

Kommutative Algebra und Einführung in die algebraische Geometrie

Sommersemester 2010

Prof. Dr. Annette Huber-Klawitter

Fassung vom 3. Dezember 2010

**Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!**

Math. Institut
Eckerstr.1
79104 Freiburg

0761-203-5560
annette.huber@math.uni-freiburg.de

Kapitel 0

Einleitung

Wir beginnen mit der Einführung des zentralen Begriffes dieser Vorlesung:

Definition 0.1. Sei k ein algebraisch abgeschlossener Körper. Der affine Raum der Dimension n über k ist

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

Elemente von \mathbb{A}^n heißen Punkte. Für $P = (a_1, \dots, a_n)$ heißen die a_i Koordinaten. Wir interpretieren den Polynomring

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

als Funktionen

$$\begin{aligned} \mathbb{A}^n &\rightarrow k \\ (a_1, \dots, a_n) &\mapsto f(a_1, \dots, a_n) \end{aligned}$$

Sei $S \subset k[X_1, \dots, X_n]$ eine Teilmenge. Die durch S definierte algebraische Menge ist die Menge

$$V(S) = \{(x_1, \dots, x_n) \in k^n \mid f(x_1, \dots, x_n) = 0 \text{ für alle } f \in S\}$$

Ist $S = \{f\}$, so heißt $V(f) = V(\{f\})$ auch affine Hyperfläche.

Beispiel. (i) Sei $n = 1$, $f = X^2 + 1$. Dann gilt $V(f) = \{\pm\sqrt{-1}\}$. Dies sind zwei oder ein Punkt. Es ist nämlich

$$\sqrt{-1} = -\sqrt{-1} \Leftrightarrow 2\sqrt{-1} = 0 \Leftrightarrow 2 = 0$$

Zur Erinnerung: Der Körper k hat Charakteristik 2 falls $2 = 0$ in k .

(ii) Sei $n = 2$, $S = X^2 + Y^2 - 1$. Dies ist eine nicht-degenerierte Quadrik (für die Teilnehmer des Proseminars). $V(f)$ hat unendliche viele Punkte - für jede Wahl von $x \in k$ zwei oder einen Wert y . Über den reellen Zahlen erhalten wir einen Kreis, aber natürlich ist \mathbb{R} nicht algebraisch abgeschlossen. Über den komplexen Zahlen ist $V(f)$ als Mannigfaltigkeit eine Kugel.

(iii) $n = 2$, $S = \{X^2 + Y^2 - 1, X + 3Y\}$

$$x = -3y \Rightarrow 1 = 9y^2 + y^2 = 10y^2$$

Falls die Charakteristik von k gleich 2 oder 5 ist, so ist die Gleichung unlösbar, also $V(S) = \emptyset$. Andernfalls ist $y = \pm 10^{-\frac{1}{2}}$ und $V(S)$ besteht aus zwei Punkten.

(iv) Sei $k = \mathbb{C}$, $n = 1$, $f = \sin(z)$. Dann ist

$$\{\sin(z) = 0\} = \mathbb{Z}\pi$$

Dies ist *keine* algebraische Menge. Zunächst ist \sin kein Polynom. Ist $g \in \mathbb{C}[Z]$ ein Polynom, so hat $V(g)$ nur endlich viele Nullstellen, während $\sin(z)$ unendlich viele hat.

Lemma 0.2. Sei $V(S) \subset \mathbb{A}_k^1$ eine algebraische Menge. Dann ist entweder $V(S) = \mathbb{A}^1$ oder $V(S)$ hat nur endlich viele Elemente.

Beweis: Angenommen, es gibt $f \in S$ mit $f \neq 0$. Dann ist $V(S) \subset V(f)$. Als Polynom in einer Variablen hat f nur endlich viele Nullstellen. Andernfalls ist $S = \emptyset$ oder $S = \{0\}$ und wir haben $V(S) = \mathbb{A}_k^1$. \square

Bemerkung. Unterschiedliche Gleichungen können also die Gleiche algebraische Menge definieren.

Allgemein bestehen alle null-dimensionalen algebraischen Mengen nur aus endlich vielen Punkten - aber dafür müssten wir erstmal definieren, was die Dimension einer Varietät ist. Dies (wie vieles andere auch) lesen wir an einem Ring ab, der zur Varietät gehört.

Definition 0.3. Sei k ein algebraisch abgeschlossener Körper, $S \subset k[X_1, \dots, X_n]$ eine Teilmenge, $V = V(S)$. Dann heißt

$\mathcal{O}(V) = k[V] = \{f : V \rightarrow k \mid \text{es gibt } F \in k[X_1, \dots, X_n],$

$$f(x_1, \dots, x_n) = F(x_1, \dots, x_n) \text{ für alle } (x_1, \dots, x_n) \in V\}$$

affiner Koordinatenring von V . Die Elemente von $k[V]$ heißen algebraische Funktionen auf V .

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

$$k[V] \cong k^d \quad f \mapsto (f(P_i))_{i=1}^d$$

wobei k^d mit der komponentenweisen Addition und Multiplikation zu einem Ring wird.

Beweis: Nach Definition von $k[V]$ ist die Zuordnung ein injektiver Ringhomomorphismus. Sei nun $(a_1, \dots, a_n) \in k^d$ ein Tupel. Das Polynom

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

erfüllt $F(P_i) = a_i$, denn P_i ist Nullstelle jedes Summanden außer dem zu i . Dies ist das gesuchte Urbild. \square

Inhalt der Vorlesung

Wir wollen die Eigenschaften von algebraischen Mengen verstehen, dies bedeutet automatisch, dass wir ihre Koordinatenringe verstehen müssen. Dazu werden wir die Grundlagen der kommutativen Algebra erarbeiten, die auch in anderen Situationen angewendet wird, etwa in der algebraischen Zahlentheorie.

Konkret:

- (i) Korrespondenz von affinen Varietäten und Koordinatenringen: Ideale, Hilbertscher Nullstellensatz
- (ii) Zur Definition einer affinen Varietät reichen endlich viele Gleichungen aus: Theorie der noetherschen Ringe und Moduln
- (iii) Funktionenkörper und lokale Ringe: Lokalisierung von Ringen und Moduln
- (iv) Dimensionstheorie: ganze Ringerweiterungen und ihre Eigenschaften
- (v) Singularitäten und Glattheit: reguläre Ringe
- (vi) Schnitte von Untervarietäten und Satz von Bezout: Graduierte Ringe, Hilbert-Samuel-Polynome

Vermutlich ist dann das Semester lange vorbei. Sonst wären algebraische Kurven und Riemann-Roch das natürliche nächste Ziel.

Literatur

kommutative Algebra:

- Atiyah, MacDonald, Introduction to commutative algebra.
Das Wichtigste schön kurz und knapp, aber auch sehr dicht geschrieben.
Enthält Unmengen von Übungsaufgaben.
- Zariski, Samuel, Commutative algebra, Vol 1 und 2
Klassiker. Enthält das Doppelte an Stoff, reicht auch für vertiefende Vorlesungen in algebraischer Geometrie.
- Bourbaki, Algèbre commutative (oder Commutative algebra)
Enzyklopädisch, eher zum Nachschlagen als zum Erarbeiten.
- Matsumura, Commutative ring theory.
- Matsumura, Commutative algebra.
Die beiden Matsumuras sind zwei verschiedene Bücher, nicht Neuauflage oder Band 1 und 2. Sie sind weder überschneidungsfrei noch deckungsgleich. Thematisch ähnlich ausführlich wie Zariski, Samuel, aber moderner.
- Eisenbud: Commutative algebra. With a view toward algebraic geometry.
Kenne ich noch nicht. Der Titel klingt genau richtig für unsere Vorlesung, der Inhalt scheint aber deutlich weiter zu gehen.

algebraische Geometrie:

Die Bücher zur algebraischen Geometrie fallen in (mindestens) drei Gruppen, je nachdem, was für k erlaubt ist:

- (i) k algebraisch abgeschlossen. Das ist unser Fall, Theorie der Varietäten. Etwas veraltet, aber gut zugänglich.
 - (ii) $k = \mathbb{C}$ mit Einsatz von analytischen Methoden, oft eine schöne Ergänzung, wenn man sich in Funktionentheorie auskennt.
 - (iii) k beliebiger Ring, Theorie der Schemata. Der allgemeinste Fall. Die Theorie der Varietäten ist ein Spezialfall, nicht etwa Voraussetzung. Da ich Zahlentheoretikerin bin, ist $k = \mathbb{Z}$ für mich besonders interessant. Wir werden uns aber dieses Semester (noch) nicht mit Schemata beschäftigen. Wer bei mir promoviert, kommt um Schemata nicht herum, wer Diplom macht vielleicht.
- Reid, Undergraduate Algebraic Geometry
Knapp, gut lesbar, übersichtlich wie ein Vorlesungsskript, umfasst aber nicht den ganzen Stoff der Vorlesung.
 - Shafarevich, Basic algebraic geometry
Klassiker, sehr geometrisch, enthält das meiste, was man über Varietäten sagen kann.

- Fulton, Algebraic Curves
Nach einer allgemeinen Einführung konzentriert sich der Text auf ebene Kurven, Bezout fehlt. Versucht mit möglichst wenig Technik auszukommen, ein wenig zu wenig für meinen Geschmack. Schöner Beweis von Riemann-Roch.
- Hartshorne, Algebraic Geometry
Kapitel I behandelt Varietäten einschließlich der Schnitttheorie im projektiven Raum, wie sie in der Vorlesung drankommt. Danach kommen Schemata und Kohomologie. Mir haben Kapitel II und III für die Promotion und noch einiges mehr gereicht.
- Mumford, The red book of varieties and schemes
Die erste Hälfte Varietäten, die zweite Schemata. Im Niveau deutlich unter Hartshorne. Ich mag es persönlich sehr gerne, insbesondere wird die Dimensionstheorie vermutlich diesem Text folgen.
- Griffith, Harris, Principles of algebraic geometry.
Klassiker über \mathbb{C} mit viel komplexer Analysis. Passt nicht zur Vorlesung, ist aber sonst sehr schön.
- Grothendieck *Éléments de géométrie algébrique.*, kurz EGA
Die Originalquelle zu Schemata. Enthält alle Grundlagen. Wer sich die Mühe macht, den Text komplett durchzuarbeiten, hat dann eine tolle Grundlage. Es sind mehrere Bände der Zeitschrift Publ. IHES, nämlich 4, 8, 11, 20, 24, 28, 32.

Kapitel 1

Grundbegriffe der algebraischen Geometrie

Den Begriff der affinen Menge und des Rings der algebraischen Funktionen kennen wir ja schon. Sei weiterhin k ein algebraisch abgeschlossener Körper. Alle Ringe sind kommutativ mit 1.

Definition 1.1. Sei $V \subset \mathbb{A}^n$ eine algebraische Menge. Es sei

$$I(V) = \{f \in \mathcal{O}(\mathbb{A}^n) \mid f(P) = 0 \text{ für alle } P \in V\}$$

das Verschwindungsideal von V .

Bemerkung. (i) Falls $V = V(S)$ für $S \subset k[X_1, \dots, X_n]$, so gilt nach Definition $S \subset I(V)$.

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

$$(f + g)(P) = f(P) + g(P) = 0 + 0 = 0 \text{ für alle } P \in V$$

(iii) Für $f \in I(V)$ und $g \in k[X_1, \dots, X_n]$ gilt $gf \in I(V)$, denn

$$(gf)(P) = g(P)f(P) = g(P)0 = 0 \text{ für alle } P \in V$$

D.h. $I(V)$ ist ein Ideal.

Definition 1.2. Sei A ein Ring. Eine Untergruppe $I \subset A$ heißt Ideal, falls für alle $x \in I$, $a \in A$ gilt $ax \in I$.

Lemma 1.3. Sei $\phi : A \rightarrow B$ ein Ringhomomorphismus. Dann ist $\text{Ker}(\phi)$ ein Ideal.

Beweis: Sei $a \in A$, $x \in \text{Ker}(\phi)$. Dann folgt

$$\phi(ax) = \phi(a)\phi(x) = \phi(a)0 = 0$$

□

8 KAPITEL 1. GRUNDBEGRIFFE DER ALGEBRAISCHEN GEOMETRIE

Nach Definition gilt $I(V) = \text{Ker}(\varrho)$, wobei ϱ die Einschränkungabbildung $\mathcal{O}(\mathbb{A}^n) \rightarrow \mathcal{O}(V)$ ist.

Satz 1.4. *Sei A ein Ring, $I \subsetneq A$ ein Ideal. Dann ist die Menge der Nebenklassen*

$$A/I := \{a + I \mid a \in A\}$$

mit der Addition und Multiplikation von Nebenklassen

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I \\ (a + I)(b + I) &= ab + I \end{aligned}$$

ein Ring. Die Projektionsabbildung $A \rightarrow A/I$ mit $a \mapsto a + I$ ist ein Ringhomomorphismus mit Kern I .

Beweis: Wie bei Quotientenvektorräumen und Restklassengruppen ist das Problem die Wohldefiniertheit von Addition und Multiplikation. Die Rechnung für die Addition ist die gleiche wie für Vektorräume. Interessanter ist die Multiplikation. Sei $a + I = a' + I$

Behauptung. $ab + I = a'b + I$

Die Voraussetzung ist äquivalent zu $a - a' \in I$. Da I ein Ideal ist, ist dann auch $ab - a'b = (a - a')b \in I$. Dies ist die Behauptung.

Der Rest folgt wie für Vektorräume.

Die Bedingung $I \neq A$ wird benötigt, damit im Restklassenring $1 + I \neq 0 + I$. \square

Korollar 1.5. *Sei $V \subset \mathbb{A}^n$ eine algebraische Menge. Dann gilt*

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

Beweis: Die Restriktionsabbildung $\varrho : \mathcal{O}(\mathbb{A}^n) \rightarrow \mathcal{O}(V)$ ist nach Definition surjektiv mit Kern $I(V)$. Daher ist die induzierte Abbildung

$$\bar{\varrho} : \mathcal{O}(\mathbb{A}^n)/I(V) \rightarrow \mathcal{O}(V) \quad f + I(V) \mapsto \varrho(f)$$

bijektiv. \square

Hier haben wir bereits den Homomorphiesatz verwendet:

Satz 1.6 (Homomorphiesatz). *Sei $\phi : A \rightarrow B$ ein Ringhomomorphismus mit Kern I . Dann ist*

$$\bar{\phi} : A/I \rightarrow \text{Im}(\phi) \quad a + I \mapsto \phi(a)$$

ein Ringisomorphismus.

Beweis: Wie für Vektorräume oder Gruppen. \square

Definition 1.7. Sei A ein Ring, $S \subset A$ eine Teilmenge. Dann setzen wir

$$\langle S \rangle = \bigcap_{S \subset I \subset A} I$$

den Schnitt aller Ideale I , die S enthalten. Dies ist das von S erzeugte Ideal.

Korollar 1.8. Sei $S \subset k[X_1, \dots, X_n]$ eine Teilmenge, $V = V(S)$ die zugehörige algebraische Menge. Dann ist

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

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

Gilt vielleicht sogar Gleichheit?

Beispiel. Sei $S = \{XY\} \subset k[X, Y]$, also $\langle XY \rangle = kXY$. Es ist

$$V(XY) = \{(x, y) \in k^2 \mid xy = 0\} = \{(0, y) \mid y \in k\} \cup \{(x, 0) \mid x \in k\}$$

das Achsenkreuz in der Ebene. Wir berechnen $I = I(V(XY))$. Sei $f = \sum_{i,j} a_{ij} X^i Y^j \in I$. Dann gilt

$$f(0, y) = \sum_{i,j} a_{ij} 0^i Y^j = \sum_j a_{0j} y^j = 0 \text{ für alle } y \in k$$

Da k algebraisch abgeschlossen ist, ist dies nur möglich, falls $a_{0j} = 0$ für alle j . Ebenso folgt $a_{i0} = 0$ für alle i . In anderen Worten: $a_{ij} \neq 0 \Rightarrow i, j > 0$. Damit ist f ein Vielfaches von XY . Es gilt tatsächlich $I = \langle XY \rangle$.

Beispiel. Sei $S = \{X^2\} \subset k[X]$. Dann ist $\langle X^2 \rangle = k[X]X^2$, $V = \{0\}$ und $I(V) = k[X]X$. Die Gleichungen X und X^2 definieren dieselbe algebraische Menge!

Definition 1.9. Sei $I \subset A$ ein Ideal. Dann heißt

$$\sqrt{I} = \{x \in A \mid \text{es gibt } n \in \mathbb{N} \text{ mit } x^n \in I\}$$

Radikal von I .

Lemma 1.10. Das Radikal ist ein Ideal.

Beweis: Seien $x, y \in \sqrt{I}$, $x^n, y^m \in I$. Dann ist

$$(xy)^n = x^n y^n \in I$$

da I ein Ideal. Außerdem

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

Falls $i \geq n$, so ist der Summand in I , da $x^i \in I$. Andernfalls ist $i < n$ und daher $m+n-i \geq m$. Dann ist der Summand in I , da $y^{m+n-i} \in I$. Jeder Summand ist in I , also auch die Summe. □

Korollar 1.11. Sei $S \subset k[X_1, \dots, X_n]$ eine Teilmenge, $V = V(S)$ die zugehörige affine Varietät. Dann gilt

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

Beweis: Sei $f \in \sqrt{\langle S \rangle}$, $f^n \in \langle S \rangle \subset I(V)$, d.h. $f(P)^n = f^n(P) = 0$ für alle $P \in V$. Da k ein Körper ist, folgt $f(P) = 0$. \square

Hier gilt tatsächlich Gleichheit! Das wird unser erstes großes Ziel sein, der Hilbertsche Nullstellensatz.

Bemerkung. Bisher haben wir nicht benutzt, dass k algebraisch abgeschlossen ist. Schon der Fall $n = 1$ zeigt aber, dass die Voraussetzung für den Hilbertschen Nullstellensatz nötig ist.

Zunächst aber noch etwas mehr Geometrie.

Zariski-Topologie

Definition 1.12. Sei $V \subset \mathbb{A}^n$ eine algebraische Menge. Eine Teilmenge $W \subset V$ heißt abgeschlossen, wenn W selbst eine algebraische Menge ist. Eine Teilmenge $U \subset V$ heißt offen, wenn $V \setminus U$ abgeschlossen ist.

Satz 1.13. Dies ist eine Topologie, die Zariski-Topologie.

Beweis: Wir müssen die Axiome eines topologischen Raums überprüfen.

- (i) \emptyset und V sind offen $\Leftrightarrow V$ und \emptyset sind abgeschlossen.
- (ii) Der Schnitt zweier offener Menge ist offen \Leftrightarrow Die Vereinigung zweier offener Mengen ist abgeschlossen.
- (iii) Die Vereinigung beliebig vieler offener Mengen ist offen \Leftrightarrow Der Schnitt von beliebig vielen abgeschlossenen Mengen ist abgeschlossen.

Zu (i): Wir wählen $S = \{0\}$ und $S = \{1\}$.

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

Behauptung. $W_1 \cup W_2 = V(S_1 S_2)$

Hier bedeutet $S_1 S_2 = \{f_1 f_2 \mid f_1 \in S_1, f_2 \in S_2\}$. Sei $P \in W_1$, also $f(P) = 0$ für alle $f \in S_1$. Dann folgt

$$fg(P) = 0 \text{ für alle } f \in S_1, g \in S_2$$

d.h. wir haben $W_1 \subset V(S_1 S_2)$. Ebenso für W_2 . Sei nun umgekehrt $P \in V(S_1 S_2)$, dh. $fg(P) = 0$ für alle $f \in S_1, g \in S_2$. Entweder ist $P \in W_1$, d.h. $f(P) = 0$ für alle $f \in S_1$. Oder es gibt ein $f_0 \in S_1$ mit $f_0(P) \neq 0$. Dann gilt für alle $g \in S_2$

$$0 = f_0(P)g(P) \Rightarrow g(P) = 0$$

In diesem Fall ist $P \in W_2$.

Zu (iii): Sei $W_\alpha = V(S_\alpha)$. Dann gilt

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

(einfach). □

In dieser Sprache sind die algebraischen Mengen die abgeschlossenen Teilmengen des \mathbb{A}^n .

Beispiel. Eine Teilmenge von $\mathbb{A}^1 = k$ ist abgeschlossen, wenn sie gleich k ist oder nur endliche viele Elemente hat. Die Topologie ist also ganz anders als bei metrischen Räumen. Je zwei offene nichtleere Mengen haben einen nichtleeren Schnitt. Jede unendliche Menge ist dicht!

Definition 1.14. *Eine algebraische Menge $V \subset \mathbb{A}^n$ mit der Zariski-Topologie heißt affine Varietät. Eine offene Teilmenge von V mit der induzierten Topologie heißt quasi-affine Varietät.*

Bemerkung. Nicht alle quasi-affinen Varietäten sind affin, z.B. $\mathbb{A}^2 \setminus \{0\}$. Das können wir aber erst später beweisen.

Bemerkung. In der älteren Literatur wird der Begriff Varietät meist für irreduzible Varietäten reserviert, dazu kommen wir noch.

12KAPITEL 1. GRUNDBEGRIFFE DER ALGEBRAISCHEN GEOMETRIE

Kapitel 2

Noethersche Ringe und Moduln

Definition 2.1. Sei A ein Ring, $I \subset A$ ein Ideal. I heißt endlich erzeugt, wenn es eine endliche Menge $S \subset I$ gibt mit $\langle S \rangle = I$.

Ein Ring heißt noethersch, wenn jedes Ideal endlich erzeugt ist.

Beispiel. (i) Sei K ein Körper. Dann gibt es nur zwei Ideale 0 und K , denn falls ein Ideal I ein Element $x \neq 0$ enthält, dann auch $x^{-1}x = 1$ und damit ganz K . Insbesondere ist jedes Ideal endlich erzeugt.

(ii) Im Falle $A = \mathbb{Z}$ sind alle Ideale von der Form (n) für $n \in \mathbb{Z}$ (das gilt sogar für die Untergruppen von \mathbb{Z} !), werden also von nur einem Element erzeugt. Solche Ideale heißen *Hauptideale*, solche Ringe heißen *Hauptidealringe*. Hauptidealringe sind noethersch.

(iii) $A = K[X]$ (K ein Körper) ist ebenfalls ein Hauptidealring. Die Ideale werden von den irreduziblen Polynomen erzeugt. (Übungsaufgabe)

Lemma 2.2. Sei $f : A \rightarrow B$ ein surjektiver Ringhomomorphismus und A noethersch. Dann ist B noethersch.

Beweis: Sei $I \subset B$ ein Ideal. Dann ist $f^{-1}I \subset A$ ebenfalls ein Ideal. Da A noethersch ist, ist $f^{-1}I$ endlich erzeugt über A . Da f surjektiv ist, ist dann auch I endlich erzeugt über B . \square

Unser Ziel ist es zu zeigen, dass für jede algebraische Menge der Ring $\mathcal{O}(V)$ noethersch ist. Dafür brauchen wir aber Rechenregeln für noethersche Ringe. Es hilft, wenn wir verallgemeinern und gleich noethersche Moduln betrachten.

Moduln

Definition 2.3. Sei A ein Ring. Ein A -Modul M ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Skalarmultiplikation

$$A \times M \rightarrow M$$

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

$$(i) \quad a(x + y) = ax + ay,$$

$$(ii) \quad (a + b)x = ax + bx,$$

$$(iii) \quad a(bx) = (ab)x,$$

$$(iv) \quad 1x = x.$$

Seien M, N Moduln. Eine Abbildung $f : M \rightarrow N$ ist ein Modulhomomorphismus, falls sie ein Homomorphismus abelscher Gruppen ist und zusätzlich für alle $a \in A$, $x \in M$ gilt: $f(ax) = af(x)$.

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

(ii) Ein \mathbb{Z} -Modul ist das Gleiche wie eine abelsche Gruppe. Modulhomomorphismen von \mathbb{Z} -Moduln sind genau die Gruppenhomomorphismen. Präzise: Die Kategorie der abelschen Gruppen ist isomorph zur Kategorie der \mathbb{Z} -Moduln.

