grad seines höchsten Monoms. Dies wiederum ist definiert als die Summe der Potenzen aller Variablen. Zum Beispiel:

$$\begin{aligned} 5 &= \mathsf{grad}\left(f_2(x,y) := \underline{x}^5 + y^4\right) \\ &= \mathsf{grad}\left(f_3(x,y) := \underline{x^2y}^3 + xy^2 + y\right) \\ &= \mathsf{grad}\left(f_4(x,y) := \underline{x}^5 + \underline{y}^5\right) \\ &= \mathsf{grad}\left(f_1(x,y) := \underline{x}^5\right) \end{aligned}$$

Lemma 2.2.2. *Der Grad einer Kurve ist wohldefiniert.*

Beweis. Hier muss man beweisen, dass aus $f \sim g$ folgt, $\mathsf{grad}(f) = \mathsf{grad}(g)$. Sei dazu $f = \lambda g$. Dann ist $\mathsf{grad}(g) = \mathsf{grad}(\lambda) + \mathsf{grad}(g) = 0 + \mathsf{grad}(g)$ da $0 \neq \lambda \in K$. □

Definition 2.2.3. *Eine Kurve vom Grad* 1 *nennt man* Gerade.

Multiple und einfache Komponenten

Definition 2.2.4. *Sei $f = f_1^{e_1} \cdots f_n^{e_n}$ eine Zerlegung in irreduziblen Faktoren. Wir nennen f_i eine* Komponente *von f und e_i die* Vielfachheit *(oder manchmal* Multiplizität*) der Komponente f_i. Eine Komponente f_i wird* einfach *genannt, wenn ihre Multiplizität eins ist. Also, wenn $e_i = 1$. Andernfalls sagt man, dass es eine* vielfache *(bzw.* multiple*) Komponente ist.*

Bemerkung 2.2.5. Von nun werden wir stets annehmen, dass Kurven irreduzibel sind, es sei denn, wir fordern explizit das Gegenteil.

Es ist bekannt, dass für Polynome eine Zerlegung in irreduziblen Komponenten eindeutig ist. Die obigen Begriffe machen aber auch für Kurven Sinn, da diese Definitionen freilich mit der Äquivalenzrelation 2.1.4 verträglich sind.

Man bemerke, dass wir laut Korollar 2.1.6 die Komponenten einer Kurve aus ihrer Nullstellenmenge (also $\mathrm{V}(f)$) zurückerhalten können. Lemma 1.2.17 jedoch besagt, dass dies nicht für die Multiplizität gilt.

Tangente auf Regulären Punkten

Definition 2.2.6. *Sei $f \in K[X,Y]$ eine Kurve und $a = (x_0, y_0) \in \mathrm{V}(f)$ ein Punkt auf der Kurve, also $f(a) = 0$. Der Punkt wird* regulär *bzw.* nichtsingulär *oder* glatt *genannt, wenn die Ableitung von f bei a nicht identisch verschwindet, also wenn*

$$f_x(a) \neq 0 \quad \textit{oder} \quad f_y(a) \neq 0$$

Sind alle Punkte $a \in \mathrm{V}(f)$ der Kurve regulär wird die Kurve selbst regulär *genannt.*

Ein Punkt, welcher nicht regulär ist, wird singulär *genannt. Liegt auf einer Kurve mindestens ein singulärer Punkt, so wird sie* singulär *genannt.*

Definition 2.2.7. *Sei $a = (x_0, y_0) \in f$ ein regulärer Punkt auf einer (irreduziblen) Kurve f. Dann heißt die Gerade*

$$f_x(a)(x - x_0) + f_y(a)(y - y_0) = 0$$

die Tangente *am Punkt a.*

Formen

Definition 2.2.8. *Ein Polynom $F \in K[x_1, \ldots, x_n]$ heißt* homogen *bzw. eine* Form*, wenn der Grad aller Monomiale gleich ist. Wir werden Formen mit großen Buchstaben bezeichnen.*

Beispiel 2.2.9. Sei unser Ring $K[x,y]$. Folgende Polynome sind homogen:

i) x^2,

ii) $x - y$,

iii) $xy + 7y^2$,

iv) $r \in K$,

v) $x^2 + xy + y^2$.

Folgende Polynome sind *nicht* homogen:

i) $1 + x$,

ii) $x^2 + y^2 + x^2y^2$,

iii) $x^2 + x^2y$.

Es ist klar, dass wir ein Polynom $f \in K[x,y]$ als eine Summe von homogenen Polynomen darstellen können, indem wir alle Monomiale des gleichen Grades zusammenfassen. Wir werden eine Form vom Grad i mit F_i bezeichnen. Zur Erinnerung, $f = F_2$ nennt man es auch eine quadratische Form.

Beispiel 2.2.10. Folgende Beispiele sind Zerlegungen von Polynomen in $K[x,y]$ in Formen:

i)
$$f = x^2 + 3x^3y + 5y^2 \;\Rightarrow\; f = \underbrace{\left(x^2 + 5y^2\right)}_{\text{Grad } 2} + \underbrace{3x^3y}_{\text{Grad } 4},$$
wobei $F_2 = x^2 + 5y^2$, $F_4 = 3x^3y$ und andernfalls $F_i = 0$;

ii)
$$f = 1 + x + y + 5xy + x^2 + 5y^2 \;\Rightarrow\; f = \underbrace{1}_{\text{Grad } 0} + \underbrace{(x+y)}_{\text{Grad } 1} + \underbrace{\left(x^2 + 5xy + 5y^2\right)}_{\text{Grad } 2},$$
wobei $F_0 = 1$, $F_1 = x + y$, $F_2 = x^2 + 5xy + 5y^2$ und $F_i = 0$ für $i \geq 3$.

Wir werden das folgende einfache Lemma öfter benutzen, ohne es explizit zu erwähnen.

Lemma 2.2.11. *Sein $F, G \in K[x_1, \ldots, x_n]$ Formen vom Grad k und l. Dann ist FG eine Form vom Grad $k + l$.*

Beweis. Dies ist trivial. Sei $F = \sum_i x_1^{a_{i1}} \cdots x_n^{a_{in}}$ mit $a_{i1} + \cdots + a_{in} = k$ für jedes i und $G = \sum_j x_1^{b_{j1}} \cdots x_n^{b_{jn}}$ mit $b_{i1} + b_{in} = l$ für jedes j. Dann ist $FG = \sum_{ij} x_1^{a_{i1}+b_{j1}} + \cdots + x_n^{a_{in}+b_{jn}}$. Damit ist also die Summe der Potenzen gleich $k + l$. □

Definition 2.2.12. *Sei $f = F_m + F_{m+1} + \cdots + F_n$ ein Polynom, wobei F_m die Form kleinsten Grades bezeichne, welche nicht verschwindet. Diese Form nennen wir die* Minimalform *von f. Die* Multiplizität *$\mu_0(f)$ von f am Punkt $0 = (0,0)$ sei definiert als der Grad m der Minimalform F_m von f, also $\mu_0(f) = m$.*

Es ist direkt ersichtlich, dass $\mu_0(f) \geq 1$ genau dann, wenn $0 \in \mathrm{V}(f)$ gilt. Die Multiplizität von f an anderen Punkten lässt sich mit Hilfe folgender Notation auf die Vielfachheit am Punkt 0 zurückführen.

Definition 2.2.13. *Sei $f \in K[x,y]$ ein Polynom und $a = (x_0, y_0)$. Wir bezeichnen mit T die* Translation *(bzw.* Parallelverschiebung*) von $0 = (0,0)$ auf a. Also, $T : \mathbb{A}^2 \to \mathbb{A}^2$, mit $T(x,y) = (x + x_0, y + y_0)$. Wir bezeichnen die Komposition $f \circ T$ mit*

$$f^T(x,y) = f(x + x_0, y + y_0).$$

Definition 2.2.14. *Sei $f \in K[x_1, \ldots, x_n]$ und $a = (x_0, y_0) \in \mathbb{A}^2$ ein Punkt. Wir definieren die* Multiplizität *von f an a als den Grad der Minimalform von f^T, also*

$$\mu_a(f) \coloneqq \mu_0\left(f^T\right).$$

In anderen Worten, wir schreiben die Translation $f^T = G_m + G_{m+1} + \cdots + G_n$ als eine Summe von Formen und bestimmen dann den geringsten Grad eines vorkommenden Monomials. Es ist nun auch klar, dass $a \notin \mathrm{V}(f)$ genau dann, wenn $\mu_a(f) = 0$.

Lemma 2.2.15. *Sei $f \in K[x,y]$ ein homogenes Polynom vom Grad n über einem algebraisch abgeschlossen Körper K. Dann gilt*

$$f = \lambda \prod L_i^{r_i},$$

wobei $\lambda \in K, L_i = a_i x + b_i y$, mit $a_i, b_i \in K$ und $\sum r_i = n$.

Beweis. Betrachte das Bild des Polynoms f unter dem Homomorphismus von K-Algebren $K[x,y] \to K[t][x]$, welcher x auf x und y auf tx abbildet. Mit anderen Worten, substituiere $y = tx$ für eine neue Variable t. Da f homogen vom Grad n ist, gilt

$$f(x,tx) = x^n f(1,t).$$

Wir definieren $g := f(1,t) \in K[t]$, sodass $f(x,tx) = x^n g(t)$. Da K algebraisch abgeschlossen ist, zerfällt g in Linearfaktoren, etwa

$$g(t) = \lambda(t-u_1)\dots(t-u_m)$$

für gewisse $\lambda, u_1, \dots, u_m \in K$. Beachte, dass $m \le n$ per Definition von g.

Sei nun $(x_0, y_0) \in D(x) \subseteq \mathbb{A}^2$, also $x_0 \neq 0$. Dann gilt:

$$f(x_0,y_0) = x_0^n f(1, \tfrac{y_0}{x_0}) = \lambda x_0^n \left(\frac{y_0}{x_0} - u_1\right) \dots \left(\frac{y_0}{x_0} - u_m\right) = \lambda x_0^{n-m}(y_0 - u_1 x) \dots (y_0 - u_m x_0)$$

Nach Lemma 1.4.1 gilt diese Gleichung sogar auf ganz $\mathbb{A}^2$, womit wir die gewünschte Zerlegung von f erhalten. □

In anderen Worten, jedes homogene Polynom ist ein Produkt von Geraden. Der Grund warum wir die Geraden zusammengefasst haben, ist, weil ein Polynom g die selben Nullstellen hat, wie all dessen (positive) Potenzen $g^k, k \ge 1$. Daher, definieren sie die selbe Kurve/Gerade. Dies ist wichtig für die folgende Definition:

Tangente auf allgemeine Punkte

Definition 2.2.16. *Sei f ein Polynom, $a = (x_0, y_0)$ ein Punkt, $f^T = G_m + G_{m+1} + \dots + G_n$ eine Zerlegung in Formen und $G_m = \prod L_i^{r_i}$, mit $L_i = a_i x + b_i y$. Dann nennen wir die Geraden*

$$a_i (x - x_0) + b_i (y - y_0)$$

die Tangenten *von f am Punkt a. Wenn alle $r_i = 1$, (aber $m \ge 2$), dann nennen wir so einen Punkt eine* herkömmliche *(oder* normale*) Singularität.*

Da T die Punkte von f auf die Punkte von f^T abbildet und daher auch die Geraden am Punkt $(0,0)$ zu Geraden am Punkt a, ergibt diese Definition Sinn.

Beispiel 2.2.17. Man betrachte die Kurven

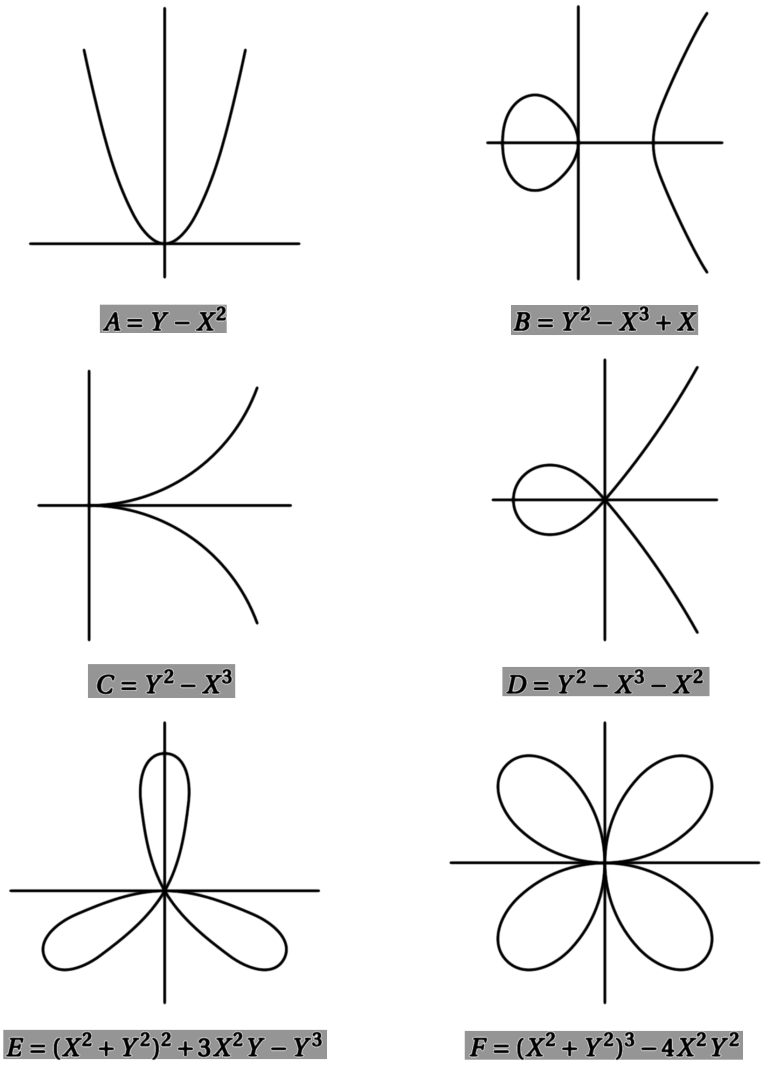


Figure 1: *
Von "Fulton - Algebraic Curves"

und den Punkt $a = (0, 0)$. Wir stellen folgende Tabelle auf:

f	f_x	f_y	$F_m = \prod L_i$	Tangenten
A	$A_x = -2x$	$A_y = 1$	y	y=0
B	$B_x = 1 - 3x^2$	$B_y = 2y$	x	x=0
C	$C_x = -3x^2$	$C_y = 2y$	$y^2 = y \cdot y$	$T_1 : y = 0 \quad = \quad T_2 : y = 0$
D	$D_x = -3x^2 - 2x$	$D_y = 2y$	$y^2 - x^2 = (x - y)(x + y)$	$T_1 : x - y = 0 \quad T_2 : x + y = 0$
E	$E_x = 4x^3 + 4xy^2 + 6xy$	$E_y = 4y^3 + 4x^2y + 3x^2 - 3y^2$	$3x^2y - y^3 = y(\sqrt{3}x - y)(\sqrt{3}x + y)$	$T_1 : y = 0 \quad T_2 : (\sqrt{3}x - y) = 0 \quad T_3 : (\sqrt{3}x + y)$
F	$F_x = 6x^5 + 12x^3y^2 + 6xy^4 + 8xy^2$	$F_y = 6x^4y + 12x^2y^3 + 6y^5 - 8x^2y$	$4x^2y^2 = 4x \cdot x \cdot y \cdot y$	$T_1 = T_2 : x = 0 \quad T_3 = T_4 : y = 0.$

Man hätte bei der linearen Zerlegung von F_m (bei der letzten Funktion), auch $4x = 0$ nehmen können. Da f und λf jedoch die selbe Kurve definieren, ist dies nicht notwendig.

Wir merken direkt, dass A und B auf $(0,0)$ regulär/nicht-singulär sind, da $A_y(0,0) = 1$ und $B_x(0,0) = 1$ und daher sind diese ungleich Null. Auf der anderen Seite haben die Kurven C, D, E, F alle eine Singularität auf dem Ursprungspunkt, da beide ihrer Ableitungen Null sind. Man merkt auch, dass wir in diesen Fällen mehr als eine Tangente habe, was äquivalent ist zu sagen, dass der homogene Summand vom kleinsten Grad (also F_m) vom Grad ≥ 2 ist. Dies ist kein Zufall, wie man am folgendem Lemma sieht.

Die Multiplizität

Lemma 2.2.18. *Eine Kurve f ist genau dann regulär am Punkt $a = (x_0, y_0)$, wenn $\mu_a(f) = 1$.*

Beweis. Sei f regulär wie in Definition 2.2.6 eingeführt. Von der Regularität haben wir als aller erstes $f(a) = 0$, was schon besagt, dass $m_a(f) = m_0(f^T) = m \geq 1$, wobei $f^T = G_m + G_{m+1} + \cdots + G_n$ (sieh Definition 2.2.14). Für jeden $k \geq 2$, muss jeder der monomialen Summanden von G_k entweder durch x^2, y^2 oder xy teilbar sein. Daher wird bei der partiellen Ableitung $f_x^T = (G_m)_x + \cdots + (G_n)_x$, jeder monomiale Summand von $(G_k)_x$ durch x oder y teilbar sein, oder gleich null sein. Ebenso $(G_k)_y$. Als solches werden beide von $(0,0)$ annihiliert. Wir schlussfolgern, dass für $m \geq 2$, $f_x(a) = f_x^T(0) = 0 = f_y^T(0) = f_y(a)$, was der Regularität von f an a widerspricht.

Umgekehrt, sei $\mu_a(f) = 1$. Da es ungleich Null ist, wissen wir schon, dass $f(a) = 0$. Da es aber spezifisch 1 ist, wissen wir, dass $f^T = G_1 + G_2 + \cdots + G_n$, wobei $G_1 = rx + sy \neq 0$, mit $r, s \in K$. Daher, ohne Verlust von Allgemeinheit können wir sagen, dass $r \neq 0$. In diesem falls ist aber $f_x(a) = f_x^T(0) = r \neq 0$, was unsere Aussage beweist. □

Beispiel 2.2.19. Die Kurve $y = x^2$ ist regulär am Punkt $(0,0)$, da als Form, wir $f = F_1 + F_2$ haben, mit $F_1 = y$ und $F_2 = -x^2$.

Es ist nun einfach zu Zeigen, dass Definition 2.2.16 mit Definition 2.2.7 im nicht-singulärem Fall (also $\mu_a(f) = 1$) übereinstimmt. In diesem Fall ist nämlich $G_m = G_1 = a_1x + b_1y$ und daher $f_x(a) = f_x^T(0) = a_1 + \frac{\partial G_2}{\partial x} + \cdots$. Da aber die G_i's homogen sind, darf in G_2 nur x^2, xy und y^2 vorkommen. In der Ableitung mit x haben wir also $2x, x$ und 0. Wenn wir nun $0 = (0,0)$ einsetzen, wird es Null. Daher ist $f_x(a) = f_x^T(0) = a_1$. Gleichwie ist $f_y(a) = f_y^T(0) = b_1$ was uns nun $a_1(x - x_0) + b_1(y - y_0) = f_x(a)(x - x_0) + f_y(a)(x - x_0)$ gibt.

Da die L_i natürlich irreduzibel sind, benutzten wir nun die Notation von Definition 2.2.4 und nennen die r_i die Vielfachheit der Tangente. Eine Tangente heißt dementsprechend auch einfach wenn $r_i = 1$ gilt.

Die Multiplizität $\mu_a(f)$ einer Funktion f am Punkt a kann man als eine Abbildung von Polynome in die ganzen Zahlen sehen. Unter dieser Abbildung gehen Produkte auf Summen, sieh folgende Proposition:

Proposition 2.2.20. *Sein f_i Polynome. Dann gilt*

$$\mu_a\left(\prod_{i=1}^{n} f_i\right) = \sum_{i=1}^{k} \mu_a\left(f_i\right).$$

Beweis. Dies ist eine allgemeine Formel, die für Leitkoeffizienten bzw. Leitformen (daher den Grad) und Minimalkoeffizienten bzw. Minimalformen stimmt und folgt direkt von Lemma 2.2.11. □

Als solches reicht es aus, sich die Multiplizität der irreduziblen Faktoren eines Polynoms auszurechnen. In diesem Fall können wir auch mehr über die Tangenten aussagen:

Korollar 2.2.21. *Sei $f = \prod f_i^{e_i}$ eine Zerlegung in irreduzible Komponenten und für die Minimalformen gelte $F_{im} = \prod_j L_{ij}^{r_{ij}}$. Für jeden Punkt a gilt $\mu_a(f) = \sum e_i \mu_a(f_i)$. Ferner, sei L eine Tangente von f_i mit Multiplizität e_i. Dann ist L eine Tangente von f mit Multiplizität $\sum e_i r_{ij}$.*

Korollar 2.2.22. *Sei $f = \prod f_i^{e_i}$ eine Zerlegung in irreduzible Komponente. Das Polynom f ist genau dann regulär am Punkt a, wenn a auf genau einem der Faktoren f_i liegt und dessen Multiplizität gleich* 1 *ist.*

2.3 Multiplizität und diskrete Bewertungsringe

Im letzten Abschnitt haben wir die Multiplizität von einem Punkt a auf einer Kurve f eingeführt. Nun wollen wir dies mit dem Halm $\mathcal{O}_a(\mathrm{V}(f))$ von $\mathrm{V}(f)$ auf a in Verbindung bringen. Von nun an werden wir $\mathcal{O}_a(f)$ anstatt $\mathcal{O}_a(\mathrm{V}(f))$ schreiben, um die Notation etwas einfacher zu machen.

Wir zeigen eine Reihe von Lemmata, mithilfe derer wir zwei wichtige Sätze beweisen können. Diese werden den Zusammenhang zwischen dem Halm $\mathcal{O}_a(f)$ und der Multiplizität $\mu_a(f)$ aufzeigen.

Definition 2.3.1. *Eine* affine Koordinatentransformation *ist eine bijektive Abbildung*

$$T = (T_1, \ldots, T_n) : \mathbb{A}^n \to \mathbb{A}^n,$$

sodass $T_i : \mathbb{A}^n \to K$ *polynomielle Funktionen vom Grad* 1 *sind.*

Eine Translation ist eine affine Koordinatentransformation. Man erinnere sich an unsere Diskussion ganz am Anfang der Vorlesung: Der affine n-Raum $\mathbb{A}^n$ ist auch ein K-Vektorraum. Wir wissen daher aus der linearen Algebra, dass jede affine Koordinatentransformation T als Summe einer Translation und einer linearen Abbildung dargestellt werden kann. Es gilt also

$$T(a) = v + Aa,$$

wobei $a, v \in \mathbb{A}^n$ mit v fixiert und A eine $n \times n$ Matrix ist. Die Bedingung, dass T bijektiv sein soll, impliziert die Invertibilität von A.

Proposition 2.3.2. *Die Menge*

$$G_T = \{T : \mathbb{A}^n \to \mathbb{A}^n\}$$

der affinen Variablenwechsel bildet eine Gruppe unter Komposition von Abbildungen.

Beweis. Es ist klar, dass die Menge der Bijektionen $\mathbb{A}^n \to \mathbb{A}^n$ unter der Komposition von Abbildungen eine Gruppe bildet, deren neutrales Element die Identitätsabbildung ist. Es genügt daher nachzuweisen, dass die Teilmenge der affinen Koordinatentransformationen eine Untergruppe bildet. Seien also $T, T' : \mathbb{A}^n \to \mathbb{A}^n$ affine Koordinatentransformationen mit $T(a) = v + Aa$ und $T'(a) = u + Ba$. Dann ist

$$(T \circ T')(a) = T(T'(a)) = T(u + Ba) = v + (Au + ABa) = (v + Au) + ABa$$

und das Inverse zu T gegeben durch

$$T^{-1}(a) = -A^{-1}v + A^{-1}a.$$

Damit ist die Menge der affinen Koordinatentransformationen abgeschlossen unter Komposition und Inversenbildung. Da die Identität offensichtlich eine affine Transformation ist, sind wir fertig. □

Ohne es zu beweisen oder zu verwenden, wollen wir erwähnen, dass, $G_T \simeq \mathbb{A}^n \rtimes \mathsf{GL}(\mathbb{A}^n)$, wobei $\mathsf{GL}(\mathbb{A}^n) = \mathsf{GL}(n, K)$ die allgemeine lineare Gruppe ist.

Sei $f \in K[x_1, \ldots, x_n]$ und $T : \mathbb{A}^n \to \mathbb{A}^n$ eine affine Koordinatentransformation. Wir definieren $f^T := f \circ T$, also mit anderen Worten,

$$f^T(a_1, \ldots, a_n) := f(T(a_1, \ldots, a_n)).$$

Lemma 2.3.3. *Seien $T, T' : \mathbb{A}^n \to \mathbb{A}^n$ affine Koordinatentransformationen und $f \in K[x_1, \ldots, x_n]$. Dann gilt*

$$\left(f^T\right)^{T'} = f^{T \circ T'},$$

wobei $T \circ T$ die Verknüpfung von Proposition 2.3.2 ist.

Beweis. Wir haben $(f^T)^{T'} = (f \circ T) \circ T' = f \circ (T \circ T') = f^{T \circ T'}$. Man kann es auch direkt per Hand für $n = 2, 3$ als Matrizen überprüfen. Für größere n werden wir die Aussage nicht brauchen.

□

Lemma 2.3.4. *Sein p, q Punkte in $\mathbb{A}^2$. Seien $l_1 \neq l_2$ verschiedene Geraden durch p und $l_1' \neq l_2'$ verschiedene Geraden durch q. Es gibt eine affine Koordinatentransformation T, so dass $T(p) = q$ und $T(l_i) = l_i'$, $i = 1, 2$.*

Beweis. Lasst uns zuerst den vereinfachten Fall ansehen, dass l_1 die x-Achse, l_2 die y-Achse und $p = 0$ ist. Da die l_i' Geraden durch q sind, lassen sich diese in der Form

$$l_i' = \{q + t(r_i - q) \mid t \in K\}$$

schreiben, wobei r_i ein beliebiger aber fester Punkt auf l_i' ist, welcher nicht gerade q ist. Wir definieren nun

$$A := (r_1 - q, r_2 - q) = \begin{pmatrix} r_{11} - q_1 & r_{21} - q_1 \\ r_{12} - q_2 & r_{22} - q_2 \end{pmatrix}$$

Da die Geraden l_1' und l_2' sich in q schneiden, aber ungleich sind, sind die Spalten von A (die Richtungsvektoren der zugehörigen Geraden) linear unabhängig, die Matrix ist also invertierbar. Wir erhalten eine affine Koordinatentransformation

$$T_1(a) := q + Aa,$$

welche 0 auf q abbildet. Weiterhin werden Punkte der Form $(t, 0)$, also Punkte auf der x-Achse l_1 auf l_1' abgebildet und ebenso werden Punkte $(0, t)$ auf der y-Achse l_2 auf l_2' abgebildet.

Der allgemeine Fall folgt nun mit Proposition 2.3.2. Nach obiger Beobachtung finden wir zu einem Punkt p und zwei ungleichen Geraden l_1, l_2 durch p eine affine Transformation T_2, welche 0 auf p, die x-Achse auf l_1 und die y-Achse auf l_2 abbildet. Die affine Transformation $T := T_1 \circ T_2^{-1} \in G_T$ erfüllt dann die gewünschten Eigenschaften. □

Lemma 2.3.5. *Sei $T : \mathbb{A}^n \to \mathbb{A}^n$ eine affine Koordinatentransformation und $a \in \mathbb{A}^n$ ein Punkt. Wir erhalten eine kanonische Abbildung auf Halmen*

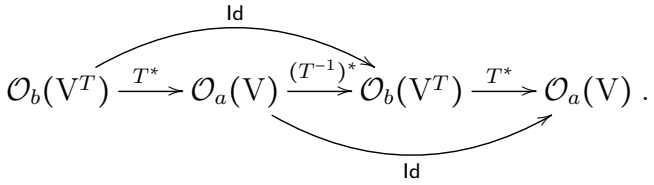
$$T^* : \mathcal{O}_{T(a)} \to \mathcal{O}_a$$

durch die Setzung $\frac{f}{g} \mapsto \frac{f^T}{g^T}$. Sei allgemeiner $\mathrm{V} \subseteq \mathbb{A}^n$ eine (irreduzible) Varietät. Falls $T|_{\mathrm{V}}$ einen Isomorphismus auf V induziert und $a \in \mathrm{V} = T(\mathrm{V})$ liegt, dann ist die induzierte Abbildung

$$T^* : \mathcal{O}_b(\mathrm{V}) \to \mathcal{O}_a(\mathrm{V})$$

ein Isomorphismus.

Beweis. Es reicht aus, wenn wir den allgemeinen Fall für V beweisen, den ersten Fall erhalten wir durch $\mathrm{V} = \mathbb{A}^n$ zurück. Die Abbildung T^* ist wohldefiniert, da $g^T(a) = g(T(a)) \neq 0$. Um zu sehen, dass $T^* : \mathcal{O}_b(\mathrm{V}^T) \to \mathcal{O}_a(\mathrm{V})$ ein Isomorphismus ist, sei $T^{-1} : \mathbb{A}^n \to \mathbb{A}^n$ die Umkehrung von T. Es ist klar, dass dies eine Abbildung $(T^{-1})^* : \mathcal{O}_a(\mathrm{V}) \to \mathcal{O}_b(\mathrm{V}^T)$, $\frac{f'}{g'} \mapsto \frac{f'^{T^{-1}}}{g'^{T^{-1}}}$ definiert. Da T^{-1} die Umkehrung von T ist, also $T_{\mathrm{V}} \circ T_{\mathrm{V}}^{-1} = \mathsf{Id}$ und $T_{\mathrm{V}}^{-1} \circ T_{\mathrm{V}} = \mathsf{Id}$ und die Komposition von affinen Transformationen laut Lemma 2.3.3 durch $(-)_a^\star$ respektiert wird (wobei das "f" des Lemmas hier das T und nicht das f ist) haben wir das folgende kommutative Diagramm:



In anderen Worten, $(T^{-1})^* \circ T^* = \mathsf{Id}$ und $T^* \circ (T^{-1})^* = \mathsf{Id}$. Wir haben also beidseitige Inverse und somit einen Isomorphismus. □

Zur Erinnerung, $\mathcal{O}_a$ ist die Lokalisation von $K[x_1, \ldots, x_n]$. Daher haben wir eine kanonische Einbettung

$$\iota_a : K[x_1, \ldots, x_n] \to \mathcal{O}_a.$$

Wir haben schon erwähnt, dass man ein Ideal $I \subseteq K[x_1, \ldots, x_n]$ zu einem Ideal $I_a := (\iota(I)) =: \subseteq \mathcal{O}_a$ machen kann. Wir wollen beweisen, dass für $|\mathrm{V}| < \infty$ endlich, $K[\mathrm{V}]$ als ein Produkt der Halme darstellbar ist. Intuitiv ist dies klar, der Beweis jedoch ist recht schwer. Ehe wir dazu kommen, müssen wir allerdings das Konzept relativ maximaler Ideale etwas erkunden.

2.3.1 Relativ Maximale Ideale

Wir erinnern daran, dass zwei ganze Zahlen n und m *relativ prim* genannt werden, wenn sie keine gemeinsamen echten Teiler besitzen. Diese Eigenschaft impliziert die Existenz einer *Bézout-Darstellung* der 1, also

$$1 = rm + sn,$$

für gewisse ganze Zahlen r, s. Anders ausgedrückt, in Termen von Idealen ist

$$(1) = (m) + (n).$$

In den ganzen Zahlen ist Teilerfremdheit zweier Zahlen und die Existenz einer solchen Bézout-Darstellung äquivalent. In allgemeinen Ringen ist der zweite Begriff jedoch stärker. Wir wollen im Folgenden die Bézout-Eigenschaft verallgemeinern und außerdem beliebige Ideale statt nur Hauptideale betrachten.

Definition 2.3.6. *Zwei Ideale $I, J \subseteq R$ werden* relativ maximal *oder* komaximal *genant, wenn*

$$I + J = (I \cup J) = (1) = R.$$

Um die Terminologie zu erläutern, beachte, dass ein maximales Ideal $\mathfrak{m}$ zu jedem anderen Ideal, welches nicht in $\mathfrak{m}$ liegt, relativ maximal ist, zum Beispiel zu jedem anderen maximalen Ideal ungleich $\mathfrak{m}$, vergleiche auch Korollar 2.3.8.

Proposition 2.3.7. *Sei K algebraisch abgeschlossen. Zwei Ideale $I, J \subseteq K[x_1, \ldots, x_n]$ sind genau dann relativ maximal, wenn $\mathrm{V}(I) \cap \mathrm{V}(J) = \varnothing$.*

Beweis. Sei $I + J = R$. Aus Teil (iv) von Lemma 1.1.17 folgt $\mathrm{V}(I) \cap \mathrm{V}(J) = \mathrm{V}(I + J) = \mathrm{V}(R) = \varnothing$, wobei die letzte Gleichung Teil (ii) desselben Lemmas ist.

Für die andere Richtung sei $\mathrm{V}(I) \cap \mathrm{V}(J) = \varnothing$. Dann gilt wieder nach Lemma 1.1.17, Teil (iv) und (ii) $\mathrm{V}(I + J) = \mathrm{V}(I) \cap \mathrm{V}(J) = \varnothing = \mathrm{V}(R)$. Aus Hilberts Nullstellensatz 1.2.43, Teil (iii) folgt also $\sqrt{I + J} = \sqrt{(1)}$. Teil (i) und (ii) aus Korollar 1.2.16 besagen nun, dass $I + J = (1) = (R)$. □

Korollar 2.3.8. *Seien $a_1, \ldots, a_N \in \mathbb{A}^n$ paarweise verschieden und $\mathfrak{m}_i$ die zu a_i assoziierten Maximalideale. Dann sind $I = \bigcap_{i \neq j} \mathfrak{m}_i$ und $J = \mathfrak{m}_j$ relativ maximal.*

Beweis. Laut Teil (iv) von Lemma 1.1.23 ist $I = \bigcap_{i \neq j} \mathfrak{m}_i = \mathrm{I}(\bigcup_{i \neq j} \{a_i\})$. Dann besagt Teil (i) von Korollar 1.1.27, dass $\mathrm{V}(I) = \bigcup_{i \neq j} \{a_i\}$ und $\mathrm{V}(J) = \{a_j\}$. Da $\mathrm{V}(I) \cap \mathrm{V}(J) = \varnothing$, ist die Bedingung von Proposition 2.3.7 erfüllt. □

Lemma 2.3.9. *Seien $I, J \subseteq R$ relativ maximal. Dann gilt $I \cap J = IJ$.*

Beweis. Nach Voraussetzung existieren $a \in I$ und $b \in J$ mit $a + b = 1$. Für ein beliebiges Element $c \in I \cap J$ gilt nun

$$c = 1 \cdot c = (a + b)c = ac + bc \in IJ + IJ = IJ,$$

wobei die Elementbeziehung gilt, da wir c zum Einen als Element von I, zum Anderen als Element von J auffassen. Daher ist $I \cap J \subseteq IJ$. Die andere Inklusion gilt immer. □

Lemma 2.3.10. *Seien $I, J \subseteq R$ relativ maximal. Dann sind auch I^n und J^m relativ maximal.*

Beweis. Da I, J relativ maximal sind, gibt es $a \in I, b \in J$, so dass $a + b = 1$. Es folgt, dass $b = ab + b^2$, was

$$1 = a + b = a + ab + b^2 = a(1 + b) + b^2 \in I + J^2$$

impliziert. Daher sind auch I und J^2 relativ maximal. Es folgt nun induktiv, dass für beliebige $n, m \geq 1$, I^n und J^m relativ maximal sind. □

Lemma 2.3.11. *Seien $I_1, \ldots, I_N \subseteq R$ Ideale eines Ringes R, sodass für jedes $1 \leq j \leq N$, die Ideale $J_j := \bigcap_{i \neq j} I_i$ und I_j relativ maximal sind. Dann gilt für jedes $n \in \mathbb{N}$, dass*

$$I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n.$$

Beweis. Wir zeigen dies per Induktion über N. Als erstes jedoch bemerken wir, dass I_i und I_j für $i \neq j$ relativ maximal sind. Dies liegt daran, dass $J_j \subseteq I_i$ und daher impliziert $J_j + I_j = (1)$, dass $I_i + I_j = (1)$.

Sei nun zunächst $N = 2$. Dann gilt laut Lemma 2.3.10, dass auch I_1^n und I_2^n relativ maximal sind. Aus Lemma 2.3.9 folgt dann

$$I_1^n \cap I_2^n = I_1^n I_2^n = (I_1 I_2)^n = (I_1 \cap I_2)^n.$$

Wir nehmen nun an, dass die Aussage für alle $k < N$ stimmt.
Behauptung: Die Ideale $I_1, \ldots, I_{N-2}, I_{N-1} \cap I_N$ erfüllen auch die Bedingung des Lemmas.

Um dies zu beweisen, brauchen wir nur zu zeigen, dass $I_{N-1} \cap I_N$ und $K = \bigcap_{i < N-1} I_i$ relativ maximal sind, da die anderen Fälle trivial sind. Per Annahme sind I_{N-1} und $J_{N-1} = \bigcap_{i \neq N-1}$ relativ maximal. Da $J_{N-1} = K \cap I_N \subseteq K$, sind I_{N-1} und K relativ maximal und aus Symmetriegründen auch I_N und K. Es folgt, dass $I_{N-1} \cap I_N$ relativ maximal zu K ist. Dies beweist die Behauptung.

Per Induktionsannahme haben wir

$$I_1^n \cap \cdots \cap I_{N-2}^n \cap (I_{N-1} \cap I_N)^n = (I_1 \cdots I_{N-2} \cdots (I_{N-1} \cap I_N))^n = (I_1 \cap \cdots \cap I_{N-2} \cap (I_{N-1} \cap I_N))^n .$$

Da I_{N-1} und I_N relativ maximal sind, gilt laut Lemma 2.3.9, dass $I_{N-1} \cap I_N = I_{N-1} I_N$. Daher wird der mittlere Term zu $(I_1 \cdots I_N)^n$. Des Weiteren können wir den Induktionsanfang $N = 2$ anwenden und erhalten

$$I_1^n \cap \cdots \cap I_{N-2}^n \cap (I_{N-1} \cap I_N)^n = I_1^n \cap \cdots \cap I_{N-2}^n \cap (I_{N-1}^n \cap I_N^n) = I_1^n \cap \cdots \cap I_N^n.$$

Daraus lässt sich schlussfolgern, dass

$$I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n . \qquad \square$$

Endliche Varietäten als Produkt von Halmen

Proposition 2.3.12. *Sei $J \subseteq K[x_1, \dots, x_n]$ ein Ideal und $\mathrm{V} = \mathrm{V}(J) = \{a_1, \dots, a_N\}$ endlich. Dann gilt*

$$K[x_1, \dots, x_n]/J \simeq \prod_{i=1}^{N} \mathcal{O}_{a_i}/J_i,$$

wobei $J_i = J\mathcal{O}_{a_i}$ unsere Kurzform ist.

Beweis. Sei $K[J] = K[x_1, \dots, x_n]/J$. Laut Proposition 1.5.12 gibt es eine kanonische Abbildung $\alpha_i : K[J] \to \mathcal{O}_{a_i}/J_i$ für jedes $1 \leq i \leq N$. Daher gibt es eine kanonische Abbildung

$$\alpha : K[\mathrm{J}] \to \prod_{i=1}^{N} \mathcal{O}_{a_i}/J, \tag{5}$$

welche komponentenweise definiert ist. Wir wollen nun beweisen, dass dies ein Isomorphismus ist. Zur Vorbereitung wollen wir zuerst beweisen, dass die drei Gleichungen (10),(11),(12) weiter unten gelten.

Seien dazu $\mathfrak{m}_i = \mathrm{I}(\{a_i\})$ die zu den Punkten a_i assoziierten maximalen Ideale. Es ist klar, dass verschiedene Punkte unterschiedliche maximale Ideale liefern. Des Weiteren, da $a_i \in \mathrm{V}(J)$, ist $J \subseteq \mathfrak{m}_i$.

Laut Teil (iii) des Nullstellensatzes 1.2.43 und (iv) von Lemma 1.1.23 gilt

$$\sqrt{J} = \mathrm{I}(\{a_1, \dots, a_N\}) = \bigcap_{i=1}^{N} \mathfrak{m}_i.$$

Daher folgt aus Lemma 1.2.14, dass es ein $d \in \mathbb{N}$ gibt, so dass

$$\left(\bigcap_{i=1}^{N} \mathfrak{m}_i\right)^d \subseteq J.$$

Laut Korollar 2.3.8 sind $\bigcap_{i \neq j} \mathfrak{m}_i$ und $\mathfrak{m}_j$ relativ maximal für jeden $1 \leq j \leq N$. Also folgt aus Lemma 2.3.11, dass

$$\bigcap_{i=1}^{N} \mathfrak{m}_i^d = (\mathfrak{m}_1 \cdots \mathfrak{m}_N)^d = \left(\bigcap_{i=1}^{N} \mathfrak{m}_i\right)^d \subseteq J. \tag{6}$$

Laut Lemma 1.2.45 gibt es für jeden $1 \leq i \leq N$ einen Polynom f_i, sodass $f_i(a_i) = 1$ aber $f_i(a_j) = 0$ für alle $j \neq i$. Anders gesagt, sodass $f_i \in \mathfrak{m}_j$ genau dann, wenn $i \neq j$.

Sei

$$e_i := 1 - (1 - f_i^d)^d.$$

Da sich die 1en wegkürzen, gibt es ein Polynom e_i', so dass $e_i = f_i^d e_i'$. Daher ist $e_i \in \mathfrak{m}_j^d \subseteq \mathfrak{m}_j$, wenn $i \neq j$. Insbesondere gilt also auch

$$e_i \in \bigcap_{j \neq i} \mathfrak{m}_j^d. \tag{7}$$

Für jedes $1 \leq i \leq N$ gilt auch

$$(1 - e_i)(a_i) = (1 - f_i^d)(a_i) = (1 - f_i^d(a_i)) = (1 - 1) = 0. \tag{8}$$

was

$$1 - e_i = (1 - f_i^d)^d \in \mathfrak{m}_i^d \tag{9}$$

impliziert. Man betrachte nun $1 - \sum_{i=1}^{N} e_i$. Für jedes fixierte i können wir es als $(1 - e_i) - \sum_{j \neq i} e_j$ gruppieren. Da $1 - e_i \in \mathfrak{m}_i^d$ und $e_j \in \bigcap_{k \neq j} \mathfrak{m}_k^d \subseteq \mathfrak{m}_i^d$, da $i \neq j$, haben wir, dass auch deren Summe in $\mathfrak{m}_i^d$ ist. Daher $1 - \sum_{i=1}^{N} e_i \in \mathfrak{m}_i^d$. Da wir ein beliebiges i fixiert hatten und die linke Seite unabhängig davon ist, folgt

$$1 - \sum_{i=1}^{N} e_i \in \bigcap_{i=1}^{N} \mathfrak{m}_i^d \subseteq J.$$

Die Formeln (7) und (9) liefern

$$e_i - e_i^2 = e_i(1 - e_i) \in \left(\bigcap_{j \neq i} \mathfrak{m}_j^d \right) \mathfrak{m}_i^d = \bigcap_{j, j \neq i} \mathfrak{m}_j^d \mathfrak{m}_i^d \subseteq J.$$

Bei der letzten Gleichung haben wir $j, j \neq i$ statt $j \neq i$ als Index geschrieben, nur um nochmal zu betonen, dass wir nur j durchlaufen. Formel (7) impliziert auch direkt

$$e_i e_j \in J,$$

wenn $i \neq j$. Sei $\overline{e_i} \in K[J] = K[x_1, \ldots, x_n]/J$ die Restklasse von e_i. Wir haben folgende Gleichungen:

$$\overline{e}_i^2 = \overline{e}_i \tag{10}$$

$$\overline{e}_i \overline{e}_j = 0 \quad \text{für} \quad i \neq j \tag{11}$$

$$\sum_{i=1}^{N} \overline{e}_i = 1. \tag{12}$$

Wir betrachten nun, was mit diesen $\overline{e}_i$'s unter α_i passiert. Als erstes bemerken wir, dass

$$e_i(a_i) = 1 \Leftrightarrow e_i \notin \mathfrak{m}_i.$$

Da $\mathcal{O}_{a_i}$ ein lokaler Ring ist (Lemma 1.5.14), folgt vom Korollar 1.5.4, dass $\frac{e_i}{1}$ in $\mathcal{O}_{a_i}$ invertierbar ist. Invertierbare Elemente werden zu Invertierbaren unter Ringhomomorphismen abgebildet. Es muss also unter der Projektion $\mathcal{O}_{a_i} \to \mathcal{O}_{a_i}/J_i$ einer Einheit zugeordnet werden. Bei der Konstruktion von $\alpha_i : K[J] \to \mathcal{O}_{a_i}/J_i$ ist dies genau das Element $\alpha_i(\overline{e}_i)$. Daher ist

$\alpha_i(\overline{e}_i) \in (\mathcal{O}_{a_i}/J_i)^*$ invertierbar. Aus (11) folgt $\alpha_i(\overline{e}_i)\alpha_i(\overline{e_j}) = \alpha_i(\overline{e}_i\overline{e}_j) = 0$, $i \neq j$. Darum muss also

$$\alpha_j(\overline{e}_i) = 0 \quad \text{für} \quad i \neq j$$

sein. Aus Gleichung (12) folgt nun

$$\alpha_i(\overline{e}_i) = \alpha_i\left(\sum_{k=1}^{N} \overline{e}_k\right) = \alpha_i(1) = 1. \tag{13}$$

Daher ist es nicht nur *eine* Einheit, sondern *die* Einheit.

Behauptung: Für jedes $g \in K[x_1, \ldots, x_n]$ mit $g(a_i) \neq 0$ gibt es ein $\overline{t} \in K[J]$, so dass $\overline{t}\overline{g} = \overline{e}_i$.

Da wir über einen Körper sind und keine weiteren Anforderungen an t stellen, ist es klar, dass wir $g(a_i) = 1$ annehmen können. Definiere $h = 1 - g$. Dann gilt

$$(1-h)(e_i + he_i + \cdots + h^{d-1}e_i) = e_i - h^d e_i. \tag{14}$$

Per Definition ist $h(a_i) = (1-g)(a_i) = 1 - g(a_i) = 0$, also $h \in \mathfrak{m}_i$, daher $h^d \in \mathfrak{m}_i^d$. Auf der anderen Seite ist laut Gleichung (7) $e_i \in \bigcap_{j \neq i} \mathfrak{m}_j^d$, was $h^d e_i \in \bigcap_{j,j\neq i} \mathfrak{m}_j^d \mathfrak{m}_i^d \subseteq \bigcap_j \mathfrak{m}_j^d \subseteq J$ impliziert. Gleichung (14) besagt nun, indem wir $(1-h) = (1-(1-g)) = g$ am Anfang einsetzen, dass

$$\overline{g}(\overline{e}_i + \overline{h}\overline{e}_i + \cdots + \overline{h}^{d-1}\overline{e}_i) = \overline{e}_i - \overline{h}^d\overline{e}_i = \overline{e}_i.$$

Wir haben also ein gewünschtes $\overline{t} = (\overline{e}_i + \overline{h}\overline{e}_i + \cdots + \overline{h}^{d-1}\overline{e}_i) \in K[J]$ gefunden und die Behauptung bewiesen.

Wir wollen nun beweisen, dass α aus (5) ein Isomorphismus ist.
Surjektivität: Sei $z = \left(\frac{r_1}{s_1}, \ldots, \frac{r_N}{s_N}\right) \in \mathcal{O}_{a_i}$ und $\overline{z} \in \prod_i \mathcal{O}_{a_i}/J_i$. Da $s_i(a_i) \neq 0$, gibt es laut unserer Behauptung ein $\overline{t}_i \in K[J]$, so dass $\overline{t}_i\overline{s}_i = \overline{e}_i \in K[J]$. Mit Gleichung (13) folgt, dass $\alpha_i(\overline{t}_i)\alpha_i(\overline{s}_i) = \alpha_i(\overline{t}_i\overline{s}_i) = \alpha_i(\overline{e}_i) = 1 \in \mathcal{O}_{a_i}/J_i$. Da α_i die kanonische Abbildung ist, welche $\overline{t}_i$ auf $\overline{\left(\frac{t}{1}\right)}$ abbildet, ist in $\mathcal{O}_{a_i}/J_i$

$$\overline{\left(\frac{r_i}{s_i}\right)} = \frac{\overline{r}_i\overline{t}_i}{1}.$$

Es folgt, dass

$$\alpha_i\left(\sum_{k=1}^{N} \overline{t}_k\overline{r}_k\overline{e}_k\right) = \alpha_i\left(\overline{t}_k\overline{r}_k\right) = \overline{\left(\frac{r_i}{s_i}\right)}.$$

Wir haben hier die linke Seite "künstlich" verkompliziert, damit dies unabhängig von den i wird. Somit wird das Element $\sum_{k=1}^{N} \overline{t}_k\overline{r}_k\overline{e}_k$ unter der kanonischen Abbildung α, welche komponentenweise durch α_i gegeben war, auf das gewünschte z abgebildet.

