Algebraische Geometrie

Vorlesung
Universität Hamburg

bei

Dr. Helge Ruddat

Mitschrift getext von André Beuckelmann

SoSe 2019

Inhaltsverzeichnis

0 Literatur

1. Skript zur Vorlesung "Kommutative Algebra und Einführung in die algebraische Geometrie" von 2017 von Prof. Dr. Annette Huber-Klawitter `http://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss17/kommalg/kommalg.pdf`.

2. “Undergraduate Algebraic Geometry” von Miles Reid
3. “Undergraduate Commutative Algebra” von Miles Reid

1 Einführung

Definition 1.1. Sei k algebraisch abgeschlossener Körper. Der *affine Raum über k* ist

$$\mathbb{A}_k^n := k^n$$

Elemente von $\mathbb{A}^n$ heißen *Punkte*. Für $P = (a_1, ..., a_n) \in \mathbb{A}^n$ heißen die a_i die *Koordinaten* von P. Es sei

$$\mathcal{O}(\mathbb{A}^n) := k[\mathbb{A}^n] := k[X_1, ..., X_n]$$

der Ring der *Funktionen* mit $f \in \mathcal{O}(\mathbb{A}^n)$ interpretiert als $\mathbb{A}^n \to k, (a_1, ..., a_n) \mapsto (f(a_1, ..., a_n))$. Für $S \subseteq k[X_1, ..., X_n]$ sei die *von S erzeugte algebraische Menge*

$$V(S) := \{(a_1, ..., a_n) \in k^n \mid f(a_1, ..., a_n) = 0 \,\forall f \in S\}$$

Für $S = \{f\}$ nennen wir $V(S) =: V(f)$ eine *Hyperfläche.*

Lemma 1.2. *Sei $S \subseteq k[X]$. Dann ist $V(S)$ entweder gleich $\mathbb{A}^1$ oder endlich.*

Beweis.

Fall 1: Es existiert $f \in S$ mit $f \neq 0$. Dann ist

$$V(S) \subseteq V(f)$$

endlich, da f nur endlich viele Nullstellen hat.

Fall 2: Es ist $S = \emptyset$ oder $S = \{0\}$. In beiden Fällen gilt $V(S) = \mathbb{A}^1$

□

Bemerkung 1.3. Verschiedene Gleichungssysteme können die gleiche Verschwindungsmenge haben.

Definition 1.4. Für $k = \overline{k}$, $S \subseteq k[X_1, ..., X_n]$, $V = V(S)$ sei

$$\mathcal{O}(V) := k[V] := \left\{ f : V \to k \;\middle|\; \begin{array}{r} \exists F \in k[X_1, ..., X_n] : f(x_1, ..., x_n) = F(x_1, ..., x_n) \\ \forall (x_1, ..., x_n) \in V \end{array} \right\}$$

der *affine Koordinatenring von V*. Elemente von $k[V]$ heißen *algebraische Funktionen auf V*.

Beispiel 1.5. Es sei $g \in k[X]$ nicht konstant, $V = V(g) = \{P_1, ..., P_d\}$. Dann ist

$$\begin{aligned} k[V] &\to k^d \\ f &\mapsto (f(P_1), ..., f(P_d)) \end{aligned}$$

ein Isomorphismus von Ringen: Die Abbildung ist nach Definition injektiv und für $(a_1, ..., a_d) \in k^d$ sei

$$F(X) = \sum_{i=1}^{d} (X - P_i + a_i) \prod_{j \neq i} \frac{X - P_j}{P_i - P_j}$$

dann ist $F(P_i) = a_i$ und somit ist F ein Urbild von $(a_1, ..., a_n)$

1.1 Grundbegriffe der algebraischen Geometrie

Es sei $k = \overline{k}$, *Ringe* bezeichne kommutative Ringe mit 1 und wir fordern, dass Ringhomomorphismen die 1 erhalten.

Bemerkung 1.6. Wir erlauben $0 = 1$. In diesem Fall ist $a = 0 \, \forall a \in R$, da $a = 1 \cdot a = 0 \cdot a = 0$ und somit $R = \{0\}$. Wir brauchen diesen Ring als Koordinatenring von $\emptyset$:

$$\mathcal{O}(\emptyset) = 0, V(1) = \emptyset$$

Definition 1.7. Für einen Ring A, heißt eine Untergruppe $I \subseteq A$ ein *Ideal*, geschrieben $I \lhd A$, falls

$$\forall x \in I, a \in A: \; ax \in I$$

Sei $V \subseteq \mathbb{A}^n$ algebraische Menge. Dann heißt

$$I(V) \coloneqq \{f \in k[X_1, ..., X_n] \mid f(p) = 0 \, \forall P \in V\}$$

das *Verschwindungsideal von V*.

Bemerkung 1.8. Das Verschwindungsideal ist tatsächlich ein Ideal, denn

(i) Falls $V = V(S), S \subseteq k[X_1, ..., X_n]$, dann $S \subseteq I(V)$.

(ii) Für $f, g \in I(V)$ ist $f + g \in I(V)$, denn

$$(f+g)(p) = f(p) + g(p) = 0$$

(iii) Für $f \in I, (V), g \in k[X_1, ..., X_n]$ ist

$$(gf)(p) = g(p) \cdot f(p) = g(p) \cdot 0 = 0$$

und daher $g \cdot f \in I(V)$

Somit ist $I(V)$ ein Ideal.

Lemma 1.9. *Sei $\varphi : A \to B$ Ringhomomorphismus. Dann ist $\ker(\varphi)$ Ideal von A.*

Beweis. Sei $a \in A$, $x \in \ker(\varphi)$. Dann ist

$$\varphi(a \cdot x) = \varphi(a) \cdot \varphi(x) = 0$$

und damit $a \cdot x \in \ker(\varphi)$ □

Bemerkung 1.10. Sei $\rho : \mathcal{O}(\mathbb{A}^n) \to \mathcal{O}(V)$ die Restriktion. Dann gilt

$$I(V) = \ker(\rho)$$

Satz 1.11. *Sei A ein Ring, $I \lhd A$ Ideal. Dann ist die Menge der Nebenklassen*

$$A/I \coloneqq \{a + I \mid a \in A\}$$

mit Addition und Multiplikation

$$(a+I)+(b+I) \coloneqq (a+b)+I$$
$$(a+I)\cdot(b+I) \coloneqq a\cdot b+I$$

ein Ring und die Projektion

$$A \to A/I$$
$$a \mapsto a+I$$

ist Ringhomomorphismus

Beweis. Wie bei Vektorräumen oder Gruppen ist die Wohldefiniertheit von $+,\cdot$ zu zeigen. $+$ geht wie bei Gruppen. Zur Wohldefiniertheit von $\cdot$:
Behauptung. Sei $a+I=a'+I$, dann ist

$$ab+I=a'b+I\,\forall b\in A$$

Beweis. Es ist $a+I=a'+I \Leftrightarrow a-a'\in I$ Da I Ideal ist, gilt

$$\begin{aligned} & b\cdot(a-a')\in I\,\forall b \\ \Leftrightarrow & ba-ba'\in I \\ \Leftrightarrow & ba+I=ba'+I \end{aligned}$$

□

Korollar 1.12. *Sei $V\subseteq\mathbb{A}^n$ algebraische Menge. Dann gilt*

$$\mathcal{O}(V)=\mathcal{O}(\mathbb{A}^n)/I(V)$$

Beispiel 1.13. Sei $f=X^2+Y^2-1$ und $k=\mathbb{C}$. Dann ist

$$\mathcal{O}(V(f))=k[X,Y]/(f\cdot k[X,Y])$$

Bemerkung 1.14. Das Korollar gilt auch für $V=\emptyset$. Da $I(V)=\mathcal{O}(\mathbb{A}^n)$ und somit

$$\mathcal{O}(\emptyset)=\mathcal{O}(\mathbb{A}^n)/I(V)=0$$

Satz 1.15 (Homomorphiesatz)**.** *Sei $\varphi:A\to B$ Ringhomomorphismus mit $I=\ker(\varphi)$. Dann ist*

$$\overline{\varphi}:A/I\to\operatorname{im}(\varphi)$$

ein Ringisomorphismus.

Beweis. Wie bei Vektorräumen oder Gruppen □

Definition 1.16. Sei A Ring, $S\subseteq A$ Teilmenge. Dann sei

$$\langle S\rangle=\bigcap_{S\subseteq I\lhd A} I$$

Das *von S erzeugte Ideal.*

Korollar 1.17. *Sei* $S \subseteq k[X_1, ..., X_n], V = V(S)$. *Dann ist*

$$\langle S \rangle \subseteq I(V)$$

Beweis. $I(V)$ ist Ideal, das S enthält. □

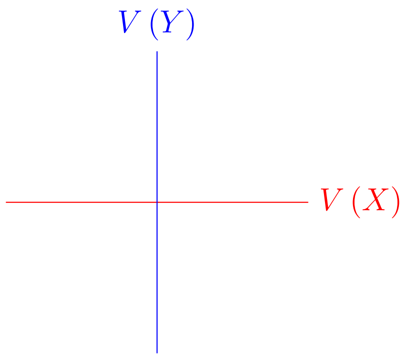
Beispiel 1.18. Es sei $S = \{X \cdot Y\} \subseteq k[X, Y]$. Dann ist

$$\langle XY \rangle = XY \cdot k[X, Y]$$

und

$$\begin{aligned} V(XY) &= \left\{(x, y) \in k^2 \mid xy = 0\right\} \\ &= \underbrace{\left\{(0, y) \in k^2 \mid y \in k\right\}}_{=V(X)} \cup \underbrace{\left\{(x, 0) \in k^2 \mid x \in k\right\}}_{=V(Y)} \end{aligned}$$

Vereinigung der Koordinatenachsen.



Für $I := I(V) = I(V(XY))$:
Es sei $f = \sum_{i,j \geq 0} a_{ij} X^i Y^j \in I$. Dann ist

$$\begin{aligned} f(0, y) &= \sum_{i,j \geq 0} a_{ij} 0^i y^j \\ &= \sum_{j \geq 0} a_{0j} y^j = 0 \; \forall y \in k \end{aligned}$$

Und damit $a_{0j} = 0 \; \forall j \geq 0$, da k algebraisch abgeschlossen und damit unendlich ist. Analog ist $a_{i0} = 0 \; \forall i \geq 0$, da $f(x, 0) = 0 \; \forall x \in k$. Und damit $f = XY \cdot g$ mit $g = \sum_{i,j \geq 1} a_{ij} X^{i-1} Y^{j-1}$. Also $I = \langle XY \rangle$

Beispiel 1.19. Gilt immer $\langle S \rangle = I(V)$? Sei $S = \{X^2\} \subseteq k[X]$. Dann ist

$$\left\langle X^2 \right\rangle = X^2 \cdot k[X], \; V\left(\left\langle X^2 \right\rangle\right) =: V = \{0\} \subseteq \mathbb{A}^1$$

Und damit

$$I := I(V) = \langle x \rangle = X \cdot k[X]$$

Die Gleichungen $X^2 = 0$ und $X = 0$ definieren die gleiche Verschwindungsmenge.

Definition 1.20. Sei $I \lhd A$ Ideal. Dann heißt

$$\sqrt{I} := \{x \in A \mid \exists n > 0 : \; x^n \in I\}$$

das *Radikalideal von* I. Ein Ideal I heißt *reduziert*, wenn $I = \sqrt{I}$.

Lemma 1.21. *$\sqrt{I}$ ist ein Ideal.*

Beweis. Sei $x, y \in \sqrt{I}$. Dann existieren $n, m > 0$ mit $x^n, y^m \in I$. O.B.d.A sei $n \geq m$. Dann ist

$$(xf)^n = \underbrace{x^n}_{\in I} \cdot f^n \in I \implies xf \in \sqrt{I} \, \forall f \in A$$

Außerdem ist

$$(x+y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}$$

Für $i \geq n$ ist $x^i \in I$ und für $i < n$ ist $y^{n+m-i} \in I$ und damit ist diese Summe in I. Also ist $x + y \in \sqrt{I}$. □

Korollar 1.22. *Sei $S \subseteq k[X_1, ..., X_n], V = V(S)$. Dann ist*

$$\sqrt{\langle S \rangle} \subseteq I(V)$$

Beweis. Sei $f \in \sqrt{\langle S \rangle}, f^n \in \langle S \rangle \subseteq I(V)$. Dann ist

$$(f(p))^n = 0 \, \forall P \in V$$

und, da k Körper ist, $f(P) = 0 \, \forall P \in V$ und somit $f \in I(V)$. □

Bemerkung 1.23. Es gilt sogar $\sqrt{\langle S \rangle} = I(V)$ (Teil des Hilbertschen Nullstellensatzes). Wir haben bisher $k = \overline{k}$ nicht verwendet. Dies ist für diese Aussage aber notwendig, denn für $X^2 + 1 \in \mathbb{R}[X]$ ist $V(X^2+1) = \emptyset$ und $I(V) = \mathbb{R}[X]$ aber $\sqrt{\langle X^2 + 1 \rangle} = \langle X^2 + 1 \rangle$

2 Zariski-Topologie

Definition 2.1. Sei $V \subseteq \mathbb{A}$ algebraische Menge. $W \subseteq V$ heißt *abgeschlossen*, wenn W selbst algebraische Menge ist. Eine Teilmenge $U \subseteq V$ heißt *offen*, wenn $V \setminus U$ abgeschlossen ist.

Satz 2.2. *Dies definiert eine Topologie auf V, die* Zariski-Topologie

Beweis. Zu zeigen:

(i) $\emptyset, V$ sind offen ($\Leftrightarrow \emptyset, V$ abgeschlossen).

(ii) Der Schnitt zweier offener Mengen ist wieder offen. ($\Leftrightarrow$ Die Vereinigung zweier abgeschlossener Mengen ist abgeschlossen)

(iii) Die Vereinigung von beliebig vielen offenen Mengen ist offen ($\Leftrightarrow$ Der Schnitt von beliebig vielen abgeschlossenen Mengen ist abgeschlossen)

Beweis:

(i) $V = V(\langle 0\rangle), \emptyset = V(1)$

(ii) Sei $W_1 = V(S_1), W_2 = V(S_2)$.

Behauptung. $W_1 \cup W_2 = V(S_1S_2),\ S_1S_2 := \{f_1f_2 \mid f_1 \in S_1, f_2 \in S_2\}$

Beweis. Sei $P \in W_1$,also

$$\begin{aligned} & f(P) = 0\ \forall f \in S_1 \\ \implies & (f \cdot g)(P) = \underbrace{f(P)}_{=0} \cdot g(P) = 0\ \forall f \in S_1, g \in S_2 \\ \implies & W_1 \subseteq V(S_1S_2) \end{aligned}$$

Analog: $W_2 \subseteq V(S_1S_2)$ und somit $W_1 \cup W_2 \subseteq V(S_1S_2)$.
Umgekehrt sei $P \in V(S_1S_2)$, also $(fg)(P) = 0\ \forall f \in S_1, g \in S_2$. Entweder $P \in W_1$ oder $\exists f_0 \in S_1 :\ f_0(P) \neq 0$. Angenommen $f_0 \neq 0$. Dann

$$\begin{aligned} & (f_0g)(P) = 0 && \forall g \in S_2 \\ \implies & \underbrace{f_0(P)}_{\neq 0} g(P) = 0 && \forall g \in S_2 \\ \implies & g(P) = 0 && \forall g \in S_2 \\ \implies & P \in W_2 \\ \implies & P \in W_1 \cup W_2 \end{aligned}$$

und somit gilt $V(S_1S_2) \subseteq W_1 \cup W_2$

(iii) Sei $W_\alpha = V(S_\alpha),\ \alpha \in I$. Dann

$$\bigcap_{\alpha \in I} W_\alpha = V\left(\bigcup_\alpha S_\alpha\right)$$

□

Beispiel 2.3. Eine Teilmenge von $\mathbb{A}^1 = k$ ist

abgeschlossen $\Leftrightarrow$ ganz $\mathbb{A}^1$ oder endlich

Die Topologie ist ganz anders als bei metrischen Räumen.

(a) Je zwei nicht-leere offene Mengen haben nicht-leeren Schnitt

(b) Jede unendliche Menge ist dicht.

Definition 2.4. Eine algebraische Menge $V \subseteq \mathbb{A}^n$ zusammen mit der Zariski-Topologie heißt *affine Varietät*. Eine offene Teilmenge von V heißt *quasi-affine Varietät* (mit induzierter Topologie von V).

Beispiel 2.5. $\mathbb{A}^2 \setminus \underbrace{\{(0,0)\}}_{V(XY)}$ ist offen in $\mathbb{A}^2$, also quasi-affine Varietät, ist aber nicht affin.

Bemerkung 2.6. In der Literatur wird oft zusätzlich gefordert, dass V irreduzibel ist.

3 Noethersche Ringe und Moduln

Definition 3.1. Sei A ein Ring, $I \triangleleft A$ heißt *endlich erzeugt*, wenn $I = \langle S \rangle$ für ein $S \subseteq A$ endlich. Ein Ring heißt *noethersch*, wenn jedes Ideal endlich erzeugt ist.

Beispiel 3.2. (i) Sei K ein Körper. Dann hat $A = K$ nur zwei Ideale: $\langle 0 \rangle, K$. Denn, falls $x \in I$ mit $x \neq 0$, dann ist $1 = x^{-1} \cdot x \in I$ und damit $I = K$. Beide sind endlich erzeugt und damit ist A noethersch.

(ii) Sei $A = \mathbb{Z}$. Alle Ideale von A haben die Form $\langle n \rangle$ für ein $n \in \mathbb{Z}$ (gilt bereits für Untergruppen). Solche Ideale heißen *Hauptideale* (von einem Element erzeugt). Ringe, bei denen jedes Ideal ein Hauptideal ist, heißen *Hauptidealringe*. Diese sind immer noethersch.

(iii) Sei $A = K[X]$ mit K Körper. Auch dieser Ring ist ein Hauptidealring. Also ist A noethersch.

Lemma 3.3. *Sei $f : A \twoheadrightarrow B$ surjektiver Ringhomomorphismus und A noethersch, dann ist auch B noethersch.*

Beweis. Sei $I \triangleleft B$ ein Ideal. Dann ist auch $f^{-1}(I) \triangleleft A$ ein Ideal. Weil A noethersch ist, gibt es eine endliche Menge $S \subseteq A$ mit $\langle S \rangle = f^{-1}(I)$. Nun ist I erzeugt von $f(S)$, weil f surjektiv ist: Ist $b \in I$, dann existiert ein $a \in f^{-1}(b)$ (surjektivität) und damit

$$a = \sum_{i=1}^{k} a_i f_i, \; a_i \in A, f_i \in S$$

Dann ist

$$b = f(a) = f\left(\sum_{i=1}^{k} a_i f_i\right) = \sum_{i=1}^{k} f(a_i) \underbrace{f(f_i)}_{f(S)}$$

und damit ist $b \in \langle f(S) \rangle$. $\square$

3.1 Moduln

Nächstest Ziel: Wir wollen zeigen, dass für jede algebraische Menge V, der Koordinatenring $\mathcal{O}(V)$ noethersch ist. Dazu brauchen wir Operationen und weitere Kenntnisse für noethersche Ringe. Es hilft, die Sache allgemeiner aufzuziehen und gleich noethersche Moduln zu betrachten.

Definition 3.4. Sei A ein Ring. Ein *A-Modul M* ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Skalarmultiplikation

$$\begin{aligned} A \times M &\to M \\ (a, x) &\mapsto a \cdot x \end{aligned}$$

sodass für alle $a, b \in A, x, y \in M$ gilt:

(i) $a(x + y) = ax + ay$

(ii) $(a + b)x = ax + bx$

(iii) $a \cdot (b \cdot x) = (a \cdot b) \cdot x$

(iv) $1 \cdot x = x$

Seien M, N A-Moduln. Eine Abbildung $f : M \to N$ heißt *Modulhomomorphismus*, falls f ein Gruppenhomomorphismus abelscher Gruppen ist und zusätzlich für alle $a \in A, x \in M$ gilt $f(a \cdot x) = a \cdot f(x)$ (A-*linearität*).

Beispiel 3.5. (i) Sei $A = K$ Körper. Ein A-Modul ist das Gleiche wie ein K-Vektorraum. Modulhomomorphismen sind die linearen Abbildungen von Vektorräumen.

(ii) Sei $A = \mathbb{Z}$. Ein $\mathbb{Z}$-Modul ist das gleiche wie eine abelsche Gruppe. Modulhomomorphismen sind genau die Abbildungen von abelschen Gruppen. Genauer: Die Kategorie der abelschen Gruppen ist isomorph zur Kategorie der $\mathbb{Z}$-Moduln.
Sei M $\mathbb{Z}$-Modul, dann ist nach Definition $(M, +)$ abelsche Gruppe. Jeder Modulhomomorphismus ist Abbildung abelscher Gruppen. Für die Gegenrichtung sei $(M, +)$ abelsche Gruppe. Wir definieren

$$\begin{aligned} 1 \cdot x &\coloneqq x && \forall x \in M \\ n \cdot x &\coloneqq (n-1) \cdot x + x = \underbrace{x + \ldots + x}_{n \text{ mal}} && \forall n \geq 0, x \in M \\ n \cdot x &\coloneqq -(-n) \cdot x && \forall n < 0, x \in M \end{aligned}$$

Dies ist $\mathbb{Z}$-Modul, denn nach Induktion ist z.B.

$$n \cdot (x + y) = (n-1)(x+y) + (x+y) = (n-1)x + (n-1)y + x + y = nx + ny$$

(iii) Sei K ein Körper. Ein $K[X]$-Modul ist das selbe wie ein K-Vektorraum V zusammen mit einem Endomorphismus $V \xrightarrow{\varphi} V$.

Beweis. Sei V ein $K[X]$-Modul. Durch Einschränken der Skalarmultiplikation auf K erhält man V als K-Vektorraum. Die Multiplikation mit X ist eine K-lineare Abbildung $V \xrightarrow{\varphi} V$:

$$\begin{aligned} X \cdot (v + w) &= X \cdot v + X \cdot w && \forall v, w \in V \\ X \cdot (\lambda \cdot v) &= (X \cdot \lambda) \cdot v = \lambda (Xv) && \forall \lambda \in K, v \in V \end{aligned}$$

Umgekehrt, wenn V ein K-Vektorraum ist mit Endomorphismus $\varphi : V \to V$, definiere

$$\left(\sum_{i=1}^{n} a_i X^i \right) \cdot v \coloneqq \sum_{i=1}^{n} a_i \varphi^i (v) \;\; \forall n \geq 0, a_i \in K, v \in V$$

□

Beobachtung 3.6. Sätze über Vektorräume mit Endomorphismen (z.B. Jordan Normalform) sind Sätze über $K[X]$-Moduln.

Beispiel 3.7. Betrachte $\mathbb{A}^2$.

(i) Sei $V_1 = \{(0, 0)\}$. Dann ist $I(V_1) = \langle X, Y \rangle$.

(ii) Für $V_1' = \{(0,1)\}$ ist $I(V_1') = \langle X-1, Y\rangle$.

(iii) Für $V_2 = \{(0,0),(1,0)\}$ ist $I(V_2) = \sqrt{(X^2 - X, XY, XY - Y, Y^2)}$.

Die Grundlegende Theorie der Moduln über A funktioniert wie bei Vektorräumen:

- linear (un)abhängig
- Erzeugendensystem
- Direkte Summen
- Untermoduln
- Quotientenmoduln

Definition 3.8. Ein Modul heißt endlich erzeugt, wenn er ein endliches Erzeugendensystem hat.

Beispiel 3.9. (i) A ist ein A-Modul für jeden Ring A. Die Untermoduln sind genau die Ideale.

(ii) Ist $\varphi : A \to B$ ein Ringhomomorphismus, wird damit B zu einem A-Modul vermöge $a \cdot b = \varphi(a) \cdot b$.

Definition 3.10. Sei M ein A-Modul. Ein linear unabhängiges Erzeugendensystem heißt *Basis*. M heißt *frei* wenn er eine Basis hat. Die Mächtigkeit der Basis heißt Rang. Das ist wohldefiniert.

Beispiel 3.11. (i) Ist A ein Körper, so sind alle A-Moduln frei (Basisexistenzsatz) und Rang=Dimension.

(ii) Sei $A = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$. Dieser Modul ist nicht frei, denn für alle $x \in M$ gilt $2x = 0$.

(iii) $A^2 \coloneqq A \oplus A$ ist frei von Rang 2 mit der Basis $\{(0,1),(0,1)\}$. $\{(1,-1),(1,1)\}$ ist Basis genau dann, wenn 2 in A invertierbar ist.

Bemerkung 3.12. Wie in der linearen Algebra sind Kern und Bild eines Modulhomomorphismus wieder Untermoduln. Ist $N \subseteq M$ ein Untermodul, dann ist M/N der Modul mit induzierter Skalarmultiplikation. Speziell, wenn $M = A$ Ring, dann ist $N \subseteq A$ Ideal und $M/N = A/N$ der Quotientenring.

Satz 3.13 (Homomorphiesatz, Isomorphiesätze)**.** *(i) Sei $f : M \to N$ ein Modulhomomorphismus. Dann ist die induzierte Abbildung $\overline{f} : M/\ker(f) \to \operatorname{im}(f)$ ein Modulisomorphismus.*

(ii) Sind $N, N' \subseteq M$ Untermoduln, so ist $(N + N')/N \cong N'/(N \cap N')$ ein kanonischer Isomorphismus.

(iii) Sind $N' \subseteq N \subseteq M$ Untermoduln, so ist $(M/N')/(N/N') \cong M/N$ ein kanonischer Isomorphismus.

Beweis. In der Algebra zeigt man diese Aussage für abelsche Gruppen, in der linearen Algebra für Vektorräume. Die Verträglichkeit der Skalarmultiplikation ist leicht zu prüfen. Beispielhaft für (ii): Betrachte den Modulhomomorphismus

$$f : N' \to (N + N') \to (N + N') /N$$

Der Kern von f ist

$$\{x \in N' \,|\, x + N = 0 + N\} = \{x \in N' \,|\, x \in N\} = N' \cap N$$

Nach (i) erhalten wir $\overline{f} : N'/ (N' \cap N) \xrightarrow{\sim} \mathrm{im}\,(f)$ einen Isomorphismus. Wir zeigen die Surjektivität von f. Ein $n \in (N + N') /N$ hat die Form

$$\underbrace{x}_{\in N} + \underbrace{x'}_{\in N'} + N = x' + N = f\,(x')$$

also ist f surjektiv □

3.2 Noethersche Moduln

Definition 3.14. Sei A ein Ring. Ein A-Modul M heißt *noethersch*, wenn jede Kette

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M$$

von Untermoduln M_i stationär wird, d.h.

$$\exists n > 0 : \; M_i = M_{i+1} \; \forall i \geq n$$

Lemma 3.15. *Ein Modul ist genau dann noethersch, wenn jeder Untermodul endlich erzeugt ist.*

Beweis. Angenommen $N \subseteq M$ ist nicht endlich erzeugt. Wir finden induktiv $x_1, x_2, ... \in N$ mit

$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \langle x_1, x_2, x_3 \rangle \subsetneq ...$$

Sei dazu $0 \neq x_1 \in N$ beliebig. Seien $x_1, ..., x_n \in N$ gewählt. Da $N/ \langle x_1, ..., x_n \rangle \neq 0$, denn N ist nicht endlich erzeugt, existiert ein $x_{n+1} \in N$, sodass

$$x_{n+1} + \langle x_1, ..., x_n \rangle \neq 0 + \langle x_1, ..., x_n \rangle$$

Somit folgt aus nicht-endlich erzeugt nicht-Kettenbedingung, also folgt aus der Kettenbedingung, dass jeder Untermodul endlich erzeugt ist. Umgekehrt sei $N_1 \subseteq N_2 \subseteq N_3 \subseteq ...$ eine Kette von Untermoduln. Betrachte den Untermoduln $N \coloneqq \bigcup_{i=1}^{\infty} N_i$. Angenommen alle Untermoduln von M sind endlich erzeugt, so ist auch N endlich erzeugt, also $N = \langle n_1, ..., n_r \rangle$. Da $n_j \in \bigcup_{i=1}^{\infty} N_i$ für alle $1 \leq j \leq r$ gibt es ein i_j mit $n_j \in N_{i_j}$. Sei $n \coloneqq \max\,\{i_1, ..., i_r\}$. Dann ist $n_1, ..., n_r \in N_n$ und somit $N_n = N$. Also ist $N_i = N \; \forall i \geq n$ □

Bemerkung 3.16. Ein Ring A ist noethersch genau dann, wenn A als A-Modul noethersch ist.

