Kommutative Algebra und Einführung in die algebraische Geometrie

Sommersemester 2022

Prof. Dr. Annette Huber-Klawitter

Fassung vom 20. Juli 2022

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

Math. Institut
Ernst-Zermelo-Str.1
79104 Freiburg

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

Kapitel 0

Einleitung

Geometrie beschäftigt sich mit Objekten wie Kreisen, Kugeln und ähnlichem. Die eigentliche Heimat ist die *Differentialgeometrie*. Dort ist der zentrale Begriff der der Mannigfaltigkeit: ein topologischer Raum, der lokal so aussieht wie eine offene Teilmenge des $\mathbb{R}^n$. Man arbeitet dann mit der vollen Kraft der Analysis.

Viele geometrische Objekte (z.B. eben Kreis und Kugel) werden jedoch durch *Polynomgleichungen* beschrieben. Sie sind Objekte der *algebraischen* Geometrie. Die Voraussetzung ist sehr einschränkend, enthält aber viele interessante Beispiele. Historisch behandelte man zuerst den Grundkörper $\mathbb{C}$ und verwendete weiter analytische Methoden. Es gelang dann aber, immer mehr Sätze mit rein algebraischen Methoden zu beweisen. Der Vorteil ist, dass dann auch andere Grundkörper erlaubt werden können oder sogar beliebige Ringe. Mein Arbeitsgebiet, die arithmetische Geometrie, arbeitet vor allem über $\mathbb{Z}$.

In dieser Vorlesung werden wir uns auf Körper einschränken, meist algebraisch abgeschlossene. Es ist nicht falsch an $\mathbb{C}$ zu denken – aber Vorsicht in positiver Charakteristik.

Algebraische Mengen

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 $P = (a_1, \ldots, a_n)$ heißen die a_i Koordinaten von P. Wir interpretieren den Polynomring*

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

als Funktionen

$$\mathbb{A}^n \to k$$
$$(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$$

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

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

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.

Ist der Körper nicht algebraisch abgeschlossen, so hat die Gleichung eventuell gar keine Lösungen. Diese Zusatzkomplikation wollen wir in diesem Semester umgeben, daher die Einschränkung auf algebraisch abgeschlossenes k.

(ii) Sei $n = 2$, $S = X^2 + Y^2 - 1$. Die Menge $V(f)$ 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 Ebene.

(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 $V(S) \subset \mathbb{A}^1_k$ 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 $V(S) = \mathbb{A}^1_k$. □

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, $S \subset k[X_1, \ldots, X_n]$ eine Teilmenge, $V = V(S)$. Dann heißt*

$$\mathcal{O}(V) = k[V] = \{f : V \to k| \text{ es gibt } F \in k[X_1, \ldots, X_n], \\ f(x_1, \ldots, x_n) = F(x_1, \ldots, x_n) \text{ für alle } (x_1, \ldots, x_n) \in V\}$$

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

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

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

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 $(a_1, \ldots, a_n) \in k^d$ 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. □

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 (wenn die Zeit reicht)

(vi) Schnitte von Untervarietäten und Satz von Bézout: Graduierte Ringe, Hilbert-Samuel-Polynome

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

Nötige Vorkenntnisse

Vor allem lineare Algebra 1 und 2. Der Inhalt der Vorlesung Algebra und Zahlentheorie wird *nicht* vorausgesetzt. Ehrlicherweise sollte gesagt sein, dass der Beweis des Hilbertschen Nullstellensatzes ohne diese Vorlesung vermutlich nicht zu verstehen ist. Diesen kann man aber als Blackbox benutzen, so dass es danach wieder weitergeht.
Zur algebraischen Geometrie passt als Ergänzung sehr gut Funktionentheorie, auch wenn in diesem Semester nicht klar werden wird, warum.

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 Master macht vielleicht.

In diesem Sinne:

- 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, Bézout 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 Schnittheorie 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.

- Griffiths, 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. Alle Ringhomomorphismen bilden 1 auf 1 ab.

Bemerkung. Es gibt ein ärgerliches Problem mit der Frage, ob $1 = 0$ erlaubt sein soll. Zur Erinnerung: in einem Körper ist nach Voraussetzung $1 \neq 0$. Ist $0 = 1$, so folgt $a = 1a = 0a = 0$ für alle a, also enthält ein Ring mit $1 = 0$ nur ein einziges Element. Wenn man ihn erlaubt, muss man ständig an den Ausnahmefall denken. Das ist lästig. Andererseits wollen wir gerne, dass die leere Menge auch einen Koordinatenring hat. Für $V(1) = \emptyset \subset \mathbb{A}^n$ setzen wir nämlich

$$\mathcal{O}(\emptyset) = 0.$$

Daher erlauben wir $1 = 0$. Auch der Nullring ist ein Ring mit 1.

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

$$I(V) = \{f \in k[X_1, \ldots, X_n] | f(P) = 0 \textit{ für alle } P \in V\}$$

das Verschwindungsideal von V.

Bemerkung. (i) Falls $V = V(S)$ für $S \subset k[X_1, \ldots, X_n]$, 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 $g \in k[X_1, \ldots, X_n]$ 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 $\phi : A \to B$ ein Ringhomomorphismus. Dann ist* $\mathrm{Ker}(\phi)$ *ein Ideal.*

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

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

□

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

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

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

mit der Addition und Multiplikation von Nebenklassen

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I$$

ein Ring. Die Projektionsabbildung $A \to A/I$ 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 oder Gruppen und wird hier weggelassen.
Interessanter ist die Multiplikation. Sei $a + I = a' + I$

Behauptung. *$ab + I = a'b + I$ für alle $b \in A$*

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. □

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

$$\overline{\varrho} : \mathcal{O}(\mathbb{A}^n)/I(V) \to \mathcal{O}(B) \qquad f + I(V) \mapsto \varrho(f)$$

bijektiv. □

Bemerkung. Das Korollar gilt auch für $V = \emptyset$, denn dann ist $I(V) = \mathcal{O}(\mathbb{A}^n)$ (jedes Polynom verschwindet auf allen – also keinen – Punkten) und $\mathcal{O}(\mathbb{A}^n)/I(V) = 0$.

Im Beweis haben wir bereits den Homomorphiesatz verwendet:

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

$$\overline{\phi} : A/I \to \mathrm{Im}(\phi) \qquad a + I \mapsto \phi(a)$$

ein Ringisomorphismus.

Beweis: Wie für Vektorräume oder Gruppen. □

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.

Man sieht leicht, dass $\langle S \rangle$ selbst ein Ideal ist.

Korollar 1.8. *Sei $S \subset k[X_1, \ldots, X_n]$ 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 $\langle XY \rangle = k[XY](XY)$. Es ist

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

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 $\langle X^2 \rangle = k[X]X^2$, $V = \{0\} \subset \mathbb{A}^1$ 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*

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

Radikal *von I. Ein Ideal heißt* reduziert*, wenn es mit seinem Radikal übereinstimmt.*

Lemma 1.10. *Das Radikal ist ein Ideal.*

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

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

da I ein Ideal. Außderdem

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

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 $y^{n+m-i} \in I$. Jeder Summand ist in I, also auch die Summe. □

Korollar 1.11. *Sei $S \subset k[X_1, \ldots, X_n]$ eine Teilmenge, $V = V(S)$ die zugehörige algebraische Menge. 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 $f(P) = 0$ für alle $P \in V$. □

Hier gilt tatsächlich Gleichheit! Das wird unser erstes großes Ziel sein, der Hilbertsche Nullstellensatz. Er erlaubt uns, zwischen Varietäten und Idealen hin und her zu schalten. Eine einfache Teilaussage können wir bereits festhalten.

Lemma 1.12. *Sei $V \subset \mathbb{A}^n$ algebraische Teilmenge. Dann gilt*

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

Beweis: 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 $V(I(V))$.

□

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 1.13. *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 1.14. *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 abgeschlossener 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 $S_1 S_2 = \{f_1 f_2 | f_1 \in S_1, f_2 \in S_2\}$. 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 endlich 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 1.15. *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.

Kapitel 2

Noethersche Ringe und Moduln

Um algebraische Varietäten zu verstehen, muss man Polynomringe über einem Körper verstehen. Wir beginnen mit einer ganz grundlegenden Eigenschaft.

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 Ideal heißen *Hauptideale*, solche Ringe heißen *Hauptidealringe*. Hauptidealringe sind noethersch.

(iii) $A = K[X]$ (K ein Körper) ist ebenfalls ein Hauptidealring. (Übungsaufgabe)

Lemma 2.2. *Sei $f : A \to B$ 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. □

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

$$A \times M \to M$$

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

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

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

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

(iv) $1x = x$.

Seien M,N Moduln. Eine Abbildung $f : M \to N$ 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 aus der linearen Algebra.

(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. Jeder Modulhomorphismus ist nach Definition ein Gruppenhomomorphismus.

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

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

Dies ist die einzige mögliche Modulstruktur. Gruppenhomomorphismen sind automatisch linear für die so definierte Skalarmultiplikation. □

Man sieht an der Beispielrechung, 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 $\phi : V \to V$.

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

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

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

Man überprüft leicht die Modulaxiome. □

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 $M \times A \to M$, 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 Rechtsidealn. 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 lineare Algebra definiert. Ein Modul heißt *endlich erzeugt*, wenn er ein endliches Erzeugendensystem hat.

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

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 $\{(1,0),(0,1)\}$.

Wie in der linearen Algebra sind Kern und Bild eine 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)**.** *(i) Sei $f : M \to N$ ein A-Modulhomomorphismus. Dann ist die induzierte Abbildung*

$$\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$$

ein Isomorphismus von A-Moduln.

(ii) Sind $N, N' \subset M$ Untermoduldn, so ist

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

ein kanonischer Isomorphismus.

(iii) 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 Ausagen 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

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

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

$$\overline{f} : N'/N' \cap N \to \operatorname{Im}(f)$$

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. □

Noethersche Moduln

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

$$M_1 \subset M_2 \subset \cdots \subset M$$

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 $x_1, x_2, \cdots \in N$ 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

$$N = \langle x_1, \dots, x_m \rangle \subset N_k \subset N_{k'} \subset N$$

also Gleichheit für alle $k' \geq k$.
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 nothersch als A-Modul. Ebenso folgt die Umkehrung. □

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*

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

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

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

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

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

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

Definition 2.9. *Ein Diagram von A-Moduln*

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

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

Lemma 2.10. *Sei A ein Ring,*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

eine kurze exakte Sequenz von A-Moduln. 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 $\pi : M_2 \to M_3$ 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)

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

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 Sitatution

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

Wir wollen zeigen, dass $X_i \to X_{i+1}$ 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. □

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

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

einen surjektiven Modulhomomorphismus. Nach Lemma 2.10 ist M noethersch. □

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 Algorithmuses (also Polynomdivision) gezeigt. Dies müssen wir variieren, da wir durch Koeffizienten nicht dividieren können. Daher:
Für jedes $n \geq 0$ sei $I_n \subset I \subset A[X]$ die Menge der Polynome in I vom Grad kleiner gleich n. Dies ist ein A-Modul. Sei

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

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 d so, dass $J_n = J_d$ 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 $A \to B$ 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*

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

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

Mit anderen Worten, es gibt einen surjektiven Ringhomomorphismus

$$A[X_1, \ldots, X_n] \to B \qquad X_i \mapsto b_i$$

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

$$I(V) = \langle f_1, \ldots, f_m \rangle$$

und offensichtlich

$$V \overset{1.12}{=} V(I(V)) = V(f_1, \ldots, f_m) = \bigcap_{i=1}^{m} V(f_i)$$

□

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 und Anwendungen

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

$$V : \Big\{ S \subset k[X_1, \ldots, X_n] \Big\} \to \Big\{ V(S) \subset \mathbb{A}^n \Big\}$$

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

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

ordnet jeder Teilmenge das Verschwindungsideal zu. Wir hatten bereits überprüft (Lemma 1.12) dass

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

für alle algebraischen Mengen.
Wir haben gesehen, dass nur reduzierte Ideale auftauchen, denn wenn $f^n \in I(V)$ für ein $f \in \mathcal{O}(\mathbb{A}^n)$, $n \in \mathbb{N}$, so ist $f \in I(V)$.
Ziel ist zu verstehen:

Theorem 3.1 (Hilbertscher Nullstellensatz)**.** *Sei k algebraisch abgeschlossener Körper. Für jede Teilmenge $S \subset k[X_1, \ldots, X_n]$ gilt*

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

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

Dies bedeutet auch $I(V(I)) = I$ für alle reduzierten Ideale I.
Den vollen Beweis verschieben wir in ein späteres Kapitel. Wir diskutieren jedoch schon jetzt eine wesentliche Reduktion auf einen Spezialfall, nämlich den der maximalen Ideale.