Injektivität: Sei $\overline{r} \in K[J]$ mit $\alpha(\overline{r}) = 0$. Daher ist $\pi_i \circ \alpha(\overline{r}) = \alpha_i(\overline{r}) = 0$, für jedes $1 \leq i \leq N$ (denn α war Komponentenweise als α_i definiert). Da aber $\alpha_i(\overline{r}) = \overline{\left(\frac{r}{1}\right)}$ ist, haben wir $\frac{r}{1} \in J_i \subseteq \mathcal{O}_{a_i}$ für einen beliebigen Repräsentanten $r \in K[x_1, \ldots, x_n]$ von $\overline{r}$. Ein beliebiges Element von J hat die Form $\sum_k \frac{b_k}{c_k}\frac{d}{1}$, wobei $\frac{b_k}{c_k} \in \mathcal{O}_{a_i}$ und $d \in J$. Indem wir es auf dem gleichen Nenner bringen, können wir annehmen, dass es von der Form $\sum_k \frac{b_k d}{c}$ ist. Da $\frac{r}{1} \in J_i$, gibt es also $b_{ki}, c_i \in K[x_1, \ldots, x_n]$, mit $c_i(a) \neq 0$ und $d_i \in J$, so dass $\frac{r}{1} = \sum_k \frac{b_{ki} d_i}{c_i}$. Daher, $rc_i = \sum_k b_{ki} d_i$. Da $d_i \in J$, ist $\sum_k b_{ki} d_i \in J$ und daher $rc_i \in J$.

Mit anderen Worten, für jedes $1 \leq i \leq N$ gibt es ein c_i mit $c_i(a_i) \neq 0$, so dass $rc_i \in J \subseteq K[x_1, \ldots, x_n]$. Nach unserer Behauptung oben gibt es also ein $\overline{t}_i \in K[J]$, so dass $\overline{t}_i \overline{c}_i = \overline{e}_i$. Mit der Formel (12) haben wir also

$$\overline{r} = \sum_i \overline{e}_i \overline{r} = \sum_i \overline{t}_i \overline{c}_i \overline{r}_i = 0$$

da $r_i c_i \in J$. Dies schließt den Beweis ab. □

Bemerkung 2.3.13. Da $\mathcal{O}_{a_i}$ ein Lokalring ist (Proposition 1.5.14), ist $\mathcal{O}_{a_i}/\mathfrak{m}_i$ ein Körper. Dies wird öfters mit κ_{a_i} bezeichnet und ist eine wichtige Konstruktion in der algebraischen Geometrie.

Korollar 2.3.14. *Sei $J \subseteq K[x_1, \ldots, x_n]$, so dass $\mathrm{V}(J) = \{a_1, \ldots, a_N\}$ eine endliche Menge ist. Dann gilt*

$$\dim_K \left(K[x_1, \ldots, x_n]/J\right) \simeq \sum_{i=1}^{N} \dim_K \left(\mathcal{O}_{a_i}/J\right).$$

Korollar 2.3.15. *Sei $J \subseteq K[x_1, \ldots, x_n]$, so dass $\mathrm{V}(J) = \{a\}$ ein Punkt ist. Dann gilt*

$$K[x_1, \ldots, x_n]/J \simeq \mathcal{O}_a/J.$$

Wir haben auch folgendes:

Korollar 2.3.16. *Sei $J \subseteq K[x_1, \ldots, x_n]$ ein Radikalideal und $\mathrm{V}(J) = \{a_1, \ldots, a_N\}$ endlich. Dann gilt*

$$K[\mathrm{V}] \simeq \prod_{i=1}^{N} \mathcal{O}_{a_i}(\mathrm{V}).$$

Beweis. Dies ist einfach nur Hilberts Nullstellensatz 1.2.43, Teil (iii), Lemma 1.5.21 und Proposition 2.3.12. □

2.3.2 Exakte Sequenzen und K-Vektorräume

Ehe wir weitermachen, müssen wir einen Kurzen Ausflug in die *Homologische Algebra* machen. Wir werden aber nur "kurz an der Oberfläche kratzen" und einige Lemmata über exakte Sequenzen beweisen.

Lemma 2.3.17. *Sein A, B K-Vektorräume. Dann gilt*

$$\dim_K(A \oplus B) = \dim_K(A) + \dim_K(B).$$

Beweis. Dies sollte von der linearen Algebra bekannt sein. Die unterliegende Menge von $A \oplus B$ ist das kartesische Produkt $A \times B$. Ist nun $\{e_1, \ldots, e_n\}$ eine Basis von A und $\{f_1, \ldots, f_m\}$ eine Basis von B, so ist $\{(e_1, 0), \ldots, (e_n, 0), (0, f_1), \ldots, (0, f_m)\}$ eine Basis von $A \oplus B$. □

Exakte Sequenzen Die meisten der Aussagen in diesem Abschnitt lassen sich auf beliebige Moduln über kommutativen Ringen verallgemeinern. Da abelsche Gruppen genau die $\mathbb{Z}$-Moduln sind, gelten die Resultate insbesondere für abelsche Gruppen. Wir werden uns aber der Vertrautheit halber auf Vektorräume beschränken.

Definition 2.3.18. *Eine Sequenz linearer Abbildungen*

$$\cdots \to A_i \xrightarrow{d_i} A_{i+1} \xrightarrow{d_{i+1}} A_{i+2} \xrightarrow{d_{i+2}} \cdots$$

wird Kettenkomplex *genannt, wenn die Gleichung $d_{i+1} \circ d_i = 0$ für jedes $i \in \mathbb{Z}$ gilt. In diesem Fall nennt man d_i das* Differential *des Komplexes im Grad i.*

Bemerkung 2.3.19. Normalerweise lässt man die Indizes der Differentiale weg und schreibt stattdessen einfach d mit der Bedingung $d^2 = 0$. Genauer definiert man $A := \bigoplus_{i \in \mathbb{Z}} A_i$ und fasst die Differentiale als Endomorphismus $d : A \to A$ auf, welcher die Bedingungen $d(A_i) \subseteq A_{i+1}$ und $d^2 = 0$ erfüllt.

Definition 2.3.20. *Ein Kettenkomplex*

$$\cdots \to A_i \xrightarrow{d_i} A_{i+1} \xrightarrow{d_{i+1}} A_{i+2} \xrightarrow{d_{i+2}} \cdots$$

wird exakt im Grad $i+1$ *genannt, wenn* $\mathsf{Bild}(d_i) = \mathsf{Ker}(d_{i+1})$. *Ist der Komplex in jedem Grad exakt, so nennen wir ihn* exakt *beziehungsweise eine* exakte Sequenz.

Bemerkung 2.3.21. In jedem Kettenkomplex gilt schon die Inklusion $\mathsf{Bild}(d_i) \subseteq \mathsf{Ker}(d_{i+1})$, dies folgt sofort aus der Bedingung $d^2 = 0$ (bzw. $d_{i+1} \circ d_i = 0$). An jeder Stelle lässt sich daher der Quotient $\mathsf{Ker}(d_{i+1})/\mathsf{Bild}(d_i)$ bilden, genannt die i-te Homologie des Komplexes. Der Komplex ist also genau dann exakt, wenn seine Homologie an jeder Stelle verschwindet. Folglich ist die Homologie ein "Maß für die Nichtexaktheit" des Komplexes. Wir werden aber nicht in diese Richtung weitergehen.

Definition 2.3.22. *Eine exakte Sequenz der Form*

$$0 \to A \xrightarrow{\alpha} C \xrightarrow{\gamma} B \to 0,$$

wo also alle bis auf drei Vektorräume des Sequenz 0 *sind, wird* kurze exakte Sequenz *genannt.*

Lemma 2.3.23. *Sei*

$$0 \to A \xrightarrow{\alpha} C \xrightarrow{\gamma} B \to 0$$

eine kurze exakte Sequenz. Dann ist α injektiv und γ surjektiv.

Beweis. Per Definition ist $\mathsf{Bild}(0 \to A) = \mathsf{Ker}(\alpha)$. Da aber $\mathsf{Bild}(0 \to A) = 0$ ist, folgt Injektivität. Andersrum, da $\mathsf{Bild}(\gamma) = \mathsf{Ker}(B \to 0) = B$, haben wir Surjektivität. □

Folgendes Lemma ist *falsch* für beliebige Moduln statt Vektorräumen.

Lemma 2.3.24. *Seien A, B, C Vektorräume. Es existiert genau dann eine kurze exakte Sequenz der Form*

$$0 \to A \xrightarrow{\alpha} C \xrightarrow{\gamma} B \to 0,$$

wenn $C \simeq A \oplus B$.

Beweis. Beachte, dass wir in jedem Fall eine kurze exakte Sequenz der Form

$$0 \to A \xrightarrow{\iota} A \oplus B \xrightarrow{\pi} B \to 0$$

haben, wobei $\iota(a) = (a, 0)$ und $\pi(a, b) = b$. Offensichtlich ist ι injektiv, π surjektiv und $\pi \circ \iota = 0$. Liegt ferner (a, b) im Kern von π, so ist $b = 0$, also $(a, b) = \iota(a)$.

Ist nun also $A \oplus B \simeq C$, etwa vermöge eines Isomorphismus $\zeta : A \oplus B \to C$, so erhalten wir eine kurze exakte Sequenz

$$0 \to A \xrightarrow{\alpha} C \xrightarrow{\gamma} B \to 0,$$

indem wir $\alpha := \zeta \circ \iota$ und $\gamma := \pi \circ \zeta^{-1}$ setzen. Da ζ als Isomorphismus sowohl injektiv als auch surjektiv ist, ist α injektiv als Komposition injektiver Abbildungen und γ aus dem analogen Grund surjektiv. Weiterhin ist

$$\gamma \circ \alpha = \pi \circ \zeta^{-1} \circ \zeta \circ \iota = \pi \circ \iota = 0,$$

also $\mathsf{Bild}(\alpha) \subseteq \mathsf{Ker}(\gamma)$. Ist schließlich $c \in \mathsf{Ker}(\gamma)$, so ist $\zeta^{-1}(c) \in \mathsf{Ker}(\pi)$ per Definition von γ. Nach obiger Betrachtung ist $\mathsf{Ker}(\pi) = \mathsf{Bild}(\iota)$, es existiert also ein $a \in A$, sodass $\iota(a) = \zeta^{-1}(c)$. Damit liegt c in $\mathsf{Bild}(\alpha)$, nämlich ist

$$c = \zeta(\zeta^{-1}(c)) = \zeta(\iota(a)) = \alpha(a).$$

Sei nun umgekehrt eine kurze exakte Sequenz

$$0 \to A \xrightarrow{\alpha} C \xrightarrow{\gamma} B \to 0$$

gegeben. Es gilt nun einen Isomorphismus $\zeta : A \oplus B \to C$ zu finden. Dazu wähle man eine Basis $(b_i)_{i \in I}$ und für jedes dieser Elemente ein Urbild $c_i \in C$ unter γ, also $\gamma(c_i) = b_i$ (dies ist möglich da γ surjektiv ist). Das erlaubt uns eine K-lineare Abbildung $\beta : B \to C$ zu definieren, indem wir $\beta(b_i) := c_i$ setzen. (Es genügt Bilder der Basiselemente anzugeben,

wir können β dann eindeutig zu eine linearen Abbildung fortsetzen). Wir definieren nun $\zeta : A \oplus B \to C$ durch

$$\zeta(a,b) := \alpha(a) + \beta(b).$$

Offenbar ist ζ linear, es gilt also noch Bijektivät zu zeigen.
Injektivität: Sei $\zeta(a,b) = \alpha(a) + \beta(b) = 0$. Dann ist $\gamma(\alpha(a) + \beta(b)) = 0$. Nun ist zum Einen $\gamma(\alpha(a)) = 0$, denn $\gamma \circ \alpha = 0$ wegen der Komplexeigenschaft, zum Anderen ist $\gamma(\beta(b)) = b$ per Definition von β. Damit folgt:

$$0 = \gamma(\alpha(a) + \beta(b)) = \gamma(\alpha(a)) + \gamma(\beta(b)) = b.$$

Dies ergibt $0 = \alpha(a) + \beta(b) = \alpha(a) + \beta(0) = \alpha(a)$, was $a = 0$ impliziert, da α laut Lemma 2.3.23 injektiv ist.
Surjektivität: Sei $c \in C$ und betrachte $c - \beta(\gamma(c)) \in C$. Da

$$\gamma(c - \beta(\gamma(c))) = \gamma(c) - \gamma(c) = 0 \in B$$

ist, haben wir, dass $c - \beta(\gamma(c)) \in \mathsf{Ker}(\gamma) = \mathsf{Bild}(\alpha)$, wegen Exaktheit. Somit gibt es ein $a \in A$, sodass $\alpha(a) = c - \beta(\gamma(c))$. Dann gilt aber

$$\zeta(a, \gamma(c)) = \alpha(a) + \beta(\gamma(c)) = c - \beta(\gamma(c)) + \beta(\gamma(c)) = c,$$

was die Surjektivität beweist.

Sei nun $A \oplus B \simeq C$. Bei Definition der direkten Summe ist $\alpha : A \to A \oplus B \simeq C$ $(a \mapsto (a,0))$ injektiv und $\beta : C \simeq A \oplus B \to B$ $(a,b) \mapsto b$ surjektiv. Dass $\mathsf{Bild}(\alpha) = \mathsf{Ker}(\beta)$ ist auch trivial: Sei $\alpha(a) = (a,0) \in \mathsf{Bild}(\alpha)$. Dann gilt

$$\beta(\alpha(a)) = \beta(a,0) = 0 \in \mathsf{Ker}(\beta).$$

Auf der anderen Seite, sei $(a,b) \in \mathsf{Ker}(\beta)$, daher $\beta(a,b) = b = 0$. Mit anderen Worten, unser Element war $(a,0)$. Doch dies ist klar im Bild von α, da $\alpha(a) = (a,0)$. □

Bemerkung 2.3.25. Die Rückrichtung des obigen Lemmas gilt auch für beliebige Moduln, eine direkte Summenzerlegung $C \simeq A \oplus B$ impliziert immer die Existenz einer entsprechenden kurzen exakten Sequenz. Die Umkehrung gilt aber für allgemeine Moduln nicht, etwa ist $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$, dennoch existiert eine kurze exakte Sequenz mit $\mathbb{Z}/4\mathbb{Z}$ in der Mitte und $\mathbb{Z}/2\mathbb{Z}$ am Rand.

Lemma 2.3.26. *Seien A, B K-Vektorräume endlicher Dimension und $\varphi : A \to B$ eine K-lineare Abbildung.*

(i) Ist φ injektiv, so ist $\dim_K(A) \leq \dim_K(B)$.

(ii) Ist φ surjektiv, so ist $\dim_K(A) \geq \dim_K(B)$.

Beweis. (i) Sei $\{e_1, \ldots, e_n\}$ eine Basis von K und betrachte $\sum_{i=1}^{n} \lambda_i \varphi(e_i) = 0$. Wir haben $0 = \sum_{i=1}^{n} \lambda_i \varphi(e_i) = \varphi\left(\sum_{i=1}^{n} \lambda_i e_i\right)$ da φ linear ist, was wegen der Injektivität von φ, $\sum_{i=1}^{n} \lambda_i e_i = 0$ und daher $\lambda_i = 0$, $1 \leq i \leq n$ impliziert. Daher sind $\{\varphi(e_1), \ldots, \varphi(e_i)\}$ linear unabhängig und $\dim_K(B) \geq \dim_K(A)$.

(ii) Sei $\{f_1, \ldots, f_m\}$ eine Basis von B und für jeden $1 \leq i \leq m$ sei $e_i \in A$, so dass $\varphi(e_i) = f_i$. Es gelte $\sum_{i=1}^{m} \lambda_i \varphi^{-1}(f_i) = 0$. Dann ist

$$\varphi\left(\sum_{i=1}^{m} \lambda_i \varphi(e_i)\right) = \sum_{i=1}^{m} \lambda_i \varphi\left(\varphi^{-1}(f_i)\right) = \sum_{i=1}^{n} \lambda_i f_i = 0,$$

was $\lambda_i = 0$, $1 \leq j \leq m$ impliziert. Daher sind die $\lambda_i \varphi^{-1}(f_i)$'s linear unabhängig und somit ist $\dim_K(A) \geq \dim_K(A)$. □

Lemma 2.3.27. *Sei $\beta : B \to C$ eine K-lineare Abbildung. Dann ist*

$$0 \to \mathsf{Ker}(\beta) \xrightarrow{\beta_K} B \xrightarrow{\beta_B} \mathsf{Bild}(\beta) \to 0$$

eine kurze exakte Sequenz von Vektorräumen und daher $B \simeq \mathsf{Ker}(\beta) \oplus \mathsf{Bild}(\beta)$. Hier sind β_K und β_B die kanonischen Abbildungen.

Beweis. Zuerst beschreiben wir die Abbildungen genauer. Zum Einen haben wir die Injektion $\beta_K : \mathsf{Ker}(\beta) \hookrightarrow B$, induziert von der Inklusion $\mathsf{Ker}(\beta) \subseteq B$ des Kerns von β in B und zum Anderen die Surjektion $\beta_B : B \twoheadrightarrow \mathsf{Bild}(\beta)$, welche $b \in B$ auf $\beta(b) \in \mathsf{Bild}(\beta) \subseteq C$ abbildet. Wir erhalten eine Sequenz

$$0 \to \mathsf{Ker}(\beta) \hookrightarrow B \twoheadrightarrow \mathsf{Bild}(\beta) \to 0,$$

welche offenbar kurzexakt ist, denn per Konstruktion ist β_K injektiv, β_B surjektiv und offenbar gilt $\mathsf{Ker}(\beta_B) = \mathsf{Ker}(\beta) = \mathsf{Bild}(\beta_K)$. Schließlich gibt uns Lemma 2.3.24 die Isomorphie $B \simeq \mathsf{Ker}(\beta) \oplus \mathsf{Bild}(\beta)$. □

Korollar 2.3.28. *Sei $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ exakt bei B. Es gilt*

(i) $\dim_K(A) \geq \dim_K(\mathsf{Ker}(\beta))$*, mit Gleichheit genau dann, wenn α injektiv ist,*

(ii) $\dim_K(B/\mathsf{Bild}(\alpha)) \leq \dim_K(C))$*, mit Gleichheit genau dann, wenn β surjektiv ist,*

(iii) $\dim_K(C) + \dim_K(A) = \dim_K(B)$ *genau dann, wenn*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

kurzexakt ist.

Beweis. Exaktheit bei B bedeutet, dass $\mathsf{Bild}(\alpha) = \mathsf{Ker}(\beta)$.
(i) Da $A \to \mathsf{Bild}(\alpha)$ surjektiv ist, besagt Teil (ii) von Lemma 2.3.26, dass

$$\dim_K(A) \geq \dim_K(\mathsf{Bild}(\alpha)) = \dim_K(\mathsf{Ker}(\beta)).$$

Die Abbildung α ist genau dann injektiv, wenn $A \simeq \mathsf{Bild}(\alpha)$, was wiederum genau dann gilt, wenn die Dimensionen gleich sind.

(ii) [*Diesen Teil erwähnen wir nur der Vollständigkeit halber, in Symmetrie zur ersten Aussage. Es sei außerdem gesagt, dass der Vektorraum $B/\mathsf{Bild}(\alpha)$ als der Kokern von α bezeichnet wird.*] Aus Exaktheit bei B folgt $B/\mathsf{Bild}(\alpha) = B/\mathsf{Ker}(\beta)$, was laut Lemma 2.3.27 gleich $\mathsf{Bild}(\beta)$ ist. Dies ist nun genau dann gleich C, wenn β surjektiv ist.

(iii) Sei die Sequenz exakt. Von Lemma 2.3.24 wissen wir direkt, dass $B \simeq A \oplus C$, was nun die Gleichheit der Dimensionen durch Lemma 2.3.17 impliziert. Die andere Richtung ist die sogenannte *Eulerformel* aus der Homologietheorie. Wer werden dies im Kurs weder beweisen, noch benutzen. □

Proposition 2.3.29. *Sei* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D \longrightarrow 0$ *exakt. Dann gilt*

$$\dim_K(A) - \dim_K(B) + \dim_K(C) - \dim_K(D) = 0.$$

Beweis. Durch wiederholte Anwendung von Lemma 2.3.27 erhalten wir folgende kurze exakte Sequenzen:

$$0 \longrightarrow \mathsf{Ker}(\alpha) \longrightarrow A \longrightarrow \mathsf{Bild}(\alpha) = \mathsf{Ker}(\beta) \longrightarrow 0$$

$$0 \longrightarrow \mathsf{Ker}(\beta) \longrightarrow B \longrightarrow \mathsf{Bild}(\beta) = \mathsf{Ker}(\gamma) \longrightarrow 0$$

$$0 \longrightarrow \mathsf{Ker}(\gamma) \longrightarrow C \longrightarrow \mathsf{Bild}(\gamma) = \mathsf{Ker}(D \to 0) \longrightarrow 0$$

$$0 \longrightarrow \mathsf{Ker}(D \to 0) \longrightarrow D \longrightarrow \mathsf{Bild}(D \to 0) \longrightarrow 0.$$

Dabei gelten die Gleichheiten der Form $\mathsf{Bild} = \mathsf{Ker}$ wegen Exaktheit der gegebenen Sequenz. Teil (iii) von Korollar 2.3.28 besagt nun

$$\begin{aligned}
\dim_K(A) &= \dim_K(\mathsf{Ker}(\alpha)) + \dim_K(\mathsf{Ker}(\beta)) \\
\dim_K(B) &= \dim_K(\mathsf{Ker}(\beta)) + \dim_K(\mathsf{Ker}(\gamma)) \\
\dim_K(C) &= \dim_K(\mathsf{Ker}(\gamma)) + \dim_K(\mathsf{Ker}(D \to 0)) \\
\dim_K(D) &= \dim_K(\mathsf{Ker}(D \to 0)) + \dim_K(\mathsf{Bild}(D \to 0)).
\end{aligned}$$

Da $\mathsf{Ker}(\alpha) = 0$ (da $0 \to A \to \cdots$ exakt und daher α injektiv ist), $\mathsf{Ker}(D \to 0) = D$ und $\mathsf{Bild}(D \to 0) = 0$, erhalten wir

$$\begin{aligned}
\dim_K(A) - \dim_K(B) + \dim_K(C) - \dim_K(D) &= 0 + \dim_K(\mathsf{Ker}(\beta)) - [\dim_K(\mathsf{Ker}(\beta)) + \dim_K(\mathsf{Ker}(\gamma))] \\
&+ \dim_K(\mathsf{Ker}(\gamma)) + \dim_K(D) - [\dim_K(\mathsf{Ker}(D)) + 0] \\
&= 0,
\end{aligned}$$

wie gewünscht. □

2.3.3 Multiplizität eines Polynoms an einem Punkt

Wie bereits angekündigt stellen wir nun eine Beziehung zwischen der Multiplizität eines Punktes a auf einer Kurve und dem Halm an diesem Punkt her. Wir besprechen zunächst den Fall $a = 0$. Das zu a gehörige Ideal ist $(x, y) = \mathrm{I}(\{a\})$.

Lemma 2.3.30. *Sei $I = (x, y)$. Dann gilt $I^n = (x^n, x^{n-1}y, \cdots, xy^{n-1}, y^n)$.*

Beweis. Für beliebige Ideale I, J in einem beliebigen Ring mit Erzeugern $(a_\alpha)_{\alpha\in A}$, $(b_\beta)_{\beta\in B}$ wird $I \cdot J$ erzeugt von

$$(a_\alpha \cdot b_\beta)_{(\alpha,\beta)\in A\times B}.$$

Zum Beispiel, $(a, b)(c, d) = (ac, ad, bc, bd)$. □

Lemma 2.3.31. *Sei $I = (x, y) \subseteq K[x, y]$. Dann ist*

$$\dim_K \left(K[x, y]/I^n\right) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

für alle $n \in \mathbb{N}$.

Beweis. Dies ist reine Kombinatorik. Wir wissen aus Lemma 2.3.30, dass

$$I^n = \left(x^n, x^{n-1}y, \cdots, xy^{n-1}, y^n\right).$$

Mit anderen Worten enthält dieses Ideal alle Polynome vom Grad $\geq n$. Elemente des Quotientenrings werden daher von Polynomen vom Grad streng kleiner als n repräsentiert. Diese sind Linearkombinationen der folgenden Formen:

$$\left\{1, \{x, y\}, \left\{x^2, xy, y^2\right\}, \left\{x^3, x^2yx, y^2, y^3\right\} \ldots, \left\{x^{n-1}, x^{n-2}y, \ldots, xy^{n-2}, y^{n-2}\right\}\right\}.$$

Die Äquivalenzklassen dieser Formen bilden also ein Erzeugendensystem des Quotienten. Dieses ist linear unabhängig, da jede K-Linearkombination dieser Formen ein Polynom vom Grad $< n$ ist, also nicht in I^n liegt, und somit nur dann 0 ist, wenn alle Koeffizienten der Linearkombination 0 sind (x und y sind ja frei in $K[x, y]$). Das System bildet also eine Basis der Mächtigkeit $1 + 2 + 3 + 4 + \cdots + n = \sum_{i=1}^{n} i$. □

Lemma 2.3.32. *Wie gewohnt sei $I = (x, y)$. Des Weiteren schreiben wir $(I^k, f) := I^k + (f)$. Für alle $k \geq \mu := \mu_0(f)$, gilt dann*

$$\dim_K \left(K[x, y]/\left(I^k, f\right)\right) = k\mu - \frac{\mu(\mu-1)}{2}.$$

Beweis. Der dritte Isomorphiesatz für $I^k \subseteq (I^k + (f)) \subseteq K[x, y]$ liefert einen surjektiven Homomorphismus von K-Algebren

$$\phi : K[x, y]/I^k \to K[x, y]/\left(I^k + (f)\right)$$

mit Kern $(I^k + (f))/I^k$. Nach dem zweiten Isomorphiesatz ist $(I^k + (f))/I^k \cong (f)/(I^k + (f))$ als K-Vektorraum. Der erste Isomorphiesatz ergibt schließlich, dass die K-lineare Surjektion

$$\psi : K[x,y] \to (f)/(I^k + (f)), \quad g \mapsto [f \cdot g]$$

einen Isomorphismus $K[x,y]/\mathsf{Ker}(\psi) \cong (f)/(I^k + (f)$ induziert. Wir zeigen nun, dass $\mathsf{Ker}(\psi) = I^{k-\mu}$ (dies ergibt Sinn, da $k \geq \mu$): Dazu schreiben wir $f = F_\mu + F_{\mu+1} + \dots$ für gewisse Formen F_i vom Grad i. Sei nun $g \in K[x,y]$ beliebig. Wir schreiben auch g als Summe von Formen, etwa $g = G_c + \dots$ für ein $c \geq 0$. Für das Produkt fg gilt nun

$$fg = F_\mu G_c + \dots \in I^{\mu+c}.$$

Damit folgt leicht, dass $\psi(g) = 0$ genau dann wenn, $c \geq k - \mu$, woraus die gewünschte Gleichheit $\mathsf{Ker}(\psi) = I^{k-\mu}$ folgt.

Obige Situation lässt sich nun nach Lemma 2.3.27 zu der folgenden kurzen exakten Sequenz zusammenfassen:

$$0 \longrightarrow K[x,y]/I^{k-\mu} \xrightarrow{\psi} K[x,y]/I^k \xrightarrow{\phi} K[x,y]/\left(I^k + (f)\right) \longrightarrow 0 \tag{15}$$

Nach Korollar 2.3.28 (iii) gilt für die Dimensionen

$$\dim K\left(K[x,y]/\left(I^k + (f)\right)\right) = \dim_K\left(K[x,y]/I^k\right) - \dim_K\left(K[x,y]/I^{k-\mu}\right).$$

Lemma 2.3.31 schließt den Beweis ab, wir erhalten die Gleichheit

$$\dim K\left(K[x,y]/\left(I^k + (f)\right)\right) = \frac{2k\mu - \mu^2 + \mu}{2} = k\mu - \frac{\mu(\mu-1)}{2}. \qquad \square$$

Für einen allgemeinen Punkt

Lemma 2.3.33. *Sei f irreduzibel, $I = (x,y) \subseteq K[x,y]$ und $T : \mathbb{A}^2 \to \mathbb{A}^2$ die affine Transformation, welche a auf 0 abbildet. Dann gilt*

$$\mathcal{O}_a(f)/\mathfrak{m}_a^n(f) \simeq K[x,y]/\left(I^n, f^T\right)$$

für alle $n \in \mathbb{N}$, wobei f^T das Bild von f unter T, $\mathfrak{m}_a(f) \subseteq \mathcal{O}_a(f)$ das maximale Ideal des lokalen Ringes bei a sei und wir $\mathfrak{m}_a^n(f) := (\mathfrak{m}_a(f))^n$ schreiben.

Beweis. Wir haben eine Kette von Isomorphismen:

$$\begin{aligned}
\mathcal{O}_a(f)/\mathfrak{m}_a^n &\overset{(1)}{\simeq} \mathcal{O}_0(f^T)/I^n \\
&\overset{(2)}{\simeq} \left(\mathcal{O}_0/f^T\right)/I^n \\
&\simeq \mathcal{O}_0/(I^n, f^T) \\
&\simeq \left(\mathcal{O}_0/I^n\right)/f^T \\
&\overset{(3)}{\simeq} \left(K[x,y]/I^n\right)/f^T \\
&\simeq K[x,y]/(I^n, f^T)
\end{aligned}$$

Dabei gilt (1) nach Lemma 2.3.5, da sicherlich $T(\mathfrak{m}_a) = \mathfrak{m}_0 = I^n$. Nach Lemma 1.5.21 gilt (2) und schließlich folgt aus Korollar 2.3.15 die Isomorphie bei (3), da $\mathrm{V}(I^n) = \mathrm{V}(I) = \{(0,0)\}$ aus einem Punkt besteht. □

Korollar 2.3.34. *Für alle $k \geq \mu$ gilt*

$$\dim_K\left(\mathcal{O}_a(f)/\mathfrak{m}_a^k\right) = k\mu - \frac{\mu(\mu-1)}{2},$$

wobei $\mu := \mu_a(f)$ die Multiplizität von f am Punkt a ist.

Beweis. Laut den Lemmas 2.3.33 und 2.3.32 gilt

$$\dim_K\left(\mathcal{O}_a(f)/\mathfrak{m}_a^k(f)\right) = \dim_K\left(K[x,y]/\left(I^k, f^T\right)\right) = k\mu^T - \frac{\mu^T(\mu^T-1)}{2},$$

wobei $\mu^T := \mu_0(f^T)$ die Multiplizität von f^T am Punkt 0 sei. Nach Definition (2.2.14) ist aber $\mu_0(f^T) = \mu_a(f)$, was den Beweis abschließt. □

Satz 2.3.35. *Sei a ein Punkt einer irreduziblen Kurve f mit Multiplizität $\mu_a(f)$. Für ausreichend große $n \in \mathbb{N}$ gilt*

$$\mu_a(f) = \dim_K\left(\mathfrak{m}_a^n(f)/\mathfrak{m}_a^{n+1}(f)\right),$$

wobei $\mathfrak{m}_a(f) \subseteq \mathcal{O} := \mathcal{O}_a(f)$, das maximale Ideal des Halms am Punkt a ist.

Beweis. Man verwende den dritten Isomorphiesatz **??** für den Fall $R = \mathcal{O}_a(f)$, $I = \mathfrak{m}^{n+1} := \mathfrak{m}^{n+1}(f)$ und $J = \mathfrak{m}^n := \mathfrak{m}^n(f)$. Wir erhalten folgende kurze exakte Sequenz von K-Vektorräumen:

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0.$$

Nach Teil (iii) von Korollar 2.3.28 gilt für die Dimensionen

$$\dim_K\left(\mathfrak{m}^n(f)/\mathfrak{m}^{n+1}(f)\right) = \dim_K\left(\mathcal{O}_a(f)/\mathfrak{m}^{n+1}(f)\right) - \dim_K\left(\mathcal{O}_a(f)/\mathfrak{m}^n(f)\right).$$

Lemma 2.3.34 impliziert nun für alle $n \geq \mu$:

$$\begin{aligned}\dim_K\left(\mathfrak{m}^n(f)/\mathfrak{m}^{n+1}(f)\right) &= (n+1)\mu - \frac{\mu(\mu-1)}{2} - \left(n\mu - \frac{\mu(\mu-1)}{2}\right)\\ &= (n+1)\mu - n\mu\\ &= \mu\end{aligned}$$

□

Wir erhalten das folgende Korollar als eine direkte Konsequenz.

Korollar 2.3.36. *Die Multiplizität von f an a hängt nur vom Halm $\mathcal{O}_a(f)$ ab.*

2.3.4 Diskrete Bewertungsringe

Definition 2.3.37. *Ein* diskreter Bewertungsring *ist ein Hauptidealbereich R, welcher genau ein nicht-triviales Primideal $\mathfrak{p} \neq 0$ besitzt.*

Ein Ring ist genau dann ein Integritätsbereich, falls das Nullideal 0 ein Primideal ist. Ein diskreter Bewertungsring hat also genau zwei Primideale: $\mathfrak{p}$ und 0. Da R ein Hauptidealbereich ist, folgt $\mathfrak{p} = (g)$ für ein irreduzibles Element $g \in R$. Des Weiteren ist jeder diskrete Bewertungsring ein lokaler Ring mit maximalem Ideal $\mathfrak{p}$, denn $0 \subseteq \mathfrak{p}$ gilt immer. Ein beliebiges Element $r \in R$ ist daher entweder in $\mathfrak{p}$ oder in $R \setminus \mathfrak{p}$, und letzteres ist laut Korollar 1.5.4 die Menge R^* der Einheiten von R. Wir können also folgern, dass jedes Element $r \in R$ von der Form $r = ug^n$ für ein $u \in R^*$ und $n \geq 0$ ist. Dabei ist $r = u = ug^0 \in R^*$, falls $n = 0$ und $r = ug^n \in (g)$, falls $n \geq 1$.

Zur Erinnerung, in jedem Integritätsbereich R sind Primelemente irreduzibel und die Umkehrung gilt, falls R sogar ein faktorieller Ring, etwa ein Hauptidealbereich, ist. Insbesondere induzieren irreduzible Elemente in einem Hauptidealbereich Primideale. Dies erlaubt uns die obige Diskussion zu folgender Proposition zu ergänzen, welche im Wesentlichen besagt, dass wir das g von oben durch ein beliebiges irreduzibles Element ersetzen können.

Proposition 2.3.38. *Ein Integritätsbereich ist genau dann ein diskreter Bewertungsring, wenn es ein irreduzibles Element $g \in R$ gibt, so dass jedes Element $r \in R$ als $r = ug^n$, für irgendein invertierbares Element $u \in R^*$ und eine natürliche Zahl $n \geq 0$ geschrieben werden kann.*

Definition 2.3.39. *Sei R ein diskreter Bewertungsring. Dann heißt die Abbildung*

$$\mathfrak{v} : R \setminus \{0\} \to \mathbb{N} \quad \text{gegeben durch} \quad r \mapsto n,$$

wobei $r = ug^n$, mit g irreduzibel, die Bewertung *des diskreten Bewertungsrings R. Wir setzen außerdem $\mathfrak{v}(0) := \infty$.*

Dass dies eine wohldefinierte Abbildung ergibt ist Gegenstand der folgenden Proposition.

Proposition 2.3.40. *Die Auswertung von Definition 2.3.39 hängt nicht vom Wahl des irreduziblen Elements ab.*

Beweis. Sei $r = ug^n = vh^m$ für Einheiten $u, v \in R^*$ und irreduzible Elemente $g, h \in R$. Da (g) und (h) Primideale ungleich (0) sind, muss $(g) = (h)$ gelten. Es folgt, dass $g = wh$ für eine Einheit $w \in R^*$. Somit ist $ug^n = uw^n h^n$ und unsere erste Gleichung gibt uns nun $uw^n h^n = vh^m$. Durchs Kürzen erhalten wir die gewünschte Aussage. □

Proposition 2.3.41. *Sei R lokaler noetherscher Integritätsbereich mit maximalem Ideal $\mathfrak{m}$. Es ist R genau dann ein diskreter Bewertungsring, wenn $\mathfrak{m}$ ein Hauptideal ist.*

Beweis. Ein diskreter Bewertungsring R ist per Definition ein Integritätsbereich und wir haben bereits diskutiert, dass R auch ein lokaler Ring ist. Als Hauptidealbereich ist R außerdem sicherlich noethersch. Per Definition folgt dann, dass das maximale Ideal ein Hauptideal ist.

Sei also umgekehrt R ein lokaler noetherscher Integritätsbereich mit maximalem Ideal $\mathfrak{m}$, sodass $\mathfrak{m} = (g)$ ein Hauptideal ist. Wir wollen nun zeigen, dass sich jedes beliebige Element $r \in R$ als $r = ug^n$ für eine Einheit $u \in R^*$ und eine natürliche Zahl $n \geq 0$ schreiben lässt, woraus die Behauptung aus Proposition 2.3.38 folgt. Beachte dazu zunächst, dass R ein lokaler Ring ist und es daher nach Korollar 1.5.4 für ein beliebiges Element $s \in R$ zwei Möglichkeiten gibt: $s \in \mathfrak{m}$ oder $s \in R^*$. Dies erlaubt uns eine Folge von Elementen $s_i \in R$ induktiv wie folgt zu definieren: Wir setzen erst $s_0 := r$. Für $i > 0$ definieren wir dann s_i in Abhängigkeit von s_{i-1}. Ist $s_{i-1} \in \mathfrak{m} = (g)$, so existiert ein $s \in R$ mit $s_{i-1} = sg$ und wir setzen $s_i := s$. Andernfalls ist $s_{i-1} \in R^*$ invertierbar und wir setzen $s_i := s_{i-1}$. Also kurz:

$$s_0 := r \quad \text{und} \quad s_i := \begin{cases} s_{i-1}, & \text{falls } s_{i-1} \in R^* \\ s, & \text{falls } s_{i-1} = sg \in \mathfrak{m} = (g) \end{cases}$$

Wir erhalten eine absteigende Kette von Idealen

$$(r) \subsetneq (s_1) \subsetneq (s_2) \subsetneq \cdots,$$

welche stabilisiert, da R noethersch ist. Es existiert daher, per Definition der s_i, ein $n \geq 0$, sodass $u := s_n$ invertierbar ist und $s_{i-1} = s_i g$ für alle $1 \leq i \leq n$. Es folgt

$$r = s_0 = s_1 g = s_2 g^2 = \cdots = s_n g^n = ug^n \qquad \square$$

Man erinnere sich an die Isomorphie von Satz 1.5.20, welches uns eine natürliche Abbildung $\varphi : K[x_1, \ldots, x_n] \to \mathcal{O}_a(f)$ gibt. Dies ist die Komposition

$$K[x_1, \ldots, x_n] \xrightarrow{\pi} K[x_1, \ldots, x_n]/(f) = K[\mathrm{V}(f)] \to K[\mathrm{V}(f)]_{\pi(\mathfrak{m}_a)} = \mathcal{O}_a(f).$$

Satz 2.3.42. *Ein Punkt a ist genau dann regulär auf einer Kurve f, wenn $\mathcal{O}_a(f)$ ein diskreter Bewertungsring ist. Ferner, sei $l = rx + sy + t$, mit $r, s, t \in K$ eine Gerade durch a, so dass l* keine *Tangente von f an a ist. Das Bild $\varphi(l) \in \mathcal{O}_a(f)$ erzeugt das maximale Ideal von $\mathcal{O}_a(f)$.*

Beweis. Sei $a = (x_0, y_0)$ ein regulärer Punkt auf f und l eine Gerade durch a, welche nicht tangential zu f ist. Laut den Lemmas 2.3.4 und 2.3.5 können wir durch eine Koordinatentransformation annehmen, dass $a = 0 = (0, 0)$, $y = 0$ die Tangente und $l = x$ unsere angenommen Gerade ist. Von Satz 1.5.20 wissen wir, dass $\mathcal{O}_a(f)$ immer ein lokaler Ring ist. Laut Proposition 2.3.41 reicht es daher aus zu beweisen, dass $(\varphi(l)) = (\varphi(x))$ das maximale Ideal von $\mathcal{O}_a(f)$ ist. Laut Satz 1.5.20 ist das maximale Ideal $\mathfrak{m}_a = (\varphi(x), \varphi(y))$ assoziiert zum Punkt $0 = (0, 0)$ auf f. Hierzu brauchen wir noch nicht, dass f am Punkt regulär ist.

Da nach dem Variablenwechsel unsere Tangente die Gerade y ist, folgt, dass $f = F_1 + F_2 + \cdots + F_n$, wobei $F_1 = y$ gilt. Daher $f = y + \{\textit{Monomiale mit Grad} \geq 2\}$. Wir fassen alle Terme mit y zusammen und erhalten

$$f = yg - x^2 h,$$

wobei h nur Terme mit x enthält und g von der Form $1 + \textit{höhere Terme}$ ist. Da $f \equiv 0$ in $K[\mathrm{V}] = K[x,y]/\mathrm{I}(\mathrm{V})$, gilt $yg = x^2 h$ in $K[\mathrm{V}]$. Insbesondere haben wir also auch $\varphi(yg) = \varphi(x^2 h)$ in $\mathcal{O}_0(f)$, da φ ja durch $K[\mathrm{V}]$ geht (faktorisiert). Wir wissen auch, dass $g(0) \neq 0$ in $K[\mathrm{V}]$, da der konstante Term von g ja 1 war. Wir schlussfolgern, dass $\varphi(g) \in \mathcal{O}_0(f)$ eine Einheit ist. Somit gilt

$$\varphi(y) = \varphi\left(x^2 h g^{-1}\right) \in (\varphi(x)) \subseteq \mathcal{O}_0(f).$$

Daraus folgt, dass das maximale Ideal $\mathfrak{m}_a = (\varphi(x), \varphi(y))$ von $\mathcal{O}_0(f)$ gleich $(\varphi(x))$ ist, wie gewünscht.

Für die umgekehrte Seite, sei $\mathcal{O}_a(f)$ ein diskreter Bewertungsring. Daher ist das maximale Ideal $\mathfrak{m}_a = (t)$ ein Hauptideal, erzeugt von einem irreduziblen Element $t \in \mathcal{O}_a(f)$. Aus Satz 2.3.35 wissen wir, dass für ein ausreichend großes $k \in \mathbb{N}$ gilt, dass

$$\mu_a(f) = \dim_K\left(\mathfrak{m}_a(f)^k / \mathfrak{m}_a(f)^{k+1}\right) = \dim_K\left(\left(t^k\right) / \left(t^{k+1}\right)\right).$$

Es ist $(t^k) = \{r \cdot t^k \mid r \in \mathcal{O}_a(f)\}$ und $r \cdot t^k \sim s \cdot t^k$ in $(t^k)/(t^{k+1})$ genau dann, wenn $r \cdot t^k - s \cdot t^k \in (t^{k+1})$, also wenn $(r-s)\,t^k = q t^{k+1}$ für irgendein $q \in \mathcal{O}_a(f)$. Da wir in einem Integritätsbereich sind, können wir mit t^k kürzen und erhalten die Bedingung $r - s = qt$, also $r - s \in (t)$. Da r und s beliebige Elemente von $\mathcal{O}_a(f)$ gewesen sind, folgt $(t^k)/(t^{k+1}) \simeq \{r \in \mathcal{O}_a(f)\}/\sim$, wobei $r \simeq s$ genau dann wenn $r - s \in (t)$. Wir haben also

$$\left(t^k\right) / \left(t^{k+1}\right) \simeq \mathcal{O}_a(f)/(t).$$

Wir definieren eine Abbildung

$$\lambda : \mathcal{O}_a(f) \to K, \quad \frac{g}{h} \to \frac{g(a)}{h(a)}$$

Der Kern der Abbildung ist offenbar $\{g \in \mathcal{O}_a(f) \mid g(a) = 0\}$, was das maximale Ideal von $\mathcal{O}_a(f)$ ist. Es muss also $\mathsf{Ker}(\lambda) = (t)$ sein, was uns nun

$$\left(t^k\right) / \left(t^{k+1}\right) \simeq \mathcal{O}_a(f)/(t) \simeq K$$

und somit

$$\dim_K\left(\left(t^k\right) / \left(t^{k+1}\right)\right) = \dim_K(K) = 1$$

gibt. Damit hat f hat Multiplizität 1 am Punkt a für jeden $k \in \mathbb{N}$. Aus Lemma 2.2.18 folgt nun, dass f an a regulär ist. □

Wir bemerken, dass eine Gerade l', welche durch a geht, keine Einheit in $\mathcal{O}_a(f)$ sein kann, da $l'(a) = 0$ gelten muss. Daher liegt $\frac{1}{l'}$ nicht in $\mathcal{O}_a(f) = \left\{\frac{\alpha}{\beta} \mid \beta(a) \neq 0\right\}$ und wir wissen, dass das Bild unter φ, von einer Gerade durch a, im maximalen Ideal $\mathcal{O}_a(f) \setminus \mathcal{O}_a^*(f)$ liegen muss. Die Aussage des Satzes 2.3.42 können wir also wie folgt umformulieren: Eine Gerade l durch a ist genau dann eine Tangente von f an a, wenn ihr Bild unter φ ein reduzibles Element von $\mathcal{O}_a(f)$ ist.

2.4 Die Schnittzahl

Sein f, g affine planare Kurven und $a \in \mathbb{A}^2$ ein Punkt. Wir wollen die *Schnittzahl*, gezeichnet $\mathfrak{I}(a, f \cap g)$, von f und g am Punkt a definieren. Da die Definition davon jedoch nicht gerade intuitiv ist, werden wir "umgekehrt" vorangehen. Wir werden zuerst die Eigenschaften auflisten, welche wir von der Schnittzahl erwarten und dann beweisen, dass es genau eine Definition dafür gibt. Anders gesagt, wir werden es *axiomatisieren*.

Axiome der Schnittzahl

Definition 2.4.1. *Wir werden hierzu einige Definitionen brauchen, welche wir hier auflisten. Wir sagen, dass f und g sich:*

(i) eigentlich *am Punkt a schneiden, wenn f und g keine gemeinsame Komponente haben, die durch a gehen. Schriftlich ausgedrückt: Aus $f = f'h$ und $g = g'h$ folgt, $h(a) \neq 0$.*

(ii) transversal *am Punkt a schneiden, wenn sowohl f wie auch g regulär an a sind und verschiedene Tangenten haben. Sprich: $\mu_a(f^T) = \mu_a(g^T) = 1$ und $f_x(a) \neq g_x(a)$ oder $f_y(a) \neq g_y(a)$.*

Eigenschaften der Schnittzahl 2.4.2. *Wir wollen, dass die Schnittzahl folgende Eigenschaften erfüllt:*

(1) Die Auswertung $\mathfrak{I}(a, f \cap g) \in \mathbb{N}$ ist genau dann eine natürliche Zahl, wenn f und g sich eigentlich am Punkt a schneiden. Es ist $\mathfrak{I}(a, f \cap g) = \infty$ genau dann, wenn f und g sich nicht *eigentlich schneiden.*

(2) Die Schnittzahl $\mathfrak{I}(a, f \cap g)$ hängt nur von den Komponenten von f und g ab, welche durch den Punkt a laufen und $\mathfrak{I}(a, f \cap g) = 0$ genau dann, wenn $a \notin f \cap g$.

(3) Seins $T : \mathbb{A}^2 \to \mathbb{A}^2$ ein affines Variablenwechsel und $a, b \in \mathbb{A}^2$ Punkte mit $T(b) = a$. Dann gilt

$$\mathfrak{I}(a, f \cap g) = \mathfrak{I}(g, f^T \cap g^T).$$

(4) Es gilt $\mathfrak{I}(a, f \cap g) = \mathfrak{I}(a, g \cap f)$.