Definition 3.17. Eine (endliche oder unendliche) Folge

$$N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3 \to \ldots \to N_n$$

von Modulhomomorphismen heißt *exakt*, falls für alle $1 \leq i < n$

$$\mathrm{im}\,(f_i) = \ker\,(f_{i+1})$$

Beispiel 3.18. (i) $0 \to N_1 \xrightarrow{f} N_2$ ist exakt genau dann, wenn f injektiv ist: Bild der Nullabbildung ist der Nulluntermodul von N_1, also $\in 0 = 0 = \ker\,(f)$,

(ii) $M_1 \xrightarrow{g} M_2 \to 0$ ist exakt genau dann, wenn g surjektiv ist: Kern der Nullabbildung ist ganz M_2, also ist die Folge exakt genau dann, wenn $\mathrm{im}\,(g) = \ker\,(0) = M_2$.

(iii) $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ ist exakt, wenn f injektiv, g surjektiv und $\ker\,(g) = \mathrm{im}\,(f) = M_1$ ist. Eine solche Folge heißt *kurze exakte Sequenz*

Definition 3.19. Ein Diagramm von A-Modulhomomorphismen

$$\begin{tikzcd} M_1 \arrow[r, "f_1"] & M_2 \\ N_1 \arrow[u, "g_1"] \arrow[r, "f_2"'] & N_2 \arrow[u, "g_2"'] \end{tikzcd}$$

heißt *kommutativ*, wenn $f_1 \circ g_1 = g_2 \circ f_2$

Lemma 3.20.

$$0 \to M_1 \xrightarrow{\iota} M_2 \xrightarrow{\pi} M_3 \to 0$$

sei exakte Sequenz von A-Moduln. Dann ist M_2 noethersch genau dann, wenn M_1 und M_2 noethersch sind.

Beweis. Sei M_2 noethersch.

Behauptung. M_1 ist noethersch.

Beweis. M_1 ist Untermodul von M_2. Jeder Untermodul von M_1 ist also auch Untermodul von M_2. Da M_2 noethersch ist, sind diese endlich erzeugt. Also ist auch M_1 noethersch.

Behauptung. M_3 ist noethersch.

Beweis. Sei $\pi : M_2 \twoheadrightarrow M_3$ die Surjektion. Gegeben sei

$$N_1 \subseteq N_2 \subseteq \ldots$$

eine Folge von Untermoduln von M_3. Dann ist

$$\pi^{-1}\,(N_1) \subseteq \pi^{-1}\,(N_2) \subseteq \ldots$$

eine Folge von Untermoduln von M_2. Da M_2 noethersch ist, wird diese Folge stationär. Da

$$N_i = \pi^{-1}\,(N_i)\,/M_1$$

nach dem Homomorphiesatz wird auch die Folge

$$N_1 \subseteq N_2 \subseteq \ldots$$

stationär. Somit ist M_3 noethersch.

Seien nun andersherum M_1, M_3 noethersche Moduln. Sei

$$X_1 \subseteq X_2 \subseteq ...$$

Folge von Untermoduln von M_2. Jedes X_i hat eine kurze exakte Sequenz

$$0 \to X_i \cap M_1 \to X_i \to \pi(X_i) \to 0$$

Die Folge der $X_i \cap M_1$ wird stationär, da M_1 noethersch ist. Die Folge der $\pi(X_i)$ wird stationär, da M_3 noethersch ist. Für i groß genug gilt daher

$$\begin{tikzcd}
0 \arrow[r] & X_{i+1} \cap M_1 \arrow[r] & X_{i+1} \arrow[r] & \pi(X_{i+1}) \arrow[r] & 0 \\
0 \arrow[r] & X_i \cap M_1 \arrow[r] \arrow[u, "\wr"'] & X_i \arrow[r] \arrow[u, phantom, "\cup|"] & \pi(X_i) \arrow[r] \arrow[u, "\wr"'] & 0
\end{tikzcd}$$

Behauptung. $\varphi : X_i \to X_{i+1}$ ist surjektiv.

Beweis. Sei $x \in X_{i+1}$. Da $\pi(X_i) \to \pi(X_{i+1})$ Isomorphismus ist, gibt es ein Urbild $\widehat{x}$ von $\pi(x)$ und, da $X_i \to \pi(X_i)$ surjektiv ist, ein Urbild x' von $\widehat{x}$. Da $\pi(x - \varphi(x')) = 0$ und die obere Folge exakt ist, gibt es ein Urbild y von $x - \varphi(x')$. Da $X_i \cap M_1 \to X_{i+1} \cap M_1$ Isomorphismus ist, gibt es ein Urbild y' davon.

$$\begin{tikzcd}
X_{i+1} \cap M_1 \arrow[rrr] & & & X_{i+1} \arrow[rrr] & & & \pi(X_{i+1}) \\
& y \arrow[r, mapsto] & x - \varphi(x') & & x \arrow[r, mapsto] & \pi(x) & \\
& y' \arrow[u, mapsto] & & & x' \arrow[r, mapsto] & \widehat{x} \arrow[u, mapsto] & \\
X_i \cap M_1 \arrow[rrr] \arrow[uuu] & & & X_i \arrow[rrr] \arrow[uuu] & & & \pi(X_i) \arrow[uuu]
\end{tikzcd}$$

Dann ist $x' + y'$ Urbild von x unter φ, denn

$$\varphi(x' + y') = \varphi(x') + \underbrace{\varphi(y')}_{x - \varphi(x')} = x$$

Also ist φ surjektiv und somit wird die Folge der X_i stationär. □

Korollar 3.21. *Sei A noetherscher Ring, M endlich erzeugter A-Modul, dann ist M noethersch.*

Beweis. A ist noethersch als Modul über sich selbst. Per Induktion ist $A^n := A^{\oplus n} := \underbrace{A \oplus ... \oplus A}_{n \text{ mal}}$ noethersch:

$$0 \to A \overset{a \mapsto (a,0)}{\to} A \oplus A^{n-1} \overset{(a,b) \mapsto b}{\to} A^{n-1} \to 0$$

ist exakte Sequenz und somit ist nach Lemma 3.20 A^n noethersch. Seien $x_1, ..., x_r \in M$ Erzeuger von M, dann ist

$$\begin{aligned} \varphi : & A^r \to M \\ & (a_1, ..., a_r) \mapsto a_1 x_1 + ... + a_r x_r \end{aligned}$$

surjektiv, da x_i Erzeuger sind. Dann ist

$$0 \to \ker(\varphi) \to A^r \to M \to 0$$

kurze Exakte Sequenz. Da A^r noethersch ist, ist nach Lemma 3.20 also auch M noethersch. $\square$

Satz 3.22 (Hilberts Basissatz)**.** *Sei A noetherscher Ring, dann ist $A[X]$ auch noethersch.*

Beweis. Sei $I \triangleleft A[X]$ ein Ideal. Wir suchen endlich viele Erzeuger von I. Falls $A = K$ Körper ist, dann ist $K[X]$ Hauptidealring, wegen Polynomdivision, und damit noethersch. Für jedes $n \geq 0$ sei $I_n \subseteq I \subseteq A[X]$ die Menge der Polynome in I von Grad höchstens n. Dies ist ein A-Modul. Es sei

$$J_n := \{a \in A \mid \exists P \in I_n : P = aX^n + ...\}$$

das *Leitkoeffizientenideal.* Dies ist Ideal von A. Des weiteren ist, da $X \cdot I_n \subseteq I_{n+1}$, $J_n \subseteq J_{n+1}$. Da A noethersch ist, wird die Folge

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq J_3 \subseteq ...$$

stationär. Sei d so, dass $J_n = J_d$ für alle $n \geq d$. Wähle für $n \leq d$ A-Erzeuger $a_1^{(n)}, ..., a_{r_n}^{(n)} \in J_n$. Weiter sei $P_j^{(n)} \in I_n$ mit $P_j^{(n)} = a_j^{(n)} X^n + ...$

Behauptung. Die $P_j^{(n)}$, für $n \leq d$, $j \in \{1, ..., r_n\}$ erzeugen I.

Beweis. Sei $Q = bX^m + ... \in I$. Per Induktion nach m: Für $m \leq d$ existieren $c_1, ..., c_{r_m} \in A$, sodass $b = \sum_{i=1}^{r_m} c_i a_i^{(m)}$. Dann ist

$$Q - \sum_{i=1}^{r_m} c_i P_i^{(m)}$$

von Grad kleiner als Q. Per Induktionsannahme ist dies von den $P_j^{(n)}$ erzeugt und somit auch Q. Sei nun $m > d$, dann gibt es $c_1, ..., c_{r_d} \in A$ mit $b = \sum_{i=1}^{r_d} c_i a_i^{(d)}$ und somit hat

$$Q - \sum_{i=1}^{r_d} c_i X^{m-d} P_i^{(d)}$$

kleineren Grad und somit ist Q nach Induktion von den $P_j^{(n)}$ erzeugt.

$\square$

Korollar 3.23. *Sei $A = \mathbb{Z}$ oder $A = K$ Körper, dann ist $A[X_1, ..., X_n]$ noethersch.*

Beweis. Per Induktion, da $A[X_1, ..., X_n] = A[X_1][X_2] ... [X_n]$. $\square$

Definition 3.24. Sei $\varphi : A \to B$ ein Ringhomomorphismus. B heißt *endlich erzeugte A-Algebra*, falls $b_1, ..., b_n \in B$ existieren, sodass sich jedes Element in B schreiben lässt als

$$b = \sum \varphi(a_{\underline{i}}) b_1^{i_1} \cdot ... \cdot b_n^{i_n}$$

für $\underline{i} = (i_1, ..., i_n) \in \mathbb{N}_0^n$. Mit anderen Worte, es gibt eine Surjektion

$$\widehat{\varphi} : A[X_1, ..., X_n] \overset{X_i \mapsto b_i}{\twoheadrightarrow} B$$

die φ erweitert.

Korollar 3.25. *Sei A noethersch, B endlich erzeugte A-Algebra, dann ist auch B noethersch.*

Beweis. Folgt aus dem Hilbertschen Basissatz 3.22 und dem Lemma 3.20. $\square$

Korollar 3.26. *Sei $k = \overline{k}, V \subseteq \mathbb{A}_k^n$ algebraische Menge. Dann ist $\mathcal{O}(V)$ noethersch. Jede algebraische Menge wird durch endlich viele Gleichungen definiert, ist also Schnitt von endlich vielen Hyperflächen.*

Beweis. Es ist $\mathcal{O}(V) = k[X_1, ..., X_n]/I(V)$ endlich erzeugte k-Algebra und somit noethersch. Somit ist

$$I(V) = \langle f_1, ..., f_r \rangle$$

Außerdem gilt

$$V = V(I(V)) = V(f_1, ..., f_r) = \bigcap_{i=1}^{r} V(f_i)$$

$\square$

Lemma 3.27. *$V = V(I(V))$ für V algebraisch.*

Beweis. V ist algebraische Menge. Also ist $V = V(S), S \subseteq I(V)$ und somit $V = V(S) \supseteq V(I(V))$. Sei $P \in V$, dann ist $f(P) = 0\ \forall f \in I(V)$ und damit $P \in V(I(V))$ $\square$

4 Hilbertscher Nullstellensatz

Ziel: Korrespondenz von Varietäten und Idealen

$$\begin{aligned} V &: \{S \subseteq k[X_1, ..., X_n]\} \to \{V \subseteq \mathbb{A}^n\} \\ I &: \{V \subseteq \mathbb{A}^n\} \to \{S \subseteq k[X_1, ..., X_n]\} \end{aligned}$$

Nach Lemma 3.27 ist $V(I(V)) = V$ für V algebraische Menge. Außerdem ist $I(V(S)) \supseteq \sqrt{\langle S \rangle}$ nach 1.22.

Satz 4.1 (Hilbertscher Nullstellensatz)**.** *Sei $k = \overline{k}$. Für jede Teilmenge $S \subseteq k[X_1, ..., X_n]$ gilt $I(V(S)) = \sqrt{S}$. Insbesondere erhalten wir eine Bijektion*

$$\{\textit{reduzierte Ideale in } k[X_1, ..., X_n]\} \leftrightarrow \{\textit{abgeschlossene Teilmengen von } \mathbb{A}^n\}$$

Denn $I(V(I)) = I$ wenn I reduziert ist.

4.1 Maximale Ideale

Definition 4.2. Sei A ein Ring, $I \lhd A$ ein Ideal, so heißt I *maximal*, wenn es maximal in der teilgeordneten Menge der echten Ideale von A ist. Das heißt, wenn $A \neq I$ und für alle $J \lhd A$ mit $I \subseteq J \subseteq A$ gilt, dass entweder $J = I$ oder $J = A$.

Beispiel 4.3. Sei $P \in \mathbb{A}^n$, dann ist

$$I(P) := I(\{P\}) = \{f \in \mathcal{O}(\mathbb{A}^n) \mid f(P) = 0\}$$

maximales Ideal, denn für $I(P) \subseteq J \subseteq A = \mathcal{O}(\mathbb{A}^n)$, wenn $f \in J \setminus I(P)$, dann $f(P) \neq 0$. Für $f' := f - f(P)$ gilt dann $f' \in I(P)$. Da J ein Ideal ist und $f, f' \in J$ ist $\underbrace{f' - f}_{0 \neq f(P) \in k} \in J$. Also ist $1 = f(P)^{-1} \cdot f(P) \in J$ und damit $J = \mathcal{O}(\mathbb{A}^n)$

Lemma 4.4. *Sei A ein Ring, $I \triangleleft A$ ein Ideal, dann ist I maximal genau dann, wenn A/I ein Körper ist.*

Beweis. Betrachte die Surjektion $\pi : A \to A/I$. Es ist $I \neq A$ genau dann, wenn $0 \neq 1$ in A/I. Sei zunächst I maximal, $0 \neq \overline{f} = f + I \in A/I$, also $f \notin I$. Da $I \subseteq \pi^{-1}\left(\langle \overline{f} \rangle\right) \subseteq A$ ideal ist, gilt entweder $I = \pi^{-1}\left(\langle \overline{f} \rangle\right)$ oder $\pi^{-1}\left(\langle \overline{f} \rangle\right) = A$. Im ersten Fall folgt $f \in \pi^{-1}\left(\langle \overline{f} \rangle\right) = I$ und damit $\overline{f} = 0$ im Widerspruch zur Annahme. Im Fall $\pi^{-1}\left(\langle \overline{f} \rangle\right) = A$ ist dann $\langle f \rangle + I = A$ und somit $1 = g \cdot f + i$ für ein $i \in I, g \in A$. Somit ist

$$1 = \pi(g) \cdot \pi(f) = \pi(g) \cdot \overline{f}$$

und damit ist $\pi(g)$ ein Inverses zu $\overline{f}$. Also ist A/I ein Körper. Sei umgekehrt A/I ein Körper. Sei $I \subseteq J \subseteq A$. Da $I \subseteq J$ gilt $J = \pi^{-1}(\pi(J))$. Somit ist

$$0 = \pi(I) \subseteq \pi(J) \subseteq A/I$$

und $\pi(J)$ ein Ideal. Da es in einem Körper nur zwei Ideale, $\langle 0 \rangle$ und den Körper selbst, gibt, ist entweder $\pi(J) = 0$ und damit $J = I$ oder $\pi(J) = A/I$ und damit $J = A$. □

Beispiel 4.5. Sei $P \in \mathbb{A}^n$ ein Punkt, dann ist $\mathcal{O}(\mathbb{A}^n)/I(P) = \mathcal{O}(P) = k$. Dies ist ein Körper und damit ist $I(P)$ maximal. Ist $P = (a_1, ..., a_n) \in k^n$, so liegen die Funktionen $X_i - a_i$ in $I(P)$. Tatsächlich gilt $I(P) = \langle X_1 - a_1, ..., X_n - a_n \rangle$

Satz 4.6 (Schwacher Nullstellensatz)**.** *Sei $k = \overline{k}$, $A := \mathcal{O}(\mathbb{A}^n)$. Die maximalen Ideale von A sind von der Form $\langle X_1 - a_1, ..., X_n - a_n \rangle$. (Beweis in 8.3)*

Beispiel 4.7. Sei $n = 1$. Alle Ideale von $k[X]$ sind die Hauptideale, also von der Form $\langle f \rangle$ für ein $f \in k[X]$. Maximale Ideale sind genau die, wo f irreduzibel ist. Wenn $k = \overline{k}$, dann sind die irreduziblen Polynome linear.

$$X^2 + 1 = (X - i)(X + i)$$

ist reduzibel in $\mathbb{C}[X]$, $X - i$ ist irreduzibel.

Beweis von 4.1 aus 4.6.

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

Beweis. Nach 1.22 gilt $I(V(J)) \supseteq \sqrt{J}$. Zu zeigen ist somit nur noch $I(V(J)) \subseteq \sqrt{J}$. Sei dazu $J = \langle f_1, ..., f_m \rangle$, $g \in I(V(J))$ und sei X_0 weitere Unbestimmte. Betrachte das Ideal $J' = \langle f_1, ..., f_m, X_0 \cdot g - 1 \rangle \triangleleft k[X_0, ..., X_n]$. Angenommen $J' \neq k[X_0, ..., X_n]$.

Behauptung. J' ist in einem maximalen Ideal J'_M enthalten.

Beweis. Falls J' nicht maximal ist, existiert ein größeres Ideal, wenn dieses nicht maximal ist, existiert noch ein größeres und so weiter. Somit erhalten wir eine aufsteigende Folge und diese wird stationär. Somit ist das stabile Ideal das gesuchte J'_M.

Nach Satz 4.6 existiert $P' = (a_0, a_1, ..., a_n) \in V(J'_M)$. Setze $P = (a_1, ..., a_n)$. Dann ist $f_j(P) = 0$ für $1 \leq j \leq n$. Da $g \in I(V(J))$ ist $g(P) = 0$. Dies ist ein Widerspruch zu $1 - a_0 g(P) = 0$ und somit ist $J' = k[X_0, ..., X_n]$. Damit gibt es $h_0, ..., h_m$ mit

$$1 = h_1 f_1 + ... + h_m f_m + h_0 (X_0 g - 1)$$

in $k[X_0, ..., X_n]$ Ersetze X_0 durch $\frac{1}{g}$ und multipliziere mit hoher Potenz von g. Dann ist

$$g^N = h'_1 f_1 + ... + h'_m f_m \in J$$

in $k[X_1, ..., X_n]$ und damit $g \in \sqrt{J}$.

□

4.2 Irreduzible Mengen

Definition 4.8. Ein topologischer Raum Y heißt *irreduzibel*, wenn $Y \neq 0$ und $Y \neq Y_1 \cup Y_2$ für $Y_i \subsetneq Y$ abgeschlossen.

Beispiel 4.9. (i) $\mathbb{R}$ mit der gewöhnlichen Topologie ist reduzibel, denn

$$\mathbb{R} = \mathbb{R}_{\leq 0} \cup \mathbb{R}_{\geq 0}$$

(ii) $\mathbb{A}^1$ mit der Zariski-Topologie ist irreduzibel.

(iii) Einelementige algebraische Mengen sind irreduzibel.

(iv) $V(X_1 \cdot X_2) = V(X_1) \cup V(X_2) \subseteq \mathbb{A}^2$ ist reduzibel.

Definition 4.10. Sei A ein Ring, $I \triangleleft A$ ein Ideal. I heißt *Primideal*, wenn $I \neq A$ und für $a, b \in A$ mit $a \cdot b \in I$ folgt $a \in I$ oder $b \in I$.

Beispiel 4.11. Sei $I = \langle n \rangle \triangleleft \mathbb{Z}$ Primideal für $n \in \mathbb{N}$. Da $I \neq \mathbb{Z}$ ist $n \neq 1$. Für alle $a, b \in Z$ gilt

$$a \cdot b \in \langle n \rangle \Leftrightarrow n | a \cdot b \underset{\text{Primideal}}{\Longrightarrow} a \in \langle n \rangle \ \vee \ b \in \langle n \rangle \Leftrightarrow n | a \ \vee \ n | b$$

Dies ist genau die Bedingung für n irreduzibel.

Bemerkung 4.12. Primideale sind immer reduziert.

Satz 4.13. *Eine affine Varietät V ist irreduzibel genau dann, wenn $I(V)$ ein Primideal ist.*

Beweis. Sei Y irreduzibel, $f, g \in \mathcal{O}(\mathbb{A}^n)$ und $f \cdot g \in I(Y)$, Es ist

$$Y \subseteq V(f) \cup V(g)$$

und damit

$$Y = (V(f) \cap Y) \cup (V(g) \cap Y)$$

Da Y irreduzibel ist, sei o.B.d.A $Y = V(f) \cap Y$ und damit $Y \subseteq V(f)$, also $f \in I(Y)$. Somit ist $I(Y)$ ein Primideal. Umgekehrt sei $J := I(V)$ ein Primideal und sei $V(J) = Y_1 \cup Y_2$ mit Y_1, Y_2 abgeschlossen. Dann ist

$$J = I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$$

Angenommen $I(Y_1) \neq J \neq I(Y_2)$ und somit gibt es ein $f_i \in I(Y_i) \setminus J$ für $i \in \{1, 2\}$ und $f_1 \cdot f_2 \in I(Y_1) \cap I(Y_2) = J$. Da J Primideal ist, gilt $f_1 \in J$ oder $f_2 \in J$ im Widerspruch zur Wahl von f_1 und f_2. Somit ist $J = I(Y_1)$ oder $J = I(Y_2)$. Sei o.B.d.A $J = I(Y_1)$. Da

$$\begin{aligned} Y &= V(I(Y)) \\ &= V(I(Y_1)) \\ &= Y_1 && \text{Lemma 3.27} \end{aligned}$$

und somit ist Y irreduzibel. $\square$

Bemerkung 4.14. Wir haben Bijektionen

$$\begin{aligned}\{\text{reduzierte Ideale}\} &\xleftrightarrow{\sim} \{\text{affine Varietäten}\}\\ \{\text{Primideale}\} &\xleftrightarrow{\sim} \{\text{irreduzible affine Varietäten}\}\\ \{\text{maximale Ideale}\} &\xleftrightarrow{\sim} \{\text{Punkte}\}\end{aligned}$$

Lemma 4.15. *Sei A ein Ring, $I \lhd A$. Dann ist I ein Primideal genau dann, wenn A/I nullteilerfrei ist und* $0 \neq 1$.

Beweis. Sei I ein Primideal. Wegen $I \neq A$ gilt $0 \neq 1$ in A/I. Sei $\overline{a} = a + I$ und $\overline{b} = b + I \in A/I$ mit $\overline{a} \cdot \overline{b} = 0$. Dann gilt $a \cdot b + I = 0 + I$. Dies ist äquivalent zu $a \cdot b \in I$. Da I Primideal ist, folgt $a \in I$ oder $b \in I$ beziehungsweise $\overline{a} = 0$ oder $\overline{b} = 0$. Umkehrung ist analog. $\square$

Korollar 4.16. *Maximale Ideale sind Primideale*

Beweis. Nach Lemma 4.4 ist A/I ein Körper für I maximales Ideal von A. Somit ist A/I nullteilerfrei und damit, nach Lemma 4.15, ist I Primideal. $\square$

Beispiel 4.17. $\mathbb{A}^n$ ist irreduzibel, denn $k[X_1, ..., X_n]$ ist nullteilerfrei. Ist $f \in k[X_1, ..., X_n]$ irreduzibel, dann ist $V(f)$ irreduzibel.

Definition 4.18. Ein topologischer Raum heißt *noethersch*, wenn jede Folge von abgeschlossenen Teilmengen

$$Y_1 \supseteq Y_2 \supseteq ...$$

stabil wird.

Beispiel 4.19. Affine Varietäten sind noethersch, denn Ketten von abgeschlossenen Mengen entsprechen Ketten von Idealen nach Hilbertschem Nullstellensatz.

Lemma 4.20. *Sei Y ein noetherscher topologischer Raum und $X \subseteq Y$ offen, dann ist auch X ein noetherscher topologischer Raum.*

Beweis. Sei $X_1 \supseteq X_2 \supseteq ...$ eine Folge von abgeschlossenen Teilmengen von X. Dann ist $\overline{X_1} \supseteq \overline{X_2} \supseteq ...$ eine Folge abgeschlossener Teilmengen von Y. Da Y noethersch ist, wird diese Folge stabil. Da gilt $X_i = \overline{X_i} \cap X$ wird auch die Folge der X_i stabil und somit ist X noethersch. $\square$

Satz 4.21. *Sei X ein noetherscher topologischer Raum. Jede abgeschlossene Teilmenge Y ist Vereinigung von endlich vielen irreduziblen Teilmengen*

Beweis. Angenommen Y ist nicht irreduzibel ist, also $Y = Y_0 \cup Y_1$ mit $Y_0, Y_1 \subsetneq Y$. Falls o.B.d.A Y_0 nicht irreduzibel ist, sei $Y_0 = Y_{00} \cup Y_{01}$ mit $Y_{00}, Y_{01} \subsetneq Y_0$ abgeschlossen und so weiter. Wenn dieser Prozess nicht endet, dann existiert eine Kette von abgeschlossenen Teilmengen, die nicht stabil wird

$$Y \supsetneq Y_0 \supsetneq Y_{00} \supsetneq ...$$

im Widerspruch dazu, dass X noethersch ist. $\square$

Definition 4.22. Sei Y eine affine Varietät. Eine irreduzible abgeschlossene Teilmenge $Y' \subseteq Y$ heißt *irreduzible Komponente*, wenn für jede irreduzible abgeschlossene Teilmenge Y'' mit $Y' \subseteq Y'' \subseteq Y$ gilt $Y' = Y''$.

Korollar 4.23 (Zerlegung in irreduzible Komponenten)**.** *Sei Y affine Varietät, dann hat Y endlich viele irreduzible Komponenten Y_i für $1 \leq i \leq r$ und es gilt $Y = Y_1 \cup ... \cup Y_r$*

Beweis. Sei $Y = Y_1 \cup ... \cup Y_m$ die Zerlegung aus Satz 4.21 mit minimalem m.
Behauptung. Sei $Y' \subseteq Y$ irreduzibel, dann ist $Y' \subseteq Y_i$ für ein i.

Beweis. Betrachte $Y_i' = Y_i \cap Y'$. Es gilt $Y' = Y_1' \cup Y_2' \cup ... \cup Y_n'$. Da Y' irreduzibel ist, ist $Y' = Y_i'$ für ein i und damit $Y' = Y_i' = Y_i \cap Y' \subseteq Y_i$

Behauptung. Jede irreduzible Komponente von Y ist gleich einem Y_i.

Beweis. Sei Y' irreduzible Komponente. Nach vorheriger Behauptung gilt $Y' \subseteq Y_i$ für ein i und somit, da Y' irreduzible Komponente ist, $Y_i = Y'$

Behauptung. $Y_1, ..., Y_n$ sind genau die irreduziblen Komponenten von Y

Beweis. O.B.d.A betrachte Y_1. Wenn $Y' \subseteq Y$ irreduzibel ist mit $Y_1 \subseteq Y'$, dann gilt nach vorheriger Behauptung $Y' \subseteq Y_i$ für ein i. Nach Minimalität gilt $i = 1$ und somit ist Y_1 irreduzible Komponente.