Beweis: Sei M ein \mathbb{Z} -Modul, dann ist nach Definition $(M, +)$ eine abelsche Gruppe. Interessant ist also die Gegenrichtung. Sei M eine abelsche Gruppe, $x \in M$, $n \in \mathbb{N}$. Wir definieren $nx = x + (n-1)x$. Für negative n setzen wir $nx = -(-n)x$. Die Modulaxiome gelten alle. Man beweist alles mit Induktion, z.B.

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

□

Man sieht an der Beispielrechnung, dass die Kommutativität von M wirklich benötigt wird.

(iii) Sei K ein Körper. Ein $K[X]$ -Modul ist dasselbe wie ein K -Vektorraum V zusammen mit einem K -Endomorphismus $\phi : V \rightarrow V$.

Beweis: Sei V ein $K[X]$ -Modul. Durch Einschränken der skalaren Multiplikation auf konstante Polynome erhält man K -Vektorraumstruktur. Die Multiplikation mit X ist eine K -lineare Abbildung $V \rightarrow V$. Ist umgekehrt

V ein K -Vektorraum mit Endomorphismus ϕ , so definieren wir die skalare Multiplikation als

$$\left(\sum_{i=0}^n a_i X^i\right)v = \sum_{i=0}^n a_i \phi^i(v) \quad n \geq 0, a_i \in K, v \in V$$

Man überprüft leicht die Modulaxiome. \square

Sätze über Vektorräume mit Endomorphismus aus der LA 2 (z.B. Jordansche Normalform) sind in Wirklichkeit Sätze über $K[X]$ -Moduln.

Bemerkung. Ob A eine Eins hat, ist für die allgemeine Theorie nicht wichtig. Ist A nicht kommutativ, so muss man unterscheiden zwischen *Linksmoduln* (Formeln wie oben) und *Rechtsmoduln* mit einer skalaren Multiplikation $M \times A \rightarrow M$, so dass das Axiom (iii) gilt in der Form: $(ma)b = m(ab)$ für alle $m \in M, a, b \in A$. Man unterscheidet dann auch zwischen Links- und Rechtsidealen. Zweiseitige Ideale sind dann diejenigen, so dass A/I wieder ein Ring wird.

Die Grundlagen der Theorie funktionieren wie für Körper. Begriffe wie linear unabhängig, Erzeugendensystem, direkte Summe, Untermodul, Quotientenmodul etc. werden genau wie in der linearen Algebra definiert. Ein Modul heißt *endlich erzeugt*, wenn er ein endliches Erzeugendensystem hat.

Beim Begriff der Basis muss man aufpassen:

Definition 2.4. Sei M ein A -Modul. Ein linear unabhängiges Erzeugendensystem von M heißt *Basis*. M heißt *frei*, falls es eine Basis gibt. Die *Mächtigkeit* einer Basis heißt *Rang* von M .

Der Rang eines Moduls ist wohldefiniert, d.h. unabhängig von der Wahl der Basis (Reduktion auf den Fall eines Körpers, Übungsaufgabe).

Beispiel. (i) Wenn A ein Körper ist, so sind alle Moduln frei. (Basisexistenzsatz, Lineare Algebra). Der Rang ist nichts anderes als die Dimension.

(ii) Sei $A = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z}$. Dieser Modul ist nicht frei, denn für jedes Element gilt $2x = 0$. Es gibt keine linear unabhängigen Teilmengen!

(iii) A^2 ist frei vom Rang 2 mit Basis $\{(1, 0), (0, 1)\}$.

Beispiel. A ist auch ein A -Modul. Die Untermoduln von A sind genau die Ideale. Ist $A \rightarrow B$ ein Ringhomomorphismus, so ist B ein A -Modul.

Wie in der linearen Algebra sind Kern und Bild eines Modulhomomorphismus Untermoduln. Ist $N \subset M$ ein Untermodul, so ist M/N ein Modul mit der induzierten Skalarmultiplikation. Ist speziell $M = A$ der Ring und $N \subsetneq M$, so erhalten wir den Ring A/N zurück.

Satz 2.5 (Homomorphiesatz, Noethersche Isomorphiesätze). *Sei $f : M \rightarrow N$ ein A -Modulhomomorphismus. Dann ist die induzierte Abbildung*

$$\bar{f} : M/\text{Ker } f \rightarrow \text{Im } f$$

ein Isomorphismus von A -Moduln. Sind $N, N' \subset M$ Untermoduln, so ist

$$(N + N')/N \cong N'/(N \cap N')$$

ein kanonischer Isomorphismus. Sind $N' \subset N \subset M$ Untermoduln, so ist

$$(M/N')/(N/N') \cong M/N$$

ein kanonischer Isomorphismus.

Beweis: In der Algebra zeigt man diese Aussagen für abelsche Gruppen, in der linearen Algebra für Vektorräume. Die Verträglichkeit mit der A -Modulstruktur ist leicht zu überprüfen. Wir zeigen beispielhaft die zweite Aussage. Wir betrachten den Homomorphismus

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

Er hat den Kern $\{x \in N' \mid x + N = 0\} = N \cap N'$. Nach dem Homomorphiesatz erhalten wir eine Isomorphismus

$$\bar{f} : N'/N' \cap N \rightarrow \text{Im}(f)$$

Zu zeigen bleibt die Surjektivität von f . Ein beliebiges Element von $(N + N')/N$ hat die Form $x + x' + N$ mit $x \in N$ und $x' \in N'$. Wegen $x + x' + N = x + N = f(x)$ liegt es im Bild. \square

Noethersche Moduln

Definition 2.6. *Sei A ein Ring, M ein A -Modul. M heißt noethersch, wenn jede Kette von Untermoduln von M*

$$M_1 \subset M_2 \subset \dots \subset M$$

stationär wird, d.h. es gibt $n \in \mathbb{N}$ mit $M_i = M_{i+1}$ für alle $i \geq n$.

Lemma 2.7. *Ein Modul ist genau dann noethersch, wenn jeder Untermodul endlich erzeugt ist. Ein Ring ist noethersch, wenn er noethersch ist als Modul über sich selbst.*

Beweis: Sei A ein Ring, M ein A -Modul, $N \subset M$ ein Untermodul. Angenommen, N ist nicht endlich erzeugt. Wir konstruieren eine Folge von Elementen $x_1, x_2, \dots \in N$ mit

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

Sei $x_1 \in N$ beliebig. Angenommen, wir haben x_1, \dots, x_n konstruiert. Da N nicht endlich erzeugt ist, gilt $\langle x_1, \dots, x_n \rangle \neq N$. Wir wählen $x_{n+1} \in N \setminus \langle x_1, \dots, x_n \rangle$. Dies hat die gewünschte Eigenschaft. Die Folge von Untermoduln wird nicht stabil, also ist M nicht noethersch.

Sei umgekehrt jeder Untermodul von M endlich erzeugt. Wir betrachten eine Folge von Untermoduln

$$N_1 \subset N_2 \subset N_3 \subset \dots$$

Es sei $N = \bigcup_i N_i$.

Behauptung. N ist ein Untermodul.

Seien $x, y \in N$, $a, b \in A$. Nach Voraussetzung ist $x \in N_i$ und $y \in N_j$ für geeignete i, j . Ohne Einschränkung ist $i \geq j$. Nach Voraussetzung ist $N_j \subset N_i$, also $x, y \in N_i$. Da N_i ein Untermodul ist, gilt $ax + by \in N_i \subset N$.

Nach Voraussetzung ist N endlich erzeugt. Seien x_1, \dots, x_m Erzeuger. Jedes x_i liegt in einem N_{k_i} . Sei $k = \max_i k_i$. Dann liegen alle x_i in N_k . Dies bedeutet

$$N = \langle x_1, \dots, x_m \rangle \subset N_k \subset N$$

also Gleichheit.

Sei nun A ein noetherscher Ring. Nach Definition sind alle Ideale, also alle Untermoduln von A endlich erzeugt. Nach der ersten Hälfte des Lemmas ist A noethersch als A -Modul. Ebenso folgt die Umkehrung. \square

Es gibt eigentlich nur eine Rechenregel für noethersche Moduln. Um die zu formulieren, führen wir die Sprache der exakten Sequenzen und kommutativen Diagramme ein. Wenn man sich daran gewöhnt hat, ist es eine sehr effiziente Art der Buchhaltung.

Definition 2.8. Eine (endliche oder unendliche) Folge von Modulhomomorphismen

$$N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3 \rightarrow \dots \rightarrow N_n$$

heißt exakt, falls für $1 < i < n$ gilt

$$\text{Im}(f_{i-1}) = \text{Ker}(f_i)$$

Beispiel. (i) $0 \rightarrow N_1 \xrightarrow{f} N_2$ ist genau dann exakt, wenn f injektiv ist: Das Bild der Nullabbildung ist der Nullmodul, also lautet die Bedingung $0 = \text{Ker}(f)$.

(ii) $M_1 \xrightarrow{g} M_2 \rightarrow 0$ ist genau dann exakt, wenn g surjektiv ist: Der Kern der Nullabbildung ist ganz M_2 , also lautet die Bedingung $\text{Im}(g) = M_2$.

(iii) $0 \rightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \rightarrow 0$ ist genau dann exakt, wenn g surjektiv ist mit Kern gleich $\text{Im}(f) \cong M_1$. Solche exakten Sequenzen heißen *kurze exakte Sequenz*.

Definition 2.9. Ein Diagramm von A -Moduln

$$\begin{array}{ccc} M_1 & \xrightarrow{f_1} & M_2 \\ g_1 \uparrow & & \uparrow g_2 \\ N_1 & \xrightarrow{f_2} & N_2 \end{array}$$

heißt kommutativ, wenn $f_1 g_1 = g_2 f_2$.

Lemma 2.10. Sei A ein Ring,

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

eine kurze exakte Sequenz. Dann ist M_2 genau dann noethersch, wenn M_1 und M_3 noethersch sind.

Beweis: Sei M_2 noethersch.

Behauptung. M_1 ist noethersch.

M_1 ist ein Untermodul von M_2 . Alle Untermoduln von M_1 sind auch Untermoduln von M_2 , also endlich erzeugt.

Behauptung. M_3 ist noethersch.

Sei $\pi : M_2 \rightarrow M_3$ die surjektive Abbildung. Gegeben sei eine Folge

$$N_1 \subset N_2 \subset \dots$$

von Untermoduln von M_3 . Wir betrachten die Urbildfolge

$$\pi^{-1}N_1 \subset \pi^{-1}N_2 \subset \dots$$

von Untermoduln von M_2 . Da M_2 noethersch ist, wird die Folge stabil. Wegen $N_i \cong \pi^{-1}N_i/M_1$ (Homomorphiesatz) ist dann auch die Ausgangsfolge stabil.

Seien nun M_1, M_3 beide noethersch. Wir betrachten eine Folge

$$X_1 \subset X_2 \subset \dots$$

von Untermoduln von M_2 .

Behauptung. Die Folge wird stabil.

Zu jedem X_i gehört eine kurze exakte Sequenz (Homomorphiesatz)

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

Die Folge der $X_i \cap M_1$ wird stabil, da M_1 noethersch. Die Folge $\pi(X_i)$ wird stabil, da M_3 noethersch. Für genügend großes i haben wir die Situation

$$\begin{array}{ccccccc} 0 & \longrightarrow & X_{i+1} \cap M_1 & \longrightarrow & X_{i+1} & \longrightarrow & \pi(X_{i+1}) \longrightarrow 0 \\ & & \cong \uparrow & & \uparrow \subset & & \uparrow \cong \\ 0 & \longrightarrow & X_i \cap M_1 & \longrightarrow & X_i & \longrightarrow & \pi(X_i) \longrightarrow 0 \end{array}$$

Wir wollen zeigen, dass $X_i \rightarrow X_{i+1}$ surjektiv ist. Sei also $x \in X_{i+1}$. Dann hat $\pi(x)$ ein Urbild in $\pi(X_i)$. Dieses hat wiederum ein Urbild $x' \in X_i$. Wir betrachten nun $y = x - x' \in X_{i+1}$. Es liegt nach Konstruktion im Kern von π , also im Bild von $X_{i+1} \cap M_1$. Nach Voraussetzung hat y dann ein Urbild in $X_i \cap M_1$, also erst recht in X_i . Wegen $x = x' + y$ haben wir ein Urbild für x gefunden. \square

Korollar 2.11. *Sei A ein noetherscher Ring, M endlich erzeugter A -Modul. Dann ist M noethersch.*

Beweis: A ist noethersch als A -Modul. Durch wiederholtes Anwenden von Lemma 2.10 sehen wir, dass $A^n = A \oplus A \oplus A \dots A$ noethersch ist für alle $n \in \mathbb{N}$. Seien x_1, \dots, x_n Erzeuger von M . Dann definiert

$$A^n \rightarrow M \quad (a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i x_i$$

einen surjektiven Modulhomomorphismus. Nach Lemma 2.10 ist M noethersch. \square

Leider kennen wir nur wenige noethersche Ringe. Das folgende Theorem ändert das ganz dramatisch.

Theorem 2.12 (Hilbertscher Basissatz). *Sei A ein noetherscher Ring. Dann ist der Polynomring $A[X]$ noethersch.*

Beweis: Sei $I \subset A[X]$ ein Ideal. Wir suchen nach endlich vielen Erzeugern. Um zu verstehen, wie wir vorgehen müssen, erinnern wir uns an den Fall, dass $A = K$ ein Körper ist. Dann wissen wir ja, dass jedes Ideal von nur einem Element erzeugt wird. Wir finden den Erzeuger als ein Polynom minimalen Grades ungleich 0. Das jedes solches Element ein Erzeuger ist, wird mit Hilfe des euklidischen Algorithmus (also Polynomdivision) gezeigt. Dies müssen wir variieren, da wir durch Koeffizienten nicht dividieren können. Daher: Für jedes $n \geq 0$ sei $I_n \subset A[X]$ die Menge der Polynome vom Grad kleiner gleich n . Dies ist ein A -Modul. Sei

$$J_n = \{a \in A \mid \text{es gibt } P \in I_n, P = aX^n + \dots\}$$

Dies ist ein Ideal von A , also endlich erzeugt. Wegen $XI_n \subset I_{n+1}$ gilt $J_n \subset J_{n+1}$. Da A noethersch ist, wird die Folge von Koeffizientenidealen

$$J_0 \subset J_1 \subset J_2 \dots$$

konstant. Sei $I_n = J_d$ für alle $n \geq d$. Wir wählen für $n \leq d$ A -Erzeuger $a_1^{(n)}, a_2^{(n)}, \dots, a_{r_n}^{(n)} \in J_n$. Wir wählen weiter $P_j^{(n)} \in I_n$ mit

$$P_j^{(n)} = a_j^n X^n + \dots$$

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

Sei $Q = bX^m + \dots$. Der Beweis wird durch Induktion über m geführt. Sei zunächst $m \leq d$. Wir rechnen in I_m und J_m . Dann gibt es $c_1, \dots, c_{r_m} \in A$, so dass

$$b = \sum_{i=1}^{r_m} c_i a_i^{(m)}$$

Es folgt:

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

hat Grad echt kleiner als m . Nach Induktionsannahme wird es durch die Erzeuger ausgedrückt, daher gilt dasselbe auch für Q .

Sei nun $m \geq d$. Dann gibt es $c_1, \dots, c_{r_d} \in A$, so dass

$$b = \sum_{i=1}^{r_d} c_i a_i^{(d)}$$

Es folgt

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

hat Grad echt kleiner als m . Wieder sind wir nach Induktionsannahme fertig. Der Induktionsanfang ist übrigens für $I_{-1} = 0$ □

Korollar 2.13. Sei $A = \mathbb{Z}$ oder $A = K$ ein Körper. Dann ist $A[X_1, \dots, X_n]$ noethersch.

Beweis: Induktion. □

Hieraus werden noch viel mehr Beispiele.

Definition 2.14. Sei $A \rightarrow B$ ein Ringhomomorphismus. B heißt endlich erzeugte A -Algebra, wenn es Elemente $b_1, \dots, b_n \in B$ gibt, so dass jedes Element $b \in B$ geschrieben werden kann als

$$b = \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} b_1^{i_1} b_2^{i_2} \dots b_n^{i_n} \quad a_{\underline{i}} \in A, \text{ fast alle } 0$$

(mit Multiindizes $\underline{i} = (i_1, \dots, i_n)$).

Mit anderen Worten, es gibt einen surjektiven Ringhomomorphismus

$$A[X_1, \dots, X_n] \rightarrow B \quad X_i \mapsto b_i$$

Korollar 2.15. *Sei A ein noetherscher Ring, B endlich erzeugte A -Algebra. Dann ist B noethersch.*

Beweis: Hilbertscher Basissatz und Lemma 2.2 □

Und damit endlich:

Korollar 2.16. *Sei k algebraisch abgeschlossener Körper, $V \subset \mathbb{A}^n$ eine algebraische Menge über k . Dann ist $\mathcal{O}(V)$ noethersch. Jede algebraische Menge wird durch endlich viele Gleichungen definiert. Sie ist Schnitt von endlich vielen Hyperflächen.*

Beweis: $\mathcal{O}(V) \cong k[X_1, \dots, X_n]/I(V)$ ist endlich erzeugte k -algebra, also noethersch. Als Ideal in einem noetherschen Ring ist $I(V)$ endlich erzeugt,

$$I(V) = \langle f_1, \dots, f_n \rangle$$

und offensichtlich

$$V(I(V)) = V(f_1, \dots, f_n) = \bigcap_{i=1}^n V(f_i)$$

Behauptung. $V = V(I(V))$

Sei $V = V(S)$. Wegen $S \subset I(V)$ folgt $V(S) \supset V(I(V))$. Sei $P \in V$. Nach Definition von $I(V)$ ist P Nullstelle jedes Elementes von $I(V)$, liegt also in $V(I(V))$. □

Es ist sehr schwer anzugeben oder zu charakterisieren, wieviele Gleichungen benötigt werden. Man benötigt wenigsten $n - \dim(V)$ -viele (das werden wir zeigen). Das ist auch der sogenannte generische Fall, den man für zufällige Gleichungen erwarten kann. Der allgemeine Fall ist jedoch offen!

Kapitel 3

Hilbertscher Nullstellensatz

Wir kehren nun wieder zur Varietätensituation zurück. Wir wollen die Korrespondenz von Idealen und affinen Varietäten verstehen.

$$V : \{S \subset k[X_1, \dots, X_n]\} \rightarrow \{V \subset \mathbb{A}^n\}$$

ordnet jeder Teilmenge eine abgeschlossene Teilmenge zu, die durch S definierte affine Varietät.

$$I : \{V \subset \mathbb{A}^n\} \rightarrow \{S \subset k[X_1, \dots, X_n]\}$$

ordnet jeder Teilmenge das Verschwindungsideal zu. Wir hatten bereits überprüft (Beweis von Korollar 2.16) dass

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

für alle algebraischen Mengen.

Nicht jedes Ideal kann auftauchen, denn wenn $f^n \in I(V)$ für ein $f \in \mathcal{O}(\mathbb{A}^n)$, $n \in \mathbb{N}$, so ist $f \in I(V)$.

Definition 3.1. Sei A ein Ring, $I \subset A$ ein Ideal. Ein Ideal heißt reduziert, wenn für alle $x \in A$, $n \in \mathbb{N}$ gilt:

$$x^n \in I \Rightarrow x \in I$$

Ziel ist zu beweisen:

Theorem 3.2 (Hilbertscher Nullstellensatz). Sei k algebraisch abgeschlossener Körper. Für jede Teilmenge $S \subset k[X_1, \dots, X_n]$ gilt

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

Insbesondere erhalten wir eine Bijektion zwischen reduzierten Idealen von $k[X_1, \dots, X_n]$ und abgeschlossenen Teilmengen von \mathbb{A}^n .

Dies bedeutet auch $I(V(I)) = I$ für alle reduzierten Ideale I .

Der Beweis wird noch etwas dauern. Wir beginnen mit einem Spezialfall, nämlich den maximalen Idealen.

Definition 3.3. Sei A ein Ring, $I \subset A$ ein Ideal. Dann heißt I maximal, wenn es maximal ist in der teilgeordneten Menge der echten Ideale. D.h. für alle Ideale J mit $I \subset J \subset A$ ist $I = J$ oder $J = A$.

Beispiel. Sei $P \in \mathbb{A}^n$. Dann ist $I(P) = \{f \in \mathcal{O}(\mathbb{A}^n) \mid f(P) = 0\}$ ein maximales Ideal, denn: Sei $I(P) \subset J \subset \mathcal{O}(\mathbb{A}^n)$ ein Ideal. Sei $f \in J \setminus I(P)$, d.h. $f(P) \neq 0$. Wir betrachten $f' = f - f(P)$. Dies ist ein Element von $I(P) \subset J$. Da J ein Ideal ist, folgt $f(P) \in J$. Da $f(P) \neq 0$, existiert $f(P)^{-1} \in k \subset \mathcal{O}(\mathbb{A}^n)$. Da J ein Ideal ist, liegt $1 = f(P)^{-1}f(P) \in J$.

Lemma 3.4. Sei A ein Ring, $I \subset A$ ein Ideal. Dann ist I genau dann maximal, wenn A/I ein Körper ist.

Beweis: Wir betrachten die surjektive Abbildung $\pi : A \rightarrow A/I$. $I \neq A$ ist äquivalent dazu, dass A/I ein Ring ist. Dies setzen wir voraus. Sei zunächst I maximal, $\bar{f} \in A/I$ eine Restklasse. Wir betrachten

$$I \subset \pi^{-1} \langle \bar{f} \rangle \subset A$$

Da I maximal ist, gilt entweder $I = \pi^{-1} \langle \bar{f} \rangle$ (d.h. $\pi^{-1}\bar{f} \in I \Rightarrow \bar{f} = 0$) oder $\pi^{-1} \langle \bar{f} \rangle = A$, d.h. es gibt $f \in \pi^{-1}\bar{f}$ und ein $g \in A$ mit $gf = 1$. Es folgt $\pi(g)\pi(f) = \pi(g)\bar{f} = 1$. Damit ist A/I ein Körper.

Sei umgekehrt A/I ein Körper und $I \subset J \subset A$ ein Ideal. Da $I \subset J$, gilt $J = \pi^{-1}\pi(J)$. Wir betrachten

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

In einem Körper gibt es nur zwei Ideale, daher ist entweder $\pi(J) = 0$ (also $J = \pi^{-1}\pi(J) = I$) oder $\pi(J) = A/I$ (also $J = A$). \square

Beispiel. Sei $P \in \mathbb{A}^n$ ein Punkt. Dann ist $\mathcal{O}(\mathbb{A}^n)/I(P) = \mathcal{O}(P) \cong k$. Dies ist ein Körper, also ist $I(P)$ maximal. Ist $P = (a_1, \dots, a_n) \in k^n$, so liegen die Funktionen $X_i - a_i$ für $i = 1, \dots, n$ in $I(P)$. Offensichtlich gilt sogar

$$I(P) = \langle X_1 - a_1, \dots, X_n - a_n \rangle$$

Theorem 3.5 (Schwacher Nullstellensatz). Sei k algebraisch abgeschlossen und $A = \mathcal{O}(\mathbb{A}^n)$. Dann sind alle maximalen Ideale von der Form

$$\langle X_1 - a_1, \dots, X_n - a_n \rangle \quad \text{mit } a_i \in k \text{ für } i = 1, \dots, n$$

D.h. alle Funktionen des maximalen Ideals haben eine gemeinsame Nullstelle, nämlich $P = (a_1, \dots, a_n)$.

Beispiel. Sei $n = 1$. Dann sind alle Ideale Hauptideale, d.h. erzeugt von einem Polynom. Die maximalen Ideale werden dabei von den irreduziblen Polynomen erzeugt. Da k algebraisch abgeschlossen ist, sind die irreduziblen Polynome linear.