(5) Es gilt

$$\mathfrak{I}(a, f \cap g) \geq \mu_a(f)\mu_a(g).$$

Gleichheit hält genau dann, wenn f und g keine gemeinsamen Tangenten am Punkt a haben. Die Schnittzahl ist also genau dann 1, wenn f und g sich transversal schneiden.

(6) Sein $f = \prod f_i^{r_i}$ und $g = \prod g_j^{s_j}$. Wir haben

$$\mathfrak{I}(a, f \cap g) = \sum_{i,j} r_i s_j \mathfrak{I}(a, f_i \cap g_j).$$

(7) Für jedes Polynom $h \in K[x, y]$ gilt

$$\mathfrak{I}(a, f \cap g) = \mathfrak{I}(a, f \cap (g + hf)).$$

Vorbereitende Lemmas Es sei erwähnt, dass dies *nicht* eine minimale Eigenschaftsliste darstellt. Wir hätten uns einiges sparen und/oder vereinfachen können. Aber es ist einfacher/geschickter dies so zu beweisen und dann auch später auszurechnen. Wir werden aber vorerst einige Lemmas beweisen, welche wir für den Beweis des folgendes Satzes brauchen werden.

Lemma 2.4.3. *Sein $f, g \in K[x,y]$ teilerfremde Polynome. Dann ist*

$$\sum_{a_i \in f \cap g} \dim_K \left(\mathcal{O}_{a_i}/(f,g)\right) = \dim_K \left(K[x,y]/(f,g)\right) < \infty.$$

Beweis. Die erste Gleichung ist Korollar 2.3.14. Von Satz 2.1.2 wisen wir, dass $\mathrm{V}(f,g) < \infty$. Daher besagt Korollar 1.2.47, dass $\dim_K \left(K[x,y]/(f,g)\right) < \infty$. □

Lemma 2.4.4. *Sein f, g Polynome, so dass sie keine gemeinsame Tangente am Punkt $a \in f \cap g$ haben. Dann haben sie keinen gemeinsamen Teiler h, mit $a \in h$.*

Beweis. Als aller erstes benutzen wir Lemma 2.3.5 um anzunehmen, dass der Punkt $a = 0$ ist. Dann wissen wir, dass $f = F_m + F_{m+1} + \cdots$ und $g = G_n + G_{n+1} + \cdots$ wie folgt als Formen aussehen, mit $m, n \geq 1$. Man nehmen an, f und g hätten einen gemeinsamen Teiler $h = H_k + H_{k+1} + \cdots$ mit $a \in h$, daher $k \geq 1$. Also, $f = hf'$ und $g = hg'$. Da die Minimalformen des Produkts gleich dem Produkt der Minimalformen ist, wissen wir, dass $F_m = H_k F'_{m-k}$ und $G_n = H_k G_{n-k}$. Dies führt nun zum Widerspruch indem wir H_k als Produkt von irreduziblen Komponenten darstellen, da diese nun gemeinsame Tangenten von f und g am Nullpunkt sind. □

Lemma 2.4.5. *Sein $L_1, L_2, \ldots$ und $M_1, M_2 \ldots$ Sequenzen von Linearformen (Formen Grad 1) in $K[x,y]$, so dass keine L_i proportional zu einem M_j ist. Daher, es gibt kein L_i, so dass $L_i = \lambda M_j$ für irgendein j oder $\lambda \in K$. Sei $A_{ij} = L_1 L_2 \cdots L_i M_1 M_2 \cdots M_j$, $i, j \geq 0$ ($A_{00} = 1$). Dann ist $\{A_{ij} \mid i + j = d\}$ eine Basis vom Ideal I^d, wobei $I = (x,y)$.*

Beweis. Als erstes erinnern wir uns, dass $I^d = (x^d, x^{d-1}y, \ldots, y^d)$ (Lemma 2.3.30). Betrachte das Vektorraum V_d, erzeugt mit $\{x^d, x^{d-1}y, \ldots, y^d\}$ und das Vektorraum W_d, erzeugt mit den A_{ij}'s, so dass $i + j = d$. Es ist klar, dass $W_d \subseteq V_d$, da A_{ij} mit $i + j = d$ ein Polynom vom Grad d ist und daher eine Lineare Kombination der Erzeuger von I^d.

Wir behaupten, dass $V_d = W_d$. Es ist klar, dass $\{x^d, x^{d-1}y, \ldots, y^d\}$ eine Basis darstellen. Da es auch genau $d + 1$ verschiedene solche A_{ij}'s gibt, ist das einzige, was wir zu beweisen haben, dass die A_{ij}'s linear Unabhängig sind.

Sein daher $\alpha_0, \ldots, \alpha_d \in K$, so dass

$$\alpha_0 A_{0,d} + \alpha_1 A_{1,d-1} + \alpha_2 A_{2,d-2} + \cdots + \alpha_d A_{d,0} = 0,$$

also

$$\alpha_0 M_1 \cdots M_d + \alpha_1 L_1 M_1 \cdots M_{d-1} + \alpha_2 L_1 L_2 M_1 \cdots M_{d-2} + \cdots + \alpha_d L_1 \cdots L_d = 0. \tag{16}$$

Da L_1 vom Grad 1 ist und daher nicht stetig Null, hat es eine (unendlich viele) Nullstelle, $(x_0, y_0) \neq (0,0)$. Man werte nun Gleichung (16) an diesem Punkt aus und erhalte

$$\alpha_0(M_1 \cdots M_d)(x_0, y_0) + L_1(\cdots)(x_0, y_0) = \alpha_0(M_1 \cdots M_d)(x_0, y_0) = 0.$$

Eine Gerade wird mit zwei Punkten definiert und alle M_i und L_i Formen sind, daher gehen diese durch $(0,0)$. Da $M_j \neq \lambda L_1$, folgt, dass $M_j(x_0, y_0) \neq 0$ für alle $1 \leq i, j \leq d$. Es muss also $\alpha_0 = 0$ gelten. Als solches können wir Gleichung (16) zu

$$\alpha_1 L_1 M_1 \cdots M_{d-1} + \alpha_2 L_1 L_2 M_1 \cdots M_{d-2} + \cdots + \alpha_d L_1 \cdots L_d = 0$$

vereinfachen. Da $L_1 \neq 0$ können wir dadurch kürzen und erhalten

$$\alpha_1 M_1 \cdots M_{d-1} + \alpha_2 A_{2,d-2} L_2 M_1 \cdots M_{d-2} + \cdots + \alpha_d L_2 \cdots L_d = 0.$$

Man wiederhole das selbe Spiel und erhalte $\alpha_k = 0$ für alle $0 \leq k \leq d$, was lineare Unabhängigkeit und damit $V_d = W_d$ beweist.

Das Lemma folgt nun direkt, da wir also jedes der Erzeuger von I^d als eine lineare Kombination der A_{ij}'s darstellen können. □

Lemma 2.4.6. *Sein f und g Kurven ohne gemeinsame Tangente am Punk a. Dann gilt $\mathfrak{m}_a^k \subseteq (f,g) \subseteq \mathcal{O}_a$ für alle $k \geq m + n - 1$.*

Beweis. Sei, o. B. d. A. $a = 0$ und $\mathfrak{m}_a = I = (x, y) \subseteq K[x, y]$. Ferner, schreibe $\mu_a(f) = m$, $\mu_a(g) = n$. Wir werden als erstes beweisen, dass es irgend einen $N \in \mathbb{N}$ gibt mit $I^N \subseteq (f,g) \subseteq \mathcal{O}_a$. Danach werden wir beweisen, dass man $N = m + n - 1$ nehmen kann. Dass die höheren Potenzen im Ideal liegen werden ist klar.

Schritt 1: Es gibt ein $N \in \mathbb{N}$ mit $I^N \subseteq (f,g) \subseteq \mathcal{O}_a$.

Sei $a \notin f$. Dann ist $f \in \mathcal{O}_a^*$ eine Einheit. Somit ist $(f,g) = \mathcal{O}_a^*$ und das Lemma wird trivial erfüllt. Gleichwie für g. Wir können daher annehmen, dass $a \in f \cap g$.

Sei $h = \mathtt{ggt}(f,g)$ der größte gemeinsame Teiler. Daher, $f = f'h$ und $g = g'h$, mit f', g' teilerfremd. Lemma 2.4.4 besagt $h(a) \neq 0$, was $a \in \mathrm{V}(f', g')$ und $h \in \mathcal{O}_a^*$ impliziert. Es folgt $(f,g) = (hf', hg') = (f', g')$. Zudem ist $\mathrm{V}(f', g')$ endlich laut Lemma 2.1.2. Wir folgern

$$\mathrm{V}(f', g') = \{a, b_1 \cdots, b_s\} \quad \text{mit} \quad b_i \neq a, 1 \leq i \leq s.$$

Laut Lemma 1.2.45 gibt es ein Polynom h', so dass

$$\begin{cases} h'(a) \neq 0 & \Rightarrow\ h'(a) \in \mathcal{O}_a^* \\ h'(b_1) = 0 \quad \text{für alle} \quad 1 \leq i \leq s & \Rightarrow\ h'x, h'y \in \mathrm{I}(\mathrm{V}(f', g')). \end{cases}$$

Für den zweiten Teil erinnere man sich, dass $a = (0,0)$, daher $x(a) = y(a) = 0$. Aus $h'x, h'y \in \mathrm{I}(\mathrm{V}(f', g'))$ folgt von Hilberts Nullstellensatz 1.2.43 Teil (iii), dass es eine $N \in \mathbb{N}$ gibt, mit $(h'x)^N, (h'y)^N \in (f', g') \subseteq K[x, y]$. Da $h' \in \mathcal{O}_a^*$, folgt $x^N, y^N \in (f', g') = (f, g) \subseteq \mathcal{O}_a$.

Man betrachte die Erzeuger von $I^{2N} = (x^{2N}, x^{2N-1}y, \ldots, xy^{2N-1}, y^{2N})$. In jedem dieser Erzeuger ist entweder die Potenz von x oder die von y größer oder gleich N. Daher impliziert $x^N, y^N \in (f,g) \subseteq \mathcal{O}_a$, dass $I^{2N} \subseteq (f,g) \subseteq \mathcal{O}_a$. Damit haben wir bewiesen, dass es eine genügend große Potenz von I gibt, welches in (f,g) liegt.

Schritt 2: Für alle $k \geq m+n-1$, ist $I^k \subseteq (f,g)$ genau dann, wenn $I^{k+1} \subseteq (f,g)$.

Die eine Seite ist trivial: Aus $I^k \subseteq (f,g)$ folgt natürlich, dass $I^{k+1} \subseteq (f,g)$. Für die andere Seite, sein $L_1, \ldots, L_m$ die Tangenten von f und $M_1, \ldots, M_n$ die Tangenten von g an a. Da wir aber mehr Geraden als nur die oben gegeben brauchen werden, wiederholen wir einfach die letzten Einträge in den jeweiligen Listen. Präziser, wir definieren $L_i = L_m$, für alle $i \geq m$ und $M_j = M_n$ für alle $j \geq n$. Wir schreiben $A_{ij} = L_1 \cdots L_i M_1 \cdots M_j$ für alle $i, j \geq 0$ ($A_{00} = 1$). Laut Lemma 2.4.5 formt die Menge $\{A_{ij} \mid i+j = d\}$ eine Basis von I^d für alle $d \geq 0$. Da ein Ideal genau dann in ein anderes liegt, wenn dessen Erzeuger darin liegen, ist $I^k \subseteq (f,g)$ genau dann, wenn $A_{ij} \in (f,g) \subseteq \mathcal{O}_a$, für alle (i,j) mit $i+j = k \geq m+n-1$.

Es ist klar, dass wenn $i+j \geq m+n-1$ gilt, dann $i \geq m$ oder $j \geq n$ gelten muss, da aus $i < m$ und $j < n$, $i+j \leq m+n-2$ folgt. O. B. d. A., sei $i \geq m$. Dann ist $A_{ij} = L_1 \cdots L_m \cdots L_i M_1 \cdots M_j = A_{m0} B$, wobei $B = L_{m+1} \cdots L_i M_1 \cdots M_j$. Hier erinnere man sich, dass $L_{m+1} \cdots L_i = (i-m) L_m$, was uns

$$A_{ij} = A_{m0} L_m^{i-m} M_1 \cdots M_j$$

gibt. Man schreibe $f = F_m + F_{m+1} + \cdots$. Dann ist $F_m = A_{m0}$, da die Tangenten am Punkt $a = 0 = (0,0)$ genau die Teiler von F_m sind. Wir bezeichnen $f' := F_{m+1} + \cdots$, was uns $f = A_{m0} + f'$ gibt, wobei alle Terme von f' nun Grad größer gleich $m+1$ haben. Dann ist $A_{m0} = f - f'$, was uns

$$A_{ij} = fB - f'B$$

gibt. Jeder Term von B ist vom Grad $i-m+j$ (Produkt von eben so vielen Geraden ohne freie Terme). Alle Terme von f' sind vom Grad $m+1$ oder größer. Es folgt, dass die Terme von $f'B$ vom Grad größer gleich $(m+1)+(i-m+j) = i+j+1$ sind. Als soles ist $f'B \in I^{k+1} \subseteq (f,g)$, wobei die Inklusion unsere ursprüngliche Annahme ist.

Weil $f \in (f,g)$, ist auch $fB \in (f,g)$. Damit ist $A_{ij} \in (f,g)$ genau dann, wenn $f'B \in (f,g)$. Das letztere haben wir bewiesen und somit auch unseren zweiten Schritt. Triviale Induktion beweist nun unseren Lemma. □

Definition und Beweis der Schnittzahl

Satz 2.4.7. *Es gibt genau eine Schnittzahl $\mathfrak{I}(a, f \cap g)$, definiert für alle planare Kurven f, g und alle Punkte $a \in \mathbb{A}^2$, welche die Eigenschaften (1)-(7) von der Liste 2.4.2 erfüllt. Es ist gegeben durch*

$$\mathfrak{I}(a, f \cap g) := \dim_K \left(\mathcal{O}_a / (f,g) \right).$$

Beweis der Eindeutigkeit. Sein $f, g \in K[x,y]$ fixiert, $a \in \mathbb{A}^2$ ein Punkt und $\mathfrak{I}_1(a, f \cap g)$, $\mathfrak{I}_2(a, f \cap g)$ zwei solche Zuordnungen, die alle Eigenschaften in 2.4.2 erfüllen. Wir wollen beweisen, dass $\mathfrak{I}_1(a, f \cap g) = \mathfrak{I}_2(a, f \cap g)$.

Laut Eigenschaft (3) wissen wir, dass $\mathfrak{I}_1(a, f \cap g) = \mathfrak{I}_2(a, f \cap g)$ genau dann, wenn $\mathfrak{I}_1(0, f^T \cap g^T) = \mathfrak{I}_2(0, f^T \cap g^T)$, wobei $0 = (0,0) \in \mathbb{A}^2$. Wir müssen also nur diesen Fall beweisen. Nach Umbenennung sei $f^T = f$ und $g^T = g$.

Laut Eigenschaft (1) wissen wir, dass $\mathfrak{I}_1(0, f \cap g)$ und $\mathfrak{I}_2(0, f \cap g)$ beide Werte in $\mathbb{N} \cup \{\infty\}$ annehmen. Es gelte, dass $\mathfrak{I}_1(0, f \cap g) = \infty$. Laut Eigenschaft (1) schneiden f und g sich *nicht* eigentlich am Punkt 0. Daher muss auch $\mathfrak{I}_2(0, f \cap g) = \infty$ gelten. Den Fall, wenn f und g einen gemeinsamen Teiler haben, welches durch 0 geht, haben wir damit schon abgedeckt.

Man nehme nun an, dass $\mathfrak{I}_1(0, f \cap g) = 0$. Laut Eigenschaft (2) folgt, dass $0 \notin f \cap g$, was wiederum $\mathfrak{I}_2(0, f \cap g) = 0$ durch (2) impliziert. Damit haben wir den Fall, wenn f oder g einen freien Term haben (was f oder g Konstant einschließt) abgeschlossen.

Wir nehmen von nun an, dass weder f noch g einen freien Term haben und sie keinen gemeinsamen Teiler haben, welches durch 0 geht.

Sei $\mathfrak{I}_1(0, f \cap g) = N \in \mathbb{N}$, mit $0 < N < \infty$. Wir wollen beweisen, dass $\mathfrak{I}_2(0, f \cap g) = N$. Da wir dies schon für $N = 0$ bewiesen haben, nehmen wir an, dass dies für alle $n < N$ gilt und beweisen durch Induktion, dass es auch für $n = N$ gelten muss.

Setze $y = 0$ und betrachte $f(x,0), g(x,0) \in K[x]$. Wir fassen diese als Polynome in einer Variablen auf. Sei $\mathsf{grad}(f(x,0)) = r$ und $\mathsf{grad}(g(x,0)) = s$. Aufgrund von Eigenschaft (4) können wir annehmen, dass $r \leq s$.

Fall 1: $r = 0$. Dann muss $y \mid f$, da f keine freie x-Komponente hat und daher ansonsten konstant wäre. Wir schlussfolgern, dass $f = yh, h \in K[x, y]$. Es folgt

$$\mathfrak{I}_i(0, f \cap g) = \mathfrak{I}_i(0, yh \cap g) = \mathfrak{I}_i(0, y \cap g) + \mathfrak{I}_i(0, h \cap g), \quad i = 1, 2, \tag{17}$$

wobei die letzte Gleichung von (6) kommt.

Wir schreiben $g = c(x) + yd(x, y)$ indem wir alle Terme ohne y als $c(x)$ auffassen und dann y vom Rest ausklammern. Natürlich ist $c(x) = g(x, 0)$. Eigenschaft (7) besagt

$$\mathfrak{I}_i(0, y \cap g) = \mathfrak{I}_i(0, y \cap g(x, 0)).$$

Sei $g(x,0) = x^m(a_0 + a_1x + \cdots + a_{s-m}x^{s-m})$. Wir klammern also x mit dessen maximalen Potenz raus. Wenn $a_0 = 0$, dann muss $g(x,0) = 0$, was eines von zwei Möglichkeiten impliziert: $g = 0$ oder $y \mid g$. Im ersten Fall ist $\mathrm{V}(g) = \mathbb{A}^2$, was keine Kurve ist und im zweiten haben f und g eine gemeinsame Komponente welches durch 0 geht: y, was unserer Annahme widerspricht. Es folgt, dass $a_0 \neq 0$. Wir erhalten

$$\mathfrak{I}_i(0, y \cap g) = \mathfrak{I}_i(0, y \cap g(x,0)) = \mathfrak{I}_i(0, y \cap x^m(a_0 + a_1x + \cdots)) = \mathfrak{I}_i(0, y \cap x^m) + \mathfrak{I}_i(0, y \cap (a_0 + a_1x + \cdots)).$$

Da $a_0 \in K$ eine Konstante ist (ungleich Null), kann 0 ja nicht eine Nullstelle von $a_0 + a_1x + \cdots$ sein. Daher ist $\mathfrak{I}(0, f \cap (a_0 + a_1x + \cdots)) = 0$ laut (2). Wir erhalten

$$\mathfrak{I}_i(0, y \cap g) = \mathfrak{I}_i(0, y \cap x^m) = m\mathfrak{I}_i(0, y \cap x)$$

von (6) und da sich x und y natürlich transversal schneiden ist $\mathfrak{I}_i(0, x \cap y) = 1$, laut (5). Es folgt, dass $\mathfrak{I}_1(0, y \cap g) = m = \mathfrak{I}_2(0, y \cap g)$. Wenn $m = 0$, dann gilt entweder $y \mid g(x, 0)$ (was nicht erlaubt ist, wie vor einigen Zeilen besprochen) oder $0 \notin g$, was auch nicht erlaubt ist, da g sonst einen freien Term hätte. Wir haben also $\mathfrak{I}_i(0, y \cap g) = m > 0$, was laut Formel (17) und der Annahme, dass $\mathfrak{I}_i(0, f \cap g) = N$,

$$\mathfrak{I}_i(0, h \cap g) < N$$

impliziert. Von der Induktionsannahme folgt $\mathfrak{I}_1(0, h \cap g) = \mathfrak{I}_2(0, h \cap g)$, was laut Formel (17) die Gleichung $\mathfrak{I}_2(0, f \cap g) = \mathfrak{I}_1(0, f \cap g) = N$ impliziert.

Fall 2: $r \geq 1$. Da wir über einen Körper sind, ist es klar (es folgt von Eigenschaften (6) und (2)), dass wir annehmen können, dass $f(x, 0)$ und $g(x, 0)$ normiert sind (Leitkoeffizienten sind 1). Wir definieren $h := g - x^{s-r} f$. Eigenschaft (7) gibt uns

$$\mathfrak{I}(0, f \cap h) = \mathfrak{I}(0, f \cap g - x^{s-r} f) = \mathfrak{I}(0, f \cap g).$$

Des weiteren ist $\mathsf{grad}(h(x, 0)) < s$, da sich die Leitkoeffizienten von $g(x, 0)$ und $x^{s-r} f(x, 0)$ ja wegmachen. Man wiederhole nun dieses Prozess für f und h (sollte der Grad von h unter dem Grad von f fallen, dann muss man f als das neue g sehen und h als das neue f) bis wir uns im ersten Fall ($r = 0$) befinden. Dies schließt unseren Beweis für die Eindeutigkeit ab. □

Beweis der Existenz. Wir definieren $\mathfrak{I}(a, f \cap g) := \dim_K (\mathcal{O}_a / (f, g)) = \dim_K (\mathcal{O}_a / (f, g)\, \mathcal{O}_a)$ (die letzte Gleichung ist nur eine Verkürzung der Schreibweise) und müssen beweisen, dass alle 7 Eigenschaften der Schnittzahl 2.4.2 erfüllt werden.

(3) Dies folgt direkt von Lemma 2.3.5. Wenn gewollt können wir daher annehmen, dass $a = 0$.

(4) Dies ist direkt klar.

(1) Das $\dim_K (\mathcal{O}_a/(f, g)) \in \mathbb{N} \cup \{\infty\}$ ist klar. Schneide sich f eigentlich mit g am Punkt a, sprich, aus $f = f'h$ und $g = g'h$ folge $h(a) \neq 0$, was äquivalent zu $h \in \mathcal{O}_a^*$ ist. Dann ist aber

$$(f, g) = (f'h, g'h) = (f', g')(h) = (f', g')$$

und somit können wir f, g teilerfremd annehmen. Für f, g teilerfremd besagt Lemma 2.4.3 aber wie gewollt

$$\sum_{a_i \in f \cap g} \dim_K (\mathcal{O}_{a_i}/(f, g)) < \infty.$$

Sei wiederum $f = f'h$ und $g = g'h$ mit $h(a) = 0$. Es folgt, dass h keine Konstante ist und somit ist es als Produkt von irreduziblen darstellbar. Sei daher $h = h_1^{e_1} \cdots h_s^{e_s}$ eine Zerlegung in Irreduziblen. Über einen Integritätsbereich kann man o. B. d. A.

sagen, dass $h_1(a) = 0$. Sei $\hat{h} := h_1^{e_1-1} \cdots h_s^{e_s}$ und $\hat{f} = f'\hat{h}$, $\hat{g} = g'\hat{h}$. Dann gilt $f = \hat{f}h_1$ und $g = \hat{g}h_1$ mit $h_1(a) = 0$. Aus den zwei Gleichungen folgt direkt $(f) \subseteq (h_1)$, $(g) \subseteq (h_1)$ also $(f, g) \subseteq (h_1)$, woraus wir

$$\dim_K (\mathcal{O}_a/(f, g)) \geq \dim_K (\mathcal{O}_a/(h))$$

schließen können (Lemma 2.3.26, Teil (ii)). Aus h_1 irreduzibel folgt laut Lemma 1.5.21

$$\dim_K (\mathcal{O}_a/(h)) = \dim_K(\mathcal{O}_a(h)) \geq \dim_K (K[h]) = \infty,$$

wobei die Ungleichung Teil (i) von Lemma 2.3.26 ist. Die letzte Gleichung ist Korollar 1.2.47, da laut Lemma 1.1.8 $\mathrm{V}(h)$ eine unendliche Menge ist.

(2) Sei $g = g'h$ mit $a \in g'$ und $a \notin h$. Da $a \notin h$, folgt, dass $h \in \mathcal{O}_a^*$ eine Einheit ist. Als solches gilt $(f, g) = (f, g'h) = (f, g')$ als Ideale von $\mathcal{O}_a$, was

$$\mathcal{O}_a/(f, g) = \mathcal{O}_a/(f, g')$$

impliziert. Somit hängt die Schnittzahl nur von der Komponente ab, auf der a liegt.

Für den weiteren Teil der Aussage merke man, dass

$$0 = \mathfrak{I}(a, f \cap g) = \dim_K (\mathcal{O}_a/(f, g))$$

genau dann, wenn $(f, g) = \mathcal{O}_a$. Wir wollen zeigen, dass dies genau dann passiert, wenn $a \notin f \cap g$. Sei dazu $(f, g) = \mathcal{O}_a$, sprich geben $r, s \in \mathcal{O}_a$, so dass $1 = fr + gs$. Da laut Korollar **??** in einem Lokalring entweder t oder $1 - t$ eine Einheit sein müssen, merken wir, dass aus $rf \notin \mathcal{O}_a^*$, $1 - rf = sg \in \mathcal{O}_a^*$ liegen muss. Somit ist entweder f oder g eine Einheit in $\mathcal{O}_a$ und kann daher nicht auf a Null werden.

Wenn andersrum $a \notin f \cap g$, also ohne Verlust der Allgemeinheit $a \notin f$, folgt, dass $f \in \mathcal{O}_a^*$ eine Einheit ist. Also, dass $(f) = (1) = \mathcal{O}_a$. Da $(f) \subseteq (f, g)$ ist $\mathcal{O}_a/(f, g) = \mathcal{O}_a/\mathcal{O}_a = \{0\}$, was natürlich Null dimensional über K ist.

(5) Laut Teil (3) ist O. B. d. A. $a = (0, 0)$. Seien $m = \mu_a(f)$ und $n = \mu_a(g)$ und $I = (x, y) \subseteq K[x, y]$. Man betrachte das folgende Diagramm:

$$\begin{array}{ccccccc} K[x,y]/I^m \times K[x,y]/I^n & \xrightarrow{\psi} & K[x,y]/I^{m+n} & \xrightarrow{\varphi} & K[x,y]/(I^{m+n}, f, g) & \longrightarrow & 0 \\ & & & & \downarrow \kappa & & \\ & & \mathcal{O}_a/(f,g) & \xrightarrow{\pi} & \mathcal{O}_a/(I^{m+n}, f, g) & \longrightarrow & 0, \end{array}$$

wobei $\psi(\overline{c}, \overline{d}) := \overline{cg + df}$. Hier sind $c, d \in K[x, y]$ Polynome und $\overline{c}, \overline{d}$ deren Restklassen modulo respektive I^n und I^m. Die anderen Abbildungen sind die kanonischen.

Beh. 1: Die obere Reihe ist exakt.

Da φ klar surjektiv ist (wir teilen durch ein größeres Ideal), ist das einzige was wir überprüfen müssen, dass $\mathsf{Bild}(\psi) = \mathsf{Ker}(\varphi)$.

Sei $\overline{h} \in \mathsf{Ker}(\varphi)$. Das heißt, $h \in (I^{m+n}, f, g) \subseteq K[x,y]$. Es gibt $\alpha, \beta \in K[x,y]$ und $r \in I^{m+n}$, so dass $h = r + \alpha f + \beta g$. Dann gilt $\psi(\overline{\beta}, \overline{\alpha}) = \overline{\beta g + \alpha f} = \overline{r + \alpha f + \beta g} = \overline{h}$, da $r \in I^{n+m}$ und daher in $K[x,y]/I^{n+m}$ zu Null wird. Wir haben gezeigt, dass $\mathsf{Ker}(\phi) \subseteq \mathsf{Bild}(\psi)$.

Sei nun $\overline{c}, \overline{d} \in K[x,y]/I^m \times K[x,y]/I^n$. Dann ist $\varphi\left(\psi\left(\overline{c}\overline{d}\right)\right) = \varphi\left(\overline{cg + df}\right) = 0$ in $K[x,y]/\left(I^{m+n}, f, g\right)$, da $cg + df \in (f,g) \subseteq (I^{m+n}, f, g)$. Damit ist $\mathsf{Bild}(\psi) \subseteq \mathsf{Ker}(\varphi)$, was die Gleichheit beweist.

Beh. 2: κ ist ein Isomorphismus.

Als erstes bemerken wir, dass $\mathrm{V}(I^k) = \{(0,0)\}$, $k \geq 1$. Da $\mathrm{V}\left(I^{m+n}, f, g\right) \subseteq \mathrm{V}(I^{m+n}) = \{(0,0)\}$, gilt, dass $\mathrm{V}\left(I^{m+n}, f, g\right) = \{a\} = \{(0,0)\}$ oder $\mathrm{V}(I^{m+n}, f, g) = \varnothing$. Im ersten Fall ist dies eine direkte Konsequenz vom Lemma 2.3.15. Der zweite Fall bedeutet, dass entweder $f(a) \neq 0$ oder $g(a) \neq 0$, also $f \in \mathcal{O}_a^*$ oder $g \in \mathcal{O}_a*$ eine Einheit ist. In beiden Fällen gilt $(I^{m+n}, f, g) = \mathcal{O}_a$ und damit ist $\mathcal{O}_a/\left(I^{n+m}, f, g\right) = 0$. Auf der anderen Seite sagt Teil (ii) von Hilberts Nullstellensatz ist $\mathrm{V}\left(I^{m+n}, f, g\right) = \varnothing$ genau dann, wenn $(I^{m+n}, f, g) = (1)$, was auch $K[x,t]/\left(I^{m+n}, f, g\right) = 0$ impliziert.

Laut Lemma 2.3.17 gilt

$$\dim_K\left(K[x,y]/I^m \times K[x,y]/I^n\right) = \dim_K\left(K[x,y]/I^m\right) + \dim_K\left(K[x,y]/I^n\right).$$

Korollar 2.3.28, Teil(i) von unserer Diskussion über exakte Sequenzen auf Seite p.78 besagt nun, dass

$$\dim_K\left(K[x,y]/I^m\right) + \dim_K\left(K[x,y]/I^n\right) \geq \dim_K\left(\mathsf{Ker}(\varphi)\right),$$

wobei Gleichheit genau dann gilt, wenn ψ eine Injektion ist. Von Lemma 2.3.27 und Lemma 2.3.28, Teil iii) haben wir

$$\dim_K\left(K[x,y]/\left(I^{m+n}, f, g\right)\right) = \dim_K\left(K[x,y]/I^{m+n}\right) - \dim_K\left(\mathsf{Ker}(\varphi)\right).$$

Wir fassen unsere Diskussion zusammen und erhalten

$$\begin{aligned}
\mathfrak{I}(a, f \cap g) &= \dim_K\left(O_a/(f,g)\right) \\
&\geq \dim_K\left(O_a/I^{m+n}, f, g\right) \quad \pi \text{ ist surj.} \quad \text{Lemma 2.3.26, (ii)} \\
&= \dim_K\left(K[x,y]/\left(I^{m+n}, f, g\right)\right) \quad \text{da } \alpha \text{ ein Isomorphismus ist} \\
&= \dim_K\left(K[x,y]/I^{m+n}\right) - \dim_K\left(\mathsf{Ker}(\varphi)\right) \\
&\geq \dim_K\left(K[x,y]/I^{m+n}\right) - \dim_K\left(K[x,y]/I^m\right) - \dim_K\left(K[x,y]/I^n\right) \\
&= \frac{(m+n)(m+n+1)}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2} \quad \text{Lemma 2.3.31} \\
&= mn
\end{aligned}$$

Es folgt, dass $\mathfrak{I}(a, f \cap g) \geq mn$ und das die Gleichheit genau dann hält, wenn die zwei Ungleichheiten gleich sind. Wir behaupten, dass diese genau dann der Fall ist, wenn f und g keine gemeinsamen Tangente am Punkt a haben. Die erste Gleichung hält wenn π ein Isomorphismus ist, was von Lemma 2.4.6 folgt.

Für die zweite Ungleichung, haben f und g verschiedene Tangenten am Punkt a. Wir wollen beweisen, dass ψ injektiv ist. Sein $\overline{c}, \overline{d} \in K[x,y]/I^m \times K[x,y]/I^n$ mit $\psi(\overline{c}, \overline{d}) = \psi\left(\overline{cg + df}\right) = 0$. Dann gilt $\overline{cg + df} \in I^{m+n}$, also $\mu(cg + df) \geq m + n$. Sein $c = C_r + C_{r+1} + \cdots, d = D_s + D_{s+1} + \cdots, f = F_m + F_{m+1} + \cdots$ und $G = G_n + G_{n+1} + \cdots$ die Darstellung unserer Polynome als Summe von Formen. Dann ist $cg+df = C_rG_n+D_sF_m+$ {höhere Terme}.

Hier muss $C_rG_n + D_sF_m$ nicht die Minimalform sein: Es muss keine Form sein, oder kann Null sein. Wenn es jedoch nicht Null ist, so muss die Minimalform eines der Summanden C_rG_n oder D_sF_m sein.

Behauptung: $r \geq m$ und $s \geq n$. Es gilt freilich

$$\mu(C_rG_n + D_sF_m + \cdots) = \mu(cg + df) \geq m + n. \tag{18}$$

Sei $C_rG_n + D_sF_m \neq 0$. Dann impliziert Gleichung 18 $\mu(C_rG_n) \geq m + n$ und $\mu(D_sF_m) \geq m_n$. Somit also $r + n \geq m + n$ und $s + m \geq m + n$ was also die Behauptung ergibt.

Sei $C_rG_n + D_sF_m = 0$. Da f und g keine gemeinsame Tangente am Punkt a haben, müssen G_n und F_m teilerfremd sein. Die Gleichung $C_rG_n = -D_sF_m$ impliziert daher $G_n \mid D_s$ und $F_m \mid C_r$, was $n \leq s$ und $m \leq r$ gibt, wie gewollt.

Umgekehrt, sei ψ injektiv. Wir wollen beweisen, dass f und g verschiedene Tangenten haben. Beweisen durch Widerspruch: Sei L eine gemeinsame Tangente. Daher, $F_m = LF'_{m-1}$ und $G_n = LG'_{n-1}$, wobei F'_{m-1} und G'_{n-1} Terme respektive vom Grad $m-1$ und $n-1$ sind. Dann gilt

$$\begin{aligned}
\psi\left(\overline{F'_{m-1}}, -\overline{G'_{n-1}}\right) &= \overline{F'_{m-1}g - G'_{n-1}f} \\
&= \overline{F'_{m-1}\left(G_n + G_{n+1} + \cdots\right) - G'_{n-1}\left(F_m + F_{m+1} + \cdots\right)} \\
&= \overline{F'_{m-1}\left(LG'_{n-1} + G_{n+1} + \cdots\right) - G'_{n-1}\left(LF'_{m-1} + F_{m+1} + \cdots\right)} \\
&= \overline{F'_{m-1}LG'_{n-1} - F'_{m-1}\left(G_{n+1} + \cdots\right) - G'_{n-1}LF'_{m-1} + G'_{n-1}\left(F_{m+1} + \cdots\right)} \\
&= \overline{F'_{m-1}\left(G_{n+1} + \cdots\right) - G'_{n-1}\left(F_{m+1} + \cdots\right)} \\
= 0
\end{aligned}$$

da all die Terme nun Grad $\geq n+m$ haben. Da jedoch $\left(\overline{F'_{m-1}}, -\overline{G'_{n-1}}\right) \neq 0$ in $K[x,y]/I^m \times K[x,y]/I^n$, ist ψ nicht injektiv, was unser Widerspruch ist.

(6) Es ist direkt klar, dass durch Induktion, es ausreicht, die Gleichung

$$\mathfrak{I}(a, f \cap gh) = \mathfrak{I}(a, f \cap g) + \mathfrak{I}(a, f \cap h)$$

zu beweisen. Als erstes betrachte man den Fall, wenn f und gh einen gemeinsamen Teiler d haben. Laut Eigenschaft (2) genügt es auch anzunehmen, dass a auf d liegt, da dies ja sonst keinen Einfluss nehmen würde und wir daher f und g dadurch kürzen könnten. Da jeder Faktor von d auch ein gemeinsamer Teiler von f und gh ist, kann man annehmen, dass d selber irreduzibel ist. Von Eigenschaft (1), die wir schon bewiesen haben, ist $\mathfrak{I}(a, f \cap gh) = \infty$. Es bleibt also zu zeigen, dass $\mathfrak{I}(a, f \cap g) = \infty$ oder $\mathfrak{I}(a, f \cap h) = \infty$. Da es aber in $K[x, y]$ eine eindeutige Darstellung in irreduziblen Komponenten gibt (Satz **??**), folgt aus $d \mid gh$, dass $d \mid g$ oder $d \mid h$. Damit ist eines der verlangten Schnittzahlen unendlich.

Wir können also annehmen, dass f und gh teilerfremd sind. Da $(f, gh) \subseteq (f, g)$, haben wir eine kanonische Abbildung $\mathcal{O}_a/(f, gh) \to \mathcal{O}_a/(f, g)$. Wir definieren eine Abbildung $\psi : \mathcal{O}_a/(f, h) \to \mathcal{O}_a/(f, gh)$, gegeben durch $\psi(\overline{z}) = \overline{gz}$. Dies ist wohldefiniert, da aus $z \in (f, h) \Leftrightarrow z = \alpha f + \beta h$ folgt, $zg = (\alpha g)f + (\beta)gh \in (f, gh)$. Es ist auch nicht schwer zu sehen, dass es ein K-Algebrahomomorphismus ist. Daher erhalten wir folgende K-Algebrahomomorphismen

$$0 \longrightarrow \mathcal{O}_a/(f, h) \xrightarrow{\psi} \mathcal{O}_a/(f, gh) \xrightarrow{\varphi} \mathcal{O}_a/(f, g) \longrightarrow 0\,. \tag{19}$$

Wir behaupten, dass dies eine exakte Sequenz ist.

- Als erstes zeigen wir, dass ψ injektiv ist. Sei $\psi(\overline{z}) = 0$. Dann ist $gz \in (f, gh)$, also $gz = \alpha f + \beta gh$. Da $\mathcal{O}_a$ laut Proposition 1.5.14 eine Lokalisation von $K[x, y]$ ist, gibt es ein $s \in K[x, y]$, mit $s(a) \neq 0$, so dass $s\alpha, s\beta, sz \in K[x, y]$ sind. Als solches gilt
$$g(sz - s\beta h) = gzs - gs\beta h = (\alpha f + \beta gh)s - gs\beta h = s\alpha f.$$
Da bei Annahme f und g teilerfremd sind, folgt, dass $f \mid s(z - \beta h)$. Also, es gibt ein $\delta \in K[x, y]$, so dass $f\delta = s(z - \beta h)$. Da $s(a) \neq 0$ ist $s \in \mathcal{O}_a^*$ eine Einheit und $z = \frac{f\delta}{s} + \beta h$. Daher, $z \in (f, h) \subseteq \mathcal{O}_a$, also $\overline{z} = 0$ in $\mathcal{O}_a/(f, h)$, wie gewünscht.
- Die induzierte Abbildung φ ist immer surjektiv, da $(f, gh) \subseteq (f, g)$, sieh Lemma **??**.
- Wir wollen zeigen, dass $\mathsf{Bild}(\psi) = \mathsf{Ker}(\varphi)$. Sei also $\overline{z} \in \mathcal{O}_a/(f, h)$ und betrachte $\varphi(\psi(\overline{z})) = \varphi(\overline{gz})$. Da $gz \in (f, g)$, folgt, dass $\varphi(\overline{gz}) = 0$ in $\mathcal{O}_a/(f, g)$, was $\mathsf{Bild}(\psi) \subseteq \mathsf{Ker}(\varphi)$ beweist.
Auf der andern Seite, sei $\overline{z} \in \mathsf{Ker}(\varphi)$. Daher, $z \in (f, g)$, also $z = \alpha f + \beta g$. Da $\psi(\overline{\beta}) = \overline{\beta g}$ und $z - \beta g = \alpha f \in (f, gh)$, haben wir ein Element $\overline{\beta}$ gefunden, welches auf $\overline{z}$ abbildet. Es folgt, dass $\mathsf{Bild}(\psi) \supseteq \mathsf{Ker}(\varphi)$, also gilt die Gleichheit.

Teil (iii) vom Korollar 2.3.28, angewendet auf die exakte Sequenz (19) impliziert nun die gewünschte Gleichung.

(7) Es ist eine triviale Eigenschaft aller Ideale, dass wenn $f \in I$ und $g \in I$, dann $g + hf \in I$, für alle Elemente h des Ringes. Daher gilt also $\mathcal{O}_a/(f,g) = \mathcal{O}_a/(f, g+hf)$, was unsere Gleichung impliziert.

□

Einige Korollare Wir haben auch folgendes Resultat, welches wir später noch benutzen werden:

Proposition 2.4.8. *Eine Gerade l ist genau dann eine Tangente einer Kurve f am Punkt a, wenn $\mathfrak{I}(a, f \cap l) > \mu_a(f)$ gilt.*

Beweis. Dies ist die 5-te Eigenschaft 2.4.2. Dies besagt nämlich, dass

$$\mathfrak{I}(a, f \cap l) > \mu_a(f)\mu_a(l) = \mu_a(f) \cdot 1 = \mu_a(f)$$

genau dann, wenn f und l eine gemeinsame Tangente haben. Da aber eine Gerade nur sich selbst als eine Tangente hat, ist die strickte Ungleichung genau dann, wenn l eine Tangente von f ist. □

Proposition 2.4.9. *Sein f, h teilerfremde planare Kurven, dann gilt*

$$\sum_a \mathfrak{I}(a, f \cap g) = \dim_K(K[x,y]/(f,g)),$$

wobei die Summe über alle Punkte genommen wird, wo f und g sich schneiden.

Beweis. Dies ist einfach nur Korollar 2.3.14, für $J = (f,g)$. □

Dies wird öfters auch die 8-te Eigenschaft genannt. Man kann die Summe natürlich auch über zusätzliche Punkte nähmen, da dort die Schnittzahl ja Null ist.

Die Schnittzahl im Koordinatenring

Definition 2.4.10. *Sein $f \in K[x,y]$ und $\overline{g} \in K[x,y]/(f)$. Wir definieren die* Schnittzahl

$$\mathfrak{I}(a, f \cap \overline{g}) := \mathfrak{I}(a, f \cap g),$$

wobei $g \in K[x,y]$ eine beliebige Hochhebung von $\overline{g}$ ist.

Lemma 2.4.11. *Die Schnittzahl $\mathfrak{I}(a, f \cap \overline{g})$ ist wohldefiniert.*

Beweis. Dies ist einfach nur Eigenschaft 7 der Schnittzahl 2.4.2: Präziser, sein g, g' zwei Hochhebungen von $\overline{g}$. Daher, $g - g' \in (f)$ also es gibt ein $h \in K[x,y]$ mit $g - g' = hf$. Dies jedoch besagt, das $g' = g + hf$ und nun benutzen wir die 7te Eigenschaft. □

Definition 2.4.12. *Sei f irreduzibel und $\varphi = \frac{g}{h} \in K(f) = Q(K[x,y])$. Wir definieren die rationale Schnittzahl*

$$\mathfrak{I}(a, f \cap \varphi) := \mathfrak{I}(a, f \cap g) - \mathfrak{I}(a, f \cap h) \in \mathbb{Z} \cup \{\infty\}.$$

Lemma 2.4.13. *Die rationale Schnittzahl ist wohldefiniert.*

Beweis. Als erstes, lasst uns die Notation erklären. Da $\varphi = \frac{g}{h}$ im Quotientenkörper $K(f)$ landet, ist bei Definition $g, h \in K[x,y]/f$. Deren Schnittzahl mit f haben wir schon in Definition 2.4.10 beschrieben. (Den Überstrich auf g und h haben wir uns hier gespart).

Sei nun $\frac{g}{h} \sim \frac{g'}{h'}$. Daher, es gibt ein $\alpha \in K[x,y]/f$, mit $\alpha \neq 0 \in K[x,y]/f$, so dass $\alpha g h' = \alpha g' h$. Wegen f irreduzibel ist $\alpha \neq 0 \in K[x,y]/f$ äquivalent zu sagen, dass f und α haben keine gemeinsamen Teiler haben. Als solches ist $\mathfrak{I}(a, f \cap \alpha) < \infty$ laut der ersten Eigenschaft. Die 6te Eigenschaft besagt nun

$$\mathfrak{I}(a, f \cap \alpha) + \mathfrak{I}(a, f \cap gh') = \mathfrak{I}(a, f \cap \alpha g h') = \mathfrak{I}(a, f \cap \alpha g' h) = \mathfrak{I}(a, f \cap \alpha) + \mathfrak{I}(a, f \cap gh'),$$

woraus wir nach kürzen mit $\mathfrak{I}(a, f \cap \alpha)$ das gewünschte erhalten.

Letztens wollen wir zeigen, dass wir in $\mathbb{Z} \cup \{\infty\}$ landen. Dies ist Äquivalent zu sagen, dass $\mathfrak{I}(a, f \cap h) \neq \infty$. Da $h \neq 0 \in K[x,y]/f$, also $h \notin (f)$, haben wir dies schon in diesem Beweis argumentiert (mit α). □

Die Schnittzahl am Halm In diesem Abschnitt ist f irreduzibel. Somit haben wir $\mathcal{O}_a(f) \subseteq K(f)$ und können Definition 2.4.12 benutzen.

Lemma 2.4.14. *Sei f regulär am Punkt a und $u, t \in \mathcal{O}_a(f)$, mit u eine Einheit und t irreduzibel. Es gilt:*

(i) $\mathfrak{I}(a, f \cap u) = 0$ *und*

(ii) $\mathfrak{I}(a, f \cap t) = 1$.

Beweis. (i) Es gilt zu beweisen, dass $\dim_K (\mathcal{O}_a/(f,u)) = 0$. Wir haben $\mathcal{O}_a/(f,u) \simeq (\mathcal{O}_a/f)/u \simeq \mathcal{O}_a(f)/u$. Da wir eine Einheit $u \in (f,u)$ im Ideal haben ist $(f,u) = (1)$.

(ii) In anderen Worten, wir haben zu zeigen, dass $\dim_K (\mathcal{O}_a/(f,t)) = 1$. Wir benutzen noch einmal die Isomorphie $\mathcal{O}_a/(f,t) \simeq \mathcal{O}_a(f)/t$. Bei Definition und Proposition 2.3.41 wissen wir, dass das Hauptdeal (t), erzeugt mit einem irreduziblen Elementen, ein Maximalideal ist. Daher ist $f \in (t)$, was $(f,t) = (t)$ ergibt und als solches teilen wir durch ein Maximalideal, was uns ein Körper gibt. Da K algebraisch abgeschlossen ist, erhalten wir den selben Körper uns als solches ist der Erweiterungsgrad 1. □

Lemma 2.4.15. *Sei f irreduzibel, regulär am Punkt a und $0 \neq \varphi = \frac{g}{h} \in \mathcal{O}_a(f)$. Es gilt*

$$\varphi = ct^n,$$

wobei $c \in \mathcal{O}_a(f)^*$ eine Einheit ist, $t \in \mathcal{O}_a(f)$ irreduzibel und

$$n = \mathfrak{I}(a, f \cap g) - \mathfrak{I}(a, f \cap h) = \mathfrak{I}(a, f \cap g).$$

Beweis. Von Satz 2.3.42 wissen wir, dass $\mathcal{O}_a(f)$ ein diskreter Bewertungsring ist und laut Proposition 2.3.40 wissen wir, dass jedes Element eindeutig in der gegebenen Form geschrieben werden kann. Es bleibt also nur zu zeigen, dass spezifisch

$$n = \mathfrak{I}(a, f \cap g) - \mathfrak{I}(a, f \cap h) = \mathfrak{I}(a, f \cap g)$$

gilt. Da bei Definition $\frac{1}{h}$ in $\mathcal{O}_a(f)$ invertierbar ist, ist $\frac{g}{h} = ct^n$ äquivalent zu $g = (hc)t^n = c't^n$. Bei Beweis von Eigenschaft (6) der Schnittzahl 2.4.2 haben wir gezeigt, dass es sich mit dem Produkt verträgt. Daher gilt

$$\mathfrak{I}(a, f \cap g) = \mathfrak{I}(a, f \cap c't^n) = \mathfrak{I}(a, f \cap c') + \underbrace{\mathfrak{I}(a, f \cap t) + \cdots + \mathfrak{I}(a, f \cap t)}_{\times n} = 0 + 1 + \cdots + 1 = n,$$

laut Lemma 2.4.14. □

Lemma 2.4.16. *Sei f irreduzibel. Eine rationale Abbildung $\varphi = \frac{g}{h} \in K(f)^*$ ist genau dann im Halm $\mathcal{O}_a(f)$, wenn $\mathfrak{I}(a, f \cap \varphi) = \mathfrak{I}(a, f \cap g) - \mathfrak{I}(a, f \cap h)$ positiv ist.*

Beweis. Sei $\varphi \in \mathcal{O}_a(f)^*$, also $0 \neq \varphi$. Da bei Definition eines Elements des Halms, wir $h(a) \neq 0$, also $a \notin f \cap h$ haben, folgt von der 2ten Eigenschaft der Schnittzahl, dass $\mathfrak{I}(a, f \cap h) = 0$. Es folgt $\mathfrak{I}(a, f \cap \varphi) = \mathfrak{I}(a, f \cap g) - \mathfrak{I}(a, f \cap h) = \mathfrak{I}(a, f \cap g) \geq 0$.