□

Definition 4.24. Sei X ein topologischer Raum. Die *Dimension* von X ist

$$\dim X = \sup \{ n \in \mathbb{N}_0 \mid \exists X_0 \subsetneq ... \subsetneq X_n : X_i \subseteq X \text{ irreduzibel} \}$$

Beispiel 4.25. (i) $X = \{P\}$, dann ist $\dim X = 0$, denn die einzige irreduzible Teilmenge ist X selbst.

(ii) $X = \mathbb{A}^1$ hat Dimension 1. Die Ketten haben die Form $\{P\} \subsetneq \mathbb{A}^1$ für jedes $P \in \mathbb{A}^1$.

(iii) Sei $V(XY, XZ) \subseteq \mathbb{A}^3$. Es gilt

$$\begin{aligned} V &= \{(x, y, z) \mid xy = 0,\, xz = 0\} \\ &= \underbrace{\{(0, y, z) \mid y, z \in k\}}_{\cong \mathbb{A}^2} \cup \underbrace{\{(x, 0, 0) \mid x \in k\}}_{\cong \mathbb{A}^1} \end{aligned}$$

und somit ist $\dim V \geq 2$

Lemma 4.26. *Die Dimension von X ist gleich der* Krulldimension *von $k[X]$, d.h. der maximalen Länge einer echten Kette von Primidealen.*

Beweis. Nach Hilbertschem Nullstellensatz 4.1. □

Bemerkung 4.27. Sogar in noetherschen Ringen muss die Krulldimension nicht endlich sein. Einige Eigenschaften der Dimension sind klar:

(i) $Y \subseteq W$ abgeschlossene Teilmenge, dann ist $\dim Y \leq \dim W$, weil jede Kette von Y auch Kette von W ist.

(ii) $\dim \mathbb{A}^n \geq n$, denn $\mathbb{A}^n \supsetneq V(X_1) \supsetneq V(X_1, X_2) \supsetneq ...$ hat Länge n

Bemerkung 4.28. Tatsächlich gilt $\dim \mathbb{A}^n = n$ was wir erst später zeigen können. Ist $k = \mathbb{C}$, so trägt jede Zariski-abgeschlossene Menge auch die gewöhnliche Topologie induziert von $\mathbb{C}^n$ und die Dimension stimmt überein mit der von uns gegebenen.

5 Offene überdeckungen

Definition 5.1. Sei V affine Varietät. Teilmengen der Form $U_f \coloneqq V \setminus V(f)$ für $f \in \mathcal{O}(V)$ heißen *standardoffen*.

Bemerkung 5.2. Wir haben bisher nur $V(f) \subseteq \mathbb{A}^n$ definiert für $f \in k[X_1, ..., X_n]$. In der Definition ist aber $f \in \mathcal{O}(V) = k[X_1, ..., X_n]/I(V)$. Der Unterschied ist harmlos, es gibt weiterhin immer ein Urbild $\widetilde{f} \in k[X_1, ..., X_n]$ und egal welches wir wählen $V(f) = V\left(\widetilde{f}\right) \cap V$. Anders gesagt

$$\begin{aligned} V(f) &= \{P \in V \mid f(P) = 0\} \\ U_f &= \{P \in V \mid f(P) \neq 0\} \end{aligned}$$

Lemma 5.3. *Sei V affine Varietät, $U \subseteq V$ offen. Dann ist U Vereinigung von standardoffenen Mengen. Insbesondere sind die standardoffenen Mengen eine Basis der Topologie.*

Beweis. Sei $U = V \setminus Z$ mit $Z = V(S)$ für ein $S \subseteq \mathcal{O}(V)$, also

$$V(S) = \bigcap_{f \in S} V(f) \implies U = V \setminus V(S) = \bigcup_{f \in S} (V \setminus V(f)) = \bigcup_{f \in S} U_f$$

□

Bemerkung 5.4. Tatsächlich kann S im Beweis endlich gewählt werden. Da $\mathcal{O}(V)$ noethersch ist, wird jede abgeschlossene Teilmenge Z wird von endlich vielen Gleichungen gegeben.

Lemma 5.5. *Sei Y noetherscher topologischer Raum, $\{U_i\}_{i \in I}$ eine* offene überdeckung*, also $U_i \subseteq Y$ offen und $Y = \bigcup_{i \in I} U_i$, dann existiert eine* endliche Teilüberdeckung*, d.h. es gibt endlich viele $i_1, ..., i_r \in I$ mit $Y = U_{i_1} \cup ... \cup U_{i_r}$.*

Bemerkung 5.6. Topologische Räume mit dieser Eigenschaft heißen *quasikompakt* (manchmal auch *kompakt*). Ein topologischer Raum heißt *kompakt*, wenn er quasikompakt und Hausdorffsch ist. Da Varietäten fast nie Hausdorffsch sind, interessieren wir uns für Quasikompaktheit

Beweis. Angenommen $\{U_i\}$ hat keine endliche Teilüberdeckung, dann konstruiere eine Folge U_{i_j} für $j \in \mathbb{N}$, sodass für $U'_{i_j} \coloneqq \bigcup_{k=1}^{j} U_{i_k}$ gilt

$$U_{i_1} \subsetneq U_{i_2} \subsetneq U_{i_3} \subsetneq ...$$

Wähle nämlich i_1 beliebig. Da Y nicht von U_{i_1} überdeckt wird, existiert $P \in Y \setminus U_{i_1}$. Da $\{U_i\}$ überdeckung von Y ist, existiert i_2 mit $P \in U_{i_2}$. Da $U_{i_1} \cup U_{i_2}$ keine überdeckung ist, existiert $Q \in Y$ mit $Q \in Y \setminus (U_{i_1} \cup U_{i_2})$ und ein i_3 mit $Q \in U_{i_3}$ und so weiter. Komplementär zur Folge U_{i_j} gibt es nun die Folge

$$Z_1 \supsetneq Z_2 \supsetneq Z_3 \supsetneq ...$$

von abgeschlossenen Mengen, im Widerspruch dazu, dass Y noethersch ist. □

Korollar 5.7. *quasi-affine Varietäten sind quasi-kompakt*

Beweis. Affine varietäten sind noethersch und nach Lemma 4.20 auch offene Teilmengen darin, also quasi-affine Varietäten. □

6 Lokale Ringe und Lokalisierung

6.1 Der irreduzible Fall

Definition 6.1. Sei A ein nullteilerfreier Ring, dann heißt

$$Q(A) = \left\{ \frac{a}{s} \;\middle|\; a \in A, s \in A \setminus \{0\} \right\}$$

Quotientenkörper von A. Dabei ist $\frac{a}{s}$ die äquivalenzklasse des Paares $(a, s) \in A \times (A \setminus 0)$ bezüglich der äquivalenzrelation

$$(a, s) \sim (a', s') :\Leftrightarrow s'a = sa'$$

für alle $a, a' \in A, s, s' \in A \setminus \{0\}$. Die Addition und Multiplikation ist die von Brüchen.

Beispiel 6.2. $Q(\mathbb{Z}) = \mathbb{Q}$

Definition 6.3. Sei V eine irreduzible affine Varietät, dann heißt

$$k(V) := Q(k[V]) = Q(\mathcal{O}(V))$$

Funktionenkörper von V. Die Elemente von $k(V)$ heißen *rationale Funktionen* auf V. Sei $P \in V$, $f \in k(V)$, dann heißt f *regulär* an P, falls $f = \frac{g}{h}$ mit $h(P) \neq 0$. In diesem Fall setzen wir $f(P) := \frac{g(P)}{h(P)} \in k$, andernfalls $f(P) := \infty$. Der Ring

$$\mathcal{O}_{V,P} := \mathcal{O}_P := \{f \in k(V) \mid f \text{ ist regulär an } P\}$$

heißt *lokaler Ring* von V an P.

Bemerkung 6.4. Es ist leicht zu sehen, dass $f(P)$ wohldefiniert ist.

Definition 6.5. Ein Ring heißt *lokal*, wenn er genau ein maximales Ideal enthält.

Lemma 6.6. *Sei V irreduzible Varietät, $P \in V$, dann ist $\mathcal{O}_P$ lokal mit maximalem Ideal $\mathfrak{m}_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}$.*

Beweis. Betrachte die Auswertungsabbildung

$$\begin{aligned} \mathrm{ev} : \mathcal{O}_P &\to k \\ f &\mapsto f(P) \end{aligned}$$

dies ist ein Epimorphismus von Ringen, da $k \subseteq k[V] \subseteq \mathcal{O}_P$. Nach dem Homomorphiesatz gilt $\mathcal{O}_P / \ker(\mathrm{ev}) \cong k$ und $\ker(\mathrm{ev}) = \mathfrak{m}_P$. Als Kern eines Ringhomomorphismus ist $\mathfrak{m}_p$ ein Ideal und nach Lemma 4.4 ist dieses maximal.

Behauptung. Jedes Element in $\mathcal{O}_P \setminus \mathfrak{m}_P$ ist invertierbar

Beweis. Sei $f = \frac{g}{h} \in \mathcal{O}_P \setminus \mathfrak{m}_P$ mit $h(P) \neq 0$. Nach Voraussetzung gilt $g(P) \neq 0$. Dann ist $\frac{h}{g}$ das Inverse zu f.

Behauptung. Jedes echte Ideal von $\mathcal{O}_P$ ist in $\mathfrak{m}_P$ enthalten.

Beweis. Sei $I \subsetneq \mathcal{O}_P$ ein Ideal. Dann enthält I keine invertierbaren Elemente. Also ist

$$I \cap (\mathcal{O}_P \setminus \mathfrak{m}_P) = \emptyset \Leftrightarrow I \subseteq \mathfrak{m}_P$$

$\square$

Wir haben mit bewiesen

Lemma 6.7. *Sei A ein Ring, $\mathfrak{m} \triangleleft A$ Ideal, dann ist A lokal genau dann, wenn $A \setminus \mathfrak{m} = A^\times$ die Menge der invertierbaren Elemente ist.*

Definition 6.8. Sei $V \subseteq \mathbb{A}^n$ quasi-affin und irreduzibel Wir setzen

$$\mathcal{O}(V) = \bigcap_{P \in V} \mathcal{O}_P \subseteq k(W), \; W = \overline{V}$$

den Ring der *algebraischen Funktionen* auf V

Bemerkung 6.9. Wir müssten jetzt eigentlich zeigen, dass für affine Varietäten diese Definition mit der vorherigen übereinstimmt. Dies beweisen wir in einem allgemeineren Kontext: ohne die Voraussetzung, dass V irreduzibel ist. Zunächst unterscheiden wir $\mathcal{O}(V) = \bigcap_{P \in V} \mathcal{O}_P$ und $k[V] = k[X_1, ..., X_n] / I(V)$

6.2 Lokalisierung von Moduln

Wir wollen mit Brüchen $\frac{m}{s}$ rechnen, wobei $m \in M, s \in R$ mit M R-Modul, mit Rechenregeln

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}$$
$$\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$$

für $a, s, s' \in R, m, m' \in M$

Definition 6.10. Sei A ein Ring. Eine Teilmenge $S \subseteq A$ heißt *multiplikativ*, wenn $1 \in S$, $0 \notin S$ und wenn S abgeschlossen ist unter Multiplikation (d.h. $s, s' \in S \implies s \cdot s' \in S$).

Beispiel 6.11. (i) Sei $f \in A$, dann ist

$$S = \left\{1, f, f^2, f^3, ...\right\}$$

genau dann multiplikativ, wenn f nicht *nilpotent* ist (d.h.$\nexists n \in \mathbb{N} : f^n = 0$)

(ii) Sei $\mathfrak{p} \subseteq A$ Primideal, dann ist $S_\mathfrak{p} = A \setminus \mathfrak{p}$ multiplikativ.

(iii) Sei A ein Ring und S die Menge aller Elemente, die nicht Null und keine Nullteiler sind, dann ist S multiplikativ. Falls A nullteilerfrei ist, gilt $S = A \setminus \{0\}$

Lemma 6.12. *Sei V irreduzible affine Varietät, $f \in k(V)$ und sei*

$$U := \{P \in V \mid f \text{ regulär in } P\}$$

dann ist U offen

Beweis. Sei
$$I := \left\{ (g,h) \in k[V]^2 \;\middle|\; f = \frac{g}{h} \right\}$$
dann ist
$$U = \bigcup_{(g,h)\in I} U_h,\ U_h := V \setminus V(h),\ V(h) = \{P \in V \mid h(P) = 0\}$$
Somit ist $U \subseteq V$ offen. □

Korollar 6.13. *Sei V quasi-affin und irreduzibel, $P \in V$, dann ist*
$$\mathcal{O}_P = \bigcup_{P \in U \subseteq V} \mathcal{O}(U)$$

Definition 6.14. Sei A Ring, $S \subseteq A$ multiplikatives System und M A-Modul. Auf $M \times S$ sei die Relation
$$(m,s) \sim (m',s') \;:\Leftrightarrow\; \exists t \in S:\ ts'm = tsm'$$
definiert. Wir schreiben $\frac{m}{s}$ für die äquivalenzklasse von (m,s). Dann heißt
$$S^{-1}M := \left\{ \frac{m}{s} \;\middle|\; m \in M, s \in S \right\}$$
die *Lokalisierung* von M an S. Wenn $f \in A$ nicht nilpotent ist, schreiben wir
$$M_f := S_f^{-1}M,\ S_f := \left\{1, f, f^2, ...\right\}$$
Für ein Primideal $\mathfrak{p} \subseteq A$ schreiben wird
$$M_\mathfrak{p} := S_\mathfrak{p}^{-1}M$$

Lemma 6.15. *Sei $A \subseteq S$, A Ring, S multiplikativ und M A-Modul, dann ist*

(i) $\sim$ eine äquivalenzrelation.

(ii) $S^{-1}M$ mit der Addition von Brüchen eine abelsche Gruppe.

(iii) $S^{-1}A$ ein Ring mit Addition und Multiplikation von Brüchen, sodass
$$\begin{aligned} A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$
ein Ringhomomorphismus ist.

(iv) $S^{-1}M$ mit der Multiplikation von Brüchen ist ein $S^{-1}A$-Modul.

Beweis. (i) Symmetrie, Reflexivität ist klar. Zur Transitivität, sei $(m,s) \sim (m',s') \sim (m'',s'')$, dann gibt es nach Definition $t, t' \in S$, sodass
$$ts'm = tsm', t's''m' = t's'm''$$
und damit
$$tt's's''m = t's''(tsm') = ts(t's'm'') = tt's'sm''$$
womit $(m,s) \sim (m'',s'')$.

(ii) Sei $\frac{m}{s} = \frac{m'}{s'}$, $\frac{n}{t} = \frac{n'}{t'}$ in $S^{-1}M$, also $ums' = um's$, $vnt' = vn't$ für $u, v \in S$. Dann gilt nach Definition

$$\begin{aligned} \frac{m}{s} + \frac{n}{t} &= \frac{tm + sn}{st} &= \frac{s't'uv\,(tm + sn)}{uvtt'ss'} &=: p \\ \frac{m'}{s'} + \frac{n'}{t'} &= \frac{t'm' + s'n'}{s't'} &= \frac{stuv\,(t'm' + s'n')}{uvtt'ss'} &=: q \end{aligned}$$

Zu zeigen: $p = q$.

$$\begin{aligned} \frac{us'm}{ss'u} = \frac{usm'}{ss'u} &\implies \frac{s't'uvtm}{uvtt'ss'} = \frac{stuvt'm'}{uvtt'ss'} \\ \frac{vt'n}{tt'v} = \frac{vtn'}{tt'v} &\implies \frac{s't'uvsn}{uvtt'ss'} = \frac{stuvs'n'}{uvtt'ss'} \end{aligned}$$

und damit $p = q$

□

Beispiel 6.16. Sei V irreduzible affine Varietät, $A = k\,[V]\,, S = A \setminus \{0\}$. Dann ist

(i) $k\,(V) = Q\,(k\,[V]) = S^{-1}A$

(ii) $P \in V$, $\mathfrak{m}_P$ zugehöriges maximales Ideal, dann ist

$$\mathcal{O}_P = A_{\mathfrak{m}_P} = S_{\mathfrak{m}_P}^{-1}A$$

Bemerkung 6.17. (i) $A \to S^{-1}A$, $a \mapsto \frac{a}{1}$ ist im Allgemeinen nicht injektiv, zum Beispiel, wenn A Nullteiler hat.

(ii) S^{-1} ist ein Funktor: Sei $f : M \to N$ ein Homomorphismus von A-Moduln. Dann definiere

$$\begin{aligned} S^{-1}f :& S^{-1}M \to S^{-1}N \\ & \frac{m}{s} \mapsto \frac{f\,(m)}{s} \end{aligned}$$

Dies ist ein Homomorphismus von $S^{-1}A$-Moduln.

Lemma 6.18. *Sei $S \subseteq A$ multiplikatives System und*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

sei exakte Sequenz von A-Moduln. Dann ist

$$S^{-1}M_1 \xrightarrow{S^{-1}f} S^{-1}M_2 \xrightarrow{S^{-1}g} S^{-1}M_3$$

exakt (S^{-1} ist ein exakter Funktor*)*

Beweis. Es ist $g \circ f = 0$ und damit, für $\frac{m_1}{s} \in S^{-1}M_1$,

$$S^{-1}\,(g \circ f)\left(\frac{m_1}{s}\right) = \frac{(g \circ f)\,(m_1)}{s} = \frac{0}{s}$$

und somit $\operatorname{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Für $\frac{m_2}{s} \in \ker(S^{-1}g) \subseteq S^{-1}M_2$ gilt

$$\frac{g(m_2)}{s} = \frac{0}{1}$$

und damit $t1g(m_2) = ts0$ für ein $t \in S$. Da g A-linear ist, gilt

$$g(tm_2) = tg(m_2) = 0$$

und damit $tm_2 \in \ker(g) = \operatorname{im}(f)$. Es gibt also $m_1 \in M_1$ mit $f(m_1) = tm_2$. Also ist

$$S^{-1}f\left(\frac{m_1}{ts}\right) = \frac{f(m_1)}{ts} = \frac{tm_2}{ts} = \frac{m_2}{s}$$

womit $\operatorname{im}(S^{-1}f) = \ker(S^{-1}g)$ $\square$

Korollar 6.19. *Sei $I \lhd A$ Ideal, $S \subseteq A$ ein multiplikatives System, dann ist $S^{-1}I \lhd S^{-1}A$ ein Ideal. Es gilt $S^{-1}I = S^{-1}A$ genau dann, wenn $S \cap I \neq \emptyset$*

Beweis. Aus der Exaktheit von S^{-1} folgt, dass $S^{-1}I \subseteq S^{-1}A$ ein Untermodul und damit ein Ideal ist. Sei $S^{-1}I = S^{-1}A$, dies ist genau dann der Fall, wenn $\frac{s}{s} = \frac{1}{1} \in S^{-1}I$ genau dann, wenn $s \in I$ und damit $S \cap I \neq \emptyset$. $\square$

Lemma 6.20. *Sei A Ring, $\mathfrak{p} \lhd A$ Primideal, dann ist $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$ ein lokaler Ring mit maximalem Ideal $\mathfrak{m}_\mathfrak{p} = S_\mathfrak{p}^{-1}\mathfrak{p}$*

Beweis. $S_\mathfrak{p}^{-1}\mathfrak{p} \lhd A_\mathfrak{p}$ ist ein Ideal. Es ist $S_\mathfrak{p}^{-1}\mathfrak{p}$ maximal, genau dann, wenn $A_\mathfrak{p} \setminus S_\mathfrak{p}^{-1}\mathfrak{p} \subseteq A_\mathfrak{p}^*$, also wenn alle Elemente von $A_\mathfrak{p} \setminus S_\mathfrak{p}^{-1}\mathfrak{p}$ invertierbar sind. Sei $\frac{a}{s} \in A_\mathfrak{p} \setminus S_\mathfrak{p}^{-1}\mathfrak{p}$, also $a \in A \setminus \mathfrak{p} = S_\mathfrak{p}$, dann ist $\frac{s}{a}$ Inverses zu $\frac{a}{s}$. $\square$

Definition 6.21. Eine Eigenschaft von Ringen und deren Moduln heißt *lokal*, wenn sie nach Lokalisierung an allen Primidealen überprüft werden kann.

Satz 6.22. *Sei A Ring, M ein A-Modul. Dann sind äquivalent*

(i) $M = 0$

(ii) $M_\mathfrak{p} = 0$ *für alle Primideale* $\mathfrak{p} \lhd A$

(iii) $M_\mathfrak{m} = 0$ *für alle maximalen Ideale* $\mathfrak{m} \lhd A$

Also ist $M = 0$ eine lokale Eigenschaft.

Beweis. *(i)* $\Longrightarrow$ *(ii)* $\Longrightarrow$ *(iii)* ist klar. Angenommen $M \neq 0$ aber $M_\mathfrak{m} = 0$ für jedes maximale Ideal $\mathfrak{m} \lhd A$. Sei $0 \neq m \in M$. Definiere

$$I := \{a \in A \mid am = 0\} \lhd A$$

Dies ist ein Ideal. Dann ist I in einem maximalen Ideal $\mathfrak{m}$ enthalten. Also ist $M_\mathfrak{m} = 0$ und somit $\frac{m}{1} = \frac{0}{1}$. Somit gibt es ein $t \in S_\mathfrak{m} = A \setminus \mathfrak{m}$ mit $tm = 0$. Damit ist $t \in I \subseteq \mathfrak{m}$ im Widerspruch zu $t \in S_\mathfrak{m}$ $\square$

6.3 Lokale Ringe von Varietäten

Definition 6.23. Sei V affine Varietät, $P \in V$ mit maximalem Ideal $\mathfrak{m}_P \lhd k[V]$, dann heißt

$$\mathcal{O}_P = k[V]_{\mathfrak{m}_P}$$

lokaler Ring an P.

Bemerkung 6.24. Diese Definition stimmt mit der vorherigen für affine und irreduzible V überein.

Wir wollen Elemente von $\mathcal{O}_P$ als Funktionen auffassen. Sie haben die Form $\frac{f}{g}$ mit $f, g \in k[V]$ und $g(P) \neq 0$. Der Bruch definiert eine Abbildung

$$\begin{aligned} \frac{f}{g} :& U_g \to k \\ & Q \mapsto \frac{f(Q)}{g(Q)} \end{aligned}$$

Die Repräsentation als Bruch ist nicht eindeutig. Angenommen $\frac{f'}{g'} = \frac{f}{g}$. Definiert $\frac{f'}{g'}$ die gleiche Funktion auf $U_{g'} \cap U_g$? Nach Definition existiert ein $h \in k[V]$ mit

$$hgf' = hg'f, \ h(P) \neq 0$$

also gilt auf $U_h \cap U_g \cap U_{g'}$

$$\frac{f}{g} = \frac{hg'f}{hgg'} = \frac{hgf'}{hgg'} = \frac{f'}{g'}$$

als Abbildungen $U_h \cap U_g \cap U_{g'} \to k$

Definition 6.25. Sei V eine affine Varietät, $P \in V$. Ein *Funktionenkeim* in P ist eine äquivalenzklasse von Paaren (U, α) wobei $P \in U \subseteq V$ offen und $\alpha : U \to k$ eine Abbildung und

$$(U, \alpha) \sim (U', \alpha') :\Leftrightarrow \exists P \in W \subseteq U \cap U' \text{ offen}: \ \alpha|_W = \alpha'|_W$$

Wir schreiben α_P für die äquivalenzklasse von (U, α)

Bemerkung 6.26. Da jede offene Teilmenge von U eine standardoffene Teilmenge enthält, reicht es für U, U', W jeweils nur standardoffene Mengen zu betrachten.

Lemma 6.27. *Sei V affine Varietät, $P \in V$. Jedes Element von $\mathcal{O}_P$ definiert einen eindeutigen Funktionenkeim in P.*

Definition 6.28. Sei V affine Varietät, $U \subseteq V$ offen. Eine Abbildung $\alpha : U \to k$ heißt *algebraisch*, wenn der Keim von (U, α) für jeden Punkt $P \in U$ in $\mathcal{O}_P$ liegt. Es sei $\mathcal{O}(U)$ der Ring der algebraischen Funktionen.

Beispiel 6.29. Im Fall $V = U$ ist jedes Element von $k[V]$ algebraisch. Ist $f \in k[V]$ nicht nilpotent, so können wir $U = U_f$ betrachten. Jedes Element $\frac{a}{f^n} \in k[V]_f$ definiert eine algebraische Funktion $U_f \to k$.

Satz 6.30. *Sei V eine affine Varietät, $f \in k[V]$ nicht nilpotent. Dann ist die natürliche Abbildung $k[V]_f \to \mathcal{O}(U_f)$ ein bijektiver Ringhomomorphismus. Insbesondere $k[V] \xrightarrow{\sim} \mathcal{O}(V)$.*

Beweis.

Behauptung. Die Abbildung ist injektiv

Beweis. Sei $\frac{a}{f^n} \in k[V]_f$ mit $\frac{a}{f^n} = 0$ als Funktion $U_f \to k$. Das heißt

$$\frac{a(Q)}{f^n(Q)} = 0 \; \forall Q \in U_f$$

und somit

$$a(Q) = 0 \; \forall Q \in U_f$$

womit $V(a) \supseteq U_f$. Also

$$V(a \cdot f) = V(a) \cup V(f) \supseteq V$$

und damit

$$I(V) \supseteq I(V(a) \cup V(f)) \overset{4.1}{=} \sqrt{\langle a \cdot f \rangle}$$

In $k[V] = k[X_1, ..., X_n] / I(V)$ gilt $0 = \sqrt{\langle a \cdot f \rangle}$ und damit $a \cdot f = 0$. Also gilt in $k[V]_f$

$$\frac{a}{f^n} = \frac{af}{f^{n+1}} = 0$$

Behauptung. Die Abbildung ist surjektiv

Beweis. Sei $\varphi : U_f \to k$ eine algebraische Funktion, d.h. für jeden $P \in U_f$ ist der Keim von (U, φ) an P in $\mathcal{O}_P$. Also gibt es a_P, f_P, sodass der Keim von $\frac{a_P}{f_P}$ mit dem von (U_f, φ) übereinstimmt. Es gibt also eine standardoffene Menge U_g mit $P \in U_g$ auf der die Funktionen übereinstimmen. O.B.d.A sei $g = f_P$, sonst erweitere $\frac{a_P}{f_P}$ zu $\frac{g a_P}{g f_P}$. U_f ist quasi-kompakt und somit überdecken schon endlich viele U_{f_P} die Menge U_f. Wir haben $U_f = \bigcup_{i=1}^N U_{f_i}$ und $\varphi_i := \varphi|_{U_i}$ hat die Form $\frac{a_i}{f_i}$. Außerdem gilt als Funktionen auf $U_i \cap U_j = U_{f_i f_j}$

$$\frac{a_i f_j}{f_i f_j} = \varphi|_{U_{f_i f_j}} = \frac{a_j f_i}{f_i f_j}$$

wegen der Injektivität gilt dies auch in $k[V]_{f_i f_j}$.

Behauptung. Für $U_f = \bigcup_{i=1}^N U_{f_i}$ ist die Sequenz

$$0 \to k[V]_f \to \bigoplus_{i=1}^{N} k[V]_{f_i} \xrightarrow{\partial} \bigoplus_{i,j} k[V]_{f_i f_j}$$

exakt, wobei $\partial : \left(\frac{a_i}{f_i}\right)_i \mapsto \left(\frac{a_j}{f_j} - \frac{a_i}{f_i}\right)_{i,j}$.