An dieser Stelle brauchen wir einen Satz aus der Körpertheorie, der typischerweise in Algebra bewiesen wird:

Lemma 3.6. Sei K ein Körper, $K \rightarrow E = K[x]$ eine K -Algebra, die von einem Element erzeugt wird. Sei außerdem E nullteilerfrei, (d.h. $ef = 0$ impliziert $e = 0$ oder $f = 0$ für alle $e, f \in E$). Dann ist E genau dann ein Körper, wenn $\dim_K E < \infty$.

Falls E Körper ist, so heißt x algebraisch über K .

Beweis: (vergleiche Algebra) Angenommen, die Monome x^i sind K -linear unabhängig. Dann ist $\dim_K E = \infty$. Andernfalls gibt es eine nicht-triviale Relation

$$\sum_{i=0}^n a_i x^i = 0 \text{ mit } a_i \in K$$

Ohne Einschränkung ist $a_n \neq 0$.

Behauptung. $1, x, \dots, x^{n-1}$ erzeugen E als K -Vektorraum.

Klar für x^n . Multiplikation der Relation mit x macht x^{n+1} linear abhängig von x, \dots, x^n , also auch von $1, \dots, x^{n-1}$. Etc.

D.h. E ist nun ein endlich-dimensionaler Vektorraum.

Behauptung. E ist Körper.

Sei $y \in E \setminus 0$. Multiplikation mit y ist eine K -lineare Abbildung $\phi_y : E \rightarrow E$. Wegen $y1 = y$ ist dies nicht die Nullabbildung. Wir betrachten das charakteristische Polynom von ϕ_y

$$\chi = \sum_{i=0}^m b_i X^i \text{ mit } b_i \in K \quad (1)$$

Nach dem Satz von Cayley-Hamilton (lineare Algebra) ist $\chi(\phi_y) = 0$. Anwenden auf (1) ergibt

$$\sum_{i=0}^m b_i y^i = 0$$

Falls $b_0 \neq 0$, so teilen wir die Relation durch y . Da E nullteilerfrei ist, erhalten wir eine neue kürzere Relation. Durch mehrfaches Anwenden erhalten wir eine Relation mit $b_0 \neq 0$, oder ohne Einschränkung $b_0 = 1$. Dann lösen wir auf:

$$-y \sum_{i=1}^{m-1} b_i y^{i+1} = 1$$

Damit hat y ein inverses Element. □

Lemma 3.7. Sei $K \rightarrow L$ ein Körperhomomorphismus, $\dim_K L < \infty$. Sei V ein endlich-dimensionaler L -Vektorraum. Dann ist V ein endlich-dimensionaler K -Vektorraum.

Beweis: Sei e_1, \dots, e_n eine K -Basis von L . Sei v_1, \dots, v_m eine L -Basis von V . Man überzeugt sich leicht, dass $\{e_i v_j | i = 1, \dots, n, j = 1, \dots, m\}$ eine K -Basis von V ist. □

Satz 3.8. *Sei K ein Körper, $K \rightarrow E$ eine endlich erzeugte K -Algebra. Wenn E ein Körper ist, so ist E eine endliche algebraische Erweiterung von K , d.h. $\dim_K E < \infty$.*

In diesem Satz verbirgt sich die Hauptarbeit auf dem Weg zum Nullstellensatz.

Beweis: Nach Voraussetzung ist $E = K[x_1, \dots, x_n]$ für Elemente $x_i \in E$. Wir wollen mit Induktion über n argumentieren. Das Lemma soll den Induktionsschluss liefern. Wegen der Transitivität der Dimension würde das funktionieren. Wir versuchen den Schluss von K auf $K[x_1]$. Der Ring $K[x_1]$ ist nullteilerfrei (da in E enthalten). Er ist nach Lemma 3.6 genau dann endlich dimensional über K , wenn er ein Körper ist. Letzteres wissen wir aber gar nicht! Daher: Wir sortieren x_1, \dots, x_n so um, dass x_1, \dots, x_r algebraisch unabhängig sind, (d.h. für $i < r$ ist x_i nicht algebraisch über $K(x_1, \dots, x_{i-1})$, dem Körper der von x_1, \dots, x_{i-1} und K erzeugt wird), aber x_{r+1}, \dots, x_n algebraisch abhängig sind über $F = K(x_1, \dots, x_r)$. Wiederholtes Anwenden von Lemma 3.6 sowie Lemma 3.7 besagen, dass E endlich-dimensional ist als F -Vektorraum.

Behauptung. *F ist endlich erzeugt als K -Algebra.*

Sei y_1, \dots, y_m eine F -Basis von E .

Wir drücken die x_1, \dots, x_n in dieser Basis aus.

$$\begin{aligned} x_i &= \sum_{j=1}^m f_{ij} y_j & f_{ij} &\in F & (*) \\ y_i y_j &= \sum_l f_{ijl} f_{ijk} y_k & f_{ijk} &\in F \end{aligned}$$

Sei F_0 die K -Unteralgebra von F , die von den f_{ij}, f_{ijl} erzeugt wird. Es ist

$$K \subset F_0 \subset F$$

F_0 ist noethersch nach Hilbertschem Basissatz.

Unterbehauptung. *F ist endlich erzeugter F_0 -Modul.*

Wir betrachten den F_0 -Modul $\langle 1, y_1, \dots, y_m \rangle$. Da $f_{ijk} \in F_0$ ist er abgeschlossen unter Multiplikation und enthält 1, also eine K -Unteralgebra von E . Weiterhin enthält er x_1, \dots, x_n , also auch $K[X_1, \dots, X_n] = E$.

F ist ein F_0 -Untermodul von E . Da E endlich erzeugter F_0 -Modul ist und F_0 noethersch, ist auch F endlich erzeugt als F_0 -Modul.

F_0 ist endlich erzeugte K -Algebra, F ein endlich erzeugter F_0 -Modul. (Beweis der Unterbehauptung) Insgesamt wird F damit zu einer endlich erzeugten K -Algebra. (Beweis der Behauptung)

Sei $F = K[u_1, \dots, u_s]$. Wir schreiben

$$u_i = \frac{f_i}{g_i} \quad f_i, g_i \in K[x_1, \dots, x_r] \cong K[X_1, \dots, X_r]$$

Sei h ein Polynom, das teilerfremd zu allen g_i ist, z.B. $h = g_1 \dots g_s + 1 \in F$. Da F ein Körper ist, gilt $h^{-1} \in F$, also

$$h^{-1} = \sum_{\underline{i}} a_{\underline{i}} u^{\underline{i}} = \sum_{\underline{i}} a_{\underline{i}} \frac{f^{\underline{i}}}{g^{\underline{i}}} \quad \Rightarrow$$

$$1 = hh^{-1} = h \frac{\text{Zähler von } h^{-1}}{\text{Hauptnenner von } h^{-1}}$$

Der Hauptnenner von h^{-1} teilt wenigstens ein g_i , ist also teilerfremd zu h . Daher ist diese Gleichung ein Widerspruch zur Existenz von u_1, \dots, u_s . Es folgt $F = K$. Wir haben bereits $\dim_F E < \infty$ gezeigt und sind fertig. \square

Beweis von Theorem 3.5: Sei k algebraisch abgeschlossen, $I \subset k[X_1, \dots, X_n]$ maximal. Dann ist $E = k[X_1, \dots, X_n]/I$ ein Körper, der als k -Algebra endlich erzeugt ist. Nach Satz 3.8 ist $\dim_k E < \infty$.

Behauptung. $E = k$.

Sei $y \in E$. Wie im Beweis von Lemma 3.6 ist y Nullstelle eines nicht-trivialen Polynoms über k . Da k algebraisch abgeschlossen ist, zerfällt es in Linearfaktoren. y ist Nullstelle eines Linearfaktors, liegt also in k .

Sei a_i das Bild von X_i in $E = k$. Dann liegt $X_i - a_i$ in I . Es ist

$$\langle X_1 - a_1, \dots, X_n - a_n \rangle \subset I$$

Beide Ideale sind maximal, also gleich. \square

Beweis von Theorem 3.2: Sei k algebraisch abgeschlossen, $J \subset k[X_1, \dots, X_n]$ ein Ideal.

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

Die Inklusion \supset ist klar.

Für die Umkehrung sei $J = \langle f_1, \dots, f_m \rangle$, $g \in I(V(J))$. Wir benutzen einen Trick. Sei X_0 eine weitere Unbestimmte. Wir betrachten das Ideal

$$J' = \langle f_1, \dots, f_m, 1 - X_0 g \rangle \subset k[X_0, \dots, X_n]$$

Angenommen, dies ist nicht ganz $k[X_0, \dots, X_n]$.

Unterbehauptung. J' ist einem maximalen Ideal enthalten.

Wenn J' nicht maximal ist, so ist es echt in einem größeren enthalten. Ist dieses nicht maximal, so gibt es ein echt größeres, etc. Da der Ring noethersch ist, endet dieser Prozess.

Nach dem schwachen Nullstellensatz Theorem 3.5 hat dieses maximale Ideal eine gemeinsame Nullstelle $P' = (a_0, \dots, a_n)$, die dann auch gemeinsame Nullstelle aller Elemente von J' ist. Insbesondere ist $P = (a_1, \dots, a_n)$ gemeinsame Nullstelle von f_1, \dots, f_n , liegt also in $V(J)$. Wegen $g \in I(V(J))$ folgt $g(P) = 0$. Dies ist ein Widerspruch zu $1 - a_0 g(P) = 0$.

Damit ist $J' = k[X_0, \dots, X_n]$. Also gibt es $h_0, \dots, h_m \in k[X_0, \dots, X_n]$ mit

$$1 = h_1 f_1 + h_2 f_2 + \dots + h_m f_m + h_0(1 - X_0 g)$$

Wir ersetzen in dieser Relation X_0 durch $1/g$ (Achtung, auch die h_i hängen von X_0 ab!) und Multiplizieren mit einer hohen Potenz von g . Dies ergibt

$$g^N = h'_1 f_1 + \dots + h'_m f_m \Rightarrow g \in \sqrt{J}$$

□

Kapitel 4

Topologische Eigenschaften

Definition 4.1. Ein topologischer Raum Y heißt irreduzibel, wenn $Y \neq \emptyset$ und er nicht Vereinigung $Y = Y_1 \cup Y_2$ von echten abgeschlossenen Teilmengen ist.

Beispiel. (i) \mathbb{R} mit der gewöhnlichen Topologie ist nicht irreduzibel.

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

(iii) Einelementige algebraische Mengen sind irreduzibel.

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

Da die Zariski-Topologie sich durch Ideale beschreiben lässt, muss auch diese Eigenschaft eine Charakterisierung in Termen des Ideals haben. Offensichtliches Problem ist Funktionen wie $X_1, X_2 \in I(V(X_1 X_2))$.

Definition 4.2. Sei A ein Ring, $I \subset A$ ein Ideal. I heißt Primideal, wenn $I \neq A$ und für alle $a, b \in A$ gilt: aus $ab \in I$ folgt $a \in I$ oder $b \in I$.

Beispiel. Sei $I = (n) \subset \mathbb{Z}$ ein Primideal, $n \in \mathbb{N}$. Wegen $I \neq \mathbb{Z}$ ist $n \neq 1$. Für alle $a, b \in \mathbb{Z}$

$$ab \in (n) \Leftrightarrow n|ab \Rightarrow n|a \text{ oder } n|b$$

Dies ist die Definition von Primelement. n ist Primzahl.

Bemerkung. Primideale sind reduziert.

Satz 4.3. Eine affine Varietät Y ist irreduzibel genau dann, wenn $I(Y)$ ein Primideal ist.

Beweis: Sei Y irreduzibel, seien $f, g \in \mathcal{O}(\mathbb{A}^n)$, $fg \in I(Y)$. Dann gilt $Y \subset V(fg) = V(f) \cup V(g)$. Daher

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

Da Y irreduzibel, so gilt ohne Einschränkung $Y = V(f) \cap Y$, also $Y \subset V(f)$ und daher $f \in I(Y)$.

Sei umgekehrt $J = I(Y)$ ein Primideal. Angenommen $V(J) = Y_1 \cup Y_2$. Dann ist $J = I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$. Angenommen $J \neq I(Y_1), I(Y_2)$. Dann gibt es $f_i \in I(Y_i) \setminus J$. Es folgt $y_1 y_2 \in I(Y_1) \cap I(Y_2) = J$. Dies ist ein Primideal, also $y_1 \in J$ oder $y_2 \in J$. Dies ist ein Widerspruch zur Wahl der y_i . Es gilt also ohne Einschränkung $I(Y) = J = I(Y_1)$. Nach dem Hilbertschen Nullstellensatz folgt $Y = Y_1$. Damit ist $V = V(J)$ irreduzibel. \square

Bemerkung. Wir haben also Bijektionen

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

Lemma 4.4. *Sei A ein Ring, $I \subset A$ ein Primideal. Dann ist I ein Primideal genau dann, wenn A/I ein nullteilerfreier Ring ist.*

Ein Ring heißt *nullteilerfrei* oder auch *Integritätsbereich*, wenn $ab = 0 \Rightarrow a = 0$ oder $b = 0$.

Beweis: Sei I Primideal. Wegen $I \neq A$ ist A/I ein Ring. Sei $\bar{a} = a + I, \bar{b} = b + I \in A/I$ mit $\bar{a}\bar{b} = 0$. Dann gilt $ab + I = 0 + I \Leftrightarrow ab \in I$. Da I Primideal ist, folgt $a \in I$ oder $b \in I$, bzw. $\bar{a} = 0$ oder $\bar{b} = 0$. Die Umkehrung geht genauso. \square

Korollar 4.5. *Maximale Ideale sind stets Primideale.*

Beweis: Körper sind nullteilerfrei. \square

Beispiel. \mathbb{A}^n ist irreduzibel, denn $k[X_1, \dots, X_n]$ ist ein Integritätsbereich. Ist $f \in k[X_1, \dots, X_n]$ irreduzibel, so ist $V(f)$ ebenfalls irreduzibel (Übungsaufgabe):

Definition 4.6. *Ein topologischer Raum heißt noethersch, wenn jede absteigende Kette*

$$Y_1 \supset Y_2 \supset \dots$$

von abgeschlossenen Teilmengen stabil wird.

Beispiel. Affine Varietäten sind noethersch, denn Ketten von Varietäten entsprechen bijektiv Ketten von Idealen.

Lemma 4.7. *Sei Y noetherscher topologischer Raum und $X \subset Y$ offen. Dann ist X noetherscher topologischer Raum.*

Beweis: Wir betrachten eine Folge

$$X_1 \supset X_2 \supset \dots$$

von abgeschlossenen Teilmengen von X . Nach Definition ist die Folge der Abschlüsse

$$\bar{X}_1 \supset \bar{X}_2 \supset \dots$$

eine Folge von abgeschlossenen Teilmengen von Y . Da Y noethersch ist, wird sie stabil. Wegen $X \cap \bar{X}_i = X_i$ ist dann auch die Ausgangsfolge stabil. \square

Satz 4.8. *Sei X ein noetherscher topologischer Raum. Dann ist jede abgeschlossene Teilmenge $Y \subset X$ Vereinigung von endlich vielen irreduziblen Teilmengen.*

Beweis: Angenommen, Y ist nicht irreduzibel, also $Y = Y_0 \cup Y_1$ mit echten abgeschlossenen Teilmengen Y_0, Y_1 . Angenommen, Y_0 ist nicht irreduzibel, also $Y_0 = Y_{00} \cup Y_{01}$ mit echten abgeschlossenen Teilmengen Y_{00}, Y_{01} . Angenommen, Y_1 ist nicht irreduzibel, also $Y_1 = Y_{10} \cup Y_{11}$ mit echten abgeschlossenen Teilmengen Y_{10}, Y_{11} . Diesen Prozess setzen wir fort. Angenommen, er endet nicht. Dann gibt es eine Kette von abgeschlossenen Teilmengen, die nicht stabil wird. Dies ist ein Widerspruch zu Y noethersch. \square

Definition 4.9. *Sei Y eine affine Varietät. Eine irreduzible abgeschlossene Teilmenge $Y' \subset Y$ heißt irreduzible Komponente, wenn für jede irreduzible abgeschlossene Teilmenge $Y' \subset Y'' \subset Y$ gilt $Y' = Y''$.*

Korollar 4.10 (Zerlegung in irreduzible Komponenten). *Sei Y eine affine Varietät. Dann hat Y endlich viele irreduzible Komponenten Y_i für $i = 1, \dots, n$ und es gilt*

$$Y = Y_1 \cup \dots \cup Y_n$$

Ist $Y' \subset Y$ irreduzibel, so gibt es i mit $Y' \subset Y_i$.

Beweis: Sei $Y = Y_1 \cup \dots \cup Y_n$ die Zerlegung aus dem Satz. Wir setzen weiter voraus, dass wir keine der irreduziblen Mengen weglassen können.

Behauptung. *Sei $Y' \subset Y$ irreduzibel. Dann gibt es i mit $Y' \subset Y_i$.*

Wir betrachten $Y'_i = Y_i \cap Y'$. Es gilt

$$Y' = \bigcup_{i=1}^n Y'_i$$

Da Y' irreduzibel ist, folgt $Y' = Y'_i$ für ein i . D.h. es gilt $Y' \subset Y_i$.

Dies zeigt, dass Y_1, \dots, Y_n die irreduzible Komponenten sind. \square

Man kann denselben Satz auch für Primideale in noetherschen Ringen beweisen. Topologisch argumentiert es sich leichter.

Definition 4.11. *Sei X ein topologischer Raum. Die Dimension von X ist*

$\dim X = \sup\{n \in \mathbb{N}_0 \mid \text{es gibt eine Kette } X_0 \supsetneq X_1 \subsetneq \dots \subsetneq X_n, X_i \subset X \text{ irreduzibel}\}$

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

(ii) $X = \mathbb{A}^1$ hat Dimension 1, die Ketten haben die Form $\{P\} \subset \mathbb{A}^1$ für beliebiges P .

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

$$V = \{(x, y, z) \mid xy = 0, xz = 0\} = \{(0, y, z) \mid y, z \in k\} \cup \{(x, 0, 0) \mid x \in k\}$$

Diese Menge hat Dimension ≥ 2 . Die irreduzible Komponente $V(Y, Z)$ hat Dimension 1.

Lemma 4.12. *Die Dimension von X ist gleich der Krulldimension von $\mathcal{O}(X)$, d.h. gleich der maximalen Länge einer echten Kette von Primidealen.*

Beweis: Klar □

Bemerkung. Sogar in noetherschen Ringen muss die Krulldimension nicht immer endlich sein.

Einige Eigenschaften der Dimension sind klar.

Bemerkung. (i) Sei $Y \subset W$ abgeschlossene Teilmengen. Dann ist $\dim Y \subset \dim W$, denn jede Kette von irreduziblen Teilmengen von Y ist auch eine in W .

(ii) $\dim \mathbb{A}^n \geq n$, denn es gibt die Kette

$$\mathbb{A}^n \supset V(X_1) \supsetneq V(X_1, X_2) \supsetneq \cdots \supsetneq V(X_1, \dots, X_n)$$

Tatsächlich gilt $\dim \mathbb{A}^n = n$, aber das wir uns noch einige Mühe machen. Insbesondere sind alle affinen Varietäten endlich-dimensional.

Ist $k = \mathbb{C}$, so trägt jede Zariski-abgeschlossene Teilmenge $Y \subset \mathbb{C}^n$ auch die gewöhnliche Topologie. Tatsächlich stimmen die Dimensionsbegriffe überein.

Offene Überdeckungen

Definition 4.13. *Sei V eine affine Varietät. Dann heißen offene Menge der Form*

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

für $f \in \mathcal{O}(V)$ standardoffene Mengen in V .

Bemerkung. Wir haben bisher nur $V(f) \subset \mathbb{A}^n$ für $f \in k[X_1, \dots, X_n]$ definiert. In der Definition ist $f \in k[X_1, \dots, X_n]/I(V)$. Das ist aber ein harmloser Unterschied. Es hat ein Urbild $\tilde{f} \in k[X_1, \dots, X_n]$. Es ist dann

$$V(f) = V(\tilde{f}) \cap V$$

und dies ist unabhängig von der Wahl von \tilde{f} . Mit anderen Worten:

$$V(f) = \{P \in V \mid f(P) = 0\}$$

Lemma 4.14. *Sei V eine affine Varietät, $U \subset V$ offen. Dann ist U Vereinigung von standardoffenen Mengen.*

Insbesondere sind die standardoffenen Menge eine Basis für die Topologie.

Beweis: Sei $U = V \setminus Z$. Dann ist $Z = V(S)$ für eine Menge $S \subset k[V]$. Daher:

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

□

Tatsächlich genügt eine endliche Vereinigung, denn jede abgeschlossene Teilmenge wird durch endlich viele Gleichungen definiert. Das folgt bereits daraus, dass die topologischen Räume noethersch sind.

Lemma 4.15. *Sei Y noetherscher topologischer Raum, $\{U_i\}_{i \in I}$ eine offene Überdeckung, d.h. $U_i \subset Y$ offen*

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

Dann existiert eine endliche Teilüberdeckung $\{U_{i_1}, \dots, U_{i_n}\}$, d.h. endliche viele $i_1, \dots, i_n \in I$ mit

$$Y = \bigcup_{j=1}^n U_{i_j}$$

Bemerkung. Topologische Räume mit dieser Eigenschaft heißen *quasi-kompakt* (oder auch kompakt, je nach Quelle). Ein topologischer Raum ist kompakt, wenn er quasi-kompakt und hausdorff ist. Da Varietäten (fast) nie hausdorff sind, interessiert uns Quasi-Kompaktheit.

Beweis: Angenommen, Y hat keine endliche Teilüberdeckung. Dann konstruieren wir induktiv eine Folge U_{i_j} für $j \in \mathbb{N}$ so dass für $U'_{i_j} = \bigcup_{1 \leq j' \leq j} U_{i_{j'}}$ gilt

$$U'_{i_1} \subsetneq U'_{i_2} \subsetneq U'_{i_3} \subsetneq \dots$$

Sei nämlich i_1 beliebig. Da Y nicht von einem U_i überdeckt wird, gibt es $P \in Y \setminus U'_{i_1}$. Da die U_i ganz Y überdecken, gibt es einen Index i_2 mit $P \in U_{i_2}$. Da Y nicht von zwei offenen Mengen überdeckt wird, gibt es $Q \in Y \setminus U_{i_1} \cup U_{i_2}$ etc. Komplementär gibt es eine absteigende Folge

$$Z_1 \supsetneq Z_2 \supsetneq \dots$$

von abgeschlossenen Mengen in Y . Dies ist ein Widerspruch dazu, dass Y noethersch ist. □

Korollar 4.16. *Alle quasi-affinen Varietäten sind quasi-kompakt.*

Beweis: Affine Varietäten sind noethersch. Nach Lemma 4.7 sind dann auch quasi-affine noethersch. Nach Lemma 4.15 sind sie quasi-kompakt. □

Kapitel 5

Lokale Ringe und Lokalisierung

Der irreduzible Fall

Definition 5.1. Sei A ein nullteilerfreier Ring. Dann heißt

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

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

$$(a, s) \sim (a', s') \Leftrightarrow as' = a's \text{ für alle } a, a', s, s' \in A, s, s' \neq 0$$

Die Addition und Multiplikation ist die Addition und Multiplikation von Brüchen.

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

Definition 5.2. Sei V eine irreduzible affine Varietät. Dann heißt

$$k(V) = Q(k[V])$$

Funktionskörper von V . Die Elemente von $k(V)$ heißen rationale Funktionen auf V . Sei $P \in V$ und $f \in k(V)$. Dann heißt f regulär in P , falls $f = \frac{g}{h}$ mit $h(P) \neq 0$. In diesem Fall setzen wir $f(P) = \frac{g(P)}{h(P)}$. Andernfalls setzen wir $f(P) = \infty$. Der Ring

$$\mathcal{O}_P = \{f \in k(V) \mid f \text{ regulär in } P\}$$

heißt lokaler Ring von V in P .

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

Definition 5.3. Ein Ring heißt lokal, wenn er genau ein maximales Ideal hat.

