Skript zur Vorlesung

Algebraische Geometrie Grundlagen

Wintersemester 2012/2013
Frankfurt am Main

Prof. Dr. Annette Werner

Inhaltsverzeichnis

1 Einführung

In der Algebraischen Geometrie studiert man Lösungsmengen von Polynomgleichungen mit geometrischen Methoden. Beispiele für Polynomgleichungen sind etwa die linearen Gleichungssysteme

$$\begin{aligned} a_{11}x_1+ \quad &\cdots \quad +a_{1n}x_n = b_1 \\ &\vdots \\ a_{m1}x_1+ \quad &\cdots \quad a_{mn}x_n = bm, \end{aligned}$$

wobei $(a_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$ und $b_1, \ldots, b_m$ Elemente eines Körpers k sind.
In der Linearen Algebra lernt man, wann ein solches Gleichungssystem eine Lösung in k^n besitzt und wie man die Lösungsmenge beschreiben kann.

Ein weiteres Beispiel sind die Polynomgleichungen in einer Unbestimmten

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

für $a_1, \ldots, a_n \in k$, die man in der Algebra studiert. Ist eine solche Gleichung über k nicht lösbar, so gibt es eine algebraische Körpererweiterung L/K, in der sie lösbar ist.

In der Algebraischen Geometrie wollen wir Lösungsmengen von beliebigen Polynomen in beliebig vielen Unbestimmten studieren. Das erfordert natürlich etwas mehr Aufwand.

Wir bezeichnen den Polynomring in n Unbestimmten über dem Körper k mit $k[x_1, \ldots, x_n]$. Für $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ setzen wir dann

$$\begin{aligned} V_k(f_1, \ldots, f_m) = \{P = (P_1, \ldots, P_n) \in k^n : \\ f_1(P_1, \ldots, P_n) = \ldots = f_m(P_1, \ldots, P_n) = 0. \end{aligned}$$

$V_k(f_1, \ldots, f_m)$ ist also die Menge aller gemeinsamen Nullstellen von $f_1, \ldots, f_m$ in k.

Beispiel:

i) Ist $f(x, y) = x^2 + y^2 - 1 \in \mathbb{Q}[x, y]$, so ist $V_{\mathbb{R}}(f) = \{(P_1, P_2) \in \mathbb{R}^2 : P_1^2 + P_2^2 = 1\}$ der Einheitskreis in $\mathbb{R}^2$.

Wir können auch

$$V_{\mathbb{Q}}(f) = \{(P_1, P_2) \in \mathbb{Q}^2 : P_1^2 + P_2^2 = 1\}$$

betrachten, dies ist die Menge der rationalen Zahlen auf dem Einheitskreis. Auch $V_{\mathbb{C}}(f) = \{(P_1, P_2) \in \mathbb{C}^2; P_1^2 + P_2^2 = 1\}$ ist definiert; dies ist allerdings nicht der Einheitskreis in $\mathbb{C}^2$!

Da f nur die Koeffizienten 0 und 1 hat, können wir f auch im Polynomring $\mathbb{F}_2[x, y]$ auffassen. Dann ist

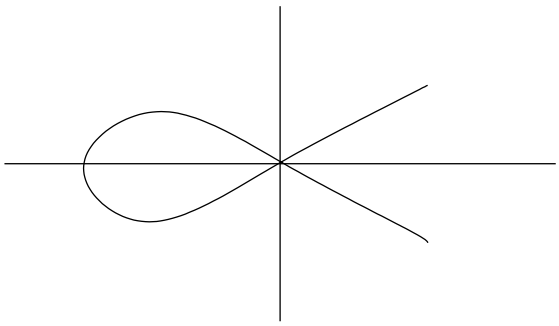
$$\begin{aligned} V_{\mathbb{F}_2}(f) &= \{P_1, P_2) \in \mathbb{F}_2^2 : P_1^2 + P_2^2 = 1\} \\ &= \{(0, 1), (1, 0)\}. \end{aligned}$$

Wir sehen schon an diesem einfachen Beispiel, dass die Nullstellenmenge von f entscheidend vom gewählten Grundkörper abhängt.

ii) Wir betrachten $f(x, y) = y^2 - x^3 - x^2$. Hier ist

$$V_{\mathbb{R}}(f) = \{(P_1, P_2) \in \mathbb{R}^2 : P_2^2 = P_1^3 + P_1^2\}.$$

Dies ist eine Kurve mit einem Doppelpunkt:



Diese Kurve lässt sich „parametrisieren“ durch die Abbildung

$$\begin{aligned} \varphi = \mathbb{R} &\to \mathbb{R}^2 \\ t &\mapsto (t^2 - 1, t^3 - t). \end{aligned}$$

Es gilt $\varphi(\mathbb{R}) \subset V_{\mathbb{R}}(f)$, wie man sofort nachrechnet.
Ferner ist φ injektiv für $t \notin \{\pm 1\}$, denn aus $t^2 - 1 = s^2 - 1$ und $t^3 - t = s^3 - s$ folgt $t(s^2 - 1) = s(s^2 - 1)$, also für $s \neq \pm 1$ auch $t = s$.

Die Tatsache, dass $\varphi(-1) = \varphi(1) = 0$ gilt, erklärt den Doppelpunkt der Kurve.

iii) Die aus der Linearen Algebra bekannte Menge

$$GL_n(k) = \{A \in k^{n \times n} : \det A \neq 0\}$$

der invertierbaren $(n \times n)-$ Matrizen mit Einträgen in k lässt sich ebenfalls als Nullstellenmenge von Polynomen schreiben.
Dazu brauchen wir n^2 Unbestimmte $(x_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,n}}$ und eine zusätzliche Unbestimmte T. Die Determinante einer Matrix ist ein Polynom in den Einträgen, wie man etwa an der Leibniz-Formel sieht. Daher ist $\det\big((x_{ij})_{i,j}\big)$ ein Polynom in $k[x_{11}, \dots, x_{nn}]$. Wir betrachten das Polynom

$$f\big((x_{ij})_{i,j}, T\big) = \det(x_{ij})T - 1 \in k[x_{11}, \dots, x_{nn}, T].$$

Es ist

$$V_k(f) = \{(a_{ij})_{i,j} \in k^{n \times n}, t \in k : \det(a_{ij})_{i,j}\, t = 1\}.$$

Diese Nullstellenmenge lässt sich mit Hilfe der Abbildung

$$GL_n(k) \to V_k(f)$$

$$A \mapsto (A, \tfrac{1}{\det A})$$

mit der Menge $GL_n(k)$ identifizieren.

iv) Wir betrachten nun für $n \geq 2$ noch das berühmte Beispiel

$$f(x, y, z) = x^n + y^n - z^n.$$

Es ist

$$V_{\mathbb{Q}}(f) = \{(a, b, c) \in \mathbb{Q}^3 : a^n + b^n = c^n\}$$

gerade die Menge der rationalen Lösungen der Fermat-Gleichung $x^n + y^n = z^n$. (Pierre de Fermat (1601 oder 1607/08 bis 1665) war ein französischer Jurist und genialer Hobbymathematiker, der u.a. das Traktat „Arithmetika“ von Diophantos von Alexandria mit Randnotizen versah.) Diese hat immer die trivialen Lösungen $(0, 1, 1)$, $(1, 0, 1)$ (und Vielfache davon) sowie $(-1, 1, 0)$, falls n ungerade ist bzw. $(0, 1, -1)$ und $(1, 0, -1)$, falls n gerade ist. Man nennt eine Lösung (a, b, c) nicht trivial, falls $abc \neq 0$ ist.
Für $n = 2$ gibt es unendlich viele nicht-triviale Lösungen, die sogenannten Pythagoräischen Tripel

$$a = 2AB \ , \ b = A^2 - B^2 \ , \ c = A^2 + B^2$$

für ganze Zahlen $A > B > 0$. Es gilt nämlich

$$\begin{aligned} a^2 + b^2 &= (2AB)^2 + (A^2 - B^2)^2 \\ &= 4A^2B^2 + A^4 - 2A^2B^2 + B^4 \\ &= (A^2 + B^2)^2 = c^2. \end{aligned}$$

Für $A = 2$ und $B = 1$ ergibt sich das bekannte Pythagoräische Tripel $(2, 3, 5)$.
Ist $n \geqq 3$, so sagt die berühmte Fermatsche Vermutung, dass die Gleichung

$$x^n + y^n = z^n$$

keine nicht-triviale Lösung in $\mathbb{Q}^3$ besitzt. Mit anderen Worten, die Nullstellenmenge $V_{\mathbb{Q}}(f)$ besteht nur aus den oben angegebenen trivialen Lösungen.

Die Fermatsche Vermutung wurde 1995 von Andrew Wiles mit den hochentwickelten Methoden der Algebraischen Geometrie bewiesen.

2 Kommutative Ringe und Moduln

Wir erinnern zunächst an einige Begriffe aus der Ringtheorie.

Ein **Ring** ist eine Menge A mit zwei Verknüpfungen $+$ und $\cdot$, für die folgende Bedingungen gelten:

i) $(A, +)$ ist eine abelsche Gruppe, insbesondere existiert also ein Nullelement 0 in A.

ii) Die Multiplikation $\cdot$ ist assoziativ und distributiv, d. h. es gilt in A

$$a(b+c) = ab + ac$$

und

$$(a+b)c = ac + bc.$$

Alle Ringe, die wir betrachten werden, sind **kommutativ mit 1**, d.h. es gilt zusätzlich

iii) $ab = ba$ für alle $a, b \in A$.

iv) Es gibt ein Einselement $1 \in A$ mit $1a = a1 = a$ für alle $a \in A$.

Ab sofort treffen wir folgende Vereinbarung: Mit Ring meinen wir immer einen kommutativen Ring mit Eins.

Beispiel:

i) Die Menge $\mathbb{Z}$ der ganzen Zahl ist ein Ring. Ebenso ist $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$ die Menge der rationalen Zahlen, ein Ring.

ii) Ist A ein Ring, so ist auch der Polynomring $A[x] = \{\sum_{n=0}^{N} a_n x^n : N \geqq 0, a_n \in A$ für alle $n = 0, \ldots, N\}$ in einer Variablen über A ein Ring. Induktiv können wir den Polynomring $A[x_1, \ldots, x_n]$ in n Variablen über A definieren..

Ein **Ringhomomorphismus** ist eine Abbildung $f : A \to B$ zwischen Ringen, für die

i) $f(a+b) = f(a) + f(b)$

ii) $f(ab) = f(a)f(b)$

iii) $f(1) = 1$

gilt.

Beispiel: Ist A ein Ring und $c \in A$, so ist die Abbildung $f : A[x] \to A$, $\sum_{n=0}^{N} a_n x^n \mapsto \sum_{n=0}^{N} a_n c^n$ ein Ringhomomorphismus.

f heißt **Isomorphismus** von Ringen, falls es einen Ringhomomorphismus $g : B \to A$ gibt, so dass $f \circ g = id_B$ und $g \circ f = id_A$ gilt. Dies ist genau dann der Fall, wenn der Ringhomomorphismus f injektiv und surjektiv ist.
Eine Teilmenge $\mathfrak{a} \subset A$ heißt **Ideal**, falls

i) $(\mathfrak{a}, +)$ eine Untergruppe von $(A, +)$ ist, d.h. es ist $0 \in \mathfrak{a}$ und $\mathfrak{a}$ ist abgeschlossen unter $+$ und $-$

ii) $\mathfrak{a}A = \mathfrak{a}$ gilt, d.h. für alle $a \in \mathfrak{a}$ und $x \in A$ ist $xa \in \mathfrak{a}$.

Ist $\mathfrak{a} \subset A$ ein Ideal, so erbt die Quotientengruppe $A/\mathfrak{a}$ eine Multiplikationsabbildung von A und wird damit selbst ein Ring. Die Abbildung

$$A \to A/\mathfrak{a}$$

$$x \mapsto x + \mathfrak{a},$$

die x auf die Nebenklasse von x modulo $\mathfrak{a}$ abbildet, ist ein surjektiver Ringhomomorphismus.

Beispiel: Die Menge $k\mathbb{Z} = \{k_n : n \in \mathbb{Z}\}$ ist ein Ideal in $\mathbb{Z}$ für jedes $k \in \mathbb{Z}$. $\mathbb{Z}/k\mathbb{Z}$ können wir mit der Menge $\{0, \ldots, k-1\}$ identifizieren, wobei die Rechenoperationen $+$ und $\cdot$ mit Hilfe der Division mit Rest modulo k definiert sind.

Beispiel: $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} \cap \mathfrak{b}$, Kern eines Ringhomomorphismus.

Ein **Nullteiler** in A ist ein Element $a \in A$, so dass ein $b \in A$ existiert mit $b \neq 0$ und $ab = 0$.

Beispiel: Ist $k > 1$ und $l > 1$, so existieren für $n = kl$ Nullteiler im Ring $\mathbb{Z}/n\mathbb{Z}$, denn es gilt

$$(k + n\mathbb{Z})(l + n\mathbb{Z}) = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}$$

und beide Faktoren sind $\neq 0$.

Definition 2.1 Ein kommutativer Ring mit 1, der keine Nullteiler enthält, heißt **Integritätsring**.