Definition 3.2. *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. $I \neq A$ und 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 $I(P) = \{f \in \mathcal{O}(\mathbb{A}^n) | f(P) = 0\}$ 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 3.3. *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 $\pi : A \to A/I$. Die Bedingung $I \neq A$ ist äquivalent dazu, dass $0 \neq 1$ in A/I. Dies setzen wir ab jetzt voraus.
Sei zunächst I maximal, $\overline{f} = f + I \in A/I$ eine Restklasse ungleich 0. Wir betrachten

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

Da I maximal ist, gilt entweder $I = \pi^{-1}(\langle \overline{f} \rangle)$ oder $\pi^{-1}\langle \overline{f} \rangle = A$. Im ersten Fall folgt $f \in \pi^{-1}\langle \overline{f} \rangle \subset I \Rightarrow \overline{f} = 0$, d.h. wir sind im zweiten Fall. Dann gibt es ein $g \in A$ mit $gf = 1$. Es folgt $\pi(g)\pi(f) = \pi(g)\overline{f} = 1$. 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 $J = \pi^{-1}\pi(J) = \pi^{-1}0 = I$) oder $\pi(J) = A/I$ (also $J = A$). □

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 $P = (a_1, \ldots, a_n) \in k^n$, so liegen die Funktionen $X_i - a_i$ für $i = 1, \ldots, n$ in $I(P)$. Offensichtlich gilt sogar

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

Theorem 3.4 (Schwacher Nullstellensatz)**.** *Sei k algebraisch abgeschlossen und $A = \mathcal{O}(\mathbb{A}^n)$. Dann sind alle maximalen Ideale von der Form*

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

Mit anderen Worten: Alle Funktionen des maximalen Ideals haben eine gemeinsame Nullstelle, nämlich $P = (a_1, \ldots, a_n)$.

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.

Den Beweis von Theorem 3.4 verschieben wir in das Kapitel zur Dimensionstheorie. Aber:

Beweis von Theorem 3.1: Sei k algebraisch abgeschlossen, $J \subset k[X_1, \ldots, X_n]$ ein Ideal.

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

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

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

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

Unterbehauptung. *J' ist einem maximalen Ideal J'_M enthalten.*

Wenn J' nicht maximal ist, so ist es echt in einem größeren enthalten, das nicht der ganze Ring ist. Ist dieses nicht maximal, so gibt es ein echt größeres, etc. Da der Ring noethersch ist, endet dieser Prozess.
Nach dem schwachen Nullstellensatz, Theorem 3.4, hat dieses maximale Ideal J'_M eine gemeinsame Nullstelle $P' = (a_0, \ldots, a_n)$, die dann auch gemeinsame Nullstelle aller Elemente von J' ist. Insbesondere ist $P = (a_1, \ldots, a_n)$ gemeinsame Nullstelle von $f_1, \ldots, f_m$, 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 $J' = k[X_1, \ldots, X_n]$. Also gibt es $h_0, \ldots, h_m \in k[X_0, \ldots, X_n]$ mit

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

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, so dass die Vorfaktoren der f_i Elemente von $k[X_1, \ldots, X_n]$ werden. Dies ergibt

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

□

Irreduzible Mengen

Wir benutzen nun den Nullstellensatz, um die topologischen Eigenschaften einer algebraischen Menge besser zu verstehen.

Definition 3.5. *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) $V(X_1X_2) = V(X_1) \cup V(X_2) \subset \mathbb{A}^2$ ist reduzibel.

Da die Zariski-Topologie sich durch Ideale beschreiben lässt, muss auch diese Eigenschaft eine Charakterisierung in Termen des Ideals haben. Offensichtliches Problem sind Funktionen wie $X_1, X_2 \in I(V(X_1X_2))$.

Definition 3.6. *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 3.7. *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. Sei $V(J) = Y_1 \cup Y_2$. 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 $f_1 f_1 \in I(Y_1) \cap I(Y_2) = J$. Dies ist ein Primideal, also $f_1 \in J$ oder $f_2 \in J$. Dies ist ein Widerspruch zur Wahl der f_i. Es gilt also ohne Einschränkung $I(Y) = J = I(Y_1)$. Wegen $Y = V(I(Y))) = V(I(Y_1)) = Y_1$ (Lemma 1.12) folgt $Y = Y_1$. Damit ist $Y = V(J)$ irreduzibel. □

Bemerkung. Wir haben also Bijektionen

$$\{\text{reduzierte Ideale}\} \leftrightarrow \{\text{affine Varietäten}\}$$
$$\{\text{Primideale}\} \leftrightarrow \{\text{irreduzible affine Varietäten}\}$$
$$\{\text{maximale Ideale}\} \leftrightarrow \{\text{Punkte}\}$$

Lemma 3.8. *Sei A ein Ring, $I \subset A$ ein Ideal. 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 $b = 0$. Außerdem verlangen wir $0 \neq 1$ in A.

Beweis: Sei I Primideal. Wegen $I \neq A$ ist $0 \neq 1$ im Ring A/I. Sei $\overline{a} = a + I, \overline{b} = b + I \in A/I$ mit $\overline{a}\overline{b} = 0$. Dann gilt $ab + I = 0 + I \Leftrightarrow ab \in I$. Da I Primideal ist, folgt $a \in I$ oder $b \in$I, bzw. $\overline{a} = 0$ oder $\overline{b} = 0$. Die Umkehrung geht genauso. □

Korollar 3.9. *Maximale Ideale sind stets Primideale.*

Beweis: Körper sind nullteilerfrei. □

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

Definition 3.10. *Ein topologischer Raum heißt* noethersch*, wenn jede absteigende Kette*

$$Y_1 \supset Y_2 \supset \ldots$$

von abgeschlossenen Teilmengen stabil wird.

Beispiel. Affine Varietäten sind noethersch, denn Ketten von Varietäten entsprechen nach dem Hilbertschen Nullstellensatz bijektiv Ketten von reduzierten Idealen.

Lemma 3.11. *Sei Y noetherscher topologischer Raum und $X \subset Y$ offen. Dann ist X noetherscher topologischer Raum.*

Beweis: Wir betrachten eine Folge

$$X_1 \supset X_2 \supset \ldots$$

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

$$\overline{X}_1 \supset \overline{X}_2 \supset$$

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

Satz 3.12. *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. □

Definition 3.13. *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 3.14 (Zerlegung in irreduzible Komponenten)**.** *Sei Y eine affine Varietät. Dann hat Y endlich viele irreduzible Komponenten Y_i für $i = 1, \ldots, n$ und es gilt*

$$Y = Y_1 \cup \cdots \cup Y_n$$

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

Beweis: Sei $Y = Y_1 \cup \cdots \cup Y_m$ die Zerlegung aus dem Satz. Wir setzen weiter voraus, dass die Zerlegung minimal gewählt ist, d.h. wir können keine der irreduziblen Mengen weglassen.

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

$$Y' = \bigcup_{i=1}^{m} Y_i'$$

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

Behauptung. *$Y_1, \ldots, Y_n$ sind irreduzible Komponenten.*

Wir betrachten ohne Einschränkung Y_1. Sei $Y_1 \subset Y' \subset Y$ mit irreduziblem Y'. Dann gilt $Y' \subset Y_i$ für ein i. Falls $i \neq 1$, so ist Y_1 in der Zerlegung überflüssig. Das wäre ein Widerspruch zur Minimalität. Also ist $Y' \subset Y_1 \subset Y'$. Das macht Y_1 zu einerirreduziblen Komponente.

Behauptung. *Jede irreduzible Komponente ist ein Y_i mit $i \leq m$.*

Wir wenden die erste Behauptung auf eine irreduzible Komponente Y' an. Es folgt $Y' = Y_i$. □

Definition 3.15. *Sei X ein topologischer Raum. Die* Dimension *von X ist*

$$\dim X = \sup\{n \in \mathbb{N}_0 |\ \textit{es gibt eine Kette } X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n, X_i \subset X \textit{ irreduzibel, abgeschlossen}\}$$

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

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

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

Lemma 3.16. *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 nach dem Hilbertschen Nullstellensatz. □

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 Teilmenge. Dann ist $\dim Y \leq \dim W$, 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

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

Tatsächlich gilt $\dim \mathbb{A}^n = n$, aber das wird 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, aber das werden wir nicht beweisen.

Offene Überdeckungen

Definition 3.17. *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 $f \in k[X_1, \ldots, X_n]$ definiert. In der Definition ist $f \in k[X_1, \ldots, X_n]/I(V)$. Das ist aber ein harmloser Unterschied. Es hat ein Urbild $\tilde{f} \in k[X_1, \ldots, X_n]$. Es ist dann

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

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

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

Lemma 3.18. *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 3.19. *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 $\{U_{i_1}, \ldots, U_{i_n}\}$, d.h. endliche viele $i_1, \ldots, i_n \in I$ 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 Quasikompaktheit.

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

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

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

$$Z_1 \supsetneq Z_2 \supsetneq \ldots$$

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

Korollar 3.20. *Alle quasi-affinen Varietäten sind quasi-kompakt.*

Beweis: Affine Varietäten sind noethersch. Nach Lemma 3.11 sind dann auch quasi-affine noethersch. Nach Lemma 3.19 sind sie quasi-kompakt. □

Kapitel 4

Lokale Ringe und Lokalisierung

Der irreduzible Fall

Definition 4.1. *Sei A ein nullteilerfreier Ring. Dann heißt*

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

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

$$(a, s) \sim (a', s') \Leftrightarrow as' = a's$$

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 4.2. *Sei V eine irreduzible affine Varietät. Dann heißt*

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

Funktionenkörper von V. *Die Elemente von $k(V)$ heißen* rationale Funktionen auf V. *Ist V quasi-affin mit Zariski-Abschluss $\overline{V}$ (und irreduzibel), so setzen wir auch*

$$k(V) = k(\overline{V}).$$

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*

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

heißt lokaler Ring von V in P.

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

Definition 4.3. *Ein Ring heißt* lokal*, wenn er genau ein maximales Ideal hat.*

Lemma 4.4. *Sei V irreduzible affine Varietät, $P \in V$. Dann ist $\mathcal{O}_P$ lokal mit maximalem Ideal $m_P = \{f \in \mathcal{O}_P | f(P) = 0\}$.*

Beweis: Wir betrachten die Auswertungfunktion

$$\mathcal{O}_P \to k, \qquad f \mapsto f(P)$$

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. □

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

Lemma 4.5. *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 4.6. *Sei $V \subset \mathbb{A}^n$ quasi-affin und irreduzibel. Dann setzen wir*

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

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 wir verschieben den Beweis, bis wir uns von der Irreduzibiltätsvoraussetzung lösen können. Fürs Erste unterscheiden wir $k[V]$ und $\mathcal{O}(V)$.