Lemma 5.4. *Sei V affine Varietät, $P \in V$. Dann ist \mathcal{O}_P lokal mit maximalem Ideal $m_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}$.*

Beweis: Wir betrachten die Auswertungsfunktion

$$\mathcal{O}_P \rightarrow k, \quad f \mapsto f(P)$$

Sie ist surjektiv da $k \subset k[V] \subset \mathcal{O}_P$ und hat den Kern m_P . Damit ist m_P maximal.

Behauptung. *Jedes Element in $\mathcal{O}_P \setminus m_P$ ist invertierbar.*

Sei $f = g/h \in \mathcal{O}_P \setminus m_P$ mit $h(P) \neq 0$. Nach Voraussetzung ist $g(P) \neq 0$. Dann ist h/g das gesuchte Inverse.

Behauptung. *Jedes echte Ideal ist in m_P enthalten.*

Sei $I \subsetneq \mathcal{O}_P$ ein echtes Ideal. Dann enthält I keine invertierbaren Elemente, d.h.

$$I \cap (\mathcal{O}_P \setminus m_P) = \emptyset \Leftrightarrow I \subset m_P$$

In dieser Situation ist jedes maximale Ideal in m_P enthalten, also gleich m_P . \square

Wir halten das Kriterium fest, dass wir gerade im Beweis verifiziert haben:

Lemma 5.5. *Sei A ein Ring, $m \subset A$ ein Ideal. Dann ist A genau dann lokal mit maximalem Ideal m , wenn $A \setminus m$ die Menge der invertierbaren Elemente von A ist.*

Definition 5.6. *Sei $V \subset \mathbb{A}^n$ quasi-affin und irreduzibel. Dann setzen wir*

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

den Ring der algebraischen Funktionen auf V .

Bemerkung. Jetzt müssen wir eigentlich sofort überprüfen, dass für affine Varietäten $k[V] = \mathcal{O}(V)$ (im obigen Sinn.) Das ist wahr, aber verschieben den Beweis, bis wir uns von der Irreduzibilitätsvoraussetzung lösen können. Fürs erste unterscheiden wir $k[V]$ und $\mathcal{O}(V)$.

Lemma 5.7. *Sei V eine irreduzible affine Varietät, $f \in k(V)$. Dann ist*

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

offen in V .

Beweis: Sei $I = \{(g, h) \in k[V]^2 \mid f = g/h\}$. Dann gilt

$$U = \bigcup_{(g,h) \in I} U_h$$

wobei wie vorher $U_h = V \setminus V(h)$. \square

Korollar 5.8. Sei V quasi-affin, irreduzibel, $P \in V$. Dann gilt

$$\mathcal{O}_P = \bigcup_{P \in U} \mathcal{O}(U)$$

wobei U alle offenen Teilmengen von V durchläuft, die P enthalten.

Die Elemente von \mathcal{O}_P heißen daher auch *Keime von algebraischen Funktionen*, ein Begriff aus der Garbentheorie.

Lokalisierung von Moduln

Wir wollen nun das Rechnen mit Brüchen $\frac{m}{s}$ verstehen, wobei m aus einem Modul kommt, s aus dem Ring. Wir erinnern uns an die Additions- und Multiplikationsregeln:

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'}, \quad \frac{a}{s} \frac{m'}{s'} = \frac{am'}{ss'}$$

Dafür muss man Nenner multiplizieren können.

Definition 5.9. Sei A ein Ring. Eine Teilmenge $S \subset A$ heißt multiplikativ, wenn $1 \in S$, $0 \notin S$ und S abgeschlossen unter Multiplikation.

Beispiel. (i) Sei $f \in A$ ein Element. Dann ist $S_f = \{1, f, f^2, \dots\}$ multiplikativ, falls f nicht nilpotent ist.

(ii) Sei $\mathfrak{p} \subset A$ ein Primideal. Dann ist $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ multiplikativ.

(iii) Sei A Ring, S die Menge aller Elemente ungleich 0, die keine Nullteiler sind. Diese Menge ist multiplikativ. Ist A nullteilerfrei, so ist dies $S = A \setminus \{0\}$.

Definition 5.10. Sei A ein Ring, $S \subset A$ multiplikativ, M ein A -Modul. Auf $M \times S$ definieren eine Relation durch

$$(m, s) \sim (m', s') \Leftrightarrow \text{es gibt } t \in S \text{ mit } ts'm = tsm'$$

für alle $m, m' \in M$, $s, s' \in S$. Wir schreiben $\frac{m}{s}$ für die Äquivalenzklasse von (m, s) . Dann heißt

$$S^{-1}M = \left\{ \frac{m}{s} \mid m \in M, s \in S \right\}$$

Lokalisierung von M an S .

Für $f \in A$ nicht nilpotent schreiben wir $M_f = S_f^{-1}M$. Für ein Primideal $\mathfrak{p} \subset A$ schreiben wir $M_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}M$.

Die Relation ist so gemacht, dass zwei Brüche gleich sind, wenn sie nach Erweitern gleich sind. Wenn der Ring keine Nullteiler enthält, genügt Erweitern auf einen gemeinsamen Nenner, z.B. das Produkt der Nenner. Wenn A Nullteiler enthält, muss man die zusätzlich Erweiterung um ein t zulassen.

Lemma 5.11. *Seien A, S, M wie in der Definition.*

(i) \sim ist eine Äquivalenzrelation.

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

(iii) $S^{-1}A$ mit der Addition und Multiplikation von Brüchen ist ein Ring. Die Abbildung $a \mapsto \frac{a}{1}$ ist ein Ringhomomorphismus.

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

Beweis: Symmetrie und Reflexivität ist klar. Sei

$$(m, s) \sim (m', s') \sim (m'', s'')$$

Dann gibt es nach Voraussetzung $t, t' \in S$ mit

$$ts'm = tsm', t's''m' = t's'm'' \Rightarrow tt's's''m = t's''(tsm') = ts(t's'm'')$$

Also $(m, s) \sim (m'', s'')$ via $tt's' \in S$.

Die Verifikation aller anderen Aussagen ist elementares Rechnen mit Brüchen. Wir behandeln beispielhaft die Wohldefiniertheit der Addition. Sei

$$\frac{m}{s} = \frac{m'}{s'}, \frac{n}{t} = \frac{n'}{t'}$$

mit $m, m', n, n' \in M, s, s', t, t' \in S$. Nach Definition gibt es dann $u, v \in S$ mit

$$\begin{aligned} \frac{us'm}{ss'u} = \frac{usm'}{ss'u} &\Rightarrow \frac{vtt'us'm}{vtt'ss'u} = \frac{vtt'usm'}{vtt'ss'u} \\ \frac{vt'n}{tt'v} = \frac{vtn'}{tt'v} &\Rightarrow \frac{uss'vt'n}{uss'tt'v} = \frac{uss'vtn'}{uss'tt'v} \end{aligned}$$

Ebenso

$$\frac{tm + sn}{st} = \frac{s't'uv(tm + sn)}{uvt't'ss'}, \frac{t'm' + s'n'}{s't'} = \frac{stuv(t'm' + s'n')}{uvt't'ss'}$$

Einsetzen ergibt die Behauptung. \square

Beispiel. Sei $A = k[V]$ für eine irreduzible affine Varietät, $S = A \setminus \{0\}$. Dann ist $k(V) = S^{-1}A$. Sei $P \in V$ und $\mathfrak{m} = I(P)$ das zugehörige maximale Ideal. Dann ist $\mathcal{O}_P = A_{\mathfrak{m}}$.

Bemerkung. Gibt es einen Nullteiler $s \in S$, so ist $A \rightarrow S^{-1}A$ nicht injektiv, denn $\frac{s}{1} = \frac{0}{1}$. (Übungsaufgabe)

Ist $f : M \rightarrow N$ ein Morphismus von A -Moduln, $S \subset A$ multiplikativ, so erhält man durch $f(\frac{m}{s}) = \frac{f(m)}{s}$ für alle $m \in M, s \in S$ einen induzierten Morphismus von $S^{-1}A$ -Moduln.

Lemma 5.12. Sei A ein Ring, $S \subset A$ eine multiplikative Menge,

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

eine exakte Sequenz von A -Moduln. Dann ist

$$S^{-1}M_1 \rightarrow S^{-1}M_2 \rightarrow S^{-1}M_3$$

eine exakte Sequenz von $S^{-1}A$ -Moduln.

Funktoren mit dieser Eigenschaft nennt man *exakt*.

Beweis: Nach Voraussetzung gilt $g \circ f = 0$. Sei nun $\frac{m_1}{s} \in S^{-1}M_1$ mit $m_1 \in M_1, s \in S$. Dann ist

$$g \circ f\left(\frac{m_1}{s}\right) = \frac{g \circ f(m_1)}{s} = \frac{0}{s}$$

Dies bedeutet $\text{Im } g \subset \text{Ker } f$.

Sei nun $\frac{m_2}{s} \in S^{-1}M_2$, das im Kern von g liegt, also

$$\frac{g(m_2)}{s} = \frac{0}{1} \Leftrightarrow \frac{tg(m_2)}{st} = st \cdot 0st \cdot 1$$

für ein $t \in S$. Wegen der A -Linearität von g folgt

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

Wegen der Exaktheit der Sequenz gibt es $m_1 \in M_1$ mit $f(m_1) = tm_2$. Dann ist

$$f\left(\frac{m_1}{ts}\right) = \frac{f(m_1)}{ts} = \frac{tm_2}{st} = \frac{m_2}{s}$$

□

Korollar 5.13. Sei A ein Ring, $S \subset A$ multiplikativ, $I \subset A$ ein Ideal. Dann ist $S^{-1}I \subset S^{-1}A$ ein Ideal. Es ist $S^{-1}I = S^{-1}A$ genau dann, wenn $S \cap I \neq \emptyset$.

Beweis: Da S^{-1} exakt ist, ist $S^{-1}I \subset S^{-1}A$ ein Untermodul, also ein Ideal. Wir haben Gleichheit genau dann, wenn $\frac{1}{s} \in S^{-1}I$, d.h. von der Form $\frac{s}{s}$ mit $s \in S$ (Nenner) und $s \in I$ (Zähler). □

Lemma 5.14. Sei A ein Ring, $\mathfrak{p} \subset A$ ein Primideal. Dann ist $A_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{p}_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}\mathfrak{p}$.

Beweis: $S_{\mathfrak{p}}^{-1}\mathfrak{p}$ ist ein Ideal. Wir zeigen, dass alle Elemente von $S_{\mathfrak{p}}^{-1}A \setminus S_{\mathfrak{p}}^{-1}\mathfrak{p}$ invertierbar sind. (Dann sind alle echten Ideale in $S_{\mathfrak{p}}^{-1}\mathfrak{p}$ enthalten, der Ring ist lokal.) Sei also $\frac{a}{s}$ im Komplement. D.h. $a \in A \setminus \mathfrak{p} = S_{\mathfrak{p}}$. Dann ist $\frac{s}{a}$ das gesuchte Inverse. □

Eine Eigenschaft von Ringen oder Moduln heißt *lokal*, wenn man sie nach Lokalisierung an allen Primidealen überprüfen kann. Beispiele sind Regularität, ganz abgeschlossen, flach. Das wichtigste Beispiel ist das folgende:

Satz 5.15. *Sei A ein Ring, M ein A -Modul. Dann sind äquivalent:*

- (i) $M = 0$
- (ii) $M_{\mathfrak{p}} = 0$ für alle Primideale $\mathfrak{p} \subset A$.
- (iii) $M_{\mathfrak{m}} = 0$ für alle maximalen Ideale $\mathfrak{m} \subset A$.

Beweis: Die ersten beiden Implikationen sind trivial. Wir müssen also (iii) nach (i) überprüfen.

Angenommen $M \neq 0$, aber $M_{\mathfrak{m}} = 0$ für alle maximalen Ideale von A . Sei $0 \neq m \in M$. Sei $I = \{a \in A \mid am = 0\}$. Dies ist ein Ideal von A , also in einem maximalen Ideal \mathfrak{m} enthalten. (Für noethersche Ringe ist dies einfach, im allgemeinen braucht man das Zornsche Lemma. Wir können uns für die algebraische Geometrie mit dem noetherschen Fall zufriedengeben.) Nach Voraussetzung ist $M_{\mathfrak{m}} = 0$, also auch $\frac{m}{1} = \frac{0}{1}$. Dies bedeutet, dass es $s \in S_{\mathfrak{m}}$ gibt mit $sm = 0$. Dann ist $s \in I \subset \mathfrak{m}$. Dies ist ein Widerspruch zu $s \in S_{\mathfrak{m}} = A \setminus \mathfrak{m}$. \square

Lokale Ringe von Varietäten

Wir kehren zurück zu den Koordinatenringen von affinen Varietäten, jetzt ohne Irreduzibilität vorauszusetzen.

Definition 5.16. *Sei V eine affine Varietät, $f \in k[V]$ (mit $f \neq 0$) und $U_f \subset V$ eine standardoffene Menge. Jedes Element $g = a/f^n \in k[V]_f$ induziert eine Funktion*

$$g : U_f \rightarrow k, \quad P \mapsto \frac{a(P)}{f(P)^n}$$

Funktionen von dieser Form heißen global algebraisch.

Sei $U \subset V$ offen. Eine Funktion $g : U \rightarrow k$ heißt lokal algebraisch, wenn es eine offene Überdeckung $U = \bigcup_{i=1}^n U_{f_i}$ gibt, so dass g global algebraisch auf jedem U_{f_i} ist. Der Ring der lokal algebraischen Funktionen wird mit $\mathcal{O}(U)$ bezeichnet.

Wir sind hier ein wenig schlampig und unterscheiden nicht zwischen einem Bruch a/f^n und der von ihm induzierten Funktion. Die beiden Begriffe lokal/global algebraisch sind in der Literatur nicht üblich, denn wir werden zeigen:

Satz 5.17. *Sei V eine affine Varietät, $U_f \subset V$ eine standardoffene Menge. Dann ist die natürliche Abbildung*

$$k[V]_f \rightarrow \mathcal{O}(U_f)$$

ein Ringisomorphismus. Insbesondere ist

$$k[V] \cong \mathcal{O}(V)$$

Beweis: Wir erledigen zunächst die Injektivität. Sei $a/f^n \in k[V]_f$ mit $f = 0$ aufgefasst in $\mathcal{O}(U_f)$, d.h. $a(Q)/f(Q)^n = 0$ für alle $Q \in U_f$. Da $f(Q) \neq 0$ in ganz U_f , bedeutet dies $a(Q) = 0$ für alle $Q \in U_f$. Mit anderen Worten, $V(a) \supset U_f$

beziehungsweise $V(a) \cup V(f) = V$. Nach dem Hilbertschen Nullstellensatz ist dann $0 = \sqrt{(af)} \Rightarrow af = 0$. Hieraus folgt in $k[V]_f$ die Gleichheit $a/1 = af/f = 0$. Das ist Injektivität.

Sei $g : U_f \rightarrow k$ lokal algebraisch, $U_f = \bigcup_{i=1}^n U_{f_i}$ eine standardoffene Überdeckung, so dass $g_i = g|_{U_{g_i}}$ global algebraisch ist, also von der Form a_i/f_i (ersetze eventuell f_i durch eine Potenz).

Man beachte, dass $U_{f_i} \cap U_{f_j} = U_{f_i f_j}$. Für $i \neq j$ gilt dann

$$\frac{a_i f_j}{f_i f_j} = g|_{U_{f_i f_j}} = \frac{a_j f_i}{f_i f_j} \in \mathcal{O}(U_{f_i f_j}) = k[V]_{f_i f_j}$$

Dies bedeutet, dass es $n \in \mathbb{N}$ gibt mit

$$f_i^n f_j^n (a_i f_j - a_j f_i) = 0 \Leftrightarrow f_j^{n+1} (a_i f_i^n) - f_i^{n+1} (a_j f_j^n)$$

zunächst für ein Paar i, j . Wir wählen n so groß, dass die Gleichung für alle i, j gleichzeitig gilt.

Nun ersetzen wir f_i durch f_i^{n+1} und a_i durch $a_i f_i^n$. Dann gilt weiterhin $g_i = a_i/f_i$ in U_{f_i} und außerdem

$$a_i f_j = a_j f_i$$

für alle i, j .

Es ist $\bigcap_{i=1}^n V(f_i) \subset V(f)$, also nach dem Hilbertschen Nullstellensatz $f \in \sqrt{\langle f_1, \dots, f_n \rangle}$. Es gibt also $m \in \mathbb{N}$ 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. $a/f^m \in k[V]_f$ repräsentiert g .

Es folgt nämlich

$$f_j a = \sum_i b_i a_i f_j = \sum_i b_i f_i a_j = a_j f^m$$

Also $a/f^m = a_j/f_j = g_j$ in U_{f_j} □

Wir betrachten nun auch die lokale Situation. Sei V eine affine Varietät, $P \in V$. Wir betrachten Paare (U, f) , wobei U eine offene Umgebung von P ist und $f \in \mathcal{O}(U)$. Auf diesen Paaren führen wir eine Äquivalenzrelation ein:

$$(U, f) \sim (U', f') \Leftrightarrow \text{es gibt ein offenes } W \subset U \cap U', f|_W = f'|_W$$

Dafür benutzt man:

Lemma 5.18. *Sei $W \subset U$ offen, $f \in \mathcal{O}(U)$. Dann ist die Einschränkung $f|_W \in \mathcal{O}(W)$.*

Wir sagen, die $\mathcal{O}(\cdot)$ bilden eine *Prägarbe*.

Beweis: Ohne Einschränkung ist $U = U_g$ ein standardaffines, $f = a/g^n$ global algebraisch. Die offene Teilmenge W hat eine endliche Überdeckung $W = \bigcup_{i=1}^n U_{g_i}$ durch standardaffine. Es genügt zu zeigen, dass $f|_{U_{g_i}}$ global algebraisch ist. Wegen $U_{g_i} \subset U_g$ können wir ohne Einschränkung annehmen, dass $g|_{g_i}$. Dann ist $f \in k[V]_{g_i}$. Dies zeigt die Behauptung. \square

Definition 5.19. Sei V affine Varietät, $P \in V$ ein Punkt. Wir betrachten Paare (U, f) mit $P \in U \subset V$ offen, $f \in \mathcal{O}(U)$. Wir erklären eine Äquivalenzrelation

$$(U, f) \sim (U', f') \Leftrightarrow \text{es gibt } P \in W \subset U \cap U', f|_W = f'|_W$$

Die Äquivalenzklassen von Paaren (U, f) heißen Keime von algebraischen Funktionen in P . Der Ring \mathcal{O}_P der Funktionenkeime heißt lokaler Ring von V in P .

Lemma 5.20. Sei V eine affine Varietät, $P \in V$ ein Punkt und $m(P) = \{f \in k[V], f(P) = 0\}$ das zugehörige maximale Ideal. Dann ist die natürliche Abbildung

$$k[V]_{m(P)} \rightarrow \mathcal{O}_P \quad \frac{a}{s} \mapsto (U_s, a/s)$$

ein Isomorphismus.

Beweis: Wir beginnen mit der Wohldefiniertheit der Abbildung. Wegen $s \notin m(P)$ ist $s(P) \neq 0$, also $P \in U_s$. Sei $a/s = a'/s'$. Dann gibt es $t \notin m(P)$ mit $ts'a = tsa'$. Es ist $U_{ts's} \subset U_s \cap U_{s'}$ und auf dieser Menge stimmen die induzierten Funktionen überein. Sie definieren also denselben Funktionenkeim.

Nun behandeln wir Surjektivität. Sei (U, f) ein Funktionenkeim. Ohne Einschränkung ist U standardaffin und f global algebraisch, also von der Form $(U_g, a/g^n)$. Wegen $P \in U_g$ ist $g(P) \neq 0$, gilt $g \in k[V] \setminus m(P)$. Damit hat die Funktion a/g^n ein Urbild in $k[V]_{m(P)}$.

Sei weiter $a/s \in k[V]_{m(P)}$ mit $(U_s, a/s) \sim (U_s, 0)$, d.h. es gibt eine offene Umgebung $W \subset U_s$ von P mit $a/s|_W = 0$. Ohne Einschränkung ist $W = U_{st}$ ein standardaffines. Nach Voraussetzung ist also

$$\frac{a(Q)t(Q)}{s(Q)t(Q)} = 0$$

für alle $Q \in U_{st}$. Wegen der Injektivität in Satz 5.17 ist dann $at/st = 0$ in $k[V]_{st}$, also erst recht in $k[V]_{m(P)}$. \square

Bemerkung. Ist V irreduzibel, so erhalten wir also Definition 5.2 für \mathcal{O}_P zurück. Dann stimmen auch Definition 5.6 und die allgemeinere Definition 5.16 für algebraische Funktionen überein.

Beweis: Sei $U \subset V$ offen, $\mathcal{O}(U)$ wie in 5.16. Zu zeigen ist

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

Die Injektivität ist klar, denn der Wert von $f \in \mathcal{O}(U)$ im Punkt P ist eindeutig durch den Wert des Keimes $(U, f) \in \mathcal{O}_P$ in P bestimmt.

Für die Umkehrung beginnen wir mit $x \in k(V)$, welches in allen $\mathcal{O}_P = k[V]_{m(P)}$ liegt. Damit gibt es für jedes P eine offene Umgebung U_P auf der x durch einen Funktionenkeim (U_P, f_P) repräsentiert wird. Damit ist x lokal algebraisch. \square

Kapitel 6

Die Kategorie der quasi-projektiven Varietäten

Definition 6.1. Sei K ein Körper. Der projektive Raum $\mathbb{P}^n(K)$ der Dimension n über K ist die Menge der eindimensionalen Untervektorräume des K^{n+1} , d.h. die Menge der Äquivalenzklassen

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\}) / \sim$$

wobei $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$ falls es $\lambda \in A^*$ gibt mit $x_i = \lambda y_i$ für $0 \leq i \leq n$. Wir schreiben $[x_0 : \dots : x_n]$ für die Äquivalenzklasse von (x_0, \dots, x_n) . Wir nennen x_0, \dots, x_n homogene Koordinaten auf $\mathbb{P}^n(K)$. Für $i = 0, \dots, n$ heißt die Teilmenge

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

i -te standardaffine Karte.

Lemma 6.2. (i) Auf U_i sind die Funktionen $y_j = x_j/x_i$ wohldefiniert und induzieren eine Bijektion

$$\phi_i : U_i \rightarrow K^n \quad [x_0 : \dots : x_n] \mapsto (y_0, \dots, y_{i-1}, y_{i+1}, \dots, y_n)$$

(ii) Es gilt $\mathbb{P}^n(K) \setminus U_i \cong \mathbb{P}^{n-1}(K)$ (Weglassen der i -ten Koordinate).

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

Beweis: Auf U_i darf durch x_i geteilt werden. Wegen $\lambda x_j / \lambda x_i = x_j / x_i$ ist y_j unabhängig von der Wahl des Repräsentanten. Die Abbildung

$$\psi_i : K^n \rightarrow \mathbb{P}^n(K) \quad (a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \mapsto [a_0 : \dots : a_{i-1} : 1 : a_{i+1} : \dots, a_n]$$

hat Werte in U_i . Offensichtlich sind ϕ_i und ψ_i invers zueinander.

Das Komplement von U_i besteht aus Punkten mit $x_i = 0$. Nach Voraussetzung hat jeder Punkt des $\mathbb{P}^n(K)$ eine Koordinate ungleich 0, liegt also in einem U_i . \square

Wir fassen K^n via ϕ_0 als offene Teilmenge des $\mathbb{P}^n(K)$ auf.

Beispiel. Für $n = 0$ besteht $\mathbb{P}^n(K)$ aus genau einem Punkt. Für $n = 1$ ist $\mathbb{P}^n(K) = K \cup \{\infty\}$.

Wir wollen nun algebraische Teilmengen als Nullstellenmengen von Polynomen definieren. Der Funktionswert eines Polynoms ist jedoch nicht wohldefiniert, da die homogenen Koordinaten nicht wohldefiniert sind.