Beispiel: $\mathbb{Z}$, jeder Körper k und jeder Polynomring $A[x_1, \ldots, x_n]$ über einem Integritätsring A sind Beispiele für Integritätsringe.

Wir benötigen nun noch einige Tatsachen über Ideale. Jedes $a \in A$ definiert ein sogenanntes **Hauptideal** $(a) = aA = \{ab : b \in A\}$.
Ist jedes Ideal $\mathfrak{a} \subset A$ ein Hauptideal, so heißt A **Hauptidealring**. Ein Ideal $\mathfrak{p} \neq A$ in A

heißt **Primideal**, falls gilt: Ist $ab \in \mathfrak{p}$ für a und b in A, so gilt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Also ist $\mathfrak{p} \subset A$ genau dann ein Primideal, wenn $A/\mathfrak{p}$ nullteilerfrei ist.

Beispiel: Ist p eine Primzahl, so ist das von p erzeugte Hauptideal $(p) = p\mathbb{Z}$ in $\mathbb{Z}$ ein Primideal. Ferner ist $(0) \subset \mathbb{Z}$ ein Primideal. Auch das Ideal $(x^2 + 1)$ in $\mathbb{R}[x]$ ist ein Primideal.
Ein Ideal $\mathfrak{m} \subset A$ heißt **maximales Ideal**, falls $\mathfrak{m} \neq A$ ist und falls für jedes Ideal $\mathfrak{m} \subset \mathfrak{a} \underset{\neq}{\subset} A$ schon $\mathfrak{m} = \mathfrak{a}$ folgt. Ein Ideal $\mathfrak{m} \subset A$ ist genau dann ein maximales Ideal, wenn $A/\mathfrak{m}$ ein Körper ist.

Beispiel: Ist p eine Primzahl, so ist $(p) \subset \mathbb{Z}$ ein maximales Ideal. Das Nullideal ist nicht maximal in $\mathbb{Z}$. Jedes maximale Ideal ist auch ein Primideal.

Ist $f : A \to B$ ein Ringhomomorphismus, und $\mathfrak{b} \in B$ ein Ideal, so ist $f^{-1}(\mathfrak{b}) \subset A$ ein Ideal. Ist $\mathfrak{b}$ ein Primideal, so ist auch $f^{-1}(\mathfrak{b})$ ein Primideal.

Definition 2.2 i) Es sei I eine beliebige Indexmenge und $(a_i)_{i\in I}$ eine Familie von Elementen aus A. Ein Ideal $\mathfrak{a}$ heißt erzeugt von $(a'_1)_{i\in I}$, wir schreiben $\mathfrak{a} = (a_i)_{i\in I}$, falls alle $a_i \in \mathfrak{a}$ sind und falls sich jedes $x \in \mathfrak{a}$ als $x = x_{i_1}a_{i_1} + \ldots + x_{i_m}a_{i_m}$ schreiben lässt mit geeigneten Indizes $i_1, \ldots, i_m \in I$ und Elementen $x_{i_1}, \ldots, x_{i_m} \in A$.

ii) Ein Ideal $\mathfrak{a} \subset A$ heißt **endlich erzeugt**, falls es endlich viele Elemente $a_1, \ldots, a_m \in \mathfrak{a}$ gibt mit $\mathfrak{a} = (a_1, \ldots, a_m)$.

Beispiel: $(x, x^2, x^3, \ldots) = (x) = \{xf : f \in A[x]\}$ ist ein endlich erzeugtes Ideal in $A[x]$.

Definition 2.3 Ein Ring A heißt **noethersch**, falls jedes Ideal endlich erzeugt ist.

Lemma 2.4 Die folgenden Aussagen sind äquivalent:

i) A ist noethersch.

ii) Jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_k \subset \ldots$ in A wird stationär, d.h. es gibt ein n_0 mit $\mathfrak{a}_{n_0} = \mathfrak{a}_n$ für alle $n \geqq n_0$.

iii) Jede nicht-leere Menge von Idealen besitzt ein maximales Element bezüglich der Inklusion.

Beweis :

i) $\Rightarrow$ ii) Sei $\mathfrak{a} = \bigcup_{i \in \mathbb{N}} \mathfrak{a}_i$. Das ist ein Ideal in A, also endlich erzeugt.

ii) Sei $\Rightarrow$ iii) M eine Menge von Idealen. $\mathfrak{a} \in \mathbf{M}$ heißt **maximal**, falls aus $\mathfrak{a} \subset \mathfrak{b}, \mathfrak{b} \in M$ folgt $\mathfrak{a} = \mathfrak{b}$. Angenommen, es gibt kein maximales Element in M. Dann konstruieren wir eine echte aufsteigende Kette. Das ist ein Widerspruch.

iii) $\Rightarrow$ i) Für ein Ideal $\mathfrak{a} \subset A$ betrachten wir $M = \{$ alle endlich erzeugten Ideale $\mathfrak{b} \subset \mathfrak{a}\}$.

□

Beispiel: Jeder Hauptidealring ist noethersch, insbesondere ist $\mathbb{Z}$ noethersch und auch $k[x]$ für einen Körper k.

Lemma 2.5 Ist A ein noetherscher Ring und $\mathfrak{a} \subset A$ ein Ideal, so ist $A/\mathfrak{a}$ ein noetherscher Ring.

Beweis : Es sei $\pi : A \to A/\mathfrak{a}$ die kanonische Abbildung. Ist $\mathfrak{b} \subset A/\mathfrak{a}$ ein Ideal, so ist $\pi^{-1}(\mathfrak{b}) \subset A$ ein Ideal. Nach Voraussetzung ist $\pi^{-1}(\mathfrak{b})$ endlich erzeugt, also $\pi^{-1}(\mathfrak{b}) = (a_1, \ldots, a_m)$ für geeignete $a_1, \ldots, a_m \in A$. Man rechnet leicht nach, dass dann $\mathfrak{b} = \big(\pi(a_1), \ldots, \pi(a_m)\big)$ gilt. Also ist $\mathfrak{b}$ endlich erzeugt. □

Definition 2.6 Sei A ein Ring. Ein $\mathbf{A-Modul}$ M ist eine Menge mit einer Verknüpfung $+$ und einer Abbildung (skalare Multiplikation)

$$A \times M \to M,$$

$$(a, m) \mapsto am$$

so dass folgende Bedingungen gelten:

i) $(M, +)$ ist eine abelsche Gruppe.

ii) $a(x + y) = ax + ay$ für $a \in A, x, y \in M$

iii) $(a + b)x = ax + bx$ für $a, b \in A, x \in M$

iv) $(ab)x = a(bx)$ für $a, b \in A, x \in M$

v) $1x = x$ für $x \in M$.

Beispiele:

i) Jedes Ideal $\mathfrak{a} \subset A$ ist ein $A-$Modul. Insbesondere ist A selbst ein $A-$Modul.

ii) Ist $A = k$ ein Körper, so sind die $A-$Moduln genau die $k-$Vektorräume.

iii) Die $\mathbb{Z}-$Moduln sind genau die abelschen Gruppen, wobei wir auf einer abelschen Gruppe die skalare Multiplikation mit $\mathbb{Z}$ so definieren:

$$ma = \begin{cases} \underbrace{a + \ldots + a}_{m-\text{mal}} & , \text{ falls } m > 0 \\ 0 & , \text{falls } m = 0 \\ \underbrace{-a - \ldots - a}_{(-m)-\text{mal}} & , \text{ falls } m < 0 \end{cases}$$

Eine Abbildung $f : M \to N$ zwischen zwei $A-$Moduln heißt **Homomorphismus** von $A-$Moduln, falls

$$f(x + y) = f(x) + f(y) \text{ und}$$
$$f(ax) = af(x)$$

für alle $a \in A,\ x, y \in M$ gilt.

Eine Teilmenge $N \subset M$ heißt **Untermodul**, falls N eine Untergruppe von M ist, die abgeschlossen unter der $A-$Multiplikation ist.

Beispiel: Ist $f : M \to N$ ein Homomorphismus, so ist Kern $f = \{x \in M : f(x) = 0\}$ ein Untermodul von M und Bild $f = \{y \in N :$ es gibt ein $x \in M$ mit $f(x) = y\}$ ein Untermodul von N.

Ist $N \subset M$ ein Untermodul, so existiert die Faktorgruppe M/N. Auf dieser können wir durch

$$A \times M/N \to M/N$$
$$(a, x + N) \mapsto ax + N$$

eine skalare Multiplikation definieren, die M/N zu einem $A-$Modul macht. Die natürliche Abbildung

$$\pi : M \to M/N$$
$$x \to x + N$$

ist ein surjektiver Homomorphismus von $A-$Moduln mit kern $\pi = N$.

Ein $A-$Modul M heißt **endlich erzeugt**, falls es Elemente $x_1, \ldots, x_n$ in M gibt, so dass sich jedes $x \in M$ als Linearkombination

$$x = \sum_{i=1}^{n} a_i x_i$$

mit geeigneten $a_1, \ldots, a_n \in A$ darstellen lässt. Die Koeffizienten $a_1, \ldots, a_n$ sind natürlich im allgemeinen nicht eindeutig bestimmt.

Ist I eine beliebige Indexmenge und ist M_i für alle $i \in I$ ein $A-$Modul, so wird die **direkte Summe**

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i, \text{fast alle } m_i = 0\}$$

der abelschen Gruppen M_i zusammen mit der skalaren Multiplikation

$$a(m_i)_{i \in I} = (am_i)_{i \in I}$$

ein $A-$Modul. Wir nennen einen $A-$Modul M, der isomorph zu $\bigoplus_{i \in I} A$ für eine beliebige Indexmenge I ist, einen **freien A$-$Modul**. Ist I eine endliche Menge mit n Elementen, so ist $M \simeq A \oplus \ldots \oplus A = A^n$. In diesem Fall gibt es ein Erzeugendensystem $x_1, \ldots, x_n$ von M, so dass jedes $x \in M$ eine Darstellung der Form $x = a_1 x_1 + \cdots + a_n x_n$ mit eindeutig bestimmten $a_1, \ldots, a_n$ besitzt.

Proposition 2.7 Sei M ein $A-$Modul. M ist genau dann endlich erzeugt, wenn M isomorph zu einem Quotienten von A^n für ein $n > 0$ ist, d.h. wenn es einen surjektiven $A-$Modul-Homomorphismus $\varphi : A^n \to M$ gibt.

Beweis : „$\Rightarrow$:“ Es sei $x_1, \ldots, x_n$ ein Erzeugendensystem von $\mathcal{M}$. Wir definieren einen $A-$Modul-Homomorphismus

$$\varphi : A^n \to M$$

durch $\varphi(a_1, \ldots, a_n) = a_1 x_1 + \ldots + a_n x_n$. Dann ist φ surjektiv, also folgt $M \simeq A^n/\text{Kern } \varphi$.
„$\Leftarrow$“: Sei $\varphi : A^n \to M$ ein surjektiver $A-$Modul-Homomorphismus. Wir bezeichnen mit $e_i = (0 \ldots 0\, 1\, 0 \ldots 0)$ den $i-$ten Einheitsvektor in A^n. Da φ surjektiv ist, wird M von $\varphi(e_1), \ldots, \varphi(e_n)$ erzeugt. □

Jetzt können wir eine wichtige Tatsache zeigen, die der Schlüssel zum Hilbertschen Basissatz ist.

Satz 2.8 Sei A ein noetherscher Ring und M ein endlich erzeugter $A-$Modul. Dann ist jeder Untermodul von M ebenfalls endlich erzeugt.

Beweis : Da M endlich erzeugt ist, gibt es nach Proposition 2.7 einen surjektiven Homomorphismus $\varphi : A^n \to M$ für ein $n > 0$. Sei $N \subset M$ ein Untermodul. Dann ist $\varphi^{-1}(N)$ ein Untermodul von A^n und $\varphi^{-1}(N) \to N$ ist ebenfalls surjektiv. Ist $\varphi^{-1}(N)$ endlich erzeugt, so ist also auch N endlich erzeugt. Daher genügt es zu zeigen, dass jeder Untermodul von A^n endlich erzeugt ist. Dies beweisen wir mit Induktion nach n. Für $n = 1$ sind die Untermoduln von A gerade die Ideale in A. Diese sind endlich erzeugt, da A ein noetherscher Ring ist. Die Behauptung gelte also für ein $n > 1$. Wir betrachten den surjektiven Homomorphismus

$$\varphi : A^{n+1} \to A^n$$

$$(a_1, \ldots, a_{n+1}) \mapsto (a_1, \ldots, a_n)$$

und den injektiven Homomorphismus

$$\psi : A \to A^{n+1}$$

$$a \mapsto (0, \ldots, 0, a).$$

Dann ist offenbar Kern $\varphi =$ Bild ψ. Also ist die Sequenz

$$0 \to A \xrightarrow{\psi} A^{n+1} \xrightarrow{\varphi} A^n \to 0$$

exakt.
Sei $N \subset A^{n+1}$ ein Untermodul. Nach Induktionsvoraussetzung ist $\psi^{-1}(N)$ als Untermodul von A und $\varphi(N)$ als Untermodul von A^n endlich erzeugt.