Lemma 4.7. *Sei V eine irreduzible affine Varietät, $f \in k(V)$ Dann ist*

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

offen in V.

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

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

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

Korollar 4.8. *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 allgemeiner 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 Multipliaktionsregeln:

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

Dafür muss man Nenner multiplizieren können.

Definition 4.9. *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 4.10. *Sei A ein Ring, $S \subset A$ multiplikative Teilmenge, 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

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

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 zusätzliche Erweiterung um ein weiteres t zulassen.

Lemma 4.11. *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 bespielhaft 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

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

Einsetzen ergibt die Behauptung. □

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 $A \to S^{-1}A$ nicht injektiv, denn $\frac{s}{1} = \frac{0}{1}$. (Übungsaufgabe)

Ist $f : M \to N$ 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. Wir schreiben $S^{-1}f$ oder auch abkürzend f für diesen induzierten Morphismus.

Lemma 4.12. *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

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

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

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

Dies bedeutet $\operatorname{Im} S^{-1}f \subset \operatorname{Ker} S^{-1}g$.
Sei nun $\frac{m_2}{s} \in S^{-1}M_2$, das im Kern von $S^{-1}g$ liegt, also

$$\frac{g(m_2)}{s} = \frac{0}{1} \Leftrightarrow t \cdot 1 \cdot g(m_2) = ts \cdot 0 \text{ für ein } t \in S.$$

Wegen der A-Linearität von g folgt

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

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

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

□

Korollar 4.13. *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 $\frac{1}{1} \in S^{-1}I$, d.h. von der Form $\frac{s}{s}$ mit $s \in S$ (Nenner) und $s \in I$ (Zähler). □

Lemma 4.14. *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 Ideal 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 4.15. *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 $I = \{a \in A | am = 0\}$. 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 $t \in S_{\mathfrak{m}}$ gibt mit $tm = 0$. Dann ist $t \in I \subset \mathfrak{m}$. Dies ist ein Widerspruch zu $t \in S_{\mathfrak{m}} = A \setminus \mathfrak{m}$. □

Lokale Ringe von Varietäten

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

Definition 4.16. *Sei V eine affine Varietät, $P \in V$ mit zugehörigem maximalen Ideal $m_p \in k[V]$. Dann heißt*

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

lokaler Ring *von V in P.*

Dies passt zu unserer Definition im irreduziblen Fall.
Wir wollen die Elemente von $\mathcal{O}_P$ als Funktionen auffassen. Die Element von $\mathcal{O}_P$ haben die Form f/g mit $f, g \in k[V]$, $g(P) \neq 0$. Der Bruch definiert also eine Abbildung

$$\frac{f}{g} : U_g \to k.$$

Die Repräsentation als Bruch ist aber nicht eindeutig. Angenommen $f/g = f'/g' \in \mathcal{O}_P$. Diese definieren also Abbildungen auf U_g und $U_{g'}$. Wie hängen die Abbildungen zusammen? Nach Definition gibt es $h \in k[V]$ mit $h(P) \neq 0$, so dass

$$hg'f = hgf' \in k[V]$$

Die beiden Seiten sind also gleich als Abbildungen $V \to k$. Hieraus folgt auf $U_h \cap U_g \cap U_{g'} = U_{hgg'}$

$$\frac{f}{g} = \frac{hg'f}{hgg'} = \frac{hgf'}{hgg'} = \frac{f'}{g'} : U_{hgg'} \to k.$$

Definition 4.17. *Sei V eine affine Varietät, $P \in V$. Ein* Funktionenkeim *in P ist eine Äquivalenzklasse von Paaren (U, α), wobei $U \subset V$ offen, $\alpha : U \to k$ eine Abbildung und*

$$(U, \alpha) \sim (U', \alpha')$$

genau dann, wenne es eine offene Teilmenge $W \subset U \cap U'$ gibt mit $P \in W$ und $\alpha|_W = \alpha'|_W$. Wir schreiben α_P für die Klasse von (U, α).

Da jede offene Umgebung von U eine standardoffene Menge enthält, genügt es standardoffene U, U' und W zu betrachten. Wir fassen unsere Vorüberlegungen zusammen:

Lemma 4.18. *Sei V eine affine Varietät, $P \in V$. Dann definiert jedes Element von $\mathcal{O}_P$ einen eindeutigen Funktionenkeim in P.*

Definition 4.19. *Sei V eine affine Varietät, $U \subset V$ offen. Eine Abbildung $\alpha : U \to k$ heißt* algebraisch*, wenn der Keim von (U, α) für jeden Punkt $P \in U$ in $\mathcal{O}_P$ liegt. Es sei $\mathcal{O}(U)$ der Ring der algebraischen Funktionen.*

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

Satz 4.20. *Sei V affine Varietät, $f \in k[V]$ nicht nilpotent. Dann ist die natürliche Abbildung*

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

ein bijektiver Ringhomomorphismus, insbesondere

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

Beweis: Wir erledigen zunächst die Injektivität. Sei $a/f^n \in k[V]_f$ gleich 0 aufgefasst als Funktion in $\mathcal{O}(U_f)$, d.h. $a(Q)/f(Q)^n = 0$ für alle $Q \in U_f$. (Dies ist wohldefiniert, da $f(Q) \neq 0$ in ganz U_f.) Es folgt $a(Q) = 0$ 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 $0 = \sqrt{\langle af \rangle} \Rightarrow af = 0$. Hieraus folgt in $k[V]_f$ die Gleichheit

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

Das ist Injektivität.

Sei $\phi : U_f \to k$ algebraisch. Für jedes $P \in U$ ist der Keim ϕ_P von ϕ ein Element $\phi_P \in \mathcal{O}_P$. Dieses wird repräsentiert durch einen Bruch a_P/f_P, dessen Keim mit ϕ_P übereinstimmt. Ohne Einschränkung gilt dies Gleichheit auf einer standardoffenen Umgebung von P, nach Erweitern des Bruch (d.h. Ersetzen von f_p durch ein Vielfaches) sogar auf U_{f_P}. Da U_f quasi-kompakt ist, genügen endlich viele der U_{f_P}, um ganz U_f zu überdecken. Damit sind wir in der folgenden Situation:

$U_f = \bigcup_{i=1}^N U_{f_i}$ eine standardoffene Überdeckung, so dass $\phi_i = \phi|_{U_{f_i}}$ von der Form a_i/f_i. Man beachte, dass $U_{f_i} \cap U_{f_j} = U_{f_i f_j}$. Für $i \neq j$ gilt dann

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

als Funktionen auf $U_{f_i f_j}$. Wegen der Injektivität gilt die Gleichheit dann bereits in $k[V]_{f_i f_j}$. Wir müssen also zeigen:

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

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

exakt, wobei die zweite Abbildung

$$(a_i/f_i)_i \mapsto (a_j/f_j - a_i/f_i)_{i,j}$$

ist.

Unser Element liegt also im Kern der zweiten Abbildung. 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 $\phi_i = a_i/f_i$ in U_{f_i} und außerdem

$$a_i f_j = a_j f_i$$

für alle i, j.
Nach Voraussetzung gilt $\bigcup_{i=1}^N U_{f_i} = U_f$. Dies impliziert $\bigcap_{i=1}^n V(f_i) \subset V(f)$, also nach dem Hilbertschen Nullstellensatz $f \in \sqrt{\langle f_1, \ldots, f_N \rangle}$. 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 ϕ.*

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} □

Bemerkung. Ist V irreduzibel, so erhalten wir also Definition 4.2 für $\mathcal{O}(U)$ zurück. Dann stimmen auch Definition 4.6 und die allgemeinere Definition 4.19 für algebraische Funktionen überein.

Kapitel 5

Die Kategorie der quasi-projektiven Varietäten

Definition 5.1. *Seien $V \subset \mathbb{A}^n$ und $W \subset \mathbb{A}^m$ affine Varietäten. Eine Abbildung*

$$f : V \to W$$

heißt Morphismus *oder* reguläre Abbildung*, wenn es Polynome $F_1, \ldots, F_m \in k[X_1, \ldots, X_n]$ gibt, so dass*

$$f(x_1, \ldots, x_n) = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)) \qquad \text{für alle } (x_1, \ldots, x_n) \in V.$$

Sie heißt Isomorphismus*, wenn sie bijektiv ist und die Umkehrabbildung ebenfalls ein Morphismus ist.*

Wir haben also automatisch ein kommutatives Diagramm

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{(F_1,\ldots,F_m)} & \mathbb{A}^m \\ \uparrow & & \uparrow \\ V & \xrightarrow{f} & W \end{array}$$

Beispiel. (i) Die Inklusion $V \subset \mathbb{A}^n$ ist ein Morphismus. Die Polynome sind $F_i = X_i$. Das obige Diagramm ist ein Diagramm von Morphismen.

(ii) Die Projektionsabbildungen $p_i : \mathbb{A}^n \to \mathbb{A}^1$, $(x_1, \ldots, x_n) \mapsto x_i$ sind Morphismen. Das Polynom ist X_i.

(iii) Sei V eine affine Varietät. Ein Morphisms $f : V \to \mathbb{A}^1$ ist nichts anderes als eine algebraische Funktion $f \in \mathcal{O}(V)$.

Nicht jeder bijektive Morphismus ist ein Isomorphismus!

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

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

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

Lemma 5.2. *Kompositionen von Morphismen sind Morphismen.*

Beweis: Das Einsetzen von Polynomen in Polynome liefert Polynome. □

Lemma 5.3. *Morphismen sind stetig, d.h. Urbilder von offenen Mengen sind offen.*

Beweis: Es ist äquivalent, zu zeigen, dass Urbilder abgeschlossener Mengen abgeschlossen sind. Da affine Varietäten die Teilraumtopologie tragen, genügt es, Abbildungen $(F_1, \ldots, F_m) : \mathbb{A}^n \to \mathbb{A}^m$ zu betrachten. Jede abgeschlossene Teilmenge von $\mathbb{A}^m$ ist Schnitt von Hyperflächen, daher genügt es $X = V(G)$ zu betrachten für ein $G \in k[X_1, \ldots, X_m]$. Das Urbild ist

$$\{(x_1, \ldots, x_n) | (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_m)) \in V(G)\} = \\ G(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_m)) = 0\}.$$

Dies ist eine algebraische Teilmenge. □

Quasi-projektive Varitäten

Wir verallgemeinern den Varietätenbegriff.

Definition 5.4. *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 $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ falls es $\lambda \in K^*$ gibt mit $x_i = \lambda y_i$ für $0 \leq i \leq n$. Wir schreiben $[x_0 : \cdots : x_n]$ für die Äquivalenzklasse von $(x_0, \ldots, x_n)$. Wir nennen $x_0, \ldots, x_n$ homogene Koordinaten *auf $\mathbb{P}^n(K)$.*
Für $i = 0, \ldots, n$ heißt die Teilmenge

$$U_i = \{[x_0 : \cdots : x_n] | x_i \neq 0\}$$

i-te standardaffine Karte.

Lemma 5.5. *(i) Auf U_i sind die Funktionen $y_j = x_j/x_i$ wohldefiniert und induzieren eine Bijektion*

$$\phi_i : U_i \to K^n \qquad [x_0 : \cdots : x_n] \mapsto (y_0, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n)$$

(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 Respräsentanten. Die Abbildung

$$\psi_i : K^n \to \mathbb{P}^n(K) \qquad (a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \mapsto [a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \ldots, a_n]$$

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. □

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

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

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 5.6. *Ein Polynom $P \in K[X_0, \ldots, X_n]$ heißt* homogen vom Grad d, *wenn es von der Form*

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

ist.