Definition 6.3. Ein Polynom $P \in K[X_0, \dots, X_n]$ heißt homogen vom Grad d , wenn es von der Form

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

ist.

Lemma 6.4. Sei f ein homogenes Polynom vom Grad d , $x = (x_0, \dots, x_n) \in K^{n+1}$, $\lambda \in K^*$. Dann gilt

$$f(\lambda x) = \lambda^d f(x)$$

Für homogene Polynome ist also der Funktionswert auf dem projektiven Raum nicht wohldefiniert, wohl aber die Eigenschaft zu verschwinden.

Ist f ein beliebiges Polynom, so schreiben wir es als $f = \sum_{d=0}^m f_d$, wobei die f_d homogen vom Grad d sind.

Definition 6.5. Sei k ein algebraisch abgeschlossener Körper, $S \subset k[X_0, \dots, X_n]$ eine Menge von Polynomen. Dann heißt

$$V(S) = \{P \in \mathbb{P}^n(k) \mid f(P) = 0 \text{ für alle homogenen } f \in S\}$$

durch S definierte projektive algebraische Menge.

Sei $V \subset \mathbb{P}^n(k)$ eine algebraische Menge. Dann heißt

$$I(V) = \{f = \sum_d f_d \in k[X_0, \dots, X_n] \mid f_d(P) = 0 \text{ für alle } P \in V, d \geq 0\}$$

Verschwindungsideal von V und

$$k[V] = k[X_0, \dots, X_n]/I(V)$$

homogener Koordinatenring von V .

Beispiel. Sei $n = 2$. Für die projektive Ebene benutzt man meist die Koordinaten $X = X_1, Y = X_2, Z = X_0$. Sei $f = X^2 + Y^2 + Z^2$. Um $V = V(f)$ zu verstehen, schneiden wir mit den standardaffinen Teilmengen. Es gilt

$$V \cap U_0 = \{[x : y : z] \mid z \neq 0, x^2 + y^2 + z^2 = 0\} \cong \{(x, y) \mid x^2 + y^2 = -1\}$$

und analog in den beiden anderen Karten. In $V(Z) = \mathbb{P}^n(k) \setminus U_0$ liegen die Punkte

$$\{[x : y : 0] \mid x^2 + y^2 = 0\} = \{[1 : \sqrt{-1} : 0], -[1 : \sqrt{-1} : 0]\}$$

Es gilt dann $I(V) = \langle X^2 + Y^2 + Z^2 \rangle$ (Übungsaufgabe). Nicht alle Elemente von $I(V)$ sind homogen, sondern nur die der Form gf mit homogenem g . Nach Definition ist dann $V(I(V)) = V$.

Lemma 6.6. *Sei V eine projektive algebraische Menge. Wir nennen eine Teilmenge $Z \subset V$ abgeschlossen, wenn sie algebraisch ist. Dies definiert eine Topologie auf V .*

Beweis: Wie im affinen Fall. Es geht nur ein, dass das Produkt von zwei homogenen Polynomen homogen ist. \square

Definition 6.7. *Sei \mathbb{P}_k^n der projektive Raum $\mathbb{P}^n(k)$ zusammen mit seiner Topologie. Eine projektive Varietät ist eine projektive algebraische Menge zusammen mit ihrer Topologie. Eine quasi-projektive Varietät ist eine offene Teilmenge einer projektiven Varietät mit der induzierten Topologie.*

Wegen $U_i = \mathbb{P}_k^n \setminus V(X_i)$ sind die standard-affinen Teilmengen offen.

Lemma 6.8. *Die Kartenabbildung $\phi_i : U_i \rightarrow \mathbb{A}^n$ ist ein Homöomorphismus, d.h. bijektiv, stetig und offen.*

Beweis: Ohne Einschränkung betrachten wir $i = 0$. Die Bijektivität haben wir schon überprüft. Sei $F \in k[X_0, \dots, X_n]$ ein Polynom, $V = V(F) \subset \mathbb{P}_k^n$. Dann gilt

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

Das Bild dieser Abbildung unter ϕ_0 ist also $V(f)$ mit $f = F(1, X_1, \dots, X_n)$. Also sind Bilder abgeschlossener Teilmengen von U_0 abgeschlossen. Sei umgekehrt $f \in k[X_1, \dots, X_n]$ ein Polynom vom Grad d . Sei F die Homogenisierung von f , d.h.

$$F = X_0^d f(X_1/X_0, \dots, X_n/X_0)$$

Dann ist

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

das gesuchte Urbild von $V(f)$, also abgeschlossen in U_0 . \square

Wir können also den projektiven Raum (und alle projektiven Varietäten) mit affinen Karten überdecken. Der Schnitt $U_i \cap U_j = \{[x_0 : \dots : x_n] \mid x_i, x_j \neq 0\}$ wird unter der Kartenabbildung ϕ_i abgebildet auf die Menge der Punkte mit $y_j \neq 0$, also die standardoffene Menge U_{y_j} . Die Kartenwechselabbildung

$$\phi_j \phi_i^{-1} : U_{y_j} \rightarrow U_{y_i}$$

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

$$\begin{aligned} (y_1, \dots, y_n) &\mapsto [1 : y_1 : \dots : y_n] = [1/y_1 : 1 : y_2/y_1 : \dots : y_n/y_1] \\ &\mapsto (1/y_1, y_2/y_1, \dots, y_n/y_1) \end{aligned}$$

Jeder Eintrag ist eine algebraische Funktion auf U_{y_1} .

Bemerkung. Quasi-affine Varietäten sind quasi-projektiv.

Definition 6.9. Seien V, W quasi-projektive Varietäten. Ein Morphismus von Varietäten ist eine stetige Abbildung

$$f : V \rightarrow W$$

die lokal algebraisch ist, d.h. für jeden Punkt $P \in V$ gibt es standardoffene Umgebungen in standardaffinen Kartenumgebungen U und U' von P und $f(P)$, so dass $f|_U : U \rightarrow W$ Werte in U' annimmt und die induzierte Abbildung

$$f|_U : U \rightarrow U' \subset \mathbb{A}^n$$

in jeder Koordinate durch eine algebraische Funktion gegeben ist.

Ein Morphismus von Varietäten heißt Isomorphismus, wenn die Abbildung bijektiv ist und die Umkehrabbildung ein Morphismus von Varietäten ist.

Nicht jeder bijektive Morphismus ist ein Isomorphismus!

Beispiel. Sei $V = V(y^2 = x^3) \subset \mathbb{A}^2$. Dann ist

$$\mathbb{A}^1 \rightarrow V \quad t \mapsto (t^3, t^2)$$

bijektiv, aber kein Isomorphismus, denn die Umkehrabbildung benötigt Wurzelfunktionen.

Wir wollen nun besser verstehen, welche Beispiele von Morphismen es gibt.

Lemma 6.10. Sei V affin, $f \in \mathcal{O}(V)$. Dann ist f stetig als Morphismus $f : V \rightarrow \mathbb{A}^1$. Es ist

$$\mathcal{O}(V) = \text{Mor}(V, \mathbb{A}^1)$$

Beweis: Es genügt zu zeigen, dass Urbilder abgeschlossener Mengen abgeschlossen sind. Dann genügt es wiederum einelementige Mengen $\{a\} \subset \mathbb{A}^1$ zu betrachten. Das Urbild von a besteht aus den Punkten mit $f(P) = a$, also den Nullstellen von $f - a$. Dies ist abgeschlossen.

Sei nun f ein Morphismus. Wir gehen die Definition durch. Jeder Punkt $P \in X$ hat eine standardoffene Umgebung U_P , so dass $f|_{U_P} \in \mathcal{O}(U_P)$. D.h. f ist lokal algebraisch. Nach Definition liegt $f \in \mathcal{O}(X)$.

Umgekehrt haben wir die Stetigkeit von $f \in \mathcal{O}_P$ gezeigt. Dies ist dann nach Definition ein Morphismus. \square

Bemerkung. Die Aussage gilt auch im quasi-affinen Fall, Übungsaufgabe.

Satz 6.11. *Die Verknüpfung von Morphismen von Varietäten ist ein Morphismus.*

Beweis: Seien $X \subset \mathbb{P}^r$, $Y \subset \mathbb{P}^s$, $Z \subset \mathbb{P}^t$ quasi-projektiv. Seien $f : X \rightarrow Y$ und $g : Y \rightarrow Z$ Morphismen. Dann ist $g \circ f$ stetig. Nun ist die lokale Bedingung an $g \circ f$ zu überprüfen.

Sei $P \in X$. Nach Definition gibt es eine standardaffine Karte von X und darin eine standardoffene Menge $U_P \subset \mathbb{A}^r$, die P enthält, sowie eine standardaffine Karte $U_{f(P)} \subset \mathbb{A}^s$ von Y , die $f(P)$ enthält, so dass die Koordinatenfunktionen

$$f_1, \dots, f_s : U_P \rightarrow \mathbb{A}^1$$

durch Elemente von $\mathcal{O}(U_P)$ gegeben sind. Weiter gibt es nach Voraussetzung ebensolche Umgebungen $V_{f(P)} \subset \mathbb{A}^s$ und $V_{g(f(P))} \subset \mathbb{A}^t$, so dass die Koordinatenfunktionen

$$g_1, \dots, g_t : V_{f(P)} \rightarrow \mathbb{A}^1$$

durch Elemente von $\mathcal{O}(V_{f(P)})$ gegeben sind.

Behauptung. *Ohne Einschränkung ist $U_{f(P)} \subset V_{f(P)}$*

Wir ersetzen $U_{f(P)}$ durch $U_{f(P)} \cap V_{f(P)}$. Dies ist als Schnitt einer standardaffinen mit einer standardoffenen Menge wieder standardoffen. Das Urbild unter f ist enthalten in U_P und enthält eine standardoffene Umgebung von P . Wir ersetzen U_P durch diese.

Behauptung. $g_i(f_1, \dots, f_s) \in \mathcal{O}(U_P)$

Zur Vereinfachung der Notation setzen wir $X = U_P$, $f_1, \dots, f_s \in \mathcal{O}(X)$, $Y = V_{f(P)}$, $g = g_i \in \mathcal{O}(Y)$. Beide sind standardoffen, also $X = \overline{X} \setminus V(u)$ für ein $u \in k[\overline{X}]$, $Y = \overline{Y} \setminus V(w)$ für ein $w \in k[\overline{Y}]$. Daher haben die f_j (ohne Einschränkung) die Form a_j/u , sowie g (ohne Einschränkung) die Form b/w . Wir setzen a_j/u für die Koordinaten von w ein. Mit anderen Worten, wir repräsentieren a_j, u durch Elemente von $k[X_1, \dots, X_s]$ und b, w durch Elemente von $k[Y_1, \dots, Y_r]$ und setzen dann ein. Das Einsetzen von Polynomen in ein Polynom ergibt wieder ein Polynom. Also sind $b(a_1/u, \dots, a_s/u), w(a_1/u, \dots, a_s/u) \in k[\overline{X}]_u = \mathcal{O}(X)$. Nach Voraussetzung ist $f(X) \subset Y$, also hat $w(a_1/u, \dots, a_s/u)$ auf X nur Werte ungleich 0. Also ist dies ein invertierbares Element von $\mathcal{O}(X)$. Damit ist der Quotient ebenfalls in $\mathcal{O}(X)$. \square

Satz 6.12. *Seien $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ affine Varietäten. Eine Abbildung $f : V \rightarrow W$ ist genau dann ein Morphismus, wenn alle Koordinatenfunktionen $f_1, \dots, f_m : V \rightarrow \mathbb{A}^1$ von f Elemente von $k[V]$ sind.*

Beweis: Die Projektionsabbildung $p_i : \mathbb{A}^m \rightarrow \mathbb{A}^1$ auf die i -te Koordinate wird durch das Polynom $X_i \in k[X_1, \dots, X_m]$ definiert, ist also ein Morphismus von Varietäten. Dann ist auch $f_i = p_i \circ f$ ein Morphismus $V \rightarrow \mathbb{A}^1$, also ein Element von $\mathcal{O}(V)$.

Sei umgekehrt $f = (f_1, \dots, f_m)$ mit $f_i \in k[V]$ und $f(P) \in W$ für alle $P \in V$.

Behauptung. f ist stetig.

Sei $V(g) \subset W$ abgeschlossen, $g \in k[W]$. Dann ist

$$f^{-1}V(g) = \{P \in V \mid g(f_1(P), \dots, gf_m(P)) = 0\}$$

Da das Einsetzen von Polynomen in ein Polynom wieder ein Polynom ergibt, ist $g(f_1, \dots, f_m) \in k[V]$, also ist $f^{-1}(V(g))$ die Nullstellenmenge eines Polynoms, also abgeschlossen.

Die lokale Bedingung an einen Morphismus ist nun sogar global erfüllt. \square

Bemerkung. Man kann das leicht umformulieren zu der Aussage, dass ein Morphismus $f : V \rightarrow W$ dasselbe ist wie ein k -Algebrenhomomorphismus $f^* : \mathcal{O}(W) \rightarrow \mathcal{O}(V)$. Dabei erhält man f^* als Komposition mit f . Ist andererseits $\phi : \mathcal{O}(W) \rightarrow \mathcal{O}(V)$ gegeben, so erhalten wir die Koordinatenfunktionen f_i als Bilder der Koordinatenfunktionen $x_i : W \rightarrow \mathbb{A}^1$, die zu einer Einbettung $W \subset \mathbb{A}^n$ gehören.

Korollar 6.13. $U = \mathbb{A}^2 \setminus \{0\}$ ist nicht affin.

Beweis: Wir benutzen die Koordinaten X, Y auf \mathbb{A}^2 .

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

Es ist

$$U = U_X \cup U_Y$$

Wir wissen, dass $\mathcal{O}(U_X) = k[X, Y]_X$, $\mathcal{O}(U_Y)_Y$. Eine algebraische Funktion auf U induziert also ein Paar $a/X^i, b/Y^j$, die als Funktionen auf $U_X \cap U_Y$, also als Elemente von $k[X, Y]_{XY}$ übereinstimmen. Es ist also

$$Y^j a = X^i b \in k[X, Y]$$

Wegen der Eindeutigkeit der Faktorisierung in irreduzible Polynome ist dann $X^i \mid a$ und $Y^j \mid b$, also ist die Funktion ganz.

Die Inklusion $U \rightarrow \mathbb{A}^2$ induziert also einen Isomorphismus auf den Ringen von algebraischen Funktionen. Wäre U affin, so müsste $U \cong \mathbb{A}^2$ sein. \square

Satz 6.14. Sei $V \subset \mathbb{A}^n$ affin, $g \in k[V]$. Dann ist die Abbildung

$$\phi : V(gX_{n+1} - 1) \rightarrow U_g \quad (x_1, \dots, x_{n+1}) \mapsto (x_1, \dots, x_n)$$

ein Isomorphismus von Varietäten.

Beweis: Wegen $g(x_1, \dots, x_n)x_{n+1} = 1$ auf $V(gX_{n+1} - 1)$ hat die Abbildung Werte in U_g . Für jeden Punkt in U_g gibt es genau einen Urbildpunkt. Wir überprüfen nun die Stetigkeit. Sei also $U \subset U_g$ standardoffen, also von der Form U_{gh} für $h \in k[V]$.

Behauptung. $\Phi^{-1}U_{gh} = V(gX_{n+1} - 1)_h := \{(x_1, \dots, x_{n+1}) \in V(gX_{n+1} - 1) \mid h(x_1, \dots, x_{n+1}) \neq 0\}$

Für die Punkte $(x_1, \dots, x_{n+1}) \in V(gX_{n+1} - 1)$ mit $h(x_1, \dots, x_n) \neq 0$ liegt das Bild unter Φ offensichtlich in U_{gh} und umgekehrt.

Sei andererseits $U \subset V(gX_{n+1} - 1)$ standardoffen, also von der Form U_f mit $f \in k[V(gX_{n+1} - 1)]$. In diesem Koordinatenring gilt $X_{n+1} = g^{-1}$, also ist er gleich $k[V]_g$. Es $U = \Phi^{-1}U_{fg}$. \square

Bemerkung. Unsere standardoffenen Mengen sind also als Varietäten *affin*, nämlich isomorph zu einer affinen Varietät. Die affinen Umgebungen bilden eine Umgebungsbasis, alle lokalen Eigenschaften können auf affinen Varietäten nachgerechnet werden. Hierzu gehören z.B. lokale Ringe und Funktionenkörper.

Definition 6.15. Sei X quasi-projektiv, $P \in X$. Dann heißt

$$\mathcal{O}_{X,P}\{(U, f) \mid P \in U \subset X \text{ offen}, f \in \mathcal{O}(U)\} / \sim$$

mit der Äquivalenz von Keimen (vergleiche Definition 5.19) lokaler Ring von X in P . Ist X quasi-projektiv und irreduzibel, so heißt

$$k(X) = \{(U, f) \mid \emptyset \neq U \subset X \text{ offen}, f \in \mathcal{O}(U)\} / \sim$$

Funktionenkörper von X .

Ist X irreduzibel, so ist jede nichtleere offene Teilmenge dicht. Je zwei offene Teilmengen haben nichtleeren Schnitt.

Bemerkung. Ist X projektiv, so gibt es eine explizite Beschreibung

$$k(X) = \left\{ \frac{f}{g} \mid f, g \in k[X], \text{ homogen vom gleichen Grad}, g \neq 0 \right\}$$

wobei $k[X]$ der homogene Koordinatenring ist. Wir werden uns diese Aussage später vornehmen.

Lemma 6.16. (i) $\mathcal{O}_{X,P}$ ist ein lokaler Ring. Ist $U \subset X$ offen mit $P \in U$, so ist $\mathcal{O}_{X,P} = \mathcal{O}_{U,P}$.

(ii) $k(X)$ ist ein Körper. Ist $U \subset X$ offen, nichtleer, so ist $k(X) = k(U)$.

Beweis: Die Aussage über die Isomorphismen ist nach der Definition der Äquivalenzrelation klar. Die Strukturaussagen können dann in der quasi-affinen Situation überprüft werden, wo sie bereits bekannt sind. \square

Satz 6.17 (Identitätssatz). Sei X irreduzibel, $f, g \in \mathcal{O}(X)$ mit $f|_U = g|_U$ auf einer offenen, nichtleeren Teilmenge $U \subset X$. Dann ist $f = g$ auf ganz X .

Beweis: Wir betrachten $f - g$. Die Teilmenge $V(f - g) \subset X$ ist abgeschlossen und enthält U , also auch \bar{U} . Da X irreduzibel ist, gilt $X = \bar{U}$. \square

Daher haben im irreduziblen Fall alle Funktionenkeime (U, f) einen maximalen Definitionsbereich, auf den sie sich eindeutig fortsetzen lassen.

Definition 6.18. Sei X irreduzibel, $\Phi \in \mathbb{P}^n(k(X))$, $P \in X$. Dann heißt Φ regulär in P , falls es einen Repräsentanten $\Phi = [\Phi_0 : \dots : \Phi_n]$ gibt, so dass alle $\Phi_i(P)$ definiert sind und nicht alle gleichzeitig verschwinden. In diesem Fall setzen wir

$$\Phi(P) = [\Phi_0(P) : \dots : \Phi_n(P)] \in \mathbb{P}^n$$

Bemerkung. $\Phi(P)$ ist wohldefiniert: Gilt $[\Phi_0 : \dots : \Phi_n] = [\Phi'_0 : \dots : \Phi'_n]$ und beide Repräsentanten sind regulär in P , so ist $\Phi_i = \Psi \Phi'_i$ für alle i . Hierbei ist $\Psi \in k(X)^*$. Ist $\Psi(P) = 0$, so ist $\Phi(P) = [0 : \dots : 0]$ nicht definiert. Ist Ψ nicht definiert in P , so auch $\Phi(P)$ nicht definiert. Also ist $\Psi(P) \neq 0$.

Satz 6.19. Seien X irreduzibel, $Y \subset \mathbb{P}_k^n$. Ein Element $\Phi \in \mathbb{P}^n(k(X))$ definiert genau dann einen Morphismus $\phi : X \rightarrow Y$, wenn Φ in allen $P \in X$ regulär ist und $\Phi(P) \in Y$ für alle $P \in X$. Jeder Morphismus $f : X \rightarrow Y$ ist von dieser Form.

Beweis: Wir beginnen mit der Rückrichtung. Wir betrachten die Komposition $f : X \rightarrow Y \rightarrow \mathbb{P}^n$. Sei $U_i \subset \mathbb{P}^n$ standardaffin mit $U = f^{-1}(X)$ nicht-leer (also dicht). Eine solche Menge gibt es, da die U_i den projektiven Raum überdecken. Dann ist $f|_U$ eine Abbildung $U \rightarrow \mathbb{A}^n$, wird also durch ein Tupel $\phi_0, \dots, \hat{\phi}_i, \dots, \phi_n \in \mathcal{O}(U)$ gegeben. Wir fassen sie in $k(U) = k(X)$ auf und setzen

$$\Phi = [\phi_0 : \dots : \phi_{i-1} : 1 : \phi_{i+1} : \dots : \phi_n]$$

Für die Rückrichtung überdecken wir X durch offene Teilmengen, auf denen Φ jeweils durch reguläre Funktionen repräsentiert wird. Durch Einschränken auf noch kleinere offenen Teilmengen erhalten wir Abbildungen, deren Bild in standardaffinen Karten liegt. Dies ist die gewünschte lokale Gestalt. Wegen der Stetigkeit im affinen Fall, ist die Funktion lokal auf Y stetig. Hieraus kann die globale Stetigkeit hergeleitet werden. \square

Kapitel 7

Dimensionstheorie

Wir greifen nun den Faden im affinen Fall wieder auf und wollen zeigen, dass die Dimension des \mathbb{A}^n tatsächlich n ist. Der Beweis wird auch viele andere Eigenschaften der Dimension implizieren. Wir benötigen wieder die Ideen aus dem Beweis des Nullstellensatzes.

In diesem Kapitel geht es um endlich erzeugte, nullteilerfreie Algebren über einem Körper K .

Definition 7.1. Sei A eine nullteilerfreie K -Algebra. Eine Menge a_1, \dots, a_n heißt algebraisch abhängig über K , wenn es ein Polynom $0 \neq P \in K[X_1, \dots, X_n]$ gibt mit Nullstelle (a_1, \dots, a_n) . Eine maximale algebraisch unabhängige Teilmenge von A heißt Transzendenzbasis von A . Die Kardinalität einer Transzendenzbasis heißt Transzendenzgrad $\text{trdeg}_K(A)$ von A über K .

Bemerkung. Normalerweise macht man diese Definition nur für Körper. Eine Transzendenzbasis von A ist aber auch eine Transzendenzbasis des Quotientenkörpers $Q(A)$, denn a und $1/a$ sind algebraisch abhängig als Nullstelle des Polynoms $X_1 X_2 - 1$.

Beispiel. Sei $A = K[X_1, \dots, X_n]$ der Polynomring. Dann sind X_1, \dots, X_n eine Transzendenzbasis von A und $\text{trdeg} A = n$.

Für $a_1, \dots, a_n \in A$ bezeichnen wir mit $K[a_1, \dots, a_n]$ den Teilring von A , der von a_1, \dots, a_n erzeugt wird. Wir bezeichnen mit $K(a_1, \dots, a_n)$ den Quotientenkörper von $K[a_1, \dots, a_n]$, also den durch a_1, \dots, a_n erzeugten Teilkörper von $Q(A)$.

Zur Erinnerung (Lemma 3.6): $K[x]$ ist genau dann ein Körper, wenn $\dim_K K[x] < \infty$ und genau dann wenn x Nullstelle eines Polynoms in $K[X] \setminus \{0\}$ ist.

Lemma 7.2. Sei A eine nullteilerfreie K -Algebra. Seien $a_1, \dots, a_n \in A$. Dann ist die Menge

$$\overline{K[a_1, \dots, a_n]} = \{a \in A \mid \{a, a_1, \dots, a_n\} \text{ algebraisch abhängig}\}$$

ein Teilring von A .

