Kommutative Algebra

Prof. Dr. Uwe Jannsen
Sommersemester 2014

Inhaltsverzeichnis

0 Erinnerung: Ringe und Polynomringe

Definition 0.1 (i) Ein Ring ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass gilt:
(a) $(R, +)$ ist eine abelsche Gruppe.
(b) Die Verknüpfung $\cdot$ ist assoziativ.
(c) Es gelten die Distributivgesetze

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \,. \end{aligned}$$

Das neutrale Element von $(R, +)$ wird mit 0 bezeichnet.

(ii) R heißt ein Ring mit Eins (oder unitaler Ring), wenn es ein Element $1 \in R$ gibt mit $1 \cdot a = a = a \cdot 1$ für alle $a \in R$.

(iii) R heißt kommutativ, wenn $\cdot$ kommutativ ist.

Bemerkung 0.2 (i) Schreibe $-a$ für das Inverse von a bezüglich $+$. Oft lässt man $\cdot$ weg, schreibt also ab für $a \cdot b$.

(ii) Es gilt $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$, das Einselement ist eindeutig, wenn es existiert, und es gilt $-a = (-1) \cdot a$.

Beispiele 0.3 (i) $\mathbb{Z}$ ist ein kommutativer Ring mit Eins.

(ii) $M_n(\mathbb{Q})$ ist ein nicht kommutativer Ring mit Eins für $n \geq 2$.

Im Folgenden betrachten wir immer kommutative Ringe mit Eins, falls nichts anderes gesagt wird.

Definition 0.4 (i) Ein Homomorphismus von Ringen (kommutativ, mit Eins) ist eine Abbildung

$$\varphi : R_1 \to R_2$$

von Ringen mit $\varphi(a + b) = \varphi(a) + \varphi(b)$ und $\varphi(ab) = \varphi(a)\varphi(b)$ und $\varphi(1) = 1$ (Es folgt, dass $\varphi : (R_1, +) \to (R_2, +)$ ein Gruppenhomomorphismus ist).

(ii) φ heißt Monomorphismus (bzw. Epimorphismus, bzw. Isomorphismus), wenn φ injektiv (bzw. surjektiv, bzw. bijektiv) ist.

Definition 0.5 Ein Ideal $\mathfrak{a} \subseteq R$ ist eine Untergruppe (bezüglich $+$) mit $ra \in \mathfrak{a}$ für alle $r \in R$.

Satz 0.6 Auf der Faktorgruppe $(R/\mathfrak{a}, +)$ gibt es eine eindeutig bestimmte Verknüpfung $\cdot$, so dass $(R/\mathfrak{a}, +, \cdot)$ ein Ring ist (kommutativ, mit Eins) und die kanonische Surjektion

$$\begin{aligned} R &\to R/\mathfrak{a} \\ r &\mapsto F := r + \mathfrak{a} \end{aligned}$$

ein Ringhomomorphismus. $R/\mathfrak{a}$ heißt der Faktorring (von R modulo $\mathfrak{a}$).

Beweis Die Verknüpfung + auf $R/\mathfrak{a}$ ist bekanntlich gegeben durch $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$, und die Verknüpfung $\cdot$ auf $R/\mathfrak{a}$ ist notwendigerweise

$$\overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2}$$

für $\overline{r} := r + \mathfrak{a}$. Man rechnet nach, dass dies wohldefiniert ist.

Satz 0.7 (Isomorphiesatz) Ist $\varphi : R_1 \to R_2$ ein Ringhomomorphismus, so ist $\ker(\varphi) = \{r \in R_1 \mid \varphi(r) = 0\}$ ein Ideal in R_1, $\varphi(R_1)$ ein Unterring von R_2 (d.h., eine Teilmenge, die mit der Einschränkung von + und $\cdot$ wieder ein Ring ist) und

$$R_1/\ker(\varphi) \to \varphi(R_1)$$

ein Ringisomorphismus.

Bemerkung 0.8 Zu jeder Familie $(a_i)_{i\in I}$ von Elementen $a_i \in R$ hat man das von den a_i erzeugte Ideal $\langle a_i \mid i \in I\rangle$. Dies ist das kleinste Ideal, welches alle a_i enthält, und besteht aus allen Linearkombinationen $r_1 a_{i_1} + \ldots + r_n a_{i_n}$ der a_i. Ist $\mathfrak{a} = \langle a_i \mid i \in I\rangle$, so heißt $(a_i)_{i\in I}$ ein Erzeugendensystem von $\mathfrak{a}$, und $\mathfrak{a}$ heißt endlich erzeugt, wenn es ein endliches Erzeugendensystem besitzt.

Sei R ein Ring.

Definition 0.9 (i) Ein Element $a \in R \setminus \{0\}$ heißt **Nullteiler**, wenn es ein $b \in R$ gibt mit $b \neq 0$ und $a \cdot b = 0$.

(ii) R heißt **Integritätsring** (oder Integritätsbereich, oder integer), wenn R keine Nullteiler besitzt und nicht der Nullring ist ($R \neq \{0\}$).

Lemma/Definition 0.10 (i) Ein Ideal $\mathfrak{p} \subseteq R$ heißt **Primideal** (oder prim), wenn die folgenden äquivalenten Bedingungen gelten:
(a) Es ist $\mathfrak{p} \neq R$, und sind $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$, so ist $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
(b) $R/\mathfrak{p}$ ist integer.

(ii) Ein Ideal $\mathfrak{m} \subseteq R$ heißt **Maximalideal** (oder maximal), wenn die folgenden äquivalenten Bedingungen gelten:
(a) Es ist $\mathfrak{m} \neq R$, und es gibt kein Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$.
(b) $R/\mathfrak{m}$ ist ein Körper.

Offenbar folgt: $\mathfrak{m}$ maximal $\Rightarrow$ $\mathfrak{m}$ prim, denn jeder Körper ist integer.

Der Polynomring $R[x]$ (in einer Variablen) über einem Ring R wird wie folgt definiert:

Naive Definition 0.11 $R[x]$ besteht aus alle 'formalen Summen'

$$f(x) = \sum_{i=0}^{m} a_i x^i \tag{0.11.1}$$

mit $n \in \mathbb{N}_0$ und $a_i \in R$. Die Addition wird durch Addition der Koeffizienten gegeben: Ist

$$g(x) = \sum_{j=0}^{n} b_j x^j \,,$$

so ist

$$f(x)+g(x) := \sum_{k=0}^{max(m,n)} (a_k+b_k)x^k\,, \tag{0.11.2}$$

wobei

$$a_k := 0 \text{ für } k>m \text{ und } b_k := 0 \text{ für } k>n\,. \tag{0.11.3}$$

Die Multiplikation wird durch formales Ausmultiplizieren gegeben:

$$f(x)\cdot g(x) = \sum_{k=0}^{m+n} c_k x^k \tag{0.11.4}$$

mit

$$c_k = \sum_{r=0}^{k} a_r b_{k-r}\,. \tag{0.11.5}$$

Ein Polynom ist keine Funktion, sondern wird als formaler Ausdruck behandelt! Insbesondere wird ein Polynom im Allgemeinen nicht durch seine Werte bestimmt.

Beispiel 0.12 Ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen (p eine Primzahl), so hat das Polynom

$$f(x) = x^p - x$$

die Eigenschaft, dass $f(a)=0$ für alle $a\in\mathbb{F}_p$ (kleiner Satz von Fermat; z.B. ist für $p=2$ $0^2-0=0$ und $1^2-1=0$).

Die Definition 0.11 ist algebraisch unbefriedigend, weil der Begriff 'formale Summe' nicht richtig definiert wird. Eine formal richtige Definition, die auch auf Polynomringe in beliebig vielen Variablen erweitert werden kann, ist

Definition 0.13 Der Polynomring über R in einer Variablen ist die Menge

$$R^{(\mathbb{N}_0)} := \{(a_i)_{i\in\mathbb{N}_0} \mid a_i = 0 \quad \text{für fast alle} \quad i\in\mathbb{N}_0\}$$

mit den Verknüpfungen

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i+b_i)_{i\in\mathbb{N}_0}$$

$$(a_i)_{i\in\mathbb{N}_0}\cdot(b_i)_{i\in\mathbb{N}_0} = (c_i)_{i\in\mathbb{N}_0} \quad \text{mit} \quad c_n = \sum_{i=0}^{n} a_i b_{n-i}\,.$$

Schreiben wir x für das Element $(0,1,0,\ldots)$, so ist

$$x^i = (0,\ldots,\underset{\substack{\uparrow\\ i-\text{te Stelle}}}{1},0,\ldots) \quad \text{für} \quad i\geq 0\,,$$

und jedes Element im Ring lässt sich eindeutig schreiben als $\sum_{i=0}^{n} a_i x^i$ mit $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in R$. Dies entspricht dem Element $(a_0, \ldots, a_n, 0, 0, \ldots)$. Umgekehrt können wir ein Element $(a_0, a_1, \ldots)$ schreiben als

$$\sum_{i=0}^{\infty} a_i x^i$$

wobei die Summe in Wirklichkeit endlich ist. Die Addition und Multiplikation ist dann wie in 0.11 beschrieben, und wir schreiben auch $R[x]$ für den Polynomring, wenn wir das Element $(0, 1, 0, \ldots)$ mit x bezeichnen.

Bemerkungen 0.14 (a) Ein Polynom ist also durch seine Koeffizienten festgelegt und nicht durch seine "Werte" (im Sinne des Einsetzens, siehe 0.15 unten).

(b) Wir haben einen kanonischen Monomorphismus von Ringen

$$\begin{array}{ccll} R & \to & R[x] & \\ a & \mapsto & a & (= ax^0 = (a, 0, \ldots)) \, . \end{array}$$

Hierüber fassen wir R immer als Unterring von $R[x]$ auf.