Sei andersrum $\mathfrak{I}(a, f \cap \varphi) \geq 0$. Wir wissen, dass g und h (das heißt, $\frac{g}{1}, \frac{h}{1}$) im Halm $\mathcal{O}_a(f)$ nicht das Nullpolynom definieren. Wir können also Lemma 2.4.15 benutzen und erhalten

$$g = c_1 t^n, \quad h = c_2 t^m \text{ im Halm } \mathcal{O}_a(f),$$

wobei $c \in \mathcal{O}_a^*(f)$, $t \in \mathcal{O}_a(f)$ irreduzibel und $n = \mathfrak{I}(a, f \cap g)$, $m = \mathfrak{I}(a, f \cap h)$. Da $\mathfrak{I}(a, f \cap g) \geq \mathfrak{I}(a, f \cap h)$, folgt, dass $n - m \geq 0$ und daher ist $\frac{g}{h} = \frac{c_1}{c_2} t^{n-m}$. Also ist es ein Element in $\mathcal{O}_a(f)$. (Denn $t \in \mathcal{O}_a(f)$). □

3 Projektive Geometrie

Im letzten Kapitel haben wir die Schnittzahl eingeführt. Doch schon mit Geraden sehen wir deren Anwendungsgrenzen. Seien $L_1 = x - y$ und $L_2 = ax + y$. Es ist klar, dass diese Geraden sich, abhängig von $a \in K$, überhaupt nicht, einmal oder unendlich oft schneiden, wobei letzteres eher ein Sonderfall ist. Intuitiv aber ist es recht klar, dass sich allgemeine Kurven vom Grad m und n höchstens mn mal schneiden (oder unendlich oft). Eine genauere Aussage ist ohne Weiteres nicht möglich.

Statt weiter in affinen Räumen zu arbeiten, betrachten wir nun die etwas "größeren" projektiven Räume. Diese ermöglichen uns den Beweis eines der Hauptsätze des Kurses, der Satz von Bézout 4.2.3, welcher besagt, dass sich zwei Kurven vom Grad m und n in der projektiven Ebene über einem algebraisch abgeschlossenen Körper *genau* mn-mal schneiden (wobei man hier die Multiplizitäten der Schnitte berücksichtigen muss). Grob gesagt, fügen wir beim Übergang vom affinen zum projektiven Raum "Punkte im Unendlichen" hinzu, welche dann beim Zählen von Schnittpunkten eingehen und dieses nützliche Ergebnis liefern. Aus dem Satz von Bézout werden wir dann einige schöne geometrische Folgerungen schließen können.

3.1 Die projektive Fläche $\mathbb{P}^2$

Sei K ein fixierter Körper. Es gibt mehrere Möglichkeiten die projektiven Räume, und im Speziellen die projektive Ebene, einzuführen. Anschaulich lässt sich $\mathbb{P}^n$ etwa als Menge der Ursprungsgeraden in $\mathbb{A}^{n+1}$ auffassen. Die folgende Definition formalisiert dies.

Der n-dimensionale projektive Raum

Definition 3.1.1. *Betrachte auf $\mathbb{A}^{n+1}_K \setminus \{0\}$ die Äquivalenzrelation $\sim$, welche gegeben ist durch*

$$a \sim b \text{ genau dann, wenn } \exists \lambda \in K^* : a = \lambda b.$$

Wir definieren den projektiven Raum $\mathbb{P}^n_K$ *als die Menge der Äquivalenzklassen von $\mathbb{A}^{n+1}_K \setminus \{0\}$ unter dieser Äquivalenzrelation. Wir schreiben auch einfach $\mathbb{P}^n := \mathbb{P}^n_K$, wenn der Basiskörper klar ist. Ist $n = 1$ so nennen wir $\mathbb{P}^1$ die* projektive Gerade *über K, falls $n = 2$, die* projektive Ebene *über K.*

Wie lassen sich Punkte von $\mathbb{P}^n$ nun als Ursprungsgeraden in $\mathbb{A}^{n+1}$ verstehen? Jede Gerade ist durch zwei verschiedene Punkte in $\mathbb{A}^{n+1}$ eindeutig festgelegt, um eine Ursprungsgerade zu spezifizieren, genügt es also einen einzigen Punkt in $\mathbb{A}^{n+1} \setminus \{0\}$ anzugeben. Zwei solcher Punkte definieren nun genau dann die selbe Ursprungsgerade, wenn sie linear abhänging, also bezüglich $\sim$ äquivalent sind.

Im Falle, dass $K = \mathbb{R}$ ist, trägt $\mathbb{A}^{n+1}_R = \mathbb{R}^{n+1}$ eine Norm, etwa die euklidische Norm, und wir können für jeden Punkt in $\mathbb{P}^n_{\mathbb{R}}$ stets einen Repräsentanten der Norm 1 finden, also einen

Repräsentanten, welcher auf der n-dimensionalen Sphäre $S^n \subseteq \mathbb{R}^{n+1}$ liegt. Tatsächlich liegen auf der Sphäre genau zwei Repräsentanten einer gegebenen Ursprungsgerade, x und $-x$, wir können daher $\mathbb{P}^n_{\mathbb{R}}$ auch als Menge der Äquivalenzklassen von S^n bezüglich der Relation $x \sim -x$ für $x \in S^n$ auffassen. Den Punkt $-x$ nennen wir auch den *Antipodalpunkt* eines gegebenen Punktes $x \in S^n$.

Betrachten wir den Fall $n = 1$, also die projektive Gerade über $\mathbb{R}$. Die 1-Sphäre S^1 ist der Kreis in der zweidimensionalen Ebene $\mathbb{R}^2$. Ein Repräsentantensystem der Antipodalrelation $x \sim -x$ auf S^1 ist durch den oberen Halbkreis gegeben, wobei wir uns aber für den Punkt $(1, 0)$ oder $(-1, 0)$ entscheiden müssten. Wir können uns die Entscheidung aber auch sparen und stattdessen diese beiden Endpunkte miteinander identifizieren. Nun erhalten wir aber wieder einen Kreis! Dies zeigt, dass $S^1/\sim$ isomorph zu S^1 ist, also $\mathbb{P}^1_{\mathbb{R}}$ einfach der Kreis S^1 ist.

Betrachten wir nun die projektive Ebene $\mathbb{P}^2_{\mathbb{R}}$ über $\mathbb{R}$. Ein Repräsentantensystem von $x \sim -x$ auf der Kugeloberflächse $S^2 \subseteq \mathbb{R}^3$ ist *fast* gegeben durch die obere Hemisphäre. Anders als im eindimensionalen Fall müssen wir aber mehr als nur zwei Endpunkte am Rand eines Halbkreises miteinander identifizieren. Der Rand der oberen Hemisphäre besteht nämlich aus den Punkten am Äquator der Kugeloberfläche, welche wir nun ebenfalls noch geeignet miteinander identifizieren müssen, nämlich genau gemäß der Antipodalrelation. Dabei sei beachtet, dass der Antipodalpunkt eines Punktes auf dem Äquator natürlich ebenfalls auf dem Äquator liegt. Nun befinden wir uns aber wieder im Fall von $n = 1$, der Äquator unter dieser Relation ist genau $\mathbb{P}^1_{\mathbb{R}}$. Das ist zwar zufällig wieder ein Kreis S^1, dieser ist aber nicht mehr trivial mit der oberen Hemisphäre verklebt. Topologisch ist die obere Hemisphäre einfach eine Kreisscheibe (welche etwas gewölbt wurde), zusammenfassend lässt sich daher sagen, dass $\mathbb{P}^2_{\mathbb{R}}$ fast eine Kreisscheibe ist, deren Rand aber nur fast ein Halbkreis ist, deren Rand nur aus einem Punkt statt zweien besteht. Dies ist aber sicherlich nicht mehr $\mathbb{S}^2$.

Für höhere n lässt sich diese Beschreibung so fortführen, $\mathbb{P}^n_{\mathbb{R}}$ lässt sich fast durch eine n-Scheibe darstellen, deren Rand fast eine Halb-$n-1$-Sphäre ist, deren Rand fast eine Halb-$n-2$-Sphäre ist … deren Rand eine Halb-0-Sphäre ist (beachte hier, $S^0 := \{-1, 1\} \subseteq \mathbb{R}^1$).

Dies ganze kann man sich besser vorstellen, indem man nicht darüber nachdenkt, was fehlt, sondern was dazukommt. Aus dieser Perspektive ist $\mathbb{P}^1_{\mathbb{R}}$ ein *offener* Halbkreis zusammen mit einem zusätzlichen Punkt, welchen wir an den Enden des Halbkreises einkleben (dieser zusätzliche Punkt übernimmt also die Rolle der miteinander identifizierten Endpunkte des Halbkreises). Wir notieren diesen zusätlichen Punkt mit ∞. Da ein offener Halbkreis homöomorph zu einem offenen beschränkten Intervall $]a, b[$ ist (man muss den Halbkreis lediglich "gerade biegen" mittels Polarkoordinaten), welches wiederum homöomorph zu $\mathbb{R}^1$ ist (etwa vermöge affiner Transformationen und tanh), erhalten wir eine Beschreibung

$$\mathbb{P}^1_{\mathbb{R}} \simeq \mathbb{A}^1_{\mathbb{R}} \sqcup \{\infty\}.$$

Dabei bezeichnet $\sqcup$ die disjunkte Vereinigung.

Bei $n = 2$ starten wir mit einer offenen Halbkugel, welche homöomorph zu einem offenen

Rechteck $]a,b[\times]c,d[$ ist, was wiederum homöomorph zu $\mathbb{R}^2$ ist. Anschließend müssen wir noch einen offenen Halbkreis mit einem zusätzlichen Punkt hinzufügen, was ja genau eine projektive Gerade $\mathbb{P}^1_{\mathbb{R}}$ ist. Wir erhalten also

$$\mathbb{P}^2_{\mathbb{R}} \simeq \mathbb{A}^2_{\mathbb{R}} \sqcup \mathbb{P}^1_{\mathbb{R}} \simeq \mathbb{A}^2_{\mathbb{R}} \sqcup \mathbb{A}^1_{\mathbb{R}} \sqcup \{\infty\}.$$

Durch Iteration dieses Arguments erhalten wir die Beschreibung

$$\mathbb{P}^n_{\mathbb{R}} \simeq \mathbb{A}^n_{\mathbb{R}} \sqcup \mathbb{P}^{n-1}_{\mathbb{R}} \simeq \mathbb{A}^n_{\mathbb{R}} \sqcup \mathbb{A}^{n-1}_{\mathbb{R}} \sqcup \cdots \sqcup \mathbb{A}^1_{\mathbb{R}} \sqcup \{\infty\}.$$

Der Punkt $\{\infty\}$ ist natürlich einfach ein 0-dimensionaler affiner Raum $\mathbb{A}^0_{\mathbb{R}}$, es folgt also

$$\mathbb{P}^n_{\mathbb{R}} \simeq \bigsqcup_{i=0}^{n} A^i.$$

Das Schöne an dieser Beschreibung ist, dass sie tatsächlich für beliebige Körper gilt. Wir werden dies später rigoroser beweisen. Dazu werden wir eine weitere Sichtweise von projektiven Räumen einführen $\mathbb{P}^n$, nämlich als eine $n+1$-fache (nicht-disjunkte) Vereinigung n-dimensionaler affiner Räume $\mathbb{A}^n$. In der Schematheorie wird diese "affine offene Überdeckung" genutzt um einzusehen, dass $\mathbb{P}^n$ tatsächlich ein Schema ist, also lokal wie ein affines Schema (in diesem Fall der affine Raum $\mathbb{A}^n$) aussieht. Diese Sichtweise werden wir hier aber natürlich nicht weiter verfolgen.

3.1.1 Homogene Koordinaten

Definition 3.1.2. *Sei $p \in \mathbb{P}^n$. Ist p die Äquivalenzklasse von $(a_1, \ldots, a_{n+1}) \in \mathbb{A}^{n+1} \setminus \{0\}$, so schreiben wir $p = [a_1 : \cdots : a_{n+1}]$ und nennen a_i die* homogenen Koordinaten *des Punktes p.*

Die homogenen Koordinaten eines Punktes $p \in \mathbb{P}^n$ sind *nicht* eindeutig bestimmt, lediglich bis auf Skalierung. Es gilt aber folgendes Lemma.

Lemma 3.1.3. *Seien $[a_1 : \cdots : a_{n+1}] = [b_1 : \cdots : b_{n+1}] \in \mathbb{P}^n$ homogene Koordinaten desselben Punktes im projektiven Raum. Dann gilt für jedes $1 \leq i \leq n+1$:*

(i) Es ist $a_i = 0$ genau dann, wenn $b_i = 0$.

(ii) Falls $a_i \neq 0$ (und damit $b_i \neq 0$) ist $\frac{a_j}{a_i} = \frac{b_j}{b_i}$ für jedes $1 \leq j \leq n+1$.

Mit anderen Worten ist es wohldefiniert zu sagen, dass eine homogene Koordinate a_i eines Punktes $p = [a_1 : \cdots : a_{n+1}]$ im projektiven Raum verschwindet und die Verhältnisse $\frac{a_j}{a_i}$ der homogenen Koordinaten sind wohldefiniert. Dies erklärt warum wir homogene Koordinaten mit Doppelpunkten, also "Divisionssymbolen", notieren.

Beweis. (i) Sei $(a_1, \dots, a_{i-1}, 0, a_{i+1}, a_n) = (\lambda b_1, \dots, \lambda b_{i-1}, \lambda b_i, \lambda b_{i+1}, \dots, b_n)$. Es folgt, dass $\lambda b_i = 0$ und da $\lambda \neq 0$, muss $b_i = 0$ sein.

(ii) Seien $(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \sim (b_1, \dots, b_{i-1}, b_i, b_{i+1}, \dots, b_n)$. Da $a_i \neq 0$ folgt, dass $(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \sim \left(\frac{a_1}{a_i}, \dots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i}\right)$. Laut Teil (i) impliziert $a_i \neq 0$, dass $b_i \neq 0$, woraus $(b_1, \dots, b_{i-1}, b_i, b_{i+1}, \dots, b_n) \sim \left(\frac{b_1}{b_j}, \dots, \frac{b_{i-1}}{b_j}, 1, \frac{b_{i+1}}{b_j}, \dots, \frac{b_n}{b_j}\right)$ und somit

$$\left(\frac{a_1}{a_i}, \dots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i}\right) \sim \left(\frac{b_1}{b_j}, \dots, \frac{b_{i-1}}{b_j}, 1, \frac{b_{i+1}}{b_j}, \dots, \frac{b_n}{b_j}\right)$$

folgt. Daher gibt es ein $\lambda \in K^*$, sodass

$$\left(\frac{a_1}{a_j}, \dots, \frac{a_{i-1}}{a_j}, 1, \frac{a_{i+1}}{a_j}, \dots, \frac{a_n}{a_j}\right) = \left(\lambda\frac{b_1}{b_j}, \dots, \lambda\frac{b_{i-1}}{b_j}, \lambda, \lambda\frac{b_{i+1}}{b_j}, \dots, \lambda\frac{b_n}{b_j}\right),$$

was $\lambda = 1$ und damit $\frac{a_j}{a_i} = \frac{b_j}{b_i}$ für alle i, j impliziert. □

Für jedes $1 \leq i \leq n$ können wir nun die Teilmenge $U_i \subseteq \mathbb{P}^n$ durch

$$U_i := \{[a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n \mid a_i \neq 0\} \tag{20}$$

definieren. Ist dann $p \in U_i$, so lässt sich p als

$$p = [a_1 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_{n+1}]$$

darstellen. Diese Darstellung zeigt, dass sich der Punkt $p \in U_i$ eigentlich schon durch n Koordinaten $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in \mathbb{A}^n$ vollständig beschreiben lässt.

Punkte im Komplement von U_i lassen sich dagegen durch Elemente in $\mathbb{P}^{n-1}$ beschreiben. Genauer definieren wir

$$H_\infty^i := \mathbb{P}^n \setminus U_i = \{[a_1 : \cdots : a_{n+1}] \mid a_i = 0\}.$$

Dann ist offenbar $H_\infty^i \simeq \mathbb{P}^{n-1}$, da wir ja einfach eine Koordinate als 0 fixieren, was laut (i) von Lemma 3.1.3 wohldefiniert ist. Oft setzen wir hier die letzte Koordinate auf 0, weshalb wir speziell $H_\infty := H_\infty^{n+1}$ definieren.

Zusammenfassend lassen sich folgende Beobachtungen treffen:

Proposition 3.1.4. *Sei $\mathbb{P}^n$ der projektive n-Raum.*

(i) Die Abbildung $\mathbb{A}^n \to U_i$, gegeben durch

$$(a_1 : \cdots : a_n) \mapsto [a_1 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_n]$$

definiert eine Bijektion für jedes $1 \leq i \leq n$.

(ii) Es gilt $\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$.

(iii) Wir haben $\mathbb{P}^n = U_{n+1} \sqcup H_\infty \simeq \mathbb{A}^n \sqcup \mathbb{P}^{n-1} \simeq \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^0 = \bigsqcup_{i=0}^{n} \mathbb{A}^n$.

Beweis. (i) Seien $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{A}^n$ mit

$$[a_1 : \cdots : a_{i_1} : 1 : a_i : \cdots : a_n] = [b_1 : \cdots : b_{i_1} : 1 : b_i : \cdots : b_n].$$

Dann gibt es ein $\lambda \in K$, sodass

$$(a_1, \ldots, a_{i_1}, 1, a_i, \ldots, a_n) = \lambda(b_1, \ldots, b_{i_1}, 1, b_i, \ldots, b_n) = (\lambda b_1, \ldots, \lambda b_{i_1}, \lambda, \lambda b_i, \ldots, \lambda b_n)$$

in $\mathbb{A}^{n+1}$. Insbesondere ist der i-te Eintrag dieser Vektoren identisch, also ist $\lambda = 1$ und damit $b_j = a_i$ für alle $1 \leq j \leq n$. Es folgt, dass $(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \in \mathbb{A}^n$.

Für die Surjektivität, sei $[a_1 : \cdots : a_{n+1}] \in U_i \subseteq \mathbb{P}^n$. Insbesondere ist $a_i \neq 0$, weshalb

$$[a_1 : \cdots : a_{n+1}] = \left[\frac{a_1}{a_i} : \cdots : \frac{a_{i-1}}{a_i} : 1 : \frac{a_{i+1}}{a_i} : \cdots : \frac{a_n}{a_i}\right]$$

gilt. Letzteres ist offenbar das Bild von $\left(\frac{a_1}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right)$.

(ii) Per Definition der Punkte p in $\mathbb{P}^n$ als Äquivalenzklasse von Punkten in $\mathbb{A}^{n+1} \setminus \{0\}$ ist mindestens eine homogene Koordinate a_i von p ungleich 0, denn nicht alle Koordinaten dürfen gleichzeitig verschwinden. Damit ist $p \in U_i$.

(iii) Die erste Gleichung ist die Definition von H_∞. Die zweite Gleichung ist Teil (i) (also dass $U_{n+1} \simeq \mathbb{A}^n$) und die Tatsache, dass $H_\infty \simeq \mathbb{P}^{n-1}$, da wir ja eine Koordinate festlegen, die anderen aber frei sind. □

3.1.2 Projektive Varietäten

Der Untersuchungsgegenstand der (klassischen) algebraischen Geometrie sind algebraische Varietäten. Im ersten Teil des Skripts haben wir affine Varietäten, also Nullstellenmengen im affinen Raum, untersucht, nun wollen wir analog projektive Varietäten als Nullstellenmengen im projektiven Raum einführen.

Projektive Nullstellen

Definition 3.1.5. *Ein Punkt* $p = [a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n$ *heißt* Nullstelle *eines Polynoms* $f \in K[x_1, \ldots, x_{n+1}]$, *falls*

$$f(a_1, \cdots, a_{n+1}) = 0,$$

für jeden *Repräsentanten* $(a_1, \ldots, a_{n+1})$ *von* $[a_1 : \cdots : a_{n+1}]$. *In diesem Fall schreiben wir* $f(p) = 0$.

Beispiel 3.1.6. i) Sei $f(x, y) = x^2 - y^2$. Dann ist $p = [1 : 1] \in \mathbb{P}^1$ eine Nullstelle von f, da für einen beliebigen Repräsentanten (λ, λ), $\lambda \in K^*$ von p gilt: $f(\lambda, \lambda) = \lambda^2 - \lambda^2 = 0$.

ii) Sei $g(x,y) = x^2 - xy$. Dann ist wieder $p = [1:1] \in \mathbb{P}^1$ eine Nullstelle, denn für jeden Repräsentanten (λ,λ) gilt $\lambda^2 - \lambda\cdot\lambda = 0$.

iii) Sei $h(x,y) = x^2 - y$. Dann ist $p = [1:1] \in \mathbb{P}^1$ *keine* Nullstelle von h. Es ist zwar $h(1,1) = 1^2 - 1 = 0$, der Repräsentant $(1,1)$ von p ist also eine Nullstelle, aber für den Repräsentanten $(2,2)$ gilt $h(2,2) = 4 - 2 = 2 \neq 0$.

Der Unterschied zwischen dem letzten und den ersten beiden Beispielen in 3.1.6 ist, dass h im Gegensatz zu f und g kein *homogenes* Polynom war. Beachte aber, dass inhomogene Polynome durchaus trotzdem projektive Nullstellen besitzen können:

Beispiel 3.1.7. Sei $f(x,y,z) = y + x^2 + y^2 - z^2$. Dann ist $p = [1:0:1] \in \mathbb{P}^2$ eine Nullstelle von f, da für jedes $\lambda \in K^*$ gilt, dass $f(\lambda,0,\lambda) = \lambda^2 - \lambda = 0$. Beachte aber, dass sich f als $(y) + (x^2+y^2-z^2)$ zerlegen lässt und p eine Nullstelle von *beiden* der homogenen Summanden ist. Dies ist kein Zufall, wie wir in Lemma 3.1.9 beweisen werden.

Für Formen lässt sich die Definition projektiver Nullstellen wie folgt vereinfachen.

Lemma 3.1.8. *Ein Punkt $p \in \mathbb{P}^n$ ist eine Nullstelle einer Form F genau dann, wenn $F(a) = 0$ für irgendeinen Repräsentanten $a \in \mathbb{A}^{n+1} \setminus \{0\}$ von $p \in \mathbb{P}^n$.*

Beweis. Ist p eine Nullstelle so ist $F(a) = 0$ für jeden Repräsentanten $a \in \mathbb{A}^{n+1} \setminus \{0\}$ per Definition. Sei also umgekehrt $a \in \mathbb{A}^{n+1} \setminus \{0\}$ ein Repräsentant von p, sodass $F(a) = 0$. Jeder weitere Repräsentant ist dann von der Form λa für ein $\lambda \in K^*$. Ist $\mathsf{grad}(F) = d$, so gilt $F(\lambda a) = \lambda^d F(a) = 0$, da F eine Form ist. Folglich ist p Nullstelle von F. □

Es gibt offensichtlich einen starken Zusammenhang zwischen Formen (homogenen Polynomen) und homogenen Koordinaten (daher auch der Name). Wir wollen dies nun weiter erforschen:

Lemma 3.1.9. *Sei $f = F_m + \cdots + F_r \in K[x_1,\ldots,x_{n+1}]$ eine Zerlegung in Formen. Ein Punkt $p \in \mathbb{P}^n$ ist genau dann eine Nullstelle von f, wenn ein Repräsentant $a \in \mathbb{A}^{n+1} \setminus \{0\}$ von p existiert, sodass $F_i(a) = 0$ für alle $m \leq i \leq r$.*

Beweis. Die eine Richtung ist wieder klar nach Definition. Sei also a ein Repräsentant von p, welcher Nullstelle aller F_i ist. Nach Lemma 3.1.8 ist dann schon *jeder* Repräsentant von p Nullstelle aller F_i, da diese Formen sind. Also gilt für jeden beliebigen Repräsentanten b von p:

$$f(b) = F_m(b) + \cdots + F_r(b) = 0 + \cdots + 0 = 0$$

Per Definition ist p damit Nullstelle von f. □

Projektive Varietäten

Definition 3.1.10. *Sei $S \subseteq K[x_1, \ldots, x_{n+1}]$. Wir definieren die* projektive Verschwindungsmenge *von S in $\mathbb{P}^n$ durch*

$$\mathrm{V}(S) := \{p \in \mathbb{P}^n \mid \forall f \in S : f(p) = 0\}.$$

Mengen dieser Art werden algebraische Mengen *in $\mathbb{P}^n$, oder* projektive Varietäten *genannt.*

Korollar 3.1.11. *Sei $f = F_m + \cdots + F_r \in K[x_1, \ldots, x_{n+1}]$ eine Zerlegung in Formen. Es ist*

$$\mathrm{V}(f) = \mathrm{V}(\{F_m, \ldots, F_r\}).$$

Wie schon im affinen Fall gilt:

Lemma 3.1.12. *Sei $I(S)$ das von S erzeugte Ideal. Dann gilt*

$$\mathrm{V}(I(S)) = \mathrm{V}(S).$$

Beweis. Offenbar gilt $\mathrm{V}(I(S)) \subseteq \mathrm{V}(S)$, da $S \subseteq I(S)$. Umgekehrt sei $p \in \mathrm{V}(S)$ und $f = r_1 f_1 + \cdots + r_n f_n$ ein beliebiges Element von $I(S)$, wobei $r_i \in K[x_1, \ldots, x_{n+1}]$, $f_i \in S$. Ist $a \in \mathbb{A}^{n+1} \setminus \{0\}$ ein beliebiger Repräsentant von p, so ist $f_i(a) = 0$ für alle $i = 1, \ldots, n$. Dann ist auch $f(a) = 0$. Da a beliebig war, ist p Nullstelle von f. Da $f \in I(S)$ beliebig war, ist $p \in \mathrm{V}(I(S))$, folglich $\mathrm{V}(S) \subseteq \mathrm{V}(I(S))$. □

Es ist leicht zu sehen, dass auch im projektiven Fall die Gleichung

$$\mathrm{V}(S \cup T) = \mathrm{V}(S) \cap \mathrm{V}(T)$$

gilt. Dies erlaubt uns den Beweis des folgenden Korollars.

Korollar 3.1.13. *Für jede projektive Varietät $\mathrm{V} \subseteq \mathbb{P}^n$ gibt es eine endliche Menge von Formen $F_1, \ldots, F_r$, so dass*

$$\mathrm{V}(F_1, \ldots, F_r).$$

Beweis. Sei $\mathrm{V} = \mathrm{V}(S)$ für eine Teilmenge $S \subseteq K[x_1, \ldots, x_{n+1}]$. Da $K[x_1, \ldots, x_{n+1}]$ ein noetherscher Ring ist, ist das von S erzeugte Ideal $I(S)$ endlich erzeugt, es existieren also Polynome $f_1, \ldots, f_k$, sodass $I(S) = (f_1, \ldots, f_k)$. Wir haben also schon einmal

$$\mathrm{V} = \mathrm{V}(S) = \mathrm{V}(I(S)) = \mathrm{V}(f_1, \ldots, f_k) = \mathrm{V}(f_1) \cap \cdots \cap \mathrm{V}(f_k)$$

Die f_i wiederum lassen sich in endlich viele Formen zerlegen, $f_i = \sum_j F_{ij}$, sodass nach Korollar 3.1.11 gilt, dass $\mathrm{V}(f_i) = \mathrm{V}(\{F_{ij}\}_j)$. Insgesamt erhalten wir

$$\mathrm{V} = \mathrm{V}\left(\{F_{1j}\}_j\right) \cap \cdots \cap \mathrm{V}\left(\{F_{kj}\}_j\right) = \mathrm{V}\left(\{F_{ij}\}_{ij}\right). \qquad \square$$

Definition 3.1.14. *Sei $X \subseteq \mathbb{P}^n$ eine Teilmenge des projektiven n-Raumes. Wir definieren das* Verschwindungsideal *von X als*

$$\mathrm{I}(X) := \{f \in K[x_1, \ldots, x_{n+1}] \mid f(p) = 0 \text{ für alle } p \in X\}.$$

Definition 3.1.15. *Ein Ideal $I \subseteq K[x_1, \ldots, x_{n+1}]$ heißt* homogen*, wenn für alle $f \in I$ mit Zerlegung $f = \sum_{i=1}^{r} F_i$ in Formen F_i gilt: $F_i \in I$, für alle $1 \leq i \leq r$.*

Lemma 3.1.16. *Ein Ideal $I \subseteq K[x_1, \ldots, x_{n+1}]$ ist genau dann homogen, wenn es endliche viele Formen $F_1, \ldots, F_r$ gibt, so dass $I = (F_1, \ldots, F_r)$.*

Beweis. Ist I ein Ideal, so finden wir wie im Beweis von 3.1.13 zunächst endlich viele Erzeuger f_i, da $K[x_1, \ldots, x_{n+1}]$ noethersch ist. Die endlich vielen homogenen Komponenten F_{ij} der f_i (pro Polynom f_i höchstens $\mathsf{grad}(f_i)$-viele) liegen dann ebenfalls schon in I, da I homogen ist. Und tatsächlich erzeugen diese I sogar, denn jedes Polynom welches sich als Linearkombination (über $K[x_1, \ldots, x_{n+1}]$) der f_i schreiben lässt, wird sich sicherlich auch als Linearkombination der F_{ij} schreiben lassen, da die f_i ihrerseits Linearkombinationen der F_{ij} sind.

Sei andererseits $I = (\{F_\alpha\})$ für gewisse Formen F_α vom Grad $\mathsf{grad}(F_\alpha) = \alpha$. Sei $g \in I$ und $g = G_m + \cdots + G_r$ eine Zerlegung in Formen G_i. Es genügt zu zeigen, dass $G_m \in I$, denn dann gilt auch $g - G_m \in I$ und ein Induktionsargument zeigt, dass dann schon jeder homogene Summand in I liegt. Nach Voraussetzung existieren gewisse $h_\alpha \in K[x_1, \ldots, x_{n+1}]$, sodass $g = \sum h_\alpha F_\alpha$. Jedes der h_α wiederum lässt sich in homogene Formen $H_{\alpha,i}$ vom Grad i zerlegen. Da die Zerlegung in Formen eindeutig ist, erhalten wir in Grad m die Gleichung

$$G_m = \sum_\alpha H_{\alpha,m-i} F_\alpha.$$

Dies ist eine Darstellung von G_m als Linearkombination der $F_\alpha \in I$, womit schon G_m selbst in I liegt. □

Lemma 3.1.17. *Sein F, G, H homogen und $H \in (F, G)$. Dann gibt es homogene Polynome A, B, so dass $H = AF + BG$.*

Beweis. Es gibt natürlich Polynome a, b, so dass $H = aF + bG$. Es gilt zu beweisen, dass wir für a und b Formen wählen können. Dies folgt direkt aus der Tatsache, dass zwei Polynome genau dann gleich sind, wenn all deren homogene Summanden gleich sind (und H selbst sein einziger homogener Summand ist). Genauer, sei $a = A_0 + \cdots + A_d$ und $b = B_0 + \cdots + B_{d'}$ die Zerlegung in homogene Komponenten. Sei $\mathsf{grad}(H) = r$, $\mathsf{grad}(F) = s$ und $\mathsf{grad}(G) = t$, dann gilt bereits

$$A_{r-s} F + B_{r-t} G = H.$$ □

Proposition 3.1.18. *Das Verschwindungsideal $\mathrm{I}(X)$ einer Teilmenge $X \subseteq \mathbb{P}^n$ des projektiven n-Raumes ist homogen.*

Beweis. Dies ist einfach nur Lemma 3.1.9. Detaillierter, sei $X \subseteq \mathbb{P}^n$ und

$$\begin{aligned} \mathrm{I}(X) &= \{g \mid g(p) = 0 \text{ für alle } p \in P\} \\ &= \{g \mid g(\hat{p}) = 0 \text{ für jeden Repräsentanten } \hat{p} \text{ von } p, \text{ für alle } p \in X\}. \end{aligned}$$

Das Lemma besagt nun, dass jeder der homogenen Summanden im Ideal liegt. □

3.1.3 Homogene Primideale und irreduzible Varietäten

Um Verwirrungen vorzubeugen, ein homogenes Primideal ist einfach nur ein Primideal, welches zusätzlich homogen ist.

Proposition 3.1.19. *Ein homogenes Ideal $\mathfrak{p} \subseteq K[x_1, \ldots, x_{n+1}]$ ist genau dann prim wenn für alle Formen $F, G \in K[x_1, \ldots, x_{n+1}]$ gilt:*

$$FG \in \mathfrak{p} \Rightarrow (F \in \mathfrak{p} \text{ oder } G \in \mathfrak{p})$$

Beweis. Ist $\mathfrak{p}$ prim, so gilt die Implikation für alle Polynome, insbesondere also für Formen. Seien umgekehrt f, g beliebige Polynome, sodass $fg \in \mathfrak{p}$. Wir zeigen nun per Induktion über den Grad N von fg, dass $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$. Ist $N = 0$, so müssen auch f und g schon konstant gewesen sein, insbesondere homogen, die Voraussetzung greift daher und es gilt $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$.

Sei nun N beliebig und gelte die Behauptung für alle Paare von Polynomen deren Produkt von Grad $< N$ ist. Sei $a := \mathsf{grad}(f)$ und $b := \mathsf{grad}(g)$, sodass $N = a + b$. Es existiert also eine Form F_a vom Grad a sowie ein Polynom f' vom Grad $\mathsf{grad}(f') < a$, sodass $f = f' + F_a$ und ebenso lässt sich $g = g' + G_b$ für entsprechende g, G_b schreiben. Dann gilt

$$\mathfrak{p} \ni fg = (f' + F_a)(g' + G_b) = f'g' + f'G_b + F_ag' + F_aG_b.$$

Da f', g' geringeren Grad als f bzw. g haben, ist F_aG_b die homogene Komponente von fg vom Grad N. Da $\mathfrak{p}$ homogen ist, folgt $F_aG_b \in \mathfrak{p}$, nach Voraussetzung also $F_a \in \mathfrak{p}$ oder $G_b \in \mathfrak{p}$. Ohne Einschränkung sei $F_a \in \mathfrak{p}$, womit folgt, dass

$$f'g = f'(g' + G_b) = f'g' + f'G_b = fg - F_a(g' + G_b) \in \mathfrak{p}.$$

Da $\mathsf{grad}(f'g) < N$, ist nach Induktionsvoraussetzung $f' \in \mathfrak{p}$ oder $g \in \mathfrak{p}$. Im zweiten Fall sind wir direkt fertig, im zweiten Fall folgt $f = f' + F_a \in \mathfrak{p}$. □

Definition 3.1.20. *Eine projektive Varietät V heißt* reduzibel*, wenn sie endliche Vereinigung projektiver Varietäten ist, welche echt in V enthalten sind. Wir nennen V* irreduzibel*, wenn V nicht reduzibel ist. Konkret ist V irreduzibel, wenn $V \neq \varnothing$ und aus $V = A \cup B$ schon $V = A$ oder $V = B$ folgt, sofern A, B projektive Varietäten sind und $A, B \subsetneq V$.*

Proposition 3.1.21. *Eine projektive Varietät $\mathrm{V} \subseteq \mathbb{P}^n$ ist genau dann irreduzibel, wenn $\mathrm{I}(\mathrm{V})$ ein Primideal ist.*

Beweis. Genau so wie der Beweis von Satz 1.2.50, nur das wir hier Proposition 3.1.19 benutzten. □

Proposition 3.1.22. *Sei $X \subseteq \mathbb{P}^n$ eine projektive Varietät. Dann existieren irreduzible projektive Varietäten $\mathrm{V}_1, \ldots, \mathrm{V}_k$, sodass $X = \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_k$ und aus $V_i \subseteq V_j$ schon $i = j$ folgt. Ferner ist diese Darstellung eindeutig bis auf Umordnung.*

Beweis. Eindeutigkeit: Sei $X = \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_k = \mathrm{W}_1 \cup \cdots \cup \mathrm{W}_l$ eine weitere Darstellung derselben Art. Es folgt, dass

$$W_i = W_i \cap X = \bigcup_{j=1}^{k} (W_i \cap V_j)\,.$$

Da W_i nach Annahme irreduzibel ist, muss $W_i = W_i \cap V_j$ für ein j gelten. Es folgt, dass $W_i \subseteq V_j$. Durch ein ähnliches Argument muss auch $V_j \subseteq W_{i'}$ sein, was $W_i \subseteq W_{i'}$ und damit $i = i'$ impliziert. Insbesondere ist auch $W_i = V_j$, was unseren Beweis abschließt.

Existenz: Ist X irreduzibel, sind wir fertig. Wenn X reduzibel ist, müssen $U, V \subsetneq X$ existieren, sodass $X = U \cup V$. Wir sind fertig, wenn U und V irreduzibel sind. Angenommen dieser Prozess kommt nicht zum Halten. Dann finden wir eine absteigende Kette projektiver Varietäten

$$\cdots \subsetneq V_{n+1} \subsetneq \mathrm{V}_n \subsetneq \mathrm{V}_{n-1} \subseteq \cdots \subsetneq \mathrm{V}_1 = \mathrm{V}.$$

Dies liefert eine aufsteigende Kette von Idealen

$$\mathrm{I}(\mathrm{V}) = \mathrm{I}(\mathrm{V}_1) \subsetneq \cdots \subsetneq \mathrm{I}(\mathrm{V}_{n-1}) \subsetneq \mathrm{I}(\mathrm{V}_n) \subsetneq \mathrm{I}(\mathrm{V}(n+1)) \subsetneq \cdots,$$

in $K[x_1 \ldots, x_n]$. Aber dieser Ring ist noethersch, ein Widerspruch. □

Wie auch im affinen Fall haben wir entgegengesetzte Zuordnungen

$$\{ \text{ Homogene Ideale von } K[x_1, \ldots, x_{n+1}] \} \underset{\mathrm{I}}{\overset{\mathrm{V}}{\rightleftarrows}} \{ \text{ Projektive Varietäten von } \mathbb{P}^n \}\,.$$

Obwohl es im Allgemeinen aus dem Kontext klar ist, werden wir im Folgenden $\mathrm{V}_{\mathbb{P}}$, $\mathrm{I}_{\mathbb{P}}$ für die projektive Verschwindungsmenge bzw. das projektive Verschwindungsideal schreiben und $\mathrm{V}_{\mathbb{A}}$, $\mathrm{I}_{\mathbb{A}}$ für die affinen Pendants. Wir werden nun einige Resultate der affinen Geometrie in die projektive Welt transportieren. Zuvor benötigen wir aber noch die folgende Definition.

Definition 3.1.23. *Sei* $\mathrm{V} \subseteq \mathbb{P}^n$ *eine projektive Varietät. Wir definieren*

$$\mathsf{Kon}(\mathrm{V}) := \left\{(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1} \mid [x_1 : \cdots : x_{n+1}] \in V \quad \text{oder} \quad (x_1, \ldots, x_{n+1}) = 0 = (0, \ldots, 0)\right\},$$

genannt der Konus *über* V.

Damit können wir einer projektiven Varietät V eine affine Varietät $\mathsf{Kon}(V)$ zuordnen. Dies ist wichtig, da es uns erlaubt viele Probleme der projektiven Geometrie auf den affinen Fall zu reduzieren. Zum Beispiel haben wir folgenden Zusammenhang zwischen den verschiedenen Verschwindungsmengen/-idealen.

Lemma 3.1.24. *(i) Sei* $\mathrm{I} \subseteq K[x_1, \ldots, x_{n+1}]$ *ein homogenes Ideal mit* $\mathrm{V}_{\mathbb{P}}(\mathrm{I}) \neq \varnothing$. *Dann gilt*

$$\mathsf{Kon}(\mathrm{V}_{\mathbb{P}}(\mathrm{I})) = \mathrm{V}_{\mathbb{A}}(\mathrm{I}).$$

(ii) Sei $\varnothing \neq \mathrm{V} \subseteq \mathbb{P}^n$ eine projektive Varietät. Dann gilt

$$\mathrm{I}_{\mathbb{A}}(\mathsf{Kon}(\mathrm{V})) = \mathrm{I}_{\mathbb{P}}(\mathrm{V}).$$

Beweis. (i) Per Definition ist $\mathrm{V}_{\mathbb{P}}(\mathrm{I}) \neq \varnothing$. Daher, es gibt ein $p \in \mathbb{P}^n$, mit $f(p) = 0$ für jedes $f \in \mathrm{I}$. Dies wiederum besagt, dass $F_i(a) = 0$ für jeden homogenen Summanden F_i von f und jeden Repräsentanten a von p. Insbesondere ist $F_0(a) = 0$ und darum haben die Polynome keine konstanten Terme. Es folgt, dass $0 \in \mathrm{V}_{\mathbb{A}}(\mathrm{I})$.

Per Definition liegt $a = (a_1, \cdots, a_{n+1}) \in \mathbb{A}^{n+1}$ in der Varietät V genau dann, wenn $f(a) = 0$ für jedes $f \in \mathrm{I}$. Da aber I homogen ist, passiert dies genau dann, wenn $F(a) = 0$, für jedes homogene Polynom $F \in I$. Für F homogen ist aber $F(a) = 0$ genau dann, wenn $F(\lambda a) = 0$ für alle $\lambda \in K^*$. Dies ist äquivalent zu sagen, dass $a \in \mathsf{Kon}(\mathrm{V}_{\mathbb{P}}(\mathrm{I}))$.

(ii) Sei $f \in \mathrm{I}_{\mathbb{P}}(\mathrm{V})$. Es ist klar, dass $f \in \mathrm{I}_{\mathbb{A}}(\mathsf{Kon}(\mathrm{V}) \setminus \{0\})$, da nach Definition $0 \notin \mathbb{P}^n$. Wir brauchen also nur zu überprüfen, dass auch 0 eine Nullstelle von jedem $f \in I_{\mathbb{P}}(\mathrm{V})$. Zerlege $f = F_0 + F_1 + \cdots + F_r$ als Summe von Formen. Per Definition ist $f(p) = 0$ für jedes $p \in \mathrm{V}$, was wiederum laut Lemma 3.1.9 genau dann passiert, wenn $F_i(a) = 0$, für alle $0 \leq i \leq r$. Hier ist $a \in \mathbb{A}^n$ ein beliebiger Repräsentant von p. Da $\mathrm{V} \neq \varnothing$ folgt direkt, dass $F_0 = 0$, woraus wir $f(0, \ldots, 0) = 0$ schlussfolgern. (Da $f \in K[x_1, \ldots, x_{n+1}]$ können wir darin $0 \in \mathbb{A}^{n+1}$ einsetzen). Also, $\mathbb{IP}(\mathrm{V}) \subseteq \mathrm{I}_{\mathbb{A}}(\mathsf{Kon}(\mathrm{V}_{\mathbb{P}}(I)))$.

Für die andere Richtung sei $f \in \mathrm{I}_{\mathbb{A}}(\mathsf{Kon}(\mathrm{V}))$. Daher ist $f(a) = 0$ für jedes a deren Äquivalenzklasse p in V liegt. Es folgt, dass $f(p) = 0$ für alle $p \in \mathrm{V}$. Damit sind wir fertig. □

Lemma 3.1.25. *Sei $J \subseteq K[x_1, \ldots, x_{n+1}]$ ein homogenes Ideal. Folgende Aussagen sind äquivalent:*

(i) $\mathrm{V}_{\mathbb{P}}(J) = \varnothing$

(ii) $\mathrm{V}_{\mathbb{A}}(J) \subseteq \{(0, \ldots, 0)\}$

(iii) $\sqrt{J} = I_{\mathbb{A}}(\mathrm{V}_{\mathbb{A}}(J)) \supseteq (x_1, \ldots, x_{n+1})$

(iv) $(x_1, \ldots, x_{n+1})^N \subseteq J$ *für irgendein* $N \geq 0$.

Beweis. Das $(i) \Leftrightarrow (ii)$ ist völlig klar. Sei $\mathrm{V}_{\mathbb{A}}(J) \subseteq \{(0, \ldots, 0)\}$, daher $\mathrm{V}_{\mathbb{A}}(J) = \{(0, \ldots, 0)\}$ oder $\mathrm{V}_{\mathbb{A}}(J) = \varnothing$. Im ersten Fall folgt aus Hilberts Nullstellensatz 1.2.43, dass $\sqrt{J} = I_{\mathbb{A}}(\mathrm{V}_{\mathbb{A}}(J)) = \mathfrak{m}_0 = (x_1, \ldots, x_{n+1})$ und im zweiten Fall, dass $\sqrt{J} = I_{\mathbb{A}}(\mathrm{V}_{\mathbb{A}}(J)) = (1)$. Damit haben wir $(ii) \Rightarrow (iii)$.

Die Implikation $(iii) \Rightarrow (iv)$ ist Lemma 1.2.14 (iv) und die letzte Äquivalenz $(iv) \Leftrightarrow (ii)$ ist auch völlig klar, was $(iv) \Rightarrow (i)$ einschließt, da (i) und (ii) äquivalent sind. □

Satz 3.1.26 (Projektiver Nullstellensatz)**.** *Sei $J \subseteq K[x_1, \ldots, x_{n+1}]$ ein homogenes Ideal.*

(1) Es gilt $\mathrm{V}_{\mathbb{P}}(J) = \varnothing$ genau dann, wenn es ein $N \in \mathbb{N}$ gibt, so dass alle Formen vom Grad $\geq N$ in J liegen. Mit anderen Worten, wenn $(x_1, \ldots, x_{n+1})^N \subseteq J$.

(2) Sei $\mathrm{V}_{\mathbb{P}}(J) \neq \varnothing$*. Dann ist* $\mathrm{I}_{\mathbb{P}}(\mathrm{V}_{\mathbb{P}}(J)) = \sqrt{J}$*, das Radikal von* J*.*

Beweis. Teil (1) ist Lemma 3.1.25. Teil (2) folgt von Lemma 3.1.24, da wir

$$\mathrm{I}_{\mathbb{P}}(\mathrm{V}_{\mathbb{P}}(J)) = \mathrm{I}_{\mathbb{A}}(\mathsf{Kon}(\mathrm{V}_{\mathbb{P}}(J))) = \mathrm{I}_{\mathbb{A}}(\mathrm{V}_{\mathbb{A}}(J)) = \sqrt{J}$$

haben. □

Es gelten noch viele weitere Analoga zu den affinen Resultaten im projektiven Fall. Die Beweise sind zumeist sehr ähnlich und oftmals sogar gleich. Zum Beispiel haben wir:

Lemma 3.1.27. *Auf* $\mathbb{P}^n$ *existiert eine Topologie, die* Zariski-Topologie*, bezüglich der genau die projektiven Varietäten die abgeschlossenen Mengen sind.*

Definition 3.1.28. *Sei* $\varnothing \neq \mathrm{V} \subseteq \mathbb{P}^n$ *eine nichtleere projektive Varietät. Der* homogene Koordinatenring *von* V *sei definiert als*

$$K_h[\mathrm{V}] := K[x_1, \ldots, x_{n+1}]/\mathrm{I}(\mathrm{V})$$

Aus 3.1.21 folgt sofort, dass V genau dann irreduzibel ist, wenn $K_h[\mathrm{V}]$ ein Integritätsbereich ist.

Definition 3.1.29. *Sei* $\mathrm{I} \subseteq K[x_1, \ldots, x_{n+1}]$ *ein homogenes Ideal. Ein Element* $F \in K_h[\mathrm{V}]$ *heißt* Form vom Grad d*, falls es eine Form* $\hat{F} \in K[x_1, \ldots, x_n, x_{n+1}]$ *vom Grad* d *gibt, sodass* $F = \overline{\hat{F}}$*.*

Mit $\overline{\hat{F}}$ bezeichnen wir die Restklasse von $\hat{F}$ unter dem Quotienten unter $\mathrm{I}(\mathrm{V})$.