Beweis. $k[V]_f \to \bigoplus_{i=1}^N k[V]_{f_i}$ ist injektiv, denn

$$\begin{array}{ccc}
k[V]_f & \longrightarrow & \bigoplus_{i=1}^N k[V]_{f_i} \\
\big\downarrow & & \big\downarrow \\
\mathcal{O}(U_f) & \longrightarrow & \bigoplus_{i=1}^N \mathcal{O}(U_{f_i})
\end{array}$$

kommutiert und die untere Abbildung ist auch injektiv. Sei nun $\left(\frac{a_i}{f_i}\right)_i \in k[V]_f \subseteq \bigoplus_{i=1}^N k[V]_{f_i}$ mit $\partial\left(\left(\frac{a_i}{f_i}\right)_i\right) = 0$. Das heißt, dass

$$\exists n \in \mathbb{N}: \; f_i^n f_j^n (a_i f_j - a_j f_i) = 0 \; \forall 1 \leq i, j \leq N$$

was dazu äquivalent ist, dass

$$f_j^{n+1}(a_i f_i^n) = f_i^{n+1}(a_j f_j^n)$$

Wir erweitern $\frac{a_i}{f_i}$ zu $\frac{a_i f_i^n}{f_i^{n+1}}$, das heißt, wir ersetzen f_i durch f_i^{n+1} und a_i durch $a_i f_i^n$. Dann gilt weiterhin $\varphi_i = \frac{a_i}{f_i}$ in U_{f_i}. Außerdem gilt

$$a_i f_j = a_j f_i \; \forall i, j \tag{$*$}$$

Wegen

$$\bigcup_{i=1}^N U_{f_i} = U_f \implies V(\langle f_1, ..., f_N \rangle) = \bigcap_{i=1}^N V(f_i) \subseteq V(f)$$

gilt nach Hilbertschem Nullstellensatz 4.1 somit $f \in \sqrt{\langle f_1, ..., f_N \rangle}$. Daher existiert ein $m \in \mathbb{N}$ und $b_i \in k[V]$ mit $f^m = \sum_{i=1}^N b_i f_i$. Sei $a = \sum_{i=1}^N b_i a_i$.

Behauptung. $\frac{a}{f^m}$ repräsentiert φ

Beweis.

$$f_j a = \sum_{i=1}^N b_i a_i f_j \overset{(*)}{=} \underbrace{\sum_{i=1}^N b_i f_i}_{f^m} a_j = f^m a_j$$

Also ist $\frac{a}{f^m} = \frac{a_j}{f_j} \; \forall j$ in U_{f_j} und $\frac{a}{f^m}$ repräsentiert φ.

□

Bemerkung 6.31. Ist V irreduzibel, so erhalten wir

$$\mathcal{O}(V) = \bigcap_{P \in V} \mathcal{O}_P \subseteq k(V)$$

wie zuvor.

Lemma 6.32. *A/I ist nilpotentfrei (*reduziert*) genau dann, wenn I reduziert ist ($I = \sqrt{I}$)*

Beweis. $f \in A$ mit $f^n \in I$ entsprechen $\overline{f} \in A/I$ mit $\overline{f}^n = 0$ □

Bemerkung 6.33. Sei V affine Varietät, dann ist $k[V]$ nilpotentfrei.

Beweis. $k[V] = k[X_1, ..., X_n]/I(V)$ und $I(V) = \sqrt{I(V)}$ □

7 Die Kategorie der quasi-affinen Varietäten

7.1 Der projektive Raum

Definition 7.1. Sei k ein Körper. Der *projektive Raum* $\mathbb{P}_k^n$ der Dimension n über k ist dpe Menge der eindimensionalen Unterräume des k^{n+1}.

Bemerkung 7.2. $\mathbb{P}_k^n$ ist die Menge der äquivalenzklassen $(k \setminus \{0\}) / \sim$ wobei

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) :\Leftrightarrow \exists \lambda \in k^\times : x_i = \lambda y_i \, \forall i \in \{0, ..., n\}$$

Wir schreiben $[x_0 : ... : x_n]$ für die äquivalenzklasse von $(x_0, ..., x_n)$. Wir nennen $x_0, ..., x_n$ die *homogenen Koordinaten* auf $\mathbb{P}_k^n$.

Definition 7.3. Für $i = 0, ..., n$ heißt die Teilmenge

$$U_i = \{[x_0 : ... : x_n] \mid x_i \neq 0\}$$

die *i-te standardoffene Karte*

Lemma 7.4. *(i) Auf U_i sind die Funktionen $y_j := \frac{x_j}{x_i}$ wohldefiniert und induzieren eine Bijektion*

$$\begin{aligned} \varphi_i : & U_i \to k^n \\ & [x_0 : ... : x_n] \mapsto (y_0, ..., y_{i-1}, y_{i+1}, ..., y_n) \end{aligned}$$

(ii) $\mathbb{P}_k^n \setminus U_i \cong \mathbb{P}_k^{n-1}$

(iii) $\mathbb{P}_k^n = \bigcup_{i=0}^n U_i$

Beweis. (i) Auf U_i kann durch x_i geteilt werden. Wegen $\frac{\lambda x_j}{\lambda x_i} = \frac{x_j}{x_i}$ ist y_j wohldefiniert. Sei

$$\begin{aligned} \psi_0 : & k^n \to U_i \\ & (a_0, ..., a_{i-1}, a_{i+1}, ..., a_n) \mapsto [a_0 : ... : a_{i-1} : 1 : a_{i+1} : ... : a_n] \end{aligned}$$

Dies ist die Umkehrabbildung zu φ

(ii) Das Komplement von U_i besteht aus den Punkten mit $x_i = 0$. Weglassen von x_i gibt Bijektion mit $\mathbb{P}_k^{n-1}$.

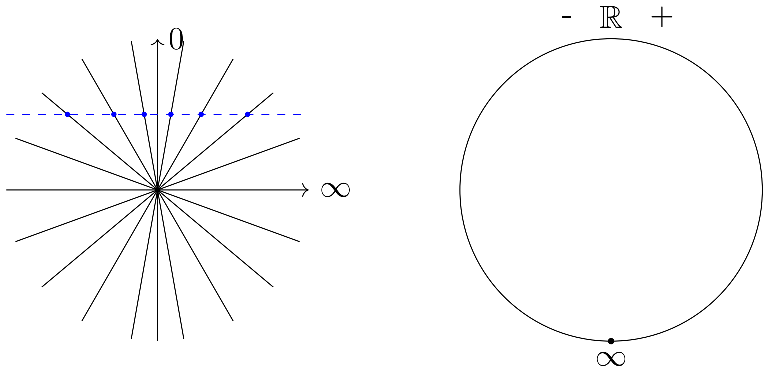
(iii) Nach Voraussetzung hat jeder Punkte $[x_0 : ... : x_n]$ ein $x_i \neq 0$ und liegt damit in U_i.

□

Bemerkung 7.5. Wir fassen $k^n \overset{\psi_0}{\hookrightarrow} \mathbb{P}_k^n$ als Teilmenge auf, unter der Bijektion φ_0.

Beispiel 7.6.$n = 0$ $\mathbb{P}_k^n$ besteht aus nur einem Punkt.

$n=2$ $\mathbb{P}^1_k = \underbrace{k}_{\{[1:a]\mid a\in k\}} \cup \underbrace{\{\infty\}}_{\{[0:1]\}}$. Für $k=\mathbb{R}$ ist $\mathbb{P}^1_{\mathbb{R}} \cup \{\infty\}$



Wir wollen algebraische Teilmengen von $\mathbb{P}^n_k$ als Nullstellen von Polynomen definieren. Der Funktionswert eines Polynoms ist jedoch nicht wohldefiniert, da die homogenen Koordinaten x_i nicht wohldefiniert sind.

Definition 7.7. Ein Polynom $P \in k[X_0,...,X_n]$ heißt *homogen von Grad d*, falls es die Form

$$P = \sum_{d_0+...+d_n=d} a_{d_0,...,d_n} X_0^{d_0} \cdot ... \cdot X_n^{d_n}$$

mit $a_{d_0,...,d_n} \in k$ hat.

Lemma 7.8. *Sei f homogen von Grad d und $(x_0,...,x_n) \in k^{n+1}, \lambda \in k^\times$, dann gilt*

$$f(\lambda x_0,...,\lambda x_n) = \lambda^d f(x_0,...,x_n)$$

Bemerkung 7.9. Für homogene Polynome ist der Funktionswert auf $\mathbb{P}^n_k$ also auch nicht wohldefiniert, aber die Eigenschaft von P, auf einer Geraden zu verschwinden ist wohldefiniert. Ist $f \in k[X_0,...,X_n]$ beliebiges Polynom, so schreiben wir es als

$$f = \sum_{d=0}^m f_d$$

mit f_d homogen von Grad d.

Definition 7.10. Sei $k=\overline{k}, S \subseteq k[X_0,...,X_n]$ Menge von Polynomen. Dann heißt

$$V(S) = \{P \in \mathbb{P}^n_k \mid f(P) = 0 \;\forall f \in S \text{ homogen}\}$$

die durch S definierte *projektive algebraische Menge*. Sei $V \subseteq \mathbb{P}^n_k$ Teilmenge, dann heißt

$$I(V) = \left\{ f = \sum_d f_d \in k[X_0,...,X_n] \;\middle|\; f_d(P) = 0 \;\forall P \in V, d \right\}$$

Verschwindungsideal von V. Wir nennen den Quotientenring

$$S[V] = k[X_0,...,X_n]/I(V)$$

homogenen Koordinatenring von V.

Beispiel 7.11. Sei $n = 2$. Für die projektive Ebene $\mathbb{P}_k^2$ benutzt man meist die Koordinaten $X = X_1$, $Y = X_2$, $Z = X_0$. Sei $f = X^2 + Y^2 + Z^2$. Um $V(f)$ zu verstehen, schneiden wir $V(f)$ mit den standardoffenen Mengen U_i.

$$\begin{aligned} V \cap U_0 &= \left\{[z : x : y] \mid z \neq 0, x^2 + y^2 + z^2 = 0\right\} \\ &\cong \left\{(x, y) \mid x^2 + y^2 = -1\right\} \subseteq \mathbb{A}_k^2 \end{aligned}$$

In $V \setminus (U_0 \cap V)$ liegen zwei Punkte $\left[0 : 1 : \sqrt{-1}\right], \left[0 : 1 : -\sqrt{-1}\right]$. Es gilt tatsächlich

$$I(V) = \left\langle X^2 + Y^2 + Z^2 \right\rangle$$

Nicht alle Elemente von $I(V)$ sind homogenen, sondern nur von der Form $g \cdot f$ mit g homogen. Nach Definition gilt $V(I(V)) = V$

Lemma 7.12. *Sei V eine projektive algebraische Menge. Wir nennen $Z \subseteq V$ abgeschlossen, wenn Z algebraisch ist. Dies definiert eine Topologie auf V.*

Beweis. Wie im affinen Fall. Das Produkt zweier homogener Polynome ist homogen. □

Definition 7.13. Sei $\mathbb{P}_k^n$ der projektive Raum zusammen mit seiner Topologie. Eine *projektive Varietät* ist eine algebraische projektive Menge $V \subseteq \mathbb{P}_k^n$ zusammen mit ihrer Topologie. Eine *quasi-projektive Varietät* ist eine offene Teilmenge einer projektiven Varietät mit induzierter Topologie.

Bemerkung 7.14. Wegen $U_i = \mathbb{P}_k^n \setminus \underbrace{V(X_i)}_{\cong \mathbb{P}_k^{n-1}}$ ist $U_i \subseteq \mathbb{P}_k^n$ offen.

7.2 Homogenisierung und Dehomogenisierung

Lemma 7.15. *Die Kartenabbildungen $\varphi_i : U_i \to \mathbb{A}^n$ sind Homöomorphismen.*

Beweis. Wir zeigen, dass φ_i eine Bijektion auf den Mengen der abgeschlossen Mengen definiert. Sei o.B.d.A $i = 0$. Sei $F \in k[X_0, ..., X_n]$ homogen und $V := V(F) \subseteq \mathbb{P}_k^n$. Dann gilt

$$V \cap U_0 = \{[1 : x_1 : ... : x_n] \mid F(1, x_1, ..., x_n) = 0\}$$

Das Bild dieser Menge unter φ_0 ist also $V(f)$ mit $f = F(1, X_1, ..., X_n)$. Da eine allgemeine abgeschlossene Menge endlicher Schnitt solcher $V(F)$ ist, ist das Bild jeder abgeschlossenen Menge wieder abgeschlossen. Sei umgekehrt $f \in k[X_1, ..., X_n]$ ein Polynom von Grad d. Sei F die *Homogenisierung* von f, das heißt

$$F = X_0^d f\left(\frac{X_1}{X_0}, ..., \frac{X_n}{X_0}\right)$$

Dann ist

$$V(F) \cap U_0 = \left\{[1 : x_1 : ... : x_n] \mid 1^d f(x_1, ..., x_n) = 0\right\}$$

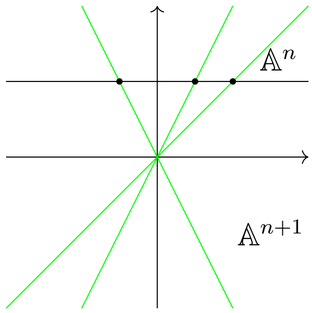
das gesuchte Urbild der abgeschlossenen Menge $V(f) \subseteq \mathbb{A}^n$. □

Beispiel 7.16. Sei $n = 2$ und $f = X^2 + 2XY + Y + 2$. Die Homogenisierung von f ist

$$\begin{aligned} F &= Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = Z^2\left(\frac{X^2}{Z^2} + 2\frac{X}{Z}\frac{Y}{Z} + \frac{Y}{Z} + 2\right) \\ &= X^2 + 2XY + YZ + 2Z^2 \end{aligned}$$

das heißt alle Monome von f werden mit Z-Faktoren zu Grad $d = 2$ aufgefüllt.

Bemerkung 7.17. Die beiden Operationen „Einsetzen von $X_0 = 1$“ und „Homogenisieren“ definieren eine Bijektion von homogenen Polynomen in $X_0, ..., X_n$ die nicht durch X_0 teilbar sind mit Elementen von $k[X_1, ..., X_n]$. Geometrisch entspricht dem eine Bijektion zwischen algebraischen Teilmengen von $\mathbb{A}^n$ und denjenigen Teilmengen von $\mathbb{A}^{n+1}$, die mit jedem Punkt auch die Ursprungsgerade durch den Punkt enthalten



Wir können den projektiven Raum und alle projektiven Varietäten mit Karten überdecken. Der Schnitt

$$U_i \cap U_j = \{[x_0 : ... : x_n] \mid x_i x_j \neq 0\}$$

$$\begin{tikzcd}
 & & \mathbb{P}^n & & \\
 & U_i \arrow[ur, phantom, "\subseteq"] \arrow[ddl, "\varphi_i"', "\sim"] & & U_j \arrow[ul, phantom, "\supseteq"] \arrow[ddr, "\varphi_j", "\sim"'] & \\
 & & U_i \cap U_j \arrow[ul, phantom, "\supseteq"] \arrow[ur, phantom, "\subseteq"] \arrow[dl, "\sim"'] \arrow[dr, "\sim"] & & \\
 \mathbb{A}^n \arrow[r, phantom, "\supseteq"] & U_{y_j} \arrow[rr, "\varphi_j \circ \varphi_i^{-1}", "\sim"'] & & U_{y_i} \arrow[r, phantom, "\subseteq"] & \mathbb{A}^n
\end{tikzcd}$$

wird unter φ_i abgebildet auf die Menge der Punkte $(y_0, ..., y_{i-1}, y_{i+1}, ..., y_n)$ mit $y_j \neq 0$, also mit $U_{y_j} \subseteq \mathbb{A}^n_{y_0,...,y_{i-1},y_{i+1},...,y_n}$. Die Kartenwechselabbildung

$$\varphi_j \circ \varphi_i^{-1} : U_{y_j} \to U_{y_i}$$

kann leicht berechnet werden. Wir geben die Formel für $i = 0, j = 1$ an:

$$\begin{aligned} \varphi_j \circ \varphi_i^{-1} : \qquad (y_1, ..., y_n) &\mapsto [1 : y_1, ..., y_n] \\ &= \left[\frac{1}{y_1} : 1 : \frac{y_2}{y_1} : ... : \frac{y_n}{y_1}\right] \\ &\mapsto \left(\frac{1}{y_1}, \frac{y_2}{y_1}, ..., \frac{y_n}{y_1}\right) \end{aligned}$$

jeder Eintrag ist eine algebraische Funktion auf U_{y_i}.

Bemerkung 7.18. Quasi-affine Varietäten sind quasi-projektive Varietäten.

Beweis.
$$U \subseteq V \xrightarrow[\varphi_0^{-1}]{\sim} V \subseteq U_0 \subseteq \mathbb{P}^n$$
□

7.3 Lokale Ringe und algebraische Funktionen

Sei V projektive Varietät, $F, G \in S[V] = k[X_0, ..., X_n]/I(V)$ homogen von gleichem Grad d. Dann ist für $P = [x_0 : ... : x_n]$ der Funktionswert
$$\frac{F}{G}(P) \coloneqq \frac{F(x_0, ..., x_n)}{G(x_0, ..., x_n)}$$
ist wohldefiniert falls $P \notin V(G)$

Definition 7.19. Sei V eine projektive Varietät mit homogenem Koordinatenring $S[V]$ und sei $P \in V$. Der lokale Ring von V in P sei definiert als
$$\mathcal{O}_P \coloneqq \left\{ \frac{F}{G} \;\middle|\; F, G \in S[V] \text{ von gleichem Grad, homogen, } G(P) \neq 0 \right\}$$
Ist V irreduzibel, so ist der der Funktionenkörper von V definiert als
$$k(V) = \left\{ \frac{F}{G} \;\middle|\; F, G \in S[V] \text{ homogen von gleichem Grad, } G \neq 0 \right\}$$

Lemma 7.20. *Sei $V \subseteq \mathbb{P}_k^n$ projektive Varietät, $P \in V$. Sei $U_i \subseteq \mathbb{P}_n^k$ eine standardoffene Karte mit $P \in U_i$. Dann gilt $\mathcal{O}_{V,P} \cong \mathcal{O}_{V \cap U_i, P}$ unter der Abbildung, die gegeben ist als Einsetzen von $X_i = 1$. Insbesondere ist also $\mathcal{O}_{V,P}$ ein lokaler Ring. Ist V irreduzibel, so gilt $k(V) \cong k(V \cap U_i)$. Insbesondere ist $k(V)$ ein Körper.*

Beweis. Sei o.B.d.A $i = 0$. Wir schreiben $V_0 \coloneqq U_0 \cap V$ für die affine Varietät. Wir zeigen zunächst, dass die Abbildung $\mathcal{O}_{V,P} \to \mathcal{O}_{V_0,P}$ surjektiv ist. Sei $\frac{f}{g} \in \mathcal{O}_{V_0,P}$ mit $f, g \in k[V_0], g(P) \neq 0$. Seien $\widetilde{f}, \widetilde{g} \in k[X_1, ..., X_n]$ Repräsentanten von f, g vom Grad d_f, d_g. Sei weiter $\widetilde{F}$ und $\widetilde{G}$ in $k[X_0, ..., X_n]$ deren Homogenisierung. Sei $F, G \in S[V]$ die äquivalenzklasse von $\widetilde{F}, \widetilde{G}$. Die Funktion $\frac{X_0^{d_g} F}{X_0^{d_f} G}$ ist das gesuchte Urbild von $\frac{f}{g}$. $X_0(P) \neq 0$, denn $P \in U_0$, $G(1, P) = g(P) \neq 0$. Zur Injektivität: Sei $\frac{F}{G} \in \mathcal{O}_{V,P}$ so, dass $\frac{F(1, X_1, ..., X_n)}{G(1, X_1, ..., X_n)} = 0$ in einer Umgebung U von P. Wir schreiben $f = F(1, X_1, ..., X_n), g = G(1, X_1, ..., X_n)$. Ohne Einschränkung ist $U = U_h$ mit $h \in k[V_0], h(P) \neq 0$. Sei H die Homogenisierung von h. Wir ersetzen G durch $H \cdot G$ und F durch $H \cdot F$. Also ohne Einschränkung $H = G$ und $\frac{f}{g}$ verschwindet auf U_g. Aus Sicht der Strukturtheorie der algebraischen Funktionen im affinen Fall (6.30) wissen wir, dass es eine Potenz von g mit $g^a f = 0$ gibt. Wir betrachten das homogene Polynom $G^a F \cdot X_0 \in S[V]$. Es verschwindet in $V(G) \cup V(X_0)$ und in U_g, also auf ganz V. Mit dem Hilbertschen Nullstellensatz 4.1 folgt $G^a F X_0 = 0$. Also gilt
$$\frac{F}{G} = \frac{X_0 G^a F}{X_0 G^{a+1}} = 0$$

Behauptung. Sei V irreduzibel, dann gilt $k(V) \cong k\left(\underbrace{V \cap U_i}_{V_i}\right)$

Beweis. Sei o.B.d.A $i = 0$. Da V irreduzibel ist, ist V_0 dicht in V und somit $\overline{V_0} = V$

$$\begin{array}{ccc} \mathbb{P}^n & \supseteq & U_0 \\ \cup\!\shortmid & & \cup\!\shortmid \\ V & \supseteq & V_0 \end{array}$$

Wir zeigen zunächst die Wohldefiniertheit von

$$\begin{gathered} k(V) \to k(V_0) \\ \frac{F}{G} \mapsto \frac{f}{g} \end{gathered}$$

Angenommen $g = 0$ in $k[V_0]$, dann verschwindet G auf V_0

$$g(a_1, ..., a_n) = G(1, a_1, ..., a_n)\ \forall (a_1, ..., a_n) \in V_0$$

und da $\overline{V_0} = V$ verschwindet G auf V und somit ist $G = 0$. Surjektivität wie im Fall $\mathcal{O}_P$. Zur Injektivität: Sei $\frac{F}{G} \in k(V)$ mit Bild $0 = \frac{f}{g} \in k(V_0)$, das heißt es gibt $0 \neq h \in k[V_0]$ mit $fh = 0$. Sei H die Homogenisierung von h. Es ist $H \neq 0$ in $S[V]$, also $HF = 0$ und $\frac{F}{G} = \frac{HF}{HG} = 0$

□

7.4 Der projektive Nullstellensatz

Definition 7.21. Ein Ideal $I \lhd k[X_0, ..., X_n]$ heißt *homogen*, wenn für jedes $f \in I$ auch $f_d \in I$ für jedes $d \geq 0$ wobei $f = \sum_{d \geq 0} f_d$ die Zerlegung in homogene Anteile ist.

Bemerkung 7.22. Ein homogenes Ideal ist von homogenen Elementen erzeugt, denn wenn $I = \langle f_1, ..., f_n \rangle$ homogen ist mit $f_1, ..., f_n \in k[X_1, ..., X_n]$ und $f_i = \sum_{d \geq 0} f_{i,d}$ und $D := \max_i \{\operatorname{grad} f_i\}$, dann gilt

$$I = \langle f_{i,d} \mid i = 1, ..., r,\ d = 0, ..., D \rangle$$

Wir wollen die Abbildungen V, I untersuchen

$$\{\text{homogene } I \lhd k[X_0, ..., X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{algebraische Mengen } V \subseteq \mathbb{P}^n\}$$

Bemerkung 7.23. Sei $S_+ := \langle X_0, ..., X_n \rangle \subsetneq S := \langle 1 \rangle$. Dies sind beides reduzierte Ideale, aber $V(S) = \emptyset = V(S_+)$. Dies ist ein Sonderfall, S_+ heißt das *irrelevante Ideal.* Die naive Verallgemeinerung des Nullstellensatzes vom affinen zum projektiven Fall ist also falsch.

Satz 7.24. *Sei I homogen mit $\emptyset \neq V(I) \subseteq \mathbb{P}^n$, dann gilt*

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

insbesondere ist $\sqrt{I}$ wieder homogen und wir erhalten eine inklusionsumkehrende Bijektion

$$\left\{\begin{array}{r}\textit{reduzierte homogene}\\ I\lhd k\left[X_0,...,X_n\right]\ \textit{ mit } I\neq S_+\end{array}\right\}\ \underset{I}{\overset{V}{\rightleftarrows}}\ \left\{\begin{array}{r}\textit{nichtleere projektive}\\ \textit{Varietäten in } \mathbb{P}^n\end{array}\right\}$$

$$\cup\!\mid \qquad\qquad\qquad\qquad \cup\!\mid$$

$$\{\textit{Primideale}\}\ \rightleftarrows\ \left\{\begin{array}{r}\textit{irreduzible nichtleere}\\ \textit{projektive Varietäten in } \mathbb{P}^n\end{array}\right\}$$

Beweis. Wie im affinen Fall ist der Beweis von $V\left(I\left(X\right)\right)=X$ für $\emptyset\neq X\subseteq\mathbb{P}^n$ völlig formal. Ebenso $I\left(V\left(J\right)\right)\supseteq\sqrt{J}$ für J homogen. Es bleibt die Gleichheit zu zeigen. Sei

$$\pi:\mathbb{A}^{n+1}\setminus\{0\}\to\mathbb{P}^n$$

die Projektion. Für $J\subseteq k\left[X_0,...,X_n\right]$ homogen schreiben wir nun $V^a\left(J\right)$ für die Verschwindungsmenge in $\mathbb{A}^{n+1}$. Da J homogen ist, gilt

$$\mathbb{A}^{n+1}\ni\left(a_0,...,a_n\right)\in V^a\left(J\right)\implies\left(\lambda a_0,...,\lambda a_n\right)\in V^a\left(J\right)\ \forall\lambda\in k$$

und

$$V\left(J\right)=\left(V^a\left(J\right)\setminus\{0\}\right)/\sim$$

wobei $\left(a_0,...,a_n\right)\sim\lambda\left(a_0,...,a_n\right)$. Also ist

$$\begin{aligned}V\left(J\right)=\emptyset&\Leftrightarrow V^a\left(J\right)\subseteq\{(0,...,0)\}\\ &\overset{4.1}{\Leftrightarrow}\sqrt{J}\supseteq\underbrace{\langle X_0,...,X_n\rangle}_{S_+}\end{aligned}$$

Im Fall $V\left(J\right)\neq\emptyset$ gilt

$$f\in I\left(V\left(J\right)\right)\Leftrightarrow f\in I\left(V^a\left(J\right)\right)\overset{4.1}{\Leftrightarrow}f\in\sqrt{J}$$

□

Bemerkung 7.25. $V^a\left(J\right)$ heißt *affiner Kegel* über $V\left(J\right)$.