Satz 0.15 (Universelle Eigenschaft des Polynomrings) Sei R' ein Ring (mit Eins!) und $\varphi : R \to R'$ ein Ringhomomorphismus (mit $\varphi(1) = 1$!). Für jedes $a \in R'$ gibt es genau einen Ringhomomorphismus

$$\varphi_a : R[x] \to R' \tag{0.15.1}$$

mit $\varphi_a|R = \varphi$ und $\varphi_a(x) = a$, nämlich

$$\varphi_a(\sum_{i=1}^{n} a_i x^i) = \sum_{i=1}^{n} \varphi(a_i) a^i \, . \tag{0.15.2}$$

Beweis Es ist klar, dass die Beziehung (0.13.2) gelten muss, wenn φ_a ein Ringhomomorphismus mit den beiden vorgegebenen Eigenschaften sein soll. Diese Definition ist andererseits wohldefiniert, und macht φ_a zu einem Ringhomomorphismus mit den beiden gewünschten Eigenschaften.

Wir haben also einfach "die Variable x durch a ersetzt" und sprechen auch von dem Einsetzungsmorphismus.

Definition 0.16 Der Polynomring $k[x_1, \ldots, x_n]$ in mehreren Variablen wird induktiv definiert durch

$$k[x_1, \ldots, x_n] = k[x_1, \ldots, x_{n-1}][x_n] \, .$$

Offenbar ist jedes Polynom in mehreren Variablen in der Form

$$f(x_1, \ldots, x_n) = \sum_{(i_1, \ldots, i_n)} a_{i_1, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

wobei $(i_1, \ldots, i_n)$ über alle Tupel in $\mathbb{N}_0^n$ läuft und $a_{i_1, \ldots, i_n} \in R$ mit $a_{i_1, \ldots, i_n} = 0$ für fast alle $(i_1, \ldots, i_n)$.

1 Noethersche Ringe

Sei R ein kommutativer Ring mit Eins.

Definition 1.1 Der Ring R heißt **noethersch** (nach Emmy Noether), wenn jedes Ideal $\mathfrak{a} \subseteq R$ endlich erzeugt ist.

Satz 1.2 Die folgenden Aussagen sind äquivalent.

(a) R ist noethersch.

(b) Jede aufsteigende Kette $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ von Idealen wird stationär, d.h., es gibt ein $n \in \mathbb{N}$ mit $\mathfrak{a}_n = \mathfrak{a}_{n+k}$ für alle $k \geq 0$.

(c) Jede nichtleere Menge I von Idealen von R besitzt ein maximales Element, d.h., es existiert ein $\mathfrak{b} \in I$ derart, dass kein $\mathfrak{a} \in I$ existiert mit $\mathfrak{b} \subsetneqq \mathfrak{a}$.

Beweis (a) $\Rightarrow$ (b): Man zeigt leicht, dass $\bigcup\limits_{n\geq 0} \mathfrak{a}_n =: \mathfrak{a}$ ein Ideal ist (je endlich viele Elemente von $\mathfrak{a}$ liegen in einem $\mathfrak{a}_m$ für geeignetes $m \in \mathbb{N}$). Ist $\mathfrak{a} = \langle a_1, \ldots, a_r \rangle$, so gibt es auch ein $\mathfrak{a}_n$ mit $a_1, \ldots, a_r \in \mathfrak{a}_n$. Die Inklusionen

$$\langle a_1, \ldots, a_r \rangle \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+k} \subseteq \mathfrak{a} = \langle a_1, \ldots, a_r \rangle$$

sind dann alles Gleichheiten.

(b) $\Rightarrow$ (c): Gäbe es in I kein maximales Element, so hätte man eine aufsteigende Kette $\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \ldots$.

(c) $\Rightarrow$ (a): Sei $\mathfrak{a}$ ein Ideal von R und I die Menge aller in $\mathfrak{a}$ enthaltenen endlich erzeugten Ideale. Wegen $\{0\} \in I$ ist I nichtleer, nach (c) gibt es also ein maximales Element $\mathfrak{c} = \langle c_1, \ldots, c_r \rangle \in I$. Es ist nach Definition $\mathfrak{c} \subseteq \mathfrak{a}$. Ist $a \in \mathfrak{a}$, so ist $\mathfrak{c}' = \langle c_1, \ldots, c_r, a \rangle \subseteq \mathfrak{a}$, $\mathfrak{c} \subset \mathfrak{c}'$, also $\mathfrak{c} = \mathfrak{c}'$ wegen der Maximalität von $\mathfrak{c}$, d.h., $a \in \mathfrak{c}$. Damit ist $\mathfrak{a} = \mathfrak{c}$ endlich erzeugt.

Beispiele 1.3 (a) Körper und Hauptidealringe sind trivialerweise noethersch; insbesondere ist $\mathbb{Z}$ noethersch.

(b) Der Ring $C([0,1], \mathbb{R})$ der stetigen reellwertigen Funktionen auf dem Intervall $[0,1]$ ist nicht noethersch: für jedes $n \in \mathbb{N}$ ist die Menge $\mathfrak{a}_n = \{f \in C([0,1], \mathbb{R}) \mid f_{|_{[0,\frac{1}{n}]}} = 0\}$ ein Ideal, und es ist $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \mathfrak{a}_3 \subsetneqq \ldots$.

(c) Ist R noethersch, so ist jedes epimorphe Bild R' von R wieder noethersch.

Satz 1.4 (Hilbertscher Basissatz) Ist R noethersch, so auch $R[X]$.

Beweis (nach Heidrun Sarges) Angenommen $\mathfrak{a} \neq \{0\}$ ist ein nicht endlich erzeugtes Ideal in $R[X]$. Dann sei f_1 ein Polynom minimalen Grades in $\mathfrak{a} \setminus \{0\}$, f_2 minimalen Grades in $\mathfrak{a} \setminus (f_1)$ usw., so dass man eine Folge $f_1, f_2, f_3, \ldots$ in $\mathfrak{a}$ erhält mit f_k minimalen Grades in $\mathfrak{a} \setminus \langle f_1, \ldots, f_{k-1} \rangle$. Sei $n_k = \deg(f_k)$ und a_k der Leitkoeffizient von f_k. Dann ist $n_{k+1} \geq n_k$ (nach Definition) und $\langle a_1, \ldots, a_k \rangle \subsetneqq \langle a_1, \ldots a_{k+1} \rangle$ für alle k, also R nicht noethersch. Wäre nämlich

$$a_{k+1} = \sum_{i=1}^{k} r_i a_i \qquad \text{mit } r_i \in R\,,$$

so läge das Polynom

$$g = \sum_{i=1}^{k} r_i x^{n_{k+1}-n_i} f_i$$

in $\langle f_1, \ldots, f_k \rangle$ und hätte den Leitkoeffizienten a_{k+1} und den Grad n_{k+1}. Dann wäre $f_{k+1} - g \in \mathfrak{a} \setminus \langle f_1, \ldots, f_k \rangle$ und $\deg(f_{k+1} - g) < n_{k+1} = \deg(f_{k+1})$, im Widerspruch zur Wahl von f_{k+1}.

Durch vollständige Induktion folgt:

Corollar 1.5 Ist R noethersch (z.B. $R = \mathbb{Z}$ oder $R =$ ein Körper K), so ist $R[X_1, \ldots, X_n]$ noethersch.

2 Moduln über Ringen und exakte Sequenzen

Sei R ein Ring mit Eins (nicht notwendig kommutativ). Der Begriff eines Moduls verallgemeinert den Begriff eines Vektorraums über einem Körper.

Definition 2.1 (a) Ein (linker) R-**Modul** ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Verknüpfung

$$\begin{array}{rcl} R\times M & \to & M \\ (r,m) & \mapsto & rm \end{array}$$

so dass gilt

$$\begin{array}{lrcl} \text{(i)} & r(m+n) & = & rm+rn \\ \text{(ii)} & (r+s)m & = & rm+sn \\ \text{(iii)} & (rs)m & = & r(sm) \\ \text{(iv)} & 1m & = & m \end{array}$$

für alle $r,s\in R$ und $m,n\in M$.

(b) Seien M und N R-Moduln. Eine Abbildung $\varphi: M\to N$ heißt **Homomorphismus von R-Moduln** (oder R-**linear**), wenn gilt:

(i) $\varphi(m_1+m_2)=\varphi(m_1)+\varphi(m_2)$ für alle $m_1,m_2\in M$ (d.h., φ ist ein Gruppenhomomorphismus von $(M,+)$ nach $(N,+)$),

(ii) $\varphi(rm)=r\varphi(m)$ für alle $m\in M, r\in R$.

Sei $Hom_R(M,N)$ die abelsche Gruppe der R-linearen Abbildungen von M nach N.

Bemerkungen 2.2 (a) Ein rechter R-Modul M ist ebenso definiert, wobei man allerdings die Eigenschaft (iii) ersetzt durch

$$\text{(iii')} \qquad (rs)m = s(rm)\,.$$

Schreibt man die Verknüpfung anders, nämlich

$$\begin{array}{rcl} M\times R & \to & M \\ (m,r) & \mapsto & mr\,, \end{array}$$

so wird hieraus die einleuchtendere Beziehung

$$m(rs)=(mr)s\,.$$

(b) Für einen kommutativen Ring sind Links- und Rechtsmoduln dasselbe.

(c) Wie üblich nennt man eine R-lineare Abbildung $\varphi: M\to N$ **Monomorphismus** (bzw. **Epimorphismus**, bzw. **Isomorphismus**), wenn sie injektiv (bzw. surjektiv, bzw. bijektiv) ist.

(d) Die Komposition von R-linearen Abbildungen ist wieder linear. Das Inverse eines R-Moduls-Isomorphismus ist wieder R-linear.

Beispiele 2.3 (a) Jede abelsche Gruppe A wird zu einem $\mathbb{Z}$-Modul durch die Definition

$$na = a + \ldots + a \quad (n\text{-mal}) \quad \text{für } n \in \mathbb{N}\,,$$

$$\begin{aligned} 0a &= 0 \\ (-n)a &= -(na) \quad \text{für } n \in \mathbb{N}\,. \end{aligned}$$

Man sieht, dass abelsche Gruppen und $\mathbb{Z}$-Moduln dasselbe sind.

(b) Ist $(M_i)_{i\in I}$ eine Familie von R-Moduln, so werden die abelschen Gruppen

$$\prod_{i\in I} M_i \quad \supseteq \quad \bigoplus_{i\in I} M_i$$

zu R-Moduln durch die Definition $r(m_i)_{i\in I} := (rm_i)_{i\in I}$.

Bezeichnung: **direktes Produkt** bzw. **direkte Summe** der R-Moduln M_i.