Lemma 5.7. *Sei f ein homogenes Polynom vom Grad d, $x = (x_0, \ldots, x_n) \in K^{n+1}$, $\lambda \in K^*$. 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 5.8. *Sei k ein algebraisch abgeschlossener Körper, $S \subset k[X_0, \ldots, X_n]$ eine Menge von Polynomen. Dann heißt*

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

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

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

Verschwindungsideal von V *und*

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

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

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

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

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

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 5.9. *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. □

Definition 5.10. *Sei $\mathbb{P}^n_k$ der projektive Raum $\mathbb{P}^n(k)$ zusammen mit seiner Topologie. Eine* projektive Varietät *ist eine projektive algbraische Menge zusammen mit ihrer Topologie. Eine* quasi-projektive Varietät *ist eine offene Teilmenge einer projektiven Varietät mit der induzierten Topologie.*

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

Lemma 5.11. *Die Kartenabbildung $\phi_i : U_i \to \mathbb{A}^n$ ist ein Homöomorphismus, d.h. bijektiv, stetig und offen.*

Beweis: Ohne Einschränkung betrachten wir $i = 0$. Die Bijektivität haben wir schon überprüft.
Wir zeigen, dass ϕ_0 eine Bijektion der Mengen von abgeschlossenen Teilmengen von U_0 und $\mathbb{A}^n$ induziert.
Sei $F \in k[X_0, \ldots, X_n]$ ein homogenes Polynom, $V = V(F) \subset \mathbb{P}^n_k$. Dann gilt

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

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

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

Dann ist

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

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

Beispiel. Sei $n = 2$, $f = X^2 + 2XY + Y + 2$, $V(f) \subset \mathbb{A}^2$. Dies ist ein Polynom vom Grad $d = 2$. Seine Homogenisierung ist

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

d.h. alle Monome von f werden mit Z-Faktoren aufgefüllt zum Grad 2.

Bemerkung. Die beiden Operationen "Einsetzen von $X_0 = 1$" und "Homogenisieren eines Polymons in den Variablen $X_1, \ldots, X_n$" definieren eine Bijektion zwischen homogenen Polynomen in $X_0, \ldots, X_n$, die nicht durch X_0 teilbar sind und Elementen von $k[X_1, \ldots, X_n]$. Geometrisch entspricht dem eine Bijektion zwischen algebraischen Teilmengen des $\mathbb{P}^n_k$ und denjenigen algebraischen Teilmengen des $\mathbb{A}^{n+1}$, die mit einem Punkt auch die Nullpunksgerade durch diesen Punkt enthalten.

Wir können also den projektiven Raum (und alle projektiven Varietäten) mit affinen Karten überdecken. Der Schnitt $U_i \cap U_j = \{[x_0 : \cdots : x_n] | x_i, x_j \neq 0\}$ 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

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

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

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

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

Bemerkung. Quasi-affine Varietäten sind quasi-projektiv.

Lokale Ringe und algebraische Funktionen

Sei V eine projektive Varietät, $F, G \in S[V]$ homogene Elemente vom selben Grad d. Dann ist für $P = [x_0 : \cdots : x_n]$ der Funktionswert

$$\frac{F}{G}(P) = \frac{F(x_0, \ldots, x_n)}{G(x_0, \ldots, x_n)}$$

unabhängig von der Wahl der homogenen Koordinate und wohldefiniert, falls $P \notin V(g)$.

Definition 5.12. *Sei V eine projektive Varietät mit homogenem Koordinatenring $S[V]$. Sei $P \in V$. Der* lokale Ring von V in P *ist definiert als*

$$\mathcal{O}_P = \left\{ \frac{F}{G} | F, G \in S[V] \text{ homogen vom selben Grad }, G(P) \neq 0 \right\}$$

Ist V irreduzibel, so ist der Funktionenkörper von V *definiert als*

$$k(V) = \left\{ \frac{F}{G} | F, G \in S[V] \text{ homogen vom selben Grad }, G \neq 0 \right\}$$

Lemma 5.13. *Sei $V \subset \mathbb{P}_k^n$ eine projektive Varietät, $P \in V$. Sei $U_i \subset \mathbb{P}_k^n$ eine standardaffine Karte mit $P \in U_i$. Dann gilt*

$$\mathcal{O}_{V,P} \cong \mathcal{O}_{V \cap U_i, P}$$

wobei die Abbildung gegeben ist durch Einsetzen $X_i = 1$. Insbesondere ist $\mathcal{O}_{V,P}$ lokal.
Ist V irreduzibel, so gilt

$$k(V) \cong k(V \cap U_i) \ .$$

Insbesondere ist $k(V)$ ein Körper.

Beweis: Sei ohne Einschränkung $i = 0$ und schreiben abkürzend $V_0 = U_0 \cap V$ für die affine Varietät.
Wir zeigen zuerst, dass die Abbildung surjektiv ist. Sei $f/g \in \mathcal{O}_{V_0,P}$, d.h. $f, g \in k[V_0]$ mit $g(P) \neq 0$. Seien $\tilde{f}, \tilde{g} \in k[X_1, \ldots, X_n]$ Repräsentaten vom Grad d_f und d_g. Seien weiter $\tilde{F}, \tilde{G} \in k[X_0, \ldots, X_n]$ deren Homogenisierungen und $F, G \in S[V]$ die Nebenklassen. Dann ist

$$\frac{X_0^{d_g} F}{X_0^{d_f} G}$$

das gesuchte Urbild.
Wir behandeln nun die Injektivität. Sei $F/G \in \mathcal{O}_{V,P}$, so dass

$$F(1, X_1, \ldots, X_n)/G(1, X_1, \ldots, X_n) = 0$$

in einer Umgebung U von P. Wir schreiben $f = F(1, X_1, \ldots, X_n)$ und $g = G(1, X_1, \ldots, X_n)$. Ohne Einschränkung ist $U = U_h$ mit $h \in k[V_0]$, $h(P) \neq 0$. Sei H die Homogenisierung von h. Wir ersetzen G und H durch HG, also ohne Einschränkung $H = G$ und f/g verschwindet auf U_g. Aus der Strukturtheorie der algebraischen Funktionen im affinen Fall wissen wir, dass es dann eine Potenz von g gibt mit $g^a f = 0$. Wir betrachten das homogene Polynom

$$G^a F X_0 \in S[V] \ .$$

Es verschwindet in $V(G) \cup V(X_0)$ und in U_g, also auf ganz V. Mit dem Hilbertschen Nullstellensatz folgt

$$G^a F X_0 = 0 \ .$$

Es folgt also

$$\frac{F}{G} = \frac{X_0 G^a F}{X_0 G^{a+1}} = 0 \ .$$

Sei nun V irreduzibel. Nach Voraussetzung ist $P \in V_0$, also $V_0 \neq \emptyset$. Da V nun irreduzibel ist, ist V_0 dicht in V. Wir zeigen zuerst, dass die Abbildung wohldefiniert ist. Sei $F/G \in k(V)$ mit Bild f/g. Angenommen, $g = 0$ in $k[V]$. Dann verschwindet G auf V_0 und (da V_0 dicht ist) auch auf V, d.h. $G = 0$. Dies ist ein Widerspruch.
Die Surjektivität folgt wir im Fall von $\mathcal{O}_P$. Wir behandeln nun die Injektivität. Sei $F/G \in k(V)$ mit Bild $f/g \in k(V_0)$. Dann gibt es $h \in k[V_0] \setminus \{0\}$ mit $fh = 0$. Sei H die Homogenisierung von h. Dann ist $H \neq 0$ in $S[V]$. Es folgt $HF = 0$, und daher $F/G = 0$. □

Morphismen von quasi-projektiven Varietäten

Definition 5.14. *Seien V, W quasi-projektive Varietäten. Eine Abbildung*

$$\alpha : V \to k$$

heißt algebraisch *in $P \in V$, wenn sie in $\mathcal{O}_P$ liegt, d.h. wenn es homogene $F, G \in S[\overline{V}]$ vom selben Grad gibt mit $G(P) \neq 0$ und $\alpha = F/G$ in einer offenen Umgebung von P.*
Ein Morphismus von Varietäten *ist eine stetige Abbildung*

$$\Phi : V \to W$$

so dass für alle $P \in V$ gilt $\Phi^* \mathcal{O}_{W,\Phi(P)} \subset \mathcal{O}_{V,P}$. Mit anderen Worten: Für alle $P \in V$ und für jede Funktion $\alpha : W \to k$, die algebraisch in $\Phi(P)$ ist, ist die Komposition

$$\alpha \circ \Phi : V \to W \to k$$

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

Bemerkung. In der Literatur findet man oft die Bezeichnung *regulär*, wo wir algebraisch sagen.

Quasi-projektive Varietäten bilden eine Kategorie:

Satz 5.15. *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 $\Phi : X \to Y$ und $\Psi : Y \to Z$ Morphismen. Dann ist $\Psi \circ \Phi$ stetig. Sei $P \in X$, $\alpha : Z \to k$ regulär in $\Psi(\Phi(P))$. Dann ist $\alpha\Psi$ regulär in $\Phi(P)$, da Ψ ein Morphismus ist. Dann ist wiederum $\alpha\Psi\Phi$ regulär in P, da Φ ein Morphismus ist. Nach Definition ist $\Psi\Phi$ ein Morphismus. □

Wir wollen nun besser verstehen, welche Beispiele von Morphismen es gibt. Wir vergleichen mit unserer Definition im affinen Fall.

Lemma 5.16. *Sei V affin, $U_f \subset V$ standardoffen. Sei $\alpha \in \mathcal{O}(U_f)$. Dann ist α stetig als Morphismus $\alpha : U_f \to \mathbb{A}^1$. Es ist*

$$\mathcal{O}(U_f) = \mathrm{Mor}(U_f, \mathbb{A}^1)$$

Beweis: Sei $\alpha = g/f^n$ mit $g \in \mathcal{O}(V)$. Wir müssen zeigen, dass Urbilder abgeschlossener Mengen abgeschlossen sind. Dabei genügt es einelementige Mengen $\{a\} \subset \mathbb{A}^1$ zu betrachten. Das Urbild von a besteht aus den Punkten mit

$$\alpha(P) = \frac{g(P)}{f(P)^n} = a \ ,$$

also den Nullstellen von $g - af^n$. Dies ist abgeschlossen.
Sei nun α ein Morphismus. Wir gehen die Definition durch. Jeder Punkt $P \in U_f$ hat eine standardoffene Umgebung U_P, so dass $\alpha|_{U_P} \in \mathcal{O}(U_P)$. D.h. α ist lokal algebraisch. Nach Definition liegt $\alpha \in \mathcal{O}(U_f)$.
Umgekehrt haben wir die Stetigkeit von $\alpha \in k[V]_f$ gezeigt. Dies ist dann nach Definition ein Morphismus. □

Satz 5.17. *Seien $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ affine Varietäten. Eine Abbildung $\Phi : V \to W$ ist genau dann ein Morphismus im Sinne von Definition 5.14, wenn sie ein Morphismus im Sinne von Definition 5.1 ist.*

Beweis: Sei $\Phi : V \to W$ ein Morphismus im Sinne der ursprünglichen Definition. Stetigkeit haben wir bereits etabiert. Sei $g \in \mathcal{O}_{\Phi(P)}$, also algebraisch in $\Phi(P)$. Dann ist $g \circ \Phi$ algebraisch in P, da das Einsetzen von Polynomen in Polynome wieder Polynome ergibt. Damit ist Φ ein Beispiel für einen Morphismus im Sinne von Definition 5.14.
Sei umgekehrt Φ ein Morphismus im Sinne der allgemeinen Definition. Die Projektionsabbildung $p_i : \mathbb{A}^m \to \mathbb{A}^1$ auf die i-te Koordinate wird durch das Polynom $X_i \in k[X_1, \ldots, X_m]$ definiert, ist also ein Morphismus von Varietäten. Dann ist auch $\Phi_i = p_i \circ \Phi$ ein Morphismus $V \to \mathbb{A}^1$, also ein Element von $\mathcal{O}(V)$. □

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

Satz 5.18. *Sei $V \subset \mathbb{A}^n$ affin, $g \in k[V]$. Dann ist die Abbildung*

$$\phi : V(gX_{n+1} - 1) \to U_g \qquad (x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n)$$

ein Isomorphismus von Varietäten.