7.5 Die Normtopologie auf $\mathbb{P}^n\left(\mathbb{R}\right)$, $\mathbb{P}^n\left(\mathbb{C}\right)$

Sei $k=\mathbb{R}$ oder $k=\mathbb{C}$. Wir betrachten

$$\mathbb{P}^n\left(k\right)\supseteq U_i\overset{\varphi_i}{\to}\mathbb{A}^n\left(k\right)=k^n$$

Definition 7.26. Erinnerung: *Normtopologie* auf $\mathbb{R}^n,\mathbb{C}^n$ ist die Topologie Mit Basis

$$B_\varepsilon\left(p\right):=\{q\in k^n\mid\|q-p\|\leq\varepsilon\}$$

für $p\in k^n,\varepsilon>0$

Betrachte die Kartenwechselabbildung

$$\begin{tikzcd}
 & U_i \arrow[dl, "\varphi_i"] & \supseteq & U_i \cap U_j \arrow[dl, "\sim"'] \arrow[dr, "\sim"] & \subseteq & U_j \arrow[dr, "\varphi_j"] & \\
k^n & \supseteq & k_j^n \arrow[rr, "\varphi_j \varphi_i^{-1}"] & & k_i^n & \subseteq & k^n
\end{tikzcd}$$

Die Abbildung $\varphi_j \varphi_i^{-1}$ ist komponentenweise gegeben durch $\frac{1}{x_j}$ oder $\frac{x_1}{x_j}$ mit $x_j \neq 0$ auf k_j^n. Diese Funktionen sind C^∞, insbesondere stetig bezüglich der Normtopologie. Damit ist $\varphi_j \varphi_i^{-1}$ Homöomorphismus bezüglich der Normtopologie. Also sind die Normtopologien der verschiedenen Karten miteinander verträglich und definieren eine Normtopologie auf $\mathbb{P}^n(k)$. Für $\mathbb{P}^n(\mathbb{R})$ heißt sie die *reelle Topologie*. Für $\mathbb{P}^n(\mathbb{C})$ die *komplexe Topologie*

Lemma 7.27. *$\mathbb{P}^n(\mathbb{R})$ und $\mathbb{P}^n(\mathbb{C})$ sind Hausdorffsch in der Normtopologie und Zariski-abgeschlossene Mengen sind Norm-abgeschlossen.*

Beweis. Sei $P, Q \in \mathbb{P}^n(K)$, $P \neq Q$, $P \in U_i$, $Q \in U_j$. Wenn $Q \in U_i$, also $P, Q \in k^n \cong U_i$, dann lassen sie sich trennen, da k^n Hausdorffsch ist. Sonst, wenn $Q \notin U_i$, dann sei C ein abgeschlossener Ball in U_i, der P enthält. Dann ist $\mathbb{P}^n(K) \setminus C$ offen und enthält Q, $\mathring{C}$ ist offen und enthält P. Des weiteren ist $\mathring{C} \cap \mathbb{P}^n(k) \setminus C = \emptyset$. Somit ist $\mathbb{P}^n(K)$ Hausdorffsch. Im $\mathbb{A}^n(k)$ sind Zariski-abgeschlossene Mengen als Nullstellenmengen von Polynomen gegeben. Da Polynome stetig in der Normtopologie sind, sind algebraische Mengen abgeschlossen in der Normtopologie. $\square$

Satz 7.28. *$\mathbb{P}^n(\mathbb{R})$ und $\mathbb{P}^n(\mathbb{C})$ sind kompakt und zusammenhängend.*

Beweis. Betrachte

$$\begin{aligned}\pi : & \mathbb{A}^{n+1}(k) \setminus \{0\} \twoheadrightarrow \mathbb{P}^n(k) \\ & (a_0, ..., a_n) \mapsto [a_0 : ... : a_n]\end{aligned}$$

Diese Abbildung ist stetig bezüglich der Normtopologie. Es reicht, dies für jede Karte zu zeigen. Also sei o.B.d.A $i = 0$

$$\begin{aligned}\overbrace{\{[a_0 : ... : a_n] \mid a_0 \neq 0\}}^{U_0} & \to k^n \\ [a_0 : ... : a_n] & \mapsto \left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right)\end{aligned}$$

und dies ist stetig. Betrachte

$$S^n = \left\{v \in \mathbb{R}^{n+1} \mid \|v\| = 1\right\} \subseteq \mathbb{R}^{n+1} \setminus \{0\}$$
$$S^{2n+1} = \left\{v \in \underbrace{\mathbb{C}^{n+1}}_{\cong \mathbb{R}^{2n+1}} \;\middle|\; \|v\| = 1\right\} \subseteq \mathbb{C}^{n+1} \setminus \{0\}$$

Die Abbildungen

$$S^n \hookrightarrow \mathbb{R}^{n+1} \setminus \{0\} \to \mathbb{P}^n(\mathbb{R})$$
$$S^{2n+1} \hookrightarrow \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n(\mathbb{C})$$

sind surjektiv, denn jede Gerade trifft S^n. Ist zum Beispiel $v \neq 0$, so ist $\frac{v}{\|v\|} \in S^n$. Weil $\mathbb{A}^n(k) \setminus \{0\} \to \mathbb{P}^n(k)$ stetig und jeweils $S^n \hookrightarrow \mathbb{R}^{n+1}$ und $S^{2n+1} \hookrightarrow \mathbb{C}^{n+1}$ stetig sind, sind also

$$S^n \twoheadrightarrow \mathbb{P}^n(\mathbb{R})$$
$$S^{2n+1} \twoheadrightarrow \mathbb{P}^n(\mathbb{C})$$

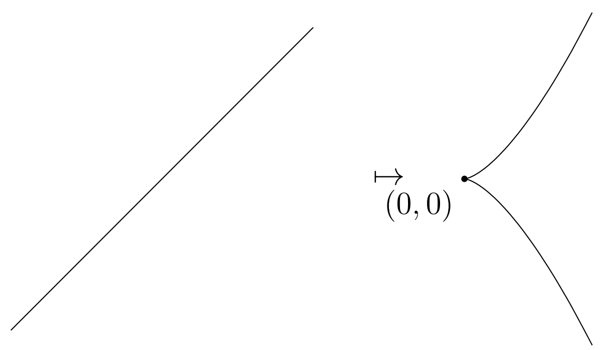
stetig. Da S^n und S^{2n+1} kompakt und zusammenhängend sind, sind dies somit auch $\mathbb{P}^n(\mathbb{R})$ und $\mathbb{P}^n(\mathbb{C})$. □

7.6 Algebraische Funktionen und Morphismen

Definition 7.29. Seien V, W quasi-affine Varietäten. Eine Abbildung $\alpha : V \to k$ heißt *algebraisch* in dem Punkt $P \in V$, wenn sie in $\mathcal{O}_P$ liegt. Das heißt, wenn es homogene $F, G \in S\left[\overline{V}\right]$ vom selben Grad gibt mit $G(P) \neq 0$ und $\alpha = \frac{F}{G}$ in einer offenen Umgebung von P. Ei *Morphismus von Varietäten* ist eine stetige Abbildung $\Phi : V \to W$, sodass für alle $P \in V$ und jede Funktion $\alpha : W \to k$ die algebraisch in $\Phi(P)$ ist, die Komposition $\alpha \circ \Phi : V \to W \to k$ algebraisch in P ist. In anderen Worten, es gilt $\Phi^* \mathcal{O}_{W,\Phi(P)} \subseteq \mathcal{O}_{V,P}$ wobei $\Phi^* : \alpha \mapsto \alpha \circ \Phi$. Ein Morphismus heißt *Isomorphismus*, wenn die Abbildung Φ bijektiv ist und die Umkehrabbildung ein Morphismus von Varietäten ist.

Bemerkung 7.30. In der Literatur findet sich oft der Begriff *regulär* statt *algebraisch*. Nicht jeder bijektive Morphismus ist ein Isomorphismus.

Beispiel 7.31. Sei $V = V(Y^2 - X^3) \subseteq \mathbb{A}^2$. Dann ist $\mathbb{A}^1 \to V, t \mapsto (t^2, t^3)$ bijektive und algebraisch (also Morphismus) aber kein Isomorphismus (betrachte an $(0,0)$ die Wurzelfunktion).



Quasi-projektive Varietäten bilden eine Kategorie:

Satz 7.32. *Die Verknüpfung von Morphismen von Varietäten sind wieder Morphismen.*

Beweis. Seien $X \subseteq \mathbb{P}^r, Y \subseteq \mathbb{P}^s, Z \subseteq \mathbb{P}^t$ quasi-projektiv. Seien $\Phi : X \to Y, \Psi : Y \to Z$ Morphismen. Dann ist $\Psi \circ \Phi : X \to Z$ stetig. Sei $P \in X$ und $\alpha : Z \to k$ algebraisch in $(\Psi \circ \Phi)(P)$. Dann ist $\alpha \circ \Psi = \Psi^* \alpha$ algebraisch in $\Phi(P) \in Y$

$$\begin{tikzcd}
X \arrow[r, "\Phi"] & Y \arrow[r, "\Psi"] & Z \arrow[d, "\alpha"] \\
P \arrow[u, phantom, "\rotatebox{90}{$\in$}"] & & k
\end{tikzcd}$$

Dann ist wiederum $\alpha \circ \Psi \circ \Phi$ algebraisch in P, weil Φ Morphismus ist. Daher ist $\Psi \circ \Phi$ ein Morphismus. □

Wir wollen besser verstehen, welche Beispiele und Eigenschaften von Morphismen es gibt. Beginnen wir mit dem affinen Fall.

Lemma 7.33. *Sei V affine Varietät, $U_f \subseteq V$ standardoffen mit $f \in k[V]$. Sei $\alpha \in \mathcal{O}(U_f)$, dann ist α stetig und Morphismus $\alpha : U_f \to k$. Es gilt*

$$k[V]_f = \mathcal{O}(U_f) = \operatorname{Mor}\left(U_f, \mathbb{A}^1\right)$$

Beweis. Sei $\alpha = \frac{g}{f^n}$, $g, f \in k[V]$. Wir müssen zeigen, dass Urbilder abgeschlossener Mengen wieder abgeschlossen sind. Es genügt, das Urbild von einem Punkt $\{a\} \subseteq \mathbb{A}^1$ zu betrachten. Dies besteht aus den Punkten P in U_f mit der Eigenschaft, dass $\alpha(P) = \frac{g(P)}{f(P)^n} = a$. Dies ist die Verschwindungsmenge von $g - af^n$ und damit abgeschlossen. α ist ein Morphismus. Sei nun umgekehrt ein Morphismus $\alpha \in \operatorname{Mor}(U_f, \mathbb{A}^1)$ gegeben. Wir gehen die Definition durch: Für jeden Punkt $P \in U_f$ ist $\mathrm{id} : k \to k$ ein Element von $\mathcal{O}_{k,\alpha(P)}$ - gegeben durch das Polynom X - und somit ist $\alpha^* \mathrm{id} = \alpha \in \mathcal{O}_{V,P}$. Damit ist aber $\alpha \in \mathcal{O}(U_f)$. □

Lemma 7.34. *Sei V quasi-affin, $f_1, ..., f_n \in \mathcal{O}(V)$, dann ist*

$$\begin{aligned}\Phi : & V \to \mathbb{A}^n \\ & P \mapsto (f_1(P), ..., f_n(P))\end{aligned}$$

Morphismus.

Beweis. Wir prüfen, dass Urbilder abgeschlossener Mengen abgeschlossen sind. Sei $V(g) \subseteq \mathbb{A}^n$ abgeschlossen. Dann ist

$$\begin{aligned}\Phi^{-1}(V(g)) &= \left\{ P \in V \;\middle|\; \underbrace{g(f_1(P), ..., f_n(P))}_{\text{Polynom}} = 0 \right\} \\ &= V(h), \; h := g(f_1, ..., f_n)\end{aligned}$$

Mit dem gleichen Argument (Einsetzen von Polynom in algebraische Funktion ist wieder algebraische Funktion) ist Φ verknüpft mit $\alpha : \mathbb{A}^n \to k$ algebraisch für α algebraisch. Somit ist Φ Morphismus. □

Satz 7.35. *Seien $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$ affine varietäten. Eine Abbildung $\Phi : V \to W \subseteq \mathbb{A}^m$ ist genau dann ein Morphismus, wenn alle Koordinatenfunktionen $\Phi_1, ..., \Phi_m : V \to \mathbb{A}^1$ von Φ Elemente von $k[V]$ sind.*

Beweis. Die Projektionsabbildungen

$$\begin{aligned}p_i : & \mathbb{A}^m \to A^1 \\ & (a_1, ..., a_m) \mapsto a_i\end{aligned}$$

auf die $i$te Koordinate wird durch das Polynom $X_i \in k[X_1, ..., X_n]$ definiert, ist also ein Morphismus von Varietäten nach Lemma 7.33. Dann ist auch $\Phi_i = p_i \circ \Phi$ Morphismus $V \to \mathbb{A}^1$, also, nach Lemma 7.33 Element von $\mathcal{O}(V) = k[V]$. Sei umgekehrt $\Phi = (\Phi_1, ..., \Phi_m)$ mit $\Phi_i \in k[V]$ und $\Phi(P) \in W$ für alle $P \in V$. Nach Lemma 7.34 ist $\Phi : V \to \mathbb{A}^m$ ein Morphismus. Da $W \subseteq \mathbb{A}^m$ abgeschlossen ist, ist auch $\Phi : V \to W$ ein Morphismus. □

Bemerkung 7.36. Man kann den Satz leicht umformulieren zu der Aussage, dass ein Morphismus $f : V \to W$ das selbe ist, wie ein k-Algebra-Homomorphismus $f^* : \mathcal{O}(W) \to \mathcal{O}(V)$.

Lemma 7.37. *Sei $U_i \subseteq \mathbb{P}^n$ die ite standardoffene Teilmenge. Dann ist die Kartenabbildung $\varphi_i : U_i \to \mathbb{A}^n$ ein Isomorphismus von quasi-projektiven Varietäten*

Beweis. Wir haben bereits gesehen, dass φ_i ein Homöomorphismus ist. Auf lokalen Ringen haben wir zudem den Isomorphismus $\mathcal{O}_{U_i,P} \xrightarrow{\sim} \mathcal{O}_{\mathbb{A}^n,\varphi(P)}$ nachgewiesen. Also ist φ_i ein Isomorphismus. $\square$

Satz 7.38. *Sei $V \subseteq \mathbb{A}^n$ affin, $g \in k[V]$. Dann ist die Abbildung*

$$\begin{aligned} \Phi : &V(gX_{n+1} - 1) \subseteq \mathbb{A}^{n+1} \to U_g \\ &(a_1, ..., a_{n+1}) \mapsto (a_1, ..., a_n) \end{aligned}$$

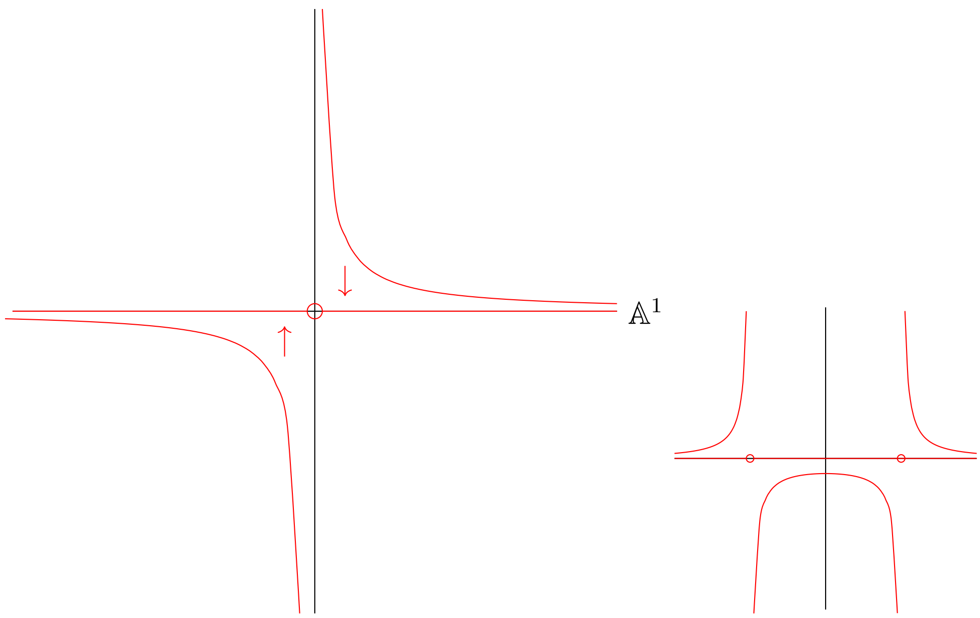
ein Isomorphismus von Varietäten.

Beweis. Wegen $g(a_1, ..., a_n)\, a_{n+1} = 1$ auf $V(gX_{n+1} - 1)$ hat die Abbildung Φ Werte in U_g. Nach dem letzten Lemma ist die Komposition $\widetilde{\Phi} : V(gX_{n+1} - 1) \to U_g \subseteq \mathbb{A}^n$ ein Morphismus und somit insbesondere stetig. Somit ist Φ stetig. Die Bedingung an lokale Ringe folgt für Φ aus der Bedingung von $\widetilde{\Phi}$, weil $U_g \subseteq V$ offen ist. Für jeden Punkt in U_g gibt es genau ein Urbildpunkt. Die Umkehrabbildung ist

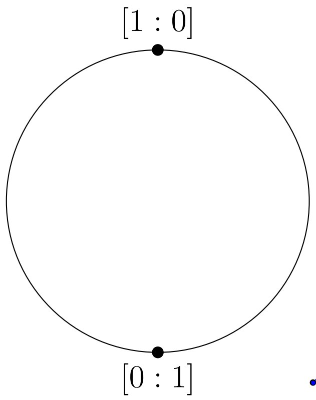
$$(a_1, ..., a_n) \mapsto \left(a_1, ..., a_n, \frac{1}{g(a_1, ..., a_n)}\right)$$

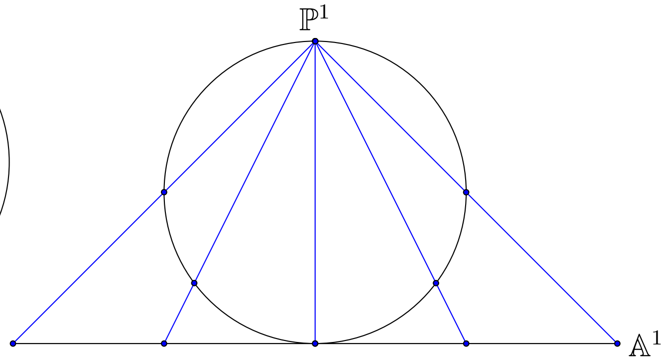
$\square$

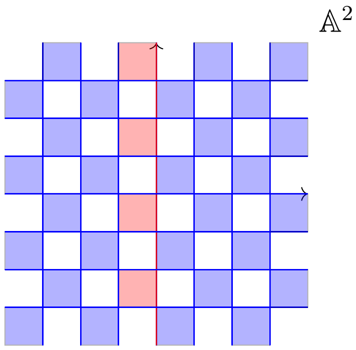
Beispiel 7.39. Offene Varietäten sind Varietäten in (möglicher Weise anderem $\mathbb{A}^m$)

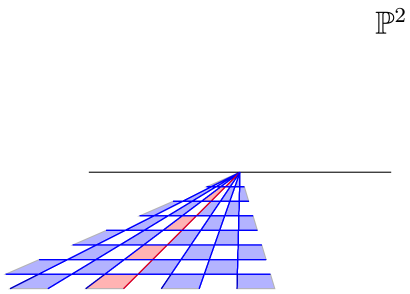


Beispiel 7.40. Projektive Varietäten.



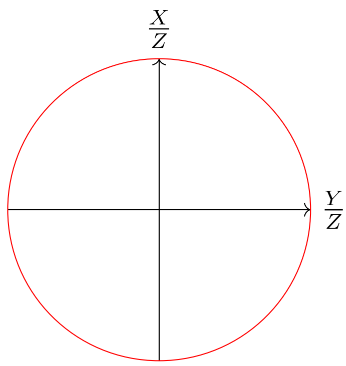




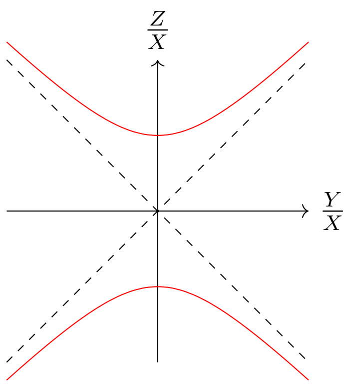


Wir betraten $X^2 + Y^2 = Z^2$.

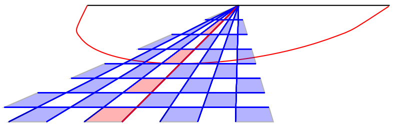
$Z \neq 0 \;\; 1 = \left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}^2\right) = 1$



$X \neq 0 \;\; 1 = \left(\frac{Y}{X}\right)^2 - \left(\frac{Z}{X}\right)^2$. Im affinen



Im projektiven:



Korollar 7.41. *Sei $X \subseteq \overline{X} \subseteq \mathbb{P}^n$ quasi-projektiv.*

(i) X hat eine endliche offene überdeckung

$$X = \bigcup_{i=1}^{m} X_i$$

mit X_i affin.

(ii) Die affinen Teilmengen von X bilden eine Basis der Topologie von X.

Beweis. (i) Es ist

$$\underbrace{X \cap U_i}_{\text{quasi-affin}} \subseteq \underbrace{\overline{X} \cap U_i}_{\text{affin}} \subseteq \mathbb{A}^n$$

Wir haben

$$\begin{aligned} X \cap U_i &= \left(\overline{X} \cap U_i\right) \setminus V\left(f_1, ..., f_k\right) \\ &= \bigcup_{j=1}^{k} \underbrace{\left(\overline{X} \cap U_i\right) \setminus V\left(f_j\right)}_{\text{standard offen, damit affin}} \end{aligned}$$

Insgesamt kann man X durch $(N+1) \cdot k = m$ affine Varietäten überdecken.

(ii) Sei $U \subseteq X$ offen. Dann ist U offen in $\mathbb{P}^n$ und somit quasi-projektiv in $\mathbb{P}^n$. Somit ist nach erstem Teil

$$U = \bigcup_{i=1}^{m} U_i$$

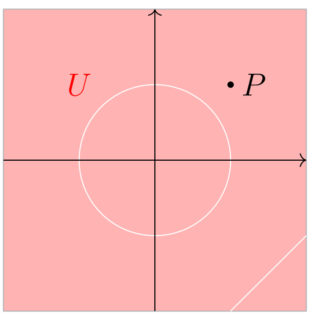
mit U_i affin.

□

Beispiel 7.42. Es ist

$$\mathcal{O}_P\left(V\right) = \left\{ \frac{f}{g} \,\middle|\, g\left(P\right) \neq 0 \right\}$$

im projektiven mit f, g homogen von gleichem Grad. Alle lokalen Eigenschaften von quasi-projektiven Varietäten lassen sich im affinen nachrechnen. Für $V \subseteq \mathbb{A}^n$ quasi-affin ist $\mathcal{O}\left(V\right) = \bigcap_{P \in V} \mathcal{O}_P$.

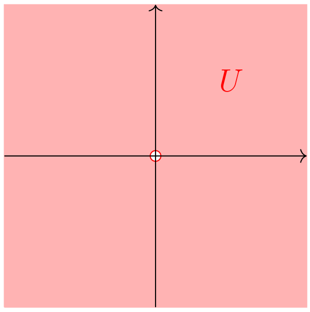


$\frac{1}{X^2+Y^2-1} \in \mathcal{O}_P$, $\frac{1}{X^2+Y^2-1} \in \mathcal{O}(U)$. Es kann notwendig sein, zwei unterschiedliche Brüche zu nehmen. Zum Beispiel sind für

$$V(XY - ZW) =: V$$

die Brüche $\frac{X}{Z}$ und $\frac{W}{Y}$ gleich, denn $XY - ZW = 0$. Jedoch sind nicht beide überall definiert.

Satz 7.43. *Die quasi-affine Varietät $U = \mathbb{A}^2 \setminus \{0\}$ ist nicht affin.*



Beweis. Wir haben einen Morphismus $\Phi : U \to A^2$. Für affine Varietäten gilt mit $\Psi : V \to W \to k$, $\Psi^* : k[W] \to k[V]$, dass Ψ genau dann Isomorphismus ist, wenn Ψ^* Isomorphismus ist. Wir rechnen $\mathcal{O}(\mathbb{A}^2)$ und $\mathcal{O}(U)$ aus. Wir wissen $\mathcal{O}(\mathbb{A}^2) = k[X, Y]$. Für $\mathcal{O}(U)$ überdecken wir U durch standard offene $U = U_X \cup U_Y$. Wir wissen

$$\mathcal{O}(U_X) = k[X, Y]_X = \left\{ \frac{f}{X^n} \;\middle|\; f \in k[X, Y] \right\}$$

$$\mathcal{O}(U_Y) = k[X, Y]_Y = \left\{ \frac{g}{Y^n} \;\middle|\; g \in k[X, Y] \right\}$$

Sei $\alpha \in \mathcal{O}(U)$ beliebig. Wir können α als $\alpha = \frac{f}{X^n}$ auf U_X und als $\alpha = \frac{g}{Y^m}$ auf U_Y schreiben. Auf $U_X \cap U_Y$ ist dann

$$\frac{f}{X^n} = \alpha = \frac{g}{Y^m} \in \mathcal{O}(U_{XY}) = k[X, Y]_{XY}$$

Somit ist

$$0 = \frac{f}{X^n} - \frac{g}{Y^m} = \frac{fY^m - X^n g}{X^n Y^m}$$

und damit

$$fY^m - X^n g = 0 \implies fY^m = X^n g$$

Aus der Eindeutigkeit der Primfaktorzerlegung in Polynomringen gilt somit $X^n | f, Y^m | g$, also $f = X^n h, g = Y^m h'$. Also

$$hX^n Y^m = h' X^n Y^m \implies h = h'$$

und daher

$$h = \frac{X^n h}{X^n} = \frac{f}{X^n} = \alpha = \frac{g}{Y^m} = \frac{hY^m}{Y^n} = h \in k[X, Y]$$

womit

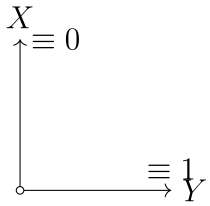
$$\mathcal{O}(U) = k[X, Y]$$

Also $\mathcal{O}(\mathbb{A}^2) = \mathcal{O}(U)$. Wäre U affin, wäre $U = \mathbb{A}^2$. $\square$

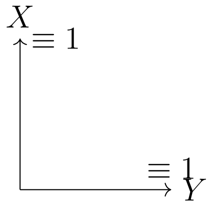
Satz 7.44 (Identitätssatz)**.** *Sei X irreduzibel, $f, g \in \mathcal{O}(X)$ und $f|_U = g|_U$ für eine offene Teilmenge $U \subseteq X$, dann ist $f = g$ auf ganz X.*

Beweis. Wir betrachten $V(f-g)$. Da $f|_U = g|_U$ gilt $U \subseteq \overbrace{V(f-g)}^{\text{abgeschlossen}}$. Also gilt auch $\overline{U} \subseteq V(f-g)$. Da X irreduzibel und offen ist, gilt $\overline{U} = X$. Also ist $X \subseteq V(f-g)$ und damit $f = g$ auf X. $\square$

Bemerkung 7.45. Sei X irreduzibel, $f, g \in \mathcal{O}(X)$. Wenn $f|_U = g|_U$ für $U \subseteq X$ offen, $U \neq \emptyset$, dann ist $f = g$. Im irreduziblen Fall haben also Funktionskeime (U, f) einen eindeutigen maximal großen Definitionsbereich. Zum Beispiel ist $\frac{X}{Y} \in k(X, Y)$ definiert auf $U_Y \subseteq \mathbb{A}^2$. Dies gilt nicht für im reduziblen Fall. Für $V = V(XY) \subseteq \mathbb{A}$ ist mit
$f = \frac{x}{x+y}$



$g = 1$



$f|_{U_x} = g|_{U_x}$.

Definition 7.46. Sei X irreduzible quasi-projektive Varietät, $\Phi \in \mathbb{P}^n(k(X)), P \in X$, dann heißt Φ *regulär* in P, falls es einen Repräsentanten $\Phi = [\Phi_0 : ... : \Phi_n]$ gibt, sodass alle Φ_i für $i \in \{0, ..., n\}$ definiert sind in P und nicht alle gleichzeitig verschwinden. In diesem Fall, setze $\Phi(P) \coloneqq [\Phi_0(P) : ... : \Phi_n(P)] \in \mathbb{P}_k^n$

Bemerkung 7.47. $\Phi(P)$ ist wohldefiniert. Gilt $[\Phi_0 : ... : \Phi_n] = [\Phi_0' : ... : \Phi_n']$ und beide Repräsentanten sind regulär in P, so ist $\Phi_i = \Psi \cdot \Phi_i'$ für ein $\Psi \in k(X)^\times$ für $i \in \{0, ..., n\}$. Es gibt einen Index i mit $\Phi_i'(P) \neq 0$ und somit $\Psi(P) = \Phi_i(P)\Phi_i'(P)^{-1} \in k$, also ist Ψ regulär in P. Wäre $\Psi(P) = 0$, so wäre $\Phi_j(P) = 0 \; \forall j$. Also ist $\Psi(P) \neq 0$ und damit $\Phi(P) = \Phi'(P) \in \mathbb{P}^n$.