Beweis: Wie in der Algebravorlesung. Wir wiederholen schnell: Jedes Element $a \in \overline{K[a_1, \dots, a_n]}$ erfüllt eine Polynomgleichung $a - P(a_1, \dots, a_n)$, ist also in $\overline{K[a_1, \dots, a_n]}$ enthalten.

Seien nun a, b algebraisch über $K[a_1, \dots, a_n]$. Dann erfüllen sie Polynomgleichungen in einer Variablen über $K_1 = K(a_1, \dots, a_n)$. Daher ist

$$\dim_{K_1} K_1[a] < \infty, \dim_{K_1[a]} K_1[a][b] < \infty \Rightarrow \dim_{K_1} K_1[a, b] < \infty$$

(vergleiche Lemma 3.7) Dann erfüllen alle Elemente von $K_1[a, b]$ eine Polynomgleichung mit Koeffizienten in K_1 . Hieraus wird nach Erweitern eine Polynomgleichung in $n + 1$ Variablen mit Koeffizienten in K . \square

Beispiel. Sei $f = X^2 + Y^2 \in K[X, Y]$, $A = K[X, Y]/(f) = K[x, y]$. Dann ist $\{x, y\}$ algebraisch abhängig, also $\overline{K[x]} = A$ nach dem Lemma. Daher ist x eine Transzendenzbasis, $\text{trdeg}(A) = 1$.

Satz 7.3. *Sei A eine nullteilerfreie K -Algebra.*

- (i) *Jede algebraisch unabhängige Menge kann zu einer Transzendenzbasis erweitert werden.*
- (ii) *Jedes System von Algebraerzeugern enthält eine Transzendenzbasis.*
- (iii) *Der Transzendenzgrad ist wohldefiniert.*

Beweis: Wie für Vektorräume. Ersetze linear abhängig durch algebraisch unabhängig. \square

Wir sind nur an endlich erzeugten Algebren interessiert, dann ist auch der Transzendenzgrad endlich.

Bemerkung. Zu Beginn des Beweises von Satz 3.8 brachten wir ein Erzeugendensystem von $K[x_1, \dots, x_n]$ in eine Ordnung, so dass x_1, \dots, x_r algebraisch unabhängig waren und x_{r+1}, \dots, x_n algebraisch abhängig von $\{x_1, \dots, x_r\}$ waren. Dort war also x_1, \dots, x_r eine Transzendenzbasis.

Theorem 7.4. *Sei A nullteilerfreie, endlich erzeugte Algebra über einem Körper K . Dann ist*

$$\dim A = \text{trdeg}_K A$$

Korollar 7.5. *Sei k algebraisch abgeschlossen. Dann ist $\dim \mathbb{A}^n = n$.*

Beweis:

$$\dim \mathbb{A}^n = \dim k[X_1, \dots, X_n] = \text{trdeg}(k[X_1, \dots, X_n]) = n$$

\square

Lemma 7.6. *Sei K Körper, A endlich erzeugte K -Algebra vom Transzendenzgrad r . Dann gilt*

$$\text{trdeg}_K(A) \leq \dim A$$

Beweis: Vollständige Induktion nach $r = \text{trdeg} A$ für alle Körper K gleichzeitig. Für $r = 0$ sind alle Elemente algebraisch über K . Wegen Lemma 3.6 und Lemma 3.7 ist $\dim_K A < \infty$ und die ist ein Körper. Als Ring hat er die Dimension 0, denn es gibt nur ein Primideal.

Sei nun $r > 1$. Wir betrachten $A = K[x_1, \dots, x_n] = K[X_1, \dots, X_n]/P$ für ein Primideal P . Ohne Einschränkung ist x_1 transzendent. Sei $S = K[X_1] \setminus \{0\}$. Dies ist eine multiplikative Menge, an der wir lokalisieren können. Es ist $S \cap P = \emptyset$, da x_1 transzendent in A . Es gilt

$$E := S^{-1}K[X_1] = S^{-1}K[x_1] = K(X_1)$$

und

$$S^{-1}A = E[X_2, \dots, X_n]/S^{-1}P$$

Hierbei ist $S^{-1}P$ ein Primideal, da $S \cap P = \emptyset$. (Nach Korollar 5.13 ist es ein echtes Ideal, Primidealeigenschaft leicht). Also ist $S^{-1}E$ eine endlich erzeugte E -Algebra mit Transzendenzgrad $r - 1$. Nach Induktionsannahme gilt

$$r - 1 \leq \dim S^{-1}A$$

D.h. es gibt eine Kette von Primidealen von $S^{-1}A$

$$0 = Q_0 \subsetneq Q_1 \subsetneq Q_2 \cdots \subsetneq Q_{r-1}$$

Ihre Urbilder \tilde{Q}_i in $S^{-1}K[X_1, \dots, X_n]$ bilden eine Kette von Primidealen, die bei $S^{-1}P$ beginnt. Wir setzen

$$P_i = \tilde{Q}_i \cap K[X_1, \dots, X_n]$$

Dies ist eine Kette von Primidealen in $K[X_1, \dots, X_n]$, die mit P beginnt. Jedes der P_i hat leeren Schnitt mit S , da $S^{-1}P_i = \tilde{Q}_i$. Daher ist die Restklasse von X_1 nicht algebraisch in $K[X_1, \dots, X_n]/P_{r-1}$.

Behauptung. P_{r-1} ist nicht maximal.

Wäre P_{r-1} maximal, so wäre $K[X_1, \dots, X_n]/P_{r-1}$ ein Körper. Da er endlich erzeugt ist als Algebra, ist er nach Satz 3.8 (für den wir hart gearbeitet haben!) endlich-dimensional als K -Vektorraum. Nach Lemma 3.6 sind dann alle Elemente algebraisch. Das ist ein Widerspruch. \square

Lemma 7.7. Seien $P \subsetneq Q$ Primideale von $K[X_1, \dots, X_n]$. Dann ist

$$\text{trdeg}(K[X_1, \dots, X_n]/Q) < \text{trdeg}(K[X_1, \dots, X_n]/P)$$

Beweis: Der Homomorphismus $K[X_1, \dots, X_n]/P \rightarrow K[X_1, \dots, X_n]/Q$ ist surjektiv. Sind also Elemente algebraisch abhängig modulo P , dann auch modulo Q . Dies bedeutet, dass \leq gilt.

Angenommen, es gilt Gleichheit. Sei $\alpha_i = X_i \pmod{P}$ und $\beta_i = X_i \pmod{Q}$. Sei ohne Einschränkung β_1, \dots, β_r eine Transzendenzbasis von $K[\beta_1, \dots, \beta_r]$. Dann

sind $\alpha_1, \dots, \alpha_r$ algebraisch unabhängig und wegen der Gleichheit der Transzendenzgrade bilden sie eine Transzendenzbasis von $K[\alpha_1, \dots, \alpha_n]$. Nun Lokalisieren wir wieder. Sei $S = K[X_1, \dots, X_r] \setminus \{0\}$. Dies ist eine multiplikative Menge. Es gilt $S \cap P = S \cap Q = \emptyset$, da X_1, \dots, X_r algebraisch unabhängig modulo P und Q bleiben. Sei

$$E = S^{-1}K[X_1, \dots, X_r] = K(X_1, \dots, X_r) = K(\alpha_1, \dots, \alpha_r) = K(\beta_1, \dots, \beta_r)$$

und es gilt

$$S^{-1}K[X_1, \dots, X_n]/P = E[\alpha_{r+1}, \dots, \alpha_n]$$

Hierin sind $\alpha_{r+1}, \dots, \alpha_n$ algebraisch über E . Nach Lemma 3.6 ist also $E[\alpha_{r+1}, \dots, \alpha_n]$ ein Körper. Dies bedeutet, dass $S^{-1}P$ ein maximales Ideal ist. Es ist aber $S^{-1}P \subset S^{-1}Q \subset S^{-1}K[X_1, \dots, X_n]$. Wegen $S \cap Q = \emptyset$ sind dies echte Inklusionen, ein Widerspruch zur Maximalität. \square

Beweis von Theorem 7.4: Sei $A = K[X_1, \dots, X_n]/P$ für ein Primideal P . Zu zeigen ist

$$\text{trdeg}(A) = \dim A$$

Nach Lemma 7.6 gilt \leq . Wir betrachten nun eine maximale Kette von Primidealen

$$0 = \overline{Q}_0 \subsetneq \overline{Q}_1 \subsetneq \dots \subsetneq \overline{Q}_{\dim A}$$

Sei Q_i das Urbild von \overline{Q}_i in $K[X_1, \dots, X_n]$, insbesondere $Q_0 = P$. Nach Lemma 7.7 gilt

$$\begin{aligned} \text{trdeg}(K[X_1, \dots, X_n]/Q_0) &> \text{trdeg}(K[X_1, \dots, X_n]/Q_1) > \dots \\ &> \text{trdeg}(K[X_1, \dots, X_n]/Q_{\dim A}) \end{aligned}$$

Da die letzte Zahl mindestens 0 ist, folgt

$$\text{trdeg}(K[X_1, \dots, X_n]) \geq \dim A$$

\square

Beispiel. Sei $f \in K[X, Y]$ eine irreduzible Gleichung. Dann ist

$$\text{trdeg}(K[X, Y]/f) = 1$$

also $\dim V(f) = 1$. Diese Varietäten heißen *ebene Kurven*.

Korollar 7.8. Sei $V \subset \mathbb{P}^n$ quasiprojektiv mit irreduziblen Komponenten V_1, \dots, V_m . Dann gilt

$$\dim(V) = \max \text{trdeg}(k(V_i)) \leq n$$

Beweis: Wegen $\dim V = \max \dim V_i$ genügt es, den irreduziblen Fall zu betrachten. Wir betrachten eine Kette maximaler Länge

$$V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_r = V$$

von irreduziblen abgeschlossenen Teilmengen. Sie beginnt mit einem Punkt. Dieser liegt in einer affinen, offenen Teilmenge U von V . Wir betrachten die Kette $V'_i = V_i \cap U$ in U . Wegen $P \in U \cap V_i$ ist diese Menge dicht in V_i und selbst irreduzibel. Es gilt also

$$r = \dim V \geq \dim U = r$$

und nach Theorem 7.4

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

Andererseits sei $\bar{V}_i \subset \mathbb{P}^n$ der Abschluss von V_i in \mathbb{P}^n . Da V_i irreduzibel ist, sind die \bar{V}_i echt ineinander enthalten. Es folgt $r \leq \dim \mathbb{P}^n = \dim \mathbb{A}^n = n$. \square

Wir erwarten, dass das Hinzufügen einer Gleichung die Dimension um 1 verringert. Das ist nicht richtig:

Beispiel. Sei $V = V(XY) \subset \mathbb{A}^2$. Dies ist eine ebene Kurve. Hierin definiert $X = 0$ eine echte abgeschlossene Teilmenge derselben Dimension.

Umgeht man dieses Problem der irreduziblen Komponenten, so wird die Idee richtig:

Theorem 7.9 (Krulls Hauptidealsatz). *Sei X irreduzible Varietät, $g : X \rightarrow \mathbb{A}^1$ ein nichtkonstanter Morphismus, Z eine irreduzible Komponente von $V(g)$. Dann gilt*

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

Dies hat weitreichende Konsequenzen:

Korollar 7.10. *Sei X irreduzibel, $Z \subsetneq X$ eine maximale irreduzible abgeschlossene Teilmenge. Dann ist*

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

Beweis: Ohne Einschränkung ist X affin, $Z = V(f_1, \dots, f_n)$ für nichtkonstante Funktionen f_i . Wegen $Z \subset V(f_1)$ liegt Z in einer irreduziblen Komponente von $V(f_1)$. Wegen der Maximalität stimmt es mit dieser überein. Nun greift Krulls Hauptidealsatz. \square

Korollar 7.11 (Äquidimensionalität). *Sei X eine irreduzible Varietät,*

$$Z_0 \subsetneq Z_1 \subsetneq \dots \subsetneq Z_n$$

eine Kette von irreduziblen abgeschlossenen Teilmengen. Diese kann zu einer Kette der Länge $\dim X$ ergänzt werden. Insbesondere hat jede maximale Kette dieselbe Länge $\dim X$.

Beweis: Ohne Einschränkung ist $Z_n = X$, Z_0 ein Punkt. Es genügt zu zeigen:

Behauptung. *Ist $\dim Z_i < \dim Z_{i+1} - 1$, so gibt es eine irreduzible Teilmenge $Z_i \subsetneq Z \subsetneq Z_{i+1}$*

Wir wählen für Z eine eine maximale irreduzible Teilmenge von Z_{i+1} , die Z_i enthält. Diese hat Dimension $\dim Z_{i+1} - 1$, liegt also echt zwischen Z_i und Z_{i+1} . \square

Endliche Morphismen

Definition 7.12. Sei $f : A \rightarrow B$ ein Ringhomomorphismus.

- (i) B heißt endlich über A , falls B ein endlich erzeugter A -Modul ist.
- (ii) Ein Element $b \in B$ heißt ganz über A , falls $A[b]$ ein endlich erzeugter A -Modul ist.
- (iii) B heißt ganz über A , falls alle Elemente von B ganz über A sind.

Bemerkung. Ein Morphismus $f : X \rightarrow Y$ von quasi-projektiven Varietäten heißt *endlich*, wenn es eine offene affine Überdeckung $Y = U_1 \cup \dots \cup U_n$ gibt, so dass für alle i das Urbild $f^{-1}U_i$ affin ist und $k[f^{-1}(U_i)]$ endlich über $k[U_i]$. Wir brauchen aber nur den affinen Fall.

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

(ii) Sei $A = \mathbb{Z}$, $B = \mathbb{Z}[\sqrt{3}]$. Dann wird B als \mathbb{Z} -Modul erzeugt von $1, \sqrt{3}$.

(iii) Sei $A = k[X]$, $B = k[X, Y]$. Dann ist B endlich erzeugt als A -Algebra, aber nicht als A -Modul, denn $1, Y, Y^2, \dots$ ist eine A -Basis. Die Erweiterung ist nicht endlich.

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

Bemerkung. In der algebraischen Zahlentheorie betrachtet man $A = \mathbb{Z}$, B die Menge aller ganzen Elemente in einem Körper K/\mathbb{Q} . Man zeigt dann, dass B ein Ring ist und sogar endlich, falls K/\mathbb{Q} endlich. Bei uns werden diese Fragen keine Rolle spielen.

Zunächst einfache Rechenregeln.

Lemma 7.13. Sei $f : A \rightarrow B$ endlicher Ringhomomorphismus.

(i) Sei $g : B \rightarrow C$ endlich. Dann ist auch $g \circ f : A \rightarrow C$ endlich.

(ii) Seien $I \subset A$, $J \subset B$ Ideale mit $f(I) \subset J$. Dann ist

$$\bar{f} : A/I \rightarrow B/J$$

endlich.

(iii) Sei $S \subset A$ multiplikativ mit $0 \notin f(S)$. Dann ist

$$S^{-1}f : S^{-1}A \rightarrow S^{-1}B$$

endlich.

Beweis: Sei b_1, \dots, b_n ein Erzeugendensystem von B . Dann sind die Restklassen $\text{mod } J$ Erzeuger von B/J . Die Brüche $b_i/1$ sind Erzeuger von $S^{-1}B$. (Die Voraussetzung $0 \notin f(S)$ wird gebraucht, damit $S^{-1}B$ ein Ring ist.)

Ist c_1, \dots, c_m ein B -Erzeugendensystem von C , so sind die $f(b_i)c_j$ ein A -Erzeugendensystem von C . \square

Lemma 7.14. *Sei $A \rightarrow B$ Ringhomomorphismus, $b \in B$ ein Element. b ist genau dann ganz über A , wenn b Nullstelle eines normierten Polynoms $F \in A[X]$ ist.*

Beweis: Sei $F = X^n + a_1X^{n-1} + \dots + a_n \in A[X]$ mit Nullstelle b .

Behauptung. $1, b, b^2, \dots, b^{n-1}$ erzeugen $A[b]$.

Es ist

$$b^n = -a_1b^{n-1} - \dots - a_n \in \langle 1, \dots, b_{n-1} \rangle_A \subset B$$

Diese Relation multiplizieren wir mit b und es folgt

$$b^{n+1} = -a_1b^n - \dots - a_nb \in \langle b, \dots, b^n \rangle_A \subset \langle 1, \dots, b^{n-1} \rangle_A$$

Ebenso folgt iterativ, dass alle b^i in diesem Modul liegen.

Sei umgekehrt $A[b]$ erzeugt von b_1, \dots, b_n . Sei b^N die maximale Potenz von b , die in b_1, \dots, b_n vorkommt. Dann lässt sich b^{N+1} als Linearkombination von b_1, \dots, b_n schreiben. Dies ergibt die gesuchte normierte Polynomrelation für b über A . \square

Endliche Morphismen sind für uns wichtig, da wir die Dimensionen vergleichen können.

Satz 7.15 (Going-Down). *Sei $f : A \rightarrow B$ endlicher Ringhomomorphismus, $P \subsetneq Q$ Primideale von B . Dann sind $f^{-1}P \subsetneq f^{-1}Q$ ebenfalls verschiedene Primideale. Insbesondere gilt*

$$\dim B \leq \dim A$$

Beweis: Urbilder von Primidealen sind Primideale. Es gilt $f^{-1}P \subset f^{-1}Q$. Angenommen, es ist $f^{-1}P = f^{-1}Q =: \mathfrak{p}$.

Behauptung. *Ohne Einschränkung ist A lokal mit maximalem Ideal \mathfrak{p} .*

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 $S^{-1}\mathfrak{p}$. Es ist $0 \notin f(S)$, da $S \cap P = \emptyset$. Daher ist $S^{-1}B$ ein Ring. Es gilt weiter $S^{-1}B = f(S)^{-1}B$ (links wird als A -Modul lokalisiert, rechts als B -Modul.) Wegen $f(S) \cap P = f(S) \cap Q = \emptyset$ bleibt $S^{-1}P \subset S^{-1}Q$ eine echte Inklusion von Primidealen. Der Ringhomomorphismus $A_{\mathfrak{p}} \rightarrow S^{-1}B$ ist endlich. Sei also nun ohne Einschränkung A wie in der Behauptung.

Behauptung. *Ohne Einschränkung ist A ein Körper.*

$A/\mathfrak{p} \rightarrow B/B\mathfrak{p}$ ist endlich. Es gilt

$$B\mathfrak{p} \subset P/B\mathfrak{p} \subsetneq Q/B\mathfrak{p}$$

d.h. die echte Inklusion von Primidealen bleibt erhalten. A/\mathfrak{p} ist ein Körper, da \mathfrak{p} maximal war.

Sei nun $A = K$, B ein endlich-dimensionaler K -Vektorraum. Wir betrachten

$$K \rightarrow B/P \rightarrow B/Q$$

Hierin sind B/P und B/Q Integritätsbereiche, die endlich sind über K . Nach Lemma 3.6 sind beides Körper, haben also nur ein maximales Ideal, nämlich 0. Dies impliziert $P = Q$, der gesuchte Widerspruch.

Die Dimensionsaussage folgt sofort: Ist eine Primidealkette in B gegeben, so bilden die Urbilder eine Primidealkette derselben Länge in A . \square

Im Allgemeinen gilt keine Gleichheit.

Beispiel. Sei $A = k[X, Y]$, $B = k[X, Y]/f$ für ein irreduzibles f . Dann ist $A \rightarrow B$ endlich, aber $\dim A = \dim \mathbb{A}^2 = 2$, $\dim B = \dim V(f) = 1$.

Das ist aber auch das einzige Problem.

Theorem 7.16 (Going-Up). *Sei $f : A \rightarrow B$ injektiver, endlicher Ringhomomorphismus, A, B nullteilerfrei, $\mathfrak{p} \subsetneq \mathfrak{q}$ Primideale von A , P ein Primideal von B mit $A \cap P = \mathfrak{p}$. Dann gibt es ein Primideal $Q \subset B$ mit $B \cap A = \mathfrak{q}$. Insbesondere gilt*

$$\dim A = \dim B$$

Hier identifizieren wir A mit seinem Bild $f(A)$.

Beweis: Wir beginnen mit der Dimensionsaussage. Nach dem vorherigen Satz gilt \geq . Jede Primidealkette in A lässt sich zu einer Kette in B liften (Induktionsanfang für das Nullideal, Induktionsschritt Going-Up). Also gilt \leq .

Wie im letzten Beweis lokalisieren wir, diesmal an \mathfrak{q} . Sei $S = S_{\mathfrak{q}} = A \setminus \mathfrak{q}$. Dies ist eine multiplikative Teilmenge von A , aber auch von B . (Hier geht die Injektivität ein!) Dann ist

$$f : A_{\mathfrak{q}} \rightarrow S^{-1}B$$

weiterhin endlicher Ringhomomorphismus. Es genügt, die Behauptung in dieser Situation zu zeigen. Ist nämlich \bar{Q} ein Primideal von $S^{-1}B$, das $S^{-1}P$ und $S^{-1}\mathfrak{q}$ enthält, so ist $\bar{Q} = S^{-1}Q$ für ein Primideal Q , das P und \mathfrak{q} enthält.

Sei also ohne Einschränkung \mathfrak{q} maximal. Wieder wie im letzten Beweis gehen wir über zu

$$A/\mathfrak{p} \rightarrow B/P$$

Dies ist endlicher Ringhomomorphismus. Sei nun \bar{Q} ein maximales Ideal von B/P , welches $\mathfrak{q}/\mathfrak{p}$ enthält. Das geht, da $\mathfrak{q}/\mathfrak{p}$ ein echtes Ideal ist. Das Urbild Q von \bar{Q} in B hat die gewünschte Eigenschaft. \square

Wir wenden dies für affine Varietäten an.

Korollar 7.17. *Sei $f : X \rightarrow Y$ endlicher Morphismus von affinen irreduziblen Varietäten so dass $k[Y] \rightarrow k[X]$ injektiv ist. Dann ist f surjektiv.*

Beweis: Sei $Q \in Y$. Dann hat das maximale Ideal $I(Q) \subset k[Y]$ einen Lift zu einem Primideal P von $k[X]$. Sei $Q' \in V(P)$, also $I(Q') \supset P \supset I(Q)$. Dann gilt $f(Q') = Q$. \square

Theorem 7.18 (Noethersches Normalisierungslemma). *Sei Y eine irreduzible affine Varietät über k der Dimension d . Dann gibt es einen endlichen surjektiven Morphismus*

$$\pi : Y \rightarrow \mathbb{A}^d$$

Beweis: $B = k[Y]$ ist ein Integritätsbereich.

Behauptung. *Es gibt einen injektiven ganzen Ringhomomorphismus*

$$f : k[X_1, \dots, X_n] \rightarrow k[Y]$$

Es ist $B = k[Y] = k[Y_1, \dots, Y_m]/\mathfrak{p}$ für ein Primideal \mathfrak{p} . Sei $y_i = Y_i \pmod{\mathfrak{p}}$. Falls $m = d$, so ist $m = \dim Y = \text{trdeg}k[y_1, \dots, y_m]$, die Elemente sind algebraisch unabhängig, also $Y = \mathbb{A}^d$ und es ist nichts zu zeigen.

Sei nun $d < m$. Wir argumentieren mit Induktion über m . Es genügt zu zeigen, dass es $B' \subset B$ gibt, so dass B endlich ist über B' und B' wird (als k -Algebra) von $m - 1$ Elementen erzeugt. (Denn dann ist B' endlich über $k[X_1, \dots, X_d]$ nach Induktionsvoraussetzung und Endlichkeit ist transitiv.)