Lemma 3.1.30. *Der Grad eines Elements* $F \in K[\mathrm{V}]$ *ist wohldefiniert.*

Beweis. Aufgabe. □

3.1.4 Hauptproblem von projektiven Varietäten - Grenzen der Koordinatenringe

Im affinen Fall hatten wir eine 1-1 Beziehung zwischen den Funktionen auf $\mathbb{A}^n$ (also polynomielle Abbildungen von $\mathbb{A}^n$ nach K) und dem Koordinatenring $K[x_1, \ldots, x_n]$ oder allgemeiner, zwischen den Funktionen auf $\mathrm{V} \subseteq \mathbb{A}^n$ und $K[\mathrm{V}]$. Genauer ließ sich ein Element $f \in K[\mathrm{V}]$ als Funktion auf V durch Auswerten auffassen, also indem wir $a \in \mathrm{V}$ auf $f(a) \in K$ abbilden.

Im projektiven Fall bekommen wir aber ein Problem. Wenn wir versuchen ein Element f des homogenen Koordinatenrings $K_h[\mathrm{V}]$ einer projektiven Varietät V an einem Punkt p von V auszuwerten, so erhalten wir im Allgemeinen je nach Wahl der homogenen Koordinaten von p unterschiedliche Ergebnisse. Betrachte etwa $\mathrm{V} = \mathbb{P}^1$, $f = x + y \in K_h[\mathrm{V}] = K[x, y]$ und $p = [1 : 1] = [2 : 2]$. Dann ist $f(1, 1) = 2 \neq 4 = f(2, 2)$.

Im Allgemeinen definieren also Elemente des Koordinatenrings durch Auswerten keine wohldefinierten Abbildungen. Die Elemente für die dies doch möglich ist, sind im folgenden Lemma charakterisiert.

Lemma 3.1.31. *Sei* $\mathrm{V} \subseteq \mathbb{P}^n$ *und* $f \in K_h[\mathrm{V}]$. *Es ist genau dann* $f(a) = f(\lambda a)$ *für alle* $a \in \mathbb{A}^{n+1} \setminus \{0\}$, $\lambda \in K^*$, *wenn* f *eine Konstante ist. Mit anderen Worten sind die einzigen Elemente* $f \in K_h[\mathrm{V}]$, *die durch die Setzung* $[a_1 : \cdots : a_{n+1}] \mapsto f(a_1, \ldots, a_{n+1})$ *eine wohldefinierte Abbildung* $\mathbb{P}^n \to K$ *definieren, die Konstanten.*

Beweis. Eine Richtung ist klar, jede Konstante definiert eine wohldefinierte Abbildung $\mathbb{P}^n \to K$. Sei also umgekehrt $f \in K_h[\mathrm{V}]$, sodass $f(a) = f(\lambda a)$ für alle $a \in \mathbb{A}^{n+1} \setminus \{0\}$ und $\lambda \in K^*$. Sei $a \in \mathbb{A}^{n+1} \setminus \{0\}$ beliebig und $f = F_0 + \cdots + F_r$ die Zerlegung von f in homogene Komponenten. Für alle $\lambda \in K^*$ gilt

$$0 = f(a) - f(\lambda a) = f(a) - F_0(a) - F_1(a)\lambda - \cdots - F_r(a)\lambda^r.$$

Mit anderen Worten hat das Polynom

$$g := (f(a) - F_0(a)) - F_1(a)X - \cdots - F_r(a)X^r \in K[X]$$

als Nullstellenmenge $\mathrm{V}(g) = K$. Dann muss aber schon $g = 0$ gelten (K ist algebraisch abgeschlossen). Folglich verschwinden alle Koeffizienten von g, weshalb $f(a) = F_0(a)$ gilt. Es ist F_0 eine Konstante, also $F_0(a) = F_0$. Da a beliebig war, ist $f = F_0$ konstant. □

Definition 3.1.32. *Der Quotientenkörper von einem homogenen Koordinatenring* $K_h[\mathrm{V}]$ *wird mit* $K_h(\mathrm{V})$ *bezeichnet und* homogener Quotientenkörper *von* V *genannt.*

Mit dem selben Argument wie auch für $K_h[\mathrm{V}]$ sehen wir, dass auch die meisten Elemente von $K_h(\mathrm{V})$ nicht Abbildungen (weder polynomial noch rational) von V nach K definieren. Wie in $K_h[\mathrm{V}]$ haben wir aber auch hier eine Klasse von Elementen, welche Abbildungen definieren:

Lemma 3.1.33. *Sei* $\mathrm{V} \subseteq \mathbb{P}^n$ *eine projektive Varietät. Die Elemente von* $K_h(\mathrm{V})$, *die durch Auswertung eine Abbildung* $\mathrm{V} \to K$ *definieren sind genau jene rationalen Funktionen* φ, *welche sich als Quotient* $\varphi = \frac{F}{G}$ *homogener Polynome* F, G *des gleichen Grades* $\mathsf{grad}(F) = \mathsf{grad}(G)$ *schreiben lassen.*

Beweis. Wir müssen beweisen, dass f/g unabhängig vom Wahl eines Repräsentanten von $p \in \mathrm{V}$ ist. Dies ist jedoch recht klar, da für ein homogenes Polynom f vom Grad d, $f(\lambda x) = \lambda^d f(x)$ gilt. Daher haben wir

$$\frac{f(p)}{g(p)} = \frac{\lambda^d f(p)}{\lambda^d g(p)} = \frac{f(\lambda p)}{g(\lambda p)},$$

wobei $d = \mathsf{grad}(f) = \mathsf{grad}(g)$. □

Auch hier sind es quasi die Elemente vom Grad 0. Das Phänomen, das wir hier sehen, ist ähnlich zum Satz von Liouville aus der Funktionentheorie. Wir werden dies aber nicht weiter vertiefen. Eine andere Richtung, die unser Gespräch hier andeutet sind die sogenannten *gradierten Ringe* (Ringe mit einer Graduierung). Aber auch diese werden wir an dieser Stelle nicht weiter erforschen.

Definition 3.1.34. *Sei* $\mathrm{V} \subseteq \mathbb{P}^n$ *eine projektive Varietät. Wir bezeichnen mit*

$$K(\mathrm{V}) := \left\{ \frac{F}{G} \in K_h(V) \;\middle|\; F, G \in K_h[V] \text{ homogen mit } \mathsf{grad}(F) = \mathsf{grad}(G) \right\}$$

den Funktionenkörper *von* V*. Elemente von* $K(\mathrm{V})$ *werden* rationale Funktionen *auf* V *genannt.*

Lemma 3.1.35. *Der Funktionenkörper* $K(\mathrm{V})$ *einer projektiven Varietät* $\mathrm{V} \subseteq \mathbb{P}^n$ *ist ein Körper und es gilt* $K \subseteq K(\mathrm{V}) \subseteq K_h(\mathrm{V})$*.*

Beweis. Die Inklusion $K(\mathrm{V}) \subseteq K_h(\mathrm{V})$ gilt per Definition und da $K_h(\mathrm{V})$ der Quotientenkörper ist, daher $1 \neq 0$, darf auch kein Element $a \neq 0$ von K unter dem Lokalisationshomomorphismus gleich Null gesetzt werden, da sonst $1 = \frac{1}{a}\frac{a}{1} = \frac{1}{a}0 = 0$ wäre. □

Zum Vergleich, die Inklusion $K_h[\mathrm{V}] \subseteq K(\mathrm{V})$ gilt im allgemeinen nicht (V irreduzibel).

Definition 3.1.36. *Sei* $p \in \mathrm{V} \subseteq \mathbb{P}^n$ *und* $\varphi \in K(\mathrm{V})$*. Wir sagen, dass* φ *bei* p definiert *ist, wenn es Formen* $F, G \in K(\mathrm{V})$ *vom gleichen Grad gibt, so dass* $\varphi = \frac{F}{G}$ *und* $G(p) \neq 0$*.*

Lemma 3.1.37. *Sei* $\varphi \in K(\mathrm{V})$ *definiert bei* $p \in \mathrm{V} \subseteq \mathbb{P}^n$*. Dann ist die* Auswertung *von* φ *bei* p*, gegeben durch* $\varphi(p) := \frac{F(p)}{G(p)}$*, wohldefiniert.*

Beweis. Sind $\varphi = \frac{F}{G} = \frac{F'}{G'}$ zwei Darstellungen, so ist $FG' = F'G$. Daher gilt also auch $F(p)G'(p) = F'(p)G(p)$ und somit $\frac{F(p)}{G(p)} = \frac{F'(p)}{G'(p)}$. □

Sei $p \in \mathrm{V} \subseteq \mathbb{P}^n$. Wir definieren

$$\mathcal{O}_p(\mathrm{V}) := \{\varphi \in K(\mathrm{V}) \mid \varphi \text{ ist definiert auf } p\}. \tag{21}$$

Lemma 3.1.38. *Sei* $\mathrm{V} \subseteq \mathbb{P}^n$ *und* $p \in \mathbb{P}$*. Dann ist* $\mathcal{O}_p(\mathrm{V})$ *ein lokaler Ring mit Maximalideal*

$$\mathfrak{m}_p(\mathrm{V}) = \left\{ \frac{F}{G} \;\middle|\; F, G \text{ homogen mit } G(p) \neq 0 \text{ und } \; F(p) = 0 \right\}.$$

Wir nennen daher $\mathcal{O}_p(\mathrm{V})$ den *lokalen Ring von* V *bei* p*.*

3.1.5 Projektive Koordinatentransformationen

Definition 3.1.39. *Eine bijektive Abbildung* $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ *heißt* lineare Koordinatentransformation *falls* $T = (T_1, \ldots, T_{n+1})$ *für gewisse Formen* T_i *vom Grad* 1 *sind.*

Es ist klar, dass sich eine lineare Koordinatentransformation als

$$T(a) = Aa$$

für eine gewisse invertierbare $(n+1) \times (n+1)$-Matrix A schreiben lässt. Insbesondere ist jede lineare Koordinatentransformation auch eine affine Koordinatentransformation, wo jedoch der Translationsvektor v gleich 0 ist. Aus der linearen Algebra wissen wir:

Lemma 3.1.40. *Sei $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ eine lineare Koordinatentransformation und L eine Gerade mit $0 \in L$ (es geht durch den Uhrsprungspunkt). Dann gilt $0 \in T(L)$.*

Korollar 3.1.41. *Sei $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ eine lineare Koordinatentransformation. Dann induziert T eine Bijektion $T : \mathbb{P}^n \to \mathbb{P}^n$. Diese induzierte Abbildung nennen wir eine* projektive Koordinatentransformation.

Um die Notation etwas einfacher zu halten werden wir V^T für $T^{-1}(\mathrm{V})$ schreiben.

Lemma 3.1.42. *Sei F_i eine Form vom Grad d_i für $i = 1, \dots, r$ und T eine projektive Koordinatentransformation, dargestellt durch Formen $T_1, \dots, T_{n+1}$ vom Grad 1. Schreiben wir $F_i^T := F_i(T_1, \dots, T_{n+1})$, so gilt*

$$\mathrm{V}(F_1, \dots, F_r)^T = \mathrm{V}(F_1^T, \dots, F_r^T).$$

Ferner ist $\mathrm{V} := \mathrm{V}(F_1, \dots, F_r)$ genau dann irreduzibel, wenn V^T irreduzibel ist.

Bemerkung 3.1.43. Man beachte, dass F^T das Bild und V^T das Urbild bezeichnet. Diese Diskrepanz ist mal wieder ein Resultat der "Richtungsänderung" die sich vom Übergang von Geometrie zu Algebra, und umgekehrt, vollzieht. So wirkt eine projektive Koordinatentransformation nicht nur auf der geometrischen Seite, auf Varietäten V, auf offensichtliche Art und Weise, sondern auch auf Seite der homogenen Koordinatenringe durch "Rückzug" entlang der Transformation. Allgemeiner induziert, wie im affinen Fall, eine Abbildung projektiver Varietäten $\mathrm{V} \to \mathrm{W}$ einen K-Algebrenmorphisms $K_h[\mathrm{W}] \to K_h[\mathrm{V}]$ zwischen den homogenen Koordinatenringen.

Beweis. Sei $p \in \mathbb{P}^n$ beliebig. Es ist $p \in \mathrm{V}^T = T^{-1}(\mathrm{V})$ genau dann, wenn $T(p) \in \mathrm{V} = \mathrm{V}(F_1, \dots, F_r)$, also genau dann wenn $F_i^T(p) = F_i(T(p)) = 0$ für alle $1 \leq i \leq r$. Das bedeutet aber gerade, dass $p \in \mathrm{V}(F_1^T, \dots, F_r^T)$, womit die gewünschte Gleichheit gezeigt ist.

Nun zur Irreduzibilität. Von Hilberts Nullstellensatz wissen wir, dass $\mathrm{V}(I) = \mathrm{V}(\sqrt{I})$. Daher gibt es ein Radikalideal $J = \sqrt{(F_1, \dots, F_r)}$, mit $\mathrm{V}(J) = \mathrm{V}(F_1, \dots, F_r)$. Da auch J endlich erzeugt ist und das Radikal eines homogenen Ideals wieder radikal ist (siehe Aufgaben), gibt es Formen $F_1', \dots, F_s'$, mit $\mathrm{V} = \mathrm{V}(F_1', \dots, F_s')$. Somit können wir ohne Einschränkung annehmen, dass die Formen $F_1, \dots, F_r$ bereits ein Radikalideal definiert haben. Proposition 3.1.21 besagt nun, dass $(F_1, \dots, F_{n+1})$ ein Primideal ist. Per Definition ist T invertierbar und wir wollen das Inverse mit $G := T^{-1}$ bezeichnen. Sei $AB \in (F_1^T, \dots, F_r^T)$. Dann ist $(F_1, \dots, F_r) \ni (AB)(G) = A(G)B(G)$. Da dies ein Primideal ist, gilt ohne Einschränkung $A(G) \in (F_1, \dots, F_r)$. Daraus wiederum folgt, dass $(A(G))(F) \in (F_1^T, \dots, F_r^T)$, was nun die Primheit von $(F_1^T, \dots, F_r^T)$ und damit laut Proposition 3.1.21 die Irreduzibilität von V^T beweist. Beachte, dass wir nun Äquivalenzumformungen getätigt haben, also direkt die "genau dann"-Aussage bewiesen haben. □

3.2 Die affine Überdeckung

Wir haben bis jetzt $\mathbb{P}^n$ als ein Quotient von $\mathbb{A}^{n+1}$ betrachtet und gesehen, dass diese Sichtweise stark eingeschränkt ist. Spezifisch, man könnte die Funktionen darüber schon nicht mehr als kein Koordinatenring auffassen. Oder anders gesagt, die globalen Funktionen sind zu wenige, um eine projektive Varietät wiederherzustellen. Die Lösung dazu ist es als eine Garbe, spezifisch Schemata aufzufassen. Wir wollen nun etwas in diese Richtung gehen, obwohl wir natürlich Formal weder Garbe noch Schemata ansprechen werden.

Was wir nun machen wollen, ist $\mathbb{P}^n$ als eine Vereinigung von $\mathbb{A}^n$ mit sich selbst ($n+1$ mal) aufzufassen. Dann werden wir uns die Funktionsringe lokal ansehen. Diese können $\mathbb{P}^n$ ganz erfassen. Auch hier kann man Parallelen zur Funktionstheorie aufbauen. Zum Beispiel ist ln oder exp nicht auf ganz $\mathbb{C}$ definiert, aber sobald man eine Gerade (Strahl) vom Definitionsbereich weglässt, sind beide Funktionen definiert. Wir haben also deutlich mehr Funktionen auf offenen Teilmengen.

Zuerst müssen wir aber Methoden aufbauen um zwischen dem Affinen und Projektivem zu wechseln.

3.2.1 Homogenisierung und Dehomogenisierung von Polynomen

Sei $f \in K[x_1 \dots, x_n]$ ein Polynom. Wir stellen dies als eine Summe von Formen $f = F_0 + \cdots + F_d$ da und definieren

$$f^* := x_{n+1}^d F_0 + x_{n+1}^{d-1} F_1 + \cdots + x_{n+1} F_{d-1} + F_d = x_{n+1}^d f\left(\frac{x_1}{x_{n+1}}, \cdots, \frac{x_n}{x_{n+1}}\right). \tag{22}$$

Es ist klar, dass dies nun eine Form in $K[x_1, \dots, x_{n+1}]$ ist. Dies wird *Homogenisierung* von f genannt.

Wir definieren nun dessen inverses: Man nehme ein homogenes Polynom $F \in K[x_1, \dots, x_{n+1}]$. Wir definieren

$$F_*(x_1, \dots, x_n) := F(x_1, \dots, x_n, 1) \tag{23}$$

und nennen es die *Dehomogenisierung* von F. Wie der Name es schon andeutet muss dies natürlich nicht mehr homogen sein.

Lemma 3.2.1. *Sein $f, g \in K[x_1, \dots, x_n]$ Polynome und $F, G \in K[x_1, \dots, x_{n+1}]$ Formen. Es gilt*

(i) $(FG)_* = F_* G_*$

(ii) $(fg)^* = f^* g^*$

(iii) $(F+G)_* = F_* + G_*$

(iv) $x_{n+1}^t (f+g)^* = x_{n+1}^s f^* + x_{n+1}^r g^*$, *wobei* $r = \mathsf{grad}(f), s = \mathsf{grad}(g)$ *und* $t = r + s - \mathsf{grad}(f+g)$.

Beweis. (i) Es gilt

$$\begin{aligned}(FG)_*(x_1,\ldots,x_n) &= FG(x_1,\ldots,x_n,1) = F(x_1,\ldots,x_n,1)G(x_1,\ldots,x_n,1)\\ &= F_*(x_1,\ldots,x_n)G_*(x_1,\ldots,x_n) = (F_*G_*)(x_1,\ldots,x_n).\end{aligned}$$

(ii) Sei $\mathsf{grad}(f) = d$ und $\mathsf{grad}(g) = d'$. Wir haben

$$\begin{aligned}(fg)^*(x_1,\ldots,x_n) &= x_{n+1}^{d+d'} fg\left(\frac{x_1}{x_{n+1}},\cdots,\frac{x_n}{x_{n+1}}\right)\\ &= x_{n+1}^{d} f\left(\frac{x_1}{x_{n+1}},\cdots,\frac{x_n}{x_{n+1}}\right) x_{n+1}^{d'} g\left(\frac{x_1}{x_{n+1}},\cdots,\frac{x_n}{x_{n+1}}\right)\\ &= f^*(x_1,\ldots,x_n)g^*(x_1,\ldots,x_n).\end{aligned}$$

(iii)

$$\begin{aligned}(F+G)_*(x_1,\ldots x_n) &= (F+G)(x_1,\ldots,x_n,1) = F(x_1,\ldots,x_n,1) + G(x_1,\ldots,x_n,1)\\ &= F_*(x_1,\ldots,x_n) + G_*(x_1,\ldots,x_n) = (F+G)_*(x_1,\ldots,x_n)\end{aligned}$$

(iv)

$$\begin{aligned}x_{n+1}^t(f+g)^* &= x_{n+1}^t x_{n+1}^{\mathsf{grad}(f+g)}\left(f\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_n}{x_{n+1}}\right) + g\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_1}{x_{n+1}}\right)\right)\\ &= x_{n+1}^{r+s}\left(f\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_n}{x_{n+1}}\right) + g\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_1}{x_{n+1}}\right)\right)\\ &= x_{n+1}^s f^*(x_1,\ldots,x_{n+1}) + x_{n+1}^r g^*(x_1,\ldots,x_{n+1}).\end{aligned}$$

□

Lemma 3.2.2. *Sei $f \in K[x_1,\ldots,x_n]$ ein Polynom und $0 \neq F \in K[x_1,\ldots,x_{n+1}]$ eine Form mit $F = x_{n+1}^r F'$, wobei $x_{n+1} \nmid F'$. Es gilt*

(i) $(f^*)_* = f$;

(ii) $(F_*)^* = F'$ *bzw.* $F = x_{n+1}^r (F_*)^*$.

Beweis. Dies ist recht klar. Unter der Notation wie oben, nehme man $f \in K[x_1,\ldots,x_n]$. Dann gilt

$$f(x_1,\ldots,x_n) \mapsto x_{n+1}^d f\left(\frac{x_1}{x_{n+1}},\cdots,\frac{x_n}{x_{n+1}}\right) \mapsto 1^d f\left(\frac{x_1}{1},\cdots,\frac{x_n}{1}\right) = f(x_1,\ldots,x_n).$$

Umgekehrt, sei $F = x_{n+1}^r F'$, wobei F' nun von x_{n+1} teilerfremd ist. Sei $\mathsf{grad}(F') = d$. Dann ist $F'_*(x_1,\ldots,x_n) = F'(x_1,\ldots,x_n,1)$ wieder ein Polynom vom Grad d. Als solches ist

$$(F'_*)^*(x_1,\ldots,x_{n+1}) = x_{n+1}^d F\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_n}{x_{n+1}},1\right) = F(x_1,\ldots,x_{n+1}),$$

da F ja homogen ist. Teil (i) von Lemma 3.2.1 ergibt nun

$$(F_*)^* = ((x_{n+1}^r)_* F'_*)^* = (F'_*)^* = F',$$

wie gewünscht. □

Es folgt, dass die Faktorisierung von f genau die selbe ist, wie die Faktorisierung von f^*. Auf der anderen Seite, ist die Zerlegung von F nicht ganz die selbe wie die Zerlegung von F_*. Dies gilt nur bis auf die Potenzen von x_{n+1}. Spezifisch haben wir also

Korollar 3.2.3. *Aus $F = GH$, mit $\mathsf{grad}(G) = a$, $\mathsf{grad}(H) = b$ folgt $F_* = G_* H_*$, mit $\mathsf{grad}(G_*) \leq a$ und $\mathsf{grad}(H_*) \leq b$. Spezifisch können G_* oder H_* konstant sein. Aus F irreduzibel folgt F_* irreduzibel.*

Auf der anderen Seite folgt aus $F_* = G_* H_*$, dass es $r, s, t \in \mathbb{N}$ gibt, so dass $x_{n+1}^r F = x_{n+1}^s G x_{n+1}^t H$.

Korollar 3.2.4. *Aus $F, G \in K[x_1, \ldots, x_{n+1}]$ teilerfremd folgt $F_*, G_* \in K[x_1, \ldots, x_n]$ teilerfremd.*

Beweis. Man nehme an, dass es $f, g, h \in K[x_1, \ldots, x_n]$, so dass $F_* = fh$ und $G_* = gh$. Dann gilt laut Teil (ii) von Lemma 3.2.1, dass $(F_*)^* = (fh)^* = f^* h^*$ und $(G_*)^* = (gh)^* = g^* h^*$, was durch Teil (ii) von Lemma 3.2.2 $F = x_{n+1}^r f^* h^*$ und $G = x_{n+1}^r g^* h^*$ impliziert. Da freilich aus $\mathsf{grad}(h) \geq 1$, $\mathsf{grad}(h^*) \geq 1$ folgt, muss $\mathsf{grad}(h) = 0$ sein, damit wir nicht zu einem Widerspruch kommen. □

3.2.2 Homogenisierung und Dehomogenisierung von Idealen und Varietäten

Sei $\mathrm{V} \subseteq \mathbb{A}^n$ und $K[x_1 \ldots, x_n] \supseteq \mathrm{I}(\mathrm{V}) = \mathrm{I}$. Wie bezeichnen mit

$$I^* := (\{f_i^* \mid f_i \in I\})$$

die *Homogenisierung* des Ideals I. In anderen Worten, wir homogenisieren jedes Polynom im Ideal und erzeugen dann ein Ideal mit dieser Menge.

Das wir dadurch ein homogenes Ideal erhalten, ist einfach nur Lemma 3.1.16. Wir definieren

$$\mathrm{V}^* := \mathrm{V}(\mathrm{I}^*) \subseteq \mathbb{P}^n$$

und nennen es die *Homogenisierung* von V. (Zur Erinnerung, wir hatten $\mathrm{I} = \mathrm{I}(\mathrm{V})$ angenommen.)

Umgekehrt, sei $\mathrm{V} \subseteq \mathbb{P}^n$ und $K[x_1, \ldots, x_{n+1}] \subseteq \mathrm{I}(\mathrm{V}) = I = (F_1, \ldots, F_r)$. Wir definieren

$$I_* := (\{(F_i)_* \mid F_i \in I\})$$

und nenne es die *Dehomogenisierung* von I. In diesem Fall haben wir eine vereinfachte Art und Weise, diese zu beschreiben:

Lemma 3.2.5. *Sei $I = (F_1, \ldots, F_r)$ ein homogenes Ideal. Dann ist*

$$I_* := ((F_1)_*, \ldots, (F_r)_*) .$$

In anderen Worten, die Dehomogenisierung eines Ideals hängt nicht vom Wahl der Erzeuger ab.

Beweis. Dies folgt direkt von Lemma 3.2.1, Teil (i) und (iii). Spezifisch, sei $I = (F_1, \ldots, F_r) = (G_1, \ldots, G_s)$. Dann kann man jedes der G_j's als $G_j = \sum_{i=1}^{r} \alpha_{ij} F_i^{e_{ij}}$ darstellen, wobei $\alpha_{ij} \in k[x_1, \ldots, x_{n+1}]$. Das Lemma besagt dann, dass $(G_j)_* = \sum_{i=1}^{r} (\alpha_{ij})_* (F_i)_*^{e_{ij}} \in ((F_1)_*, \ldots, (F_r)_*)$, was $((G_1)_*, \ldots, (G_s)_*) \subseteq ((F_1)_*, \ldots, (F_r)_*)$ impliziert. Bei Symmetrie hält auch die andere Seite und wir sind fertig. Hier haben wir nicht angenommen, dass r oder s endlich ist. Damit können wir einfach das ganze Ideal als eines der erzeugenden Mengen wählen. □

Bemerkung 3.2.6. Der Grund, warum man das Gleiche mit der Homogenisierung nicht machen kann, ist weil bei Teil (iv) vov Lemma 3.2.1, wir x_{n+1}^t haben. Daher können wir nicht schlussfolgern, dass $g_j^* \in (f_1^*, \ldots, f_r^*)$ sein wird, nur, dass es ein $t \in \mathbb{N}$ gibt, so dass $x_{n+1}^t g_j^* \in (f_1^*, \ldots, f_r^*)$.

Wir definieren

$$\mathrm{V}_*(I) := \mathrm{V}(I_*) \subseteq \mathbb{A}^n$$

und nennen es die *Dehomogenisierung* von V. Es gilt natürlich folgendes:

Lemma 3.2.7. *Sei $\mathrm{V} = \mathbb{A}^n$. Dann ist $\mathrm{V}^* = \mathbb{P}^n$. Auf der anderen Seite, für $\mathrm{V} = \mathbb{P}^n$ ist $\mathrm{V}_* = \mathbb{A}^n$.*

Beweis. Dies ist trivial, da in beiden Fällen die Ideale (0) sind. □

Lemma 3.2.8. *Sei $\mathrm{I} \subseteq K[x_1, \ldots, x_n]$ ein Ideal und $\mathrm{J} \subseteq K[x_1, \ldots, x_{n+1}]$ ein homogenes Ideal. Es gilt*

(i) $(\mathrm{I}^*)_* = \mathrm{I}$;

(ii) $\mathrm{J} \subseteq (J_*)^*$

(iii) $(\mathrm{V}^*(\mathrm{I}))_* = \mathrm{V}(I)$

(iv) $(\mathrm{V}_*(\mathrm{J}))^* \cup \mathrm{V}(x_{n+1}) = \mathrm{V}(J) \cup \mathrm{V}(x_{n+1})$. *Die Gleichheit* $(\mathrm{V}_*(\mathrm{J}))^* = \mathrm{V}(J)$ *gilt genau dann, wenn es ein erzeugendes System* $\mathrm{J} = (F_1, \ldots, F_r)$ *gibt, so dass* $x_{n+1} \nmid F_i$ *für alle* $1 \leq i \leq r$. *Andernfalls gilt schon* $(\mathrm{V}_*(\mathrm{J}))^* \cup \mathrm{V}(x_{n+1}) = \mathrm{V}(J)$.

Beweis. (i) & (ii) Dies sind einfach nur Teil (i) & (ii) von Lemma 3.2.2 respektive.
(iii) Bei Definition und Teil (i) von diesem Lemma haben wir $(\mathrm{V}^*(\mathrm{I}))_* = \mathrm{V}((\mathrm{I}^*)_*) = \mathrm{V}(\mathrm{I})$.
(iv) Dies folgt von unserer Bemerkung 3.2.6. □

Lemma 3.2.9. *Sei $I \subseteq K[x_1, \ldots, x_n]$ radikal. Dann ist I^* radikal.*

Beweis. Aufgabe. □

Lemma 3.2.10. *Sei $\mathfrak{p} \subseteq K[x_1, \ldots, x_n]$ prim. Dann ist $\mathfrak{p}^* \subseteq K[x_1, \ldots, x_{n+1}]$ prim.*

Beweis. Aufgabe. □

Wir erinnern uns, dass wir Teilmengen von $\mathbb{A}^n$ als Teilmegen von $\mathbb{P}^n$ auffassen können. Hier nochmal als Lemma formuliert:

Lemma 3.2.11. *Sei U_{n+1} wie in Formel (20) auf Seite 107 definiert. Dann ist die Abbildung*

$$\varphi_{n+1} : \mathbb{A}^n \to U_{n+1} \subseteq \mathbb{P}^n, \quad \text{gegeben durch} \quad (a_1, \ldots, a_n) \mapsto [a_1 : \ldots : a_n : 1]$$

eine Bijektion.

Dies gilt natürlich für jeden $1 \leq i \leq n+1$, aber für eine einheitliche Notation wählen wir die letzte Koordinate. Damit betten wir also $\mathbb{A}^n$ in $\mathbb{P}^n$ durch

$$\varphi_{n+1} : \mathbb{A}^n \to U_{n+1} \subseteq \mathbb{P}^n$$

ein. Wir haben nun eine zweite Möglichkeit kennengelernt, Varietäten zu homogenisieren, bzw. dehomogenisieren: Sein $W \in \mathbb{A}^n$ und $X \subseteq \mathbb{P}^n$. Wir können

$$V(I(\varphi_{n+1}(W))) \subseteq \mathbb{P}^n$$

(also, die kleinste Projektive Varietät, welches $\varphi(W)$ enthält) und

$$V\left(I\left(\varphi_{n+1}^{-1}(X)\right)\right)$$

(die kleinste (affine) Varietät, welches $\varphi_{n+1}^{-1}(X)$ enthält) betrachten. Wir wollen dies etwas studieren und unter anderem beweisen, dass diese Konstruktionen mit den Konstruktionen W^* und W_* übereinstimmen. Vorerst sagen wir aber folgendes:

Lemma 3.2.12. *Es gilt $V(I(\varphi_{n+1}^{-1}(X))) = \varphi_{n+1}^{-1}(X)$. In andern Worten $\varphi_{n+1}^{-1}(X)$ ist schon eine affine Varietät.*

Beweis. Sei $W = V(J)$. Bei Definition ist

$$\begin{aligned} \varphi_{n+1}^{-1}(X) &:= \{(a_1, \ldots, a_n) \mid [a_1 : \ldots : a_n : 1] \in W\} \\ &= \{(a_1, \ldots, a_n) \mid F_i(a_1, \ldots, a_n, 1) = 0, \quad \text{für jeden} \quad F_i \in J\} \\ &= \{(a_1, \ldots, a_n) \mid (F_i)_*(a_1, \ldots, a_n) = 0, \ F_i \in J\}, \end{aligned}$$

daher die Menge der Nullstellen von einer Menge von Polynomen (ob dies ein Ideal ist oder nicht, ist unwichtig). □

Bemerkung 3.2.13. Wenn wir $\mathbb{P}^n$ als einen topologischen Raum auffassen, haben wir hier bewiesen, dass die Einbettung φ_{n+1} stetig ist, da das Urbild einer abgeschlossenen Menge eine abgeschlossene Menge ist.

Proposition 3.2.14. *Sein* $\mathrm{V} \subseteq \mathrm{W} \subseteq \mathbb{A}^n$ *und* $X \subseteq Y \subseteq \mathbb{P}^n$*. Es gilt*

(i) $X_* = \varphi_{n+1}^{-1}(X)$*;*

(ii) $\varphi_{n+1}(\mathrm{V}) = \mathrm{V}^* \cap U_{n+1}$*;*

(iii) $\mathrm{V}^* = \mathrm{V}\left(\mathrm{I}(\varphi_{n+1}(\mathrm{V}))\right) \subseteq \mathbb{P}$*. In anderen Worten,* $\mathrm{V}^* \subseteq \mathbb{P}^n$ *ist die kleinste projektive Varietät, welches* $\varphi_{n+1}(\mathrm{V})$ *enthält.*

(iv) $\mathrm{V}^* \subseteq \mathrm{W}^* \subseteq \mathbb{P}^n$*;*

(v) $X_* \subseteq Y_* \subseteq \mathbb{A}^n$*;*

(vi) Aus $\mathrm{V} = \bigcup_i \mathrm{V}_i \subseteq \mathbb{A}^n$ *irreduzible Zerlegung folgt* $\mathrm{V}^* = \bigcup_i \mathrm{V}_i \subseteq \mathbb{P}^n$ *irreduzible Zerlegung. Spezifisch, aus* $\mathrm{V} \subseteq \mathbb{A}^n$ *irreduzibel folgt,* $\mathrm{V}^* \subseteq \mathbb{P}^n$ *irreduzibel.*

Beweis. (i) Sei $X = \mathrm{V}(J)$ mit $J = (F_1, \ldots, F_r)$. Bei Definition ist

$$X_* = \mathrm{V}((F_1)_*, \ldots, (F_r)_*) = \{(a_1, \ldots, a_n) \mid F_i(a_1, \ldots, a_n, 1) = 0\},$$

was mit $\varphi_{n+1}^{-1}(X)$ übereinstimmt (sieh Beweis von Lemma 3.2.12).

(ii) Sei $\mathrm{V} = \mathrm{V}(I)$. Wir können annehmen, dass I radikal ist, da wir $\mathrm{V}(I) = \mathrm{V}(\sqrt{I})$ haben. Bei Definition ist

$$\begin{aligned} \varphi_{n+1}(\mathrm{V}(\mathrm{I})) &= \{[a_1 : \cdots : a_n : 1] \mid (a_1, \ldots, a_n) \in \mathrm{V}(\mathrm{I})\} \\ &= \{[a_1 : \cdots : a_n : 1] \mid f(a_1, \ldots, a_n) = 0 \ \forall \ f \in I\}. \end{aligned}$$

Auf der anderen Seite ist

$$\begin{aligned} \mathrm{V}^*(I) \cap U_{n+1} &= \mathrm{V}(I^*) \cap U_{n+1} = \{[a_1 : \cdots : a_n, a_{n+1}] \mid a_{n+1}^d f\left(\frac{a_1}{a_{n+1}}, \ldots, \frac{a_n}{a_{n+1}}\right) = 0 \ \text{ und } \ a_{n+1} \neq 0\} \\ &= \left\{\left[\frac{a_1}{a_{n+1}} : \cdots : \frac{a_n}{a_{n+1}} : 1\right] \mid f\left(\frac{a_1}{a_{n+1}}, \ldots, \frac{a_n}{a_{n+1}}\right) = 0, \ a_{n+1} \neq 0\right\}. \end{aligned}$$

Diese zwei Mengen sind gleich, $[\frac{a_1}{a_{n+1}} : \cdots : \frac{a_n}{a_{n+1}}, 1] \sim [a_1 : \cdots : a_n : a_{n+1}]$, da $\lambda = a_{n+1} \neq 0$.

(iii) Sei $W \subseteq \mathbb{P}^n$ eine algebraisch Teilmenge, welches $\varphi_{n+1}(\mathrm{V})$ enthält, also $\varphi_{n+1}(\mathrm{V}) \subseteq W$. Man nehme ein $F \in \mathrm{I}(W)$. Daher, es ist Null auf ganz W, also ist es auch Null auf dessen Teilmenge $\varphi_{n+1}(\mathrm{V})$, also $F \in \mathrm{I}(\varphi_{n+1}(\mathrm{V}))$, was $F_* \in \mathrm{I}(\mathrm{V})$ impliziert. Teil (ii) von Lemma 3.2.2 besagt nun, dass $F = x_{n+1}^r (F_*)^* \in \mathrm{I}(\mathrm{V})^*$, da $F_* \in \mathrm{I}(\mathrm{V})$, also $(F_*)^* \in \mathrm{I}(\mathrm{V})^*$. Es folgt $\mathrm{I}(W) \subseteq \mathrm{I}(\mathrm{V})^* = \mathrm{I}(\mathrm{V}^*)$ was $\mathrm{V}^* = \mathrm{V}(\mathrm{I}(\mathrm{V}^*)) \subseteq \mathrm{V}(\mathrm{I}(W)) = W$ impliziert.

(iv) & (v) Dies folgt direkt von den Definitionen.

(vi) Sei $V \subseteq \mathbb{A}^n$. Von Lemma 3.2.8 folgt, dass $F \in I(V)^*$ genau dann, wenn $F_* \in I(V)$. Laut Lemma 3.2.10 wissen wir, dass Irreduzibilität von V, die Irreduzibilität von V^* impliziert.

Sei nun $V = \bigcup_i V_i \subseteq \mathbb{A}^n$ eine irreduzible Dekomposition. Da $V_i \subseteq V$ folgt von Teil (iii) diese Lemmas, dass $V_i^* \subseteq V^*$, also ist auch deren Vereinigung eine Teilmenge. Da $\bigcup_i V_i \subseteq V$, folgt von Teil (iii) und (ii), dass $\bigcup_i V_i^* \subseteq V^*$. Daher ist $V^* = \bigcup_i V_i^* \subseteq \mathbb{P}^n$ eine Dekomposition. Da V_i irreduzibel V_i^* irreduzibel impliziert, ist es eine irreduzible Darstellung und wir sind fertig. □

Aufgrund von Teil (iv) von Proposition 3.2.14 haben wir direkt folgende Definition:

Definition 3.2.15. *Sei* $V \subseteq \mathbb{A}^n$. *Dann nennen wir* $V^* \subseteq \mathbb{P}^n$ *den* projektiven Abschluss *von* V.

Lemma 3.2.16. *Sei* $V \subseteq \mathbb{A}^n$. *Es gilt* $I(V)^* = I(V^*)$.

Beweis. Bei Definition ist $V^* = V(I(V)^*)$. Da I(V) ein Radikalideal ist (affiner Nullstellensatz 1.2.43), folgt von Lemma 3.2.9, dass auch $I(V)^*$ ein Radikalideal ist. Sei zuerst $V^* \neq \varnothing$. Laut dem projektiven Nullstellensatz 3.1.26 wissen wir dann, dass $I(V^*) = I(V(I(V)^*)) = I(V)^*$, wie gewünscht.

Wenn $V^* = \varnothing$, muss $I(V^*) = I(\varnothing) = (1)$ gelten. Teil (iii) von Proposition 3.2.14 besagt $\varphi_{n+1}(V) \subseteq V^*$, woraus $V = \varnothing$ und daher $I(V)^* = I(\varnothing)^* = (1)^* = (1)$ folgt. □

3.2.3 Dehomogenisierung von Elementen des Koordinatenrings

Als nächstes wollen wir Elemente von $K_h[V]$ dehomogenisieren. Homogenisation ist so leider nicht möglich, da die äquivalente Konstruktion vom Wahl des Repräsentantens abhängen würde.

Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät und V^* dessen projektiver Abschluss. Sei $f \in K_h[V^*] = K[x_1, \ldots, x_{n+1}]/I(V)^*$. Wir definieren $F_* \in K[V] = K[x_1, \ldots, x_n]/I(V)$ wie folgt: man hebe das Element F hoch zu einem Element $\hat{F} \in K[x_1, \ldots, x_{n+1}]$ (daher, $F = \hat{F} + I(V^*)$), dehomogenisiere es (also betrachte $\hat{F}_* \in K[x_1, \ldots, x_n]$) und schließlich nehme die Restklasse

$$F_* := \overline{\hat{F}_*} \in K[V].$$

Lemma 3.2.17. *Die Konstruktion oben ist wohldefiniert.*

Beweis. Sein G, H Repräsentanten von F. Daher, $G - H = A \in I(V^*)$. Laut (iii) von Lemma 3.2.1 und (i) von Lemma 3.2.8 gilt $G_* - H_* = (G - H)_* = A_* \in (V^*)_* = I(V)$. □

Es ist klar, dass dies den Fall $V = \mathbb{P}^n$ verallgemeinert. Man erinnere sich an die Definition 3.1.34 eines Funktionskörpers $K(V)$ auf Seite 117.

Proposition 3.2.18. *Die Abbildung*

$$\alpha : K(\mathrm{V}^*) \to K(\mathrm{V}) \qquad \text{gegeben durch} \qquad \frac{F}{G} \mapsto \frac{F_*}{G_*}$$

ist ein Isomorphismus, wobei $F, G \in K_h[\mathrm{V}]_*$ Formen vom gleichem Grad sind. Spezifisch ist also

$$K(\mathbb{P}^n) \simeq K(\mathbb{A}^n) = K(x_1, \ldots, x_n).$$

Beweis. Als erstes zeigen wir, dass es wohldefiniert ist. Sei $\frac{F}{G} \sim \frac{F'}{G'}$. Daher, es gibt ein T, so dass $TFG' = TF'G$. Teil (i) von Lemma 3.2.1 besagt nun, dass $T_*F_*G'_* = T_*F'_*G_*$, daher $\frac{F_*}{G_*} = \frac{F'_*}{G'_*}$. Das es ein Ringhomomorphismus ist, ist klar.

Sei $\frac{f}{g} \in K(\mathrm{V})$. Dann bildet laut Lemma 3.2.2, Teil (i), $\frac{f^*}{g^*}$ genau auf $\frac{f}{g}$ ab. Man beachte jedoch, dass $\mathsf{grad}(f^*)$ nicht mit $\mathsf{grad}(g^*)$ übereinstimmen muss. Bei Definition 3.1.34 müssen die Grade jedoch gleich sein. Wir können dies einfach beheben, indem wir den Nenner oder Zähler mit erine geeigneten Potenz von x_{n+1} multiplizieren: Sprich $\frac{x_{n+1}^N f^*}{g^*}$ oder $\frac{f^*}{x_{n+1}^N g^*}$ betrachten. Da under der Dehomogenisierung x_{n+1} auf 1 abbildet, wird es immer noch auf $\frac{f}{g}$ abbilden und somit haben wir Surjektivität bewiesen.

Da es eine Ringhomomorphismus zwischen Körpern ist, muss es injektiv sein und wir sind fertig. □

Sei $p \in \mathrm{V} \subseteq \mathbb{A}^n$ und betrachte $\mathcal{O}_p(\mathrm{V})$, wie in Definition 1.5.18. Durch die Einbettung $\varphi_{n+1} : \mathbb{A}^n \hookrightarrow \mathbb{P}^n$ können wir p auch in V^* auffassen und daher $\mathcal{O}_P(\mathrm{V}^*)$, wie in Formel (21) auf Seite 117 definiert, betrachten.

Proposition 3.2.19. *Es gibt eine Isomorphie*

$$\alpha : \mathcal{O}_p(\mathrm{V}^*) \to \mathcal{O}_p(\mathrm{V}).$$

Spezifisch also auch

$$\mathcal{O}_p(\mathbb{P}^2) \simeq \mathcal{O}_p.$$

Beweis. Es gilt $\mathcal{O}_p(\mathrm{V}) = (K[x_1, \ldots, x_n]/\mathrm{I}(\mathrm{V}))_{\mathfrak{m}_p}$ und $\mathcal{O}_p(\mathrm{V}^*) = (K[x_1, \ldots, x_{n+1}]/\mathrm{I}(\mathrm{V}^*))_{\mathfrak{m}_p}$. Wir definieren die Abbildung durch $\alpha\left(\frac{\overline{F}}{\overline{G}}\right) = \frac{\overline{F}_*}{\overline{G}_*}$, wobei $G(p) \neq 0$. Als erstes meren wir, dass dies Sinn macht, da wir direkt $\overline{G}_*(p) \neq 0$ schlussfolgern können.

Sei $\frac{\overline{F}_*}{\overline{G}_*} = 0$. Daher, es gibt ein $\overline{t} \in K[\mathrm{V}]$ mit $\overline{t}(p) \neq 0$, so dass $\overline{tF}_* = 0$ in $K[\mathrm{V}]$, sprich $tF_* \in \mathrm{I}(\mathrm{V})$. Es folgt auch direkt, dass $t(p) \neq 0$. Aus den Eigenschaften von Idealen folgt direkt, dass für jeden $r \geq 0$, wir $x_{n+1}^r t^* F \in \mathrm{I}(\mathrm{V})^* = \mathrm{I}(\mathrm{V}^*)$ haben. Laut Teil (ii) von Lemma 3.2.2 folgt, dass $t^*F \in \mathrm{I}(\mathrm{V}^*)$, sprich $\overline{t^*F} = 0$ in $K_h[\mathrm{V}^*]$, was uns nun $\frac{\overline{F}}{\overline{G}} = 0$ und somit Injektion liefert.

□

Für eine jegliche projektive Varietät $\mathrm{W} \subseteq \mathbb{P}^n$ ergibt die Überdeckung $\bigcup_{i=1}^{n+1} U_i = \mathbb{P}^n$ (Teil (iii) von Proposition 3.1.4) eine Überdeckung $\bigcup_{i=1}^{n+1} (U_i \cap \mathrm{W}) = \mathrm{W}$.

Man erinnere sich an die Konstruktion von W_*. Dies kann man natürlich mit jedem der φ_i, $1 \leq i \leq n+1$ machen. Lass uns diese mit W_i bezeichnen. Teil (ii) von Proposition 3.2.14 besagt, dass $\mathrm{W}_i = \mathrm{W} \cap U_i$. Als solches haben wir also $\mathrm{W} = \bigcup_{i=1}^{n+1} \mathrm{W}_i$. In anderen Worten:

Proposition 3.2.20. *Jede projektive Varietät $\mathrm{W} \subseteq \mathbb{P}^n$ kann als eine Vereinigung von $n+1$ affinen Varietäten W_i dargestellt werden.*

Daher hat also jeder Punkt $p \in \mathbb{P}^n$ eine Umgebung U_p, welches ganz in einem der V_i's liegt. In andern Worten, jede *lokale Frage* (also, Fragen wie Regularität, da eine Varietät genau dann regulär ist, wenn es in jedem Punkt regulär ist, also für jeden Punkt es eine Umgebung gibt, wo die Varietät regulär ist) kann affin Beantwortet werden.

Korollar 3.2.21. *Sei $p \in \mathrm{V} \subseteq \mathbb{P}^n$ ein allgemeiner Punkt, und $U_1, \ldots, U_k$ die affinen offen Mengen, in denen p liegt. Daher $p = (x_1 : \cdots : x_k : 0 : \cdots : 0)$, mit $x_j \neq 0$ für $1 \leq j \leq k$. Sei $p_j = \left(\frac{x_1}{x_j} : \cdots : \frac{x_{j-1}}{x_j} : 1 : \frac{x_{j-1}}{x_j} : \cdots : x_k : 0 \cdots : 0\right) \in U_j$ das zugehörige Punkt in der gegebenen affinen Überdeckung. Dann gilt*

$$\mathcal{O}_p(\mathrm{V}) \simeq \mathcal{O}_{p_j}(\mathrm{V}_j) \simeq K[\mathrm{V}_i]_{\mathfrak{m}_{p_j}},$$

wobei $\mathfrak{m}_{p_j}$ das zu p_j zugehörige Primideal ist.

Beweis. Dies ist ein Korollar von Propositionen 3.2.19. Spezifisch wissen wir, dass jedes $p \in \mathbb{P}^n$ in irgendeinem U_i ist. Aus Symmetriegründen können wir sagen, dass $p = p_{n+1} \in U_{n+1}$. Wir können also p als ein Punkt von $\mathbb{A}^n$ unter der Isomorphie $\varphi_{n+1} : \mathbb{A}^n \to U_{n+1}$ auffassen. □

4 Planare projektive Kurven

4.1 Lokale Eigenschaftgen und die projektive Schnittzahl

4.1.1 Definitionen und Notationen von lokalen Eigenschaften

Sein $F, G \in K[x, y, z]$ Formen. Wir sagen, dass $F \sim G$, wenn es ein $0 \neq \lambda \in K$ gibt, so dass $G = \lambda F$. Von nun an, werden wir Formen unter dieser Äquivalenzrelation sehen.