Satz 7.48. *Sei X irreduzible quasi-projektive Varietät, $Y \subseteq \mathbb{P}_k^n$ quasi-projektiv. Ein Element $\Phi \in \mathbb{P}^n(k(X))$ definiert genau dann einen Morphismus $\Phi : X \to Y$, wenn Φ in allen Punkten $P \in X$ regulär ist und $\Phi(P) \in Y \; \forall P \in X$. Jeder Morphismus $f : X \to Y$ ist von dieser Form.*

Beweis. Sei $\Phi \in \mathbb{P}^n(k(X))$ regulär in allen $P \in X$ und $\Phi(P) \in Y \; \forall P \in X$. Wir überprüfen, dann Φ ein Morphismus ist. O.B.d.A. (durch übergang zu affiner überdeckung) sind X, Y affin und $Y \subseteq U_0$. Nach Voraussetzung ist dann $\Phi_0(P) \neq 0 \; \forall P \in X$. Wir gehen über zu $\Phi_i' = \Phi_i / \Phi_0$ für $i \in \{0, ..., n\}$. Nach Voraussetzung ist Φ_i' algebraisch. Damit ist $\Phi' : X \to \mathbb{A}^n$ ein Morphismus von affinen Varietäten. Nach Voraussetzung faktorisiert Φ' über $Y \subseteq \mathbb{A}^n$. Also ergibt $\Phi' : X \to Y$ einen Morphismus. Nun betrachten wir die Rückrichtung. Für die

Komposition

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[rr, bend left, "\Psi"] & Y \arrow[r] & \mathbb{P}^n \\
\cup\vert & & \cup\vert \\
V_i = \Psi^{-1}(U_i) \arrow[rr, "\Psi|_{V_i}"] & & U_i
\end{tikzcd}$$

gibt es ein i mit $V_i \neq \emptyset$, denn die U_i überdecken $\mathbb{P}^n$, V_i liegt dicht in X, also $k(X) = k(V_i)$. Nun ist $\Psi|_{V_i}$ ein Morphismus $V_i \to \mathbb{A}^n$, also gegenben durch ein Tupel $\Phi_0^i, ..., \Phi_{i-1}^i, \Phi_{i+1}^i, ..., \Phi_n^i$. Wir fassen $\Phi_0^i, ..., \Phi_n^i \in k(X)$ auf und setzen

$$\Psi^i := \left[\Phi_0^i : ... : 1 : ... : \Phi_n^i\right]$$

Die verschiedenen Φ^i sind kompatibel und somit ergeben sie ein wohldefiniertes Element in $\mathbb{P}^n(k(X))$. Das Resultat gilt, denn $P \in X$ impliziert, dass es ein i gibt mit $P \in V_i$. □

Bemerkung 7.49. In vielen klassischen Texten wird $\Phi \in \mathbb{P}^n(k(X))$ für die Definition des Begriffs des Morphismus benutzt. Damit muss man sich jedoch auf X irreduzibel einschränken.

8 Hilbertscher Nullstellensatz und Dimensionentheorie

Zurück zu affiner Geometrie. Wir werden zeigen, dass $\dim \mathbb{A}^n = n$ und den Hilbertschen Nullstellensatz beweisen.

8.1 Endliche Morphismen

Sei $\varphi : A \to B$ ein Ringhomomorphismus, $b_1, ..., b_n \in B$. Wir schreiben $A[b_1, ..., b_n]$ für den Unterring von B, der von $\varphi(A)$ und $b_1, ..., b_n$ erzeugt wird.

Bemerkung 8.1. A ist nicht unbedingt Unterring von $A[b_1, ..., b_n]$. Dies ist der Fall, wenn φ nicht injektiv ist. Außerdem ist dies kein Polynomring, denn die b_i können Relationen haben.

Definition 8.2. Sei $f : A \to B$ Ringhomomorphismus, dann

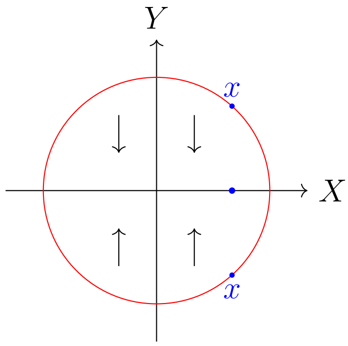
(i) B heißt *endlich* über A, wenn B endlich erzeugter A-Modul ist.

(ii) Ein Element $b \in B$ heißt *ganz* über A, falls $A[b]$ endlich erzeugter A-Modul ist.

(iii) B heißt *ganz* über A, falls alle Elemente von B ganz über A sind.

Definition 8.3. Ein Morphismus $f : X \to Y$ von quasi-projektiven Varietäten heißt *endlich*, wenn es eine offene überdeckung $Y = U_1 \cup ... \cup U_n$ gibt, sodass $f^{-1}(U_i)$ affin ist und $k[f^{-1}(U_i)]$ endlich über $k[U_i]$.

Beispiel 8.4. (i) Sei $A = k[X], B = k[X,Y]/f$ mit $f = X^2 + Y^2 - 1$. Dann wird B als A-Modul von $1, Y \bmod f$ erzeugt, also ist B endlich über A.



(ii) Sei $A = \mathbb{Z}, B = \mathbb{Z}\left[\sqrt{3}\right]$, dann wir B als A-Modul von 1 und $\sqrt{3}$ erzeugt, also ist $A \to B$ endlich.

(iii) Sei $A = k[X], B = k[X,Y]$, dann ist B endlich erzeugte A-Algebra aber nicht als A-Modul, denn $1, Y, Y^2, Y^3, ...$ ist eine A-Basis von B. Die Ringerweiterung ist nicht endlich.

(iv) Sei $A = k$ ein Körper, dann ist B endlich über A genau dann, wenn $\dim_K B < \infty$.

Bemerkung 8.5. (i) Ist in Beispiel (iv) auch $B = L$ ein Körper und $\dim_k B < \infty$, so spricht man von einer *endlichen Körpererweiterung* L/K.

(ii) In der algebraischen Zahlentheorie betrachtet man $A = \mathbb{Z}$ und B Menge der ganzen Elemente in $k/\mathbb{Q}$ mit $k/\mathbb{Q}$ endliche Körpererweiterung. Man zeigt B ist ein Ring, der endlich über $A = \mathbb{Z}$ ist.

Lemma 8.6. *Sei $f : A \to B$ endlicher Ringhomomorphismus.*

(i) Sei $g : B \to C$ endlich, dann ist $g \circ f$ endlich.

(ii) Seien $I \lhd A, J \lhd B$ Ideale mit $f(I) \subseteq J$, dann ist $\overline{f} : A/I \to B/J$ endlich.

(iii) Sei $S \subseteq A$ multiplikativ, dann ist $S^{-1}f : S^{-1}A \to S^{-1}B$ endlich.

Beweis. Sei $b_1, ..., b_n$ Erzeugendensystem von B als A-Modul

(i) Ist $c_1, ..., c_m \in C$ ein Erzeugendensystem von C als B-Modul, so ist $(g(b_i)\,c_j)_{ij}$ Erzeugendensystem von C als A-Modul.

(ii) Die Restklassen der b_i modulo J sind Erzeugendensystem von B/J als A/I-Modul.

(iii) Die Elemente $\frac{b_1}{1}, ..., \frac{b_n}{1}$ sind Erzeugendensystem von $S^{-1}B$ als $S^{-1}A$-Modul.

□

Lemma 8.7. *Sei $A \to B$ ein Ringhomomorphismus, $b \in B$ ist ganz über A genau dann, wenn b Nullstelle eines normierten Polynoms $F \in A[X]$ ist.*

Beweis. Sei $F = X^n + a_1X^{n-1} + ... + a_n \in A[X]$ mit Nullstelle b, also $F(b) = 0$.
Behauptung. $1, b, ..., b^{n-1}$ erzeugen $A[b]$ als A-Modul.

Beweis. Wir haben
$$b^n = -a_1 b^{n-1} - ... - a_n$$
und somit $b \in \langle 1, b, ..., b^{n-1} \rangle$. Per Induktion:
$$b^{n+k} = -a_1 b^{n+k-1} - ... - a_n b^k \in \left\langle 1, b, ..., b^{n-1} \right\rangle$$

Andersherum sei $A[b]$ endlich erzeugt von $b_1, ..., b_r \in A[b]$,
$$b_i = \sum_{j=0}^{k_i} a_{ij} b^j$$
Sei b^N maximale Potenz von b, die in den b_i vorkommt, dann ist, da $b^{N+1} \in \langle b_1, ..., b_r \rangle$ und somit
$$b^{N+1} = \sum_{i=1}^{r} a_i b_i = \sum_{i=1}^{r} a_i \sum_{j=0}^{k_i} a_{ij} b^j$$
und somit ist b Nullstelle von $F = X^{N+1} - \sum_{i=0}^{r} a_i \sum_{j=0}^{k_i} a_{ij} X^j$. □

Lemma 8.8. *Sei k ein Körper und $k \to E$ endliche k-Algebra mit E nullteilerfrei, dann ist E ein Körper.*

Beweis. Sei $y \in E \setminus \{0\}$ und sei
$$\begin{aligned} \varphi_y : & E \to E \\ & e \mapsto e \cdot y \end{aligned}$$
die Multiplikation mit y. Wegen $1 \cdot y = y \neq 0$ ist φ_y nicht die Nullabbildung. Sei
$$\chi = \sum_{i=0}^{m} b_i X^i$$
mit $b_i \in k$ das charakteristische Polynome von φ_y. Nach dem Satz von Cayley-Hamilton gilt $\chi(\varphi_y) = 0$. Also ist
$$0 = \chi(\varphi(1)) = \sum_{i=0}^{m} b_i y^i$$
Sei o.B.d.A $b_0 \neq 0$ andernfalls erhalten wir aus
$$y \cdot \sum_{i=0}^{m-1} b_{i+1} y^i = 0$$
wegen der Nullteilerfreiheit die Relation
$$\sum_{i=0}^{m-1} b_{i+1} y^i = 0$$
Sei weiterhin o.B.d.A $b_0 = 1$. Dann haben wird
$$y \left(\sum_{i=1}^{m} b_i y^{i-1} \right) + 1 = 0$$
und somit ist $-\sum_{i=1}^{m} b_i y^{i-1}$ invers zu y. □

Satz 8.9 (Going-Down)**.** *Sei $f : A \to B$ ein endlicher Ringhomomorphismus, $P \subsetneq Q$ Primideale von B. Dann sind $f^{-1}(P) \subsetneq f^{-1}(Q)$ verschiedene Primideale. Insbesondere gilt* $\dim B \leq \dim A$.

Beweis. Urbilder von Primidealen sind immer Primideale. Es gilt klar $f^{-1}(P) \subseteq f^{-1}(Q)$. Angenommen $f^{-1}(P) = f^{-1}(Q) = \mathfrak{p}$

Behauptung. Wir können annehmen, dass A lokal mit maximalem Ideal $\mathfrak{p}$ ist.

Beweis. Sei $S = S_{\mathfrak{p}} = A \setminus \mathfrak{p}$. Wir lokalisieren an S. Dann ist $S^{-1}A = A_{\mathfrak{p}}$ lokal mit maximalem Ideal $S^{-1}\mathfrak{p}$. Primideale in $S^{-1}A$ entsprechen Primidealen in A, die von S disjunkt sind. Es ist $0 \notin f(S)$, da $S \cap \mathfrak{p} = \emptyset$ und $\mathfrak{p} = f^{-1}(P)$. Weiter gilt $\underbrace{S^{-1}B}_{\text{Als } A\text{-Modul}} = \underbrace{f(S)^{-1}B}_{\text{Als } B\text{-Modul}}$. Wegen $f(S) \cap P = \emptyset, f(S) \cap Q = \emptyset$ bleibt $S^{-1}P \subsetneq S^{-1}Q$ echte Inklusion, wenn $P \subsetneq Q$. Der Ringhomomorphismus $A_{\mathfrak{p}} \to S^{-1}B$ ist endlich nach Lemma 8.6. Also können wir annehmen, dass A lokal mit $\mathfrak{p}$ maximal ist.

Behauptung. Wir können annehmen, dass A Körper ist.

Beweis. Wir betrachten

$$A/\mathfrak{p} \to B/B\mathfrak{p}$$

Dies ist endlich nach Lemma 8.6 und $A/\mathfrak{p}$ ist ein Körper, da $\mathfrak{p}$ maximal ist. Wir haben $B\mathfrak{p} \subseteq P \subsetneq Q$ und somit ist $P/B\mathfrak{p} \subsetneq Q/B\mathfrak{p}$.

Sei somit $A = k$ Körper und B endliche k-Algebra. Wir betrachten

$$k \to B/P \to B/Q$$

B/P und B/Q sind nullteilerfrei, da P und Q Primideale sind. Nach Lemma 8.1 sind B/P und B/Q Körper. Da $B/P \to B/Q$ surjektiv ist, muss diese Abbildung somit Isomorphismus sein und daher gilt $P = Q$.
Die Dimensionsaussage $\dim B \leq \dim A$ folgt direkt, denn die Urbilder einer Primidealkette in B bilden eine Primidealkette gleicher Länge in A. Die Gleichheit gilt im Allgemeinen nicht. □

Beispiel 8.10. Sei $A = k[X,Y]$ und $B = k[X,Y]/f$ für f irreduzibel. Dann ist A/B endlich, aber es gilt - wie wir später sehen werden - $\dim A = \dim \mathbb{A}^2 = 2$, aber $\dim B = \dim V(f) = 1$.

Satz 8.11 (Going-Up)**.** *Sei $f : A \to B$ injektiver endlicher Ringhomomorphismus, A und B nullteilerfrei, $\mathfrak{p} \subsetneq \mathfrak{q}$ Primideale von A, P ein Primideal von B mit $A \cap P = \mathfrak{p}$, dann existiert ein Primideal $Q \triangleleft B$ mit $P \subsetneq Q$ und $Q \cap A = \mathfrak{q}$. Insbesondere gilt* $\dim A = \dim B$. *Hier identifizieren wir A mit $f(A)$.*

Beweis. Zur Dimension: Nach Satz 8.9 gilt $\dim A \geq \dim B$. Jede kette von Primidealen in A lässt sich induktiv zu einer Kette in B hochheben und somit gilt $\dim A \leq \dim B$.
Wir lokalisieren an $\mathfrak{q}$: Sei $S = S_{\mathfrak{q}} = A \setminus \mathfrak{q}$. Dies ist eine multiplikative Menge in A und nach Injektivität auch in B. Somit ist $S^{-1}f : A_{\mathfrak{q}} \to S^{-1}B$ injektiver endlicher Ringhomomorphismus. Es reicht also, die Behauptung in diesem Fall zu zeigen, denn für ein Primideal $\widetilde{Q} \triangleleft S^{-1}B$, das $S^{-1}P$ und $S^{-1}\mathfrak{q}$ enthält, ist $\widetilde{Q} = S^{-1}Q$ für ein Q und Q erfüllt die Aussage des Satzes.
Sei somit o.B.d.A $\mathfrak{q}$ maximal. Wie im letzten Beweis betrachten wir $A/\mathfrak{p} \to B/P$. Dies ist

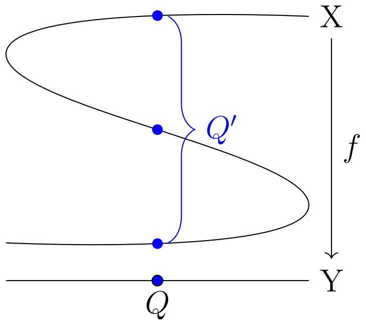
in endlicher, injektiver Ringhomomorphismus. Sei nun $\overline{Q}$ maximales Ideal von B/P, das $\mathfrak{q}/\mathfrak{p}$ enthält. Das Urbild Q von $\overline{Q}$ hat die gewünschte Eigenschaft, denn

$$\underbrace{A/\mathfrak{q}}_{\text{Körper}} \xrightarrow{\text{endlich}} \underbrace{B/Q}_{\text{Körper}} = (B/\mathfrak{q})\,/\overline{Q}$$

wobei B/Q nach Lemma Körper ist. Da Abbildungen von Körpern immer injektiv sind, gilt $Q \cap A = \mathfrak{q}$ □

Korollar 8.12. *Sei $f : X \to Y$ endlicher Morphismus von affinen Varietäten so, dass $k[Y] \to k[X]$ injektiv ist, dann ist f surektiv und* $\dim X = \dim Y$

Beweis. Zur Surjektivität: Sei $Q \in Y$, dann hat das maximale Ideal $I(Q)$ eine Hebung zu einem Primideal $P \triangleleft k[X]$. Sei $Q' \in V(P)$, also $I(Q') \supseteq P \supseteq I(Q)$. Dann gilt $f(Q') = Q$.



$$P := I(Q')$$

$$\begin{tikzcd}
g \circ f & \in & k[X] & \supseteq & P \\
g \arrow[u] & \in & k[Y] \arrow[u, "f^*"] & \supseteq & I(Q)
\end{tikzcd}$$

□

8.2 Transzendenzgrad und seine Eigenschaften

In diesem Abschnitt arbeiten wir mit nullteilerfreien endlich erzeugten k-Algebren.

Definition 8.13. Sei A eine nullteilerfreie k-Algebra. Eine Menge$\{a_1, ..., a_n\} \subseteq A$ heißt *algebraisch abhängig* über k, wenn es ein Polynom $0 \neq P \in k[X_1, ..., X_n]$ gibt mit $(a_1, ..., a_n)$ als Nullstelle. Eine maximale algebraisch unabhängige Teilmenge von A heißt *Transzendenzbasis*. Die Kardinalität einer Transzendenzbasis heißt *Transzendenzgrad* $\operatorname{trdeg}_K A$ von A über k.

Bemerkung 8.14. Oft wird diese Definition nur für Körper betrachtet. Eine Transzendenzbasis von A über k ist auch Transzendenzbasis des Quotientenkörpers $Q(A)$ über k, denn a und $\frac{1}{a}$ sind algebraisch abhängig wegen des Polynoms $X_1X_2 - 1$

Beispiel 8.15. Sei $A = k[X_1, ..., X_n]$ der Polynomring, dann sind $X_1, ..., X_n$ algebraisch unabhängig. Tatsächlich ist $X_1, ..., X_n$ eine Transzendenzbasis von A über k. In k ist $a \in k \setminus \{0\}$ schon algebraisch abhängig, denn es ist Nullstelle von $X - a$.

Definition 8.16. Für $a_1, ..., a_n \in A$ bezeichnen wir mit $k[a_1, ..., a_n]$ den kleinsten Unterring von A, der k und $a_1, ..., a_n$ enthält. Es ist

$$k[a_1, ..., a_n] = \left\{ \sum_{(i_1,...,i_n)}^{\text{endlich}} b_{i_1,...,i_n} a_1^{i_1} \cdot ... \cdot a_n^{i_n} \,\middle|\, b_{i_1,...,i_n} \in k \right\} \subseteq A$$

Mit $k(a_1, ..., a_n)$ bezeichnet man den Quotientenkörper von $k[a_1, ..., a_n]$

$$k(a_1, ..., a_n) \subseteq Q(A)$$

Lemma 8.17. *Sei A nullteilerfreie k-Algebra. Sei $a_1, ..., a_n \in A$. Dann ist die Menge*

$$\overline{k[a_1, ..., a_n]} := \left\{ a \in A \;\middle|\; \begin{array}{r} \{a\} \text{ ist algebraisch} \\ \text{abhängig über } k(a_1, ..., a_n) \end{array} \right\}$$

ein Teilring von A.

Beweis. Jedes Element $a \in k[a_1, ..., a_n]$ erfüllt eine Polynomgleichung

$$a - P(a_1, ..., a_n) = 0$$
$$X - P(a_1, ..., a_n) = 0$$

Seien nun a, b algebraisch über $k(a_1, ..., a_n)$ (das heißt, $\{a\}, \{b\}$ jeweils algebraisch abhängig). Somit erfüllen a, b Polynomgleichungen mit Koeffizienten in $k_1 := k(a_1, ..., a_n)$. Also

$$\dim_{k_1} k_1[a] < \infty, \ \dim_{k_1[a]} k_1[b] < \infty$$

und damit auch

$$\dim_{k_1} k_1[a, b] < \infty$$

Sei $c \in k_1[a, b]$. nach Lemma 8.7 erfüllt c eine normierte Polynomgleichung über k_1, also ist $\{c\}$ algebraisch abhängig über k_1. □

Beispiel 8.18. Sei $f = X^2 + Y^2 \in k[X, Y]$ und $A = k[X, Y] / \langle f \rangle = k[x, y]$ wobei $x = X \bmod \langle f \rangle$,$y = Y \bmod \langle f \rangle$. Dann ist $\{x, y\}$ algebraisch abhängig, aber $\{x\}$ ist algebraisch unabhängig. $\overline{k[x]} = A$, $\operatorname{trdeg}_k A = 1, y \notin k[x]$ aber $y \in \overline{k[x]}$

Satz 8.19. *Sei A nullteilerfreie k-Algebra.*

(i) Jede algebraisch unabhängige Menge lässt sich zu einer Transzendenzbasis ergänzen.

(ii) Jedes System von Algebraerzeugern enthält eine Transzendenzbasis.

(iii) Der Transzendenzgrad ist wohldefiniert.

Beweis. Wie für Vektorräume mit algebraischer Abhängigkeit statt linearer Abhängigkeit. □

8.3 Nullstellensatz

Satz 8.20 (Noethernormalisierung). *Sei k ein Körper, B endlich erzeugte nullteilerfreie k-Algebra vom Transzendenzgrad $\operatorname{trdeg}_k B = d$. Dann existieren $x_1, ..., x_d \in B$ die algebraisch unabhängig über k sind, sodass B endlich über $k[x_1, ..., x_d]$ ist. Mit anderen Worten, es existiert ein endlicher injektiver Ringhomomorphismus*

$$\begin{aligned} k[X_1, ..., X_n] &\to B \\ X_i &\mapsto x_i \end{aligned}$$

Bemerkung 8.21. (i) $k[X_1, ..., X_d]$ und B haben den gleichen Transzendenzgrad d und Dimension wegen Going-Up 8.11.

(ii) Sei V eine irreduzible affine Varietät. Nach Noethernormalisierung 8.20 existiert ein endlicher surjektiver Morphismus

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

wobei $d = \operatorname{trdeg} k[V]$ und $\dim V = \dim \mathbb{A}^d$.

Beweis von 8.20. Es ist $B = k[Y_1, ..., Y_m]/\mathfrak{p}$ für ein Primideal $\mathfrak{p}$. Sei $y_i := Y_i \bmod \mathfrak{p}$. Falls $m = d$, dann sind $y_1, ..., y_m$ algebraisch unabhängig und $\mathfrak{p} = 0$. Somit ist $B = k[Y_1, ..., Y_m]$. Für $d < m$ zeigen wir die Aussage per Induktion nach m. Es genügt also zu zeigen, dass $B' \subseteq B$ existiert, sodass B endlich über B' ist und B' als k-Algebra von $m-1$ Elementen erzeugt wird. Da $m > d$ existiert eine Polynomrelation $0 \neq f \in k[Y_1, ..., Y_m]$ mit $f \in \mathfrak{p}$ und $f(y_1, ..., y_m) = 0$. Seien $r_2, ..., r_m \in \mathbb{N}$. Setze $z_i := y_i - y_1^{r_i}$ für $i \in \{2, ..., m\}$. Dann gilt $f(y_1, z_2 + y_1^{r_2}, ..., z_m + y_1^{r_m})$. Also ist $(y_1, z_2, ..., z_m)$ Nullstelle von

$$F(Y_1, Z_2, ..., Z_m) := f(Y_1, Z_2 + Y_1^{r_1}, ..., Z_m + Y_1^{r_m}) \in k[Y_1, Z_2, ..., Z_m]$$

Ein Monom $a \prod Y_i^{b_i}$ in f induziert mehrere Terme in F, unter anderem den führenden Term in Y_1:

$$aY_1^{b_1 + r_2 b_2 + ... + r_m b_m}$$

Wenn die r_i groß genug sind und weit genug auseinander liegen, dann haben alle resultierenden Monome unterschiedliche Grade in Y_1. Eines davon hat den höchsten Grad

$$bY_1^N + \text{kleinere Terme bezüglich } Y_1$$

Dann ist $b^{-1}F(Y_1, z_2, ..., z_m)$ eine normierte Gleichung für Y_1 über $k[z_2, ..., z_m]$. Wir setzen

$$B' = k[z_2, ..., z_m] \subseteq k[z_2, ..., z_m][y_1] = B$$

Nach Lemma 8.7 ist y_1 ganz über $k[z_2, ..., z_m]$ und somit ist B endlich über B' $\square$

Satz 8.22 (Körpertheoretischer Nullstellensatz)**.** *Sei k ein Körper und $k \to E$ eine endlich erzeugte k-Algebra. Wenn E ein Körper ist, dann ist E eine endliche Erweiterung von k.*

$$\dim_k E < \infty$$

Beweis. Sei $d = \operatorname{trdeg}_k E$. Nach der Noethernormalisierung 8.20 ist E eine endliche Erweiterung von $k[X_1, ..., X_d]$. Nach Going-Up 8.11 ist

$$0 = \dim E = \dim k[X_1, ..., X_d] \geq d$$

und somit ist $d = 0$. Also ist E endlich über k. $\square$

Beweis des schwachen Nullstellensatzes 4.6. Sei k algebraisch abgeschlossen, $I \lhd k[X_1, ..., X_n]$ maximales Ideal, dann ist $E = k[X_1, ..., X_n]/I$ eine endlich erzeugte k-Algebra und da I maximal ist, ist E ein Körper. Nach vorherigem Satz 8.22 ist $\dim_k E < \infty$.

Behauptung. Es gilt $E = k$

Beweis. Sei $y \in E$, dann ist $k[y]$ endlich über k, also ist y Nullstelle eines nicht-trivialen Polynoms $f \in k[X]$. Da k algebraisch abgeschlossen ist, zerfällt f in Linearfaktoren

$$f = (X - a_1) \cdot ... \cdot (X - a_d)$$

Somit ist y Nullstelle eines der Linearfaktoren, o.B.d.A des ersten, und somit gilt $y = a_0 \in k$.

Sei nun a_i das Bild von X_i in E, also $a_i = X_i \bmod I$, also ist

$$\underbrace{\langle X_1 - a_1, ..., X_n - a_n\rangle}_{\text{maximal}} \subseteq \underbrace{I}_{\text{maximal}}$$

Weil $E = k$ gilt somit $I = \langle X_1 - a_1, ..., X_n - a_n\rangle$. □

8.4 Dimension

Lemma 8.23. *Seien $P \subsetneq Q$ Primideale von $k[X_1, ..., X_n]$, dann gilt*

$$\operatorname{trdeg} k[X_1, ..., X_n]/Q < \operatorname{trdeg} k[X_1, ..., X_n]/P$$

Beweis. Der Homomorphismus

$$k[X_1, ..., X_n]/P \to k[X_1, ..., X_n]/Q$$

ist surjektiv und somit sind Elemente, die modulo P algebraisch abhängig sind auch modulo Q algebraisch abhängig. Es gilt also

$$\operatorname{trdeg} k[X_1, ..., X_n]/Q \leq \operatorname{trdeg} k[X_1, ..., X_n]/P$$

Angenommen $\operatorname{trdeg} k[X_1, ..., X_n]/Q = \operatorname{trdeg} k[X_1, ..., X_n]/P$. Sei $\alpha_i := X_i \bmod P$, $\beta_i := X_i \bmod Q$. Sei o.B.d.A $\beta_1, ..., \beta_r$ eine Transzendenzbasis von $k[\beta_1, ..., \beta_r]$ dann sind die Urbilder $\alpha_1, ..., \alpha_r$ auch algebraisch unabhängig und wegen der Gleichheit der Transzendenzgrade eine Transzendenzbasis von $k[\alpha_1, ..., \alpha_r]$. Nun lokalisieren wir. Sei $S = k[X_1, ..., X_r] \setminus \{0\}$. Dies ist eine multiplikative Menge. Es gilt $S \cap P = S \cap Q = \emptyset$, da $X_1, ..., X_r$ algebraisch unabhängig modulo P beziehungsweise Q sind. Sei

$$\begin{aligned} E = S^{-1}k[X_1, ..., X_r] &= k(X_1, ..., X_r) \\ &= k(\alpha_1, ..., \alpha_r) \\ &= k(\beta_1, ..., \beta_r) \end{aligned}$$

und $S^{-1}k[X_1, ..., X_n]/P = E[\alpha_{r+1}, ..., \alpha_n]$. Hierin sind $\alpha_{r+1}, ..., \alpha_n$ algebraisch über E. Nach Lemma 8.1 ist $E[\alpha_1, ..., \alpha_n]$ ein Körper. Also ist $S^{-1}P$ ein maximales Ideal. Es gilt aber

$$S^{-1}P \subsetneq S^{-1}Q \subsetneq S^{-1}k[X_1, ..., X_n]$$

wegen $S \cap Q = \emptyset$ im Widerspruch zur Maximalität von $S^{-1}P$. □

Satz 8.24. *Sei A nullteilerfreie, endlich erzeugte k-Algebra und k ein Körper, dann gilt* $\dim A = \operatorname{trdeg}_k A$. *Insbesondere gilt* $\dim \mathbb{A}^n = n$

Beweis. Nach Noethernormalisierung 8.20 existiert eine injektive endliche Ringerweiterung

$$K[X_1, ..., X_d] \hookrightarrow A$$

Mit Going-Up 8.11 ist somit

$$\dim A = \dim k[X_1, ..., X_d] \geq d = \operatorname{trdeg} A$$

Sei $A = k[X_1, ..., X_n]/P$ für P prim.