Da $m > d$, gibt es eine Relation $f \in k[Y_1, \dots, Y_m]$

$$f(y_1, \dots, y_m) = 0$$

Seien $r_2, \dots, r_m \in \mathbb{N}$. Wir setzen

$$z_i = y_i - y_1^{r_i} \quad \text{für } i = 2, \dots, m$$

Dann gilt

$$f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = 0$$

d.h. (y_1, z_2, \dots, z_m) ist Nullstelle eines Polynoms

$$F(Y_1, Z_2, \dots, Z_m) = f(Y_1, Z_2 + Y_1^{r_2}, \dots, Z_m + Y_1^{r_m}) \in k[Y_1, Z_2, \dots, Z_m]$$

Ein Monom $a \prod Y_i^{b_i}$ in f induziert mehrere Terme in F , u.a. den führenden Term in y_1

$$a y_1^{b_1 + r_2 b_2 + \dots + r_m b_m}$$

Wenn die r_i groß genug sind und weit genug auseinander, dann haben alle diese Monome unterschiedliche Grade. Einer von ihnen hat den höchsten Grad

$$F(Y_1, Z_2, \dots, Z_m) = b Y_1^N + \text{kleinere Terme bzgl. } Y_1$$

Dann ist $1/bF(Y_1, z_2, \dots, z_m)$ eine normierte Gleichung für y_1 über $k[z_2, \dots, z_m]$. Wir setzen

$$B' = k[z_2, \dots, z_m] \subset k[z_2, \dots, z_m][y_1] = B$$

Nach Lemma 7.14 ist B ganz über B' . □

Lemma 7.19. *Sei $A = k[X_1, \dots, X_d]$, $A \rightarrow B$ endlicher Ringhomomorphismus, B ein Integritätsring, $b \in B$ ein Element. Dann ist b Nullstelle eines irreduziblen normierten $F \in A[T]$*

$$F = T^m + a_1 T^{m-1} + \dots + a_m$$

mit Nullstelle b . Wir fassen Multiplikation mit B als $Q(A)$ -lineare Abbildung $Q(B) \rightarrow Q(B)$ 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 $F \in A[T]$. Wir wählen F irreduzibel über A . Nach dem Gauß-Lemma ist das Polynom sogar irreduzibel in $Q(A)[T]$. Es gilt $Q(B') = Q(A)[b]$, ein Vektorraum mit Basis $1, b, \dots, b^{m-1}$. Wir berechnen die Matrix M der Multiplikation mit b

$$b : Q(B') \rightarrow Q(B')$$

und erhalten $\det(b) = \pm a_m$.

B ist endlich erzeugt über A also Modul, also ist $B = A[b, b_1, \dots, b_n]$ für endlich viele ganze Elemente b_i . Hieraus folgt $Q(B) = Q(A)[b, b_1, \dots, b_n]$ und dies ist ebenfalls ein endlich-dimensionaler $Q(A)$ -Vektorraum.

Damit gilt: $Q(A) \subset Q(B') \subset Q(B)$, alles endlich-dimensionale Vektorräume über $Q(A)$. Die $Q(A)$ -Matrix der Multiplikation mit b auf $Q(B)$ ist eine Blockdiagonalmatrix mit Blöcken die Matrix der Multiplikation mit b auf $Q(B')$. Also ist $\det(b)$ eine Potenz von $\pm a_m$. □

Beweis von Theorem 7.9: Sei Y irreduzible Varietät, $g : Y \rightarrow \mathbb{A}^1$ nicht-konstanter Morphismus, Z irreduzible Komponente von $V(g)$. Wir wollen zeigen, dass

$$\dim Z = \dim Y - 1$$

Zunächst zerlegen wir $V(g)$ in irreduzible Komponenten $Z \cup Z_1 \cup \dots \cup Z_n$. Sei

$$U \subset X \setminus (Z_1 \cup \dots \cup Z_n)$$

affin mit $U \cap Z \neq \emptyset$. Wir ersetzen Y durch U . D.h. es genügt, den affinen Fall zu betrachten und $Z = V(g)$ ist irreduzibel.

Sei $d = \dim Y$. Nach dem Noetherschen Normalisierungslemma gibt es einen endlichen surjektiven Morphismus

$$\pi : X \rightarrow \mathbb{A}^d$$

Wir suchen $V(g') \subset \mathbb{A}^d$ mit $\pi(Z) = V(g')$. Dann ist nämlich wegen Going-Up

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

Wir betrachten $A = k[\mathbb{A}^d] = k[X_1, \dots, X_d]$, $B = k[Y]$. Wir setzen

$$g' = \det(g)$$

Nach dem Lemma liegt dies in A .

Behauptung. $g' \in k[Y]g \subset k[Y]$

g' ist Potenz des konstanten Terms des Minimalpolynoms. Wegen

$$\pm g' = g(g^{n-1} + a_1 g^{n-2} + \dots + a_{n-1})$$

folgt

$$g' \in \langle g \rangle \subset k[Y]$$

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

Die Inklusion \supset folgt aus der vorherigen Behauptung. Sei $h \in \sqrt{\langle g \rangle} \cap A$, d.h.

$$h^N = \alpha g \in k[Y]$$

Wir nehmen die Determinante dieser Relation und erhalten in A

$$\det(h)^N = \det(\alpha)g'$$

also die gesuchte Relation.

Daher ist

$$k[X_1, \dots, X_d]/I(V(g')) \rightarrow k[Y]/I(V(g))$$

injektiver endlicher Ringhomomorphismus von Integritätsringen. Wegen Going-Up haben beide dieselbe Dimension. Links stimmt sie mit

$$\dim k[X_1, \dots, X_d]/\langle g' \rangle = \operatorname{trdeg}_k k[X_1, \dots, X_d]/\langle g' \rangle = d - 1$$

überein. □

Der Vollständigkeit halber:

Satz 7.20 (Gauß-Lemma). *Sei A ein nullteilerfreier Ring mit eindeutiger Primfaktorzerlegung, $F \in A[T]$ ein normiertes Polynom, $G \in Q(A)[T]$ ebenfalls normiert mit $G|F$. Dann gilt $G \in A[T]$.*

Beweis: Algebra-Bücher oder Zahlentheorie. □

Kapitel 8

Schnitttheorie im projektiven Raum

Ziel ist der Beweis des Satzes von Bézout über Schnitte von Untervarietäten des projektiven Raums. Zur Motivation hier schon mal die ebene Version.

Satz 8.1 (Bézout für Kurven). *Seien $C_1, C_2 \subset \mathbb{P}^2$ verschiedene irreduzible Kurven vom Grad d_1, d_2 . Dann hat $C_1 \cap C_2$ mit Vielfachheit gezählt genau $d_1 d_2$ viele Punkte.*

Definition 8.2. *Sei $f \in k[X_0, \dots, X_n]$ irreduzibel vom Grad d . Dann heißt $V(f) \subset \mathbb{P}^n$ ebene projektive Kurve vom Grad d .*

Jetzt fehlt noch die Schnittmultiplizität.

Definition 8.3. *Seien $C_1, C_2 \subset \mathbb{P}^2$ Kurven, $P \in C_1 \cap C_2$. Dann heißt*

$$i(C_1, C_2, P) = \dim_k \mathcal{O}_{C_1, P} \otimes_{\mathcal{O}_{\mathbb{P}^2, P}} \mathcal{O}_{C_2, P}$$

Schnittmultiplizität von C_1 und C_2 in P .

Bemerkung. Die lokalen Ringe nur von einer Umgebung von P abhängen, können wir in den Rechnungen affine ebene Kurven betrachten. Sei $C_1, C_2 \subset \mathbb{A}^n$ und $I(C_1) = \langle f_1, \dots, f_s \rangle, I(C_2) = \langle g_1, \dots, g_t \rangle$. Wir setzen $J = \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$. Dann gilt

$$\mathcal{O}_{C_1, P} \otimes_{\mathcal{O}_{\mathbb{A}^n, P}} \mathcal{O}_{C_2, P} = (k[X_1, \dots, X_n]/J)_{I(P)}$$

(Wer Tensorprodukte nicht mag, nimmt das als Definition.) Es ist $C_1 \cap C_2 = V(J)$ und

$$I(C_1 \cap C_2) = \sqrt{J}$$

Die Schnittmultiplizitäten messen also den Unterschied zwischen J und seinem Radikal.

Beispiel. Sei $C_1 = L$ eine affine Gerade, $C_2 = V(f)$ mit f . Ohne Einschränkung ist $L = V(X)$, $P = (0, 0)$. Dann ist

$$\begin{aligned}\mathcal{O}_{\mathbb{A}^2, P} &= k[X, Y]_{\langle X, Y \rangle} \\ \mathcal{O}_{L, P} &= (k[X, Y]/X)_{\langle X, Y \rangle} \cong k[Y]_{(Y)} \\ \mathcal{O}_{V(f), P} &= (k[X, Y]/f)_{(X, Y)} \\ \mathcal{O}_{L, P} \otimes \mathcal{O}_{V(f), P} &\cong (k[X, Y]/X \otimes k[X, Y]/f)_{(X, Y)} = (k[Y]/f(0, Y))_{(Y)}\end{aligned}$$

Das Polynom $f(0, Y)$ zerfällt als Produkt von Linearfaktoren $(Y - y)$. Für $y \neq 0$ liegt der Faktor in (Y) , ist also in der Lokalisierung invertierbar. Sei m die Multiplizität von $Y - 0$ in $F(0, Y)$. Dann ist

$$(k[Y]/f(0, Y))_{(Y)} = (k[Y]/Y^m)_{(Y)} = k[Y]/Y^m$$

denn in dieser Quotient ist bereits ein lokaler Ring mit einzigem Primideal $Y \bmod Y^m$. Er hat die k -Basis $1, Y, \dots, Y^{m-1}$, also Dimension m .

Bemerkung. Wenn die Kurven C_1 und C_2 keine irreduziblen Komponenten gemeinsam haben, so hat der Schnitt die Dimension 0, besteht also nur aus endlich vielen Punkten. Es ist nicht schwer zu zeigen, dass dann die Schnittmultiplizität endlich ist. Es folgt aber auch aus dem Satz von Bézout, daher gehen wir das jetzt nicht an.

Graduierte Ringe und Moduln

Definition 8.4. (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 Multiplikationsabbildung

$$\mu : S \times S \rightarrow S$$

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

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

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

von A -Moduln zusammen mit einer skalaren Multiplikation

$$\mu : S \times M \rightarrow M$$

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

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

(iv) Ein graduiertes Ideal von S ist ein gradierter Untermodul von S .

Beispiel. Sei $A = K$ ein Körper. Dann ist $K[X_0, \dots, X_n]$ ein gradierter Ring mit $K[X_0, \dots, X_n]_d$ der Vektorraum der homogenen Polynome vom Grad d .

Lemma 8.5. Ist $V \subset \mathbb{P}_k^n$ eine projektive Varietät, so ist $I(V)$ ein graduiertes Ideal.

Beweis: Wir erinnern uns:

$$I(V) = \left\{ \sum f_d \mid f_d(V) = 0 \right\}$$

Die Menge ist abgeschlossen unter Addition und Multiplikation mit homogenen Polynomen. Da jedes Polynom Summe von homogenen Polynomen ist, ist $I(V)$ ein Ideal.

Sei $f_d \in I(V)$ homogen vom Grad d , $s_m \in k[X_0, \dots, X_n]_m$ homogen vom Grad m . Dann ist $s_m f_d$ homogen vom Grad $m + d$. Damit ist $I(V)$ ein graduiertes Ideal. \square

Lemma 8.6. Sei S gradierter Ring, $I \subset S$ gradierter Modul. Dann ist

$$S/I \cong \bigoplus_{d=0}^{\infty} S_d/I_d$$

wieder graduiert.

Beweis: Wir betrachten die offensichtliche Abbildung von rechts nach links. Sie ist offensichtlich surjektiv.

Sei $s = \sum_{d=0}^n s_d$ im Kern, d.h. $s \in I$. Dann gilt $s_d \in I_d$ für alle d , da I ein graduiertes Ideal ist. Die Abbildung ist auch injektiv. \square

Korollar 8.7. Sei $V \subset \mathbb{P}^n$ projektiv. Der homogene Koordinatenring $S(V) = k[X_0, \dots, X_n]/I(V)$ ist eine graduierte k -Algebra.

Bemerkung. Wir hatten denselben Ring schon einmal mit $k[V]$ bezeichnet. Die Notation $S(V)$ ist klarer. S soll an die symmetrische Algebra erinnern, denn

$$k[X_0, \dots, X_n] = \text{Sym}^* k^{n+1}$$

Lemma 8.8. Sei R ein gradierter Ring, $S \subset R$ eine multiplikative Menge, die aus homogenen Elementen besteht. Dann ist $S^{-1}R$ ein gradierter Ring. Wir erhalten eine Bijektion zwischen den graduierten Primidealen von $S^{-1}R$, und den graduierten Primidealen von R , die S nicht schneiden.

Beweis: $S^{-1}R_d = \{f/s \in S^{-1}R \mid f \in R_{\deg s+d}\}$ ist die Graduierung. Die anderen Aussagen folgen wie im nicht-graduierten Fall. \square

Ist $P \subset R$ ein graduiertes Primideal, so definieren wir $R_P = S^{-1}R$ mit S die Menge der homogenen Elemente von $R \setminus P$. Dies ist ein lokaler gradierter Ring mit maximalem Ideal $S^{-1}P$.

Schnitttheorie lässt sich nun auf die Theorie der Moduln über dem homogenen Koordinatenring zurückführen.

Definition 8.9. Sei M ein endlich erzeugter graduierter Modul über $S = k[X_0, \dots, X_n]$. Dann heißt

$$\phi_M : \mathbb{Z} \rightarrow \mathbb{Z} \quad \phi_M(d) = \dim_k M_d$$

Hilbert-Funktion von M .

Am interessantesten sind natürlich die homogenen Koordinatenringe von Untervarietäten.

Theorem 8.10. Sei M ein endlich erzeugter graduierter $k[X_0, \dots, X_n]$ -Modul. Dann gibt es ein eindeutiges Polynom $P_M \in \mathbb{Q}[z]$ mit

$$P_M(d) = \phi_M(d) \text{ für groß genug}$$

Es gilt

$$\deg P_M = \dim V(I(M))$$

wobei $I(M) = \{s \in k[X_0, \dots, X_n] \mid sM = 0\}$.

Definition 8.11. Sei $V \subset \mathbb{P}^n$. Das Hilbert-Polynom P_V von V ist das Hilbertpolynom von $S(Y)$. Ist

$$P_V(z) = a_d z^d + \dots + a_0 \quad a_0 \neq 0$$

so heißt $d!a_d$ Grad von V .

Bemerkung. Wegen $I(S(V)) = I(V)$ gilt $d = \deg P_V = \dim V$. Wir werden sehen, dass der Grad im Fall ebener Kurven mit der ersten Definition übereinstimmt.

Beispiel. (i) Sei $M = S = k[X_0, X_1]$. Dann hat S_d die k -Basis $X_0^a X_1^{d-a}$, enthält also $d+1$ Elemente. Es ist also

$$\phi_S(d) = d+1$$

und das Hilbert-Polynom ist $z+1$. Der Grad des Polynoms ist 1, wie die Dimension. Nach Definition hat \mathbb{P}^2 den Grad $1!1 = 1$.

(ii) Sei $f = X_0 X_1 - X_2^2$, $M = S(V(f))$. Beim Rechnen in M können jeweils quadratische Potenzen von X_2 eliminiert werden, die beiden anderen Variablen können frei gewählt werden. Also hat M_d die k -Basis

$$X_0^a X_1^{d-a} \quad a = 0, \dots, d \quad X_0^b X_1^{d-b-a} X_2^b \quad b = 0, \dots, d-1$$

Also

$$\phi_M(d) = 2d+1, P_{V(f)} = 2z+1$$

Definition 8.12. Ein numerisches Polynom ist ein Polynom $P \in \mathbb{Q}[z]$ mit $P(n) \in \mathbb{Z}$ für alle $n \in \mathbb{Z}$ genügend groß.

Beispiel. $\binom{z}{3}$ hat ganze Werte für $z \in \mathbb{N}_0$.

Lemma 8.13. (i) Sei $F \in \mathbb{Q}[z]$ ein numerisches Polynom. Dann gilt

$$F(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \dots + c_r \quad c_i \in \mathbb{Z}$$

(ii) Sei $f : \mathbb{Z} \rightarrow \mathbb{Z}$ eine Funktion, $\Delta(f)(n) = f(n+1) - f(n)$ sei gleich einem numerischen Polynom $G \in \mathbb{Q}[z]$ für n genügend groß. Dann gibt es ein numerisches Polynom P mit $P(n) = f(n)$ für n genügend groß.

Beweis: Wir argumentieren mit Induktion über r . Hat F den Grad 0, so ist F konstant als Funktion, und die Behauptung gilt.

Allgemein lässt sich $\binom{z}{r}$ entwickeln als

$$\binom{z}{r} = \frac{z^r}{r!} + \dots$$

Daher kann $F(z)$ eindeutig in der angegebenen Form geschrieben werden, wobei $c_i \in \mathbb{Q}$. Wir betrachten $\Delta(P)$. Dies ist ein numerisches Polynom vom Grad $r-1$. Außerdem gilt

$$\begin{aligned} \Delta \binom{z}{r} &= \frac{(z+1) \dots (z+1-r+1)}{r!} - \frac{z(z-1) \dots (z-r+1)}{r!} \\ &= \frac{z(z-1) \dots (z-r+2)}{r!} (z+1-z+r-1) \\ &= \binom{z}{r-1} \end{aligned}$$

Hieraus folgt

$$\Delta P = c_0 \binom{z}{r-1} + \dots + c_{r-1}$$

Nach Induktionsannahme gilt $c_0, \dots, c_{r-1} \in \mathbb{Z}$. Dann muss auch c_r ganz sein. Nun wenden wir uns der zweiten Aussage zu. Sei

$$G = c_0 \binom{z}{r} + \dots + c_r \quad c_i \in \mathbb{Z}$$

Wir setzen

$$\tilde{F} = c_0 \binom{z}{r+1} + \dots + c_r \binom{z}{1}$$

Dann gilt $\Delta \tilde{F} = G$, also $\Delta(f_{\tilde{F}})(n) = 0$ für genügend großes n . Mit anderen Worten

$$c_{r+1} := f(n+1) - \tilde{F}(n+1) = f(n) - \tilde{F}(n) \quad n \text{ genügend groß}$$

Also folgt $c_{r+1} \in \mathbb{Z}$. Dann erfüllt

$$F = \tilde{F} + c_{r+1}$$

die Behauptung. □

Korollar 8.14. *Ist F ein numerisches Polynom, $F = a_r z^r + \dots$ mit $a_r \neq 0$, so gilt $r!a_r \in \mathbb{Z}$.*

Lemma 8.15. *Sei $S = k[X_0, \dots, X_n]$, $P \subset S$ ein homogenes Primideal. Sei*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

eine kurze exakte Sequenz von graduierten Moduln. Dann ist

$$P \supset I(B) \Leftrightarrow P \supset I(A) \text{ oder } P \supset I(C)$$

Es gilt

$$V(I(B)) = V(I(A)) \cup V(I(C))$$

Beweis: Es gilt $I(C) \subset I(A), I(B)$ und $I(A)I(C) \subset I(B)$ (leicht). Angenommen $I(B) \subset P$, $I(A), I(C) \not\subset P$. Dann gibt es $s \in I(A)$ mit $s \notin P$, $t \in I(C)$ mit $t \notin P$. Aber $st \in I(A)I(C) \subset I(B) \subset P$. Dies ist ein Widerspruch zur Primidealeigenschaft von P .

Die Umkehrung ist klar. Die Aussage über die Varietäten folgt, wenn man maximale Ideale betrachtet. □

Satz 8.16. *Sei M ein endlich erzeugter graduierter Modul über $S = k[X_0, \dots, X_n]$. Dann gibt es eine Filtrierung*

$$0 = M^0 \subset M^1 \subset \dots \subset M^r = M$$

durch graduierte Untermoduln, so dass

$$M^i/M^{i-1} \cong (S/P_i)[l_i]$$

für ein homogenes Primideal $P_i \subset S$, $l_i \in \mathbb{Z}$.

Ist $P \subset S$ ein homogenes Primideal. Dann ist $P \supset I(M)$ genau dann, wenn $P \supset P_i$ 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, \dots, P_r . Die Häufigkeit mit der ein minimales P_i auftaucht ist unabhängig von der Wahl der Filtrierung.

Bemerkung. Weder die Filtrierung noch die auftauchenden P_i sind eindeutig.

Beweis: Hier zunächst die wesentliche Konstruktion. Sei $m \in M$ homogen, $I(m) = \{s \in S \mid sm = 0\}$. Dies ist ein homogenes Ideal. Wir betrachten die Menge der $I(m)$ für $m \neq 0$. Da der Ring S noethersch ist, enthält sie ein maximales Element $I(x)$.

Behauptung. $I(x)$ ist ein Primideal.

Sei $ab \in I(x)$ und $b \notin I(x)$, also $abx = 0$, $bx \neq 0$. Ohne Einschränkung können a, b homogen gewählt werden (zerlege a, b in homogene Komponenten, vergleiche homogene Anteile von abm von oben.). Es ist $I(x) \subset I(bx)$. Wegen der Maximalität gilt Gleichheit. Es ist $a \in I(bx)$, also $a \in I(x)$, wie zu zeigen war. Sei $l = \deg(x)$. Wir betrachten $M^1 = \langle x \rangle$. Dann gilt

$$M^1 \cong S/I(x)[l]$$

Nun betrachten wir M/M^1 , finden hierin einen Untermodul N von der gewünschten Form und setzen M^2 das Urbild von N . Induktiv erhalten wir eine Kette von Untermoduln

$$0 \subset M^1 \subset M^2 \subset M^3 \dots$$

Da M noethersch ist, endet dieser Prozess mit $M = M^r$.

Die Aussage über homogene Primideale folgt aus dem Lemma 8.15. Sei P ein minimales Primideal, das $I(M)$ enthält. Wir lokalisieren an P und erhalten eine Filtrierung

$$0 \subset M_P^1 \subset M_P^2 \dots M_P^r$$

Es ist $(S/P_i)_P \neq 0$ genau dann, wenn $P_i \subset P$. Da P minimal ist, also nur dann, wenn $P_i = P$. Dies bedeutet, dass die Kette genau soviele nicht-triviale Inklusionen enthält, wie $P_i = P$ vorkommt.

Die Unabhängigkeit von der Wahl der Kette ist ein allgemeines Prinzip. Entscheidend ist, dass der Körper $(S/P)_P$ ein einfacher S_P -Modul ist, also keine nicht-trivialen Untermoduln enthält. \square

Beweis von Theorem 8.10: Wir betrachten den graduierten Modul M . In einer kurzen exakten Sequenz

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

gilt

$$\phi_M = \phi_{M'} + \phi_{M''} \quad V(I(M)) = V(I(M')) \cup V(I(M''))$$

Die Behauptung für M' und M'' impliziert also die für M . (Beachte, dass der führende Koeffizient von $P_{M'}, P_{M''}$ nicht negativ ist, da $\phi_{M'}, \phi_{M''}$ für große n nicht negativ sind.) Nach dem letzten Satz genügt es daher $M = (S/P)[l]$ zu betrachten. Die Operation $[l]$ bedeutet $z \mapsto z + l$, also genügt sogar $M = S/P$.

1. Fall: $P = \langle X_0, \dots, X_n \rangle$. Dann ist $S/P = k$, $\phi_M(n) = 0$ für $n > 0$, also $P_M = 0$ vom Grad $-\infty$ und $V(P) = \emptyset$ hat Dimension $-\infty$.

2. Fall: $P \neq \langle X_0, \dots, X_n \rangle$. Ohne Einschränkung ist $X_0 \notin P$. Wir betrachten die kurze exakte Sequenz von graduierten Moduln

$$0 \rightarrow M \xrightarrow{X_0} M[1] \rightarrow M'' \rightarrow 0$$

Die erste Abbildung ist injektiv da P ein Primideal ist und $X_0 \notin P$. Es folgt

$$\phi_{M''}(n) = \phi_M(n+1) - \phi_M(n) = \Delta(\phi_M)(n)$$

Wegen $X_0 \in I(M'')$ gilt $I(M'') \supsetneq P$, also

$$V(I(M'')) \subset V(P) \cap V(X_0) \subsetneq V(P)$$

insbesondere, $\dim V(I(M'')) < \dim V(P)$. Mit Induktion über die Dimension der Varität können wir voraussetzen, dass die Aussage des Theorems für M'' gilt. Nach Lemma 8.13 existiert ϕ_M . Der führende Koeffizient ist positiv, da ϕ_M positiv ist für große n . \square

Satz 8.17. (i) Für $Y \subset \mathbb{P}^n$ nichtleer ist $\deg Y \in \mathbb{N}$.