Wir wählen ein Erzeugendensystem $x_1, \ldots, x_r$ von $\psi^{-1}(N)$ und Elemente $y_1, \ldots, y_s \in N$, so dass $\varphi(y_1), \ldots, \varphi(y_s)$ ein Erzeugendensystem von $\varphi(N)$ ist. Jetzt sei $x \in N$ ein beliebiges Element. Dann ist $\varphi(x) \in \varphi(N)$, also von der Form $\varphi(x) = b_1\varphi(y_1) + \ldots + b_s\varphi(y_s)$ für $b_1, \ldots, b_s \in A$. Daher ist $x' = x - (b_1y_1 + \ldots + b_sy_s)$ in Kern $\varphi =$ Bild ψ enthalten, also gilt $x' = \psi(x'')$ für ein $x'' \in A$. Da x' in N liegt, liegt $x'' \in \psi^{-1}(N)$. Somit ist x'' von der Form $x'' = a_1x_1 + \ldots + a_rx_r$ für $a_1, \ldots, a_r \in A$. Insgesamt folgt

$$x = a_1\psi(x_1) + \ldots + a_r\psi(x_r) + b_1y_1 + \ldots + b_sy_s.$$

Daher ist $\psi(x_1), \ldots, \psi(x_r), y_1, \ldots, y_s$ ein Erzeugendensystem von N, d.h. N ist endlich erzeugt.

□

Ein $A-$Modul, der die Eigenschaft hat, dass alle seine Untermoduln endlich erzeugte $A-$Moduln sind, heißt **noetherscher A−Modul**.

Satz 2.8 lässt sich also auch so umformulieren: Ein endlich erzeugter Modul über einem noetherschen Ring A ist noethersch. Insbesondere ist ein noetherscher Ring A auch als Modul über sich selbst noethersch.

Jetzt können wir den Hilbertschen Basissatz beweisen.

Satz 2.9 (Hilbert'scher Basissatz)
Ist A ein noetherscher Ring, so ist auch der Polynomring $A[X]$ noethersch.

Beweis : Es sei $\mathfrak{a} \subset A[X]$ ein Ideal. Wir wollen zeigen, dass $\mathfrak{a}$ endlich erzeugt ist. Dafür können wir $\mathfrak{a} \neq 0$ annehmen. Nun betrachten wir die Menge aller Leitkoeffizienten von Elementen in $\mathfrak{a}$:

$$\mathfrak{b} = \{a \in A : a \neq 0 \text{ und } aX^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathfrak{a}\} \cup \{0\}.$$

$\mathfrak{b}$ ist ein Ideal in A, also nach Voraussetzung endlich erzeugt. Ist $\mathfrak{b} = (a_1, \ldots, a_m)$ mit $a_i \neq 0$ aus A, so gibt es für alle i ein Polynom: $f_i(X) \in \mathfrak{a}$, dessen Leitkoeffizient a_i ist. Wir bezeichnen den Grad von $f_i(X)$ mit r_i. Wir betrachten das Ideal $\mathfrak{a}' = (f_1, \ldots, f_m)$ in $A[X]$. Offenbar ist $\mathfrak{a}' \subset \mathfrak{a}$.
Es sei r das Maximum der Grade $r_1, \ldots, r_m$. Ferner bezeichnen wir mit M den $A-$Untermodul aller Polynome vom Grad $\leqq r-1$ in $A[X]$. Er wird erzeugt von den Polynomen $1, x, x^2, \ldots, x^{r-1}$. Wir zeigen nun $\mathfrak{a} = \mathfrak{a}' + (\mathfrak{a} \cap M)$. Die Inklusion „$\supset$" ist klar. Um „$\subset$" zu zeigen, betrachten wir ein beliebiges Polynom $f(X) = \alpha X^n + \ldots + \alpha_0$ in $\mathfrak{a}$. Ist $n < r$, so ist $f \in M$ und wir sind fertig. Ist $n \geqq r$, so schreiben wir den Leitkoeffizienten $\alpha \in \mathfrak{b}$ als $\alpha = c_1 a_1 + \ldots + c_m a_m$ für geeignete $c_1, \ldots, c_m \in A$. Das Polynom $h_1(X) = \sum_{i=1}^{n} c_i X^{\overbrace{n-r_i}^{\geqq 0}} f_i$ liegt in $\mathfrak{a}'$. Wir betrachten $g_1(X) = f(X) - h_1(X) \in \mathfrak{a}$. Der Koeffizient vor X^n von $g_1(X)$ ist $\alpha - \sum_{i=1}^{n} c_i a_i = 0$, also hat g_1 einen Grad $\leq n-1$. Ist grad $(g_1) < r$, so liegt g_1 in $\mathfrak{a} \cap M$ und wir erhalten $f \in \mathfrak{a}' + (\mathfrak{a} \cap \mathcal{M})$. Andernfalls wiederholen wir das obige Verfahren mit $g_1(X)$ und konstruieren ein Polynom $h_2(X) \in \mathfrak{a}'$, so dass der Grad von $g_1(X) - h_1(X)$ echt kleiner als der Grad von $g_1(X)$

ist. Nach endlich vielen Schritten erhalten wir so ein Polynom in $\mathfrak{a} \cap M$, und es folgt $f \in \mathfrak{a}' + (\mathfrak{a} \cap M)$.

Nun ist $(\mathfrak{a} \cap M)$ als Untermodul des endlich erzeugten $A-$Moduls M nach Satz 2.8 selbst ein endlich erzeugter $A-$Modul. Als Summe von zwei endlich erzeugten $A-$Moduln ist somit $\mathfrak{a}$ endlich erzeugt. □

Korollar 2.10 Ist A ein noetherscher Ring, so ist für jedes $n \geq 1$ der Polynomring $A[X_1, \ldots, X_n]$ noethersch.

Beweis : Das folgt mit Induktion aus Satz 2.9, da $A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$ gilt. □

3 Der Hilbert'sche Nullstellensatz

Wir wollen nun Nullstellenmengen von Polynomen über algebraisch abgeschlossenen Körpern studieren.

Es sei K ein **algebraisch abgeschlossener** Körper, d.h. jedes nicht-konstante Polynom $f \in K[X]$ hat eine Nullstelle in K. Das kann man auch so ausdrücken: K hat keinen echten algebraischen Erweiterungskörper.

Beispiel: $\mathbb{C}$ ist ein algebraisch abgeschlossener Körper.

Mit $A = K[X_1, ..., X_n]$ bezeichnen wir den **Polynomring in** n **Variablen über** K. Ferner definieren wir den n-dimensionalen affinen Raum über K als

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

$\mathbb{A}^n(K)$ ist also der Vektorraum der n-dimensionalen Zeilenvektoren über K.
Ist $P = (P_1, ..., P_n)$ ein Punkt des $\mathbb{A}^n(K)$ und $f \in A = K[X_1, ..., X_n]$, so ist $f(P) = f(P_1, ..., P_n) \in K$. Ist $f(P) = 0$, so nennen wir P **Nullstelle von** f.

Definition 3.1 Es sei $T \subset A$ eine beliebige Menge von Polynomen. Die **Nullstellenmenge** von T ist definiert als

$$V(T) = \{P \in \mathbb{A}^n(K) : f(P) = 0 \text{ für alle } f \in T\}.$$

Mit Hilfe des Hilbert'schen Basissatzes können wir zeigen, dass für die Beschreibung von $V(T)$ endlich viele Polynome ausreichen. Wir bezeichnen mit (T) das von T erzeugte Ideal in A, es gilt also

$$(T) = \{f_1 t_1 + ... + f_n t_n : f_1, ..., f_n \in A, t_1, ..., t_n \in T, n \geqq 0\}.$$

Man prüft leicht, dass (T) das kleinste Ideal in A ist, das T enthält.

Offenbar gilt $V(T) = V((T))$, d.h. die Nullstellenmenge von T stimmt mit der Nullstellenmenge des von T erzeugten Ideals überein. Nach dem Hilbert'schen Basissatz 2.9 ist A noethersch, also ist (T) endlich erzeugt. Ist $(T) = (t_1, ..., t_n)$, so gilt

$$V(T) = V((T)) = \{P \in \mathbb{A}^n(K) : t_1(P) = ... = t_n(P) = 0\}.$$

Also ist $V(T)$ die Nullstellenmenge einer endlichen Teilmenge von A.

Definition 3.2 Eine Teilmenge $Y \subset \mathbb{A}^n(K)$ heißt **algebraische Menge**, wenn es ein Ideal $\mathfrak{a} \subset A$ gibt mit $V(\mathfrak{a}) = Y$.

Lemma 3.3 Es sei I eine beliebige Indexmenge. Dann gilt für Ideale $\mathfrak{a}, \mathfrak{b}, (\mathfrak{a}_i)(i \in I)$:

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

ii) Ist $\mathfrak{a} \subset \mathfrak{b}$, so folgt $V(\mathfrak{b}) \subset V(\mathfrak{a})$

iii) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$

iv) $V(\sum\limits_{i \in I} \mathfrak{a}_i) = \bigcap\limits_{i \in I} V(\mathfrak{a}_i)$.

Hier ist die Summe $\sum\limits_{i \in I} \mathfrak{a}_i$ der Ideale $\mathfrak{a}_i$ definiert als

$$\sum_{i \in I} \mathfrak{a}_i = \{a_{i_1} + ... + a_{i_m} : m \geqq 0, \{i_1, ..., i_m\} \subset I, a_{i_1} \in \mathfrak{a}_{i_1}, ..., a_{i_m} \in \mathfrak{a}_{i_m}\}$$

Beweis :

i) Das Nullpolynom verschwindet auf ganz $\mathbb{A}^n(K)$ und es gibt keinen Punkt $P \in \mathbb{A}^n(K)$, der Nullstelle eines jeden Polynoms ist.

ii) Folgt sofort aus der Definition von $V(\mathfrak{a})$.

iii) „$\subset$“: Angenommen, $P \in \mathbb{A}^n(K)$ ist weder in $V(\mathfrak{a})$ noch in $V(\mathfrak{b})$ enthalten. Dann gibt es ein $f \in \mathfrak{a}$ mit $f(P) \neq 0$ und ein $g \in \mathfrak{b}$ mit $g(P) \neq 0$. Also ist $fg \in \mathfrak{a} \cap \mathfrak{b}$ ein Polynom mit $fg(P) \neq 0$, d.h. $P \notin V(\mathfrak{a} \cap \mathfrak{b})$.

„$\supset$“: Folgt wegen $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$ und $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$ aus ii).

iv) „$\subset$“: Da $\mathfrak{a}_j \subset \sum_{i \in I} \mathfrak{a}_i$ für alle $j \in I$ gilt, folgt dies aus ii).

„$\supset$“: Ist $P \in \bigcap_{i \in I} V(\mathfrak{a}_i)$, so gilt $f(P) = 0$ für alle $f \in \mathfrak{a}_i$ und alle $i \in I$. Dann ist aber auch $f(P) = 0$ für alle $f \in \sum_{i \in I} \mathfrak{a}_i$, d.h. es gilt $P \in V(\sum_{i \in I} \mathfrak{a}_i)$.

□

Wir nennen eine Teilmenge $U \subset \mathbb{A}^n(K)$ **offen**, wenn das Komplement von U eine abgebraische Menge ist, d.h. wenn $\mathbb{A}^n(K) \backslash U = V(\mathfrak{a})$ für ein Ideal $\mathfrak{a} \subset A$ gilt.

Lemma 3.3 besagt dann:

- $\mathbb{A}^n(K)$ und $\emptyset$ sind offen in $\mathbb{A}^n(K)$.
- Der Schnitt von zwei offenen Mengen ist offen.
- Die Vereinigung von beliebig vielen offenen Mengen ist offen.

Wir erhalten mit diesem Begriff offener Mengen also eine Topologie auf $\mathbb{A}^n(K)$. Diese heißt **Zariski-Topologie**.

Vorsicht: Trägt K eine Topologie, wie etwa im Fall $K = \mathbb{C}$, so erbt auch der Raum der Zeilenvektoren $\mathbb{A}^n(K)$ eine Topologie. Dies ist aber eine ganz andere als die Zariski-Topologie. Die Zariski-Topologie ist recht grob, wie das folgende Beispiel zeigt.

Beispiel: Ist $n = 1$, also $A = K[X]$, so ist jedes Ideal in A ein Hauptideal. Also sind alle algebraischen Mengen in $\mathbb{A}^1(K)$ von der Form $V(f)$ für ein $f \in K[X]$. Daher ist $U \subset \mathbb{A}^1(K)$ offen genau dann, wenn es ein $f \in K[X]$ gibt mit

$$U = \{P \in \mathbb{A}^1(K) : f(P) \neq 0\}.$$

Also sind die offenen Mengen genau die Teilmengen von $\mathbb{A}^n(K)$, deren Komplement endlich ist, plus die leere Menge.

Definition 3.4 Ist $X \subset \mathbb{A}^n(K)$ eine beliebige Teilmenge, so definieren wir

$$I(X) = \{f \in A : f(P) = 0 \text{ für alle } P \in X\}.$$

Die Teilmenge $I(X) \subset A$ ist ein Ideal in A, wie man leicht nachrechnet.

Lemma 3.5 Es seien X und Y Teilmengen von $\mathbb{A}^n(K)$

i) Ist $X \subset Y$, so folgt $I(Y) \subset I(X)$.

ii) Es gilt $X \subset V(I(X))$. Ist X eine algebraische Menge, so gilt sogar $X = V(I(X))$.

iii) Ist $\mathfrak{a} \subset A$ ein Ideal, so gilt $\mathfrak{a} \subset I(V(\mathfrak{a}))$.