(c) Ist K ein Körper , so ist ein K-Modul dasselbe wie ein K-Vektorraum.

(d) Die Multiplikation in einem Ring R macht R zu einem R-Modul.

Definition 2.4 Ein R-Modul M heißt **freier** R-Modul, wenn es eine Familie $(m_i)_{i\in I}$ von Elementen $m_i \in M$ gibt, so dass gilt: Jedes Element $m \in M$ besitzt eine eindeutige Darstellung

$$m = \sum_{i\in I} r_i m_i\,,$$

mit $r_i \in R$ und $r_i = 0$ für fast alle $i \in I$ (so dass die Summe rechts endlich ist, wenn wir die Summanden mit $r_i = 0$ weglassen). Eine solche Familie $(m_i)_{i\in I}$ heißt Basis von M.

Beispiele 2.5 (a) Sei I eine Menge. Dann ist der R-Modul

$$F_R(I) := \bigoplus_{i\in I} R$$

frei mit Basis $(e_i)_{i\in I}$, wobei $e_i = (\delta_{ji})_{j\in I}$, mit dem Frolicker-Symbol

$$\delta_{ji} = \begin{cases} 1 & , \quad j = i \\ 0 & , \quad j \neq i \end{cases}$$

(mit $0, 1 \in R$). $F_R(I)$ heißt auch der freie R-Modul über I. Manchmal identifiziert man e_i mit i und schreibt die Elemente als formale Linearkombinationen

$$\sum_{i\in I} r_i i\,,$$

mit $r_i \in R$ wobei $r_i = 0$ für fast alle i.

(b) Der $\mathbb{Z}$-Modul $M = \mathbb{Z}/5\mathbb{Z}$ ist nicht frei, denn für jedes $m \in \mathbb{Z}/5\mathbb{Z}$ ist $1 \cdot m = m = 6 \cdot m$. Aber M ist ein freier Modul über dem Ring $\mathbb{Z}/5\mathbb{Z}$.

Lemma 2.6 (universelle Eigenschaft des freien Moduls) Sei M ein R-Modul und $(m_i)_{i\in I}$ eine Familie von Elementen $m_i \in M$. Dann gibt es genau einen R-Modul-Homomorphismus

$$\varphi : F_R(I) \to M$$

mit $\varphi(e_i) = m_i$ für alle $i \in I$ (Es gilt also $Hom_R(F_R(I), M) \xrightarrow{\sim} Abb(I, M)$ vermöge $\varphi \mapsto (\varphi(e_i))_{i\in I}$).

Beweis: Setze $\varphi((r_i)) = \sum_{i\in I} r_i m_i$.

Bemerkung 2.7 M ist genau dann frei mit Basis $(m_i)_{i\in I}$ wenn das obige φ ein Isomorphismus ist.

Definition 2.8 Sei M ein R-Modul. Ein (R-)Untermodul von M ist eine Teilmenge $N \subseteq M$, für die gilt:

(i) N ist Untergruppe bezüglich $+$,

(ii) für alle $n \in N$ und $r \in R$ gilt $rn \in N$.

Beispiel 2.9 Die Untermoduln des R-Moduls R (siehe 2.3 (d)) sind gerade die Ideale von R.

Lemma 2.10 Ist $\varphi : M \to N$ ein Homomorphismus von R-Moduln, so ist $\ker\varphi$ ein Untermodul von M und $\operatorname{im}\varphi$ ein Untermodul von N.

Beweis: leicht!

Satz 2.11 Ist M ein R-Modul und $N \subseteq M$ ein Untermodul, so wird die Faktorgruppe

$$M/N$$

zu einem R-Modul durch die Definition

$$r(m + N) \;:=\; rm + N \quad \text{für } r \in R, m \in M$$

(also $r \cdot \overline{m} = \overline{rm}$, wenn $\overline{m}$ die Nebenklasse von $m \in M$ bezeichnet). Die Surjektion $\pi : M \to M/N$ ist R-linear. Der Modul M/N wird als Quotientenmodul (oder Faktormodul) von M nach (oder modulo) N bezeichnet.

Beweis: selbst! Ebenso folgt sofort:

Bemerkungen 2.12 Der Homomorphiesatz sowie erster und zweiter Isomorphiesatz übertragen sich auf R-Moduln:

(a) Eine R-lineare Abbildung $\varphi : M \to N$ induziert einen R-Modul-Isomorphismus

$$M/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi\,.$$

(b) Für Untermoduln $N_1, N_2 \subset M$ hat man einen R-Modul-Isomorphismus

$$N_1/(N_1 \cap N_2) \xrightarrow{\sim} (N_1 + N_2)/N_2\,.$$

(c) Für Untermoduln $M_3 \subset M_2 \subset M_1$ hat man einen R-Isomorphismus

$$(M_1/M_3)/(M_2/M_3) \xrightarrow{\sim} M_1/M_2\,.$$

Definition 2.13 (a) Ein Komplex von R-Moduln ist eine Sequenz

$$\ldots \to M^n \stackrel{d^n}{\to} M^{n+1} \stackrel{d^{n+1}}{\to} M^{n+2} \to \ldots ,$$

wobei die M^n R-Moduln sind und die d^n lineare Abbildungen mit $d^{n+1}d^n = 0$ (Wir lassen offen, ob die Sequenz unendlich ist oder irgendwo abbricht). Offenbar folgt aus $d^{n+1}d^n = 0$

$$im\, d^n \subseteq \ker d^{n+1} .$$

(b) Die n-te Kohomologie des Komplexes ist der R-Modul

$$H^n(M^{\cdot}) = \ker d^n / \text{ im } d^{n-1}$$

(c) Der Komplex heißt exakt an der Stelle n, wenn $H^n(M^{\cdot}) = 0$, bzw. exakt, wenn er an allen Stellen exakt ist.

Definition 2.14 Eine exakte Sequenz von R-Moduln

$$0 \to M \to N \to P \to 0$$

heißt kurze exakte Sequenz.

Lemma 2.15 Eine Sequenz von R-Moduln

$$0 \to M \stackrel{i}{\to} N \stackrel{p}{\to} P \to 0$$

ist genau dann exakt, wenn gilt:
(i) i ist injektiv.
(ii) p ist surjektiv.
(iii) $im(i) = \ker(p)$.

Beweis $\ker(i) = im(0 \to M) = 0$ gilt genau dann, wenn i injektiv ist, und $im(p) = \ker(P \to 0) = P$ gilt genau dann, wenn p surjektiv ist.

Bemerkung 2.16 Für eine kurze exakte Sequenz wie oben liefert der Homomorphiesatz eine Isomorphie

$$N/i(M) \stackrel{\sim}{\to} P ,$$

und wir können M mit $i(M)$ identifizieren. Ist umgekehrt $p : N \to P$ ein Epimorphismus von R-Moduln und $M = \ker(p)$, so erhalten wir eine exakte Sequenz

$$0 \to M \stackrel{i}{\to} N \stackrel{p}{\to} P \to 0 ,$$

wobei i die Inklusion ist. In diesem Sinne entspricht eine kurze exakte Sequenz

$$0 \to M \to N \to P \to 0$$

einer Beziehung

$$N/M \stackrel{\sim}{\to} P .$$

Definition 2.17 Für einen Morphismus $\varphi : M \to N$ von R-Moduln heißt der Quotient $N/im(\varphi)$ der Cokern von φ; Bezeichnung $coker(\varphi)$.

Bemerkung 2.18 Wir erhalten also eine exakte Sequenz

$$0 \to \ker(\varphi) \to M \xrightarrow{\varphi} N \to coker(\varphi) \to 0\,.$$

Lemma 2.19 Sei

$$\begin{array}{ccc} M' & \xrightarrow{\varphi'} & N' \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle g} \\ M & \xrightarrow{\varphi} & N \end{array}$$

ein kommutatives Diagramm von R-Moduln (das heißt, alle Abbildungen sind R-Modulhomomorphismen, und es ist $\varphi' f = g\varphi$). Dann erhalten wir eindeutig bestimmte R-Modulhomomorphismen

$$\begin{array}{rrcrcl} & \tilde{f} & : & \ker(\varphi) & \to & \ker(\varphi') \\ \text{und} & \tilde{g} & : & coker(\varphi) & \to & coker(\varphi')\,, \end{array}$$

die das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\varphi') & \longrightarrow & M' & \xrightarrow{\varphi'} & N' & \longrightarrow & coker(\varphi') & \longrightarrow & 0 \\ & & {\scriptstyle \tilde{f}}\uparrow & & {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle \tilde{g}} & & \\ 0 & \longrightarrow & \ker(\varphi) & \longrightarrow & M & \xrightarrow{\varphi} & N & \longrightarrow & coker(\varphi) & \longrightarrow & 0 \end{array}$$

kommutativ machen (d.h., alle Quadrate sind kommutativ). Man sagt, dass $\widetilde{f}$ und $\widetilde{g}$ von f bzw. g induziert sind.

Beweis Offenbar muss $\tilde{f} = f|_{\ker(\varphi)}$ sein, und wir haben nur zu zeigen, dass $f(\ker(\varphi)) \subseteq \ker(\varphi')$. Ist aber $x \in \ker(\varphi)$, d.h., $x \in M$ mit $\varphi(x) = 0$, so ist

$$\begin{array}{rcl} 0 & = & g\varphi(x) \\ & = & \varphi'(f(x)) \quad \text{[Kommutativität des mittleren Quadrats]}, \end{array}$$

also $f(x) \in \ker(\varphi')$.

Für die Abbildung $\tilde{g}$ folgt notwendigerweise

$$\begin{array}{rrcl} \tilde{g}: \; coker(\varphi) = & N/im(\varphi) & \to & N'/im(\varphi') = coker(\varphi) \\ & y + im(\varphi) & \mapsto & g(y) + im(\varphi') \end{array}$$

und wir haben zu zeigen, dass dies wohldefiniert ist. Sei also $y + im(\varphi) = y' + im(\varphi)$, d.h., $y - y' \in im(\varphi)$, d.h., $y - y' = \varphi(x)$ für ein $x \in M$. Dann ist

$$g(y) - g(y') = g(y - y') = g\varphi(x) = \varphi' f(x) \in im(\varphi')\,,$$

d.h., $g(y) + im(\varphi') = g(y') + im(\varphi')$. Offenbar sind $\tilde{f}$ und $\tilde{g}$ eindeutig bestimmt.