Definition 4.1.1. *Eine planare projektive Kurve (oder einfach Kurve) ist eine Äquivalenzklasse von Formen $F \in K[x, y, z]$, unter der Relation $F \sim G$, wenn es ein $\lambda \in K$ gibt, so dass $G = \lambda F$.*

Der Grad einer Kurve ist definiert als den Grad eines der Repräsentanten davon. Da $0 \neq \lambda \in K$ beim multiplizieren mit einem Polynom F, den Grad nicht verändert, ist diese Definition nicht vom Wahl des Repräsentanten abhängig.

Wir werden die selben Notationen und Definitionen die wir im affinen Fall geben haben auch hier benutzen. Beispiele davon sind einfache und vielfache Komponente etc. Wenn man sich also an eine Definition nicht erinnert kann man es da nachschauen. Gleichwie schreiben wir auch $\mathcal{O}_p(F)$ statt $\mathcal{O}_p(\mathrm{V}(F))$.

Die Tatsache, dass lokale Fragen auf dem affinen Fall zurückgeführt werden kann, erlaubt uns auch, Definitionen im projektivem Fall sinnvoll einzuführen. Zum Beispiel, Satz 2.3.35 besagt, dass die Multiplizität eines Punktes auf einer (affinen) Kurve nur vom lokalen Ring an diesem Punkt abhängt. Wir definieren also:

Definition 4.1.2. *Sei F eine projektive planare Kurve mit $p \in U_i$ für irgendein $i = 1, 2, 3$. Wir definieren die* Multiplizität *von F auf p als $\mu_p(F) := \mu_p(F_*)$, wobei F_* die Dehomogenisierung von F mit φ_i ist.*

Korollar 3.2.21 (3.2.21 .. latex ..) besagt, dass es nicht am Wahl von U_i abhängt.

Lemma 4.1.3. *Die Multiplizität ist invariant unter einem projektivem Variablenwechsel.*

Beweis. Folgt von den Korollaren 3.2.21 (3.2.21 .. latex ..) und 2.3.36. □

Definition 4.1.4. *Eine projektive planare Kurve vom Grad 1 heißt eine* Gerade.

Lemma 4.1.5. *Sei $\{p_1, \ldots, p_r\} \subseteq \mathbb{P}^n$. Es gibt eine Gerade (im Sinne von Definition 4.1.4) $L \in K[x, y, z]$, so dass $L(p_i) \neq 0$ für alle $1 \leq i \leq r$.*

In anderen Worten, die Gerade geht durch keinen der Punkte.

Beweis. Man nehme einen Punkt $q \neq p_i$, $1 \leq i \leq r$. Da 2 Punkte eine Gerade festlegen, gibt es auf $r+1$ Punkten maximal $k := \frac{r(r+1)}{2}$ verschiedene Geraden. Daher gibt es, von q ausgehend und mit einem der p_i verbindend, maximal $k < \infty$ verschiedene Geraden. Sei $q = [u : v : w]$ mit $w \neq 0$. Eine beliebige Gerade durch q ist von der Form $L_a := x + ay - \frac{u+av}{w} z$. Da L_a und

L_b genau dann die gleiche Gerade definieren, wenn $a = b$ (der Koeffizient von x ist 1) und es unendlich viele $a \in K$ gibt, können wir eine (unendlich viele) Geraden finden, welche durch keine der p_r gehen. □

Wir erinnern uns daran, dass ein lineares Variablenwechsel eine invertierbare Matrix ist. Daher, $T : \mathbb{P}^2 \to \mathbb{P}^2$ ist quasi ein invertierbares 3×3 Matrix $T = (t_{ij})$. Damit wir ein Punkt $p = [a : b : c]$ auf $T(p) = [t_{11}a + t_{12}b + t_{13} : t_{21}a + t_{22}b + t_{23}c : t_{31}a + t_{23}b + t_{33}c]$ abgebildet.

Bemerkung 4.1.6. Man erinnere sich, dass Punke in $\mathbb{P}^n$ genau die Geraden in $\mathbb{A}^{n+1}$ waren, welche durch den Urprung gehen. Gleichwie sind auch die Geraden in $\mathbb{P}^n$, genau die Flächen in $\mathbb{A}^{n+1}$, welche durch den Ursprung gehen. Diese sollte beom Verständniss des folgenden Lemmas helfen.

Lemma 4.1.7. *Sein p', q', r', s' und p'', q'', r'', s'' Punkte auf $\mathbb{P}^2$, so dass keine 3 (von einer der 2 Mengen) auf einer Gerade liegen. Es gibt eine eindeutige invertierbare Matrix $T = (t_{ij})$, so dass $T(p) = p'$, $T(q) = q'$, $T(r) = r'$ und $T(s) = s'$.*

Beweis. Sein $p = [1 : 0 : 0]$, $q = [0 : 1 : 0]$, $r = [0 : 0 : 1]$, $s = [1 : 1 : 1]$ und $p' = [a_1 : a_2 : a_3]$, $q' = [b_1 : b_2 : b_3]$, $r' = [c_1 : c_2 : c_3]$, $s' = [d_1 : d_2 : d_3]$. Da p', q', r' nicht auf einer Gerade liegen, ist die Matrix

$$T'' = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

invertierbar. (Affine gesehen, wären ansonsten die 3 Vektoren auf einer Ebene). Als solches hat das System von linearen Gleichungen

$$\begin{aligned} \lambda a_1 + \mu b_1 + \nu c_1 &= d_1 \\ \lambda a_2 + \mu b_2 + \nu c_2 &= d_2 \\ \lambda a_3 + \mu b_3 + \nu c_3 &= d_3 \end{aligned}$$

eine eindeutige Lösung. Des weiteren sind λ, μ und ν ungleich Null, da keine 3 Punkte auf einer Gerade liegen. Wäre nämlich $\lambda = 0$, dann wäre $\mu x + \nu y - z = 0$ eine Gerade auf der die Punkte q', r' und s' liegen würden (affin: $\mu x + \nu y - z = 0$ wäre eine Ebene auf der die Geraden q', r', s' liegen würden). Definiere

$$T' = \begin{pmatrix} \lambda a_1 & \mu b_1 & \nu c_1 \\ \lambda a_2 & \mu b_2 & \nu c_2 \\ \lambda a_3 & \mu b_3 & \nu c_3 \end{pmatrix}.$$

Es gilt

$$T'(p) = [\lambda a_1 : \lambda a_2 : \lambda a_3] = [a_1 : a_2 : a_3] = p'$$

und gleichwie

$$T'(q) = q', \qquad T'(r) = r'.$$

Schließlich haben wir auch

$$T'(s) = [\lambda a_1 + \mu b_1 + \nu c_1 : \lambda a_2 + \mu b_2 + \nu c_2 : \lambda a_3 + \mu b_3 + \nu c_3] = [d_1 : d_2 : d_3] = s'.$$

Gleichwie definieren wir die Matrix S, welches p, q, r, s auf p'', q'', r'', s'' abbildet. Nun definiert $S \times T'^{-1}$ unsere gewünschte Matrix. □

Korollar 4.1.8. *Sein $p, p' \in \mathbb{P}^2$, $L_1, L_2, L_1', L_2' \subseteq \mathbb{P}^2$ projektive Geraden, mit $L_1 \neq L_2$, $L_1' \neq L_2' \subseteq \mathbb{P}^2$, so dass $p \in L_1$, $p \notin L_2$ und $p' \in L_1'$, $p' \notin L_2'$. Es gibt ein projektives Variablenwechsel $T : \mathbb{P}^n \to \mathbb{P}^n$, so dass $T(p) = p'$ und $T(L_i) = L_i'$, $i = 1, 2$.*

Beweis. Man nehme einen Punkt $q \in L_1$, welches nicht auf L_2 liegt und 2 Punkte $r, s \in L_2$, welche nicht auf L_1 liegen. Wir können dies machen, da $L_1 \neq L_2$. Da auch $p \in L_1$, $p \notin L_2$, liegen keine 3 von den Punkten p, q, r, s auf einer Gerade. Gleichwie mit L_i' für die Punkte p', q', r', s'. Lemma 4.1.7 besagt nun, dass wir ein lineares Variablenwechsel T finden können, welches p auf p' überfuhrt, q auf q' etc.

Da eine Gerade durch 2 Punkte definiert wird, geht L_i auf L_i' und p natürlich auf p'. □

4.1.2 Die projektive Schnittzahl

Den Halm konnten wir in der projektiven Geometrie problemlos vom affinen einfügen. Damit können wir so ziemlich alle lokalen Eigenschaften auch im projektiven Fall vom Halm bestimmen. Als Beispiel ist Regularität eine lokale Eigenschaft. Wir benutzen in der projektiven Welt die selbe Definition wie im Affinen, sieh Definition 2.2.6. Daher besagt Proposition 2.3.42 (nach Anwendung vom Korollar 3.2.3), dass für F irreduzibel, $\mathcal{O}_p(F)$ ein diskreter Bewertungsring ist.

Ein kleines Problem aber taucht mit der Schnittzahl a-priori auf: Dies ist zwar auch lokal Definiert (sie Satz 2.4.7), jedoch teilt man es dann noch mit dem Ideal erzeugt mit f und g. Das Problem hier ist, dass wir $F, G \in K[\mathrm{V}]$ nicht direkt als Elemente von $K(\mathrm{V})$ auffassen können, da $K(\mathrm{V})$ *nicht* das Quotientenkörper ist, sondern dessen Unterkörper bestehend aus rationalen Polynomen vom Grad Null (also, $\varphi = \frac{A}{B}$ mit $\mathsf{grad}(A) = \mathsf{grad}(B)$). Damit ist $\frac{F}{1}$ also nicht in $K(\mathrm{V})$. Diesen Problem lösen wir wie folgt:

Sei $p \in \mathbb{P}^2$ ein Punkt und L eine Gerade, welches nicht durch p geht. Sei F eine Kurve vom Grad d. Wir setzen $F_* := F/L^d$ (was eine rationale Funktion ist). Es gilt $F_* \in K(\mathbb{P}^2)$, da $\mathsf{grad}(F) = \mathsf{grad}(L^d)$. Sei L' eine andere Gerade, welches nicht durch p geht. Dann gilt $F/(L')^d = (L/L')^d F_*$.

Nun merke man folgendes, $(L/L') \in \mathcal{O}_p(\mathbb{P}^2)^*$ ist eine Einheit, da $L'(p) \neq 0$. Daher, unsere Definition hängt vom Wahl einer Gerade ab, aber nur bis auf eine Einheit, was in Algebra kein Problem ist. Man bemerke, dass sogar die Faktorisierung in Primzahlen nur bis auf Einheiten möglich ist.

Spezifisch ist es für uns keine Hürde, da wir folgendes Korollar haben:

Korollar 4.1.9. *Sein* $\mathsf{grad}(F) = m$, $\mathsf{grad}(G) = n$ *und* L, L' *Geraden, welche nicht durch* p *gehen. Dann gilt*

$$\mathcal{O}_p(\mathbb{P}^2)/(F/L^m, G/L^n) = \mathcal{O}_p(\mathbb{P}^2)/(F/(L')^m, G/(L')^n).$$

Beweis. Dies folgt einfach von der Tatsache, dass $(F/(L')^m, G/(L')^n) = ((L/L')F/L^m, (L/L')G/L^n) = (F/L^m, G/L^n)$, weil Einheiten im Ideal keinen Unterschied machen. □

Als solches ist die Definition

$$\mathcal{O}_p(\mathbb{P}^2/(F_*, G_*)) := \mathcal{O}_p(\mathbb{P}^2/(F/L^m, G/L^n)) \tag{24}$$

nicht vom Wahl der Gerade Abhängig. Hier ist mit F_* die "neue" Definition F/L^n gemeint.

Die Tatsache, dass wir F_* nun zweimal definiert haben, ist auch kein Problem, wie wir es nun zeigen wollen. Zuerst erinnere man sich, dass unter einem geeignetem projektivem Variablenwechsel, wir jede Gerade L in jede andere überführen können (Korollar 4.1.8), spezifisch auch in die Gerade $L_z(x, y, z) = z$, wessen Nullstellen $z = 0$, was klar $\{(x : y : 0) \mid x, y \in K\}$ ist. Bei der Einbettung $\varphi_3 : \mathbb{A}^2 \to \mathbb{P}^2$, $(x, y) \mapsto (x : y : 1)$, wird die Gerade L_z nicht getroffen. Dies wird auch die "Gerade bei Unendlich" genant. Natürlich ist es im Fall von $\mathbb{P}^n$ die "Hyperfläche bei Unendlich".

Sei $\alpha : K(\mathbb{P}^2) \to K(\mathbb{A}^2)$ die Isomorphie von Proposition 3.2.18, gegeben durch $\frac{F}{G} \mapsto \frac{F_*}{G_*}$.

Lemma 4.1.10. *Sei* $L_z = z$ *die Gerade bei Unendlich und* F *eine Form vom Grad* d*. Dann ist* $\alpha(F/L_z^d) = F(x, y, 1)$*, was mit der Definition von* F_* *in Abschnitt 3.2.1 übereinstimmt.*

Beweis. Da L_z ja z war, ist $L_z^d = z^d$, daher $F/L_z^d = F/z^d$. Wir erhalten

$$\alpha(F/z^d) = F_*/z_*^d = F_*/1^d = F(x, y, 1).$$

□

Für F, G projektive planare Kurven definieren wir die Schnittzahl am Punkt $p \in \mathbb{P}^2$ als

$$\mathfrak{I}(p, F \cap G) := \dim_K \left(\mathcal{O}_p(\mathbb{P}^2)/(F_*, G_*)\right) = \dim_K \left(\mathcal{O}_p/(F_*, G_*)\right),$$

wobei $\mathcal{O}_p$ wie gewohnt $\mathcal{O}_p(\mathbb{A}^2)$ bezeichnet. Die letzte Gleichung ist Proposition 3.2.19. In der Mitte benutzen wir die Definition in Gleichung (29).

Satz 4.1.11. *Die projektive Schnittzahl, wie oben definiert, erfüllt die Eigenschaften (1) - (7) in 2.4.2, mit der Ausnahme, dass wir nun Formen statt Polynome haben, bei (3)* $T : \mathbb{P}^2 \to \mathbb{P}^2$ *eine projektive Variablenwechsel ist und bei (7) wir die zusätzliche Bedingung* $\mathsf{grad}(H) = \mathsf{grad}(G) - \mathsf{grad}(F)$ *auf* H *stellen.*

Bemerkung 4.1.12. Die Bedingung $\mathsf{grad}(H) = \mathsf{grad}(G) - \mathsf{grad}(F)$ ist notwendig, damit $G + HF$ wieder eine Form ist.

Man erinnere sich nun an Proposition 2.4.8. Da es eine "genau dann" Aussage ist, können wir dies als Definition annehmen und übersetzen es so im projektiven Fall:

Definition 4.1.13. *Eine (projektive) Gerade L heißt* Tangente *von F am Punkt p, genau dann wenn $\mathfrak{I}(p, F \cap L) > \mu_p(F)$ gilt.*

Definition 4.1.14. *Ein Punkt p auf F heißt* normale *oder* herkömmlicher Singularität *wenn F genau $\mu_p(F)$ verschiedene Tangenten am Punkt p hat.*

Definition 4.1.15. *Zwei Kurven F, G werden* projektiv äquivalent *genannt, wenn es einen projektiven Variablenwechsel $T : \mathbb{P}^2 \to \mathbb{P}^2$ gibt, so dass $G = F^T$.*

Projektive Äquivalenzen erhalten so ziemlich alle Eigenschaften, wie auch im affinen Fall. Der Leser / die Leserin ist ermutigt dies ab und zu selber zu überprüfen.

4.2 Der Satz von Bézout

Wie am Anfang vom Kapitel 3 erwähnt, ist eines der Hauptgründe warum wir projektive Geometrie studieren, genau sagen zu können, wie oft sich Kurven schneiden. Dies ist der sogenannte Satz von Bézout.

Eher wir dies jedoch beweise, bedürfen wir noch einige Lemmas:

Lemma 4.2.1. *Zwei planare teilerfremde projektive Kurven F, G schneiden sich nur endlich oft.*

Beweis. Die Punkte $[a, b, c]$ die auf F oder G landen kann man als eine disjunkte Vereinigung von Punkten auffassen $U_z = \{[a : b : c] \mid c \neq 0\}$ und $H_\infty = \{[a : b : 0]\}$. Im ersten Fall, also U_z, sind wir im affinen Fall. Lemma 3.2.4 impliziert, dass $F_*, G_* \in K[x, y]$ teilerfremd sind. In Satz 2.1.2 haben wir schon gezeigt, dass sich F_* und G_* nur endlich oft schneiden.

Wir brauchen uns also nur noch die Punkte $[a : b : 0]$ ansehen, welche auf F und G liegen. Damit sind wir in $\mathbb{P}^1$ gelandet. Auch dies stellen wir als die disjunkte Vereinigung der Punkte $\{[a : b] \mid b \neq 0\}$ und $\{[a : 0]\}$ dar. Im ersten Fall sind wir in $\mathbb{A}^1$, damit hat jedes Polynom nur endlich viele Nullstellen, daher muss auch der Schnitt von 2 endlich sein und im zweiten Fall haben wir nur noch eine Variable, als ist auch da alles endlich (wir haben tatsächlich maximal eine solche Nullstelle). □

Sei $R = K[x, y, z]$ und $R_d \subseteq R$ die Menge der Formen vom Grad d. Es ist klar, dass dies ein K-Vektorraum ist, da wir solche Formen immer noch einander addieren und mit einem Skalar multiplizieren können.

Lemma 4.2.2. *Es gilt* $\mathsf{grad}_K(R_d) = \frac{(d+1)(d+2)}{2}$.

Beweis. Es ist klar, dass die Erzeuger $x^d, x^{d-1}y, x^{d-1}z, x^{d-2}y^2, x^{d-2}yz, x^{d-2}z^2, \ldots, z^d$ sind. Es gilt also die Anzahl all solcher Kombinationen zählen. Lass diese Zahl λ_d sein. Wir wollen zeigen, dass $\lambda_d = \frac{(d+1)(d+2)}{2}$. Dies ist einfach durch Induktion. Bei $d = 1$ stimmt es natürlich.

Man nehme es für $d - 1$ an. Um es für d zu beweisen, gruppiere man die Elemente wie folgt: alle die durch x teilbar sind und alle die x gar nicht enthalten. Es ist klar, dass die Elemente die durch x teilbar sind, gleich wieder von der selben Form sind, nur von einem Grad weniger. Daher, es sind alle Monomiale vom Grad $d-1$, also ist ihre Anzahl gleich λ_{d-1}. Die Elemente, die x nicht enthalten, sind Monomiale vom Grad d, aber nun in 2 Variablen. Diese sind klar $d + 1$ viele. Es gilt also

$$\begin{aligned}
\lambda_d &= \lambda_{d-1} + (d+1) \\
&= \frac{((d-1)+1)((d-1)+2)}{2} + \frac{2(d+1)}{2} \\
&= \frac{(d+1)(d+2)}{2}.
\end{aligned}$$

□

Satz 4.2.3 (Der Satz von Bézout)**.** *Sein F, G teilerfremde planare projektive Kurven über einen algebraisch abgeschlossenen Körper K vom Grad $\mathsf{grad}(F) = n$, $\mathsf{grad}(G) = m$. Es gilt*

$$\sum_p \mathfrak{I}(p, F \cap G) = nm.$$

Beweis. Von Lemma 4.2.1 wissen wir, dass sich F und G nur endlich oft schneiden. Die Summe macht also Sinn. Des weiteren können wir durch Lemma 4.1.5 eine Gerade finden, welche auf keinen dieser Punkte geht. Korollar 4.1.8 ermöglicht es uns annehmen, dass diese Gerade $L_z = z$ ist, was unsere "Gerade bei Unendlich" ist . Daher, alle unsere Schnittpunkte liegen in $\varphi_3(\mathbb{A}^3) \simeq U_3 = \{(x, y, 1) \mid x, y \in K\}$. Es folgt, dass

$$\sum_p \mathfrak{I}(p, F \cap G) = \sum_p \mathfrak{I}(p, F_* \cap G_*) = \dim_K K[x, y]/(F_*, G_*)$$

wobei die zweite Gleichung Proposition 2.4.9 ist.

Sein

$$\Gamma_* \coloneqq K[x, y]/(F_*, G_*), \quad \Gamma \coloneqq K[x, y, z]/(F, G), \quad R \coloneqq K[x, y, z]$$

und lass $\Gamma_d \subseteq \Gamma$ das K-Vektorraum sein, welches nur aus Formen vom Grad d besteht. Gleichwie auch R_d.

Schritt 1: Für alle $d \geq m + n$ gilt $\dim_K(\Gamma_d) = mn$.

Sei $\pi : R \to \Gamma$ die natürliche Projektion. Wir definieren Abbildungen

$$\varphi : R \times R \to R, \quad (A, B) \mapsto AF + BG$$

und

$$\psi : R \to R \times R, \quad C \mapsto (GC, -FC),$$

was uns folgendes gibt:

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \longrightarrow 0\,. \tag{25}$$

Wir behaupten, dass dies eine exakte Sequenz ist.

ψ ist injektiv: Sei $(GC, -FC) = (0, 0)$. Dann ist $GC = 0$, $CF = 0$ also ist $C = 0$ oder $F, G = 0$, da R ein Integritätsbereich ist. Bei Definition von Kurven sind $F, G \neq 0$ also ist $C = 0$, was Injektivität beweist.

π ist surjektiv: Dies ist direkt klar.

$\mathsf{Bild}(\psi) = \mathsf{Ker}(\varphi)$: [$\mathsf{Bild}(\psi) \subseteq \mathsf{Ker}(\varphi)$:] In anderen Worten, wir haben zu zeigen, dass $\varphi \circ \psi = 0$. Dies gilt da

$$C \mapsto (GC, -FC) \mapsto FGC - GFC = 0.$$

[$\mathsf{Bild}(\psi) \supseteq \mathsf{Ker}(\varphi)$:] Sei $(A,B) \in \mathsf{Ker}(\varphi)$. Also $\varphi(A,B) = AF + BG = 0$ in $R = K[x,y,z]$. Daher, $AF = -BG$. Da aber F,G keine gemeinsamen Teiler in R haben, muss $F \mid B$ und $G \mid A$ gelten. Daher, es gibt $U,V \in R$, so dass $B = UF$ und $A = VG$. Dies ergibt

$$FVG = -GB = -GUF$$

was $V = -U$ impliziert. Damit haben wir ein $C = V$ gefunden, so dass $\psi(C) = (A,B)$.

$\mathsf{Bild}(\varphi) = \mathsf{Ker}(\pi)$: [$\mathsf{Bild}(\varphi) \subseteq \mathsf{Ker}(\pi)$:] Wir haben zu zeigen, dass $\pi \circ \varphi = 0$. Es gilt

$$(A,B) \mapsto AF + BG \mapsto \overline{AF + BG} \equiv 0,$$

da $AF + BG \in (F,G) \subseteq R$.

[$\mathsf{Bild}(\varphi) \supseteq \mathsf{Ker}(\pi)$:] Sei $M \in \mathsf{Ker}(\pi)$. Daher, $M \in (F,G) \subseteq R$, was $M = AF + BG$ impliziert, für irgendwelche $A,B \in R$. Es folgt, dass es (A,B) gibt, so dass $\varphi(A,B) = M$.

Dies beweist die Exaktheit des obigen Sequenzs. Indem wir die Abbildungen auf fixierte Grade einschränken, ergibt die Exaktheit von (25), die Exaktheit der folgenden Sequenz

$$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \longrightarrow 0\,.$$

Man muss dafür nur noch überprüfen, dass die Grade, welche wir als Indexe geschrieben haben, richtig sind. Eine Form C vom Grad $d-n-m$ wird auf $(CF,-CG)$ durch ψ abgebildet. Hier hat also CF Grad $(d-n-m)+n$ und $\mathsf{grad}(CG) = (d-n-m)+m$. Wir brauchen auch, dass $d \geq m+n$ ist, damit wir in Γ_d nicht auf Null landen.

So ähnlich auch mit den anderen Abbildungen.

Nun benutzen wir Proposition 2.3.29 und die Tatsache, dass $\dim_K(S \times T) = \dim_K(S) + \dim_K(T)$ gilt und erhalten

$$\dim_K(\Gamma_d) = \dim_K(R_{d-m-n}) - [\dim_K(R_{d-m}) + \dim_K(R_{d-m})] + \dim_K(R_d).$$

Lemma 4.2.2 ergibt nun

$$\dim_K(\Gamma_d) = \frac{(d-m-n+1)(d-m-n+2)}{2} - \left[\frac{(d-m+1)(d-m+2)}{2} + \frac{(d-n+1)(d-n+2)}{2}\right] + \frac{(d+1)(d+2)}{2},$$

was mit einfacher Arithmetik mn ergibt.

Schritt 2: Es gilt $\dim_K(\Gamma_d) = \dim_K(\Gamma_*)$.

Sei $d \geq m+n$ und wähle $A_1,\ldots,A_{mn}$, so dass $\overline{A}_1,\ldots,\overline{A}_{mn}$ eine Basis von Γ_d formen. Für jeden dieser A_i, bezeichnen wir mit $A_{i*} := A_i(x,y,1) \in K[x,y]$ die Dehomogenisierung und mit $\overline{A}_{i*}$ dessen Restklasse in Γ_*. Wenn wir beweisen, dass die Menge dieser $\overline{A}_{i*}$'s, $1 \leq i \leq mn$

eine Basis von Γ_* formen, ist unser Satz bewiesen, da wir $\sum_p \mathfrak{I}(p, F \cap G) = \dim_K(\Gamma_*)$ schon argumentiert hatten.

Um dies zu zeigen, müssen vorerst folgende Behauptungen beweisen:
Behauptung 1: Für alle $r \geq 0$ ist $\overline{z^r A_1}, \ldots, \overline{z^r A_{mn}}$ eine Basis von Γ_{d+r}.

Man definiere die Abbildung

$$l_z : \Gamma \to \Gamma \quad \text{gegeben durch} \quad H \mapsto zH.$$

Für jeden $k \in \mathbb{N}$ ist $l_{zk} : \Gamma_k \to \Gamma_{k+1}$ die Beschränkung auf die Elemente vom Grad k (indem wir mit z multiplizieren wird der Grad ja natürlich um 1 erhöht). Indem wir beweisen, dass $l_z : \Gamma \to \Gamma$ injektiv ist, wird folgen, dass auch l_{zk} injektiv ist. Da laut Schritt 1 für alle $d \geq m + n$ die Dimensionen $\Gamma_d = \Gamma_{d+1} = \Gamma_{d+2} = \cdots$ stabilisieren, wird die Injektivität von $l_{zd} : \Gamma_d \to \Gamma_d$, $d \geq m + n$ die Bijektivität von l_{zd} implizieren. (Zur Erinnerung, ein Vektorraumhomomorphismus zwischen endlichdimensionalen Vektormären ist genau dann bijektiv, wenn es injektiv ist).

Als solches wird eine Basis auf eine Basis abgebildet. Da die A_i's so gewählt waren, dass die $\overline{A}_i$'s eine Basis von Γ_d bildeten, werden auch die $l_{zd}(\overline{zA}_i)$'s eine Basis von Γ_{d+1} bilden. Unter Iteration sind natürlich $\overline{z^r A}_i$'s eine Basis von Γ_{d+r}, was Behauptung 1 beweist.

Es bleibt also nur noch die Injektivität von l_z zu zeigen:
Behauptung 2: Die Abbildung $l_z : \Gamma \to \Gamma$ ist injektiv.

Sei $\hat{H} \in K[x, y, z]$ eine Hochhebung von $H \in \Gamma = K[x, y, z]/(F, G)$. Wir müssen beweisen, dass aus $z\hat{H} = AF + BG$, für irgendwelche $A, B \in K[x, y, z]$, die Existenz von $A', B' \in K[x, y, z]$ mit $\hat{H} = A'F + B'G$ folgt. Also, dass aus $\overline{z}H = 0$ in Γ, $H = 0$ folgt.

Für eine Form $J \in K[x, y, z]$, bezeichne mit $J_0 := J(x, y, 0)$. Dann folgt aus $z\hat{H} = AF+BG$, dass $(z\hat{H})_0 = (AF + BG)_0$, also $A_0F_0 = -B_0G_0$ (da $z_0 = 0$). Da bei unserer Annahme (ganz am Anfang des Beweises des Satzes) F und G mit z nicht interagieren und teilerfremd sind, sind auch F_0 und G_0 teilerfremd. Es folgt, dass es $C, D \in K[x, y, 0] \simeq K[x, y]$ gibt, so dass $A_0 = G_0C$ und $B_0 = F_0D$. Daher

$$(G_0C)F_0 = -B_0G_0 = -F_0DG_0,$$

was $C = -D$ impliziert. Setze

$$\tilde{A} := A - CG, \quad \tilde{B} := B + CF.$$

Es gilt $(\tilde{A})_0 = A_0 - CG_0 = 0 = B_0 + CF_0 = (\tilde{B})_0$, weil $C_0 = C$. Somit ist z eine Nullstelle von $\tilde{A}$ und $\tilde{B}$, also sind sie durch z teilbar. Es gibt daher A', B', so dass $\tilde{A} = zA'$ und $\tilde{B} = zB'$. Es folgt, dass

$$\tilde{A}F + \tilde{B}G = (A - CG)F + (B + CF)G = AF + BG = z\hat{H}$$

und

$$\tilde{A}F + \tilde{B}G = zA'F + zB'G = z(A'F + B'G),$$

was

$$z\hat{H} = z(A'F + B'G)$$

impliziert und damit $\hat{H} = A'F + B'G$. Dies Beweist die Behauptung.

Nun können wir Schritt 2 beweisen: dass die $\{\overline{A}_{i*}\}_{1\le i\le mn}$ eine Basis von Γ_* bilden.
Die $\overline{A}_{i*}$ erzeugen Γ_*: Sei $h \in \Gamma_*$ ein Element und $\hat{h} \in K[x,y]$ dessen Hochhebung. Wir homogenisieren es zu $\hat{h} \in K[x,y,z]$. Wir brauchen jedoch, dass es vom Grad $d+r$ ist. Um dies sicherzustellen, multiplizieren wir das ganze mit z^N, für genügend großen $N \in \mathbb{N}$, so dass $z^N\hat{h}^* \in K[x,y,z]$ eine Form vom Grad $d+r$ ist. Behauptung 1 besagt, dass die Restklasse von $z^N\hat{h}^*$ unter dem Ideal (F,G) von den $z^r\tilde{A}, \ldots, z^r A_{mn}$ erzeugt wird. Daher, es gibt $\lambda_i \in K$ und $B, C \in K[x,y,z]$, so dass

$$z^N\hat{h}^* = \sum_{i=1}^{mn} \lambda_i z^r A_i + BF + CG.$$

Da $z_* = 1$, besagen Teil (i) und (iii) von Lemma 3.2.1, dass

$$\hat{h} = (z^N\hat{h}^*)_* = \sum_{i=1}^{mn} \lambda_i A_{i*} + B_*F_* + C_*G_*.$$

Damit ist

$$h = \sum_{i=1}^{mn} \lambda_i \overline{A}_{i*},$$

wie gewünscht.
Die $\overline{A}_{i*}$ sind linear Unabhängig: Sei $\sum_{i=1}^{mn} \lambda_i \overline{A}_{i*} = 0$. Daher, $\sum_{i=1}^{mn} \lambda_i A_{i*} \in (F_*, G_*)$, also $\sum_{i=1}^{mn} \lambda_i A_{i*} = bF_* + cG_*$, für irgendwelche $b, c \in K[x,y]$. Teile (ii) und (iv) von Lemma 3.2.1, zusammen mit Teil (ii) von Lemma 3.2.2, besagt nun die Existenz von $r, s, t \in \mathbb{N}$, so dass

$$\sum_{i=1}^{mn} z^r \lambda_i A_i = z^s b^* F + z^t c^* G.$$

Da die rechte Seite im Ideal $(F,G) \subseteq K[x,y,z]$ liegt, ist die Restklasse der linken Seite $\sum_{i=1}^{mn} \lambda_i \overline{z^r A_i} \equiv 0$ in Γ, spezifisch sogar in Γ_{d+r}, da die A_i's in Γ_d waren und z^r ja Grad r hat. Laut Behauptung 1 formen die $\{\overline{z^r A_i}\}_{1\le i\le mn}$ ein Basis von Γ_{d+r}, was $\lambda_i = 0$ für alle $1 \le i \le mn$ impliziert. Dies beweist nun die lineare Unabhängigkeit und damit den Satz von Bézout. □

Im Zusammenhand mit Eigenschaft (5) der Schnittzahl in 2.4.2, haben wir folgende Korollare:

Korollar 4.2.4. *Für Teilerfremde F, G gilt*

$$\sum_p \mu_p(F)\mu_p(G) \le \mathsf{grad}(F)\mathsf{grad}(G).$$

Korollar 4.2.5. *Sein F, G Kurven welche sich an genau $\mathsf{grad}(F) \cdot \mathsf{grad}(G)$ verschiedene Punkte schneiden. Dann sind all diese Punkte regulär auf F und G.*

Korollar 4.2.6. *Sein F, G Kurven welche sich an strikt mehr als $\mathsf{grad}(F) \cdot \mathsf{grad}(G)$ verschiedenen Punkten schneiden. Dann haben sie eine gemeinsame Komponente.*

4.3 Divisoren

Definition 4.3.1. *Sei F eine projektive planare Kurve. Ein* Divisor *D auf F ist definiert als eine formelle Summe*

$$D = \sum_{p \in F} n_p p,$$

mit $n_p \in \mathbb{Z}$, so dass $n_p = 0$ für fast alle *(das heißt alle außer endlich viele) p's.*

Anders gesagt, ein Element ist von der Form $n_1 p_1 + \cdots n_k p_k$, wobei $n_i \in \mathbb{Z}$ und $F(p_i) = 0$. Zwei solche Divisoren D_1 und D_2 werden addiert, indem man die zugehörigen Koeffizienten addiert. Wenn eines der Punkte, die in D_1 vorkommen nicht in D_2 vorkommen, dann setzt man einfach einen 0 als Koeffizienten. Zum Beispiel, $(2p_1 + 3p_2) + (4p_1 + 5p_3 + p_4) = 6p_1 + 3p_2 + 5p_3 + p_4$. Manchmal werden diese auch 0-Zyklen genannt.

Es ist klar, dass die Menge aller Divisoren eine abelsche Gruppe formen. Es ist die *freie abelsche Gruppe mit Basis F*. Diese Gruppe wird mit $\mathrm{Div}(F)$ bezeichnet.

Eine andere Art und Weise dies zu sagen ist, dass wir die direkte Summe (*nicht* den Produkt) (von abelschen Gruppen) von $\mathbb{Z}$ mit sich selbst nehmen, und zwar so oft, wie wir Punkte auf der Kurve haben. Dies ist normalerweise gewaltig, öfters sogar unzählbar groß.

Definition 4.3.2. *Wir definieren den* Grad *eines Divisors als*

$$\mathsf{grad}(\sum n_p p) := \sum n_p \in \mathbb{Z}.$$

Definition 4.3.3. *Wir sagen, dass ein Divisors* positiv *ist, wenn für* alle *$p \in F$, $n_p \geq 0$. Dies induziert eine Ordnung, wobei $\sum n_p p \geq \sum m_p p$, genau dann wenn $\sum n_p p - \sum m_p p$ ein positiver Divisor ist. Also, für alle $p \in F$, $n_p \geq m_p$.*

Wir haben das folgende direkt von der Definition:

Lemma 4.3.4. *Dies ist eine Ordnung und es ist mit der Gruppenstruktur verträglich: Daher, aus $D_1 \leq D_2$, $D_1' \leq D_2'$ folgt $D_1 + D_1' \leq D_2 + D_2'$.*

Lemma 4.3.5. *Die Gradabbildung*

$$\mathsf{grad} : \mathrm{Div}(F) \to \mathbb{Z}$$

ist ein surjektiver Gruppenhomomorphismus.

Beweis. Das dies die Gruppenstruktur erhält, ist völlig klar, da $\mathsf{grad}(\sum n_p p + \sum m_p p) = \mathsf{grad}(\sum (n_p + m_p) p) = \sum (n_p + m_p) = \sum n_p + \sum m_p = \mathsf{grad}(\sum n_p p) + \mathsf{grad}(\sum m_p p)$. Es ist natürlich auch surjektiv, da man für jeden $N \in \mathbb{N}$, einfach einen Punkt p nehmen kann und $n_p = N$ setzen und $n_q = 0$ für alle $q \neq p$. □

Definition 4.3.6. *Wir bezeichnen den Kern der Gradabbildung mit*

$$\mathrm{Div}^0(F) = \{D \in \mathrm{Div}(F) \mid \mathsf{grad}(D) = 0\}.$$

Da es der Kern eines Gruppenhomomorphismus ist, ist es eine Untergruppe. Wir können uns daher den Quotienten

$$\mathrm{Div}(F)/\mathrm{Div}^0(F)$$

ansehen. Der Hauptisomorphiesatz für Gruppen besagt, dass eine surjektive Abbildung zu einer Isomorphie wird, wenn man die Ausgangsgruppe mit dem Kern der Abbildung teilt. Daher:

Lemma 4.3.7. *Die Induzierte Abbildung*

$$\overline{\mathsf{grad}} : \mathrm{Div}(F)/\mathrm{Div}^0(F) \xrightarrow{\sim} \mathbb{Z}$$

ist ein Isomorphismus.

Man kann sich also $\mathrm{Div}(F)$ als eine "quasi $\mathbb{Z}$-fache Kopie von $\mathrm{Div}^0(F)$" vorstellen, wo für jede ganze Zahl (also Grad) wir die Divisoren vom Grad 0 schreiben.

Divisoren sind dazu da, damit wir uns lokale Informationen auf einmal anzusehen können. Dies ist öfters sehr hilfreich in Algebra. Zum Beispiel können wir nun eine einfache, aber wichtige, Verallgemeinerung der Schnittzahl 2.4.9 einführen:

Definition 4.3.8. *Sein F, G teilerfremde planare projektive Kurven mit $\mathsf{grad}(F) = m$, $\mathsf{grad}(G) = n$. Dann definieren wir*

$$F \bullet G := \sum_{p \in F} \mathfrak{I}(p, F \cap G)p$$

und nennen es den Schnittdivisor.

Obwohl wir in diesem Fall nicht die Notation div zuvor schreiben, ist $F \bullet G$ ein Divisor, kein Polynom/Abbildung. Man bemerke, dass wir hier über ganz $p \in F$ aufaddieren. Teilerfremd brauchen wir, damit wir nicht unendlich viele der Koeffizienten $\mathfrak{I}(p, F \cap G)$ ungleich Null haben. Laut Proposition 4.2.1 und Eigenschaft (2) der Schnittzahl 2.4.2 sind in diesem Fall nur endlich viele der $\mathfrak{I}(p, F \cap G)$ ungleich Null. Als solches ist es tatsächlich ein Divisor.

Es ist klar, dass wir die Summe auch über die Punkte von G nehmen können, ohne, dass sich etwas ändert, da die einzigen Punkte mit Koeffizienten ungleich Null im Schnitt von F und G liegen. Wenn man präzise sein will (da $\sum_{p \in F} \mathfrak{I}(p, F \cap G)p$ und $\sum_{p \in G} \mathfrak{I}(p, F \cap G)p$ in zwei verschiedenen Gruppen liegen!), kann man hier auch die Vereinigung der Nullstellen der Kurven nehmen, was wieder eine Kurve ist (es gilt ja, $\mathrm{V}(F) \cup \mathrm{V}(G) = \mathrm{V}(FG)$).

Der Schnittdivisor $F \bullet G$ ist ein positiver Divisor und laut Bézout 4.2.3 gilt $\mathsf{grad}(F \bullet G) = \mathsf{grad}(F)\mathsf{grad}(G)$. Es ist vielleicht nicht direkt klar, warum dies eine Verbesserung der Schnittzahl darstellt. Wir werden dies in den nächsten Seiten besser verstehen. Lass uns als Hauptgrund schon dies sagen, dass wir nicht mehr an einem Punkt festgebunden sind, sonder zwei Kurven im Ganzen dadurch studieren können. Solche Sachen sind in der Algebra öfters von großer Bedeutung, auch wenn man es nicht immer direkt sieht.

Aufgrund der sehr engen Beziehung zwischen dem Schnittzahl und des Schnittdivisor, lassen sich viele der Eigenschaften hier übersetzen. Wir werden hier nur einige Auflisten, die wir brauchen werden.

Proposition 4.3.9. *Sein F, G teilerfremde Kurven. Es gilt*

(i) $F \bullet G = G \bullet F$,

(ii) $F \bullet GH = F \bullet G + F \bullet H$,

(iii) $F \bullet (G + AF) = F \bullet G$, *wenn* $\mathsf{grad}(A) = \mathsf{grad}(G) - \mathsf{grad}(F)$.

Hier ist mit GH und AF das (normale) Produkt der (homogenen) Polynome gemeint.

Beweis. Da das Schnittdivisor rein mit dem Schnittzahl definiert wird, ist dies einfach nur (4), (6) und (7) von den Eigenschaften der Schnittzahl 2.4.2, unter Anwendung des Satzes 4.1.11. □

Ein spezieller Fall des Schnittdivisors ist das folgende:

Definition 4.3.10. *Sei $\overline{G} \in K_h[\mathrm{V}(F)] \setminus \{0\}$ homogen und $G \in K[x,y,z]$ eine der Hochhebungen. Wir definieren den Divisor*

$$\mathrm{div}(\overline{G}) := \sum_{p \in F} \mathfrak{I}(p, F \cap G) p = F \bullet G \ \in \mathrm{Div}(F).$$

Lemma 4.3.11. *Dies hängt nicht vom Wahl der Hochhebung ab.*

Beweis. Sein $G, G' \in K[x,y,z]$ zwei Hochhebungen von $\overline{G}$. Wir brauchen nur zu beweisen, dass die Schnittzahlen $\mathfrak{I}(p, F \cap G), \mathfrak{I}(p, F \cap G')$ miteinander übereinstimmen. Da F irreduzibel ist, ist $\mathrm{I}(F)$ prim (Proposition 3.1.21) und daher radikal (Lemma 1.2.48). Von Hilberts Nullstellensatz 1.2.43 (iii) haben wir daher $\mathrm{I}(\mathrm{V}(F)) = (F)$. Wir haben also $G - G' \in (F)$, in anderen Worten $\overline{G} = \overline{G}' \in K_h[\mathrm{V}(F)]$, daher sind also $\mathcal{O}_p/(F,G) \simeq (K[x,y,z]/(F))_{\mathfrak{m}_p}/\overline{G} \simeq (K[x,y,z]/(F))_{\mathfrak{m}_p}/\overline{G'} \simeq \mathcal{O}_p/(F,G')$. □

Es ist direkt klar, dass dieser Divisor positiv ist. Es enthält die gesamte Information von den Nullstellen von $\overline{G}$ (gemeinsamen Nullstellen von F und G) und der Vielfachheit dieser Nullstellen. Dies kann man auch für Rationale Funktionen fortsetzen.

Definition 4.3.12. *Sei $\varphi \in K(\mathrm{V}(F))^*$. Daher, $\varphi \neq 0$ und $\varphi = \frac{\overline{F}}{\overline{H}}$ wobei $\overline{F}, \overline{H} \in K[\mathrm{V}(F)]$. Sein $F, G \in K[x,y,z]$ Hochhebungen. Wir definieren*

$$\mathrm{div}(\varphi) := \sum_{p \in F} [\mathfrak{I}(p, F \cap G) - \mathfrak{I}(p, F \cap H)]\, p = \mathrm{div}(\overline{G}) - \mathrm{div}(\overline{H}) \in \mathrm{Div}(F).$$

Wohldefiniertheit haben wir schon im obigen Lemma 4.3.11 gezeigt.

Proposition 4.3.13 (Satz von Bézout für Divisore)**.** *Sei $\overline{G} \in K[\mathrm{V}(F)] \setminus \{0\}$ und $\varphi \in K(\mathrm{V}(F))^*$. Es gilt*

$$\mathsf{grad}(\mathrm{div}(\overline{G})) = \mathsf{grad}(F)\mathsf{grad}(G)$$

und

$$\mathsf{grad}(\mathrm{div}(\varphi)) = 0.$$

Beweis. Bei Definition gilt $\mathsf{grad}(\mathrm{div}(\overline{G})) = \sum_p \mathfrak{I}(p, F \cap G)$, was Laut Bézout 4.2.3 wiederum Gleich $\mathsf{grad}(F)\mathsf{grad}(G)$ ist.

Bei der Zweiten Gleichung haben wir

$$\mathsf{grad}(\mathrm{div}(\varphi)) = \mathsf{grad}\left(\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right)\right) = \mathsf{grad}(\mathrm{div}(\overline{G})) - \mathsf{grad}(\mathrm{div}(\overline{H})) = \mathsf{grad}(F)\mathsf{grad}(G) - \mathsf{grad}(F)\mathsf{grad}(H).$$

Bei Definition von $K(\mathrm{V}(F))$ gilt $\mathsf{grad}(G) = \mathsf{grad}(H)$, was die Aussage impliziert. □

Korollar 4.3.14. *Das Bild des Gruppenhomomorphismus*

$$\mathrm{div} : K(\mathrm{V}(F))^* \to \mathrm{Div}(F)$$

liegt in $\mathrm{Div}^0(F)$.

Definition 4.3.15. *Divisore, die im Bild von* $\mathrm{div} : K(\mathrm{V}(F))^* \to \mathrm{Div}^0(F)$ *liegen werden* Hauptdivisore *oder* Prinzipaldivisore *genannt und mit* $\mathsf{HDiv}(F)$ *bezeichnet.*

Da sie das Bild von einem Gruppenhomomorphismus sind, stellen sie selber eine Gruppe da. Diese Divisore werden eine wichtige Rolle bei der Konstruktion der Picardgruppe 4.6.1 spielen.

Lemma 4.3.16. *Sei eine rationale Abbildung* $\varphi \in K(\mathrm{V}(F))^*$ *definiert auf allen Punkten* $p \in F$. *Dann ist* $\mathrm{div}(\varphi)$ *ein positiver Divisor.*

Beweis. Dies folgt direkt von Lemma 2.4.16. □

Beispiel 4.3.17 (Zu Lemma 2.4.16). Sei $F = y$, $G = x(y - x^2)$, $H = y^3 + x^2$ und $p = (0, 0)$. Der einzige Punkt im Schnitt von F und G ist $p = (0, 0)$, gleichwie auch von F und H. Die Schnittzahlen sind $\mathfrak{I}(p, F \cap G) = 3$ und $\mathfrak{I}(p, F \cap H) = 2$. Als solches ist $\mathrm{div}(G) = 3p$ und $\mathrm{div}(H) = 2p$, was $\mathrm{div}(\varphi) = p$ und $\mathsf{grad}(\varphi) = 1 \geq 0$ ergibt. Es muss $\varphi = \frac{\overline{G}}{\overline{H}}$ ein positiver Divisor sein.

Man könnte denken, dass dies nicht der Fall sein kann, da $H \nmid G$. Jedoch ist $\varphi \in K(\mathrm{V}(F))$ und da muss es definiert sein. Es gilt $\varphi \equiv \frac{x^3}{x^2} \sim \frac{x}{1}$, da $y \equiv 0$ in $K[x, y]/\mathrm{V}(F)$ und daher auch in $K(\mathrm{V}(F))$. Als solches ist φ regulär.

4.4 (Max) Noetherscher Fundamentalsatz

Wir stellen uns nun folgende Frage: Sein F, G, H planare projektive Kurven, so dass $H \bullet F \geq G \bullet F$. Gibt es eine Kurve B, so dass $B \bullet F = H \bullet F - G \bullet F$?

Last uns darüber nachdenken, was dies bedeutet. Um zu sehen, warum dies wichtig ist, vereinfachen wir die Lage und nehmen zusätzlich an, dass sich F, G und H überall mit Schnittzahl 1 schneiden. Also, die Kurven auf allen Schnittpunkten transversal sind. Dann ist die Lage wie folgt: überall wo sich F und G schneiden, schneiden sich auch F und H. Sein $p_1, \ldots, p_n$ die Punkte wo sich F und H schneiden, aber nicht auf G liegen. Eine Kurve B wie oben ist nun eine Kurve, die sich mit F *genau* an den Punkten $p_1, \ldots, p_n$ schneidet und sonst nirgends.