(ii) Wenn $Y = Y_1 \cup Y_2$ 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 $H \subset \mathbb{P}^n$ Hyperfläche, $I(H) = \langle f \rangle$ mit f homogen vom Grad d . Dann gilt

$$\deg H = d$$

Beweis: P_Y ist ein Polynom vom Grad $r = \dim Y$. Der führende Koeffizient hat die Form $c_0/r!$ für eine ganze Zahl c_0 . Er ist positiv, da $P_Y(n) > 0$ für große n .
Zu (2): Seien I_1, I_2 die Ideale von Y_1 und Y_2 . Dann gilt

$$I := I(Y) = I(Y_1) \cap I(Y_2)$$

Es gilt $V(I_1 + I_2) = Y_1 \cup Y_2$. Wir haben also eine kurze exakte Sequenz

$$0 \rightarrow S/I \rightarrow S/I_1 \oplus S/I_2 \rightarrow S/I_1 + I_2 \rightarrow 0$$

Es folgt

$$P_Y = P_{S/I} = P_{S/I_1} - P_{S/I_2} - P_{S/I_1 + I_2} = P_{Y_1} + P_{Y_2} - P_{Y_1 \cup Y_2}$$

Wegen der Dimensionsvoraussetzung ist der führende Koeffizient

$$\frac{\deg Y}{r!} = \frac{\deg Y_1}{r!} + \frac{Y_2}{r!}$$

Zu (3): $P_{k[X_0, \dots, X_n]}$. Für $d > 0$ hat der Raum der homogenen Polynome vom Grad d in $n + 1$ -Variablen die Dimension

$$\binom{z+n}{n} = \frac{z^n}{n!} + \dots$$

Zu (4): Sei $I(H) = \langle f \rangle$ mit f vom Grad d . Wir betrachten

$$0 \rightarrow S[-d] \xrightarrow{f} S \rightarrow S/\langle f \rangle \rightarrow 0$$

Dann folgt

$$\begin{aligned}
P_H(z) &= \binom{z+n}{n} - \binom{z-d+n}{n} \\
&= \left(\frac{z^n}{n!} + \frac{1}{n!} \left(\sum_{i=1}^n i \right) z^{n-1} + \dots \right) - \left(\frac{z^n}{n!} + \frac{1}{n!} \left(\sum_{i=1-d}^{n-d} i \right) z^{n-1} + \dots \right) \\
&= 0z^n + \left(\frac{n(n+1)}{2} - \frac{n(n-2d+1)}{2} \right) \frac{z^{n-1}}{n!} + \dots \\
&= \frac{d}{(n-1)!} z^{n-1} + \dots
\end{aligned}$$

□

Definition 8.18. Sei $Y \subset \mathbb{P}^n$ eine Varietät der Dimension r und $H \subset \mathbb{P}^n$ eine Hyperfläche, die mit Y keine Komponenten gemeinsam hat. Sei Z eine irreduzible Komponente von $Y \cap H$ der Dimension $r-1$. Dann ist die Schnittmultiplizität $i(Y, H; Z_j)$ von Y und H in Z gegeben als die Vielfachheit, mit der $I(Z)$ in der Kette aus Satz 8.16 für $M = S/I(Y) + I(H)$ vorkommt.

Bemerkung. Wenn H keine Hyperfläche ist, so wird es komplizierter. Nämlich:

$$i(Y, Y'; Z) = \sum_{i=0}^{\infty} \text{len Tor}_{S_P}^i(S(Y)_P, S(Y')_P)$$

mit $P = I(Z)$.

Lemma 8.19. Sind Y, H Kurven in \mathbb{P}^2 , so stimmt dies mit der Definition 8.3 überein.

Beweis: In dieser Situation ist $Z = Q$ ein Punkt, $P := I(Z)$ ein maximales Ideal. Wir betrachten $M = S/I(H) + I(Y)$.

Nach Satz 8.16 gibt es eine endliche Filtrierung

$$M_P^0 \subset M_P^1 \cdots \subset M_P^r = M_P$$

wobei in jedem Schritt

$$(M^i/M^{i-1})_P \cong \begin{cases} 0 \\ (S/P)_P \cong k \end{cases}$$

Daher ist die Vektorraumdimension von M_P gleich der Anzahl der Länge der Kette, also der Schnittmultiplizität im Sinne der letzten Definition. □

Theorem 8.20 (Satz von Bézout). Sei $Y \subset \mathbb{P}^n$ eine Untervarietät, $H \subset \mathbb{P}^n$ eine Hyperfläche, die mit Y keine gemeinsamen Komponenten hat. Sei

$$Y \cap H = Z_1 \cup \dots \cup Z_s$$

die Zerlegung in irreduzible Komponenten. Dann gilt

$$\sum_{j=1}^s i(Y, H; Z_j) \deg Z_j = (\deg Y)(\deg H)$$

Beweis: Sei $I(H) = \langle f \rangle$ vom Grad d . Wir betrachten wieder

$$0 \rightarrow S/I(Y)[d] \xrightarrow{f} S(Y) \rightarrow M \rightarrow 0$$

mit $M = S/I(Y) + I(H)$. Es folgt

$$P_M(z) = P_Y(z) - P_Y(z-d)$$

Wir vergleichen die höchsten Koeffizienten auf beiden Seiten. Sei $\deg Y = e$, $\dim Y = r$, also

$$\begin{aligned} P_Y(z) &= \frac{e}{r!} z^r + e_1 z^{r-1} + \dots \\ P_Y(z) - P_Y(z-d) &= \frac{e}{r!} z^r + e_1 z^{r-1} + \dots - \left[\frac{e}{r!} (z-d)^r + e_1 (z-d)^{r-1} + \dots \right] \\ &= \frac{e}{r!} z^r + e_1 z^{r-1} - \frac{e}{r!} z^r - dr \frac{e}{r!} z^{r-1} - e_1 z^{r-1} + \dots \\ &= \frac{der}{r!} z^{r-1} + \dots \end{aligned}$$

Andererseits berechnen wir P_M direkt. Wir filtrieren

$$0 = M^0 \subset M^1 \subset \dots \subset M^t = M$$

mit $M^i/M^{i-1} \cong (S/P_i = [l_i])$ für Primideale P_i . Dann ist

$$P_M = \sum_{i=1}^t P_i \quad P_i = P_{(S/P_i)[l_i]}$$

Wenn $V(P_i)$ die Dimension r_i und den Grad f_i hat, dann gilt

$$P_i = \frac{f_i}{r_i!} z^{r_i} + \dots$$

Zum führenden Koeffizienten von P_M tragen nur diejenigen Summanden mit $r_i = r-1$ bei. Die zugehörigen P_i sind die Primideale der irreduziblen Komponenten von $V(I(M)) = Y \cap H$. Jedes solche P_i tritt nach Definition $i(Y, H; V(P_i))$ mal auf und der führende Koeffizient ist $\deg V(P_i)/(r-1)!$. Also

$$P_M = \sum P_i = z^{r-1} \left(\sum_{\dim V(P_i)=r-1} \frac{\deg f_i}{(r-1)!} \right) + \dots$$

Koeffizientenvergleich beweist das Theorem. □

Bemerkung. Speziell in \mathbb{P}^2 sind alle Kurven Hyperflächen. Es ergibt sich als Spezialfall der Satz von Bézout in der Version von Satz 8.1.

Korollar 8.21. Sei $C \subset \mathbb{P}^n$ eine Kurve, $f \in S(C)$ homogen vom Grad m . Dann gilt

$$\sum_{P \in C} \dim \mathcal{O}_P / \langle f \rangle = m \deg C$$

Beweis: Wir liften f nach $S = k[X_0, \dots, X_n]$. Seien f_1, \dots, f_s die irreduziblen Faktoren. Da die Dimension additiv ist, genügt es die irreduziblen Faktoren zu betrachten. Sei also ohne Einschränkung f irreduzibel. Wir setzen $H = V(f) \subset \mathbb{P}^n$. Es ist $I(H) = \langle f \rangle$. Nach dem Theorem von Bézout gilt

$$\sum_{P \in H \cap C} \dim(S(C) / \langle f \rangle)_{I(P)} = \deg H \deg C$$

Falls $P \notin H \cap C$, so ist $S(C) / f = 0$, diese Summanden tragen nicht bei. Schließlich gilt $(S(C) / \langle f \rangle)_{I(P)} = \mathcal{O}_P / \langle f \rangle$. \square

Das Element $f \in S(C)$ definiert einen Morphismus

$$f : C \rightarrow \mathbb{P}^1$$

Das Korollar sagt, dass jeder Punkt die gleiche Anzahl Urbilder (mit Vielfachheit) hat. Hieraus folgt dann, dass f endlich ist und die Erweiterung $k(\mathbb{P}^1) \rightarrow k(C)$ ebenfalls.

Kapitel 9

Ausblick

Einige klassische Gegenstände der algebraischen Geometrie sind bei uns zu kurz gekommen.

Singularitäten

Beispiel. Wir vergleichen die affinen Varietäten über \mathbb{C}

$$V_1 = V(Y^2 - X(X-1)(X-2)) \quad V_2 = V(Y^2 - X^2(X_1))$$

Beide sind irreduzibel. Beim Zeichnen der reellen Punkte sieht man bei der zweiten eine Überkreuzung in $(0, 0)$. Vom Standpunkt der reellen oder komplexen Analysis ist V_1 eine Mannigfaltigkeit, V_2 nicht.

Definition 9.1. Sei $V \subset \mathbb{A}^n$ affin, $I(V) = \langle f_1, \dots, f_m \rangle$. Dann heißt

$$\text{Jac}(V) = \left(\frac{\partial f_i}{\partial X_j} \right)_{i,j}$$

Jacobi-Matrix von V . Ein Punkt $P \in V$ heißt regulär, falls $\text{Jac}(V)$ den Rang $n - \dim V$ hat, singular andernfalls. V heißt nicht-singulär, falls alle Punkte von V regulär sind.

Beispiel. Für das obige V_i erhalten wir

$$\text{Jac}(V_1) = ((X-1)(X-2) + X(X-1) + X(X_2), 2Y) \quad \text{Jac}(V_2) = (2X(X-1) + X^2, 2Y)$$

Sei $0 \neq 2$. Dann haben die singulären Punkte in beiden Fällen $Y = 0$. Da der Punkt auf V_i liegen muss, sind die Punkte $(0, 0)$, $(1, 0)$, $(2, 0)$ bzw. $(0, 0)$, $(1, 0)$ interessant. V_1 ist glatt, V_2 ist singulär in $(0, 0)$.

Die obige Definition zeigt die Nähe zur Analysis, es handelt sich um das Kriterium, das im Satz über implizite Funktionen benötigt wird. Es lässt sich aber auch rein algebraisch umformulieren.

Definition 9.2. Sei A ein endlich-dimensionaler lokaler Ring mit maximalem Ideal m und Restklassenkörper $K = A/m$. A heißt regulär, falls $\dim_K m/m^2 = \dim A$. Ein beliebiger Ring A heißt regulär, falls für alle maximalen Ideal m von A der Ring A_m regulär ist.

Damit:

Satz 9.3. Sei $V \subset \mathbb{A}^n$ affine Varietät. Dann ist V genau dann regulär in $P \in V$, falls \mathcal{O}_P regulär ist. V ist regulär genau dann, wenn $k[V]$ regulär ist.

Es gibt noch eine weitere Charakterisierung über die Existenz von endlichen projektiven Auflösungen.

Bemerkung. Eindimensionale reguläre Ringe sind genau die diskreten Bewertungsringe. Sie kommen also als lokale Ringe von glatten Kurven vor. Ihre Besonderheit ist, dass ein Basisvektor $\pi \in m/m^2$ ein Primelement ist - bis auf Einheit sogar das einzige. Diskrete Bewertungsringe sind Hauptidealringe. Sie spielen in der algebraischen Zahlentheorie eine große Rolle.

Kurven

In diesem Abschnitt sei $C \subset \mathbb{P}^n$ eine glatte irreduzible projektive Kurve. (Wofür Glattheit gebraucht wird, wird nicht klar werden, da wir nichts beweisen.)

Es gilt

$$k(C) = (S(C)_0)_0$$

die Elemente vom Grad 0 in der Lokalisierung von $S(C)$ am Primideal 0. Mit anderen Worten: $f = a/s$ mit $a, c \in S(C)$ beide homogen vom selben Grad.

Definition 9.4. Ein Divisor auf C ist eine formale, endliche Linearkombination von Punkten

$$D = \sum_{P \in C} n_P P \quad n_P \in \mathbb{Z}, \text{ fast alle } 0$$

Der Grad von D ist $\deg D = \sum n_P$. Sei $\text{Div}(C)$ die Gruppe der Divisoren. Sei $f = a/s \in k(C)^*$ mit $a, s \in S(C)$ homogen vom selben Grad. Dann heißt

$$v_P(f) = \dim_k \mathcal{O}_P / \langle a \rangle - \dim_k \mathcal{O}_P / \langle s \rangle$$

Vielfachheit von f in P . Der Divisor

$$(f) = \sum_{P \in C} v_P(f) P$$

heißt Hauptdivisor von f .

Die Divisorenklassengruppe $\text{Cl}(C)$ von C ist definiert als $\text{Div}(C)$ modulo die Untergruppe der Hauptdivisoren.

Lemma 9.5. Hauptdivisoren sind wohldefinierte Elemente von $\text{Div}(C)$ vom Grad 0.

Beweis: Sei $m = \deg a = \deg s$. Nach Korollar 8.21 ist

$$m \deg(C) = \sum \dim \mathcal{O}_P / \langle a \rangle = \sum \dim \mathcal{O}_P / \langle s \rangle$$

Daher sind nur endliche viele der Summanden ungleich 0 und die Differenz (f) hat Grad 0. Ersetzt man a/s durch einen äquivalenten Bruch as'/ss' , so bleibt $v_P(f)$ gleich. \square

Bemerkung. $v_P : k(C) \rightarrow \mathbb{Z} \cup \{\infty\}$ ist diskrete Bewertung mit Bewertungsring \mathcal{O}_P .

Wir haben also eine kurze exakte Sequenz

$$0 \rightarrow \text{Cl}^0(C) \rightarrow \text{Cl}(C) \xrightarrow{\deg} \mathbb{Z} \rightarrow 0$$

Theorem 9.6 (Abel-Jacobi). *Es gibt eine glatte projektive Varietät $\text{Jac}(C)$ der Dimension g (das Geschlecht von C) mit*

$$\text{Jac}(C) = \text{Cl}^0(C)$$

als Menge.

Tatsächlich trägt $\text{Jac}(C)$ die Struktur einer kommutativen algebraischen Gruppe, d.h. die Addition und Subtraktion sind Morphismen von Varietäten. Die Jacobische ist ein Beispiel für eine abelsche Varietät.

Und nun noch zum wichtigsten Satz über Kurven.

Definition 9.7. *Seien $D = \sum n_P P, D' = \sum n'_P P$ Divisoren. Wir schreiben $D \geq D'$, falls $n_P \geq n'_P$ für alle $P \in C$.*

Für $D \in \text{Div}(C)$ heißt

$$L(D) = \{f \in k(C) \mid (f) \geq -D\}$$

Linearsystem zu D . Sei $l(D) = \dim_k L(D)$

Man kann sich jetzt einige elementare Eigenschaften für die $L(D)$ überlegen, z.B. ist $l(D) = 0$, falls $\deg D < 0$. $l(D)$ hängt nur von der Divisorenklasse von D ab.

Theorem 9.8 (Riemann-Roch). *Sei C glatte projektive Kurve. Dann gibt es ein eindeutig bestimmtes $g \in \mathbb{N}_0$ (das Geschlecht von g) und ein $K \in \text{Div}(C)$, so dass für alle $D \in \text{Div}(C)$*

$$l(D) - l(K - D) = 1 - g + \deg(D)$$

Ein direkter Beweis findet sich in dem kleinen Büchlein von Fulton über algebraische Kurven. In Hartshorne Kapitel IV steht ein sehr schneller Beweis mit kohomologischen Methoden.

Das Geschlecht lässt sich aus dem Grad der Kurve berechnen. Die einzige Kurve vom Geschlecht 0 ist \mathbb{P}^1 . Ebene Kurven vom Grad 3 haben Geschlecht 1. In diesem Fall ist $K = 0$, also

$$l(D) - l(-D) = \deg(D)$$

Die folgende Aussage ist dann nur eine Übungsaufgabe:

Satz 9.9. *Sei E glatte Kurve vom Geschlecht 1, $P_0 \in E$ ein Punkt. Dann ist die Abbildung*

$$E \rightarrow \text{Cl}^0(E) \quad P \mapsto P - P_0$$

bijektiv.

Seminar: Eine Kurve von Geschlecht 1 ist also ihre eigene Jacobische. Solche Kurven heißen *elliptisch*. Sie sind Gegenstand des Seminars im Wintersemester. Sie haben eine sehr reiche Struktur - insbesondere wenn der Grundkörper nicht mehr algebraisch abgeschlossen ist. Es soll um die arithmetischen Anwendungen gehen, aber natürlich wollen wir vorher auch die geometrische und analytische Situation verstehen.

Vorlesung Funktionentheorie II: Die Theoreme von Riemann-Roch und Abel-Jacobi kann man auch für kompakte Riemannsche Flächen, also eindimensionale komplexe Mannigfaltigkeiten beweisen. Hieraus folgt dann, dass jede solche Riemannsche Fläche eine projektive Kurve über \mathbb{C} ist. Diese Themen werden in der Vorlesung Funktionentheorie II behandelt werden. Überhaupt ist Funktionentheorie sehr nach verwandt mit algebraischer Geometrie. Viele Sätze über algebraische Varietäten (z.B. Bézout) wurden zunächst nur analytisch bewiesen. Manchmal gibt es bis heute kein algebraisches Argument.

Vorlesungen Strasbourg: Im nächsten Jahr wird es in Straßburg Master-vorlesungen geben zu den Themen

- Géométrie Algébrique complexe (Komplexe algebraische Geometrie)
- Géométrie symplectique (Symplektische Geometrie)
- Systèmes dynamiques en arithmétique et en analyse (Dynamische Systeme in Arithmetik und Analysis)

Die erste Veranstaltung wird eine Mischung von Funktionentheorie und algebraischer Geometrie sein, also fast eine Fortsetzung unserer Einführung. Symplektische Geometrie steht zwischen Differentialgeometrie und komplexer Geometrie. Die Objekte sind dann oft in Wirklichkeit projektive algebraische Varietäten. Stringtheorie (Stichwort Spiegelsymmetrie) benutzt dies sehr stark.

Arithmetische Geometrie

Arithmetische Geometrie kombiniert Zahlentheorie und algebraische Geometrie. Der Grundkörper ist \mathbb{Q} , eine endliche Erweiterung von \mathbb{Q} oder auch ein endlicher oder lokaler Körper.

Definition 9.10. Sei k ein Körper mit algebraischem Abschluss \bar{k} . Eine projektive Varietät V/k ist eine algebraische Varietät über \bar{k} , die durch Gleichungen in $k[X_0, \dots, X_n]$ definiert wird. Ist K/k eine Körpererweiterung, so heißt die Menge $V(K)$ der Punkte mit Koordinaten in K Menge der K -wertigen Punkte von V .

Lösungen von Polynomgleichungen über \mathbb{Q} werden also als Punkte einer Varietät aufgefasst. Überraschenderweise haben geometrische Eigenschaften der Varietät arithmetische Konsequenzen.

Theorem 9.11 (Faltings, Mordell-Vermutung). Sei K endliche Körpererweiterung von \mathbb{Q} , C/K eine glatte projektive Kurve vom Geschlecht größer gleich 2. Dann ist $C(K)$ endlich.

Der Beweis wird mit Arakelov-Theorie geführt, einer Kombination von Differentialgeometrie und algebraischer Geometrie über \mathbb{Z} .

Ist der Grundkörper \mathbb{F}_p , so ist $V(\mathbb{F}_p) \subset \mathbb{P}^n(\mathbb{F}_p)$ eine endliche Menge.

Definition 9.12. Sei V/\mathbb{F}_p eine quasi-projektive Varietät. Wir setzen

$$N_r = |V(\mathbb{F}_{p^r})|$$

Dann heißt

$$Z(V, t) = \exp \sum_{r=1}^{\infty} N_r \frac{t^r}{r} \in \mathbb{Q}[[t]]$$

Zeta-Funktion von V .

Beispiel. $V = \mathbb{P}^1$. Dann ist

$$N_r = |\mathbb{P}^1(\mathbb{F}_{p^r})| = |(\mathbb{F}_{p^r}^2 \setminus \{0\})/\mathbb{F}_{p^r}^*| = (p^{2r} - 1)/(p^r - 1) = p^r + 1$$

und daher

$$\begin{aligned} Z(\mathbb{P}^1, t) &= \exp \sum_{r=1}^{\infty} \frac{(1 + p^r)t^r}{r} \\ &= \exp \left(\sum_{r=1}^{\infty} \frac{t^r}{r} + \sum_{r=1}^{\infty} \frac{(pt)^r}{r} \right) \\ &= \exp(-\log(1-t) - \log(1-pt)) \\ &= \frac{1}{(1-t)(1-pt)} \end{aligned}$$

Weil rechnete viele weitere Beispiele durch und vermutete dann allgemein:

Theorem 9.13 (Weil-Vermutungen). Sei V glatte projektive Varietät der Dimension d .

(i) (Rationalität) $Z(V, t) \in \mathbb{Q}(t)$.

(ii) $Z(V, t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}}$ mit $P_i(t) \in \mathbb{Z}[t]$ mit konstantem Term 1.

- (iii) Ist V eine Kurve, so ist $\deg P_1 = g(C)$, das Geschlecht. (Allgemein: $\deg P_i = b_i$, die Dimension der i -ten singulären Kohomologie von V/\mathbb{C}).
- (iv) (Funktionalgleichung)
- (v) (Riemannsche Vermutung) Alle Nullstellen von P_i haben den Absolutbetrag $p^{-i/2}$

Wieder haben geometrische Eigenschaften arithmetische Konsequenzen! Weil konnte die Aussagen für Kurven beweisen. (Im Fall von elliptischen Kurven wollen wir das im Seminar sehen.) Er sah auch ein Erklärungsmuster: Es sollte eine rein algebraische definierte Kohomologietheorie geben $V \mapsto H^i(V)$. Dann sollte P_i das charakteristische Polynom des Frobeniushomomorphismus auf H^i sein. Der Beweis der Rationalität wäre eine Art Fixpunktformel für diesen Endomorphismus. Grothendieck gelang die Konstruktion dieser Kohomologietheorie und damit der Beweis aller Aussagen bis auf die Riemannsche Vermutung. Diese wurde von Deligne gezeigt.

In der Vorlesung der nächsten zwei Semester soll dieser Beweis (oder möglichst viel davon) nachvollzogen werden. Themen werden sein:

- (i) Singularitäten, glatte Morphismen und étale Morphismen
- (ii) Varietäten über beliebigen Körpern
- (iii) Garben, Garbenkohomologie
- (iv) Die étale Topologie und étale Kohomologie
- (v) elementare und nicht-elementare Eigenschaften von étaler Kohomologie
- (vi) Rationalität
- (vii) ...

Inhaltsverzeichnis

0	Einleitung	1
1	Grundbegriffe der algebraischen Geometrie	7
2	Noethersche Ringe und Moduln	13
3	Hilbertscher Nullstellensatz	23
4	Topologische Eigenschaften	29
5	Lokale Ringe und Lokalisierung	35
6	Quasi-projektive Varietäten	45
7	Dimensionstheorie	53
8	Schnitttheorie im projektiven Raum	65
9	Ausblick	77