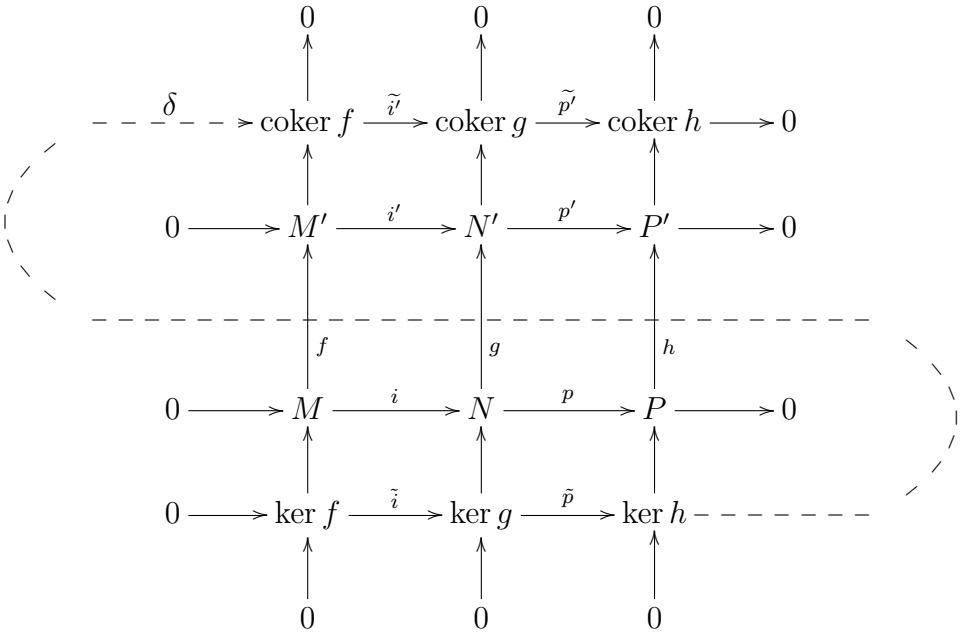
Satz 2.20 (Schlangenlemma) Sei

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i'} & N' & \xrightarrow{p'} & P' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & N & \xrightarrow{p} & P & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von R-Moduln (und R-Modul-Homomorphismen), mit exakten Zeilen. Dann haben wir eine kanonische exakte Sequenz von R-Moduln

$$0 \to \ker(f) \xrightarrow{\tilde{i}} \ker(g) \xrightarrow{\tilde{p}} \ker(h) \xrightarrow{\delta} coker(f) \xrightarrow{\tilde{i}'} coker(g) \xrightarrow{\tilde{p}'} coker(h) \to 0 \tag{2.20.1}$$

Beweis Der Name kommt von dem folgenden Gesamtdiagramm



Hier sind die Spalten nach Bemerkung 2.18 exakt, und die Modulhomomorphismen $\tilde{i}, \tilde{p}, \widetilde{i'}, \widetilde{p'}$ sind nach Lemma 2.19 von i, p, i' und p' induziert.

Die Definition von δ ist weniger offensichtlich. Sie folgt dem gestrichelten Weg: Ist $x \in \ker(h)$, so liegt $x \in P$, und wegen der Surjektivität von p gibt es ein $n \in N$ mit $p(n) = x$. Sei $n' = g(n) \in N'$. Dann ist $p'(n') = 0$, denn es ist $p'(n') = p'g(n) = hp(n) = h(x) = 0$, da $x \in \ker(h)$ nach Voraussetzung. Da die Sequenz $0 \to M' \xrightarrow{i'} N' \xrightarrow{p'} P' \to 0$ exakt ist und $p'(n') = 0$ ist, gibt es ein $m' \in M'$ mit $i'(m') = n'$ ($im(i') = \ker(p')$). Wir definieren nun

$$\delta(x) = \text{ Bild von } m' \text{ in coker } f.$$

Wir müssen zeigen, dass dies wohldefiniert ist, denn wir haben eine Wahl für $n \in N$ mit $p(n) = x$ getroffen. Ist $n_1 \in N$ ein anderes Element mit $p(n_1) = x$, so folgt wie oben die Existenz eines Elementes $m_1' \in M'$ mit $i'(m_1') = n_1' := g(n_1)$. Wir haben nun zu zeigen, dass m' und m_1' dasselbe Bild in $coker(f)$ haben. Es ist aber $n_1 - n \in \ker(p)$, denn es ist $p(n_1 - n) = p(n_1) - p(n) = x - x = 0$. Wegen der Exaktheit von $0 \to M \xrightarrow{i} N \to P \to 0$ gibt es also ein $m \in M$ mit $i(m) = n_1 - n$. Damit gilt

$$i'(m_1' - m_1) = n_1' - n' = g(n_1) - g(n) = g(n_1 - n) = gi(m) = i'f(m)\,,$$

da wegen der Kommutativität des Diagramm $gi = i'f$ gilt. Da weiter i' injektiv ist, gilt sogar

$$m_1' - m_1 = f(m)\,.$$

Da per Definition $coker(f) = M'/im(f)$, haben also m_1 und m_1' dasselbe Bild in dieser Gruppe, was zu zeigen war.

Nachdem wir alle Abbildungen definiert haben, zeigen wir nun die Exaktheit von (2.20.1). Der Homomorphismus $\tilde{i}$ ist injektiv, da die Abbildungen $\ker(f) \hookrightarrow M \xrightarrow{i} N$ injektiv sind, also auch die Komposition, also auch $\ker(f) \xrightarrow{\tilde{i}} \ker(g) \hookrightarrow N$. Dies kann nur sein, wenn schon $\tilde{i}$ injektiv ist. Ähnlich zeigt man die Surjektivität von $\widetilde{p'}$.

Nun zeigen wir die Exaktheit bei $\ker(g)$. Offenbar ist $\tilde{p}\tilde{i} = 0$, denn dies ist die Einschränkung von $pi = 0$ auf $\ker f$. Sei weiter $y \in \ker(g)$ mit $\tilde{p}(y) = 0$. Dann ist auch $p(y) = 0$, also $y = i(z)$ für ein $z \in M$ wegen der Exaktheit dieser Zeile (so dass $im(i) = \ker(p)$).

Wir bemerken nun, dass $z \in \ker(f)$: Es ist nämlich $i'f(z) = gi(z) = g(y) = 0$, da $y \in \ker(g)$ Da i' injektiv ist, folgt hieraus aber, dass $f(z) = 0$, also $z \in \ker(f)$. Damit liegt y im Bild von $\ker(f)$.

Nun zeigen wir die Exaktheit bei $\ker(h)$. Mit den Bezeichnungen von oben folgern wir: Ist $x \in \ker(h)$ mit $\delta(x) = 0$, so wird m' auf 0 in $coker(f)$ abgebildet, liegt also im Bild von f. Sei $m \in M$ mit $f(m) = m'$. Betrachte nun $n - i(m)$. Es ist $p(n - i(m)) = p(n) = x$ (da $pi = 0$) und andererseits $g(n - i(m)) = g(n) - gi(m) = n' - i'f(m) = n' - i'(m') = 0$ nach Konstruktion von m'. Also ist $x = p(n - i(m))$ mit $n - i(m) \in \ker(g)$, d.h., $x \in im(\tilde{p})$.

Exaktheit an den anderen Stellen (d.h., in der Kokern-Sequenz): selbst!

Satz 2.20' Als Variante erhält man: Ist

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \xrightarrow{i'} & N' & \xrightarrow{p'} & P' \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle g} \\ & & M & \xrightarrow{i} & N & \xrightarrow{p} & P \longrightarrow 0 \end{array}$$

ein kommutatives Diagramm von R-Moduln mit exakten Zeilen, so hat man eine exakte Sequenz

$$\ker(f) \to \ker(g) \to \ker(h) \xrightarrow{\delta} coker(f) \to coker(g) \to coker(h)$$

Beweis: Dies folgt genauso wie in Satz 2.20, wobei nicht benötigt wird, dass i injektiv und p surjektiv ist.

Wir erhalten die folgende Anwendung auf Komplexe.

Sprechweise 2.21: Für einen Komplex (M^n, d^n) heißen die Elemente in $\ker d^n$ n-Zykel und die Elemente in $im\, d^{n-1}$ n-Ränder.

Definition 2.22 Ein Morphismus von Komplexen von R-Moduln

$$f : M^{\cdot} \to N^{\cdot}$$

besteht aus einer Familie von R-Modul-Homomorphismen $f_n : M^n \to N^n$, so dass alle Diagramme

(2.22.1)
$$\begin{array}{ccc} M^{n+1} & \xrightarrow{f_{n+1}} & N^{n+1} \\ {\scriptstyle d_M^n}\uparrow & & \uparrow{\scriptstyle d_N^n} \\ M^n & \xrightarrow{f_n} & N^n \end{array}$$

kommutieren (also $d_N^{n+1} f_n = f_{n+1} d_M^n$).

(a) Eine Sequenz von Komplexen

$$0 \to M^{\cdot} \xrightarrow{f} N^{\cdot} \xrightarrow{g} P^{\cdot} \to 0$$

heißt exakt, wenn alle Sequenzen

$$0 \to M^n \xrightarrow{f_n} N^m \xrightarrow{g_n} P^n \to 0$$

Lemma 2.23 Ist

$$f : M^{\cdot} \to N^{\cdot}$$

ein Morphismus von Komplexen von R-Moduln, so induziert f kanonische Morphismen der Kohomologiemoduln

$$f_* = H^n(f_{\cdot}) : H^n(M^{\cdot}) \to H^n(N^{\cdot})$$

für alle n.

Beweis Nach Lemma 2.19, angewandt auf die Diagramme (2.22.1), induziert $f_n : M^n \to N^n$ R-Modulhomomorphismen

$$\begin{array}{ccc} \ker d_M^n & \longrightarrow & \ker d_N^n \\ \uparrow & & \uparrow \\ im\, d_M^{n-1} & \longrightarrow & im\, d_N^{n-1} \end{array}$$

(beachte: $im\, d_M^{n-1} \subseteq \ker d_M^n$ wegen $d_M^n d_M^{n-1} = 0$; entsprechend für N), und damit, wieder nach 2.19, einen Homomorphismus der Cokerne

$$f_* : H^n(M^{\cdot}) = \ker d_M^n / im\, d_M^{n-1} \to \ker d_N^n / im\, d_N^{n-1} = H^n(N^{\circ})\,.$$

Bezeichnet $[m]$ die Kohomologieklasse eines Zykels $m \in \ker d_M^n$, so wird also $[m]$ einfach auf $[f_n(m)]$ abgebildet.