Behauptung. $\dim A \leq \operatorname{trdeg}_k A$.

Beweis. Sei $\{0\} = \overline{Q_0} \subsetneq ... \subsetneq \overline{Q_{\dim A}}$ eine maximale Kette von Primidealen. Sei Q_i das Urbild von $\overline{Q_i}$ in $k[X_1, ..., X_n]$, insbesondere $Q_0 = P$. Nach vorherigem Lemma 8.23 gilt

$$\operatorname{trdeg} \underbrace{k[X_1, ..., X_n] / Q_0}_{A} > \operatorname{trdeg} k[X_1, ..., X_n] / Q_1 > ... > \operatorname{trdeg} k[X_1, ..., X_n] / Q_{\dim A} \geq 0$$

und somit $\operatorname{trdeg} A \geq \dim A$

□

Beispiel 8.25. Sei $f \in k[X, Y]$ irreduzibel. Dann ist $\operatorname{trdeg}_k k[X, Y] / \langle f \rangle = 1$ und somit gilt $\dim V(f) = 1$. Diese Varietäten heißen *affine ebene Kurven*.

Korollar 8.26. *Sei $V \subseteq \mathbb{P}^n$ eine quasi-projektive Varietät mit irreduziblen Komponenten $V_1, ..., V_m$, dann gilt*

$$\dim V = \max_i \operatorname{trdeg} k(V_i) \leq n$$

Beweis. Es ist

$$\dim V = \max_i \dim V_i$$

Somit genügt es, die Aussage für V irreduzibel zu zeigen. Sei $n = \dim V$. Für eine Kette

$$W_0 \subsetneq W_1 \subsetneq ... \subsetneq W_n = V$$

vom irreduziblen W_i, quasi-projektiv betrachten wir eine affine Karte U, die W_0 enthält. Dann ist $U_i = W_i \cap U \neq \emptyset$ affin und wir haben eine Kette

$$U_0 \subsetneq U_1 \subsetneq ... \subsetneq U_n = U$$

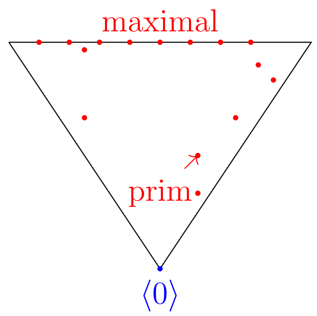
von affinen Varietäten und somit

$$\dim U \geq \dim V$$

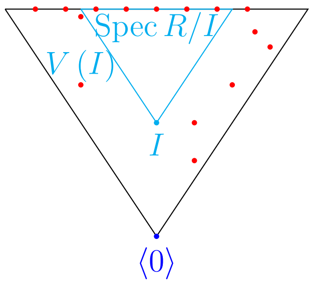
Andererseits bekommen wir für jede Kette in U eine Kette in V durch abschließen. Also $\dim U \leq \dim V$ und damit

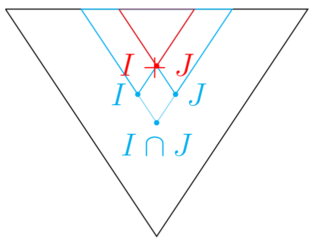
$$\dim V = \dim U = \operatorname{trdeg} k(U) = \operatorname{trdeg} k(V)$$

□

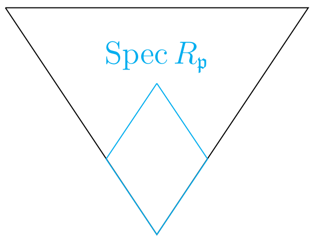


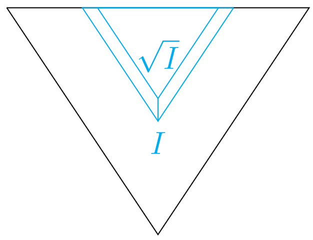
Spec $R = \{\mathfrak{p} \subseteq R \mid \mathfrak{p} \text{ prim}\}$



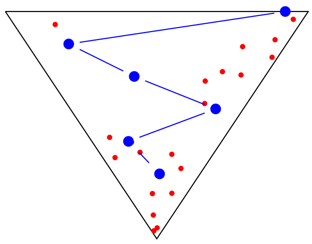


$$\begin{tikzcd}
& I+J & \\
I \arrow[ur, hook] & & J \arrow[ul, hook'] \\
& I\cap J \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

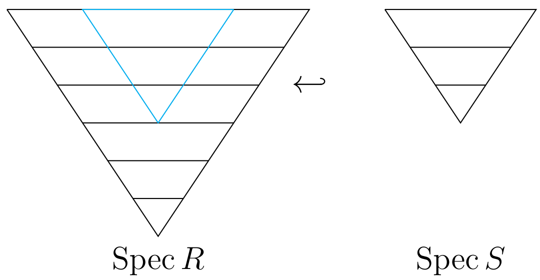




Krulldimension

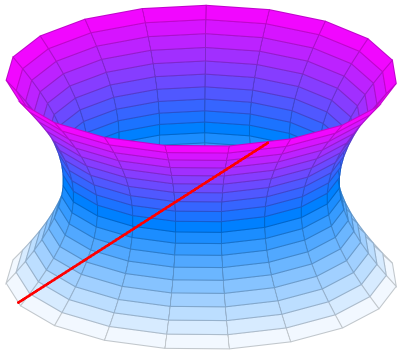


$$f : R \twoheadrightarrow S$$



Bemerkung 8.27. Nicht jedes Ideal von Kodimension 1 wird durch eine Gleichung beschrieben. Es gibt eindimensionale Ringe, die nicht faktoriell sind.

Beispiel 8.28.

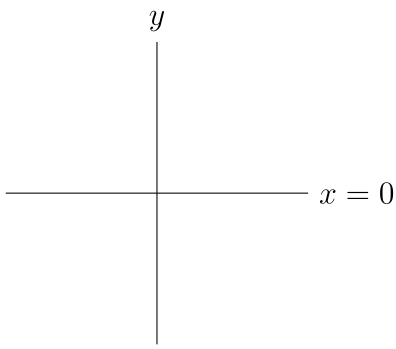


Theorem (Krullscher Hauptidealsatz)**.** *Sei X eine irreduzible Varietät, $g : X \to \mathbb{A}^1$ ein nicht konstanter Morphismus, $Z \subseteq V(g)$ eine irreduzible Komponente. Dann gilt*

$$\dim Z = \dim X - 1$$

Bemerkung 8.29. Irreduzibel ist Notwendig.

Beispiel 8.30. $V = V(XY), \dim V = 1$. Dann ist $I(V \cap V(X)) = \langle XY, X \rangle = \langle X \rangle$ und $\dim V \cap V(X) = 1$.



Lemma 8.31. *Sei $A = k[X_1, ..., X_d]$, $A \to B$ endlich und injektiv, B Integritätsring, $b \in B$. Dann ist b Nullstelle eines normierten Polynoms $F = T^m + a_1 T^{m-1} + ... + a_m$. Wir fassen Multiplikation mit b in B als $Q(A)$-lineare Abbildung $Q(B) \to Q(B)$ auf. Dann gilt*

$$\det(b) = \pm a_m^s$$

für ein $s \in \mathbb{N}$ insbesondere ist $\det(b) \in A$*.*

Beweis. Da A noethersch ist und B/A endlich, ist auch $B' = A[b]$ endlich über A. Also ist b Nullstelle eines normierten Polynoms $F \in A[T]$. O.B.d.A. sei F irreduzibel über A.

Lemma (Gauss-Lemma). Sei A nullteilerfrei mit eindeutiger Primfaktorzerlegung, $F \in A[T]$ normiert, $G \in Q(A)[T]$ normiert und $G|F$, dann ist $G \in A[T]$

Nach Gauss-Lemma ist somit F irreduzibel in $Q(A)$. Es gilt $Q(B') = Q(A)[b]$ und dies ist ein $Q(A)$-Vektorraum mit Basis $1, b, b^2, ..., b^{n-1}$. Wir betrachten die Matrix M der Multiplikation mit b

$$Q(B') \xrightarrow{\cdot b} Q(B')$$

$$M = \begin{pmatrix} 0 & 0 & ... & 0 & -a_m \\ 1 & 0 & ... & 0 & -a_{m-1} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & ... & 1 & -a_2 \\ 0 & 0 & ... & 0 & 1-a_1 \end{pmatrix}$$

B ist endlich erzeugt als A-Modul, also $B = A[b, b_1, ..., b_n]$ für endlich viele b_i. Dann ist $Q(A)[b_1, ..., b_n] = Q(B)$ und $Q(B)/Q(A)$ ist endlich. Somit ist

$$Q(A) \subseteq Q(B') \subseteq Q(B)$$

endliche Körpererweiterung. Die $Q(A)$-Matrix der Multiplikation mit b auf $Q(B)$ ist Blockdiagonalmatrix

$$\begin{pmatrix} M & & & & \\ & M & & & \\ & & M & & \\ & & & M & \\ & & & & \ddots \end{pmatrix}$$

und somit ist $\det(b) = \det(M)^s = \pm a_m^s$ $\square$

Theorem 8.32 (Krullscher Hauptidealsatz). *Sei X irreduzibel und $g : X \to \mathbb{A}^1$ nicht-konstanter Morphismus und Z irreduzible Komponente von $V(g)$ mit $Z \neq \emptyset$, dann ist* $\dim Z = \dim X - 1$

Korollar 8.33. *Sei X irreduzibel, $Z \subsetneq X$ maximale irreduzible abgeschlossene Teilmenge. Dann ist* $\dim Z = \dim X - 1$.

Beweis. Sei o.B.d.A X affin, dann ist $Z = V(f_1, ..., f_n)$ für f_i nicht-konstant. Wegen $S \subseteq V(f_1)$ liegt Z in einer irreduziblen Komponente von $V(f_1)$ und somit, nach Maximalität, ist Z gleich dieser Komponente. Somit folgt die Aussage aus dem Krullschen Hauptidealsatz 8.32. $\square$

Korollar 8.34. *Sei X irreduzibel, $Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_n$ Kette von irreduziblen Teilmengen. Sie kann zu einer Kette der Länge* $\dim X$ *ergänzt werden. Insbesondere haben alle maximalen Ketten die gleiche Länge.*

Beweis. Sei o.B.d.A $Z_n = X$ und Z_0 ein Punkt.

Behauptung. Ist $\dim Z_i < \dim Z_{i+1} - 1$, so existiert ein $Z_i \subsetneq Z \subsetneq Z_{i+1}$.

Beweis. Sei Z maximale irreduzible Teimenge von Z_{i+1}, die Z_i enthält. Dann gilt $\dim Z = \dim Z_{i+1} - 1$ und somit $\dim Z_i \subsetneq Z$.

$\square$

Beweis von 8.32. Sei X irreduzibel, $g : X \to \mathbb{A}^1$ nicht-konstant. Sei $Z \subseteq V(g)$ irreduzible Komponente. Wir Zerlegen $V(g) = Z \cup Z_1 \cup ... \cup Z_n$ in irreduzible Komponenten. Sei $U \subsetneq X \setminus (Z_1 \cup ... \cup Z_n)$ affin mit $U \cap Z \neq \emptyset$. $U \cap Z$ ist dicht in Z. Wir ersetzen X durch U und Z durch $Z \cap U$. Es reicht somit, den affinen Fall zu betrachten. Sei $Z = V(g)$, $d = \dim X$. Nach Noethernormalisierung 8.20 existiert eine endliche Surjektion

$$\pi : \quad \begin{tikzcd} X \arrow[rr] \arrow[dr, "g"'] & & \mathbb{A}^d \arrow[dl, dashed, "g'"] \\ & \mathbb{A}^1 & \end{tikzcd}$$

Wir suchen $V(g') \subseteq \mathbb{A}^d$ mit $\pi(Z) = V(g')$, denn dann gilt mit Going-Up 8.11

$$\dim V(g) = \dim V(g') = \operatorname{trdeg}_k k[V(g')] = d-1$$

Wir betrachten $A = k[\mathbb{A}^d] = k[X_1, ..., X_d]$ und $B = k[X]$ und setzen $g' = \det(g)$. Nach Lemma 8.31 gilt $g' \in A$.

Behauptung. $g' \in \langle g \rangle \subseteq k[X] = B$

Beweis. Sei $T^m + a_1 T^{m-1} + ... + a_m$ das Polynom aus dem Lemma. Wegen $-a_m = g(g^{m-1} + a_1 g^{m-2} + ... + a_$ ist $a_m \in \langle g \rangle$ und damit $g' = \pm a_m^s \in \langle g \rangle$.

Behauptung. $\sqrt{\langle g \rangle} \cap k[X_1, ..., X_d] = \sqrt{\langle g' \rangle}$

Beweis. Nach erster Behauptung gilt $\sqrt{\langle g' \rangle} \subseteq \sqrt{\langle g \rangle} \cap k[X_1, ..., X_d]$. Sei nun $h \in \sqrt{\langle g \rangle} \cap A$, also $h^N = \alpha \cdot g \in k[X] = B$. Anwenden der Determinante liefert

$$\det(h)^N = \det(\alpha) \cdot \underbrace{\det(g)}_{g'}$$

Weil $h \in A$ folgt, dass $\det(h)$ Potenz von h ist.

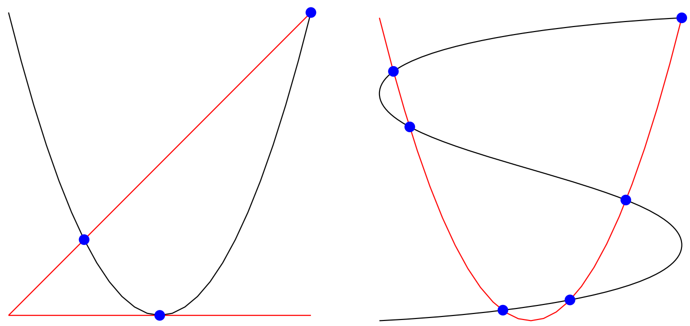
Somit ist

$$k[X_1, ..., X_d] / I(V(g')) \to k[X] / I(V(g))$$

endlicher injektiver Ringhomomorphismus. Nach Going-Up 8.11 haben diese Ringe somit die gleiche Dimension. Diese ist $\dim Z = d-1$. $\square$

Theorem (Bézout)**.** *Seien C_1 und C_2 verschiedene irreduzible ebene Kurven in $\mathbb{P}^2$, dann hat $C_1 \cap C_2$, gezählt mit Vielfachheit, $d_1 \cdot d_2$ viele Punkte, wobei $d_1 = \deg C_1$ und $d_2 = \deg C_2$.*

Beispiel 8.35.



9 Graduierte Ringe und Moduln

Definition 9.1. (i) Sei A ein Ring. Eine graduierte A-Algebra ist eine direkte Summe

$$S = \bigoplus_{d=0}^{\infty} S_d$$

von A-Moduln zusammen mit einer Multiplikation

$$\mu : S \times S \to S$$

mit $\mu(S_n, S_m) \subseteq S_{n+m}$ die S zu einer A-Algebra macht $A \to S_0$

(ii) Sei S eine graduierte A-Algebra. Ein graduierter S-Modul ist eine direkte Summe

$$M = \bigoplus_{d=-\infty}^{\infty} M_d$$

von A-Moduln zusammen mit einer Skalarmultiplikation

$$\mu : S \times M \to m$$

sodass $\mu(S_n, M_d) \subseteq M_{n+d}$, die M zu einem S-Modul macht.

(iii) Sei M graduierter S-Modul, $l \in \mathbb{Z}$, dann ist $M[l] := M$ mit der Graduierung $M[l]_d = M_{l+d}$ graduierter Modul.

(iv) Ein homogenes Ideal von S ist ein graduierter Untermodul.

Beispiel 9.2. Sei $A = k$ Körper, dann ist $k[X_0, ..., X_n]$ eine graduierte k-Algebra wobei $k[X_0, ..., X_n]_d$ die homogenen Polynome von Grad d sind.

Lemma 9.3. *Ist $V \subseteq \mathbb{P}^n_k$ projektive Varietät, so ist $I(V)$ homogenes Ideal von $k[X_0, ..., X_n]$.*

Beweis. Es ist

$$I(V) = \left\{ \sum_{\text{endl.}} f_d \;\middle|\; f_d \text{ homogen von Grad } d \right\}$$

abgeschlossen unter $+$ und Multiplikation mit homogenen Polynomen.

$$I(V)_d = I(V) \cap k[X_0, ..., X_n]_d = \{f_d \mid f_d \text{ homogen von Grad } d\}$$

ist graduierter Modul. Sei $f_d \in I(V)$ homogen von Grad d, $s_m \in k[X_0, ..., X_n]_m$, dann ist $f_d \cdot s_m \in I(V)_{d+m}$. □

Lemma 9.4. *Sei S ein graduierter Ring, $I \triangleleft S$ homogenes Ideal, dann ist $S/I \cong \bigoplus_{d=0}^{\infty} S_d/I_d$ graduierter Ring.*

Beweis. Es gibt eine surjektive Abbildung

$$\pi : \bigoplus_{d=0}^{\infty} S_d/I_d \to S/I$$
$$s_d + I_d \in S_d/I_d \mapsto s_d + I$$

Sei $s = \sum_{d=0}^{n} s_d \in \ker(\pi)$, also $s \in I$, dann ist $s_d \in I_d$ und damit $s = 0$. Somit ist π Isomorphismus □

Korollar 9.5. *Sei $V \subseteq \mathbb{P}^n$ projektiv. Der homogene Koordinatenring*

$$S[V] = k[X_0, ..., X_n] / I(V)$$

ist k-Algebra

Bemerkung 9.6. Notation S soll an „symmetrische Algebra“ erinnern, denn $k[X_1, ..., X_n] \cong \mathrm{Sym}^* V$ für V ein k-Vektorraum der Dimension n wobei

$$\mathrm{Sym}^* V = \left\{ \underbrace{V \times .... \times V}_{d} \to k \text{ symmetrisch und multilinear} \right\}$$

zum Beispiel ist

$$X^2 + 2XY - Y^2 = \begin{pmatrix} X & Y \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \end{pmatrix}$$

Lemma 9.7. *Sei R graduierter Ring, $S \subseteq R$ eine multiplikative Menge, die aus homogenen Elementen besteht. Dann ist $S^{-1}R$ graduierter Ring. Wir erhalten eine Bijektion von*

$$\begin{array}{c} I \mapsto \pi^{-1}(I) \\ \left\{ \begin{array}{r} \textit{homogene Ideale} \\ \textit{von } S^{-1}R \end{array} \right\} \leftrightarrow \left\{ \begin{array}{r} \textit{homogene Ideale} \\ I \triangleleft R \textit{ mit } I \cap S = \emptyset \end{array} \right\} \\ S^{-1}I \leftarrow\!\shortmid I \end{array}$$

wobei $\pi : R \to S^{-1}R$, kompatibel damit, „prim“ zu sein.

Beweis. Es ist

$$\left(S^{-1}R\right)_d = \left\{ \frac{f}{s} \in S^{-1}R \;\middle|\; f \in R_{\deg s + d} \right\}$$

und

$$S^{-1}R = \bigoplus_{d=0}^{\infty} \left(S^{-1}R\right)_d$$

Die Bijektion ist wie bei nicht-graduierten Ringen. □

Definition 9.8. Für $P \triangleleft R$ homogenes Primideal sei $R_P := S^{-1}R$ mit $S = \{f \in R \setminus P \mid f \text{ homogen}\}$. Dies ist ein lokaler graduierter Ring mit maximalem Ideal $S^{-1}P$

Definition 9.9. Sei M endlich erzeugter graduierter Modul über $S = k[X_0, ..., X_n]$, dann heißt

$$\Phi_M : \mathbb{Z} \to \mathbb{Z} \tag{9.1}$$
$$d \mapsto \dim_k M_d \tag{9.2}$$

Hilbert-Funktion von M.

Satz 9.10. *Sei M endlicher erzeugter graduierter $k[X_0, ..., X_n]$-Modul, dann existiert ein Polynom $P_M \in \mathbb{Q}[Z]$ mit $P_M(d) = \Phi_M(d)$ für $d \gg 0$. Dieses Polynom heißt* Hilbertpolynom *von M. Es gilt*

$$\deg P_M = \dim V(I(M))$$

wobei $I(M) = \{s \in k[X_0, ..., X_n] \mid s \cdot M = 0\}$

Beispiel 9.11. $S = k[X]$ ist gradduiert mit $S_d = k \cdot X^d$. Es ist $\dim_k s_d = 1$ für $d \geq 0$ und $\dim_k s_d = 0$ für $d < 0$. Für $M = S$ ist $P_M = 1$.

Definition 9.12. Sei $V \subseteq \mathbb{P}^n$. Das *Hilbertpolynom* von V ist das Hilbertpolynom von $S(V)$. Ist $P_V(Z) = a_d Z^d + ... + a_0$ mit $a_d \neq 0$, dann heißt $d! \cdot a_d$ der *Grad* von V.

Bemerkung 9.13. Wegen $I(S(V)) = I(V)$, mit $S(V)$ als $k[X_0, ..., X_n]$-Modul, gilt

$$d = \deg P_V = \dim V$$

Wir werden sehen, dass im Falle ebener Kurven die Graddefinition mit der schon gemachten übereinstimmt.

Beispiel 9.14. Sei $f = X_0X_1 - X_2^2$ und $M = S(V(f))$. Beim Rechnen in M können quadratische Potenzen von X_2 eliminiert werden. Also hat M_d die k-Basis $X_0^a X_1^{d-a}$ für $a \in \{0, ..., d\}$ und $X_0^b X_1^{d-b-1} X_2$ für $b \in \{0, ..., d-1\}$. Also ist $\Phi_M(d) = 2d + 1$ und damit $P_{V(f)} = 2Z + 1$. Das Polynom hat Grad $1 = \dim V(f)$. Der Grad von $V(f) = 1! \cdot 2 = 2 = \deg f$

Definition 9.15. Ein *numerisches Polynom* ist ein Polynom $\mathbb{Q}[Z]$ mit $P(n) \in \mathbb{Z}$ für alle $n \in \mathbb{Z}, n \gg 0$.

Beispiel 9.16. $\binom{Z}{3} = \frac{Z(Z-1)(Z-2)}{3!}$ hat ganze Werte für $Z \geq 3$.

Lemma 9.17. *(i) Sei $F \in \mathbb{Q}[Z]$ numerisches Polynom, dann ist*

$$F(Z) = c_0 \binom{Z}{r} + c_1 \binom{Z}{r-1} + ... + c_r$$

mit $c_i \in \mathbb{Z}$.

(ii) Sei $f : \mathbb{Z} \to \mathbb{Z}$ eine Funktion, $\Delta(f)(n) := f(n+1) - f(n)$ sei ein numerisches Polynom $G \in \mathbb{Q}[Z]$ für $n \gg 0$. Dann existiert $P \in \mathbb{Q}[Z]$ numerisches Polynom mit $P(n) = f(n)$ für $n \gg 0$

Beweis. (i) Induktion über r. Hat F den Grad 0, so ist F konstant und die Behauptung gilt. Allgemein lässt sich $\binom{Z}{r}$ entwickeln als

$$\binom{Z}{r} = \frac{Z^r}{r!} + ...$$

Daher lässt sich $F(Z)$ eindeutig in der angegebenen Form schreiben mit $c_i \in \mathbb{Q}$. Wir betrachten $\Delta(F)$. Dies ist ein numerisches Polynom von Grad $r - 1$. Außerdem gilt

$$\begin{aligned}\Delta \binom{Z}{r} &= \frac{(Z+1) \cdot ... \cdot (Z+1-r+1)}{r!} - \frac{Z(Z-1) \cdot ... \cdot (Z-r+1)}{r!} \\ &= \frac{Z(Z-1) \cdot ... \cdot (Z-r+2)}{r!} \left(\underbrace{Z + 1 - Z + r - 1}_{r} \right) \\ &= \binom{Z}{r-1}\end{aligned}$$

Hieraus folgt $\Delta(F) = c_0 \binom{Z}{r-1} + ... + c_{r-1}$. Nach Induktionsannahme gilt $c_i \in \mathbb{Z} \forall 0 \leq i < r$. Dann muss auch c_r ganz sein.

(ii) Sei $G = c_0 \binom{Z}{r} + ... + c_r$ mit $c_i \in \mathbb{Z}$. Wir setzen $\widetilde{F} = c_0 \binom{Z}{r+1} + ... + c_r \binom{Z}{1}$. Somit ist $\Delta\left(\widetilde{F}\right) = G$ und somit $\Delta\left(f - \widetilde{F}\right)(n) = 0$ für $n \gg 0$. Anders gesagt

$$\begin{aligned} c_{r+1} &\coloneqq f(n+1) - \widetilde{F}(n+1) \\ &= f(n) - \widetilde{F}(n) \end{aligned}$$

für $n \gg 0$. Also folgt $c_{r+1} \in \mathbb{Z}$ und $F = \widetilde{F} + c_{r+1}$ ist das gesuchte Polynom.

□

Korollar 9.18. *Ist F ein numerisches Polynom $F = a_r Z^r + ... + a_0$ mit $a_r \neq 0$, so gilt $r! a_r \in \mathbb{Z}$.*

Lemma 9.19. *Sei $S = k[X_0, ..., X_n]$ und $\mathfrak{p} \triangleleft S$ homogenes Primideal. Sei*

$$0 \to A \to B \to C \to 0$$

eine exakte Sequenz von graduierten S-Moduln, dann ist

$$P \supseteq I(B) \Leftrightarrow P \supseteq I(A) \vee P \supseteq I(C)$$

Es gilt

$$V(I(B)) = V(I(A)) \cup V(I(C))$$

Beweis. Es gilt $I(B) \subseteq I(A) \cap I(C)$ und $I(A) I(C) \subseteq I(B)$. Angenommen $I(B) \subseteq P$ und $I(A), I(C) \nsubseteq P$. Dann existieren $s \in I(A)$ mit $s \notin P$ und $t \in I(C)$ mit $t \notin P$. Aber $st \in I(A) I(C) \subseteq I(B) \subseteq P$ im Widerspruch dazu, dass P Primideal ist. Wenn umgekehrt $P \supseteq I(A)$ oder $P \supseteq I(C)$, dann ist $I(B) \subseteq I(A) \cap I(C) \subseteq P$. Die Aussage über Varietäten folgt, wenn man für P maximale Ideale betrachtet. □

Korollar 9.20. *Sei*

$$0 \to A \to B \to C \to 0$$

eine kurze exakte Sequenz von graduierten Moduln. Wenn der Satz über die Existenz des Hilbertpolynoms für A und C gilt, so gilt er auch für B.