Dies ist geometrisch eine sehr interessante Frage und die Wichtigkeit davon werden wir im Abschnitt 4.5 genauer sehen. Die Frage ist etwas allgemeiner gestellt, da die Schnittzahl ja größer als 1 sein kann. Dann zieht die Frage nach B auch folgendes in Betracht: angenommen F und H "schneiden sich am Punkt p 17 mal" (Schnittzahl ist 17) und am Punkt q "12 mal" (Schnittzahl ist 12) und F und G 14 und 10 mal an den Punkten p und q. Gibt es eine Kurve B, welches ich mit F am Punkt p genau 3 mal und am Punkt q genau 2 mal schneidet?

Diese geometrische Frage kann man durch eine algebraisch Aussage sehr oft beantworten. Da ist es ebenso sehr klar (vielleicht sogar mehr noch), warum dies wichtig ist. Der Satz von Max Noether 4.4.4 unten beschäftigt sich genau mit dieser Aussage und wird uns ermöglichen, diese Frage zu beantworten.

Lasst uns aber kurz überlegen, wann es eine solche Kurve B gibt. Als erstes merken wir, dass $\mathsf{grad}(B) = \mathsf{grad}(H) - \mathsf{grad}(F)$ gelten muss. Zudem haben wir folgendes:

Proposition 4.4.1. *Sein F, G, H Kurven mit $H \bullet F \geq G \bullet F$. Wenn $H \in (F, G)$, gibt es eine Kurve B, mit $B \bullet F = H \bullet F - G \bullet F$.*

Beweis. Sei $H \in (F, G)$. Daher, es gibt Formen $A, B \in K[x, y, z]$, so dass $H = AF + BG$, sieh Lemma 3.1.17. Dann gilt laut Proposition 4.3.9, Teil (iii) und dann Teil (ii), dass

$$F \bullet H = F \bullet (AF + BG) = F \bullet BG = F \bullet B + F \bullet G.$$

Da Divisoren ja eine abelsche Gruppe formen können wir natürlich subtrahieren und wir erhalten

$$B \bullet F = H \bullet F - G \bullet F.$$

□

Bemerkung 4.4.2. Der Grund, warum wir im Bewies von Proposition 4.4.1 spezifisch nach Formen suchen ist, weil wir wollen dass B eine projektive Kurve ist, nicht Schnitt von projektiven Varietäten. Zur Erinnerung, eine Summe von Formen $A + B$ korrespondiert zum Schnitt der projektiven Varietäten von A und B.

Definition 4.4.3. *Sei $p \in \mathbb{P}^2$ und $F, G, H \in K[x,y,z]$ kurven, so dass F und G teilerfremd sind. Wir sagen, dass die Kurven F, G, H die* Noethersche Eigenschaft *am Punkt p erfüllen, wenn die Dehomogenisierung $H_* \in (F_*, G_*) \subseteq \mathcal{O}_p$ im Ideal liegt.*

Nun können wir den Hauptsatz des Abschnitts formulieren.

Satz 4.4.4 (Max Noethers Fundamentalsatz)**.** *Sein F, G, H projektive planare Kurven, so dass F, G teilerfremd sind. Dann gibt es Formen $A, B \in K[x,y,z]$, so dass $H = AF + BG$, genau dann, wenn für jeden Punkt $p \in F \cap G$, die Noethersche Eigenschaft erfüllt ist.*

In anderen Worten, die Kurve H ist *global* im Ideal (F, G), wenn es an jedem Punkt lokal in das Ideal (F_*, G_*) liegt. So etwas wird *Lokal-Global-Prinzip* (oder Hasse-Prinzip) in Algebra/Zahlentheorie genant und ist extrem wichtig. Ein weiterer Beispiel davon ist der Satz von Hasse–Minkowski aus der algebraischen Zahlentheorie, welches besagt, dass quadratische Formen genau dann Äquivalent sind, wenn diese lokal Äquivalent sind. Zum Beispiel haben Polynome vom bestimmten Typ genau dann eine Lösung über $\mathbb{Q}$, wenn sie eine Lösung über $\mathbb{R}$ und über den p-adischen Zahlen haben.

Beweis. Wie immer beim Hasse-Prinzip ist eine Seite auch hier klar: aus Global folgt lokal. Daher wenn $H \in (F, G)$, dann ist $H_* \in (F_*, G_*) \in \mathcal{O}_p$. Für die andere Seite, nehmen wir an (wie auch im Beweis von Bézouts Satz 4.2.3), dass all die Punkte wo sich F und G schneiden nicht auf der Gerade $L_z = z$ liegen. (Das können wir, wie gewöhnt, durch einen projektiven Variablenwechsel machen). Wir formulieren dies als $\mathrm{V}((F, G, z)) = \varnothing$.

Betrachte $F_* = F(x, y, 1)$, $G_* = G(x, y, 1)$ und $H_* = (x, y, 1)$. Von der Annahme, dass die Noethersche Eigenschaft für alle $p \in F \cap G$ hält, folgt, dass $H_* \equiv 0$ in $\mathcal{O}_p/(F_*, G_*)$. Satz 2.3.12 gibt uns die Isomorphie $K[x,y]/(F_*, G_*) \simeq \prod_{p \in F_* \cap G_*} \mathcal{O}_p/(F_*, G_*) = \prod_{p \in F \cap G} \mathcal{O}_p/(F_*, G_*)$, wobei die letzte Gleichung von der Tatsache kommt, dass keines der Schnittpunkte von F und G auf der Linie $L_z = z$ liegen. Da aber $(0, \cdots, 0)$ natürlich das Null des Produkts ist, folgt, dass $H_* \equiv 0$ in $K[x,y]/(F_*, G_*)$, in anderen Worten $H_* \in (F_*, G_*) \subseteq K[x,y]$.

Als solches folgt, dass es $a, b, \in K[x,y]$ gibt, mit $H_* = aF_* + bG_*$. Durch die Anwendung von Teil (ii), (iv) Lemma 3.2.1 und Teil (ii) von Proposition 3.2.2 wissen wir, dass es $A, B \in K[x,y,z]$ und $r \in \mathbb{N}$ gibt, so dass $z^r H = AF + BG$. Man erinnere sich nun an Behauptung 2 im Beweis vom Satz vom Bézout 4.2.3 Dort haben wir gezeigt, dass die Abbildung $\alpha \mapsto z\alpha$ von $K[x,y,z]/(F, G) \to K[x,y,z]/(F, G)$ für teilerfremde F, G injektiv war. Wir haben

$$\begin{aligned} z^r H = AF + BG &\Leftrightarrow z^r H \in (F, G) \subseteq K[x,y,z] \\ &\Leftrightarrow \overline{z^r H} = 0 \in K[x,y,z]/(F, G) \\ &\Leftrightarrow \overline{H} = 0 \in K[x,y,z]/(F, G) \\ &\Leftrightarrow H \in (F, G), \end{aligned}$$

wie gewünscht. □

Wir haben nun eine starke algebraische Methode gefunden, um unsere Frage zu beantworten. Da dies jedoch eher eine geometrische Frage war, wollen wir nun auch ein geometrische Charakterisierung dafür finden. Anderes gesagt, um eine geometrische Frage zu beantworten gehen wir erst Richtung Algebra und dann zurück zur Geometrie. Dies wird in Proposition 4.4.6 gleich gemacht. Zuerst aber das folgende Lemma:

Lemma 4.4.5. *Sein $F, G, H \in K[x, y, z]$ projektive planare Kurven, mit $F = F_1F_2$, F_1 irreduzibel, so dass $p \in F_1 \cap G$ aber $p \notin F_2 \cap G$. Die Noethersche Eigenschaft am Punkt p ist für F_1, G, H genau dann erfüllt, wenn es für F, G, H erfüllt ist.*

Beweis. Dies folgt direkt von der Tatsache, dass aus $p \notin F_2$, $p \notin (F_2)_*$ und daher $(F_2($_$* \in \mathcal{O}_p^*$ eine Einheit ist. Also gilt $((F_1)_*, G_*) = (F_*, G_*)$ als Ideale von $\mathcal{O}_p$. Daher ist H_* genau dann in einem, wenn es im anderen ist. □

Proposition 4.4.6. *Sein F, G, H planare projektive Kurven mit $F = F_1F_2$, F_1 irreduzibel und $p \in F_1 \cap G$, $p \notin F_2 \cap G$. Die Noethersche Eigenschaft ist am Punkt p erfüllt wenn* eines *der folgenden Aussagen hält:*

(i) F und G schneiden sich transversal am Punkt p und $p \in H$;

(ii) F ist regulär auf p und $\mathfrak{I}(p, F \cap H) \geq \mathfrak{I}(p, F \cap G)$.

(iii) F und G haben keine gemeinsame Tangente an p und $\mu_p(H) \geq \mu_p(F) + \mu_p(G) - 1$.

Beweis. Als erstes bemerken wir, dass die drei Eigenschaften auch für F_1 gelten. Regularität wird erhalten, da $1 = \mu_p(F) = \mu_p(F_1F_2) = \mu_p(F_1) + \mu_p(F_2) = \mu_p(F_1) + 0 = \mu_p(F_1)$. Wenn nun F und G keine gemeinsame Tangente haben, können natürlich auch F_1 und G keine gemeinsame Tangente haben. Damit wird Transversalheit erhalten. Da $\mathfrak{I}(a, F_2 \cap G) = 0$ muss also auch $\mathfrak{I}(p, F_1 \cap H) \geq \mathfrak{I}(p, F_1 \cap G)$ gelten. Auch muss $\mu_p(H) \geq \mu_p(F_1) + \mu_p(G) - 1$ sein, da $\mu_p(F_2) = 0$. Es folgt nun von Lemma 4.4.5, dass wir direkt $F = F_1$ irreduzibel annehmen können, was wir nun machen.

(ii) Sei $p \in U_{n+1}$. Korollar 3.2.3 besagt, dass F_* irreduzibel ist. Laut Lemma 1.5.21 gilt also $\mathcal{O}_p/F_* \simeq \mathcal{O}_p(F_*)$. Betrachte $\overline{G}_*, \overline{H}_* \in \mathcal{O}_p(F_*)$. Da F regulär ist am Punkt p (dies wird bei der Dehomogenisation erhalten), können wir Lemma 2.4.15 anwenden und schreiben $\overline{G}_* = ct^n$, $\overline{H}_* = c't^m$, wobei $n = \mathfrak{I}(p, F \cap G)$ und $m = \mathfrak{I}(p, F \cap H)$. Hier haben wir Proposition 3.2.19 benutzt. Wir haben auch Proposition 2.3.40 benutzt, damit wir bei $\overline{G}_*$ und $\overline{H}_*$ das selbe irreduzible t nehmen könnten. Da nun aber $m \geq n$, folgt, dass $\overline{G}_* \mid \overline{H}_*$ in $\mathcal{O}_p(F_*)$, also $\overline{H}_* \subseteq (\overline{G_*}) \subseteq \mathcal{O}_p(F_*)$. Es folgt, dass $H_* \subseteq (G_*, F_*) \subseteq \mathcal{O}_p$ und somit ist die Noethersche Eigenschaft erfüllt.

(iii) Da wir eine lokale Eigenschaft erforschen und diese unter einer projektiven Transformation invariant bleibt, können wir annehmen, dass $p = [0 : 0 : 1]$, also das Nullpunkt von $\mathbb{A}^n$. Laut Proposition 3.2.21 haben wir auch $\mu_p(H_*) \geq \mu_p(F_*) + \mu_p(G_*) - 1$.

Man erinnere sich an die Definition der Multiplizität am Punkt $0 \in \mathbb{A}^2$. Es ist dann direkt ersichtlich, dass aus $\mu_0(f) \geq t$, $f \in (x, y)^t$ folgt. Daher impliziert die Aussage $\mu_p(H) \geq$

$\mu_p(F) + \mu_p(G) - 1$, dass $H_* \in (x,y)^t$, mit $t = \mu_p(F) + \mu_p(G) - 1$. Laut Lemma 2.4.6 ist $(x,y)^t \subseteq (F_*, G_*) \subseteq \mathcal{O}_p$, was dann mit Proposition 3.2.19 $H \in (F_*, G_*) \subseteq \mathcal{O}_p$ und dadurch unsere Aussage ergibt.

(i) Dies ist ein direkter Konsequenz von sowohl Teil (i) wie auch Teil (iii). □

Korollar 4.4.7. *Sein F, G, H planare projektive Kurven (wo alle reduzibel sein dürfen). Es gibt eine Kurve B mit $B \bullet F = H \bullet F - G \bullet F$ wenn eines der folgen Eigenschaften erfüllt wird:*

(i) F und G treffen sich in $\mathsf{grad}(F)\mathsf{grad}(G)$ verschiedenen Punkten und H geht durch all diese Punkte;

(ii) F ist regulär auf jedem der Punkte $p \in F \cap G$ und $H \bullet F \geq G \bullet F$.

Spezifisch gilt auch $\overline{H} = \overline{BG}$ und $\operatorname{div}(\overline{B}) = \operatorname{div}(\overline{H}) - \operatorname{div}(\overline{G})$, wobei $\overline{B}, \overline{G}, \overline{H} \in K[\mathrm{V}(F)] \setminus 0$.

Beweis. Dies folgt von Teil (ii) der obigen Proposition 4.4.6. Bei Teil (i) besagt der Satz von Bézout 4.2.3, dass für jeden $p \in F \cap G$, die Schnittzahl $\mathfrak{I}(p, F \cap G) = 1$ ist. Daher folgt von Korollar 4.2.5, dass jeder Punkt regulär ist. Weil H auf jedem dieser Punkte liegt, ist auch $\mathfrak{I}(p, F \cap H) \geq 1 = \mathfrak{I}(p, F \cap G)$. Damit sind die erforderlichen Eigenschaften erfüllt. Teil (ii) ist direkt das zweite Teil der obigen Proposition.

Die Gleichheit $\operatorname{div}(\overline{B}) = \operatorname{div}(\overline{H}) - \operatorname{div}(\overline{G})$ gilt, da bei Definition

$$\operatorname{div}(\overline{X}) = \sum_{p \in F} \mathfrak{I}(p, F \cap X) = X \bullet F$$

gelten. Wir haben $\overline{H} = \overline{BG}$, da wir, laut dem Satz von Noether 4.4.4, $H \in (F, G)$ haben. Also, $H = AF + BG$ in $K[x,y,z]$. Da wir aber nun Modulo F sind, wird dies zum gewünschten $\overline{H} = \overline{BG} \in K[\mathrm{V}(F)]$. □

4.5 Der Satz von Pappos

Wir wollen nun einige kleine Anwendungen von dem Satz von Bezout und dem Noetherschem Fundamentalsatz demonstrieren.

Definition 4.5.1. *Wir nennen einen Divisor $D \in \mathrm{Div}(F)$ einen* Punktdivisor*, wenn $D = 1 \cdot p_j$, für irgendeinen $p_j \in F$. Daher, aus $D = \sum_{i=1}^{r} k_i p_i$, $k_i \in \mathbb{N}$, $p_i \in F$ folgt, dass $k_i = 0$ für alle $1 \leq i \leq r$, außer genau einem j. Für diesen j muss zudem $k_j = 1$ sein. Dies wird auch das Punktdivisor assoziiert zum Punkt p_j genannt und wir schrieben dies öfters einfach als P_j.*

Proposition 4.5.2. *Sein F, G, H Kurven mit $\mathsf{grad}(F) = \mathsf{grad}(H) = n$, $\mathsf{grad}(G) = n - 1$,*

$$F \bullet H = \sum_{i=1}^{n^2} P_i, \quad F \bullet G = \sum_{i=1}^{n(n-1)} P_i,$$

wobei die P_i's Punktdivisoren sind und man nehme an, dass F regulär auf $p_1, \ldots, p_{n(n-1)}$ ist. Dann liegen $p_{n(n-1)+1}, \ldots, p_{n^2}$ auf einer Gerade.

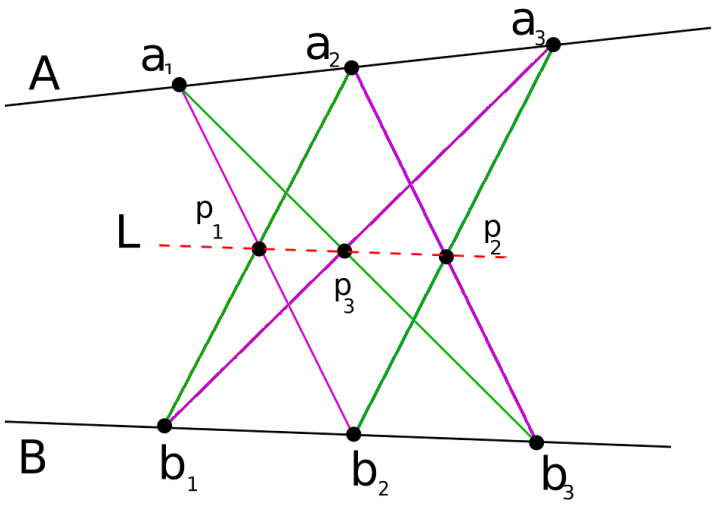
Beweis. Wir wissen direkt von Teil (ii) von Korollar 4.4.7, dass es also eine Kurve B gibt, mit $F \bullet B = F \bullet H - F \bullet G$. Daher,

$$F \bullet B = \sum_{i=1}^{n^2} P_i - \sum_{i=1}^{n(n-1)} P_i = \sum_{i=n(n-1)+1}^{n^2} P_i.$$

Dies impliziert $\mathsf{grad}(F \bullet G) = \underbrace{1 + \cdots + 1}_{n \text{ Mal}} = n$. Auf der anderen Seite sagt der Satz von Bézout für Divisore 4.3.13, dass $\mathsf{grad}(F \bullet G) = \mathsf{grad}(F) \cdot \mathsf{grad}(B)$ was zusammen $\mathsf{grad}(F) \cdot \mathsf{grad}(B) = n$ ergibt. Da $\mathsf{grad}(F) = n$ muss $\mathsf{grad}(B) = 1$ sein. Also muss B eine Gerade sein und da $p_{n(n-1)+1}, \ldots, p_{n^2}$ auf B liegen, ist unsere Proposition fertig. □

Satz 4.5.3 (Der Satz von Pappos)**.** *Sein A, B Geraden und man nehme je drei Punkte auf A und drei auf B. Nummeriere sie a_1, a_2, a_3 und b_1, b_2, b_3. Betrachte die Geraden L_1, L_2 und L_3, definiert durch a_1, b_2, a_2, b_3 und a_3, b_1. Gleichwie die Geraden M_1, M_2 und M_3 definiert durch b_1, a_2, b_2, a_3 und b_3, a_1. Betrachte die Schnittpunkte $p_1 = L_1 \cap M_1$, $p_2 = L_2 \cap M_2$ und $p_3 = L_3 \cap M_3$.*

Diese Punkte liegen auf einer Gerade.



Beweis. Dies folgt natürlich von Proposition 4.5.2, für $n = 3$. Sei $G = AB$, $F = L_1L_2L_3$ und $H = M_1M_2M_3$. Es ist klar, dass F auf den Punkten $a_1, a_2, a_3, b_1, b_2, b_3$ regulär ist. Des weiten gilt

$$F \bullet G = A_1 + A_2 + A_3 + B_1 + B_2 + B_3$$

und

$$F \bullet H = A_1 + A_2 + A_3 + B_1 + B_2 + B_3 + P_1 + P_2 + P_3.$$

Hier sind die A_i' etc. die zu den Punkten a_i zugehörigen Punktdivisoren. (Um sich von den letzten Gleichungen zu überzeugen, bemerke, dass all diese Punkte in den Schnitten von F und G, bzw. von F und H liegen. Des weiteren sind diese schon 6 bzw 9, was impliziert, dass es keine weiteren Punkte/Punktdivisoren mehr geben kann.)

Damit sind die Bedingungen der obigen Proposition erfüllt und als solches müssen die Punkte p_1, p_2 und p_3 auf einer Gerade. □

4.6 Die Picardgruppe

Sei F eine projektive planare Kurve. Die Gruppe $\mathrm{Div}(F)$ ist normalerweise, wie schon erwähnt, riesig. Wir können aber daraus eine andere Gruppe machen, welches deutlich kleiner ist, aber trotzdem sehr viel Information enthält: Die Picardgruppe. Dies kann man deutlich allgemeiner definieren als wir es machen werden, es ist aber trotzdem meistens endlich erzeugt.

Definition 4.6.1. *Sei F eine projektive planare Kurve. Dann wird die Quotientengruppe*

$$\mathsf{Pic}(F) := \mathrm{Div}(F)/\mathsf{HDiv}(F)$$

die Picardgruppe *von F genannt.*

In anderen Worten, zwei Divisore $D_1, D_2 \in \mathrm{Div}(F)$ definieren eine Klasse in der Picardgruppe, wenn es eine rationale Funktion $\varphi \in K(\mathrm{V}(F))^*$ gibt, mit $D_1 - D_2 = \mathrm{div}(\varphi)$. In diesem Fall sagen wir auch, dass D_1 und D_2 *linear äquivalent* sind.

Man erinnere sich an Korollar 4.3.14. Wir haben gesagt, dass $\mathsf{HDiv}(F) \subseteq \mathrm{Div}^0(F) \subseteq \mathrm{Div}(F)$ gilt. Daher können wir auch $\mathrm{Div}^0(F)$ durch $\mathsf{HDiv}(F)$ teilen. Wir bezeichnen

$$\mathsf{Pic}^0(F) := \mathrm{Div}^0(F)/\mathsf{HDiv}(F).$$

Da die Äquivalenzrelation die selbe ist, ist es klar, dass $\mathsf{Pic}^0(F) \subseteq \mathsf{Pic}(F)$ eine Untergruppe ist. Unsere Diskussion von Lemma 4.3.7 gibt uns auch

$$\mathsf{Pic}(F)/\mathsf{Pic}^0(F) \simeq \mathbb{Z}. \tag{26}$$

Also, $\mathsf{Pic}^0(F)$ trägt quasi die selbe Information wie $\mathsf{Pic}(F)$. Wir werden aber ab und zu immer noch die größere Gruppe $\mathsf{Pic}(F)$ betrachten, je nachdem, was gelegener ist.

Der Grad eines Divisors ist auch für die Picardgruppe wohldefiniert. Es gilt nämlich folgendes:

Lemma 4.6.2. *Sein $D \sim D'$ linear äquivalent. Dann gilt* $\mathsf{grad}(D) = \mathsf{grad}(D')$.

Beweis. Bei Definition von lineare Äquivalenz gibt es ein $\varphi \in K[\mathrm{V}(F)]^*$, mit $D_1 - D_2 = \mathrm{div}(\varphi)$. Da der Grad ein Gruppenhomomorphismus ist (Lemma 4.3.5), gilt $\mathsf{grad}(D_1) - \mathsf{grad}(D_2) = \mathsf{grad}(\varphi)$, was nach Teil (ii) von Proposition 4.3.13 $\mathsf{grad}(D_1) = \mathsf{grad}(D_2)$ ergibt. □

4.6.1 Die Picardgruppe von Kurven mit Grad ≤ 2

Kurven mit Grad 1. Sei $\mathsf{grad}(F) = 1$ eine projektive planare Kurve. Man wähle sich ein Punkt $p \in F$ auf F und ziehe dann eine Gerade L_p, verschieden von F, welches durch p geht. Da $\mathsf{grad}(F) = 1$, schneiden sich F und L_p kein weiteres mal und es ist klar, dass $\mathrm{div}(L_p) = F \bullet L_p = P$. Wie gewohnt ist hier P das Divisor assoziiert zu $p \in F$, mit $n_p = 1$ und $n_q = 0$ für jeden anderen Punkt $q \in F$.

Sei $q \in F$ ein weiterer Punkt, Q dessen Punktdivisor und L_q eine Gerade durch q, ungleich F. Dann ist $\operatorname{div}(L_q) = Q$ und $\varphi = \frac{L_p}{L_q}$ eine rationale Funktion mit $\operatorname{div}(\varphi) = P - Q$. Bei Definition der linearen Äquivalenz gilt also $P - Q \sim 0$ in der Picardgruppe.

Sei nun D ein Divisor auf F mit $\mathsf{grad}(D) = 0$. Da jedes Divisor, bei Definition, eine Summe von "trivialen" Divisoren ist (also Divisor der Form P, für irgendein $p \in F$), gilt, dass

$$D = P_1 + \ldots + P_n - Q_1 - \cdots - Q_n.$$

Daher ist $D \sim 0$ und wir schlussfolgern:

$$\mathsf{Pic}^0(F) = 0,$$

die triviale Gruppe. Von der Gleichung (26), auf der Seite 149 haben wir also

$$\mathsf{Pic}(F) \simeq \mathbb{Z}.$$

Kurvem vom Grad 2.

Lemma 4.6.3. *Sei F eine Kurve vom Grad 2 und $p, q \in F$ mit $p \neq q$. Es gibt eine rationale Funktion $\varphi \in K(F)$, so dass $\mu_p = 1$, $\mu_q = -1$ und $\mu_a = 0$ für jeden Punkt $a \in F$, mit $a \neq p$ und $a \neq q$.*

Beweis. Aufgabe. □

In unserer Diskussion mit Kurven vom Grad 1, haben wir eigentlich dieses Lemma in dem Fall bewiesen. Es folgt direkt, dass wir unser Argument für projektive Geraden, also F mit $\mathsf{grad}(F) = 1$, wiederholen können und wir erhalten

$$\mathsf{Pic}^0(F) = 0$$

und

$$\mathsf{Pic}(F) \simeq \mathbb{Z}.$$

4.6.2 Die Picardgruppe von Kurven mit Grad ≥ 3

Durchgehend in diesem Abschnitt ist F eine irreduzible nicht-singuläre projektive planare Kurve mit $\mathsf{grad}(F) = d \geq 3$.

Lemma 4.6.4. *Sein $p, q \in F$ mit $p \neq q$. Dann gilt $P \not\sim Q$ als Divisore.*

Beweis. Wir beweisen es durchs Widerspruch. Sei $P \sim Q$. In anderen Worten, es gibt eine rationale Funktion $\varphi = \frac{G}{H}$, mit $\mathsf{grad}(G) = \mathsf{grad}(H)$, so dass $P - Q = \operatorname{div}(\varphi) = \operatorname{div}(G) - \operatorname{div}(H)$. Sei L eine beliebige Gerade durch q, aber nicht tangential, welches zusätzlich nicht durch

p geht. Es gilt $\operatorname{div}(L) = Q + D$, wobei D ein positiver Divisor ist mit $\mathsf{grad}(D) = d - 1 \geq 2$ welches weder P noch Q als Summanden enthält. Es gilt

$$\begin{aligned}\operatorname{div}(GL) &= \operatorname{div}(G) + \operatorname{div}(L)\\ &= \operatorname{div}(G) - \operatorname{div}(H) + \operatorname{div}(H) + \operatorname{div}(L)\\ &= P - Q + \operatorname{div}(H) + Q + D\\ &= P + \operatorname{div}(H) + D\\ &\geq \operatorname{div}(H).\end{aligned}$$

Laut Teil (ii) von Korollar 4.4.7, wissen wir, dass es eine Kurve L' gibt, mit $\mathsf{grad}(L') = \mathsf{grad}(GL) - \mathsf{grad}(H) = \mathsf{grad}(L) = 1$ (da $\mathsf{grad}(G) = \mathsf{grad}(H)$). Es muss also L' eine Gerade sein, so dass $\operatorname{div}(L') = \sum_{a_i \in F} \mathfrak{I}(a_i, F \cap L')a_i = D + P$. Da aber $\mathsf{grad}(D) \geq 2$ und $\operatorname{div}(L) = Q + D$ war, liegen zumindest 2 (möglicherweise 1 Punkt mit Multiplizität 2) 2 Punkte sowohl auf L wie auch auf L'. Dies legt eine Gerade eindeutig fest, woraus $L = L'$ und daher, $p = q$ folgt. □

Dies gibt uns 2 direkte Korollare.

Korollar 4.6.5. *Die Gruppe* $\mathsf{Pic}^0(F)$ *ist nicht-trivial.*

Korollar 4.6.6. *Sei o ein ausgewähltes Punkt auf F. Die kanonische Abbildung*

$$\Phi : \mathrm{V}(F) \to \mathsf{Pic}^0(F), \quad \text{gegeben durch} \quad p \mapsto P - O$$

ist injektiv.

Beweis. Sei $\Phi(p) = \Phi(q)$. Daher, $P - O \sim Q - O$, was $P \sim Q$ impliziert, da dies natürlich mit der Gruppenstruktur (der Divisore) verträglich ist. Vom Lemma 4.6.4 wissen wir direkt, dass $p = q$ in $\mathrm{V}(F)$, was unsere Aussage beweist. □

Ein ausgewähltes Punkt ist ein beliebiges, aber fixiertes, Punkt auf F. Wir haben es mit o bezeichnet, weil es für uns bald die Einheit sein wird.
Es sollte gesagt werden, dass dies eine sehr erstaunliches Resultat ist. Wie es sich herausstellt (sieh Satz 4.7.4), gilt im Fall von $\mathsf{grad}(F) = 3$ sogar eine Bijektion. Daher können wir die Gruppenstruktur von $\mathsf{Pic}^0(F)$ auf $\mathrm{V}(F)$ übertragen. Es stellt sich heraus, dass diese Gruppenstruktur mit der in Satz 4.7.2 übereinstimmt. Die von Pic^0 induzierte Gruppenstrukture wurde zuerst erkannt! (von Poincaré), es gab aber viele partielle Resultate vorher. Namen wir Fermat, Bachet, Newton, Jacobi, Clebsch und andere sollten hier auch genannt werden.

4.7 Elliptische Kurven

Wir wollen nun projektive Kurven vom Grad 3 genauer studieren. Es stellt sich heraus, dass man auf deren Nullstellen eine Gruppenstruktur einführen kann. Damit fängt man ein Bereich an, welches Elliptische Kurven genannt wird und es ist eines der schönen Bereiche der algebraischer Geometrie. Es hat auch viele aktuelle Anwendungen in der Kryptographie und anderen angewandten Bereichen.

4.7.1 Die Verknüpfung durch die Geometrie

Proposition 4.7.1. *Sein A, B, C Kurven vom Grad 3 mit A irreduzibel. Man nehme an, dass $A \bullet B = \sum_{i=1}^{9} P_i$, wobei A regulär auf den p_i's ist. Sei $A \bullet C = \sum_{i=1}^{8} P_i + Q$. Dann gilt $q = p_9$.*

In andern Worten, wenn 8 der Schnittpunkte von A und B mit 8 der Schnittpunkte von A und C übereinstimmen, dann stimmen sie auch am neunten überein.

Beweis. Sei L eine Gerade, welches durch p_9 geht, aber nicht durch q. Da $\mathsf{grad}(L) = 1$ und $\mathsf{grad}(A) = 3$, ist laut Bézout $A \bullet L = P_9 + R + S$ wobei r, s einfach Punkte auf A sind. Man wähle die Gerade so, dass $p_9 \neq r \neq s$, was man natürlich immer kann.

Betrachte nun $A \bullet LC$, wobei LC einfach das Produkt der zugehörigen Polynome ist. Laut Proposition 4.3.9, Teil (ii), gilt

$$\begin{aligned} A \bullet LC &= A \bullet L + A \bullet C \\ &= (P_9 + R + S) + (\sum_{i=1}^{8} P_i + Q) \\ &= \sum_{i=1}^{9} P_i + R + S + Q \\ &= A \bullet B + R + S + Q. \end{aligned}$$

Da $A \bullet LC \geq A \bullet B$ und A regulär auf jedem der Punkte $p_1, \ldots, p_9$ ist, impliziert Teil (ii) von Proposition 4.4.7, dass es eine Kurve L' gibt, mit $A \bullet L' = A \bullet LC - A \bullet B = A \bullet B + R + S + Q - A \bullet B = R + S + Q$. Wie auf Seite 4.4 schon bemerkt muss $\mathsf{grad}(L') = \mathsf{grad}(LC) - \mathsf{grad}(B) = 4 - 3 = 1$. Also, L' ist eine Gerade und wird als solches durch 2 verschiedene Punkte fixiert.

Da aber L und L' auf den zwei (ungleichen) Punkten r und s miteinander übereinstimmen, muss $L = L'$ gelten. Damit muss natürlich auch ihrer dritter Schnittpunkt mit A gleich sein, also $p_9 = q$. □

Die Pre-Verknüpfung Sei A eine reguläre Kurve vom Grad 3 und sein p, q Punkte auf A. Wenn $p \neq q$, gibt es genau eine Kurve L, welches durch die Punkte p, q geht. Bei Bézout schneidet sich A und L an 3 (nicht zwingend verschiedenen) Punkten. Da wir aber nur zwei Punkte p, q im Schnitt $A \cap L$ hatten, gibt es einen weiteren Punkt w, welches wir mit $\varphi(p, q)$

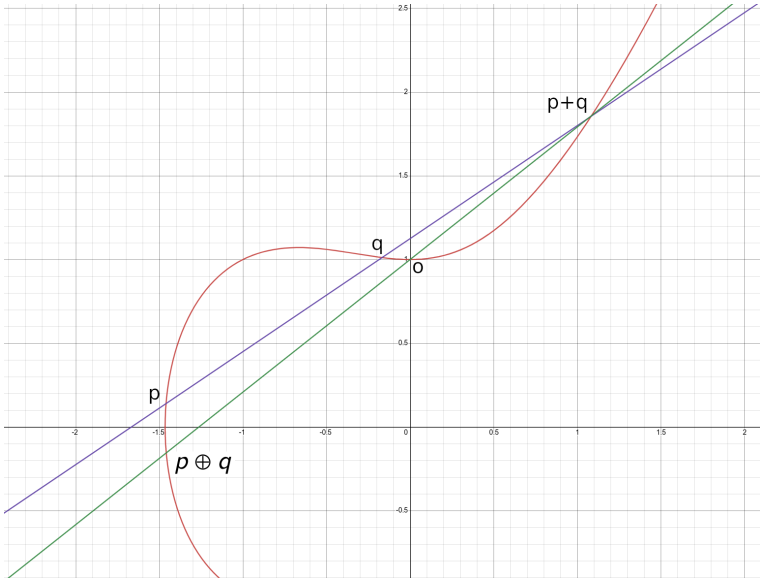
bezeichnen. Wir definieren also $p+q := \varphi(p,q) = w$ und nennen es die *pre-Verknüpfung*. Hier kann natürlich $w = p$ oder $w = q$ gelten, wenn eines von denen ein Doppelpunkt ist.

Wenn $p = q$, dann nehmen wir die Tangente $L = T_p$ von A am Punkt $p = q$. In dem Fall schneidet sich L mit A am Punkt $p = q$ mit Multiplizität 2, daher gibt es, wieder nach Bézout, einen weiteren Punkt w welches im Schnitt $A \cap L$ liegt. Wir definieren $p + q := \varphi(p,q) = w$.

In diesem Fall ist A noch keine Gruppe, es ist keine besonders vertraute algebraische Struktur. Wir haben nicht einmal eine Einheit, denn es gibt ja a-priori keinen besonderen Punkt auf der Kurve A. Es ist auch nicht assoziativ! Wenn wir aber einen Punkt wählen und es Null nennen, können wir durch eine einfache Iteration eine Gruppenstruktur auf den Nullstellen von A definieren. Mehr als das, dies wird sogar eine Abelsche Gruppe sein.

Die Verknüpfung Wie machen es wie folgt: Sei $o \in A$ ein beliebiger, fixierter Punkt. Setze

$$p \oplus q := \varphi(o, \varphi(p,q)) = o + (p+q). \tag{27}$$



Aufgepasst, die Pre-Verknüpfung ist nicht assoziativ. Daher ist die Klammer auf $p + q$ wichtig. Daher, wir verbinden die zwei Punkte p, q mit einer Gerade und den dritten Schnittpunkt dieser Gerade verbinden wir mit unserem ausgewählten Punkt o. Der dritte Schnittpunkt dieser neuen Gerade ist unsere eigentliche Verknüpfung von p und q.

Satz 4.7.2. *Die Verknüpfung $\oplus : A \times A \to A$, gegeben durch $(p,q) \mapsto \varphi(o, \varphi(p,q))$ definiert die Struktur einer abelschen Gruppe auf A, mit o als Einheit.*

Beweis. • Assoziativität: Sein $p, q, r \in A$. Definiere L_1 als die eindeutige Gerade, welches $L_1 \bullet A = P + Q + S'$ für irgendein $s' \in A$ erfüllt. Wenn $p \neq q$, ist es klar, dass L_1 eindeutig

bestimmt ist, da zwei ungleiche Punkte ja eine Gerade festlegen. Wenn $p = q$, dann ist bei Definition von $p + q$ ja die Tangente von A an $p = q$. Auch dies ist also eindeutig festgelegt.

Gleichwie definieren wir M_1 mit $M_1 \bullet A = O + S' + S$. Daher, $s = \varphi(o, \varphi(p, q)) = p \oplus q$. Definiere L_2 als $L_2 \bullet A = S + R + T$. Wir brauchen nicht t mit o verbinden. Den Grund sehen wir gleich.

Auf der anderen Seite, sei $M_2 \bullet A = Q + R + U'$ und $L_3 \bullet A = O + U' + U$. Also $u = \varphi(o, \varphi(q, r)) = p \oplus r$. Wir verknüpfen nun mit p und erhalten $M_3 \bullet A = P + U + T'$.

Da $(p \oplus q) \oplus r = \varphi(o, t)$ und $p \oplus (q \oplus r) = \varphi(o, t')$, genügt es zu beweisen, dass $t = t'$.

Definiere hierzu die Kurven $L := L_1 L_2 L_3$ und $M = M_1 M_2 M_3$. Beide sind klar vom Grad 3. Deren Schnittpunkte mit A stimmen auf den Punkten o, p, q, r, s, s', u, u' überein. Die 9-ten zusätzlichen Schnittpunkte sind t und t'. Proposition 4.7.1 besagt nun, dass $t = t'$ gelten muss.

- Kommutativität: Dies ist völlig klar, da wir bei der Gerade Anfangs- und Endpunkte nicht unterscheiden.
- Einheit: Sei $p \in A$ und definiere L durch $L \bullet A = P + O + U$. Wir haben $L' \bullet A = U + O + U'$, wobei $u' = p \oplus o$ ist. Da L und L' auf u und o übereinstimmen, muss $L = L'$ und $u' = p$ gelten. Damit ist $p \oplus o = p$.
- Inverse: Das Inverser zu p ist $p + (o + o)$. Um dies zu sehen, sei $L_1 \bullet A = O + O + Z$ $(z = o + o)$ und $L_2 \bullet A = Z + P + Y$ $(y = z + p)$. Sei $L_3 \bullet A = P + Y + X$ $(x = p + y)$ und $L_4 \bullet A = X + O + W$ $(w = x + o)$ und damit also $w = p \oplus [p + (o + o)]$.

  Da nun L_2 und L_3 auf p und y miteinander übereinstimmen, muss $L_2 = L_3$ gelten. Da dies/diese A 3 mal schneiden, muss $z = x$ gelten. Daher können wir $L_4 \bullet A = O + Z + W$ umschreiben und nun stimmen L_1 und L_4 auf o und w überein. Mit dem selben Argument muss also $w = o$ gelten und damit haben wir gezeigt, dass p ein Inverses hat. □

4.7.2 Die Verknüpfung durch die Picardgruppe

Lemma 4.7.3. *Sei F eine irreduzible reguläre Kurve vom Grad 3. Für alle Punkte $a, b \in F$ gilt*

$$a + (a + b) = b.$$

Spezifisch gibt es für alle drei Punkte $p, q, r \in F$ einen Punkt s, so dass

$$P + Q \sim R + S$$

linear äquivalent als Divisore sind. (Die Addition ist die Addition der Divisore, nicht die pre-Verknüpfung der Punkte).

Beweis. Sei L_1 eine Gerade, so dass $L_1 \bullet F = A+B+C$ und $L_2 \bullet F = C+A+D$. Da L_1 und L_2 auf a und b übereinstimmen, folgt, dass $L_1 = L_2$ und daher müssen alle derer Schnittpunkte mit F übereinstimmen, woraus $b = d = a + (a + b)$ folgt.

Sei $s = r + (p + q)$. Dann gilt $r + s = r + [r + (p + q)] = p + q$, laut dem ersten Teil dieses Lemmas, mit $a = r, b = (p + q)$. Daher, es gibt zwei Geraden, M_1, M_2, wobei M_1 durch r und s geht, M_2 durch p und q und M_1, M_2 sich auf dem Punkt $u = r + s = p + q$ treffen. Dann gilt $M_1 \bullet F = \operatorname{div}(M_1) = P + Q + U$ und $M_2 \bullet F = \operatorname{div}(M_2) = R + S + U$, daher $U = \operatorname{div}(M_2) - R - S$, woraus $\operatorname{div}(M_1) = P + Q + \operatorname{div}(M_2) - R - S$ folgt. Wir haben also

$$P + Q - (R + S) = \operatorname{div}(M_1) - \operatorname{div}(M_2) + R + S = \operatorname{div}\left(\frac{M_1}{M_2}\right),$$

und damit die lineare Äquivalenz. □

Satz 4.7.4. *Sei* $\mathsf{grad}(F) = 3$ *und* o *ein ausgewähltes Punkt auf* F*. Die kanonische Abbildung*

$$\Phi : \mathrm{V}(F) \to \mathsf{Pic}^0(F), \quad \text{gegeben durch} \quad p \mapsto P - O,$$

ist ein Isomorphismus.

Beweis. Als erstes zeigen wir, dass dies eine Bijektion ist. Injektivität ist Korollar 4.6.6. Für die Surjektivität, sei $D \in \mathsf{Pic}^0(F)$ beliebig. Da es bei Definition von Pic^0 Grad Null hat, ist es von der Form

$$D = P_1 + \cdots + P_m - Q_1 - \cdots - Q_m, \tag{28}$$

wobei die p_i, q_i (nicht zwangsweise verschiedene) Punkte auf $\mathrm{V}(F)$ sind. Sei $m = 1$. Daher, $D = P_1 - Q_1$. Dann gibt es laut Lemma 4.7.3 einen $s \in F$, so dass $P_1 + O \sim Q_1 + S$, was

$$D = P_1 - Q_1 \sim S - O$$

impliziert. Doch dies bedeutet genau, dass $\Phi(S) = S - O \sim D$, was die Surjektivität beweist.

Sei nun $m \geq 2$. Wieder nach Lemma 4.7.3 gibt es einen Punkt $s \in F$, so dass $P_1 + P_2 \sim Q_1 + S$. Daher können wir Formel (28) zu

$$D \sim S + P_3 + \cdots + P_m - Q_2 - \cdots - Q_m$$

reduzieren. Indem wir nun S als einen neuen P_2 auffassen, merken wir, dass wir von m auf $m - 1$ gegangen sind. Dies beweist die Bijektion.

Um den Isomorphismus zu beweisen, sei $p, q \in F$. Man erinnere sich, dass $p \oplus q = (p+q)+o$. Sei $L_1 \bullet F = P + Q + U$ und $L_2 \bullet F = U + O + V$. Daher, $v = p \oplus q$. Wir haben $\Psi(p) + \Psi(q) = P - O + Q - O$ und $\Psi(p \oplus q) = V - O$. Wir haben zu beweisen, dass $V = P + Q - O$.

Wie im Beweis von Lemma 4.7.3, impliziert $\operatorname{div}(L_1) = L_1 \bullet F = P + Q + U$ und $\operatorname{div}(L_2) = L_2 \bullet F = U + O + V$ (indem wir U von einem bestimmen und im anderen einsetzen), dass $\operatorname{div}\left(\frac{L_1}{L_2}\right) + O + V = P + Q$, was uns

$$\operatorname{div}\left(\frac{L_1}{L_2}\right) + V = P + Q - O,$$

und somit

$$V \sim P + Q - O$$

gibt. Dies schließt den den Beweis ab. □

Korollar 4.7.5. *Die zwei Verknüpfungen definiert auf* $\mathrm{V}(F)$ *sind gleich.*

Korollar 4.7.6. *Die (geometrische) Gruppenstruktur, definiert in Formel 27 ist unabhängig vom Wahl des ausgesonderten Punktes* $o \in F$*.*

Beweis. Dies folgt, da $\mathsf{Pic}^0(F)$ klar nicht vom Wahl des ausgewählten Punktes abhängt. □

4.8 Der Satz von Riemann-Roch - Nicht mehr Teil des Kurses!

Bemerkung 4.8.1. Der folgende Teil ist nicht mehr Teil des Kurses. Es wird nicht abgefragt werden. Bei der Erstellung habe ich auch nicht auf Details geachtet. Es gibt vermutlich auch einige (viele?) Fehler. Es wurde nur reingelassen, falls jemand Interesse hat und es einfacher findet den Kurs "fertigzulesen" als sich das Thema in einem unvertrautem Buch/Vorlesungsskript nachzulesen.

Das letzte wird jedoch stark empfohlen, falls man sich mit dem Thema besser vertraut machen will. Die nachfolgenden paar Seiten sollen höchstens einen kleinen Überblick geben.

Unsere Funktion F ist regulär (auf allen Punkten) und irreduzibel.

Eines der wichtigsten Objekte in der algebraischen Geometrie, gar in ganz Algebra, sind Funktionen. Um ein Objekt X zu studieren, studieren wir öfters die Abbildungen von oder nach X. Zum Beispiel, wenn X eine Varietät über K ist, betrachten wir Abbildungen von X nach K.

Das Studium von rationalen Funktionen ist als solches von großer Bedeutung. Das Problem ist jedoch, dass diese unendlich viele ist. Sie bilden sogar eine unendlich dimensionalen Vektorraum. Auf der anderen Seite, wenn wir uns nur auf reguläre rationale Funktionen einschränken haben wir folgendes:

Proposition 4.8.2. *Sei F eine projektive planare Kurve über einen algebraisch abgeschlossenen Körper. Dann gilt*

$$\bigcap_{p \in F} \mathcal{O}_p(\mathrm{V}(F)) = K.$$

Beweis. Sei $\varphi = \frac{\overline{G}}{\overline{H}}$. Laut Lemma 4.3.16 ist $\mathrm{div}(H) \leq \mathrm{div}(G)$. Anders gesagt, $F \bullet H \leq F \bullet G$. Teil (ii) vom Korollar 4.4.7 besagt nun die Existenz einer Kurve B mit $B \bullet F = G \bullet F - H \bullet F$ und $\overline{H} = \overline{BG}$. Da bei Definition $\mathsf{grad}(G) = \mathsf{grad}(H)$, folgt, dass $\mathsf{grad}(B) = \mathsf{grad}(G) - \mathsf{grad}(H) = 0$, also eine Konstante $c \in K$. Daher ist also $\overline{BG} = c$ und somit ist $\varphi = c \in K$. □

In anderen Worten, die einzigen Abbildungen die auf allen Punkten von $\mathrm{V}(f)$ regulär sind, sind die Konstanten Polynome. Das Phänomen, das wir hier sehen, ist ähnlich zum Satz von Liouville aus der Funktionentheorie. Wir werden dies aber nicht weiter ansprechen.

Korollar 4.8.3. *Der Kern der Abbildung* $\mathrm{div} : K(\mathrm{V}(F))^* \to \mathrm{Div}^0(F) \subseteq \mathrm{Div}(F)$ *ist*

$$\mathsf{Ker}(\mathrm{div}) = K^*.$$

Beweis. Sei $\varphi \in K(\mathrm{V}(F))^*$ mit $\mathrm{div}(\varphi) = 0$. Es gilt laut Proposition 4.8.2, dass $\frac{\varphi}{=} c \in K^*$ und wir sind fertig. □

Beweis. Sei $\varphi \in K(\mathrm{V}(F))^*$ mit $\mathrm{div}(\varphi) = 0$. Es gilt laut Proposition 4.8.2, dass $\frac{\varphi}{=} c \in K^*$ und wir sind fertig. □

Anders gesagt, bis auf Konstante werden rationale Funktionen von deren Divisoren unterschieden.

Letztlich ist es also so, dass rationale Funktionen "zu viele" sind, aber reguläre rationale Funktionen "zu wenige". Wie Goldlöckchen suchen wir also etwas dazwischen: Rationale Funktionen, welche "fast überall" regulär sind. Daher, nur endlich viele Polstellen haben. Wir werden beweisen, dass dies ein endlichdimensionaler Vektorraum ist und daher ist ihre Dimension eine wichtige Invariante. Es ist nicht direkt klar warum, aber diese Invariante wird öfters von großer Bedeutung sein. Die Gleichung, welches dies genau beschreibt, ist der Satz von Riemann-Roch.