Beweis :

i) und iii) folgen sofort aus den Definitionen

ii) $X \subset V(I(X))$ ist klar. Ist $X = V(\mathfrak{a})$ eine algebraische Menge, so ist nach iii) $\mathfrak{a} \subset I(V(\mathfrak{a})) = I(X)$, also mit Lemma 3.3 ii) $V(I(X)) \subset V(\mathfrak{a}) = X$.

□

Im allgemeinen ist die Inklusion $\mathfrak{a} \subset I(V(\mathfrak{a}))$ aus Lemma 3.5 iii) eine echte Inklusion. So gilt etwa für das Ideal $\mathfrak{a} = (X^2) \subset K[X]$, dass

$$V(\mathfrak{a}) = \{P \in K : P^2 = 0\} = \{0\}$$

ist, woraus

$$I(V(\mathfrak{a})) = \{a_1X + ... + a_nX^n : a_1, ..., a_n \in K, n \geqq 1\} = (X)$$

folgt.

Mit Hilfe des Hilbert'schen Nullstellensatzes werden wir später $I(V(\mathfrak{a}))$ bestimmen. Dafür brauchen wir folgenden Begriff:

Definition 3.6 Ist $\mathfrak{a}$ ein Ideal in einem beliebigen Ring A, so ist das **Radikal** von $\mathfrak{a}$ definiert als

$$\sqrt{\mathfrak{a}} = \{f \in A : \text{es gibt ein } k \geqq 1 \text{ mit } f^k \in \mathfrak{a}\}.$$

Offenbar gilt also $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$. Das Radikal von $\mathfrak{a}$ ist ein Ideal (Übungsaufgabe).

Beispiel: Für das Ideal $(X^2) \subset K[X]$ gilt $\sqrt{(X^2)} = (X)$.

Wir wollen später zeigen, dass allgemein $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ gilt. Dazu brauchen wir ein paar algebraische Vorarbeiten.

Lemma 3.7 Es seien $C \subset B \subset A$ Ringe.

i) Ist A ein endlich erzeugter B-Modul und B ein endlich erzeugter C-Modul, so ist A ein endlich erzeugter C-Modul.

ii) Ist A ein endlich erzeugter B-Modul, so ist A **ganz über** B, d.h. jedes Element $x \in A$ erfüllt eine Gleichung der Form

$$x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0 = 0$$

für geeignete $b_0, ..., b_{n-1} \in B$.

iii) Erfüllt umgekehrt ein $x \in A$ eine Gleichung der obigen Form, so ist

$$B[x] := \{b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0 : b_0, ..., b_n \in B, n \geqq 0\}$$

ein endlich erzeugter B-Modul.

Beweis :

i) Ist $(a_1, ..., a_m)$ ein Erzeugendensystem von A als B-Modul und $(b_1, ..., b_n)$ ein Erzeugendensystem von B als C-Modul, so hat jedes $a \in A$ eine Darstellung als $a = \beta_1 a_1 + ... + \beta_m a_m$ mit geeigneten $\beta_i \in B$. Diese können wir schreiben als $\beta_i = \gamma_{i_1} b_1 + ... + \gamma_{i_n} b_n$ mit geeigneten $\gamma_{i_j} \in C$. Setzen wir diese Ausdrücke in die Gleichung für a ein, so sehen wir, dass $(a_i b_j)_{\substack{i=1,...,m \\ j=1,...,n}}$ ein Erzeugendensystem von A als C-Modul ist.

ii) Es sei $(a_1, ..., a_m)$ ein Erzeugendensystem von A als B-Modul. Ist $x \in A$, so ist auch $xa_i \in A$, also gibt es Elemente $b_{i_j} \in B$ mit

$$xa_i = b_{i_1}a_i + ... + b_{i_m}a_m \quad \text{für alle } i = 1, ..., m.$$

Also gilt $\sum_{j=1}^{m} (x\delta_{ij} - b_{ij})a_j = 0$.

Wir betrachten nun die $(m \times m)$-Matrix $M = (x\delta_{ij} - b_{ij})_{i,j=1,...,m}$. Es ist $M \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = 0$. Ist M^{adj} die zu M adjungierte Matrix, so gilt

$$M^{adj}M = \text{det}M \cdot E_m,$$

also auch

$$0 = M^{adj}M \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \text{det}M \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix},$$

woraus

$$(\text{det}M) \cdot a_i = 0 \text{ für } i = 1, ..., m \text{ folgt.}$$

Nun lässt sich das Element $1 \in A$ linear aus den Erzeugern $a_i, ..., a_m$ kombinieren, woraus $\text{det}M = \text{det}M \cdot 1 = 0$ in A folgt. Rechnen wir $\text{det}M$ aus, so stellen wir fest, dass $\text{det}M$ ein normiertes Polynom in x mit Koeffizienten in B ist, d.h. es gilt

$$0 = \text{det}M = x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0$$

für geeignete $b_0, ..., b_{n-1} \in B$.

iii) Gilt $x^n = -b_{n-1}x^{n-1} - ... - b_1x - x_0$, so ist $B[x]$ als B-Modul von $1, x, x^2, ..., x^{n-1}$ erzeugt.

□

Lemma 3.8 (Lemma von Nakayama) Es seien $B \subset A$ Ringe, so dass $A \neq 0$ ein endlich erzeugter B-Modul ist. Dann gilt für jedes maximale Ideal $\mathfrak{m}$ von B, dass $\mathfrak{m}A \neq A$ ist. Hier ist $\mathfrak{m}A = \{\sum_{i=1}^{n} m_i x_i : n \geqq 1, m_i \in \mathfrak{m}, x_i \in A\}$ das von $\mathfrak{m}$ in A erzeugte Ideal.

Beweis : Angenommen, es gilt $\mathfrak{m}A = A$. Es sei $(a_1, ..., a_m)$ ein Erzeugendensystem von A als B-Modul. Da $a_i \in A = \mathfrak{m}A$ ist, gibt es Elemente $b_{i_j} \in \mathfrak{m}$ mit

$$a_i = b_{i_1} a_1 + ... + b_{i_m} a_m \quad \text{für alle } i = 1, ..., m.$$

Wie im Beweis von 3.7 ii) betrachten wir die Matrix $M = (\delta_{ij} - b_{ij})_{i,j=1,...,m}$ und schließen $\det M = 0$. Rechnen wir $\det M$ aus, so stellen wir fest, dass

$$\det M = 1 + b \quad \text{für ein } b \in \mathfrak{m} \text{ gilt.}$$

Also ist $1 \in \mathfrak{m}$ im Widerspruch zu der Tatsache, dass $\mathfrak{m}$ ein maximales Ideal ist. □

Das Lemma von Nakayama gilt auch allgemeiner für beliebige endlich erzeugte B-Moduln, die nicht unbedingt Ringe sein müssen. Dazu muss man den obigen Beweis etwas modifizieren.

Lemma 3.9 Es sei A ein Körper und $B \subset A$ ein Unterring, so dass A ein endlich erzeugter B-Modul ist. Dann ist auch B ein Körper.

Beweis : Es sei $b \neq 0$ ein Element von B. Da A ein Körper ist, existiert $b^{-1} \in A$. Wir müssen zeigen, dass b^{-1} bereits in B liegt. Nach Lemma 3.7 ii) erfüllt b^{-1} eine Gleichung der Form

$$b^{-n} + b_{n-1} b^{-(n-1)} + ... + b_1 b^{-1} + b_0 = 0$$

für geeignete $b_0, ..., b_{n-1} \in B$.
Nach Multiplikation mit b^{n-1} ergibt sich

$$b^{-1} = -b_{n-1} - ... - b_1 b^{n-2} + b_0 b^{n-1} \in B.$$

□

Wir erinnern jetzt noch an den Begriff einer Algebra über einem Ring B. Ein B-Modul A, der gleichzeitig ein Ring ist, so dass noch

$$b(fg) = (bf)g = g(bf)$$

für alle $b \in B$ und $f, g \in A$ gilt, heißt **B-Algebra** (genauer gesagt: kommutative B-Algebra mit 1).

Beispiel: Der Polynomring $B[X_1, ..., X_n]$ ist eine B-Algebra.

Allgemeiner gilt für jeden Ring A und jeden Unterring $B \subset A$, dass A eine B-Algebra ist.

Definition 3.10 Eine B-Algebra A heißt **endlich erzeugt** (genauer gesagt: endlich erzeugt als B-Algebra), wenn es endlich viele Elemente $b_1, ..., b_n \in B$ gibt, so dass sich jedes $b \in B$ als Polynom in den b_i schreiben lässt. Mit anderen Worten, für jedes $b \in B$ gibt es ein $f \in B[X_1, ..., X_n]$ mit $b = f(b_1, ..., b_n)$.

Beispiel: Ist $\mathfrak{a} \subset B[X_1, ..., X_n]$ ein Ideal, so ist die B-Algebra $B[X_1, ..., X_n]/\mathfrak{a}$ endlich erzeugt.

Eine B-Algebra A trägt insbesondere die Struktur eines B-Moduls. Ist A als B-Modul endlich erzeugt, so ist A auch als B-Algebra endlich erzeugt. Die Umkehrung gilt allerdings nicht! Der Polynomring $A = B[X_1, ..., X_n]$ ist etwa als B-Modul nicht endlich erzeugt, wohl aber als B-Algebra.

Satz 3.11 (Noether-Normalisierung) Es sei K ein unendlicher Körper und A eine von $(a_1, ..., a_n)$ erzeugte K-Algebra. Dann gibt es eine Zahl m mit $0 \leqq m \leqq n$ und Elemente $y_1, ..., y_m \in A$, so dass gilt:

i) $(y_1, ..., y_m)$ sind **algebraisch unabhängig** über K, d.h. es gibt kein Polynom $0 \neq f \in K[X_1, ..., X_m]$ mit $f(y_1, ..., y_m) = 0$ in A.

ii) A ist ein endlich erzeugter $K[y_1, ..., y_m]$-Modul, wobei $K[y_1, ..., y_m] = \{a \in A :$ es gibt ein Polynom $h \in K[X_1, ..., X_m]$ mit $a = h(y_1, ..., y_m)\}$ ist.

Bemerkung: Die Bedingung, dass $(y_1, .., y_m)$ algebraisch unabhängig über K sind, bedeutet, dass der natürliche Homomorphismus

$$\begin{aligned} \varphi : K[X_1, ..., X_m] &\to A \\ f &\mapsto f(y_1, ..., y_m) \end{aligned}$$

injektiv ist. Sein Bild ist definitionsgemäß gerade $K[y_1, ..., y_m]$. Also gilt $K[y_1, ..., y_m] \simeq K[X_1, ..., X_m]$, d.h. $K[y_1, ..., y_m]$ ist isomorph zu dem Polynomring in m Variablen über K.

Beweis : Wir betrachten den Homomorphismus von $K-$Algebren

$$\psi : K[X_1, ..., X_n] \to A$$
$$f \mapsto f(a_1, ..., a_n).$$

Da A als K-Algebra von $(a_1, ..., a_n)$ erzeugt wird, ist ψ surjektiv. Es sei $\mathfrak{a} = \text{Kern}\psi$. Ist $\mathfrak{a} = 0$, so können wir $y_1 = a_1, ..., y_n = a_n$ und $m = n$ wählen und haben die Behauptung bewiesen. Also nehmen wir $\mathfrak{a} \neq 0$ an.
Ist $n = 1$, so ist $\mathfrak{a} = (f)$ ein Haupideal in $K[X]$. Wir können den Erzeuger f normiert wählen. Es gilt $f(a_1) = 0$. Nach Lemma 3.7 iii) ist also $A = K[a_1]$ ein endlich erzeugter K-Modul, und wir können $m = 0$ wählen und haben die Behauptung bewiesen.

Also können wir per Inklusion annehmen, dass die Behauptung für K-Algebren A mit $\leqq (n-1)$ Erzeugern bewiesen ist. Wir wählen ein $f \neq 0$ in $\mathfrak{a}$. Ist $d = \deg f$ der Grad von f, so können wir f schreiben als $f = F_d + G$ mit einem homogenen Polynom F_d vom Grad d und einem Polynom G vom Grad $\leqq d-1$. Das Polynom F_d ist also eine Summe von Monomen der Form $cX_1^{i_1} \cdot ... \cdot X_n^{i_n}$ mit $i_1 + ... + i_n = d$ und $c \in K$.
Da K ein unendlicher Körper ist, gibt es Elemente $\gamma_1, ..., \gamma_{n-1} \in K$ mit $F_d(\gamma_1, ..., \gamma_{n-1}, 1) \neq 0$, denn $F_d(X_1, ..., X_{n-1}, 1)$ ist ein Polynom $\neq 0$ in $K[X_1, ..., X_{n-1}]$ (Übungsaufgabe).