Beweis: Wegen $g(x_1, \ldots, x_n)x_{n+1} = 1$ auf $V(gX_{n+1} - 1)$ hat die Abbildung Werte in U_g. Nach dem letzten Satz ist die Komposition

$$\tilde{\Phi} : V(gX_{n+1} - 1) \to U_g \subset \mathbb{A}^n$$

ein Morphismus, insbesondere stetig. Dann ist auch Φ stetig, da $U_g \subset \mathbb{A}^n$ offen ist. Die Bedingung an lokale Ringe folgt für Φ folgt sofort aus der für $\tilde{\Phi}$.
Für jeden Punkt in U_g gibt es genau einen Urbildpunkt. Die Umkehrabbildung ist gegeben durch

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, 1/g(x_1, \ldots, x_n)) \ .$$

Wie im affinen Fall respektiert sie lokale Ringe. □

Unsere standardoffenen Mengen sind also als Varietäten *affin*, nämlich isomorph zu einer affinen Varietät. Nicht alle quasi-affinen Varietäten sind affin.

Beispiel. Für $U = \mathbb{A}^2 \setminus \{0\} =$ gilt $\mathcal{O}(U) = \mathcal{O}(\mathbb{A}^2)$. Es ist nicht affin. (Übungsaufgabe)

Wir betrachten nun den quasi-projektiven Fall, den wir auf den affinen reduzieren wollen.

Lemma 5.19. *Sei $U_i \subset \mathbb{P}^n_k$ die i-te standardaffine Teilmenge. Dann ist die Kartenabbildung $\phi_i : U_i \to \mathbb{A}^n$ ein Isomorphismus von Varietäten.*

Beweis: Wir haben bereits gesehen, dass es sich um einen Homöomorphismus handelt. Auf lokalen Ringen erhalten wir den Isomorphismus aus Lemma 5.13. □

Korollar 5.20. *Sei X eine quasi-projektive Varietät. Dann hat X eine endliche offene Überdeckung $X = \bigcup_{i=1}^m X_i$, so dass jedes X_i affin ist. Die affinen offenen Teilmengen bilden eine Basis der Topologie.*

Beweis: Sei $X \subset \mathbb{P}^n_k$. Jeder Punkt von X liegt in einer standardaffinen Teilmenge U_i, also in einer quasi-affinen Varietät. Diese lässt sich durch standard-offene überdecken, also durch affine. Also ist X Vereinigung von affinen offenen Untervarietäten. Da X noethersch ist, genügt eine endliche Teilüberdeckung. Die Aussage lässt sich auch auf jede offene Teilmenge von X anwenden, daher bilden die affinen offenen Untervarietäten eine Basis der Topologie. □

Bemerkung. Alle lokalen Eigenschaften können auf affinen Varietäten nachgerechnet werden. Hierzu gehören z.B. lokale Ringe und Funktionenkörper.

Seien X, Y quasi-projektiv, $\Phi : X \to Y$ ein Morphismus. Dann gehen wir wie folgt vor: Wir überdecken Y durch affine Varietäten U_i $(i = 1, \ldots, n)$. Für jedes U_i ist $\Phi^{-1}(U_i) \subset X$ offen, da Φ stetig ist. Dann überdecken wir das Urbild durch offene affine Untervarietäten V_{ij} für $j = 1, \ldots, n_i$. Durch Einschränken erhalten wir Morphismen von affinen Varietäten

$$\Phi_{ij} : V_{ij} \to U_i.$$

Wir wissen bereits, wie diese global durch Polynome beschrieben werden. Man sieht leicht, dass umgekehrt solche Daten einen Morphismus definieren, wenn die Φ_{ij} auf den Schnitten der V_{ij} übereinstimmen. Wir verzichten auf eine genaue Formulierung.
Wir konzentrieren uns nun auf den einfacheren irreduziblen Fall.

Satz 5.21 (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 $\overline{U}$. Da X irreduzibel ist, gilt $X = \overline{U}$. □

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

Definition 5.22. *Sei X irreduzible quasi-projektive Varität, $\Phi \in \mathbb{P}^n(k(X))$, $P \in X$. Dann heißt Φ* regulär in P*, falls es einen Repräsentanten*

$$\Phi = [\Phi_0 : \cdots : \Phi_n]$$

gibt, so dass alle $\Phi_i(P)$ für $i = 0, \ldots, n$ definiert sind und nicht alle gleichzeitig verschwinden. In diesem Fall setzen wir

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

Bemerkung. $\Phi(P)$ ist wohldefiniert: Gilt $[\Phi_0 : \cdots : \Phi_n] = [\Phi'_0 : \cdots : \Phi'_n]$ und beide Repräsentanten sind regulär in P, so ist $\Phi_i = \Psi\Phi'_i$ für alle i. Hierbei ist $\Psi \in k(X)^*$. Es gibt einen Index i mit $\Phi'_i(P) \neq 0$. Es folgt $\Psi(P) = \Phi(P)\Phi'_i(P)^{-1} \in k$, d.h. Ψ ist regulär in P. Wäre $\Psi(P) = 0$, so wäre $\Phi_j(P) = 0$ für alle j. Also ist $\Psi(P) \neq 0$. Daher ist $\Phi(P) = \Phi'(P)$.

Satz 5.23. *Sei X irreduzible quasi-projektive Varität, $Y \subset \mathbb{P}^n_k$ quasi-projektiv. Ein Element $\Phi \in \mathbb{P}^n(k(X))$ definiert genau dann einen Morphismus $\phi : X \to Y$, wenn Φ in allen $P \in X$ regulär ist und $\Phi(P) \in Y$ für alle $P \in X$. Jeder Morphismus $f : X \to Y$ ist von dieser Form.*

Beweis: Sei $\Phi \in \mathbb{P}^n(k(X))$ regulär in allen $P \in X$ und $\Phi(P) \in Y$ für alle P. Wir überprüfen, dass es sich um einen Morphismus handelt. Ohne Einschränkung (Übergang zu einer offenen Überdeckung) sind X und Y affin und $Y \subset U_0$. Nach Voraussetzung ist dann $\Phi_0(P) \neq 0$ für alle $P \in X$. Wir gehen über zu $\Phi'_i = \Phi_i/\Phi_0$ für $i = 0, \ldots, n$. Nach Voraussetzung ist Φ'_i algebraisch. Damit ist $\Phi' : X \to \mathbb{A}^n$ ein Morphismus von affinen Varietäten, der nach Voraussetzung über Y faktorisiert, also ein Morphismus.
Nun betrachten wir die Rückrichtung. Wir betrachten die Komposition $\psi : X \to Y \to \mathbb{P}^n$. Sei $U_i \subset \mathbb{P}^n$ standardaffin mit $V_i = \psi^{-1}(U_i)$ nichtleer (also dicht in X). Eine solche Menge gibt es, da die U_i den projektiven Raum überdecken. Dann ist $\psi|_{V_i}$ eine Abbildung $V_i \to \mathbb{A}^n$, wird also durch ein Tupel $\phi^i_0, \ldots, \hat{\phi}_i, \ldots, \phi^i_n \in \mathcal{O}(U)$ gegeben. Wir fassen sie in $k(U) = k(X)$ auf und setzen

$$\Phi^i = [\phi^i_0 : \cdots : \phi^i_{i-1} : 1 : \phi^i_{i+1} : \cdots : \phi^i_n]$$

Die verschiedenen Φ^i stimmen auf dem Schnitt ihrere Definitionsbereiche überein, sind also als Elemente des $\mathbb{P}^n(k(X))$ gleich. Jeder Punkt von X liegt in einem V_i, der Morphismus ist also überall regulär. □

Bemerkung. In vielen klassischen Texten wird dies als Definition eines Morphismus von Varietäten genommen. Man muss sich dann allerdings auf irreduzible Varietäten einschränken.

Kapitel 6

Hilbertscher Nullstellensatz und 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. Nebenbei beweisen wir auch den Hilbertschen Nullstellensatz.

Endliche Morphismen

Sei $A \to B$ ein Ringhomomorphismus, $b_1, \ldots, b_n \in B$ Elemente. Wir schreiben $A[b_1, \ldots, b_n]$ für den Teilring von B, der als A-Algebra von $b_1, \ldots, b_n$ erzeugt wird.

Definition 6.1. *Sei $f : A \to B$ 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 $f : X \to Y$ von quasi-projektiven Varietäten heißt *endlich*, wenn es eine offene affine Überdeckung $Y = U_1 \cup \cdots \cup U_n$ 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 $1, Y \mod f$. 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 $1, Y, Y^2, \ldots$ 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. (i) Ist in (iv) auch $B = L$ ein Körper, so nennt man L/K eine *endliche Körpererweiterung*. Ihre Eigenschaften werden ausführlich in der Algebra-Vorlesung besprochen.

(ii) 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 6.2. *Sei $f : A \to B$ endlicher Ringhomomorphismus.*

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

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

$$\overline{f} : A/I \to B/J$$

endlich.

(iii) Sei $S \subset A$ multiplikativ. Dann ist

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

endlich.

Beweis: Sei $b_1, \ldots, b_n$ ein Erzeugendensystem von B als A-Modul. Dann sind die Restklassen $\bmod J$ Erzeuger von B/J. Die Brüche $b_i/1$ sind Erzeuger von $S^{-1}B$.
Ist $c_1, \ldots, c_m$ ein Erzeugendensystem von C als B-Modul, so sind die $g(b_i)c_j$ ein A-Erzeugendensystem von C. □

Bemerkung. Sind E/L und L/K endliche Körpererweiterungen, so ist nach (i) auch die Erweiterung E/K endlich.

Lemma 6.3. *Sei $A \to B$ Ringhomomorphismus, $b \in B$ ein Element. Das Element b ist genau dann ganz über A, wenn b Nullstelle eines normierten Polynoms $F \in A[X]$ ist.*

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

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

Es ist

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

Diese Relation multiplizieren wir mit b und es folgt

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

Ebenso folgt iterativ, dass alle b^i in diesem Modul liegen.
Sei umgekehrt $A[b]$ erzeugt von $b_1, \ldots, b_n$. Sei b^N die maximale Potenz von b, die in $b_1, \ldots, b_n$ vorkommt. Dann lässt sich b^{N+1} als Linearkombination von $b_1, \ldots, b_n$ schreiben. Dies ergibt die gesuchte normierte Polynomrelation für b über A. □

Wir erinnern an einen Satz aus der Körpertheorie.

Lemma 6.4. *Sei K Körper, $K \to E$ eine endliche, nullteilerfreie K-Algebra. Dann ist E ein Körper.*

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

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

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

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

Falls $b_0 = 0$, 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. □

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

Satz 6.5 (Going-Down)**.** *Sei $f : A \to B$ 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 $S \cap \mathfrak{p} = \emptyset$. 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 $A_{\mathfrak{p}} \to S^{-1}B$ ist endlich.
Sei also nun ohne Einschränkung A wie in der Behauptung.