Satz 2.24 Ist

$$0 \to M^{\cdot} \xrightarrow{f} N^{\cdot} \xrightarrow{g} P^{\cdot} \to 0$$

eine kurze exakte Sequenz von Komplexen, so erhält man eine kanonische exakte Sequenz

$$\ldots \to H^n(M^{\cdot}) \xrightarrow{H^n(f)} H^n(N^{\cdot}) \xrightarrow{H^n(g)} H^n(P^{\cdot}) \xrightarrow{\delta^n} H^{n+1}(M^{\cdot}) \to \ldots$$

Diese heißt die assoziierte **lange exakte Kohomologiesequenz**, und δ^n heißt der **Verbindungshomomorphismus**.

Beweis Die Abbildungen $H^n(f)$ und $H^n(g)$ wurden oben definiert. Wir definieren nun δ^n. Die obige exakte Sequenz von Komplexen induziert ein kommutatives Diagramm

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \ker d_M^{n+1} & \longrightarrow & \ker d_M^{n+1} & \longrightarrow & \ker d_P^{n+1} \\
 & & \uparrow{\scriptstyle \widetilde{d_M^n}} & & \uparrow{\scriptstyle \widetilde{d_N^n}} & & \uparrow{\scriptstyle \widetilde{d_P^n}} \\
 & & M^n/im\, d_M^{n-1} & \xrightarrow{\tilde{f}_n} & N^n/im\, d_N^{n-1} & \xrightarrow{\tilde{g}_n} & P^n/im\, d_p^{n-1} \longrightarrow 0
\end{array}
\tag{2.24.1}
$$

Hierbei ist der R-Modulhomomorphismus $\widetilde{d_M^n}$ von

$$d_M^n : M^n \to M^{n+1}$$

induziert, mittels des Homomorphiesatzes, denn $im\, d_M^{n-1}$ liegt nach Definition eines Komplexes in $\ker d_M^n$ ($d_M^n\, d_M^{n-1} = 0$). Entsprechend sind dann $\widetilde{d_N^n}$ und $\widetilde{d_P^n}$ (wohl-)definiert.

Ebenso induziert $f_n : M^n \to N^n$ wegen der Kommutativität von

$$
\begin{array}{ccc}
M^n & \xrightarrow{f_n} & N^n \\
\uparrow{\scriptstyle d_M^{n-1}} & & \uparrow{\scriptstyle d_N^{n-1}} \\
M^{n-1} & \xrightarrow{f_{n-1}} & N^{n-1}
\end{array}
$$

einen R-Modulhomomorphismus $\tilde{f}_n : M^n/im\, d_M^{n-1} \to N^n/in\, d_N^{n-1}$ nach 2.19. Analog erhalten wir $\tilde{g}_n$.

Weiter sind die Zeilen in (2.24.1) exakt.

Für die obere Zeile folgt dies mit dem Schlangenlemma für die Kerne in dem kommutativen Diagramm mit exakten Zeilen

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M^{n+2} & \longrightarrow & N^{n+2} & \longrightarrow & P^{n+2} & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle d_M^{n+1}} & & \uparrow{\scriptstyle d_N^{n+1}} & & \uparrow{\scriptstyle d_P^{n+1}} & & \\
0 & \longrightarrow & M^{n+1} & \longrightarrow & N^{n+1} & \longrightarrow & P^{n+1} & \longrightarrow & 0
\end{array}
$$

Für die untere Zeile benutzt man das Schlangenlemma für die Cokerne in

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M^n & \longrightarrow & N^n & \longrightarrow & P^n & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle d_M^{n-1}} & & \uparrow{\scriptstyle d_N^{n-1}} & & \uparrow{\scriptstyle d_P^{n-1}} & & \\
0 & \longrightarrow & M^{n-1} & \longrightarrow & N^{n-1} & \longrightarrow & P^{n-1} & \longrightarrow & 0\,.
\end{array}
$$

Mit der Variante 2.20' des Schlangenlemmas folgt nun aus (2.24.1) die Exaktheit von

$$H^n(M^\cdot) \to H^n(N^\cdot) \to H^n(P^\cdot) \xrightarrow{\delta} H^{n+1}(M^\cdot) \to H^{n+1}(N^\cdot) \to H^{n+1}(P^\cdot)\,,$$

denn es ist

$$
\begin{array}{rcccl}
\ker \widetilde{d_M^n} & = & \ker d_M^n/im\, d_M^{n-1} & = & H^n(M^\cdot) \\
\operatorname{coker} \widetilde{d_M^n} & = & \ker d_M^{n+1}/im\, d_M^n & = & H^{n+1}(M^\cdot)\,,
\end{array}
$$

und dies gilt analog auch für $N^\cdot$ und $P^\cdot$.

3 Lokalisierungen und lokale Ringe

Der folgende Begriff verallgemeinert den Begriff des Quotientenkörpers. Sei A ein kommutativer Ring mit Eins.

Definition 3.1 Eine Teilmenge $S \subseteq A$ heißt multiplikativ (oder multiplikativ abgeschlossen), wenn $1 \in S$ und wenn mit a und b in S auch $a \cdot b$ in S liegt.

Beispiele 3.2 (a) Für jedes $f \in A$ ist die Menge $\{f^n \mid n \in \mathbb{N}_0\}$ multiplikativ (wobei wir setzen: $f^0 := 1$).

(b) *(wichtig!)* Sei $\mathfrak{a} \subseteq A$ ein Ideal. Die Menge $A \setminus \mathfrak{a}$ ist genau dann multiplikativ, wenn $\mathfrak{a}$ ein Primideal ist.

(c) Erinnerung: ein Element $f \in A$ heißt Nullteiler wenn es ein $g \neq 0$ in A gibt mit $f \cdot g = 0$. Die Menge U_A der Nicht-Nullteiler in A ist multiplikativ.

Sei $S \subseteq A$ multiplikativ. Betrachte auf der Menge $A \times S$ die folgende Relation

$$(a, s) \sim (a', s') :\Leftrightarrow \text{ es ex. ein } t \in S \text{ mit } ts'a = tsa'$$

Dann ist $\sim$ eine Äquivalenzrelation: Reflexivität und Symmetrie sind klar, und für die Transitivität "braucht man das t" in der Definition, falls S Nullteiler hat:

$$t(s'a - s\,a') = 0 \quad , \quad t'(s''a' - s'a'') = 0 \quad \Rightarrow \quad t\,t's'(s''a - s\,a'') = 0$$

Für $(a, s) \in A \times S$ sei $\frac{a}{s}$ die Äquivalenzklasse von (a,s) bezüglich $\sim$. Die Menge $A \times S/\sim$ der Äquivalenzklassen wird mit A_S (oder $S^{-1}A$ oder $A[S^{-1}]$) bezeichnet.

Satz/Definition 3.3 (a) A_S wird mit den Verknüpfungen

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &:= \frac{at+bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st} \end{aligned}$$

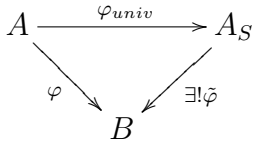
ein Ring (kommutativ, mit Eins) und heißt die Lokalisierung von A nach S.

(b) Die Abbildung

$$\begin{aligned} \varphi_{univ} : A &\to A_S \\ a &\mapsto \frac{a}{1} \end{aligned}$$

ist ein Ringhomomorphismus und alle Elemente in $\varphi_{univ}(S)$ sind invertierbar in A_S.

(c) (universelle Eigenschaft) Ist $\varphi : A \to B$ ein Ringhomomorphismus derart, dass $\varphi(S)$ aus lauter invertierbaren Elementen besteht, so gibt es einen eindeutig bestimmmten Ringhomomorphismus $\widetilde{\varphi} : A_S \to B$, der das Diagramm



kommutativ macht.

Beweis: (a) Wohldefiniertheit: Ist $\frac{a}{s} = \frac{a'}{s'}$ und $\frac{b}{t} = \frac{b'}{t'}$, so gibt es $s_1, s_2 \in S$ mit $s_1(s'a - sa) = 0$ und $s_2(t'b - tb') = 0$. Dann ist $s_1 s_2[(s't'(at + bs) - st(a't' + b's'))] = 0$, also

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'} ,$$

sowie $s_1 s_2[s't'ab - sta'b'] = 0$, also

$$\frac{ab}{st} = \frac{a'b'}{s't'} .$$

Der Beweis der Ring-Eigenschaften ist einfach unter der Benutzung der "Kürzungsregel"

$$\frac{a}{s} = \frac{ta}{ts} \quad \text{für } t \in S .$$

(b) Wegen $\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$ und $\frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$ ist φ_{univ} ein Ringhomomorphismus, und für $s \in S$ ist $\frac{1}{s}$ ein Inverses von $\varphi(s) = \frac{s}{1}$.

(c) Setze $\tilde{\varphi}(\frac{a}{s}) = \varphi(s)^{-1} \cdot \varphi(a)$. Dann folgen alle Eigenschaften einfach (Eindeutigkeit: $\varphi(a) = \tilde{\varphi}(\frac{a}{1}) = \tilde{\varphi}(\frac{a}{s} \cdot \frac{s}{1}) = \tilde{\varphi}(\frac{a}{s}) \cdot \tilde{\varphi}(\frac{s}{1}) = \tilde{\varphi}(\frac{a}{s}) \cdot \varphi(s) \Rightarrow \tilde{\varphi}(\frac{a}{s}) = \varphi(s)^{-1} \cdot \varphi(a)$.

Beispiele 3.4 (a) Enthält S die Null, so ist $A_S = 0$ (der Nullring).

(b) Für $f \in A$ und $S_f := \{f^n | n \in \mathbb{N}_0\}$ (vergl. 3.2 (a)) schreibt man auch A_f(oder $A[f^{-1}]$) für A_{S_f}.