Also gilt für $a_1' = a_1 - \gamma_1 a_n, ..., a_{n-1}' = a_{n-1} - \gamma_{n-1} a_n$ die Gleichung

$$0 = f(a_1, ..., a_n) = f(a_1' + \gamma_1 a_n, ..., a_{n-1}' + \gamma_{n-1} a_n, a_n) =$$
$$F_d(a_1' + \gamma_1 a_n, ..., a_{n-1}' + \gamma_{n-1} a_n, a_n) + G(a_1' + \gamma_1 a_n, ..., a_1' + \gamma_{n-1} a_n, a_n).$$

Diese beiden Summanden wollen wir als Polynome in der Variablen a_n mit Koeffizienten im Ring $K[a_1', ..., a_{n-1}']$ betrachten. Da $\deg G \leqq d-1$ ist, hat der zweite Summand einen Grad $\leqq d-1$ in a_n. Der erste Summand ist eine Summe von Elementen der Form

$$c(a_1' + \gamma_1 a_n)^{i_1} \ ... \ (a_{n-1}' + \gamma_n a_n)^{i_{n-1}} a_n^{i_n}$$

für $c \in K$ und $i_1 + ... + i_n = d$. Multiplizieren wir dies aus und ordnen nach Potenzen von a_n, so stellen wir fest, dass der Faktor vor a_n^d gerade $c\gamma_1^{i_1} \ ... \ \gamma_{n-1}^{i_{n-1}}$ ist.

Also gilt

$$F_d(a'_1 + \gamma_1 a_n, ..., a'_{n-1} + \gamma_{n-1} a_n, a_n) =$$

$$F_d(\gamma_1, ..., \gamma_{n-1}, 1) a_n^d + \text{ Terme kleinerer Ordnung in } a_n.$$

Da $F_d(\gamma_1, ..., \gamma_{n-1}, 1) \neq 0$ ist, haben wir somit ein normiertes Polynom mit Koeffizienten in $K[a'_1, ..., a'_{n-1}]$ gefunden, das in a_n verschwindet.
Nach Lemma 3.7 iii) ist $(K[a'_1, ..., a'_{n-1}])[a_n]$ also ein endlich erzeugter $K[a'_1, ..., a'_{n-1}]$-Modul. Da A als K-Algebra von $(a_1, ..., a_n)$ erzeugt wird, ist auch $(a'_1, ..., a'_{n-1}, a_n)$ ein Erzeugendensystem von A als K-Algebra. Also gilt $A = K[a'_1, ..., a'_{n-1}][a_n]$. Nach Induktionsvoraussetzung gibt es ferner Elemente $y_1, ..., y_m$ mit $0 \leqq m \leqq n-1$, die algebraisch über K sind, so dass $K[a'_1, ..., a'_{n-1}]$ ein endlich erzeugter $K[y_1, ..., y_m]$-Modul ist. Nach Lemma 3.7 i) ist dann auch A ein endlich erzeugter $K[y_1, ..., y_m]$-Modul und die Behauptung ist bewiesen. □

Jetzt können wir folgende wichtige Konsequenz der Noether Normalisierung zeigen.

Satz 3.12 Es sei K ein unendlicher Körper und L ein Erweiterungskörper von K, der als K-Algebra endlich erzeugt ist. Dann ist L/K eine endliche Körpererweiterung, also insbesondere algebraisch.

Beweis : Wir wenden Noether Normalisierung (Satz 3.11) auf L an. Es gibt also Elemente $y_1, ..., y_m \in L$, die algebraisch unabhängig über K sind, da dass L ein endlicher $K[y_1, ..., y_m]$-Modul ist. Nach Lemma 3.9 ist $K[y_1, ..., y_m]$ ein Körper, also lässt sich jedes y_i^{-1} als Polynom in $y_1, ..., y_m$ schreiben. Multiplizieren wir diese Gleichung mit y_i, so erhalten wir ein Polynom $f \neq 0$ mit $f(y_1, ..., y_m) = 0$. Das widerspricht der algebraischen Unabhängigkeit, wenn $m \geqq 1$ ist. Also ist $m = 0$, d.h. L ist ein endlicher K-Modul, also eine endliche Erweiterung über K. □

Sowohl der Satz 3.11 von der Noether Normalisierung als auch Satz 3.12 gelten für beliebige, nicht notwendig unendliche Körper. Dann muss man sich im Beweis von 3.11 aber etwas mehr anstrengen.

Jetzt können wir diese algebraischen Resultate dazu benutzen, um etwas über algebraische Mengen herauszukommen.

Satz 3.13 (Hilbert'scher Nullstellensatz) Es sei K ein algebraisch abgeschlossener Körper. Dann gilt

i) Jedes maximale Ideal in $A = K[X_1, ..., X_n]$ ist von der Form $\mathfrak{m} = (X_1 - a_1, ..., X_n - a_n)$ für ein $P = (a_1, ..., a_n) \in \mathbb{A}^n(K)$.

ii) Ist $\mathfrak{a} \subset A$ ein Ideal mit $\mathfrak{a} \neq A$, so gilt $V(\mathfrak{a}) \neq \emptyset$.

iii) Für jedes Ideal $\mathfrak{a} \subset A$ gilt $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Beweis :

i) Ist $P = (a_1, ..., a_n) \in \mathbb{A}^n(K)$, so gilt $I(P) = (X_1 - a_1, ..., X_n - a_n)$ (Übungsaufgabe), also ist dieses Ideal der Kern der Auswertungsabbildung

$$\begin{aligned} \varphi : K[X_1, ..., X_n] &\to K \\ f &\mapsto f(a_1, ..., a_n). \end{aligned}$$

Somit ist $(X_1 - a_1, ..., X_n - a_n)$ ein maximales Ideal.

Sei umgekehrt $\mathfrak{m} \subset A$ ein maximales Ideal. Dann ist $L = K[X_1, ..., X_n]/\mathfrak{m}$ ein Körper und gleichzeitig eine endlich erzeugte K-Algebra. Nach Satz 3.12 ist L algebraisch über K. Also folgt $L = K$, da K algebraisch abgeschlossen ist. Somit ist

$$\psi : K \subset K[X_1, ..., X_n] \xrightarrow{\pi} K[X_1, ..., X_n]/\mathfrak{m}$$

ein Isomorphismus.
Wir betrachten $b_i = x_i + \mathfrak{m} \in K[X_1, ..., X_n]$ und setzen $a_i = \psi^{-1}(b_i)$. Dann ist $x_i - a_i \in$ Kern $\pi = \mathfrak{m}$. Also folgt $(x_1 - a_1, ..., x_n - a_n) \subset \mathfrak{m}$. Da $(x_1 - a_1, ..., x_n - a_n)$ ein maximales Ideal ist, gilt sogar $(x_1 - a_1, ..., x_n - a_n) = \mathfrak{m}$.

ii) Es sei $\mathfrak{a} \subsetneq A$ ein Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subset \mathfrak{m}$ (ÜA). Nach i) gilt $\mathfrak{m} = (x_1 - a_1, ..., x_n - a_n)$ für geeignete $a_1, ..., a_n \in K$, woraus $(a_1, ..., a_n) \in V(\mathfrak{a})$ folgt.

iii) Ist $f \in \sqrt{\mathfrak{a}}$, so ist $f^k \in \mathfrak{a}$ für ein $k \geqq 1$, also gilt nach Lemma 3.5 $f^k \in I(V(\mathfrak{a}))$, woraus $f \in I(V(\mathfrak{a}))$ folgt. Wir müssen also nur noch $I(V(\mathfrak{a})) \subset \sqrt{\mathfrak{a}}$ zeigen.

Sei $f \in I(V(\mathfrak{a}))$ gegeben. Ohne Einschränkung ist $f \neq 0$.
Wir wählen ein Erzeugendensystem $g_1, ..., g_r \in K[X_1, ..., X_n]$ des Ideals $\mathfrak{a}$. Wir nehmen nun eine zusätzliche Unbestimmte X_{n+1} hinzu und betrachten das Ideal $\mathfrak{b} = (g_1, ..., g_r, X_{n+1}f - 1)$ in $K[X_1, ..., X_n, X_{n+1}]$.
Angenommen $V(\mathfrak{b}) \neq \emptyset$. Dann gibt es ein Punkt $(a_1, ..., a_n, a_{n+1}) \in \mathbb{A}^{n+1}(K)$ mit $g_1(a_1, ..., a_n) = ... = g_r(a_1, ..., a_n) = 0$ und $a_{n+1}f(a_1, ..., a_n) = 1$.
Somit liegt $(a_1, ..., a_n)$ in $V(\mathfrak{a})$. Da $f \in I(V(\mathfrak{a})$ ist, folgt $f(a_1, ..., a_n) = 0$, was im Widerspruch zu $a_{n+1}f(a_1, ..., a_n) = 1$ steht.
Also ist $V(\mathfrak{b}) = \emptyset$. Mit ii) folgt daraus $b = K[X_1, ..., X_n, X_{n+1}]$. Also ist 1 eine Linearkombination von $g_1, ..., g_n, X_{n+1}f - 1$ mit Koeffizienten in $K[X_1, ..., X_n, X_{n+1}]$, d.h. es gilt

$$1 = \sum_{i=1}^{r} h_i g_i + h_0(X_{n+1}f - 1)$$

für geeignete $h_0, h_1, ..., h_r \in K[X_1, ..., X_n, X_{n+1}]$.

Da $f \neq 0$ ist, liegt $\frac{1}{f} \in \text{Quot}(K[X_1, ..., X_n])$ und es folgt

$$1 = \sum_{i=1}^{r} h_i(X_1, ..., X_n, \tfrac{1}{f}) g_i(X_1, ..., X_n)$$

in Quot$K[X_1, ..., X_n]$.
Es sei m der höchste Grad, mit dem X_{n+1} in einem der Polynome $h_1, ..., h_r$ auftaucht. Dann folgt nach Multiplikation mit f^m die Gleichung

$$f^m = \sum_{i=1}^{r} h_i(X_1, ..., X_n, \tfrac{1}{f}) f^m g_i.$$

Nun liegen die Elemente $h_i(X_1, ..., X_n, \frac{1}{f})f^m$ in $K[X_1, ..., X_n]$, also folgt

$$f^m \in (g_1, ..., g_r) \in \mathfrak{a} \quad \text{und damit } f \in \sqrt{\mathfrak{a}}.$$

□

Teil ii) des Hilbert'schen Nullstellensatzes (3.13) besagt, dass jedes Ideal $\neq (1)$ mindestens eine Nullstelle in $\mathbb{A}^n(K)$ besitzt. Die Voraussetzung, dass K algebraisch abgeschlossen ist, ist hier entscheidend. Sonst ist dies natürlich schon für Polynome mit einer Variable im allgemeinen falsch.

Der Hilbert'sche Nullstellensatz impliziert folgendes Lösbarkeitskriterium von Systemen polynomialer Gleichungen:

Korollar 3.14 Sei K ein algebraisch abgeschlossener Körper und $f_1, ..., f_r \in K[X_1, ..., X_n]$. Das System polynomialer Gleichungen

$$\begin{aligned} f_1(a_1, ..., a_n) &= 0 \\ &\vdots \\ f_r(a_1, ..., a_n) &= 0 \end{aligned}$$

ist genau dann unlösbar über K, wenn es Polynome $g_1, ..., g_r \in K[X_1, ..., X_n]$ gibt mit

$$g_1 f_1 + ... + g_r f_r = 1.$$

Beweis : Das System von polynomialen Gleichungen

$$f_1(a_1, ..., a_n) = f_2(a_1, ..., a_n) = ... = f_r(a_1, ..., a_n) = 0$$

ist genau dann unlösbar über K, wenn für das Ideal $\mathfrak{a} = (f_1, ..., f_r) \subset K[X_1, ..., X_n]$ gilt $V(\mathfrak{a}) = \emptyset$. Nach 3.13 ii) ist das äquivalent zu $\mathfrak{a} = K[X_1, ..., X_n]$, also zu einer Linearkombination der 1 mit Koeffizienten $g_1, ..., g_r \in K[X_1, ..., X_n]$. □

Definition 3.15 Ein Ideal $\mathfrak{a}$ in einem beliebigen Ring heißt Radikalideal, falls gilt

$$\sqrt{\mathfrak{a}} = \mathfrak{a}.$$

Für jedes Ideal $\mathfrak{b}$ ist $\sqrt{\mathfrak{b}}$ ein Radikalideal, denn es gilt

$$\sqrt{\sqrt{\mathfrak{b}}} = \sqrt{\mathfrak{b}} \text{ (Übungsaufgabe).}$$

Korollar 3.16 Sei K algebraisch abgeschlossen. Die Zuordnungen I und V liefern eine inklusionsumkehrende bijektive Korrespondenz

$$\left\{ \begin{array}{l} \text{algebraische} \\ \text{Mengen in } \mathbb{A}^n(K) \end{array} \right\} \begin{array}{c} \xrightarrow{I} \\ \xleftarrow[V]{} \end{array} \begin{array}{l} \{\text{Radikalideale} \\ \text{in } K[x_1 \dots x_n]\} \end{array}$$

Beweis : Nach Lemma 3.3 und Lemma 3.5 sind die Abbildungen I und V inklusionsumkehrend. Wir müssen noch zeigen, dass für jede algebraische Menge $X \subset \mathbb{A}^n(K)$ das Ideal $I(X)$ ein Radikalideal ist. Gilt $f^n \in I(X)$, so ist für jedes $P \in X$

$$f^n(P) = 0.$$

Daraus folgt $f(P) = 0$, also ist $f \in I(X)$. Somit gilt tatsächlich $\sqrt{I(V)} = I(V)$. Nach Lemma 3.5, ii) ist $X = V\big(I(X)\big)$, und nach dem Hilbertschen Nullstellensatz Satz 3.13 gilt für jedes Radikalideal $\mathfrak{a}$:

$$I\big(V(\mathfrak{a})\big) = \sqrt{\mathfrak{a}} = \mathfrak{a}.$$

Somit sind die Abbildungen I und V invers zueinander, also Bijektionen. □

4 Lokalisierung

Wir wollen zunächst Lokalisierungen von Ringen kennenlernen.