Wir werden Divisoren benutzen um rationale Funktionen mit endlich vielen Polen zu beschreiben.

Definition 4.8.4. *Sei $D \in \mathrm{Div}(F)$ ein Divisor. Wir definieren*

$$L(D) \coloneqq \{\varphi \in K(\mathrm{V}(F)) \mid \mathrm{div}(\varphi) + D \geq 0\} \cup \{0\} \subseteq K(\mathrm{V}(F)).$$

Lemma 4.8.5. *Die Teilmenge $L(D) \subseteq K(\mathrm{V}(F))$ ist ein K-Vektorraum.*

Beweis. Sein $\varphi, \psi \in L(D)$ und $\lambda \in K$. Daher, $\mathrm{div}(\varphi), \mathrm{div}(\psi) \geq D$ was laut Lemma 2.4.15f

$$\mathrm{div}(\varphi + \psi) \geq \min(\mathrm{div}(\varphi) + \mathrm{div}(\psi)) \geq D$$

ergibt.

Auf der anderen Seite, sei $\lambda \neq 0$. Dann ist

$$\mathrm{div}(\lambda\psi) = \mathrm{div}(\lambda) + \mathrm{div}(\psi) = \mathrm{div}(\psi) \geq D$$

laust Teil (ii) von Lemma **??** und (i) von Lemma 2.4.14. Im Falle $\lambda = 0$ haben wir $\lambda\psi = 0 \in L(D)$, da es bei Definition die Null enthält. □

Definition 4.8.6. *Wir definieren*

$$l(D) \coloneqq \dim_K L(D) \in \mathbb{N} \cup \infty.$$

Sei $D = \sum_{p \in F} n_p p \in \mathrm{Div}(F)$ ein Divisor. Man bedenke, was $\mathrm{div}(\varphi) + D \geq 0$ bedeutet. Es heißt, dass an jedem Punkt $p \in F$, $\mathfrak{I}(p, \varphi \cap F) \geq -n_p$. Da D ein Divisor ist, sind nur endlich viele der Koeffizienten n_p ungleich Null. In anderen Worten φ ist regulär an allen, außer vielleicht einer endlichen Anzahl von Punkten: genau wie gewollt. Spezifisch gilt:

(a) Für $n_p > 0$ hat φ maximal eine Polstelle vom Grad n_p und

(b) Für $n_p < 0$ hat φ zumindest eine Nullstelle von n_p.

Wie wünschen nun die Dimension $l(D)$ des Vektorraumes $L(D)$ zu berechnen. Dies wird nicht immer möglich sein, aber der Satz von Riemann-Roch wird es öfters ermöglichen.

Lemma 4.8.7. *Es gilt* $L(0) = K$ *und* $l(0) = 1$.

Beweis. Bei Definition ist es die Menge der rationalen Funktionen, die an jedem Punkt regulär sind. Daher besagt Korollar 4.8.2, dass $L(0) = K$ ist. Es folgt, dass $l(0) = \dim_K L(0) = \dim_K K = 1$. □

Lemma 4.8.8. *Sei* $D \in \mathrm{Div}(F)$ *ein Divisor mit* $\mathsf{grad}(D) < 0$. *Dann gilt* $L(D) = \{0\}$ *was* $l(D) = 0$ *impliziert.*

Beweis. Sei $0 \neq \varphi \in L(D)$ ein Element ungleich Null. Daher $\varphi \in K(\mathrm{V}(F))^*$, mit $\mathrm{div}(\varphi) + D \geq 0$. Da der Grad ein Gruppenhomomorphismus ist würde dies $\mathsf{grad}(\mathrm{div}(\varphi)) + \mathsf{grad}(D) \geq 0$ implizieren. Proposition 4.3.13 führt nun zum Widerspruch, da $\mathsf{grad}(\mathrm{div}(\varphi)) = 0$ und daher $\mathsf{grad}(D) \geq 0$ sein muss, wir aber sagten, dass $\mathsf{grad}(D) < 0$ ist. □

Lemma 4.8.9. *Sein* $D_1, D_2 \in \mathrm{Div}(F)$ *Divisore.*

(i) Wenn $D_1 \leq D_2$, *dann ist* $L(D_1) \subseteq L(D_2)$ *und daher* $l(D_1) \subseteq l(D_2)$.

(ii) Wenn $D_1 \sim D_2$ *linear äquivalent sind, daher es ein* $\varphi \in K(\mathrm{V}(F))^*$ *gibt, mit* $D_1 - D_2 = \mathrm{div}(\varphi)$, *dann ist die Abbildung*

$$L(D_1) \to L(D_2), \quad \text{gegeben durch} \quad \psi \mapsto \psi\varphi,$$

ein Isomorphismus. Spezifisch gilt also $l(D_1) = l(D_2)$.

Beweis. (i) Dies folgt direkt von Lemma 4.3.4. Nämlich von $\mathrm{div}(\varphi) \in L(D_1)$, also $\mathrm{div}(\varphi) + D \geq 0$, haben wir dann die Ungleichung $\mathrm{div}(\varphi) + D_2 \geq \mathrm{div}(\varphi) + D_1 \geq 0$.

(ii) Sei $\psi \in D_1$, daher $\mathrm{div}(\psi) + D_1 \geq 0$. Bei Teil (ii) von Lemma **??** gilt dann

$$0 \leq \mathrm{div}(\psi) + D_1 = \mathrm{div}(\psi) + \mathrm{div}(\varphi) + D_2 = \mathrm{div}(\psi\varphi) + D_2,$$

also ist $\phi\varphi \in L(D_2)$. Als solches macht die Abbildung Sinn. Das Inverse dazu ist gegeben durch $\psi' \mapsto \frac{\psi'}{\varphi}$. Diese sind natürlich invers zueinander da $\frac{\varphi\psi}{\varphi} = \psi$ und $\varphi\frac{\psi'}{\varphi} = \psi'$. □

Korollar 4.8.10. *Die Abbildung* $l(-) : \mathsf{Pic}(F) \to \mathbb{N} \cup \infty$ *ist wohldefiniert.*

Beweis. Dies ist quasi Teil (ii) des obigen Lemmas 4.8.9. □

Viele der Methoden um $l(D)$ zu berechnen werden "Induktion" benutzen. Daher, wir werden öfters $l(D)$ auf $l(D + P)$ reduzieren wollen. Hierzu wird uns das folgende Resultat behilflich sein:

Lemma 4.8.11. *Sei* $p \in F$ *ein Punkt. Es gilt* $\mathsf{grad}(P) = 1$.

Proposition 4.8.12. *Sei* $D \in \mathrm{Div}(F)$ *ein Divisor.*

(i) Für jeden Punkt $p \in F$ gilt

$$l(D+P) = l(D) \quad \text{oder} \quad l(D+P) = l(D)+1.$$

(ii) Für jeden Divisor $D \leq D'$ gilt

$$l(D) \leq l(D') \leq l(D) + \mathsf{grad}(D'-D).$$

Beweis. (i) Da $D \leq D+P$ folgt $L(D) \subseteq L(D+P)$ aus Lemma 4.8.9, Teil (i), woraus $l(D) \leq l(D+P)$ folgt. Sei n_p das Koeffizient von p in D. Damit ist also n_p+1 das Koeffizient von p in $D+P$. Wir haben die Komposition $L(D+P) \subseteq K(\mathrm{V}(F)) \hookrightarrow \mathcal{O}_p(F) = K(\mathrm{V}(F))_{\mathfrak{m}_p}$ von injektiven Abbildungen, mit der wir also φ als ein Element von $\mathcal{O}_p(f)$ auffassen können. Laut Satz 2.3.42 ist $\mathcal{O}_p(f)$ ein diskreter Bewertungsring und daher können wir dank Proposition 2.3.38 $\varphi = ct^n$ schreiben, wobei c eine Einheit und t irreduzibel ist.

Betrachte die Abbildung

$$\Phi : L(D+P) \to K, \quad \varphi \mapsto (t^{n_p+1}\varphi)(p) = (ct^{n+n_p+1})(p).$$

Es ist klar, dass dies wohldefiniert ist, da laut Lemma 2.4.14 wir $\mathfrak{I}(p, f \cap ct^{n+n_p+1}) = n+n_p+1 \geq 0$ haben (da $n_p+1 \geq 0$ bei Annahme). Lemma 2.4.16 besagt nun, dass dies am Punkt p regulär ist.

Der Kern dieser Abbildung ist die Menge der ct^{n+n_p+1}, welche auf p eine Nullstelle haben. Also, wo die Schnittzahl $\mathfrak{I}(p, f \cap ct^{n+n_p+1}) = n+n_p+1$ streng positiv ist: daher $n+n_p \geq 0$ gilt. Da bei Proposition 2.4.15 wir $n = \mathfrak{I}(p, f \cap g) - \mathfrak{I}(p, f \cap h)$, wobei $\varphi = \frac{g}{h}$, ist dies äquivalent zu sagen, dass die Menge der φ's ist, mit $\varphi + D \geq 0$. In andern Worten,

$$\mathsf{Ker}(\Psi) = L(D).$$

Der Hauptisomorphiesatz besagt nun

$$L(D+P)/L(D) \simeq \mathrm{Im}(\Psi) \subseteq K.$$

Da das Bild $\mathrm{Im}(\Psi)$ ein Untervektorraum von K ist, muss es K oder 0 sein. Im ersten Fall haben wir $l(D+P) = l(D)+1$, im zweiten $l(D+P) = l(D)$.

(ii) Dies folgt direkt vom ersten Teil, da man D' von D erhält, indem man $\mathsf{grad}(D'-D)$ Punktdivisoren hinzuaddiert. □

Proposition 4.8.13. *Sei $a \in f$ regulär und $\mathfrak{v}$ die Auswertung des diskreten Bewertungsringes $\mathcal{O}_a(f)$. Für jeden $\varphi = \frac{g}{h} \in \mathcal{O}_a(f)$ gilt*

$$\mathfrak{v}(\varphi) = \mu_a(\varphi) := \mathfrak{I}(a, g \cap f) - \mathfrak{I}(a, h \cap f) = \mathsf{grad}(\mathrm{div}(\varphi)).$$

(Def 4.3.12)

Bemerkung 4.8.14. Dies muss vor Proposition 4.8.12.

Korollar 4.8.15. *Sei $D \in \mathrm{Div}(F)$ ein Divisor mit $\mathsf{grad}(D) \geq 0$. Es gilt*

$$l(D) \leq \mathsf{grad}(D) + 1.$$

Spezifisch, $l(D)$ ist immer endlich, also $L(D)$ ist immer ein endlichdimensionaler Vektorraum.

Beweis. Sei $n = \mathsf{grad}(D) + 1$ und $p \in F$ ein Punkt. Da der Grad laut Lemma 4.3.5 ein Gruppenhomomorphismus ist, gilt

$$\mathsf{grad}(D - nP) = \mathsf{grad}(D) - \mathsf{grad}(nP) = \mathsf{grad}(D) - n\mathsf{grad}(P) = \mathsf{grad}(D) - n = -1 < 0,$$

wobei die vorletzte Gleichung von Lemma 4.8.11 kommt und die letzte weil n so gewählt war. Lemma 4.8.8 besagt nun, dass $L(D - nP) = 0$. Da $D - nP \leq D$ ist, besagt Teil (ii) des obigen Lemmas 4.8.11, dass

$$l(D) \leq (D - nP) + \mathsf{grad}(D - (D - nP)) = l(D - nP) + \mathsf{grad}(nP) = 0 + n = \mathsf{grad}(D + 1).$$

Da der Grad von D immer endlich ist, ist also $l(D)$ immer endlich. □

Beispiel 4.8.16 ($l(D)$ kann $\mathsf{grad}(D) + 1 - g$ werden).

Satz 4.8.17 (Der Satz von Riemann)**.** *Sei $\mathsf{grad}(F) = d$. Es gibt eine kleinste natürliche Zahl $g \in \mathbb{N}$, welches nur von F abhängt, so dass für jeden Divisor $D \in \mathrm{Div}(F)$,*

$$l(D) \geq \mathsf{grad}(D) + 1 - g.$$

Diese Zahl ist gegeben durch $g = \binom{d-1}{2}$.

Beweis. Wir werden beweisen, dass $g = \binom{d-1}{2}$ die kleinste ganze Zahl ist, für den dies gilt. Die Eindeutigkeit folgt dann direkt, da "die kleinste ganze Zahl" ja automatisch eindeutig ist.

Als erstes zeigen wir, dass die Ungleichheit gilt $l(D) \geq \mathsf{grad}(D) + 1 - \binom{d-1}{2}$ gilt.

Behauptung 1: Sein $D \sim D'$ linear äquivalent und gelte $l(D) \geq \mathsf{grad}(D) + 1 - g$. Dann gilt $l(D') \geq \mathsf{grad}(D') + 1 - g$.

Dies folgt direkt von Teil (ii) von Lemma 4.8.9 und Lemma 4.6.2.

Behauptung 2: Sei $D' \leq D$ und es gelte $l(D) \geq \mathsf{grad}(D) + 1 - g$. Dann gilt auch $l(D') \geq \mathsf{grad}(D') + 1 - g$.

Da $D' \leq D$ folgt aus Proposition 4.8.12, Teil (ii), dass

$$\begin{aligned} l(D') &\geq l(D) - \mathsf{grad}(D - D') \\ &\geq \mathsf{grad}(D) + 1 - g - \mathsf{grad}(D - D') \\ &= \mathsf{grad}(D) + 1 - g - \mathsf{grad}(D) + \mathsf{grad}(D') \\ &= \mathsf{grad}(D') + 1 - g, \end{aligned}$$

wobei wir hier $\mathsf{grad}(D - D') = \mathsf{grad}(D) - \mathsf{grad}(D')$ laut Lemma 4.3.5 haben.

Nun zum Eigentlichen Beweis: Sei $D \in \mathrm{Div}(F)$ ein beliebiger Divisor und schreibe es als

$$D = P_1 + \cdots + P_n - E,$$

wobei $n \geq d = \mathsf{grad}(F)$, $p_i \in F$ beliebige Punkte auf F sind, mit P_i als dessen assoziierte Divisore und $E \geq 0$ ein positiver Divisor. Da wir keine weitere Anforderung auf E stellen, können wir diese Gleichung hinschreiben. Spezifisch, die Divisore P_i können ruhig Summanden von E sein und die Punkte können auch nach belieben gleich sein.

Für jede $1 \leq i \leq n$, sei L_i eine Gerade (ungleich F), welches durch p_i verläuft. Wir definieren den Divisor

$$D' := D + \frac{z^n}{L_1 \cdots L_n}.$$

Da $\mathsf{grad}(L_i) = 1$ für alle $1 \leq i \leq n$ ist $\mathsf{grad}(z^n) = \mathsf{grad}(L_1 \cdots L_n)$ und somit ist $\frac{z^n}{L_1 \cdots L_n} \in K(\mathrm{V}(F))^*$ eine rationale Abbildung. Es folgt, dass $\mathrm{div}\left(\frac{z^n}{L_1 \cdots L_n}\right) \in \mathsf{HDiv}(F)$ und damit sind $D \sim D'$ linear äquivalent. Ferner gilt

$$D' = P_1 + \cdots + P_n - E + \mathrm{div}(z^n) - \sum_{i=1}^{n} \mathrm{div}(L_i) \leq P_1 + \cdots P_n - E + \mathrm{div}(z^n) - P_1 - \cdots - P_n \leq \mathrm{div}(z^n),$$

wobei die erste Gleichung Lemma**??** ist und die erste Ungleichung von der Tatsache, dass $\mathrm{div}(L_i) = \sum_{p \in F} \mathfrak{I}(p, L_1 \cap F)$ bei Definition ist. Da p_i bei Definition auf L_i liegt (und natürlich auf F) ist P_i eines der Summanden von $\mathrm{div}(L_i)$.

Bei Beispiel 4.8.16 gilt $l(\mathrm{div}(z^n)) \geq \mathsf{grad}(\mathrm{div}(z^n)) + 1 - g$. Laut Behauptung 2 gilt es nun also auch für D' und Behauptung 1 sagt, dass es nun für D hält, wie gewollt.

Das $g = \binom{d-1}{2}$ nun die kleinste solche Zahl ist folgt auch vom Beispiel 4.8.16, wo wir zeigen, dass diese Zahl für jede Kurve erreicht wird. Dies ergibt nun den Bewies. □

Definition 4.8.18. *Das $g = \binom{d-1}{2}$ vom Satz 4.8.17 wird das* (algebraische) Genus *von F genannt.*

Mehr als das, wir sehen direkt, dass es nur vom Grad von F abhängt.

Ohne zu beweisen sagen wir, dass es auch in der Topologie einen Genus gibt. Für den Fall $K = \mathbb{C}$ stimmen diese Definitionen miteinander überein.

Korollar 4.8.19. *Für jeden Divisor $D \in \mathrm{Div}(F)$ mit $\mathsf{grad}(D) \geq 0$ gilt*

$$\mathsf{grad}(D) + 1 - g \leq l(D) \leq \mathsf{grad}(D) + 1,$$

wobei $g = \binom{d-1}{2}$, mit $d = \mathsf{grad}(F)$.

Beweis. Die ist eine Zusammenführung von Riemanns Satz 4.8.17 und Korollar 4.8.15. □

Wir wollen dies nun zu einer Gleichung machen. Die Dimension $l(D)$ ist aber von mehr als nur von $\mathsf{grad}(F)$ und $\mathsf{grad}(D)$ abhängig, zumindest für kleine $\mathsf{grad}(D)$, wie das folgende Beispiel zeigt:

So ähnlich in Max Noethers Satz, stellen wir uns nun die Frage, ob es einen Divisor $D' \in \mathrm{Div}(F)$ gibt, mit $\mathsf{grad}(D') = l(D) - (\mathsf{grad}(D) + 1 - g)$. Die Antwort darauf ist ja und mehr als das, dies ist recht einfach von D zu erstellen. Hierzu aber zuerst eine Definition:

Definition 4.8.20. *Sei $\mathsf{grad}(F) = d$ und $L \neq F$ eine Gerade. Definiere*

$$K_F := [(d-3)\mathrm{div}(L)] \in \mathsf{Pic}(F)$$

Wir schreiben $F_k \in \mathsf{Pic}(F)$, da wir es als einen Element der Picardgruppe auffassen. In anderen Worten, $(d-3)\mathrm{div}(L)$ ist in $\mathrm{Div}(F)$, aber wir betrachten dessen Klasse in der Quotientengruppe $\mathsf{Pic}(F) = \mathrm{Div}(F)/\mathsf{HDiv}(F)$. Daher haben wir folgendes

Lemma 4.8.21. *Sei $\mathsf{grad}(F) = d$ und $L, L' \neq F$ Geraden. Dann gilt*

$$K_F = [(d-3)\mathrm{div}(L)] = K'_F = [(d-3)\mathrm{div}(L')],$$

wobei wir es als Äquivalenzklassen.

Beweis. In anderen Worten, wir wollen beweisen, dass $(d-3)\mathrm{div}(L) \sim (d_3)\mathrm{div}(L')$ linear äquivalent sind, als Elemente von $\mathrm{Div}(F)$. Dies ist trivial, da alle Geraden äquivalent sind in $\mathsf{Pic}(F)$, denn $\mathrm{div}(L) - \mathrm{div}(L') = \mathrm{div}(\frac{L}{L'}) \in \mathsf{HDiv}(F)$. Die erste Gleichung ist Teil (ii) von Lemma **??**. □

Daher ist die Definition von K_F nicht von der Wahl der Gerade abhängig. Es mag vielleicht etwas verwirrend sein, warum wir dies "kanonisch" nennen. Der Grund ist jedoch, weil diese eine Stabilitätseigenschaft haben, sieh Proposition 4.8.23:

Lemma 4.8.22. *Sei $g = \binom{d-1}{2}$ das Genus von F. Dann gilt $\mathsf{grad}(K_F) = 2g - 2$.*

Beweis. Laut Lemma **??** und Proposition 4.3.13 gilt

$$\begin{aligned}
\mathsf{grad}(K_F) &= \mathsf{grad}[(d-3)\mathrm{div}(L)] \\
&= (d-3)\mathsf{grad}(\mathrm{div}(L)) \\
&= (d-3)\mathsf{grad}(F) \\
&= (d-3)d \\
&= 2\binom{d-1}{2} - 2 \\
&= 2g - 2.
\end{aligned}$$

□

Proposition 4.8.23. *Für jeden Punkt $p \in F$ gilt*

$$l(K_F + P) = l(K_F).$$

Beweis. Sei $d = \mathsf{grad}(F) \leq 2$. Dann besagt Lemma 4.8.22, dass $l(K_F) = 2g - 2 = 2\binom{d-1}{2} - 2$ streng negativ ist. Laut Lemmas 4.8.8 und 4.8.11 ist also $L(K_F) = \varnothing = L(K_F + P)$.

Man nähme nun an, dass $\mathsf{grad}(F) \geq 3$. Sei L eine Gerade durch p, welches keine Tangente von F am Punkt p ist. Da $\mathsf{grad}(\mathrm{div}(L)) = d \geq 3$ (Prop. 4.3.13) und der Grad von P, dem Divisor assoziiert zu p gleich 1 ist (Lemma 4.8.11) gilt, dass $\mathrm{div}(L) - P$ ein positiver Divisor ist, welches P nicht enthält. Hier benutzen wir noch die Tatsache, dass L keine Tangente von F am Punkt p ist, da sonst bei $\mathsf{grad}(F) = 3$ passieren kann, dass F und L sich am Punkt p dreimal schneiden. Dann wäre $\mathsf{grad}(\mathrm{div}(L) - P) = 0$, also nicht mehr streng positiv. Dies haben wir aber vermieden.

Man erinnere sich, dass man bei der Definition 4.8.20 vom kanonischem Divisor K_F, eine beliebige Gerade nehmen kann. Die Klasse ist dann laut Lemma 4.8.21 gleich. Wir nehmen hier also die Gerade L, welches wir eben konstruiert haben und betrachten den Repräsentanten $(d-3)\mathrm{div}(L)$ von K_F. Es ist klar, dass es ausreicht, $L(K_F + P) \simeq L(K_F)$ zu beweisen, denn wenn Vektorräume isomorph sind, sind ihre Dimensionen ja natürlich gleich. Bei Teil (i) von Lemma 4.8.9 gilt $L(K_F) \subseteq L(K_F + P)$. Es bleibt also noch zu zeigen, dass $L(K_F + P) \subseteq L(K_F)$.

Sei dazu $0 \neq \varphi = \frac{\overline{G}}{\overline{H}} \in L(K_F + P)$. Bei Definition von $L(K_F + P)$ gilt daher $\mathrm{div}(\varphi) + K_F + P \geq 0$. Bei Definition 4.8.20 von K_F gilt also $\mathrm{div}(\varphi) + (d-3)\mathrm{div}(L) + P \geq 0$, daher

$$\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) + (d-3)\mathrm{div}(L) + P \geq 0.$$

Laut Lemma **??** (ii) führt dies zu

$$\mathrm{div}\left(\overline{G}\right) - \mathrm{div}\left(\overline{H}\right) + (d-3)\mathrm{div}(L) + P \geq 0,$$

dann

$$\mathrm{div}(\overline{G}) + (d-2)\mathrm{div}(L) \geq \mathrm{div}(\overline{H}) + \mathrm{div}(L) - P$$

und schließlich

$$\mathrm{div}(\overline{G}L^{d-2}) \geq \mathrm{div}(\overline{H}) + \mathrm{div}(L) - P \geq \mathrm{div}(\overline{H}).$$

Laut Noethers Satz (Korollar 4.4.7) gibt es eine Kurve B, vom Grad $\mathsf{grad}(\overline{G}L^{d-2}) - \mathsf{grad}(\overline{H}) = d-2$ da bei Definition $\mathsf{grad}(\overline{G}) = \mathsf{grad}(\overline{H})$, so dass

$$\mathrm{div}(B) = \mathrm{div}(\overline{G}L^{d-2}) - \mathrm{div}(\overline{H}) \geq \mathrm{div}(L) - P. \tag{29}$$

Die letzte Gleichung gilt, da $\mathsf{grad}(\mathrm{div}(L) - P) \leq d-1$. (Es ist gleich $d-1$, wenn P nur einmal auf F liegt). Man erinnere sich, was $\mathrm{div}(B) \geq \mathrm{div}(L) - P$ bedeutet. Es heißt, dass an jedem Punkt $q \in F$, $\mathfrak{I}(q, B \cap F) \geq \mathfrak{I}(q, L \cap F) - P$. Spezifisch, wenn $q \neq p$ gilt

$$\mathfrak{I}(q, B \cap F) \geq \mathfrak{I}(q, L \cap F).$$

Laut Satz 2.4.7 ist dies äquivalent zu sagen, dass

$$\dim_K(\mathcal{O}_q/(F,B)) \geq \dim_K(\mathcal{O}_q/(F,L)),$$

für jeden $q \neq p$, was anders gesagt $(F,B) \subseteq (F,L)$ in $\mathcal{O}_q$ bedeutet. Spezifisch ist also $B \in (F,L)$, aufgefasst als Element bzw. Ideal von $\mathcal{O}_q$, also $(B,L) \subseteq (F,L) \subseteq \mathcal{O}_q$. Daher $\dim_K(\mathcal{O}_q/(B,L)) \geq \dim_K(\mathcal{O}_q/(F,L))$, was wieder vom Satz 2.4.7

$$\mathfrak{I}(q, B \cap L) \geq \mathfrak{I}(q, F \cap L)$$

impliziert. Man nehme nun die Summe von diesen $q \neq p$ in F auf. Wir erhalten

$$\sum_{q \neq p \in F} \mathfrak{I}(q, B \cap L) \geq \sum_{q \neq p \in F} \mathfrak{I}(q, F \cap L) = \mathsf{grad}(\mathrm{div}(L) - P) = d - 1.$$

Da der Grad von B gleich $d-2$ ist (sieh oben) und $\mathsf{grad}(L) = 1$, folgt vom Satz von Bezout 4.3.13, dass $\sum_{p \in F} \mathfrak{I}(p, B \cap L) = d - 2$ ist. Daher kann $\sum_{q \neq p \in F} \mathfrak{I}(q, B \cap L)$ nur dann größer gleich $d-1$ sein, wenn L und B einen gemeinsamen Teiler haben. Da L vom Grad 1 ist, muss also L ein Teiler von B sein. Dies wiederum bedeutet, dass $\mathrm{div}(B) \geq \mathrm{div}(L)$ ist. Wie in Formel (29) gezeigt ist $\mathrm{div}(B) = \mathrm{div}(\overline{G}L^{d-2}) - \mathrm{div}(\overline{H})$, was uns also nun

$$\mathrm{div}(\overline{G}L^{d-2}) - \mathrm{div}(\overline{H}) \geq \mathrm{div}(L)$$

gibt. Dies schließt nun unseren Beweis ab, da wir

$$\begin{aligned} \mathrm{div}(\overline{G}L^{d-2}) - \mathrm{div}(\overline{H}) &= \mathrm{div}(\overline{G}) + \mathrm{div}(L^{d-2}) - \mathrm{div}(\overline{H}) \\ &= \mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) + (d-2)\mathrm{div}(L) \end{aligned}$$

haben. Da die linke Seite $\geq \mathrm{div}(L)$ ist, haben wir also

$$\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) + (d-2)\mathrm{div}(L) \geq \mathrm{div}(L),$$

daher

$$\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) + (d-2)\mathrm{div}(L) - \mathrm{div}(L) \geq 0,$$

was uns letztendlich

$$\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) + (d-3)\mathrm{div}(L) \geq 0$$

gibt. Bei Definition 4.8.20 des kanonischen Divisors ergibt dies

$$\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) + K_F \geq 0.$$

Bei Definition von $L(D)$ sag dies, dass $\mathrm{div}\left(\frac{\overline{G}}{\overline{H}}\right) = \mathrm{div}(\varphi) \in L(K_F)$. □

Lemma 4.8.24. *Für jeden Divisor $D \in \mathrm{Div}(F)$ gilt*

$$l(D) - l(K_F - D) \geq \mathsf{grad}(D) + 1 - g.$$

Beweis. Wir werden dies durch eine "umgekehrte" Induktion auf D beweisen: Also, dass wenn die Aussage für $\mathsf{grad}(D) = i$ stimmt, es auch für $i-1$ stimmen muss. Daher ist unser Induktionsanfang wie folgt:

Sei $\mathsf{grad}(D) > 2g-2$. Dann hält die Aussage des Lemmas.
Laut Lemma 4.8.22 und Lemma 4.3.5 gilt $\mathsf{grad}(K_F - D) = \mathsf{grad}(K_F) - \mathsf{grad}(D) < 0$, was durch Lemma 4.8.8 $l(K_F - D) = 0$ impliziert. Dies ist nun Riemanns Satz 4.8.17.

Wenn die Aussage für D hält, hält es auch für $D - P$ für jeden $p \in F$.
Man nehme an, dass $l(D) - l(K_F - D) \geq \mathsf{grad}(D) + 1 - g$. Laut Teil (i) von Lemma 4.8.12 ist $l(D) = l(D-P+P) = l(D-P)$ oder $l(D) = l(D-P+P) = l(D-P)+1$. Daher, $l(D-P) = l(D)$ oder $l(D-P) = l(D)-1$, also $l(D-P) \geq l(D)-1$. Aus dem selben Lemma erhalten wir auch, dass $l(K_F - D + P) \geq l(K_F - D) - 1$. Wir fassen es zusammen zu

$$\begin{aligned} l(D-P) - l(K_F - D + P) &\geq l(D) - 1 - (l(K_F - D) + 1) \\ &\geq \mathsf{grad}(D) + 1 - g - 2 \\ &= \mathsf{grad}(D - P) - g \end{aligned}$$

wobei die letzte (zweite) Ungleichung die Induktionsannahme ist und die letzte Gleichung einfach nur die Definition vom Grad eines Divisors ist. Wir wollen aber $l(D-P) - l(K_F - D + P) \geq \mathsf{grad}(D-P) - g + 1$ beweisen. Dies wird direkt folgen, wenn wir zeigen, dass die Ungleichung $l(D-P) - l(K_F - D + P) = l(D) - 1 - (l(K_F - D) + 1)$ streng ist. Da aber $l(D-P) \geq l(D) - 1$ und $l(K_F - D + P) \geq l(K_F - D) - 1$ ist dies äquivalent zu sagen, dass $l(D-P) > l(D)-1$ oder $l(K_F - D + P) > l(K_F - D) - 1$ gilt. Wir machen es durch Widerspruch.

Sei also $l(D-P) = l(D) - 1$ und $l(K_F - D + P) = l(K_F - D) - 1$. Daher gilt also $L(D-P) \subsetneq L(D)$ und $L(K_F - D) \subsetneq L(K_F - D + P)$. In anderen Worten, dass es rationale Funktionen

$$\varphi \in L(D) \setminus L(D-P), \qquad \psi \in L(K_F - D + P) \setminus L(K_F - D)$$

gibt. Lass uns $\varphi \in L(D) \setminus L(D-P)$ genauer betrachten. Sei $\mathrm{div}(\varphi) = \sum_{q \in F} m_q q$ und $D = \sum_{q \in F} n_q q$. Dann bedeutet $\varphi \in L(D) \Leftrightarrow \mathrm{div}(\varphi) + D \geq 0$, dass $\sum_{q \in F} (m_q + n_q) q \geq 0$. Auf der anderen Seite, $\varphi \notin L(D-P) \Leftrightarrow \mathrm{div}(\varphi) + D - P \not\geq 0$ genau dann, wenn es einen $q \in F$ gibt, mit $[\sum_{q \in F} (m_q + n_q) q] - p < 0$. Da für alle $q \neq p$, dies zum Widerspruch führen wird, ist $\varphi \notin L(D-P)$ genau dann, wenn $m_p + n_p - 1 < 0$. Aber $m_p + n_p \geq 0$ gilt immer noch. Daher muss $m_p + n_p = 0$ sein. Wir fassen es zusammen als

$$\varphi \in L(D) \setminus L(D-P) \;\Leftrightarrow\; \begin{cases} m_q + n_q \geq 0 & \text{für alle } q \in F \\ m_p + n_p = 0 & \text{für unseren spezifischen } p. \end{cases}$$

Genau so erhalten wir

$$\psi \in L(K_F - D + P) \setminus L(K_F - D) \;\Leftrightarrow\; \begin{cases} m'_q + k_q - n_q \geq 0 & \text{für alle } q \in F \\ m'_p + k_p - n_p + 1 = 0 & \text{für unseren spezifischen } p, \end{cases}$$

wobei $\operatorname{div}(\psi) = \sum_{q \in F} m'_q q$ und $K_F = \sum_{q \in F} k_q q$.

Wir betrachten nun den Produkt $\varphi\psi$. Laut Lemma **??**, Teil (ii), gilt

$$\operatorname{div}(\varphi\psi) = \operatorname{div}(\varphi) + \operatorname{div}(\psi) = \sum_{q \in F} m_q q + \sum_{q \in F} m'_q q.$$

Von unseren Formeln in den Klammern haben wir

$$\begin{cases} m_q + m'_q + k_q & \geq (-n_q) + (-k_q + n_q) + k_q = 0 & \text{für alle } q \in F \\ m_p + m'_p + k_p + 1 & = (-n_q) + (-k_p + n_p - q) + k_q + 1 = 0 & \text{für unseren spezifischen } p. \end{cases}$$

Dies ist wiederum äquivalent zu sagen, dass $\varphi\psi \in L(K_F + P) \setminus L(K_F)$, was laut Proposition 4.8.23 ein Widerspruch ist. Damit wäre unser Induktionsschritt bewiesen.

Da jedes Divisor D nur endlich viele Koeffizienten ungleich Null hat, wird man jedes Divisor D als die Differenz eines Divisors D', mit $\mathsf{grad}(D') > 2g - 2$ und endlich vielen Punkten p_i darstellen können. Dies schließt unseren Lemma ab. □

Satz 4.8.25 (Der Satz von Riemann-Roch)**.** *Für jeden Divisor D gilt*

$$l(D) - l(K_F - D) = \mathsf{grad}(D) + 1 - g.$$

Beweis. Wir müssen nur $l(D) - l(K_F - D) \leq \mathsf{grad}(D) + 1 - g$ beweisen, denn die andere Seite ist Lemma 4.8.24 oben. Doch das selbe Lemma gibt uns auch die andere Seite, wenn wir es "geschickt" anwenden: Da es für jeden Divisor D gilt, gilt es auch für $K_F - D$. Daher

$$l(K_F - D) - l(K_F - (K_F - D)) \geq \mathsf{grad}(K_F - D) + 1 - g,$$

was uns

$$l(K_F - D) - l(D) \geq \mathsf{grad}(K_F - D) + 1 - g$$

gibt. Lemmas 4.3.5 und 4.8.22 geben uns nun $\mathsf{grad}(K_F - D) = \mathsf{grad}(K_F) - \mathsf{grad}(D) = 2g - 2 - \mathsf{grad}(D)$, daher

$$l(K_F - D) - l(D) \geq 2g - 2 - \mathsf{grad}(D) + 1 - g.$$

Mit -1 multipliziert und etwas vereinfacht ist dies

$$l(D) - l(K - D) \geq \mathsf{grad}(D) + 1 - g,$$

genau wie gewollt. Dies schließt den Beweis ab. □

Korollar 4.8.26. *Sei $D \in \mathrm{Div}(F)$ ein Divisor mit $\mathsf{grad}(D) > 2g-2$. Es gilt*

$$l(D) = \mathsf{grad}(D) + 1 - g.$$

Beweis. Laut Lemmas 4.3.5 und 4.8.22 gilt

$$\mathsf{grad}(K_F - D) = \mathsf{grad}(K_F) - \mathsf{grad}(D) < 2g - 2 - 2g + 2 = 0.$$

Aus Lemma 4.8.8 wissen wir, dass $l(K_F - D) = 0$. Der Satz von Riemann-Roch 4.8.25 gibt nun das gewünschte Resultat. □

In anderen Worten, der Satz von Riemann 4.8.17 wird auch ohne einen zusätzlichen Divisor streng, für Divisore mit einem genügend großem Grad. In solchen Fällen können wir also $l(D)$ alleine durch $\mathsf{grad}(D)$ berechnen. Öfters wird Korollar 4.8.26 als Satz von Riemann-Roch bezeichnet, vor allem weil diese schwache Version öfters ausreichend ist.

Korollar 4.8.27. *Es gilt $l(K_F) = g$.*

Beweis. Man setze im Satz von Riemann-Roch 4.8.25 $D = 0$ ein. Dies gibt $l(0) - l(K_F) = \mathsf{grad}(0) + 1 - g$. Da $L(0) = 0$ ergibt es das gewünschte Resultat. □

5 Appendix

5.1 Das Lemma von Gauß

Wir wollen folgendes Lemma beweisen:

Satz 5.1.1 (Gaußsches Lemma)**.** *Zwei Polynome $f, g \in K[x, y]$ haben genau dann einen gemeinsamen Teiler, wenn sie einen gemeinsamen Teiler in $K(x)[y]$ haben.*

Hierzu führen wir zuerst einige Notationen und Begriffe ein:

5.1.1 Primitive Polynome

Sei $R = K[y]$ und $\mathsf{Q} = \mathsf{Q}(K[y]) = K(y)$ dessen Quotientenkörper.

Definition 5.1.2. *Wir sagen, dass die Koeffizienten $\{a_i\}_{i=0}^n$ eines Polynoms*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$$

relativ prim *sind, wenn das Ideal mit ihnen erzeugt ganz R ergibt. In anderen Worten, wenn*

$$(a_0, a_1, \ldots, a_n) = (1) = R.$$

Bemerkung 5.1.3. Diese Definition ist mit teilerfremd eng verbunden. Es ist aber, so wie wir es definiert haben, nicht äquivalent. Sogar schon bei $R = \mathbb{Z}$ ist das Polynom $f(x) = 7x + 2$ relativ prim, da $(7, 2) = 1$ aber $f(x) = 7$ ist es nicht, da $(7) \neq (1)$. Genauso auch bei $R = K[y]$. Hier ist $f(x) = 7yx + 2(y - 1)$ relativ prim, da

$$(7y, 2(y - 1)) = (1),$$

denn aus $7y \in I$ folgt $y \in I$ (da $7 \in K^*$) und aus $2(y - 1) \in I$ folgt $y - 1 \in I$, woraus wir $1 \in I$ schlussfolgern können.

Wenn als solches f zwei oder mehr Koeffizienten hat ist dieser Begriff relativ vertraut. Dies ist aber nur über $\mathbb{Z}$ bzw. $K[y]$ der Fall. Wären wir über $R = \mathbb{Z}[y]$, bräuchten wir mindestens 3 Koeffizienten um dies mit teilerfremd in Verbindung zu bringen. Dies hat natürlich was mit der Krull Dimension zu tun (maximale Länge die eine strikte Inklusion von Primidealen haben kann). Für uns ist dies aber nicht weiter relevant.

Definition 5.1.4. *Ein Polynom $f \in R[x]$ heißt* primitiv *wenn die Koeffizienten von f teilerfremd sind.*

Lemma 5.1.5. *Sein $\alpha(x), \beta(x) \in R[x]$ primitive Polynome, so dass $\alpha(x) = r\beta(x)$ mit $r \in \mathsf{Q}^*$. Dann ist $r \in R^* = K^*$.*

Beweis. Sein $\{a_i\}_{i=0}^n$ die Koeffizienten von $\alpha(x)$, $\{b_j\}_{i=0}^m$ die Koeffizienten von $\beta(x)$ und $r = \frac{c}{d}$, $c \in R$, $d \in R \setminus 0$. Von der Definition der Primitivität folgt, dass

$$(1) = (a_0, a_1, \ldots, a_n) = (\frac{c}{d}b_0, \frac{c}{d}b_1, \ldots, \frac{c}{d}b_m),$$

woraus

$$(d) = (d)(1) = (d)(a_0, \ldots, a_n) = (c)(b_0, \ldots, b_m) = (c)(1) = (c)$$

folgt, da β auch primitiv ist. Aber $(d) = (c)$ impliziert, dass sich d und c mit einer Einheit unterscheiden. Die Einheiten von $R = K[y]$ sind natürlich die Einheiten von K und wir sind fertig. □

Proposition 5.1.6. *Für ein Polynom $0 \neq f \in \mathsf{Q}[x]$ gibt es ein primitives $f_p \in R[x]$, welches man durch das Multiplizieren mit einem Element $0 \neq c \in \mathsf{Q}$ erhält. Das primitive Polynom is eindeutig bis auf eine Einheit $u \in R^* = K^*$.*

Beweis. Der Beweis wird durch Konstruktion gegeben: Sei

$$f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$$

und $b = b_0 \times \cdots \times b_n$. Dann ist

$$bf = c_0 + c_1x + \cdots + c_nx^n \in R[x].$$

Sei $I = (c_1, \ldots, c_n) \subseteq R$ das Ideal erzeugt mit den Koeffizienten. Da $R[x]$ ein Hauptidealbereich ist gibt es ein $c \in$ mit $I = (c)$. Daher, $c \mid c_i$ für alle $1 \leq i \leq n$. Wir folgern

$$f_p := \frac{b}{c}f \in R[x],$$

was nun primitiv ist. Eindeutigkeit folgt von Lemma 5.1.5, denn sein $u, v \in \mathsf{Q}$, so dass uf und vf beide primitiv sind. Da $uf = \frac{u}{v}vf$ muss $\frac{u}{v} \in R^*$. □

Sei $\mathfrak{m} \subseteq R$ ein Maximalideal. Es gilt $(R/\mathfrak{m})[x] \simeq R[x]/\mathfrak{m}$. Somit kann man Polynome über R zu Polynome über $R/\mathfrak{m}$ reduzieren.

Lemma 5.1.7. *Ein Polynom $f(x) \in R[x]$ ist primitiv genau dann wenn $\overline{f} \neq 0 \in R[x]/\mathfrak{m}$ für jeden Maximalideal $\mathfrak{m} \in R$.*

Beweis. Sein $f = a_0 + a_1x + \cdots + a_nx^n$ und $\mathfrak{m}$ ein Maximalideal. Es gilt

$$\overline{f}(x) = 0 \in R[x]/\mathfrak{m} \iff a_i \in \mathfrak{m}, \forall\ 1 \leq i \leq n \iff (a_0, a_1, \ldots, a_n) \subseteq \mathfrak{m} \neq (1).$$

□

Definition 5.1.8. *Eine Menge M, zusammen mit einem ausgewählten Element $1 \in M$ und einer binären Verknüpfung $\cdot : M \times M \to M$ wird* Monoid *genannt, wenn für alle $a, b \in M$ gilt*

i) $a1 = 1a = a$,

ii) $(ab)c = a(bc)$.

Hier schreiben wir natürlich ab für $\cdot(a,b)$. *Das Monoid wird kommutativ genannt, wenn zusätzlich* $ab = ba$ *gilt.*

Lemma 5.1.9. *Die primitiven Polynome über* R *formen ein kommutatives Monoid unter der Multiplikation.*

Beweis. Sein $f(x), g(x) \in R[x]$, so dass $f(x)g(x)$ nicht primitiv ist. Es gibt somit ein Maximalideal $\mathfrak{m}$ mit $c_i \in \mathfrak{m}$ für jeden Koeffizienten c_i von $f(x)g(x)$. Es folgt $f(x)g(x) = 0 \in R[x]/\mathfrak{m}$. Da $R/\mathfrak{m}$ ein Körper und daher ein Integritätsbereich ist, gilt $f(x) = 0$ oder $g(x) = 0$ in $R[x]/\mathfrak{m}$. Es folgt, dass alle Koeffizienten von f oder g in $\mathfrak{m}$ liegen und somit ist f oder g nicht primitiv.

Die Einheit ist natürlich $1 \in R[x]$. Kommutativität ist klar und folgt aus der Kommutativität von $R[x]$. □

Satz 5.1.10 (Das Lemma von Gauß)**.** *Es sein* $f(x), g(x), h(x) \in \mathbb{Q}[x]$ *mit*

$$f(x) = g(x)h(x).$$

Dann gilt

$$f_p(x) = ug_p(x)h_p(x)$$

mit $u \in R^* = K^*$ *eine Einheit.*

Beweis. Sein $a, b, c \in \mathbb{Q}$, so dass $f_p(x) = af(x)$, $g_p(x) = bg(x)$ und $h_p(x) = ch(x)$.

$$\Rightarrow f(x) = \frac{1}{a}f_p(x), g(x) = \frac{1}{b}g_p(x) \quad \text{und} \quad h(x) = \frac{1}{c}h_p(x).$$

$$\Rightarrow \frac{1}{a}f_p(x) = \frac{1}{b}g_p(x)\frac{1}{c}h_p(x)$$

$$\Rightarrow f_p(x) = \frac{a}{bc}g_p(x)h_p(x).$$

Da sowohl $\alpha(x) := f_p(x)$ (Lemma 5.1.9 (Lemma direkt davor, LaTeX macht gerade nicht mit..)) wie auch $\beta(x) := g_p(x)h_p(x)$ primitiv sind, folgt von Lemma 5.1.5, dass $\frac{a}{bc} \in R^*$. □

Korollar 5.1.11. *Genau dann ist* $f(x) \in R[x]$ *irreduzibel über* R *wenn es irreduzibel über* $\mathbb{Q}$ *ist.*

Index

$K(\mathrm{V})$, 56

Affine Koordinatentransformation, 70
Affiner Raum, 5
Algebraische
    Menge, 9
    Varietät, 9
Algebraisches Element, 26
Auswertung eines projektiven Punktes, 117

Bewertung, 87

Dehomogenisierung, 119
    Ideal, 121
    Varietät, 122
Diskreter Bewertungsring, 87
Divisor, 139
    Haupt, 142
    Linaer äquivalent, 149
    Positiv, 139
Divisors
    Grad, 139

Element
    Form vom Grad d, 115
Elliptische Kruve
    Pre-Verknüpfung, 153

Funktionenkörper, 117

Ganz
    Element, 26
    Erweiterung, 26
    Ring, 26
Genus, 162
Gerade, 63

Halm, 55
Hauptidealbereich, 26
Homogen
    Ideal, 111
Homogene Koordinaten, 106
Homogenisierung, 119
    Ideal, 121
    Varietät, 121

Ideal
    Relativ maximal, 73
    Radikal, 18
Integritätsbereich, 5
Irreduzibel (topologisch), 33
Irreduzibles Element, 27
    Äquivalenz, 27
Isomorphismsus von Varietäten, 43

Kettenkomplex, 79
Komponente, 63
    Einfache Komponente, 63
    Multiple Komponente, 63
    Multiplizität, 63
    Vielfache Komponente, 63
    Vielfachheit, 63
Konus, 113
Koordinatenring, 36
    Homogen, 115
Koordinatentransformation
    Projektiv, 118
Kurve
    Halm, 56
Kurve (Affine planare), 61
    Grad, 63
    Multiplizität am Punkt, 65
    Regulär, 64
    Singulär, 64

Lokaler Ring, 52
Lokalisierung, 21
Lokalisierung an einem Primideal, 52

Maximales Element, 15
Minimalform, 65
Multiplikative Teilmenge, 21

Multiplizität, 65
    Projektiver Punkt, 128

Noethersche Eigenschaft, 144
Noetherscher Ring, 15
Nullstelle, 7
    Projektive, 108

Parallelverschiebung
    Affin, 65
Picardgruppe, 149
Polynom
    Form, 64
    Homogen, 64
Polynomfunktion, 35
Primitiv, 169
Projektiv äquivalent, 132
Projektive algebraische Menge, 110
Projektive Ebene, 104
Projektive Gerade, 104
Projektive Varietät, 110
Projektiver Abschluss, 125
Projektiver Raum, 104
Punkt
    Glatt, 64
    Nichtsingulär, 64
    Regulär, 64
    Singulr
      Porjektiv, 132
    Singulär, 64
      Normal bzw. herkömmlich, 66

Quotientenkörper, 25
    Homogen, 116

Rationale Abbildung, 48
Rationale Abbildung, 47
Rationale Funktion, 46, 117
    Definiert auf $p \in \mathbb{P}^n$, 117
Relative Primheit, 169

Schnitt
    Divisor, 140
    Eigentlich, 91
    Transversal, 91
    Zahl, 91
      Projektiv, 131
Schnittzahl
    Koordinatenring, 101
Sequenz
    Exakt, 79
Stetige Abbildung, 39

Tangente
    Projektiv, 132
    Regulärer Punkt, 64
Tangenten
    Allgemeiner Punkt, 66
Translation
    Affin, 65

Varietät
    Unter-, 38
Verschwindungsideal, 11

Zariski-Topologie, 11