(c) Allgemein sei für eine beliebige Menge $M \subseteq A$ definiert: $A[M^{-1}] := A[S_M^{-1}]$, wobei S_M die von M erzeugte multiplikative Teilmenge von A ist (existiert, als Durchschnitt aller multiplikativen Teilmengen S, die M enthalten). Dann hat $A[M^{-1}]$ eine analoge universelle Eigenschaft für Morphismen $\varphi : A \to B$, für die $\varphi(m)$ invertierbar ist für alle $m \in M$.

(d) Ist $\mathfrak{p} \subseteq A$ ein Primideal, so setze

$$A_{\mathfrak{p}} := A[(A \setminus \mathfrak{p})^{-1}] .$$

(e) Ist $U_A \subseteq A$ die Menge der Nicht-Nullteiler (vgl. 4.2.(c)), so heißt

$$Quot(A) := A[U_A^{-1}]$$

der totale Quotientenring von A.

(f) Ist A ein Integritätsbereich, so ist $U_A = A \setminus \{0\}$ und $Quot(A)$ ist ein Körper (*jedes* $\frac{a}{b} \neq 0$ hat ein Inverses!), der übliche *Quotientenkörper* von A.

Lemma 3.5 Die Abbildung $A \to A_S$ ist genau dann injektiv, wenn S keine Nullteiler enthält. Insbesondere ist also $A \to Quot(A)$ injektiv.

Beweis: selbst

Satz 3.6. Sei $\varphi : A \to B$ ein Homomorphismus von Ringen, und seien $S \subseteq A$ und $T \subseteq B$ multiplikative Teilmengen mit $\varphi(S) \subseteq T$. Dann existiert genau ein Ringhomomorphismus $\varphi' : A_S \to B_T$ der φ fortsetzt, d.h., der

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle \varphi_{univ}}\downarrow & & \downarrow{\scriptstyle \varphi_{univ}} \\ A_S & \xrightarrow{\varphi'} & B_T \end{array}$$

kommutativ macht.

Beweis: $(\varphi_{univ} \circ \varphi)(S)$ besteht ganz aus Einheiten; nach der universellen Eigenschaft 3.3. (c) gibt es also genau einen Ringhomomorphismus, der das untere Dreieck in

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & \overset{\varphi_{univ}\circ\varphi}{\searrow} & \downarrow \\ A_S & \longrightarrow & B_T \end{array}$$

kommutativ macht.

Corollar 3.7. Seien

$$\begin{array}{ccccccc} A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & & \text{Ringhomomorphismen} \\ \cup| & & \cup| & & \cup| & & \\ S & \to & T & \to & U & & \text{multiplikative Teilmengen} \end{array}$$

Dann gilt $\psi' \circ \varphi' = (\psi \circ \varphi)' : A_S \to C_U$.

Beweis: $\psi' \circ \varphi'$ leistet dieselbe Kommutativität wie $\psi \circ \varphi$.

Satz/Definition 3.8 Für einen A-Modul M und eine multiplikative Teilmenge $S \subseteq A$ definiere

$$M_S = (M \times S)/\sim$$

wobei $(m, s) \sim (m', s')$ falls ein $t \in S$ existiert mit $ts'm = tsm'$ (Andere Bezeichnungen: $S^{-1}M$ oder $M[S^{-1}]$). Die Äquivalenzklasse von (m, s) sei mit $\frac{m}{s}$ bezeichnet. Dann wird M_S ein A_S-Modul durch die Definitionen

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st} \quad , \quad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

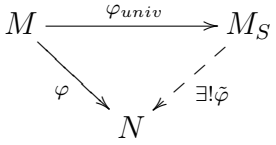
für $m, n \in M,\ s, t \in S$ und $a \in A$.

(b) (universelle Eigenschaft) Es gibt einen kanonischen A-Modul-Homomorphismus $\varphi_{univ} : M \to M_S$, und für $s \in S$ ist

$$\begin{array}{rccc} L_s : M_S & \to & M_S \\ x & \mapsto & s \cdot x \end{array}$$

ein Isomorphismus. Ist N ein weiterer A-Modul derart, dass für jedes $s \in S$ die Abbildung $L_s : N \to N, n \mapsto sn$, ein Isomorphismus ist, und ist $\varphi : M \to N$ ein A-Modul-Homomorphismus, so gibt es einen eindeutig bestimmten A-Modul-Homomorphismus

$\tilde{\varphi} : M_S \to N$ der



kommutativ macht. Weiter ist $\tilde{\varphi}$ ein A_S-Modul-Homomorphismus, wobei N ein A_S-Modul ist vermöge $\frac{a}{s}n = (L_s)^{-1}(an)$ für $n \in N$, $a \in A$ und $s \in S$.

(c) Insbesondere induziert jeder A-Modul-Homomorphismus $f : M \to N$ einen A_S-Modul-Homomorphismus

$$f_S : M_S \to N_S$$

mit $f_S(\frac{m}{s}) = \frac{f(m)}{s}$ für $m \in M, s \in S$.

Beweis der Behauptungen: Ähnlich wie für Satz 3.3.

Definition 3.9 (a) Für ein Primideal $\mathfrak{p} \subseteq A$ und die multiplikative Menge $S_\mathfrak{p} = A \setminus \mathfrak{p}$ schreibe $M_\mathfrak{p}$ statt $M_{S_\mathfrak{p}}$ (dies ist also ein $A_\mathfrak{p}$-Modul).

(b) Für $S_f = \{f^n | f \in \mathbb{N}_0\}, f \in A$, schreibe M_f statt M_{S_f} (dies ist ein A_f-Modul).

Satz 3.10 Lokalisierung ist exakt, d.h., ist $S \subseteq A$ eine multiplikative Teilmenge und

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

eine exakte Sequenz von A-Moduln, so ist auch

$$(M_1)_S \xrightarrow{f_S} (M_2)_S \xrightarrow{g_S} (M_3)_S$$

exakt (Daher folgt dasselbe für beliebige exakte Sequenzen).

Beweis: Sei $\frac{m_2}{s} \in (M_2)_S$ mit $0 = g_S(\frac{m_2}{s}) = \frac{g(m_2)}{s}$. Dann existiert ein $r \in S$ mit $0 = rg(m_2) = g(rm_2)$. Nach Voraussetzung existiert ein $m_1 \in M_1$ mit $rm_2 = f(m_1)$. Es folgt $\frac{m_2}{s} = \frac{f(m_1)}{rs} = f_S(\frac{m_1}{rs})$, d.h., $ker\, g_S \subseteq im f_S$. Die Inklusion $im f_S \subseteq ker\, g_S$ ist klar, denn es gilt $g_S f_S = 0$, wegen $gf = 0$.

Beispiele 3.11: (a) Ist $N \subseteq M$ ein Untermodul, $\mathfrak{p}$ ein Primideal, so gilt

$$(M/N)_\mathfrak{p} \cong M_\mathfrak{p}/N_\mathfrak{p}$$

(betrachte $0 \to N \to M \to M/N \to 0$).

(b) Ist

$$0 \to A \to B \to C \to 0$$

eine exakte Sequenz von abelschen Gruppen, so ist

$$0 \to A_\mathbb{Q} \to B_\mathbb{Q} \to C_\mathbb{Q} \to 0 \tag{3.11.1}$$

exakt, wobei wir definieren: $A_\mathbb{Q} := A_{(0)} = (\mathbb{Z} \setminus \{0\})^{-1}A$. Dies ist ein Modul über $(\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z} = \mathbb{Q}$, also ein $\mathbb{Q}$-Vektorraum, und es gilt $\dim_\mathbb{Q} A_\mathbb{Q} = rg\, A$. Aus der exakten Sequenz (3.11.1) und der Additivität der Dimension in exakten Sequenzen folgt

$$rg\, B \;=\; rg\, A + rg\, C\,.$$

Definition/Lemma 3.12 (a) Ein Ring A heißt lokal, wenn die folgenden äquivalenten Eigenschaften gelten:

(i) A hat genau ein maximales Ideal $\mathfrak{m}$.

(ii) Die Menge $A \setminus A^\times$ der Nichteinheiten ist ein Ideal.

(b) Es ist in diesem Fall $\mathfrak{m} = A \setminus A^\times$, und der Körper $A/\mathfrak{m}$ heißt der Restklassenkörper von A.

Beweis der Behauptungen: Für jeden Ring A ist

$$A \setminus A^\times = \bigcup_{\substack{\mathfrak{a} \subsetneq A \\ \text{Ideal}}} \mathfrak{a}\,, \tag{3.12.1}$$

denn es gilt für $f \in A$: $f \in A \setminus A^\times \;\Leftrightarrow\; 1 \notin (f) \;\Leftrightarrow\; (f) \neq A$.

Gilt nun (i), so ist $A \setminus A^\times = \mathfrak{m}$ (da alle $\mathfrak{a} \subseteq \mathfrak{m}$), und es folgt (ii). Gilt umgekehrt (ii), ist also $A \setminus A^\times$ ein Ideal, so enthält es alle Ideale $\mathfrak{a} \subsetneq A$, ist also maximal und das einzige maximale Ideal.

Beispiele 3.13: (a) Ein Körper ist ein lokaler Ring (mit maximalem Ideal (0)).

(b) Der Nullring ist kein lokaler Ring.

(c) Ist A ein lokaler Ring, so ist der Ring $R = A[[x_1, \ldots, x_n]]$ der formalen Potenzreihen in den Variablen $x_1, \ldots, x_n$ ein lokaler Ring und der Ringhomomorphismus $A \to A[[x_1, \ldots, x_n]]$ induziert einen Isomorphismus der Restklassenkörper: Wegen

$$A[[x_1, \ldots, x_n]] = A[[x_1, \ldots, x_{n-1}]][[x_n]]$$

können wir dies durch Induktion über n beweisen; es ist also ohne Einschränkung $n = 1$. Ein Element $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$ ist aber genau dann eine Einheit, wenn der konstante Term a_0 eine Einheit ist (Beweis selbst: löse $f \cdot g = 1$). Es folgt $A[[x]] \setminus A[[x]]^\times = (x) + \mathfrak{m}\, A[[x]]$ ($\mathfrak{m}$ das maximale Ideal von A); dies ist aber ein Ideal.