Definition 4.1 Sei A ein Ring (wie immer kommutativ mit 1) und $S \subset A$ eine multiplikative Teilmenge, d.h. es gilt $1 \in S$ und für $s, t \in S$ ist auch $st \in S$. Die **Lokalisierung** $S^{-1}A$ von A nach S ist dann definiert als der Quotient von $A \times S$ nach folgender Äquivalenzrelation

$$(a, s) \sim (b, t) \Leftrightarrow \text{ es gibt ein } u \in S \text{ mit } (at - bs)u = 0.$$

Hier müssen wir natürlich nachprüfen, dass die so definierte Relation wirklich eine Äquivalenzrelation ist. Reflexivität und Symmetrie sieht man sofort. Um die Transitivität zu zeigen, seien $(a, s) \sim (b, t)$ und $(b, t) \sim (c, w)$. Dann gibt es $u, v \in S$ mit $(at - bs)u = 0$ und $(bw - ct)v = 0$. Also ist auch $(aw - cs)tuv = (at - bs)uvw + (bw - ct)vus = 0$. Da S multiplikativ ist, liegt tuv in S, also folgt $(a, s) \sim (c, w)$.

$S^{-1}A$ ist also definiert als die Menge aller Äquivalenzklassen von $\sim$ in $A \times S$. Wir schreiben $a/s = \{(b, t) : (b, t) \sim (a, s)\} \in S^{-1}A$ für die Äquivalenzklasse von (a, s).

Wir definieren

$$\begin{aligned} a/s + b/t &= (at + bs)/st \quad \text{und} \\ a/s \cdot b/t &= ab/st. \end{aligned}$$

Man rechnet leicht nach, dass diese Verknüpfungen $+$ und $\cdot$ auf $S^{-1}A$ wohldefiniert, d.h. unabhänging von der Wahl des Vertreters der Äquivalenzklasse sind. Zusammen mit diesen Verknüpfungen wird $S^{-1}A$ zu einem kommutativen Ring. (Übungsaufgabe).

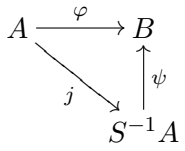
Die Abbildung $j : A \to S^{-1}A$, gegeben durch $j(a) = a/1$ ist ein Ringhomomorphismus. Im allgemeinen ist j weder injektiv noch surjektiv. Für jedes $s \in S$ existiert in $S^{-1}A$ das Inverse $1/s$ von $j(s)$, d.h. es gilt $j(s) \in (S^{-1}A)^\times$. Hier bezeichnen wir mit $(S^{-1}A)^\times$ die Menge der invertierbaren Elemente von $S^{-1}A$. Wir nennen ein invertierbares Element in einem Ring auch **Einheit**.
Beispiel:

i) Ist $0 \in S$, so gibt es nur eine Äquivalenzklasse und $S^{-1}A = \{0\}$.

ii) Ist A ein Integritätsring und $S = A \setminus \{0\}$, so gilt $(a, s) \sim (b, t) \Leftrightarrow at - bs = 0$. In diesem Fall ist $S^{-1}A = \text{Quot}\, A$ ein Körper, der sogenannte **Quotientenkörper** von A, und $j : A \to \text{Quot}\, A$ ist injektiv. Für $A = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$ ist also $S^{-1}A = \mathbb{Q}$.

Die Lokalisierung $S^{-1}A$ von A nach S hat folgende universelle Eigenschaft:

Lemma 4.2 Es sei $\varphi : A \to B$ ein Ringhomomorphismus, so dass $\varphi(s)$ für alle $s \in S$ eine Einheit in B ist. Dann existiert genau ein Ringhomomorphismus $\psi : S^{-1}A \to B$, der das folgende Diagramm kommutativ macht:



Beweis : Wir setzen $\psi(a/s) = \varphi(a)\varphi(s)^{-1}$. Ist $(a, s) \sim (b, t)$, so folgt $(at - bs)u = 0$ für ein $u \in S$. Also gilt $(\varphi(a)\varphi(t) - \varphi(b)\varphi(s))\varphi(u) = 0$. Da $\varphi(s), \varphi(t)$ und $\varphi(u)$ in $B^\times$ sind, folgt $\varphi(a)\varphi(s)^{-1} = \varphi(b)\varphi(t)^{-1}$. Also ist ψ wohldefiniert, d.h. unabhänging vom gewählten Vertreter der Äquivalenzklasse. Man rechnet leicht nach, dass ψ ein Ringhomomorphismus ist und $\varphi = \psi \circ j$ erfüllt.
Ist $\psi' : S^{-1}A \to B$ ein weiterer Ringhomomorphismus mit $\varphi = \psi' \circ j$, so folgt $\psi'(a/1) = \psi'(j(a)) = \varphi(a) = \psi(j(a)) = \psi(a/1)$ für alle $a \in A$. Also gilt $\psi'(a/s) = \psi'(a/1)\psi'(1/s) = \psi'(a/1)\psi'(s/1)^{-1} = \psi(a/1)\psi(s/1)^{-1} = \psi(a/s)$. □

Lemma 4.3 Sei S eine multiplikative Teilmenge in A.

i) Für jedes Ideal $\mathfrak{a} \subset A$ ist

$$S^{-1}\mathfrak{a} = \{\frac{a}{s} : a \in \mathfrak{a}, s \in S\}$$

ein Ideal in $S^{-1}A$.

ii) $S^{-1}\mathfrak{a} = S^{-1}A$ genau dann, wenn $S \cap \mathfrak{a} \neq \emptyset$.

iii) Für jedes Ideal $\mathfrak{b}$ in $S^{-1}A$ gibt es ein Ideal $\mathfrak{a} \subset A$ mit

$$\mathfrak{b} = S^{-1}\mathfrak{a}.$$

Ist $S^{-1}\mathfrak{a}$ ein Primideal, so ist $\mathfrak{a}$ ein Primideal. Ist $\mathfrak{a}$ ein Primideal mit $\mathfrak{a} \cap S = \emptyset$, so ist $S^{-1}\mathfrak{a}$ ein Primideal.
Beweis :

i) Übungsaufgabe.

ii) Gilt $S^{-1}\mathfrak{a} = S^{-1}A$, so ist $1 \in S^{-1}\mathfrak{a}$, also $1 = \frac{a}{s}$ für ein $a \in \mathfrak{a}$ und ein $s \in S$. Dann existiert ein $t \in S$ mit $(s-a)t = 0$. Also ist $st = at \in \mathfrak{a} \cap S$.

Gilt umgekehrt $s \in S \cap \mathfrak{a}$, so ist $1 = \frac{s}{s} \in S^{-1}\mathfrak{a}$, daher ist $S^{-1}\mathfrak{a} = S^{-1}A$.

iii) Sei $b \subset S^{-1}A$ ein Ideal. Wir setzen $\mathfrak{a} = j^{-1}(\mathfrak{b})$ für die kanonische Abbildung $j = A \to S^{-1}A$. Da j ein Ringhomomorphismus ist, ist $\mathfrak{a} \subset A$ ein Ideal. Für jedes $s \in S$ und $a \in A$ gilt dann

$$\frac{a}{s} = \frac{1}{s} \cdot j(a) \in \mathfrak{b}.$$

Daher ist $S^{-1}\mathfrak{a} \subset \mathfrak{b}$. Ist umgekehrt $b \in \mathfrak{b}$, so schreiben wir

$$b = \frac{1}{s} \cdot j(a)$$

für ein $a \in A$.
Mit b ist auch $sb = j(a)$ in $\mathfrak{b}$, also liegt $a \in j^{-1}(\mathfrak{b}) = \mathfrak{a}$. Somit gilt auch die andere Inklusion

$$\mathfrak{b} \subset S^{-1}\mathfrak{a},$$

also ist $\mathfrak{b} = S^{-1}\mathfrak{a}$.
Ist $\mathfrak{b}$ ein Primideal, dann ist das Urbild $\mathfrak{a} = j^{-1}(\mathfrak{b})$ auch ein Primideal. (Das gilt für jeden Ringhomomorphismus: Übungen) Ist $\mathfrak{a}$ ein Primideal mit $\mathfrak{a} \cap S = \emptyset$, so betrachten wir

$$\frac{a}{s}, \frac{b}{t} \in S^{-1}A \text{ mit}$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in S^{-1}\mathfrak{a}.$$

Das heißt, es gibt ein $r \in S, c \in \mathfrak{a}$ und ein $u \in S$ mit

$$(abr - stc)u = 0,$$

woraus

$$abru = stcu \in \mathfrak{a}$$

folgt. Da $\mathfrak{a}$ ein Primideal ist, das kein Element aus S enthält, folgt $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$. Also liegt $\frac{a}{s} \in S^{-1}\mathfrak{a}$ oder $\frac{b}{s} \in S^{-1}\mathfrak{a}$. □

Uns interessieren vor allem die folgenden Beispiele für Lokalisierungen:

Beispiel:

i) Für jedes $f \in A$ ist $S = \{1, f, f^2, ...\}$ eine multiplikative Teilmenge von A. Wir schreiben $A_f = S^{-1}A$ und nennen A_f die **Lokalisierung von** A **nach** f.

   Für $A = \mathbb{Z}$ und $f = 3$ ist etwa $\mathbb{Z}_3$ die Menge aller rationalen Zahlen $\frac{a}{b}$ mit ggT$(a, b) = 1$ und b eine Dreierpotenz.

ii) Ist $\mathfrak{p}$ ein Primideal in A, so ist $S = A \setminus \mathfrak{p}$ eine multiplikative Teilmenge von A. Wir schreiben $A_\mathfrak{p} = S^{-1}A$ und nennen $A_\mathfrak{p}$ die **Lokalisierung von** A **nach** $\mathfrak{p}$.

Lemma 4.4 Ist $\mathfrak{p}$ ein Primideal in A, so ist $\mathfrak{p}A_\mathfrak{p} := S^{-1}\mathfrak{p} = \{a/s : a \in \mathfrak{p}, s \in A \setminus \mathfrak{p}\}$ das einzige maximale Ideal in $A_\mathfrak{p}$.

Beweis : Das folgt aus Lemma 4.3. □

Definition 4.5 Ein Ring, der nur ein maximales Ideal enthält, heißt **lokaler Ring**.

Ist A ein lokaler Ring und $\mathfrak{m} \subset A$ das einzige maximale Ideal, so ist jedes Element in $A \setminus \mathfrak{m}$ eine Einheit. (Übungsaufgabe).

Lemma 4.6 Ist A ein Ring und $\mathfrak{p}$ ein Primideal, so vermittelt die kanonische Abbildung

$$j : A \to A_\mathfrak{p}$$

einen injektiven Ringhomomorphismus

$$A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}.$$

Es gilt Quot $(A/\mathfrak{p}) \simeq A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$.

Beweis : Die Abbildung j ist definiert als $j(a) = \frac{a}{1}$. Ist für ein $a \in A$ das Element $\frac{a}{1}$ in $\mathfrak{p}A_\mathfrak{p} = S^{-1}\mathfrak{p}$ für $S = A\setminus\mathfrak{p}$ enthalten, so gilt

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

für ein $b \in \mathfrak{p}$ und ein $s \notin \mathfrak{p}$.

Also gilt $t(as-b)=0$ für ein $t \notin \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist und $tas = tb \in \mathfrak{p}$ gilt, folgt $a \in \mathfrak{p}$. Daher ist

$$\overline{j} : A/\mathfrak{p} \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$$

tatsächlich injektiv. $A/\mathfrak{p}$ ist ein Integritätsring, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ ein Körper, denn $\mathfrak{p}A_{\mathfrak{p}}$ ist ein maximales Ideal in $A_{\mathfrak{p}}$. Wir können die Einbettung $\overline{j}$ von $A/\mathfrak{p}$ in $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ also fortsetzen zu einer Einbettung

$$\begin{array}{rcl} \mathrm{Quot}(A/\mathfrak{p}) & \to & A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \\ \frac{p}{q} & \mapsto & \frac{\overline{j}(p)}{\overline{j}(q)} \end{array} .$$

Ist $\frac{a}{s}$ ein beliebiges Element in $A_{\mathfrak{p}}$, so folgt aus $s \notin \mathfrak{p}$, dass die Restklasse $q = s + \mathfrak{p} \neq 0$ ist. Daher ist für $p = a + \mathfrak{p}$ das Element

$$\frac{p}{q} \in \mathrm{Quot}(A/\mathfrak{p})$$

ein Urbild von $\frac{a}{s} + \mathfrak{p}A_{\mathfrak{p}}$.
Also folgt

$$\mathrm{Quot}(A/\mathfrak{p}) \simeq A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

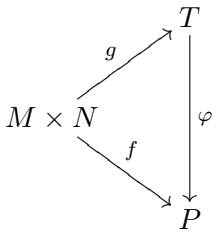
□

5 Tensorprodukt

Proposition 5.1 Es seien M und N Moduln über dem Ring A. Dann gibt es ein Paar $(T,\, g)$ bestehend aus einem A-Modul T und einer A-bilinearen Abbildung

$$g : M \times N \to T,$$

so dass gilt:
Für jeden A-Modul P und jede A-bilineare Abbildung $f : M \times N \to P$ gibt es genau einen A-Modulhomomorphismus (also eine lineare Abbildung) $\varphi : T \to P$, so dass folgendes Diagramm kommutiert:



Sind $(T,\, g)$ und $(T',\, g')$ zwei Paare mit dieser Eigenschaft, so existiert genau ein Isomorphismus $j : T \to T'$ mit $j \circ g = g'$.