Beweis. Es gilt $\Phi_B(d) = \Phi_A(d) + \Phi_C(d)$ für $d \in \mathbb{Z}$. Gibt es Hilbertpolynome P_A für A und P_C für C, dann ist $P_B \coloneqq P_A + P_C$ das Hilbertpolynom für B. Als Hilbertpolynome haben alle drei positive Leitkoeffizienten. Also folgt aus dem Satz für A und C sowie vorherigem Lemma 9.19, dass

$$\begin{aligned} \deg P_B &= \max\left(\deg P_A, \deg P_c\right) \\ &= \max\left(\dim V(I(A)), \dim V(I(C))\right) \\ &= \dim\left(V(I(A)) \cup V(I(C))\right) \\ &= \dim V(I(B)) \end{aligned}$$

□

Beispiel 9.21. Sei $S = k[X_0, X_1]$ und $B = S/\langle X_0X_1\rangle$. Dann ist $I(B) = \langle X_0X_1\rangle = \langle X_0\rangle \cdot \langle X_1\rangle$ und

$$0 \to \underbrace{X_0B}_{=:A} \to B \to \underbrace{B/X_0B}_{=:C} \to 0$$

ist exakt. Es ist $A_d = k \cdot X_0^d$ und somit $\Phi_A(d) = 1$ für $d \geq 0$, also $P_A = 1$. Außerdem gilt $C_d = k \cdot X_1^d$ und damit ist $\Phi_B(d) = 1$ und $P_C = 1$. Also ist $P_B = P_A + P_C = 1 + 1 = 2$. Des weiteren gilt $I(A) = \langle X_1\rangle$ und $I(C) = \langle X_0\rangle$, womit $I(B) = I(A) \cdot I(C)$.

Satz 9.22. *Sei M endlich erzeugter graduierter Modul über $S = k[X_0, ..., X_n]$. Es gibt eine Filtrierung*

$$0 = M^0 \subseteq M^1 \subseteq M^2 \subseteq ... \subseteq M^r = M$$

durch graduierte Untermoduln, sodass

$$M^i/M^{i-1} \cong (S/P_i)[l_i]$$

für homogene Primideale $P_i \lhd S, l_i \in \mathbb{Z}$. Sei $P \subseteq S$ homogenes Primideal, dann ist $P \supseteq I(M)$ genau dann, wenn $P \supseteq P_i$ für ein i. Insbesondere sind die minimalen Primideale von $I(M)$ (die zu den irreduziblen Komponenten von $V(I(M))$ gehören) genau die minimalen Elemente von $P_1, ..., P_r$. Die Häufigkeit mit der ein minimales P_i vorkommt ist unabhängig von der Wahl der Filtrierung.

Bemerkung 9.23. Weder die Filtrierung noch die (nicht-minimalen) P_i sind eindeutig.

Beweis. Sei $m \in M$. Wir definieren

$$I(m) := \{s \in S \mid sm = 0\}$$

Dies ist ein homogenes Ideal. Wir betrachten die Menge $\{I(m) \mid m \neq 0 \text{ homogen}\}$. Da S noethersch ist, enthält diese ein maximales Element $I(x)$.
Behauptung. $I(x)$ ist Primideal

Beweis. Es ist $1 \notin I(x)$, da $1 \cdot x = x \neq 0$. Sei $ab \in I(x)$ und $b \notin I(x)$, also $abx = 0$ und $bx \neq 0$. O.B.d.A seien a und b homogen (sonst zerlegen wir a und b in die homogenen Anteile). Es gilt $I(x) \subseteq I(bx)$. Nach Maximalität von $I(x)$ ist somit $I(x) = I(bx)$. Da $a \in I(bx)$ ist somit $a \in I(x)$.

Sei $l = \deg x$. Wir wählen $M^1 := \langle x\rangle \subseteq M$. Dann gilt $M^1 \cong \left(\underbrace{S/I(x)}_{Sx}\right)[l]$. Nun wiederholen wir die Konstruktion und finden eine Untermodul $N \subseteq M/M^1$ und definieren M^2 als das Urbild unter der Projektion

$$\begin{array}{ccc} M & \longrightarrow & M/M^1 \\ \text{\rotatebox{90}{$\subseteq$}} & & \text{\rotatebox{90}{$\subseteq$}} \\ M^2 & \longrightarrow & N \end{array}$$

Induktiv erhalten wir

$$0 \subseteq M^1 \subseteq M^2 \subseteq M^3 \subseteq ...$$

Da M noethersch ist, endet der Prozess mit $M = M^r$. Die Aussage für homogene Primideale P folgt aus Lemma 9.19. Sei P ein minimales Primideal, das $I(M)$ enthält. Wir lokalisieren (im nicht-graduierten Sinne) an P und erhalten $0 \subseteq M_P^1 \subseteq M_P^2 \subseteq M_P^3 \subseteq ... = M_P$. Es ist $(S/P_i)_P \neq 0$ genau dann, wenn $P_i \subseteq P$. Das heißt, die lokalisierte Kette hat so viele Inklusionen, wie P_i vorkommt. Die Unabhängigkeit der Anzahl von der Filtrierung folgt, da die Anzahl mit der Dimension $\dim_{(S/P)_P} M_P$ übereinstimmt, was eben davon unabhängig ist. □

Beweis von 9.10. Per Induktion über die Dimension von $V(I(M))$. Wegen Korollar 9.20 und Satz 9.22 reicht es, den Fall zu betrachten, wo $M = (S/P)[l]$, wobei P ein homogenes Primideal ist. Die Operation $[l]$ bedeutet $z \mapsto z + l$. Es reicht also sogar, den Fall S/P anzuschauen.

1. Fall Wenn $P = \langle X_0, ..., X_n \rangle$, dann ist $S/P = k =: M$ und somit ist $\Phi_M(n) = 0$ für $n \geq 0$. Also ist $P_M = 0$ und der Grad ist $-\infty$ und die Verschwindungsmenge $V(P) = \emptyset$ hat Dimension $-\infty$.

2. Fall Wenn $P \neq \langle X_0, ..., X_n \rangle$, dann sei o.B.d.A $X_0 \notin P$. Wir betrachten die kurze exakte Sequenz.

$$0 \to M \xrightarrow{\cdot X_0} M[1] \to \underbrace{M''}_{=M[1]/X_0 M} \to 0$$

wobei $M = S/P$ und $I(M) = P$. Die Abbildung $\cdot X_0$ ist injektiv, da S/P nullteilerfrei ist. Es folgt, dass $\Phi_{M''}(n) = \Phi_M(n+1) - \Phi_M(n) = \Delta(\Phi_M)(n)$. Es ist

$$I(M'') \supseteq \underbrace{I(S/P)}_{P} + \langle X_0 \rangle$$

Wegen $X_0 \notin P$ und Krulls Hauptidealsatz 8.32 folgt

$$\begin{aligned} \dim V(I(M'')) &\leq \dim\,(V(P) \cap V(X_0)) \\ &= \dim V(P) - 1 \end{aligned}$$

Mit Induktion über $\dim I(M)$ können wir voraussetzen, dass die Aussage für M'' gilt. Nach dem Lemma 9.17 existiert somit ein Hilbertpolynom P_M vom Grad $\deg P_{M''} + 1$. Auch der Fall $\dim V(P) = 0$ ist vom Beweis abgedeckt, denn dann ist $V(P) \cap V(X_0) = \emptyset$ und $P + \langle X_0 \rangle = \langle X_0, ..., X_n \rangle$. Damit ist hier das Polynom konstant aber nicht Null.

□

10 Satz von Bézout

Satz 10.1 (Satz von Bézout für Kurven)**.** *Seien $C_1, C_2 \subseteq \mathbb{P}^2$ verschiedene irreduzible Kurven von Grad d_1 und d_2, dann hat $C_1 \cap C_2$ gezählt mit Vielfachheit genau $d_1 \cdot d_2$ Schnittpunkte.*

Bemerkung 10.2. In der übung 10a haben wir gesehen, dass für $C_1^0 \subseteq \mathbb{A}^2$ und C_2 Gerade $C_1^0 \cap C_2 \leq d_1 \cdot 1$. Schnittpunkte können nach ∞ entweichen.

Definition 10.3. Seien $C_1, C_2 \subseteq \mathbb{P}^2$ Kurven, $P \in C_1 \cap C_2$. Dann ist

$$i(C_1, C_2, P) := \dim_k \mathcal{O}_{C_1,P} \otimes_{\mathcal{O}_{\mathbb{P}^2,P}} \mathcal{O}_{C_2,P}$$

die *Schnittmultiplizität* von C_1 und C_2 in P.

Bemerkung 10.4. Da die lokalen Ringe nur von einer affinen Umgebung von P abhängen, können wir für die Berechnung von $i(C_1, C_2, P)$ eine affine Karte von $\mathbb{P}^2$ betrachten, die P enthält $P \in \mathbb{A}^2 \cong U_i \subseteq \mathbb{P}_2$. Sei $C_1^0 \coloneqq C_1 \cap \mathbb{A}^2$ und $C_2^0 \coloneqq C_2 \cap \mathbb{A}^2$ und seien $I(C_1^0) = \langle f \rangle$ und $I(C_2^0) = \langle g \rangle$. Dann gilt

$$\mathcal{O}_{C_1,P} \otimes_{\mathcal{O}_{\mathbb{P}^2,P}} \mathcal{O}_{C_2,p} = (k[X,Y] / \langle f, g \rangle)_{I(P)}$$

Es gilt $C_1^0 \cap C_2^0 = C_1 \cap C_2 \cap \mathbb{A}^2 = V(f,g)$ und $I(C_1^0 \cap C_2^0) = \sqrt{\langle f, g \rangle}$. Die Schnittmultiplizität misst also den Unterschied von $\langle f, g \rangle$ und $\sqrt{\langle f, g \rangle}$

Lemma 10.5. *Sind $f, g \in k[X,Y]$ teilerfremd, so gilt* $\dim_k k[X,Y] / \langle f, g \rangle < \infty$.

Beweis. Nach Krulls Hauptidealsatz 8.32 gilt $\dim k[X,Y] / \langle f, g \rangle = 2 - 2 = 0$. Nach Noethernormalisierung 8.20 angewandt auf

$$k \hookrightarrow k[X,Y] / \langle f, g \rangle$$

ist dies endliche Ringerweiterung und somit die Dimension endlich. □

Lemma 10.6. *Seien f, g teilerfremd. Dann gilt*

$$\dim_k k[X,Y] / \langle f, g \rangle = \sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \dim_k (k[X,Y] / \langle f, g \rangle)_{I(P)}$$

Insbesondere ist $\dim_k (k[X,Y] / \langle f, g \rangle)_{I(P)} < \infty$

Beweis. Nach Filtrierungssatz 9.22 für den $k[X,Y]$-Modul $M \coloneqq k[X,Y] / \langle f, g \rangle$ existiert

$$0 = M^0 \subseteq M^1 \subseteq ... \subseteq M^r = M$$

mit $M^i / M^{i-1} \cong k[X,Y] / P_i$ für $P_i \supseteq I(M)$ und $P_i \subseteq k[X,Y]$ prim. Es gilt $I(M) = \langle f, g \rangle$.
Behauptung. Sei $Q \triangleleft k[X,Y]$ prim mit $Q \supseteq \langle f, g \rangle$, dann ist $Q = I(P)$ für ein $P \in C_1 \cap C_2 \cap \mathbb{A}^2$.

Beweis. $V(f,g) = C_1 \cap C_2$ hat Dimension Null, besteht also aus endlich vielen Punkten. Es gilt $Q \supseteq \langle f, g \rangle$ genau dann, wenn $V(Q) \subseteq V(f,g)$ nach Hilberschem Nullstellensatz 4.1. Dies ist genau dann der Fall, wenn $V(Q) = P$ für ein $P \in C_1 \cap C_2 \cap \mathbb{A}^2$. □

Die Menge der P_i mit Vielfachheit ist somit unabhängig von der Filtrierung, da alle P_i minimal sind. Es ist

$$\begin{aligned} \underbrace{\dim_M k}_{=r} &= \sum_{i=1}^{r} \dim_k \underbrace{M_i / M_{i-1}}_{\cong k} \\ &= \sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \dim_k M_{I(P)} \end{aligned}$$

□

Definition 10.7. Sei $f \in k[X_0, ..., X_n]$ irreduzibel, homogen von Grad d. Dann heißt $V(f) \subseteq \mathbb{P}^n$ *projektive Hyperfläche* von Grad d.

Satz 10.8. *(i) Für $Y \subseteq \mathbb{P}^n$ nicht leer ist* $\deg Y \in \mathbb{N}_{>0}$

(ii) Wenn $Y = Y_1 \cap Y_2$ *mit* $\dim Y_1 = \dim Y_2 = r$ *und* $\dim Y_1 \cap Y_2 < r$*, dann gilt*

$$\deg Y = \deg Y_1 + \deg Y_2$$

(iii) $\deg \mathbb{P}^n = 1$

(iv) Sei $H \subseteq \mathbb{P}^n$ *Hyperfläche mit* $I(H) = \langle f \rangle$ *und* f *homogen von Grad* d*, dann ist*

$$\deg H = d$$

Beweis. (i) Das Hilbertpolynom P_Y ist von Grad $r = \dim Y$. Der Leitkoeffizient hat die Form $\frac{c_0}{r!}$ für ein $c_0 \in \mathbb{Z}$. Da $Y \neq \emptyset$ ist $\dim_k k[Y]_n > 0$ für $n \gg 0$ und somit $P_Y(z) > 0$ für $z \gg 0$. Also ist $c_0 > 0$.

(ii) Seien I_1, I_2 die Ideale von Y_1, Y_2, dann gilt $I := I(Y) = I(Y_1) \cap I(Y_2)$. Außerdem ist $V(I_1 + I_2) = Y_1 \cap Y_2$. Mit $S := k[\mathbb{P}^n] = k[X_0, ..., X_n]$ haben wir dann eine kurze exakte Sequenz

$$0 \longrightarrow S/I \xrightarrow{a \mapsto (a,-a)} S/I_1 \oplus S/I_2 \xrightarrow{+} S/(I_1 + I_2) \longrightarrow 0$$

es folgt

$$\begin{aligned} P_Y = P_{S/I} &= P_{S/I_1} + P_{S/I_2} - P_{S/(I_1+I_2)} \\ &= P_{Y_1} + P_{Y_2} - P_{Y_1 \cap Y_2} \end{aligned}$$

Wegen der Dimensionsvoraussetzung ist der Leitkoeffizient von P_Y

$$\frac{\deg Y}{r!} = \frac{\deg Y_1}{r!} + \frac{\deg Y_2}{r!}$$

(iii) Für $P = P_{k[X_0,...,X_n]}$ und $d > 0$ gilt $\dim_k k[X_0, ..., X_n]_d = \binom{d+n}{n}$ und somit

$$P(z) = \binom{z+n}{n} = \frac{z^n}{n!} + ...$$

und somit $\deg \mathbb{P}^n = 1$.

(iv) Sei $I(H) = \langle f \rangle$. Betrachte

$$0 \longrightarrow S[-d] \xrightarrow{\cdot f} S \longrightarrow S/\langle f \rangle \longrightarrow 0$$

Es ist

$$\begin{aligned} P_H(z) &= \binom{z+n}{n} - \binom{z-d+n}{n} \\ &= \left(\frac{z^n}{n!} + \frac{1}{n!} \left(\sum_{i=1}^{n} i \right) z^{n-1} + ... \right) - \left(\frac{z^n}{n!} + \frac{1}{n!} \left(\sum_{i=1-d}^{n-d} i \right) z^{n-1} + ... \right) \\ &= \left(\frac{n(n+1)}{2} - \frac{n(n-2d+1)}{2} \frac{z^{n-1}}{n!} \right) + ... \\ &= \frac{d}{(n-1)!} z^{n-1} + ... \end{aligned}$$

$\square$

Definition 10.9. Sei $Y \subseteq \mathbb{P}^n$ eine Varietät der Dimension r und $H \subseteq \mathbb{P}^n$ eine Hyperfläche, die keine Komponente von Y enthält. Sei Z eine irreduzible Komponente von $Y \cap H$. Dann ist die Schnittmultiplizität $i(Y, H, Z)$ von Y und H in Z definiert als die Vielfachheit, mit der $I(Z)$ in der Kette einer Filtrierung von $M = S/(I(Y) + I(H))$ vorkommt.

Bemerkung 10.10. Diese Definition verallgemeinert die Definition für Kurven. Bemerke außerdem, das jede ebene Kurve eine Hyperfläche ist

Satz 10.11 (Satz von Bézout)**.** *Sei $Y \subseteq \mathbb{P}^n$ Untervarietät mit* $\dim(Y) \geq 1$ *and $H \subseteq \mathbb{P}^n$ eine Hyperfläche, die keine Komponente von Y enthält. Sei $Y \cap H = Z_1 \cup ... \cup Z_s$ die Zerlegung in irreduzible Komponenten. Dann gilt*

$$\sum_{j=1}^{s} i(Y, H, Z_j) \deg Z_j = \deg Y \cdot \deg H$$

Beweis. Sei $I(H) = \langle f \rangle$ mit f homogen von Grad d. Betrachte für $S = k[X_0, ..., X_n]$

$$0 \to S/I(Y)[-d] \xrightarrow{\cdot f} S(Y) \to M \to 0$$

wobei $M = S/(I(Y) + I(H))$. Es folgt

$$P_M(z) = P_Y(z) - P_Y(z-d)$$

Wir vergleichen den höchsten Koeffizienten auf beiden Seiten. Sei $\deg Y = e, \dim Y = r$, also

$$P_Y(z) = \frac{e}{r!} z^r + e_1 z^{r-1} + ...$$

dann ist

$$\begin{aligned} P_Y(z) - P_Y(z-d) &= \left(\frac{e}{r!} z^r + e_1 z^{r-1} + ...\right) - \left(\frac{e}{r!}(z-d)^r + e_1 (z-d)^{r-1}\right) \\ &= \frac{e}{r!} z^r + e_1^{r-1} - \frac{e}{r!} z^r + der z^{r-1} r! - e_1 \frac{z^{r-1}}{+} ... \\ &= \frac{der}{r!} z^{r-1} + ... \\ &= \frac{de}{(r-1)!} z^{r-1}, \end{aligned}$$

wobei hier $r - 1 \geq 0$, d.h. $\dim Y \geq 1$ eingeht. Andererseits berechnen wir P_M über eine Filtrierung

$$0 = M^0 \subseteq M^1 \subseteq ... \subseteq M^t = M$$

mit $M^i/M^{i-1} \cong (S/Q_i)[l_i]$ für Primideale $Q_i \triangleleft S$. Dann gilt $P_M = \sum_{i=1}^t P_i$ wobei $P_i = P_{(S/Q_i)[l_i]}$. Wenn $V(Q_i)$ die Dimension r_i und den Grad f_i hat, dann gilt $P_i = \frac{f_i}{r_i!} z^{r_i} + ...$ Zum Leitkoeffizient von P_M tragen nur diejenigen Summanden P_i mit $r_i = r - 1$ bei. Die zugehörigen Q_i sind nach Krulls Hauptidealsatz 8.32 genau die Koeffizienten die Primideale der irreduziblen Komponenten von $V(I(M)) = V(I(Y) + I(H)) = Y \cap H = Z_1 \cup ... \cup Z_s$. Das heißt, solche Q_i mit $Q_i = I(Z_j)$ für ein j. Jedes solche Q_i tritt nach Definition $i(Y, H, Z_j)$ mal auf. Der Leitkoeffizient ist dann $\frac{\deg V(Q_i)}{(r-1)!}$. Also ist

$$P_M = \sum_{i=1}^{t} P_i = \sum_{j=1}^{s} \frac{\deg Z_j}{(r-1)!} i(Y, H, Z_j) z^{r-1} + ...$$

$\square$

Korollar 10.12. *Der Satz von Bézout für Kurven 10.1 folgt direkt: Die Z_j sind die Punkte $C_1 \cap Z_2$. Für diese Punkte P ist* $\deg P = 1$.

Korollar 10.13. *Sei $C \subseteq \mathbb{P}^n$ eine Kurve. Sei $f \in S(C)$ homogen von Grad m. Dann gilt*

$$\sum_{P \in C} \dim \mathcal{O}_P / \langle f \rangle = m \cdot \deg C$$

Beweis. Seien $f_1, ..., f_s$ die irreduziblen Faktoren von f, dann ist

$$\dim \mathcal{O}_P / \langle f \rangle = \sum_{i=1}^{s} \dim \mathcal{O}_P / \langle f_i \rangle$$

also können wir o.B.d.A. f als irreduzibel annehmen
Wir heben f von $S(C)$ zu $S = k[X_0, ..., X_n]$ unter

$$\begin{array}{ccccc} S & \twoheadrightarrow & S(C) & = & S/I(C) \\ \Cup & & \Cup & & \\ f & \longmapsto & f & & \end{array}$$

Setze $H = V(f) \subseteq \mathbb{P}^n$. Dann ist $I(H) = \langle f \rangle$. Der Satz von Bézout 10.11 liefert

$$\sum_{P \in H \cap C} \dim \left(S(C) / \langle f \rangle\right)_{I(P)} = \deg H \cdot \deg C$$

Falls $P \notin H \cap C$, dann ist $\left(S(C) / \langle f \rangle\right)_{I(P)} = 0$. □

Zwei Elemente $g, f \in S(C)_m$ mit $V(f) \cap V(g) = \emptyset$, dann ist ein Morphismus nach $\mathbb{P}^1$ definiert durch

$$\begin{aligned} \varphi : & C \to \mathbb{P}^1 \\ & P \mapsto [g(P) : f(P)] \end{aligned}$$

Das vorige Korollar 10.13 rechnet das Urbild von $[1:0]$ mit Vielfachheit aus, also $\deg f \cdot \deg C$. Hieraus folgt, dass φ endlich ist. Außerdem hat $k(\mathbb{P}^1) \hookrightarrow k(C)$ den Grad $\deg f \cdot \deg C$.

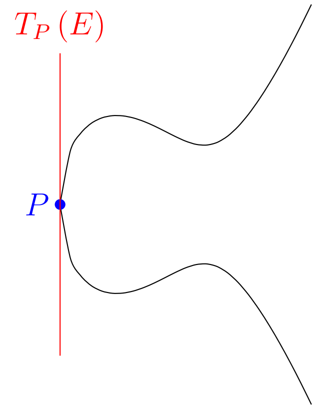
11 Elliptische Kurven und das Gruppengesetz

Sei $\operatorname{char}(k) = 0$

Definition 11.1. Eine Kurve $E \subseteq \mathbb{P}^2$ von Grad 3 ohne singuläre Punkte (d.h. alle Punkte sind nicht singulär) heißt *elliptische Kurve.*

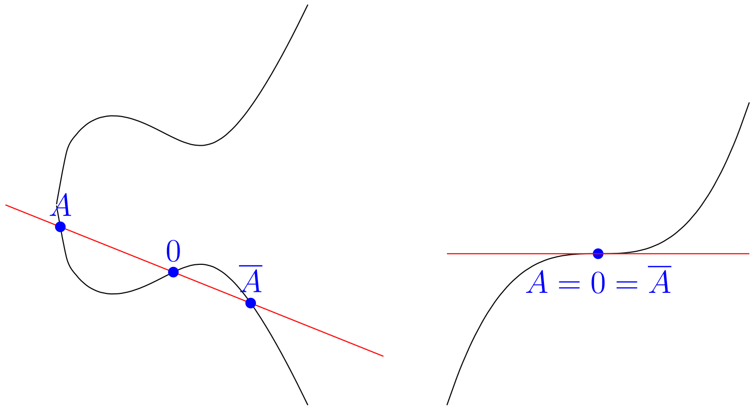
Bemerkung 11.2. (i) Elliptische Kurven sind irreduzibel: Angenommen $E = C_1 \cup C_2$, dann folgt nach Bézout $C_1 \cap C_2 \neq 0$. Jeder Punkt in $C_1 \cap C_2$ ist singulär. Das heißt $T_P(C_1 \cup C_2) \cong \mathbb{A}^2$.

(ii) Sei $P \in E$ mit E elliptische Kurve, dann existiert eine eindeutige Gerade $L \subseteq \mathbb{P}^2$ durch P mit $i(E, L, P) > 1$, nämlich $L = \overline{T_P E} \subseteq \mathbb{P}^2$



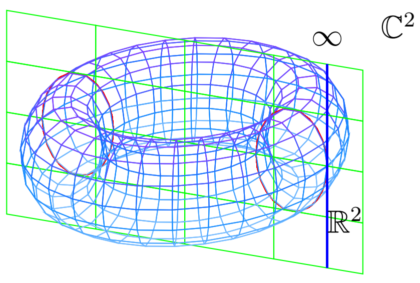
Definition 11.3. Sei E elliptische Kurve und $0 \in E$ ein Punkt.

(i) Für $A \in E$ sei $\overline{A}$ der Dritte Punkt auf der Geraden durch A und 0 geschnitten mit E. Der Satz von Bézout liefert die Existenz.



(ii) Für $A, B \in E$ sei R der dritte Punkt auf der Geraden durch A und B geschnitten mit E. Wir definieren $A + B := \overline{R}$.

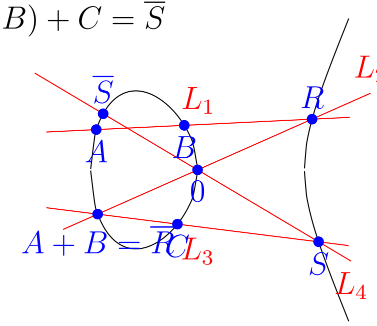
Beispiel 11.4. Elliptische Kurve im komplexen und im Reellen.



Satz 11.5. *Diese Konstruktion definiert eine abelsche Gruppenstruktur auf der Menge der Punkte von E, wobei 0 das neutrale Element ist.*

Beweis. Zur Assoziativität

$$(A+B)+C=\overline{S}$$



Die Konstruktion $(A+B)+C$ benötigt vier Geraden L_1, L_2, L_3, L_4 wie im Bild. Ganz ähnlich benötigt $A+(B+C)$ ebenfalls vier Geraden M_1, M_2, M_3, M_4. Wir wollen zeigen, dass

$$E\cap(L_1\cup M_2\cup L_3)=E\cap(M_1\cup L_2\cup M_3)$$

und dies sind nach Satz von Bézout neun Punkte. Davon sind acht Punkte tatsächlich nach Konstruktion gleich und wir wollen die Gleichheit des neunten Punktes zeigen, weil dieser jeweils $\overline{(A+B)+C}$ bzw. $\overline{A+(B+C)}$ ist. Da $\dim_k k[X,Y,Z]_3=10$ und die Bedingung durch einen Punkt zu gehen eine eindimensionale Bedingung ist, ist der Raum aller kubischen Gleichungen, deren zugehörige Kurven durch die besagten 8 Punkte gehen also zweidimensional. Dieser Raum ist bereits von zwei der drei kubischen Gleichungen zu $E, (L_1\cup M_2\cup L_3), (M_1\cup L_2\cup M_3)$ erzeugt. Daraus folgt, dass sich je zwei dieser Kubiken in den gleichen 9 Punkten schneiden und die Assoziativität ist für den Fall bewiesen, wo diese 9 Punkte verschieden sind. Die Menge, wo sie verschieden sind ist Zariski-dicht und die zwei Konstruktionen $(A+B)+C$ und $A+(B+C)$ liefern zwei Morphismen $E\times E\times E\to E$, welche auf einer Zariski-dichten Menge gleich sind. Damit sind sie dann überall gleich. $\square$