Der folgende Satz liefert viele Beispiele für lokale Ringe.

Satz 3.14 Sei A ein Ring und $\mathfrak{p} \subseteq A$ ein Primideal. Dann ist die Lokalisierung $A_\mathfrak{p}$ ein lokaler Ring mit maximalen Ideal $\mathfrak{p}A_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1}\mathfrak{p} = \{\frac{a}{b} \mid a \in \mathfrak{p},\ b \notin \mathfrak{p}\}$. Der Restklassenkörper $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ ist isomorph zu $Quot(A/\mathfrak{p})$.

Für einen Ringhomomorphismus $\varphi : A \to B$ und ein Ideal $\mathfrak{a} \subseteq A$ sei dabei $\mathfrak{a}B = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N},\ a_i \in \mathfrak{a},\ b_i \in B \right\}$ das von $\mathfrak{a}$ in B erzeugte Ideal, wobei wir für $a \in A$ und $b \in B$ setzen: $ab := \varphi(a) \cdot b$.

Beweis: 1) Wir zeigen zunächst die Gleichheit

$$\mathfrak{p}A_\mathfrak{p} = \left\{ \frac{b}{s} \mid b \in \mathfrak{p},\ s \in A \setminus \mathfrak{p} \right\}. \tag{3.14.1}$$

Zunächst ist die rechte Seite ein Ideal in $A_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1}A$, denn für $a \in A, b, c \in \mathfrak{p}$ und $s, t \in A \setminus \mathfrak{p}$ gilt

$$\begin{aligned} \frac{b}{s} + \frac{c}{t} &= \frac{tb + sc}{st} \in (A \setminus \mathfrak{p})^{-1}\mathfrak{p}\,, \\ \frac{a}{s} \cdot \frac{c}{t} &= \frac{ac}{st} \in (A \setminus \mathfrak{p})^{-1}\mathfrak{p}\,. \end{aligned}$$

Jedes Element $\sum_{i=1}^{r} b_i \frac{a_i}{t_i} \in \mathfrak{p}A_\mathfrak{p}$ (mit $b_i \in \mathfrak{p}, a_i \in A, t_i \in A \setminus \mathfrak{p}$) liegt also in $(A \setminus \mathfrak{p})^{-1}\mathfrak{p}$ (da $b_i \frac{a_i}{t_i} = \frac{b_i a_i}{t_i}$). Die umgekehrte Inklusion ist klar.

2) Hiermit sieht man, dass die folgenden Aussagen für $\frac{a}{s} \in A_\mathfrak{p}$ $(a \in A, s \in A \setminus \mathfrak{p})$ äquivalent sind:

$$\frac{a}{s} \notin \mathfrak{p}A_\mathfrak{p} \quad \Leftrightarrow \quad a \in A \setminus \mathfrak{p} \quad \Leftrightarrow \quad \frac{a}{s} \in A_\mathfrak{p}^\times\,. \tag{3.14.2}$$

Denn nach (3.14.1) gilt $\frac{a}{s} \notin \mathfrak{p}A\mathfrak{p} \Rightarrow a \notin \mathfrak{p}$; weiter gilt $a \in A \setminus \mathfrak{p} \Rightarrow \frac{a}{s} \in A_\mathfrak{p}^\times$ (ein Inverses von $\frac{a}{s}$ ist dann $\frac{s}{a}$). Schließlich gilt: $\frac{a}{s} \in A_\mathfrak{p}^\times \Rightarrow \frac{a}{s} \notin \mathfrak{p}A_\mathfrak{p}$, denn sonst wäre $1 = \frac{a}{s} \cdot (\frac{a}{s})^{-1} \in \mathfrak{p}A_\mathfrak{p}$, also $1 = \frac{b}{t}$ mit $b \in \mathfrak{p}$, $t \in A \setminus \mathfrak{p}$. Dann gäbe es ein $t' \in A \setminus \mathfrak{p}$ mit $t't = b$ im Widerspruch dazu, dass $t't \in A \setminus \mathfrak{p}$ aber $b \in \mathfrak{p}$. Mit (3.14.2) folgt nun $\mathfrak{p}A_\mathfrak{p} = A_\mathfrak{p} \setminus A_\mathfrak{p}^\times$, d.h., nach 3.12 ist $A_\mathfrak{p}$ lokal mit maximalem Ideal $\mathfrak{p}A_\mathfrak{p}$.

3) Der Ringhomomorphismus $A \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ induziert eine Einbettung $A/\mathfrak{p} \hookrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, und die universelle Eigenschaft des Quotientenkörpers induziert eine Einbettung

$$Quot(A/\mathfrak{p}) \hookrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}\,.$$

Diese ist auch surjektiv: Ist $\frac{a}{b} \in A_\mathfrak{p}$, mit $a \in A$ und $b \in A \setminus \mathfrak{p}$, so ist für die Restklassen $\overline{a}, \overline{b}$ in $A/\mathfrak{p}$ offenbar $\overline{b} \neq 0$, und das Element $\frac{\overline{a}}{\overline{b}} \in Quot(A/\mathfrak{p})$ wird auf die Restklasse von $\frac{a}{b}$ abgebildet.

Lokale Ringe sind insbesondere wegen der folgenden zwei Sätze interessant.

Satz 3.15 Für einen A-Modul M gilt

$$M = 0 \quad \Leftrightarrow \quad M_\mathfrak{p} = 0 \quad \text{für alle Primideale } \mathfrak{p} \subseteq A\,.$$

Beweis: Für die nicht-triviale Richtung sei $M_\mathfrak{p} = 0$ für alle Primideale $\mathfrak{p} \subseteq A$. Sei $x \in M$. Dann ist der **Annulator von** x

$$ann(x) := \{a \in A \mid ax = 0\}$$

offenbar ein Ideal in A. Gilt $x \neq 0$, so ist $1 \notin ann(x)$, also $ann(x)$ ein echtes Ideal in A. Dann gibt es ein maximales Ideal $\mathfrak{m} \subseteq A$ mit $ann(x) \subseteq \mathfrak{m}$ (siehe Algebra I, Satz 16.8). Wegen $M_\mathfrak{m} = 0$ gibt es aber ein $b \notin \mathfrak{m}$ mit $bx = 0$, also $b \in ann(x)$, Widerspruch!

Corollar 3.16 Ein Homomorphismus von A-Moduln

$$\varphi : M \to N$$

ist genau dann injektiv (bzw. surjektiv, bzw. bijektiv), wenn dies für alle induzierten Homomorphismen

$$\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}} \quad (\mathfrak{p} \subseteq A \text{ Primideal})$$

(siehe 3.8 (c)) gilt.

Beweis: Sei

$$0 \to K \to M \xrightarrow{\varphi} N \to C \to 0$$

exakt (also $K = \ker \varphi$ und $C = \operatorname{coker} \varphi$). Nach Satz 3.10 sind dann alle Sequenzen

$$0 \to K_{\mathfrak{p}} \to M_{\mathfrak{p}} \xrightarrow{\varphi_{\mathfrak{p}}} N_{\mathfrak{p}} \to C_{\mathfrak{p}} \to 0$$

exakt. Zusammen mit Satz 3.15 folgt die Behauptung (Zum Beispiel: φ injektiv $\Leftrightarrow$ $K = 0 \Leftrightarrow K_{\mathfrak{p}} = 0 \; \forall \mathfrak{p} \Leftrightarrow \varphi_{\mathfrak{p}}$ injektiv $\forall \mathfrak{p}$).

Satz 3.17 (Krull-Nakayama-Lemma) Sei A ein Ring und $I \subseteq A$ ein Ideal, welches in allen maximalen Idealen von A enthalten ist. Sei M ein A-Modul und $N \subseteq M$ ein Untermodul derart, dass M/N endlich erzeugt ist. Gilt $M = N + IM$, so ist schon $M = N$.

(Die Beziehung $M = N + IM$ sollte so gelesen werden, dass der Homomorphismus $\varphi : N/IN \to M/IM$ surjektiv ist, d.h., dass $im\,\varphi = N + IM/IM = M/IM$; es ist also "$M = N$ modulo I").

Beweis Seien $m_1, \ldots, m_t \in M$ derart, dass die Bilder in $\overline{M} := M/N$ ein minimales Erzeugendensystem bilden. Angenommen $t > 0$. Wegen $\overline{M} = I\overline{M}$ gibt es eine Gleichung

$$\overline{m}_t = \sum_{j=1}^{t} a_j \overline{m}_j \quad , \quad \text{mit } a_j \in I, j = 1, \ldots, t\,.$$

Es folgt

$$(1 - a_t)\overline{m}_t = \sum_{j=1}^{i-1} a_j \overline{m}_j\,.$$

Aber $1 - a_t$ ist eine Einheit, denn sonst wäre $(1 - a_t)$ ein echtes Ideal, also $1 - a_t$ in einem maximalen Ideal $\mathfrak{m}$ erhalten, woraus $1 \in \mathfrak{m}$ folgen würde – Widerspruch! Durch Multiplikation mit $(1 - a_t)^{-1}$ folgt, dass $\overline{M}$ schon von $\overline{m}_1, \ldots, \overline{m}_{t-1}$ erzeugt wird – Widerspruch!

Corollar 3.18 Sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und M ein endlich erzeugter A-Modul. Sind $m_1, \ldots, m_t \in M$ Elemente, deren Restklassen $\overline{m}_1, \ldots, \overline{m}_t$ den Modul $M/\mathfrak{m}M$ erzeugen, so wird M von $m_1, \ldots, m_t$ erzeugt.

Beachte: $M/\mathfrak{m}M$ ist ein endlich-dimensionaler Vektorraum über dem Restklassenkörper $k = A/\mathfrak{m}$!

Beweis: Anwendung von Satz 3.17 auf den von $m_1, \ldots, m_t$ erzeugten Untermodul $N = \langle m_1, \ldots m_t \rangle_A \subseteq M$ und $I = \mathfrak{m}$.