Beweis : Die Eindeutigkeitsaussage folgt leicht aus der universellen Eigenschaft.
Um die Existenz zu zeigen, betrachten wir den freien A-Modul

$$C = \bigoplus_{(x,y)\in M\times N} A.$$

Die Elemente von C sind Linearkombinationen der Form $\sum_{(x,y)\in M\times N} a_{xy}\, e_{(x,y)}$, wobei $e_{(x,y)}$ die kanonische Basis des freien A-Moduls $\bigoplus_{(x,\,y)\in M\times N} A$ ist.
Es sei D der Untermodul von C, der von allen Elementen der folgenden Form für $(x, y) \in M$ und $a \in A$ erzeugt wird:

$$\begin{aligned} e_{(x+x',y)} &- e_{(x,y)} - e_{(x',y)} \\ e_{(x,y+y')} &- e_{(x,y)} - e_{(x,y')} \\ e_{(ax,y)} &- a\, e_{(x,y)} \\ e_{(x,ay)} &- a\, e_{(x,y)} \end{aligned}$$

Wir setzen $T = C/D$ und bezeichnen mit $x \otimes y$ das Bild von $e_{(x,y)} \in C$ im Quotienten T. Dann wird T als A-Modul von den Elementen der Form $x \otimes y$ für $x \in M$ und $y \in N$ erzeugt. Es gilt ferner in T

$$\begin{aligned} (x + x') \otimes y &= x \otimes y + x' \otimes y, \\ x \otimes (y + y') &= x \otimes y + x \otimes y', \\ (a\, x) \otimes y &= a(x \otimes y) = x \otimes (a\, y). \end{aligned}$$

Daher ist die Abbildung

$$g : M \times N \to T,$$

definiert durch $g(x, y) = x \otimes y$, bilinear. Ist $f : M \times N \to P$ eine beliebige bilineare Abbildung in einen A-Modul P, so können wir durch $e_{(x,y)} \mapsto f(x, y)$ einen A-Modulhomomorphismus $\tilde{\varphi} : C \to P$ definieren. Da f bilinear ist, verschwindet $\tilde{\varphi}$ auf D. Also erhalten wir einen A-Modulhomomorphismus $\varphi : T \to P$. Es ist $\varphi(x \otimes y) = \tilde{\varphi}(e_{(x,y)}) = f(x, y)$. Also gilt $\varphi \circ g = f$. Da T durch die Elemente der Form $x \otimes y$ erzeugt ist, ist φ durch diese Bedingung eindeutig bestimmt. □

Wir nennen T das **Tensorprodukt** von M und N und bezeichnen es als $T = M \otimes_A N$ oder $M \otimes N$. Als A-Modul ist $M \otimes_A N$ von allen Elementen der Form $x \otimes y$ (mit $x \in M$ und $y \in N$) erzeugt. Diese werden auch als **reine Tensoren** bezeichnet. Ein beliebiges Element in $M \otimes_A N$ hat also die Form $\sum_{i=1}^{n} a_i\, x_i \otimes y_i$ mit $a_i \in A$, $x_i \in M$ und $y_i \in N$.

Proposition 5.2 i) Sind M_1, ..., M_r A-Moduln, so gibt es ein Paar (T, g) bestehend aus einem A-Modul T und einer multilinearen Abbildung $g : M_1 \times ... \times M_r \to T$, so dass gilt:
Für jeden A-Modul P und jede multilineare Abbildung $f : M_1 \times ... \times M_r \to P$ existiert genau ein A-Modulhomomorphismus $\varphi : T \to P$ mit $\varphi \circ g = f$.

ii) Sind M, N und P drei A-Moduln, so gibt es eindeutig bestimmte Isomorphismen

a) $M \otimes_A N \to N \otimes_A M$

b) $(M \otimes_A N) \otimes_A P \to M \otimes_A (N \otimes_A P) \to M \otimes_A N \otimes_A P$

c) $(M \oplus N) \otimes_A P \to (M \otimes_A P) \oplus (N \otimes_A P)$

d) $A \otimes_A M \to M$,

so dass jeweils folgende Bedingungen erfüllt sind:

a) $x \otimes y \mapsto y \otimes x$

b) $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$

c) $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$

d) $a \otimes x \mapsto a\,x$

Beweis : Man definiert die gewünschten Isomorphismen und ihre Umkehrabbildungen durch die universelle Eigenschaft des Tensorprodukts. □

Für einen $A-$Modulhomomorphismus $f : M \to N$ und einen $A-$Modul P bezeichnen wir mit $f \otimes id : M \otimes_A P \to N \otimes_A P$ die lineare Abbildung mit $f \otimes id(m \otimes p) = f(m) \otimes p$ für alle $m \in M, p \in P$. Sie existiert aufgrund der universellen Eigenschaft des Tensorproduktes.

In den Übungen haben wir Lokalisierungen von Moduln kennengelernt.

Proposition 5.3 Sei $S \subset A$ eine multiplikative Teilmenge und M ein $A-$Modul. Dann existiert genau ein Isomorphismus von $S^{-1}A-$Moduln

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

mit $f(\frac{a}{s} \otimes m) = \frac{am}{s}$ für alle $a \in A, m \in M$ und $s \in S$.

Beweis : Die Abbildung

$$\begin{array}{ccc} S^{-1}A \times M & \to & S^{-1}M \\ (\frac{a}{s}, m) & \mapsto & \frac{am}{s} \end{array}$$

ist eine bilineare Abbildung von $A-$Moduln. Nach der universellen Eigenschaft des Tensorproduktes existiert also genau ein $A-$Modul-Homomorphismus

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

mit $f(\frac{a}{s} \otimes m) = \frac{am}{s}$.

Dieser ist offenbar surjektiv. Es sei $\sum_i \frac{a_i}{s_i} \otimes m_i$ ein beliebiges Element aus $S^{-1}A \otimes_A M$. Für $s = \prod_i s_i \in S$ und $t_i = \prod_{j \neq i} s_i \in S$ gilt dann

$$\begin{aligned} \sum_i \frac{a_i}{s_i} \otimes m_i &= \sum_i \frac{ati}{s} \otimes m_i \\ &= \sum_i \frac{1}{s} \otimes at_i m_i \\ &= \frac{1}{s} \otimes \sum_i at_i m_i. \end{aligned}$$

Daher ist jedes Element in $S^{-1}A \otimes_A M$ von der Form $\frac{1}{s} \otimes m$ für ein $m \in M$. Angenommen $f(\frac{1}{s} \otimes m) = 0$. Dann folgt $\frac{m}{s} = 0$ in $S^{-1}M$, also ist $tm = 0$ für ein $t \in S$. Dann ist aber auch

$$\frac{1}{s} \otimes m = \frac{t}{ts} \otimes m = \frac{1}{ts} \otimes tm = \frac{1}{ts} \otimes 0 = 0,$$

also ist f injektiv.

Ferner ist für $\frac{1}{s} \otimes m \in S^{-1}A \otimes_A M$ und $t \in S$

$$f\Big((\frac{1}{t}(\frac{1}{s} \otimes m)\Big) = f\Big(\frac{1}{st} \otimes m\Big) = \frac{m}{st} = \frac{1}{t}\Big(\frac{m}{s}\Big) = \frac{1}{t} f\Big(\frac{1}{s} \otimes m\Big),$$

also ist f auch $S^{-1}A-$linear. □

Proposition 5.4 Es seien M und N zwei $A-$Moduln und $S \subset A$ eine multiplikative Teilmenge. Dann gibt es genau einen Isomorphismus von $S^{-1}A-$Moduln

$$g : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$$

mit

$$g\Big(\frac{m}{s} \otimes \frac{n}{t}\Big) = \frac{m \otimes n}{st}.$$

Insbesondere gilt für jedes Primideal $\mathfrak{p} \subset A$

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \simeq (M \otimes_A N)_\mathfrak{p},$$

wobei wir $M_\mathfrak{p} = S^{-1}M$ für $S = A \backslash \mathfrak{p}$ schreiben.

Beweis : Aus der universellen Eigenschaft des Tensorproduktes folgt, dass es genau einen Homomorphismus g gibt, der auf reinen Tensoren die gewünschte Eigenschaft hat.

Ferner existiert genau ein $A-$Modulhomomorphismus

$$h : M \otimes_A N \to S^{-1}M \otimes_{S^{-1}A} S^{-1}N$$

mit $h(m \otimes n) = m \otimes n$.

Da die rechte Seite ein $S^{-1}A-$Modul ist, können wir diesen fortsetzen zu einem $S^{-1}A-$Modulhomomorphismus

$$S^{-1}(M \otimes_A N) \to S^{-1}M \otimes_{S^{-1}A} S^{-1}N,$$

der für alle $x \in M \otimes_A N$ und $s \in S$ das Element $\frac{x}{s}$ auf $\frac{h(x)}{s}$ abbildet. Dies ist eine Umkehrabbildung zu g. □

Sei A ein Ring. Eine Sequenz von $A-$Moduln und $A-$Modulhomomorphismen

$$\ldots \to M_{i-1} \overset{f_i}{\to} M_i \overset{f_{i+1}}{\to} M_{i+1} \to \ldots$$

heißt exakt in M_i, falls

$$\text{Kern}(f_{i+1}) = \text{Bild}(f_i)$$

gilt. Wir nennen eine solche Sequenz exakt, falls sie in allen M_i exakt ist. Insbesondere gilt:

$0 \to M_1 \overset{f}{\to} M_2$ ist exakt genau dann, wenn f injektiv ist.

$M_1 \overset{g}{\to} M_2 \to 0$ ist exakt genau dann, wenn g surjektiv ist.

Für zwei $A-$Moduln M und N ist die Menge

$$\text{Hom}_A(M, N) = \{f : M \to N, f \text{ ist ein } A - \text{Modulhomomorphismus}\}$$

versehen mit den Verknüpfungen

$$(f + g)(m) = f(m) + g(m)$$

und

$$(af)(m) = af(m)$$

ebenfalls ein $A-$Modul. Ein $A-$Modulhomomorphismus $M_1 \stackrel{g}{\to} M_2$ induziert einen $A-$Modulhomomorphismus

$$\begin{array}{rcl} g^* : \mathrm{Hom}(M_2, N) & \to & \mathrm{Hom}(M_1, N) \\ f & \mapsto & f \circ g. \end{array}$$

Analog induziert ein $A-$Modulhomomorphismus $h : N_1 \to N_2$ einen $A-$Modulhomomorphismus

$$\begin{array}{rcl} h_* : \mathrm{Hom}(M, N_1) & \to & \mathrm{Hom}(M, N_2) \\ f & \mapsto & h \circ f \end{array}$$

Lemma 5.5 i) Die Sequenz

$$M' \stackrel{f}{\to} M \stackrel{g}{\to} M'' \to 0$$

ist genau dann exakt, wenn für alle $A-$Moduln N die Sequenz

$$0 \to \mathrm{Hom}(M'', N) \stackrel{g^*}{\to} \mathrm{Hom}(M, N) \stackrel{f^*}{\to} \mathrm{Hom}(M', N)$$

exakt ist.

ii) Die Sequenz

$$0 \to N' \stackrel{f}{\to} N \stackrel{g}{\to} N''$$

ist genau dann exakt, wenn für alle $A-$Moduln M die Sequenz

$$0 \to \mathrm{Hom}(M, N') \stackrel{f_*}{\to} \mathrm{Hom}(M, N) \stackrel{g_*}{\to} \mathrm{Hom}(M, N'')$$

exakt ist.

Beweis : Übungsaufgabe. □

Nun betrachten wir eine bilineare Abbildung

$$f : M \times N \to P.$$

Dies liefert einen $A-$Modulhomomorphismus

$$\begin{array}{rcl} M & \to & \mathrm{Hom}(N, P) \\ m & \mapsto & \big(n \mapsto f(m, n)\big). \end{array}$$

Umgekehrt liefert jeder $A-$Modulhomomorphismus von M nach $\mathrm{Hom}(N, P)$ eine bilineare Abbildung von $M \times N$ nach P.

Da sich die Menge der bilinearen Abbildungen $M \times N \to P$ wegen der universellen Eigenschaft des Tensorproduktes mit

$$\mathrm{Hom}(M \otimes_A N, P)$$

identifizieren lässt, erhalten wir einen Isomorphismus von $A-$Moduln

$$\mathrm{Hom}(M \otimes_A N, P) \to \mathrm{Hom}\big(M, \mathrm{Hom}(N, P)\big).$$

Proposition 5.6 Es sei

$$M' \stackrel{f}{\to} M \stackrel{g}{\to} M'' \to 0$$

eine exakte Sequenz von $A-$Moduln. Für jeden $A-$Modul N ist dann auch

$$M' \otimes_A N \stackrel{f\otimes id}{\to} M \otimes_A N \stackrel{g\otimes id}{\to} M'' \otimes_A N \to 0$$

exakt.