Behauptung. *Ohne Einschränkung ist A ein Körper.*

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

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

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

$$K \to B/P \to B/Q$$

Hierin sind B/P und B/Q Integritätsbereiche, die endlich sind über K. Nach Lemma 6.4 sind beides Körper. Eine surjektive Abbildung von Körpern ist ein Isomorphismus. 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. □

Im Allgemeinen gilt keine Gleichheit.

Beispiel. Sei $A = k[X, Y]$, $B = k[X, Y]/f$ für ein irreduzibles f. Dann ist $A \to B$ endich, aber es gilt (wie wir noch sauber zeigen werden) $\dim A = \dim \mathbb{A}^2 = 2$, $\dim B = \dim V(f) = 1$.

Das ist aber auch das einzige Problem.

Theorem 6.6 (Going-Up)**.** *Sei $f : A \to B$ 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 $P \subsetneq Q$ und $Q \cap A = \mathfrak{q}$. 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

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

weiterhin endlicher Ringhomomorphismus. Es genügt, die Behauptung in dieser Situation zu zeigen. Ist nämlich $\tilde{Q}$ ein Primdideal von $S^{-1}B$, das $S^{-1}P$ und $S^{-1}\mathfrak{q}$ enthält, so ist $\tilde{Q} = S^{-1}Q$ für ein Primideal Q, das P und $\mathfrak{q}$ enthält.
Sei also ohne Einschränkung $\mathfrak{q}$ maximal. Wieder wie im letzen Beweis gehen wir über zu

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

Dies ist endlicher Ringhomomorphismus. Sei nun $\overline{Q}$ 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 $\overline{Q}$ in B hat die gewünschte Eigenschaft. □

Wir wenden dies für affine Varietäten an.

Korollar 6.7. *Sei $f : X \to Y$ endlicher Morphismus von affinen irreduziblen Varietäten so dass $k[Y] \to k[X]$ injektiv ist. Dann ist f surjektiv und* $\dim X = \dim Y$.

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 $f(Q') = Q$. □

Der Transzendenzgrad und seine Eigenschaften

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

Definition 6.8. *Sei A eine nullteilerfreie K-Algebra. Eine Menge $a_1, \ldots, a_n$ heißt* algebraisch abhängig über K*, wenn es ein Polynom $0 \neq P \in K[X_1, \ldots, X_n]$ gibt mit Nullstelle $(a_1, \ldots, a_n)$. Eine maximale algebraisch unabhängige Teilmenge von A heißt* Transzendenzbasis *von A. Die Kardinalität einer Transzendenzbasis heißt* Transzendenzgrad $\mathrm{trdeg}_K(A)$ *von A über K.*

Bemerkung. Oft 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 $X_1X_2 - 1$.

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

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

Lemma 6.9. *Sei A eine nullteilerfreie K-Algebra. Seien $a_1, \ldots, a_n \in A$. Dann ist die Menge*

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

ein Teilring von A.

Beweis: Wie in der Algebravorlesung. Wir wiederholen schnell: Jedes Element $a \in K[a_1, \ldots, a_n]$ erfüllt eine Polynomgleichung $a - P(a_1, \ldots, a_n)$, ist also in $\overline{K[a_1, \ldots, a_n]}$ enthalten.
Seien nun a, b algebraisch über $K[a_1, \ldots, a_n]$. Dann erfüllen sie nach Voraussetzung jeweils eine Polynomgleichung in einer Variablen über $K_1 = K(a_1, \ldots, a_n)$. 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 6.2 (i)). Sei $c \in K_1[a, b]$. Dann ist $\dim_{K_1} K_1[c] < \infty$ und nach Lemma 6.3 erfüllt 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. □

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, $\mathrm{trdeg}(A) = 1$.

Satz 6.10. *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 abhängig. □

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

Nullstellensatz

Theorem 6.11 (Noethersches Normalisierungslemma)**.** *Sei K Körper, B endlich erzeugte nullteilerfreie K-Algebra vom Transzendenzgrad d. Dann gibt es Elemente*

$$x_1, \ldots, x_d \in B \ ,$$

die algebraisch unabhängig über K sind, so dass B endlich über $K[x_1, \ldots, x_d]$. Mit anderen Worten, es gibt eine endlichen injektiven Algebrenhomomorphismus

$$K[X_1, \ldots, X_d] \to B \ .$$

Bemerkung. (i) $K[X_1, \ldots, X_d]$ und B haben denselben Transzendengrad und nach Going-Up dieselbe Dimension. Wir werden das benutzen, um zu zeigen, dass beides übereinstimmt.

(ii) Sei V eine irreduzible affine Varietät. Nach dem Normalisierungslemma gibt es dann einen endlichen surjektiven Morphismus

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

wobei $d = \mathrm{trdeg}(k[V])$. Es gilt $\dim V = \dim \mathbb{A}^d$ (und beides ist gleich d, wie wir sehen werden.)

Beweis: Es ist $B = K[Y_1, \ldots, Y_m]/\mathfrak{p}$ für ein Primideal $\mathfrak{p}$. Sei $y_i = Y_i \mod \mathfrak{p}$.
Falls $m = d$, so ist $m = \mathrm{trdeg}k[y_1, \ldots, y_m]$. Die Elemente sind algebraisch unabhängig, also $B \cong K[Y_1, \ldots, Y_m]$ 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 $k[X_1, \ldots, X_d]$ nach Induktionsvoraussetzung und Endlichkeit ist transitiv.)
Da $m > d$, gibt es eine Relation $f \in k[Y_1, \ldots, Y_m]$

$$f(y_1, \ldots, y_m) = 0 \ .$$

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

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

Dann gilt

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

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

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

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

$$aY_1^{b_1 + r_2 b_2 + \cdots + r_m b_m}$$

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

$$F(Y_1, Z_2, \ldots, Z_m) = bY_1^N + \text{ kleinere Terme bzgl. } Y_1$$

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

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

Nach Lemma 6.3 ist B ganz über B'. □

Satz 6.12 (Körpertheoretischer Nullstellensatz)**.** *Sei K ein Körper, $K \to E$ eine endlich erzeugte K-Algebra. Wenn E ein Körper ist, so ist E eine endliche algebraische Erweiterung von K, d.h.* $\dim_K E < \infty$.

Beweis: Sei $d = \mathrm{trdeg}E$. Nach Noether-Normalisierung ist E endliche Erweiterung von $K[X_1, \ldots, X_d]$. Nach Going-up gilt

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

Es gilt also $d = 0$. □

Beweis des schwachen Nullstellensatzes Theorem 3.4: Sei k algebraisch abgeschlossen, $I \subset k[X_1, \ldots, X_n]$ maximal. Dann ist $E = k[X_1, \ldots, X_n]/I$ ein Körper, der als k-Algebra endlich erzeugt ist. Nach Satz 6.12 ist $\dim_k E < \infty$.

Behauptung. $E = k$.

Sei $y \in E$. Dann ist y endlich über k. Nach Lemma 6.3 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

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

Beide Ideale sind maximal, also gleich. □

Dimension

Lemma 6.13. *Seien $P \subsetneq Q$ Primideale von $K[X_1, \ldots, X_n]$. Dann ist*

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

Beweis: Der Homomorphismus $K[X_1, \ldots, X_n]/P \to K[X_1, \ldots, X_n]/Q$ ist surjektiv. Sind also Elemente algebraisch abhängig modulo P, dann auch modulo Q. Dies bedeutet, dass $\leq$ gilt.
Angenommen, es gilt Gleichheit. Sei $\alpha_i = X_i \mod P$ und $\beta_i = X_i \mod Q$. Sei ohne Einschränkung $\beta_1, \ldots, \beta_r$ eine Transzendenzbasis von $K[\beta_1, \ldots, \beta_n]$. Dann sind die Urbilder $\alpha_1, \ldots, \alpha_r$ algebraisch unabhängig und wegen der Gleichheit der Transzendenzgrade bilden sie eine Transzendenzbasis von $K[\alpha_1, \ldots, \alpha_n]$. Nun Lokalisieren wir wieder. Sei $S = K[X_1, \ldots, X_r] \setminus \{0\}$. Dies ist eine multiplikative Menge. Es gilt $S \cap P = S \cap Q = \emptyset$, da $X_1, \ldots, X_r$ algebraisch unabhängig modulo P und Q bleiben. Sei

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

und es gilt

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

Hierin sind $\alpha_{r+1}, \ldots, \alpha_n$ algebraisch über E. Nach Lemma 6.4 ist also $E[\alpha_{r+1}, \ldots, \alpha_n]$ ein Körper. Dies bedeutet, dass $S^{-1}P$ ein maximales Ideal ist. Es ist aber $S^{-1}P \subset S^{-1}Q \subset S^{-1}K[X_1, \ldots, X_n]$. Wegen $S \cap Q = \emptyset$ sind dies echte Inklusionen, ein Widerspruch zur Maximalität. □

Theorem 6.14. *Sei A nullteilerfreie, endlich erzeugte Algebra über einem Körper K. Dann ist*

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

Insbesondere ist $\dim \mathbb{A}^n = n$.

Beweis: Nach Noether Normalisierung gibt es eine injektive, endliche Ringerweiterung $K[X_1, \ldots, X_d] \to A$, wobei $d = \operatorname{trdeg} A$. Es folgt mit Going up

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

Wir zeigen nun die andere Implikation. Sei $A = K[X_1, \ldots, X_n]/P$ für ein Primideal P. Zu zeigen ist

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

Wir betrachten nun eine maximale Kette von Primidealen

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

Sei Q_i das Urbild von $\overline{Q}_i$ in $K[X_1, \ldots, X_n]$, inbesondere $Q_0 = P$. Nach Lemma 6.13 gilt

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

Da die letzte Zahl mindestens 0 ist, folgt

$$\operatorname{trdeg}(K[X_1, \ldots, X_n]/P) \geq \dim A$$

□

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

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

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

Korollar 6.15. *Sei $V \subset \mathbb{P}^n$ quasiprojektiv mit irreduziblen Komponenten $V_1, \ldots, V_m$. Dann gilt*

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

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

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

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 6.14

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

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

Wir erwarten im Prinzip, 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 6.16 (Krulls Hauptidealsatz)**.** *Sei X irreduzible Varietät, $g : X \to \mathbb{A}^1$ ein nichtkonstanter Morphismus, Z eine irreduzible Komponente von $V(g)$. Dann gilt*

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

Dies hat weitreichende Konsequenzen:

Korollar 6.17. *Sei X irreduzibel, $Z \subsetneq X$ eine maximale irreduzible abgeschlossene Teilmenge. Dann ist*

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

Beweis: Ohne Einschränkung ist X affin, $Z = V(f_1, \ldots, f_n)$ 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. □

Korollar 6.18 (Äquidimensionalität)**.** *Sei X eine irreduzible Varietät,*

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

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}. □

Vor dem Beweis von Krulls Hauptidealsatz brauchen wir noch etwas Vorbereitung.

Lemma 6.19. *Sei $A = k[X_1, \ldots, X_d]$, $A \to B$ endlicher Ringhomomorphismus, B ein Integritätsring, $b \in B$ ein Element. Dann ist b Nullstelle eines irreduziblen normierten $F \in A[T]$*

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

mit Nullstelle b. Wir fassen Multiplikation mit B als $Q(A)$-lineare Abbildung $Q(B) \to Q(B)$ auf. Dann gilt $\det(b) = \pm a_m^s$ für ein $s \in \mathbb{N}$. Insbesondere ist $\det(b) \in A$.