Beweis : Sei P ein beliebiger $A-$Modul und $Q = \mathrm{Hom}(N, P)$. Nach Lemma 5.5 i) ist dann

$$0 \to \mathrm{Hom}(M'', Q) \to \mathrm{Hom}(M, Q) \to \mathrm{Hom}(M', Q)$$

exakt, also aufgrund der Bemerkung vor der Proposition auch

$$0 \to \mathrm{Hom}(M'' \otimes_A N, P) \to \mathrm{Hom}(M \otimes_A N, P) \to \mathrm{Hom}(M' \otimes_A N, P).$$

Also folgt die Behauptung aus Lemma 5.5 i). □

Wir sagen dazu auch : „Tensorieren ist rechtsexakt."

Die Behauptung des Lemmas kann für andere exakte Sequenzen als die in Proposition 5.6 verwendeten falsch sein.

Beispiel 5.7 Sei $A = Z$. Wir betrachten die exakte Sequenz

$$\begin{array}{rcl} 0 \to \mathbb{Z} & \stackrel{f}{\to} & \mathbb{Z} \\ x & \mapsto & 2x. \end{array}$$

Wir tensorieren mit dem $A-$Modul $N = \mathbb{Z}/2\mathbb{Z}$ und erhalten

$$\begin{array}{ccc} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} & \stackrel{f\otimes id}{\to} & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \\ \wr\downarrow & & \wr\downarrow \\ \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z}, \end{array}$$

wobei $f\otimes$ id die Nullabbildung ist, denn

$$\begin{aligned}(f\otimes id)(x\otimes y) &= f(x)\otimes y\\ &= 2x\otimes y\\ &= x\otimes 2y\\ &= x\otimes 0\\ &= 0.\end{aligned}$$

Daher ist $f\otimes id$ nicht injektiv.

Definition 5.8 Ein $A-$Modul N heißt flach, falls für jede exakte Sequenz

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

von $A-$Moduln auch

$$M'\otimes_A N \xrightarrow{f\otimes id} M\otimes_A N \xrightarrow{g\otimes id} M''\otimes_A N$$

exakt ist.

Beispiel 5.9 i) A ist ein flacher $A-$Modul.

ii) Jeder freie $A-$Modul ist flach.

Proposition 5.10 Für einen $A-$Modul N sind die folgenden Eigenschaften äquivalent:

i) N ist flach.

ii) Für jede kurze exakte Sequenz

$$0\to M' \xrightarrow{f} M \xrightarrow{g} M''\to 0$$

von $A-$Moduln ist

$$0\to M'\otimes_A N \xrightarrow{f\otimes id} M\otimes_A N \xrightarrow{g\otimes id} M''\otimes_A N\to 0$$

exakt.

iii) Für jeden injektiven $A-$Modulhomomorphismus $f : M'\to M$ ist

$$f\otimes id : M'\otimes_A N\to M\otimes_A N$$

injektiv.

Beweis : i) $\Rightarrow$ iii) folgt aus der Definition der Flachheit angewandt auf $0 \to M' \to M$.
iii) $\Rightarrow$ ii) folgt aus Proposition 5.6.
ii) $\Rightarrow$ i) Ist $M' \stackrel{f}{\to} M \stackrel{g}{\to} M''$ eine exakte Sequenz von $A-$Moduln, so betrachten wir

$$0 \to \text{Bild } f \to M \stackrel{g}{\to} \text{Bild } g \to 0.$$

Diese Sequenz ist wegen Bild $f =$ kern g ebenfalls exakt. Also ist nach Voraussetzung auch

$$0 \to (\text{Bild } f) \otimes_A N \to M \otimes_A N \stackrel{g\otimes id}{\to} (\text{Bild } g) \otimes_A N \to 0$$

exakt. Aus (Bild $f) \otimes_A N =$ Bild $(f \otimes id)$ folgt dann, dass

$$M' \otimes_A N \stackrel{f\otimes id}{\to} M \otimes_A N \stackrel{g\otimes id}{\to} M'' \otimes_A N$$

exakt ist. □

Nun betrachten wir einen Ring A und zwei A-Algebren B und C. Dann sind B und C insbesondere A-Moduln, also existiert das Tensorprodukt $B \otimes_A C =: D$. Wir betrachten die Abbildung

$$\begin{array}{rcl} B \times C \times B \times C & \to & B \otimes_A C = D \\ (b,\, c,\, b',\, c') & \mapsto & bb' \otimes cc' \end{array}$$

Diese ist A-linear in jedem Faktor und induziert daher nach Proposition 1.1 einen A-Modulhomomorphismus

$$B \otimes_A C \otimes_A B \otimes_A C \to D.$$

Nach 1.2 ist $B \otimes_A C \otimes_A B \otimes_A C \simeq (B \otimes_A C) \otimes_A (B \otimes_A C) = D \otimes_A D$. Also erhalten wir einen A-Modulhomomorphismus $\mu : D \otimes_A D \to D$ mit der Eigenschaft $\mu(b \otimes c,\, b' \otimes c') = bb' \otimes cc'$. Damit haben wir auf dem Tensorprodukt $D = B \otimes_A C$ eine Multiplikation definiert, die D zu einem kommutativen Ring mit Einselement $1_B \otimes 1_C$ macht. Über den Ringhomomorphismus

$$\begin{array}{rcl} A & \to & D = B \otimes_A C \\ a & \mapsto & a\,1_B \otimes 1_C = 1_B \otimes a 1_C \end{array}$$

wird D zu einer A-Algebra.
Ferner haben wir A-Algebrenhomomorphismen

$$\begin{array}{rcl} B & \to & D = B \otimes_A C \\ b & \mapsto & b \otimes 1_C \end{array}$$

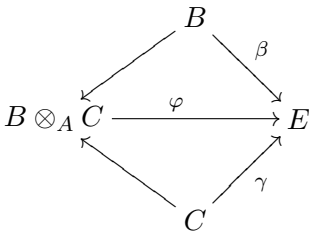
und

$$\begin{aligned} C &\to D = B \otimes_A C \\ c &\mapsto 1_B \otimes c. \end{aligned}$$

Proposition 5.11 Die A-Algebra $B \otimes_A C$ hat folgende universelle Eigenschaft. Ist E eine beliebige A-Algebra zusammen mit A-Algebrenhomomorphismen

$$\beta : B \to E \quad \text{und} \quad \gamma : C \to E,$$

so existiert genau ein A-Algebrenhomomorphismus $\varphi : B \otimes_A C \to E$, so dass das Diagramm



kommutiert.

Beweis : Wir betrachten die bilineare Abbildung

$$\begin{aligned} B \otimes_A C &\to E \\ (b, c) &\mapsto \beta(b)\gamma(c). \end{aligned}$$

Man rechnet nach, dass der A-Modulhomomorphismus $\varphi : B \otimes_A C \to E$ zu (β, γ), der nach der universellen Eigenschaft 1.1 existiert, mit den Ringstrukturen verträglich ist. □

Definition 5.12 Eine Kategorie $\mathfrak{a}$ besteht aus einer Klasse Ob von „Objekten“ sowie für alle Objekte A, B aus einer Menge Hom (A, B) von Morphismen, so dass gilt:

i) Hom (A, A) enthält ein Element id_A.

ii) Es gibt eine Verknüpfungsabbildung für alle Objekte A, B und C

$$\begin{aligned} \text{Hom}(A, B) \times \text{Hom}(B, C) &\to \text{Hom}(A, C) \\ f, g &\mapsto g \circ f \end{aligned}$$

mit

$$id_B \circ g = g \text{ für alle } g \in \text{Hom } (B, C)$$

und

$$f \circ id_B = f \text{ für alle } f \in \mathrm{Hom}(A, B).$$

iii) Es ist $(f \circ g) \circ h = f \circ (g \circ h)$.

Definition 5.13 Eine abelsche Kategorie ist eine Kategorie $\mathfrak{a}$, so dass für alle Objekte A, B in $\mathfrak{a}$ die Menge $\mathrm{Hom(A, B)}$ eine abelsche Gruppe ist, die folgenden Bedingungen genügt:

1) $\mathrm{Hom(A, B)} \times \mathrm{Hom(B, C)} \xrightarrow{\circ} \mathrm{Hom(A, C)}$ ist bilinear,
und es gibt ein Objekt 0 in $\mathfrak{a}$, so dass für alle A die Mengen $\mathrm{Hom(A, 0)}$ und $\mathrm{Hom(0, A)}$ nur aus einem Element bestehen.

2) $\mathfrak{a}$ enthält endliche direkte Summen und endlich direkte Produkte.

3) a) Jeder Morphismus $f : A \to B$ hat einen Kern, das heißt, es gibt ein $g : C \to A$, so dass für alle X in $\mathfrak{a}$
$0 \to \mathrm{Hom(X, C)} \xrightarrow{\mathrm{g}} \mathrm{Hom(X, A)} \xrightarrow{\mathrm{f}} \mathrm{Hom(X, B)}$ exakt ist.

b) Jeder Morphismus $f : A \to B$ hat einen Kokern, das heißt, es gibt ein $h : B \to C$, so dass für alle X in $\mathfrak{a}$
$0 \to \mathrm{Hom(C, X)} \to \mathrm{Hom(B, X)} \to \mathrm{Hom(A, X)}$ exakt ist.

4) Ist der Kern von $f : A \to B$ gerade 0, so ist f der Kern seines Kokerns. Ist der Kokern von $f : A \to B$ gleich 0, so ist f der Kokern seines Kerns. Ein Morphismus dessen Kern und Kokern 0 sind, ist ein Isomorphismus.

Beispiel

1) Die Kategorie Ab der abelschen Gruppen.

2) Die Kategorie der Mengen ist keine abelsche Kategorie, ebenso die Kategorie topologischer Räume.

3) Die Kategorie $\mathrm{Mod(A)}$ der Moduln über dem Ring A (wie immer kommutativ mit 1) ist eine abelsche Kategorie.

Definition 5.14 Ein Komplex A° in einer abelschen Kategorie ist eine Kollektion von Objekten A^i, $i \in \mathbb{Z}$ und Morphismen $d^i : A^i \to A^{i+1}$ mit $d^{i+1} \circ d^i = 0$. (Sind die A^i nur für $i \geq 0$ gegeben, so setzt man die anderen $= 0$).

Jetzt brauchen wir ein paar Begriffe über Funktoren:
Ein kovarianter Funktor $F : \mathfrak{a} \to b$ von der Kategorie $\mathfrak{a}$ in die Kategorie b ist eine Regel, die jedem Objekt A aus A ein Objekt $F(A)$ aus b und jedem Morphismus $f : A \to B$ in $\mathfrak{a}$ einen Morphismus $F(f) : F(A) \to F(B)$ zuordnet, so dass

i) $F(id_A) = id_{F(A)}$ und

ii) $F(g \circ f) = F(g) \circ F(f)$

gilt. Ein kontravarianter Funktor ordnet $f : A \to B$ einen Morphismus $F(f) : F(B) \to F(A)$ zu, so dass i) und statt ii) $F(g \circ f) = F(f) \circ F(g)$ gilt.
Ein kovarianter Funktor $F : \mathfrak{a} \to b$ zwischen zwei abelschen Kategorien heißt additiv, falls die Abbildung $\mathrm{Hom(A,B)} \longrightarrow \mathrm{Hom(F(A),F(B))}$, die durch $f \mapsto F(f)$ gegeben ist, ein Homomorphismus abelscher Gruppen ist. F heißt linksexakt, falls F additiv ist und jede kurze exakte Sequenz $0 \to A' \to A \to A'' \to 0$ in eine exakte Sequenz $0 \to F(A') \to F(A) \to F(A'')$ überführt. (Hier muss man die Exaktheit von Sequenzen mit Hilfe von Kernen und Kokernen, die in einer abelschen Kategorie existieren, umschreiben.)
Überführt F stattdessen die kurze exakte Sequenz in eine exakte Sequenz

$$F(A') \to F(A) \to F(A'') \to 0,$$

so heißt F rechtsexakt.
Ist F links– und rechtsexakt, so nennen wir F exakt. Analoge Begriffe gelten für kontravariante Funktoren (linksexakt bedeutet hier, dass $0 \to A' \to A \to A'' \to 0$ in $0 \to F(A'') \to F(A) \to F(A')$ überführt wird).
Beispiel: $\mathfrak{a}$ eine abelsche Kategorie, A ein Objekt. Dann ist

$$\begin{aligned} \mathrm{Hom(A,0)} : \mathfrak{a} &\to \mathrm{Ab} \\ B &\to \mathrm{Hom(A,B)} \end{aligned}$$

ein kovarianter linksexakter Funktor, und

$$\begin{aligned} \mathrm{Hom(A,0)} : \mathfrak{a} &\to \mathrm{Ab} \\ B &\mapsto \mathrm{Hom(A,B)} \end{aligned}$$

ein kontravarianter rechtsexakter Funktor. (Übungsaufgabe, folgt aus den Axiomen einer abelschen Kategorie.)