Beweis: Da A noethersch ist und B/A endlich, ist auch $B' = A[b]$ endlich über A. Also ist b Nullstelle eines normierten Polynoms $F \in A[T]$. 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 $1, b, \ldots, b^{m-1}$. Wir berechnen die Matrix M der Multiplikation mit b

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

und erhalten $\det(b) = \pm a_m$.
B ist endlich erzeugt als A-Modul, also ist $B = A[b, b_1, \ldots, b_n]$ für endlich viele ganze Elemente b_i. Dann ist $Q(A)[b, b_1, \ldots, b_n]$ ein Körper, also gleich $Q(B)$. und $Q(B)/Q(A)$ ist ebenfalls endlich.
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 $\pm a_m$. □

Der Vollständigkeit halber:

Satz 6.20 (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. □

Beweis von Theorem 6.16: Sei Y irreduzible Varietät, $g : Y \to \mathbb{A}^1$ 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 $Z \cup Z_1 \cup \cdots \cup Z_n$. Sei

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

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

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

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

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

Nach dem Lemma liegt dies in A.

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

Sei $T^m + a_1 T^{m-1} + \cdots + a_m$ das Polynom zu g aus dem Lemma. Wegen

$$\pm a_m = g(g^{m-1} + a_1 g^{m-2} + \cdots + a_{m-1})$$

gilt

$$a_m \in \langle g \rangle \ .$$

g' ist Potenz von a_m, also erst recht

$$g' \in \langle g \rangle \ .$$

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

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 in B die Determinante dieser Relation und erhalten in A

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

Wegen $h \in A$ ist $\det h$ eine Potenz von h, also haben wir die gesuchte Relation gefunden.
Daher ist

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

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

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

überein. □

Kapitel 7

Das Hilbert-Polynom

Für projektive Varietäten gibt es noch eine dritte Methode, die Dimension zu beschreiben. Sie geht aus vom homogenen Koordinatenring. Nebenbei wird eine weitere Invariante eingeführt, der *Grad* einer projektiven Varietät. Er ist wichtig für den Satz von Bézout und seinen höher-dimensionalen Verallgemeinerungen.

Satz 7.1 (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.*

Leider werden wir nicht genug Zeit für den Beweis haben.

Graduierte Ringe und Modun

Definition 7.2. *(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

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

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 graduierter S-Modul *ist eine direkte Summe*

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

von A-Moduln zusammen mit einer skalaren Multiplikation

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

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

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

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

Beispiel. Sei $A = K$ ein Körper. Dann ist $K[X_0, \ldots, X_n]$ ein graduierter Ring mit $K[X_0, \ldots, X_n]_d$ der Vektorraum der homogenen Polynome vom Grad d.

Lemma 7.3. *Ist $V \subset \mathbb{P}_k^n$ eine projektive Varietät, so ist $I(V)$ ein graduiertes Ideal.*

Beweis: Wir erinnern uns:

$$I(V) = \left\{ \sum f_d | f_d(V) = 0 \right\}$$

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, $s_m \in k[X_0, \ldots, X_n]_m$ homogen vom Grad m. Dann ist $s_m f_d$ homogen vom Grad $m + d$. Damit ist $I(V)$ ein homogenes Ideal. □

Lemma 7.4. *Sei S graduierter Ring, $I \subset S$ homogenes Ideal. 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 homogenes Ideal ist. Die Abbildung ist auch injektiv. □

Korollar 7.5. *Sei $V \subset \mathbb{P}^n$ projektiv. Der* homogene Koordinatenring *$S(V) = k[X_0, \ldots, X_n]/I(V)$ ist eine graduierte k-Algbra.*

Bemerkung. S soll an die symmetrische Algebra erinnern, denn

$$k[X_0, \ldots, X_n] \cong \mathrm{Sym}^* V$$

wobei V ein k-Vektorraum der Dimension $n + 1$.

Definition 7.6. *Sei M ein endlich erzeugter graduierter Modul über $S = k[X_0, \ldots, X_n]$. Dann heißt*

$$\phi_M : \mathbb{Z} \to \mathbb{Z} \qquad \phi_M(d) = \dim_k M_d$$

Hilbert-Funktion *von M.*

Am interessantesten sind natürlich die homogenen Koordinatenringe von Untervarietäten.

Theorem 7.7. *Sei M ein endlich erzeugter graduierter $k[X_0, \ldots, X_n]$-Modul. Dann gibt es ein eindeutiges Polynom $P_M \in \mathbb{Q}[z]$ mit*

$$P_M(d) = \phi_M(d) \text{ für } d \text{ groß genug}$$

P_M heißt Hilbert-Polynom *von M. Es gilt*

$$\deg P_M = \dim V(I(M))$$

wobei $I(M) = \{s \in k[X_0, \ldots, X_n] | sM = 0\}$.

Definition 7.8. *Sei $V \subset \mathbb{P}^n$. Das* Hilbert-Polynom *P_V von V ist das Hilbertpolynom von $S(Y)$. Ist*

$$P_V(z) = a_d z^d + \cdots + a_0 \qquad a_d \neq 0$$

so heißt $d! a_d$ Grad von V.

Bemerkung. Wegen $I(S(V)) = I(V)$ gilt $d = \deg P_V = \dim V$. Ist $V \subset \mathbb{P}^n$ eine Hyperfläche mit $I(V) = \langle f \rangle$, so stellt sich heraus, dass der Grad von V gleich dem Grad von f ist.

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 $\mathbb{P}^1$ 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 eleminiert werden, die beiden anderen Variabeln können frei gewählt werden. Also hat M_d die k-Basis

$$X_0^a X_1^{d-a} \text{ für } a = 0, \ldots, d \qquad X_0^b X_1^{d-b-a} X_2 \text{ für } b = 0, \ldots, d-1$$

Also

$$\phi_M(d) = 2d + 1, \quad P_{V(f)} = 2z + 1$$

Der Grad des Polynoms ist 1, der Grad von $V(f)$ ist $1!2 = 2 = \deg(f)$.

Ein Element des Beweises sind Rechenregeln für unsere Polynome.

Definition 7.9. *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. $\binom{z}{3} = \frac{z(z-1)(z-2)}{3!}$ hat ganze Werte für $z \in \mathbb{N}_0$.

Lemma 7.10. *(i) Sei $F \in \mathbb{Q}[z]$ ein numerisches Polynom. Dann gilt*

$$F(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \cdots + c_r \qquad c_i \in \mathbb{Z}$$

(ii) Sei $f : \mathbb{Z} \to \mathbb{Z}$ 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 $\Delta(F)$. 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

$$\Delta F = c_0 \binom{z}{r-1} + \cdots + c_{r-1}$$

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

$$G = c_0 \binom{z}{r} + \cdots + c_r \qquad c_i \in \mathbb{Z}$$

Wir setzen

$$\tilde{F} = c_0 \binom{z}{r+1} + \cdots + c_r \binom{z}{1}$$

Dann gilt $\Delta\tilde{F} = G$, also $\Delta(f - \tilde{F})(n) = 0$ für genügend großes n. Mit anderen Worten

$$c_{r+1} := f(n+1) - \tilde{F}(n+1) = f(n) - \tilde{F}(n) \qquad n \text{ genügend groß}$$

Also folgt $c_{r+1} \in \mathbb{Z}$. Dann erfüllt

$$F = \tilde{F} + c_{r+1}$$

die Behauptung. □

Korollar 7.11. *Ist F ein numerisches Polynom, $F = a_r z^r + \dots$ mit $a_r \neq 0$, so gilt $r! a_r \in \mathbb{Z}$.*

Auch wenn wir nur an Hilbert-Polynomen für Ringe interessiert sind, ist es sehr vorteilhaft auch Moduln zu betrachten.

Bemerkung. Sei

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

eine exakte Sequenz von endlich erzeugten graduierten S-Moduln. Dann gilt

$$\phi_{M_2} = \phi_{M_1} + \phi_{M_3}.$$

Haben wir Hilbert-Polynome für M_1 und M_3 gefunden, so gilt

$$P_{M_2} = P_{M_1} + P_{M_3}.$$

Beweisidee von Theorem 7.7: Der Beweis wird mit Induktion über die Dimension von $V(I(M))$ geführt. Da ϕ_M additiv in kurzen exakten Sequenzen ist, kann man sich auf einfache Bausteine reduzieren, das ist der Fall $M = S/P[l]$ für ein homogenes Primideal. Der Verschiebeoperator entspricht einem Koordinatenwechsel $z \mapsto z + l$, daher reicht $l = 0$.
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

$$0 \to M \xrightarrow{X_0} M[1] \to M'' \to 0$$

Die erste Abbildung ist injektiv, da P ein Primideal ist und $X_0 \notin P$. Wieder wird die Additivität in kurzen exakten Sequenzen benutzt und die Induktionsvoraussetzung für M''. □

Satz 7.12. *(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 (ii): 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 $V(I_1 + I_2) = Y_1 \cap Y_2$. Wir haben also eine kurze exakte Sequenz

$$0 \to S/I \to S/I_1 \oplus S/I_2 \to S/(I_1 + I_2) \to 0$$

Es folgt

$$P_Y = P_{S/I} = P_{S/I_1} + P_{S/I_2} - P_{S/(I_1+I_2)} = P_{Y_1} + P_{Y_2} - P_{Y_1 \cap Y_2}$$

Wegen der Dimensionsvoraussetzung ist der führende Koeffizient

$$\frac{\deg Y}{r!} = \frac{\deg Y_1}{r!} + \frac{\deg Y_2}{r!}$$

Zu (iii): Wir betrachten $P_{k[X_0,\ldots,X_n]}$. Für $d > 0$ hat der Raum der homogenen Polynome vom Grad d in $n+1$-Variablen die Dimension

$$\binom{z+n}{n} = \frac{z^n}{n!} + \ldots$$

Alternativ argumentieren wir mit Induktion nach n und der exakten Sequenz

$$0 \to S \xrightarrow{X_n} S[1] \to k[X_0, \ldots, X_{n-1}] \to 0 \ ,$$

d.h. $\Delta P_S = P_{k[X_0,\ldots,X_{n-1}]}$.
Zu (iv): Sei $I(H) = \langle f \rangle$ mit f vom Grad d. Wir betrachten

$$0 \to S[-d] \xrightarrow{f} S \to S/\langle f \rangle \to 0$$

Dann folgt

$$\begin{aligned}
P_H(z) &= \binom{z+n}{n} - \binom{z-d+n}{n} \\
&= \left(\frac{z^n}{n!} + \frac{1}{n!}(\sum_{i=1}^{n} i) z^{n-1} + \ldots \right) - \left(\frac{z^n}{n!} + \frac{1}{n!}(\sum_{i=1-d}^{n-d} i) z^{n-1} + \ldots \right) \\
&= 0z^n + \left(\frac{n(n+1)}{2} - \frac{n(n-2d+1)}{2} \right) \frac{z^{n-1}}{n!} + \ldots \\
&= \frac{d}{(n-1)!} z^{n-1} + \ldots
\end{aligned}$$

□

Kapitel 8

Ausblick

Wir haben bereits gesehen, dass nicht-konstante $f \in k[X,Y]$ eine affine Varietät der Dimension 1 definieren, bzw. homogene $F \in k[X,Y,Z]$ eine projektive Varietät der Dimension 1. Wir nennen diese Varietäten *ebene Kurven*. In diesem Kapitel interessieren wir uns nur für irreduzible Gleichungen und Kurven.

Beispiel. Wir vergleichen

$$V_1 : y^2 = x(x-1)(x_2)$$

und

$$V_2 : y^2 = x^2(x-1)$$

Beide Varietäten enthalten den Punkt $(0,0)$, haben dort aber völlig verschiedenes Verhalten.

Definition 8.1. *Sei $V(f) \subset \mathbb{A}^2$ irreduzibel, $P \in V(f)$. Der Punkt heißt* singulär*, falls $\nabla(f) = (\partial f/\partial X, \partial f/\partial Y)$ in P eine Nullstelle hat,* nicht-singulär *andernfalls. Die Kurve $V(f)$ heißt* nicht-singulär*, wenn sie keine singulären Punkte enthält.*

In dem Beispiel $f = Y^2 - X^2(X-1)$

$$\frac{\partial f}{\partial X} = -2X(X-1) - X^2$$
$$\frac{\partial f}{\partial Y} = 2Y$$

Eine gemeinsame Nullstelle (x,y) hat also $y = 0$ (wir setzen ab jetzt Charakteristik ungleich 2 voraus), liegt in $V(f)$, also $0 = x^2(x-1)$, d.h. $x = 0, 1$. Beim Einsetzen von $x = 1$ in die partielle Ableitung erhalten wir -1, beim Einsetzen von $x = 0$ erhalten wir 0. Einziger singulärer Punkt ist $(0,0)$.

Bemerkung. Eine Kurve der Form $Y^2 = g(X)$ ist genau dann singulär, wenn g mehrfache Nullstellen hat.

Bemerkung. Sei $k = \mathbb{C}$, $P = (x_0, y_0) \in V(f) \subset \mathbb{C}^2$ nicht-singulär. Sei ohne Einschränkung $\partial f/\partial X(P) \neq 0$. Nach der komplexen Version des Satzes über implizite Funktionen gibt es dann eine komplex differenzierbare Abbilung $\phi : U \to \mathbb{C}$ auf einer Umgebung von y_0 und eine offfene Umgebung $U' \subset \mathbb{C}^2$ von P, so dass

$$f(\phi(y), y) = 0 \qquad \text{für alle } y \in U$$

und alle Punkte von $V(f) \cap U'$ sind von dieser Form.
Mit anderen Worten: $V(f)$ ist lokal der Graph einer differenzierbaren Funktion. Die Abbildung

$$\psi : V(f) \cap U' \to U, \quad (x, y) \mapsto y$$

hat das Inverse ϕ. In der Sprache der Differentialtopologie: $V(f)$ ist eine komplexe Mannigfaltigkeit und ψ ist eine Karte.

Besonders interessant sind die Gleichungen vom Grad 3.

Definition 8.2. *Sei $f \in k[X, Y, Z]$ homogen vom Grad 3, so dass $V(f)$ nicht-singulär. Dann heißt $E = V(f)$* elliptische Kurve.

Sie sind einfach genug, dass man viel beweisen kann, aber kompliziert genug, dass man viele interessante Aussagen machen kann. Insbesondere tragen sie eine *Gruppenstruktur*. Es gibt drei Arten diese Gruppenstruktur zu beschreiben. Wir beginnen mit der geometrischen.

Satz 8.3. *Sei $E \subset \mathbb{P}^2$ elliptisch. Sei $L \subset \mathbb{P}^2$ eine projektive Gerade. Dann schneiden sich E und L in genau drei Punkten, mit Vielfachheit gezählt.*

Für $P \in E \cap L$ definieren wir hierbei die Schnittmultiplizität als

$$\dim_k(k[E]_P/I(L)).$$

Beispiel. Wir betrachten die elliptische Kurve

$$Y^2Z = X(X - Z)(X - 2Z)$$

die Gerade $L = V(X)$. Die beiden Varietäten schneiden sich in $V(X, Y^2Z)$, also $\{P = [0 : 0 : 1], Q = [0 : 1 : 0]\}$. Wir berechnen die Schnittmultiplizitäten. Für P rechnen wir in der affinen Karte $Z \neq 0$. Wir haben

$$k[E]/I(L)_P = k[X, Y]/\langle Y^2 - X(X - 1)(X - 2), X\rangle = k[Y]/Y^2$$

Dieser Vektorraum hat die Dimension 2, die Schnittmultiplizität ist 2.
Für Q rechnen wir in der affinen Karte $Y \neq 0$. Dort lautet die Gleichung $Z = X(X - Z)(X - 2Z)$, also

$$k[E]_Q/I(L) = k[X, Z]/\langle Z - X(X - Z)(X - 2Z), X\rangle = k[Z]/Z = k$$

die Schnittmultiplizität ist also 1.

Beweis: (Skizze) Wir benutzen die Geradengleichung, um eine Variable zu eliminierenIn einer geeigneten affinen Karte handelt es sich noch um eine Gleichung vom Grad 3 in Variablen. Mit Vielfachheit hat sie genau 3 Nullstellen. □

Definition 8.4. *Sei $E \subset \mathbb{P}^2$ elliptisch, $O \in E$ fest. Für $P, Q \in E$ sei R der dritte Schnittpunkt der Geraden durch P und Q mit E. Es sei $P \oplus Q$ der dritte Schnittpunkt der Geraden durch O und R mit E.*

Satz 8.5. *$(E, \oplus)$ ist eine kommutative Gruppe.*

Beweis: (Idee) Das neutrale Element ist O. Sei L die Tangente an E in O und O' der dritte Schnittpunkt von L und E. Wir finden $-P$ als den dritten Schnittpunkt der Geraden durch P und O' mit E. Die Komposition ist offensichtlich kommutativ.
Schwieriger ist das Assoziativgesetz. Meist leitet man es aus dem Satz von Bézout her über die Anzahl von Schnittpunkten von Kurven vom Grad n und m. Details finden sich z.B. im Buch von Brieskorn über ebene Kurven. □

Über $\mathbb{C}$ können wir das Gruppengesetzt auch analytisch beschreiben. $E \subset \mathbb{P}^2_{\mathbb{C}}$ ist eine kompakte 1-dimensionale Mannigfaltigkeit, also eine kompakte *Riemannsche Fläche*. Ihr Geschlecht ist 1. Tatsächlich ist sie isomorph zu $\mathbb{C}/\Omega$, wobei $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ein *Gitter* ist, d.h. $\omega_1/\omega_2 \notin \mathbb{R}$ und damit $\mathbb{R}$-linear unabhängig. In der komplexen Analysis heißen komplex differenzierbare Funktionen

$$f : \mathbb{C}/\Omega \to \hat{\mathbb{C}} = \mathbb{P}^1_{\mathbb{C}}$$

auch *elliptisch*. Der Prototyp ist die *Weierstraßsche $\wp$-Funktion*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Sie erfüllte eine Differentialgleichung der Form

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

für $g_2, g_3 \in \mathbb{C}$. Die Abbildung

$$z \mapsto [\wp : \wp' : 1]$$

definiert dann einen analytischen Isomorphismus

$$\mathbb{C}/\Omega \to V(Y^2Z - 4X^3 - g_2XZ^2 - g_3Z^3).$$

Satz 8.6. *Die Abbildung ist ein Gruppenhomomorphismus.*

Den Beweis kann man bei genügend Kenntnis der Eigenschaften von $\wp$ mit der Hand führen. Besser ist eine Uminterpretation, die weitere Begriffe benötigt.

Definition 8.7. *Sei $C \subset \mathbb{P}^2$ eine nicht-singuläre Kurve. Ein* Divisor *auf C ist eine endliche formale Summe*

$$D = \sum_{P \in C} n_P P$$

für $a_i \in \mathbb{Z}$, $P_i \in C$. Sein Grad *ist*

$$\deg(D) = \sum_{P \in C} n_P.$$

Das Linearsystem *zu D ist*

$$L(D) = \{f \in k(C) | \mathrm{ord}_P f \geq -n_P\}.$$

Wir schreiben

$$l(D) = \dim_k L(D).$$

Hierin ist $\mathrm{ord}_P f$ die Nullstellen- oder Polstellenordnung von f. Für $f \in k[C]$ in einer affinen Karte ist es

$$\dim_k k[C]_P / \langle f \rangle.$$

Theorem 8.8 (Riemann-Roch)**.** *Sei $C \subset \mathbb{P}^2$ nicht-singuläre Kurve, D ein Divisor. Dann gilt*

$$l(D) - L(K - D) = 2g - 2 + \deg(D),$$

wobei K ein kanonischer Divisor ist und g das Geschlecht.

In dem Fall, der uns gerade interessiert ist $g = 1$ und $K = 0$. Die Formel vereinfacht sich zu

$$l(D) - l(-D) = \deg(D).$$

Definition 8.9. *Zwei Divisoren D_1 und D_2 heißen* rational äquivalent*, wenn $D_1 - D_2 = \div(f) = \sum \mathrm{ord}_P(f) P$ für ein $f \in k(C)^*$.*

Korollar 8.10. *Die Abbildung*

$$P \mapsto [P] - [O]$$

definiert einen Gruppenisomorphismus zwischen E und der Gruppe der Divisoren vom Grad 0 modulo rationaler Äquivalenz.

Die seltsame Vorschrift erklärt sich also daraus, dass der Divisor $[P] + [Q] + [R]$ der Schnittpunkt einer Geraden mit E rational äquivalent zu 0 ist.

Arithmetische Anwendungen

Sei nun $f \in \mathbb{Q}[X, Y, Z]$ homogen vom Grad 3, $E = V(f)$. Wir schreiben $E(\mathbb{Q})$ für Lösungen von f in $\mathbb{P}^2_{\mathbb{Q}}$. Wir setzen voraus, dass f eine Lösung O mit Koordinaten in $\mathbb{Q}$ hat. Die geometrische Konstruktion des Gruppengesetzes funktioniert weiterhin.

Theorem 8.11 (Mordell)**.** *Die Gruppe $E(\mathbb{Q})$ ist endlich erzeugt.*

Sie hat also die Form

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus \oplus_i \mathbb{Z}/n_i\mathbb{Z}$$

Der endliche Anteil ist sehr gut verstanden. Möglich ist nur

$$\mathbb{Z}/N\mathbb{Z} \quad N = 1, 2, \ldots, 10, 12$$

oder

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \quad N = 1, 2, 3, 4$$

(Mazur 1978). Der Rang r ist sehr rätselhaft. Er wird beschrieben durch die Vermutung von Birch und Swinnerton-Dyer. Für $r \geq 2$ ist hierzu nichts bekannt, z.B. wissen wir nicht, ob r beliebig groß werden kann.

Ein anderer Fall von großem Interesse sind elliptische Kurven über einem endlichen Körper $\mathbb{F}_p$. In diesem Fall ist $E(\mathbb{F}_p)$ endlich und wir können die Lösungen abzählen.

Definition 8.12. *Sei $E/\mathbb{F}_p$ eine elliptische Kurve. Wir setzen*

$$a_r = |E(\mathbb{F}_{p^r})|$$

und

$$Z(E, t) = \exp(\sum_{i=1}^{\infty} a_r \frac{t^r}{r}) \in \mathbb{Q}[t].$$

Theorem 8.13 (Weil)**.**

$$Z(E, t) = \frac{(1 - \alpha t)(1 - \beta t)}{(1 - t)(1 - pt)}$$

für $\alpha, \beta \in \overline{\mathbb{Q}}$ ganz über $\mathbb{Z}$ mit $|\alpha| = |\beta| = \sqrt{p}$.

Durch Koeffizientenvergleich erhält man:

Korollar 8.14 (Hasse-Schranke)**.**

$$||E(\mathbb{F}_p)| - p - 1| \leq 2\sqrt{p}$$

Die Gruppe $E(\mathbb{F}_q)$ wird in der modernen Kryptographie zum Verschlüsseln benutzt. Hierbei ist es gut, wenn die Gruppe viele Element hat, also E so gewählt wird, dass die Hasse-Schranke möglichst optimal ausgenutzt wird.

Inhaltsverzeichnis