Bemerkung 3.19 Corollar 3.18 wird im Allgemeinen falsch, wenn M nicht endlich erzeugt ist: Sei p eine Primzahl. Für den $\mathbb{Z}_{\langle p \rangle}$-Modul $\mathbb{Q}$ gilt $\mathbb{Q}/\langle p \rangle \mathbb{Z}_{\langle p \rangle}\mathbb{Q} = \mathbb{Q}/p\mathbb{Q} = 0$, aber $\mathbb{Q} \neq 0$. Tatsächlich ist $\mathbb{Q}$ auch kein endlich erzeugter $\mathbb{Z}_{\langle p \rangle}$-Modul.

4 Diskrete Bewertungsringe

Diese sind interessant für die (Kommutative) Algebra und die Zahlentheorie.

Definition 4.1 Sei K ein Körper. Eine **diskrete Bewertung** auf K ist eine Abbildung

$$v : K \setminus \{0\} \to \mathbb{Z}$$

mit den Eigenschaften

(i) $v(x \cdot y) = v(x) + v(y)$,
(ii) $v(x + y) \geq \min\{v(x), v(y)\}$,

für alle $x, y \in K \setminus \{0\}$.

Bemerkung 4.2 Offenbar bedeutet (i) gerade, dass $v : K^\times \to \mathbb{Z}$ ein Gruppenhomomorphismus ist. Ist die Bewertung **nicht-trivial**, d.h., v nicht der Nullhomomorphismus, so ist $im\, v = n\mathbb{Z}$ für ein eindeutig bestimmtes $n \in \mathbb{N}$, und v heißt **normiert**, wenn $im\, v = \mathbb{Z}$ ist. Beachte: Ist v nicht-trivial, $im\, v = n\mathbb{Z}$ mit $n \in \mathbb{N}$, so ist $\frac{1}{n}v$ normiert.

Beispiele 4.3 (a) Für eine Primzahl p definiere die p-**adische Bewertung** v_p auf $\mathbb{Q}$ durch

$$v_p(x) = n_p\,,$$

falls

$$x = \pm \prod_q q^{n_q} \quad (n_q \in \mathbb{Z},\ \text{fast alle null})$$

die Primfaktorzerlegung von x ist (q läuft über alle Primzahlen). Zum Beispiel ist $v_3(12) = 1, v_2(12) = 2, v_p(12) = 0$ für $p > 3$. Für jedes p ist v_p eine normierte diskrete Bewertung auf $\mathbb{Q}$ (Übungsaufgabe!).

(b) Sei k ein Körper und $k[x]$ der Polynomring. Für $f = \frac{p(x)}{q(x)} \in k(x)^\times$ setze

$$v_\infty(f) = -\deg p(x) + \deg q(x)\,,$$

wobei $\deg p(x)$ der Grad eines Polynoms $p(x)$ ist. Dies ist eine normierte diskrete Bewertung auf $k(x)$ (Übungsaufgabe!).

Lemma/Definition 4.4 Sei v eine nicht-triviale diskrete Bewertung auf dem Körper K. Dann ist

$$A_v = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\} \tag{4.4.1}$$

ein lokaler Ring und heißt der **Bewertungsring von** v. Das maximale Ideal von A_v ist

$$\mathfrak{p}_v = \{x \in K^\times \mid v(x) > 0\} \cup \{0\}\,, \tag{4.4.2}$$

und es ist

$$A_v^\times = \{x \in K^\times \mid v(x) = 0\} \tag{4.4.3}$$

die Gruppe der Einheiten von A_v.

Beweis der Behauptungen: Für $x, y \in K \setminus \{0\}$ mit $v(x), v(y) \geq 0$ ist $v(xy) = v(x)+v(y) \geq 0$ und $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$. Hieraus folgt leicht, dass A_v ein Unterring von K ist (Fallunterscheidung für $x = 0$ oder $y = 0$). Ebenso sieht man, dass $\mathfrak{p}_v$ ein Ideal in A_v ist. Weiter sieht man wegen der Homomorphieeigenschaft von v sofort, dass (4.4.3) gilt ($xy = 1 \Rightarrow v(x) + v(y) = v(1) = 0$). Zusammen mit (4.4.2) folgt $\mathfrak{p}_v = A_v \setminus A_v^\times$; mit 5.12 (ii) folgt also, dass A_v lokal mit maximalen Ideal $\mathfrak{p}_v$ ist.

Beispiele 4.5 (a) Der Bewertungsring zur p-adischen Bewertung v_p auf $\mathbb{Q}$ ist

$$\mathbb{Z}_{\langle p \rangle} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b \right\},$$

mit maximalem Ideal $p\mathbb{Z}_{\langle p \rangle}$.

(b) Der Bewertungsring zur Grad-Bewertung v_∞ auf $k(x)$ (siehe 4.3 (b)) ist

$$A_\infty = \left\{ \frac{p(x)}{q(x)} \in k(x) \mid \deg q \geq \deg p \right\}.$$

(c) Ist $v : K^\times \to \mathbb{Z}$ eine nicht-triviale diskrete Bewertung und $\tilde{v}$ die zugehörige normierte Bewertung (siehe Bemerkung 4.2), so ist $A_v = A_{\tilde{v}}$.

Definition 4.6 Ein Integritätsring A heißt **diskreter Bewertungsring**, wenn es eine nicht-triviale diskrete Bewertung v auf $K = Quot(A)$ gibt, so dass $A = A_v$, der Bewertungsring von v ist.

Beispiele 4.7 Nach Beispiel 4.5 (a) ist für jede Primzahl p der Ring $\mathbb{Z}_{\langle p \rangle}$ ein diskreter Bewertungsring.

Satz 4.8 Für einen Integritätsring A sind äquivalent:

(a) A ist diskreter Bewertungsring.

(b) A ist lokal und ein Hauptidealring und A ist kein Körper.

Beweis (a) $\Rightarrow$ (b): Sei $A = A_v$ für die diskrete Bewertung v auf K. Ohne Einschränkung sei v normiert (Bemerkung 4.5 (c)). Nach 4.4 ist A_v ein lokaler Ring und kein Körper. Sei $\pi \in A$ ein Element mit $v(\pi) = 1$ und sei $\mathfrak{a} \subseteq A$ ein Ideal. Sei

$$m = \min\{v(x) \mid x \in \mathfrak{a}\} \in \mathbb{N}_0$$

(Beachte: $v(x) \geq 0$ für alle $x \in A$). Dann gilt

$$\mathfrak{a} = \langle \pi^m \rangle. \tag{4.8.1}$$

Sei nämlich $x \in \mathfrak{a} \setminus \{0\}$. Dann ist $n := v(x) \geq m$ und für $u := x \cdot \pi^{-n} \in K^\times$ gilt $v(u) = v(x) + v(\pi^{-n}) = n - n = 0$. Also ist $u \in A^\times$ eine Einheit und

$$x = u \cdot \pi^n \in \langle \pi^m \rangle$$

wegen $n \geq m$.

Umgekehrt gibt es nach Definition von m ein $y \in \mathfrak{a}$ mit $v(y) = m$, und wie eben folgt $y = v\pi^m$ mit einer Einheit $v \in A^\times$. Es folgt $\pi^m = v^{-1}y \in \mathfrak{a}$ und damit $\langle \pi^m \rangle \subseteq \mathfrak{a}$.

(b) $\Rightarrow$ (a): Sei A ein lokaler Hauptidealring und kein Körper. Das eindeutig bestimmte maximale Ideal $\mathfrak{m} \subseteq A$ ist dann ein Hauptideal; etwa $\mathfrak{m} = \langle \pi \rangle$ für ein Element $0 \neq \pi \in A$. Dann ist π ein Primelement. Ist π' ein weiteres Primelement in A, so ist $\langle \pi' \rangle$ ein maximales Ideal (da A ein Hauptidealring ist, siehe Algebra), also gleich $\mathfrak{m} = \langle \pi \rangle$, da A nur ein maximales Ideal hat. Also sind π' und π assoziiert. Es gibt also bis auf Assoziiertheit nur das Primelement π. Da A als Hauptidealring ein faktorieller Ring ist (siehe Algebra), gilt für jedes $x \in A \setminus \{0\}$

$$x = u \cdot \pi^n \tag{4.8.2}$$

mit einem eindeutig bestimmten $n \in \mathbb{N}_0$ und einer (eindeutig bestimmten) Einheit u. Entsprechend gilt dies für jedes $x \in K^\times$, wobei $n \in \mathbb{Z}$. Definiere nun die Abbildung $v : K^\times \to \mathbb{Z}$ durch

$$v(x) = n \quad \text{falls (4.8.2) gilt.} \tag{4.8.3}$$

Dann ist v eine diskrete Bewertung (Übungsaufgabe). Weiter gilt offenbar $x \in A \setminus \{0\} \Leftrightarrow v(x) \geq 0$, also $A = A_v$.

Bemerkung 4.9 Sei A ein diskreter Bewertungsring.

(a) Ist v eine normierte diskrete Bewertung auf $K = Quot(A)$ mit $A = A_v$, so ist v eindeutig bestimmt. Sei nämlich v' eine zweite solche Bewertung und seien $\pi, \pi' \in A$ Elemente mit $v\langle \pi \rangle = 1 = v'(\pi')$. Dann gilt nach dem Beweis von 4.8 (siehe (4.8.1)) $\langle \pi \rangle = \mathfrak{m} = \langle \pi' \rangle$ für das maximale Ideal $\mathfrak{m} \subseteq A$, also $\pi' = u\pi$ für eine Einheit $u \in A^\times$, und damit $v(x) = v'(x)$ für alle $x \in K^\times$ (warum?).

(b) Jedes Element $\pi \in A$ mit $\langle \pi \rangle = \mathfrak{m}$ (also mit $v(\pi) = 1$ für die eindeutig bestimmte normierte diskrete Bewertung v zu A) heißt **Primelement von** A (oder **Primelement für** v).

Beispiele 4.10 Ist p eine Primzahl, so ist p ein Primelement für die p-adische Bewertung v_p auf $\mathbb{Q}$.

5 Das Tensorprodukt

Sei R ein kommutativer Ring mit Eins.

Satz/Definition 5.1 (a) Für zwei R-Moduln M, N gibt es einen bis auf eindeutige Isomorphie eindeutig bestimmten R-Modul $M \otimes_R N$, genannt das **Tensorprodukt** von M und N, mit der folgenden universellen Eigenschaft:

Es gibt eine R-bilineare Abbildung $\psi_{univ} : M \times N \to M \otimes_R N$ derart, dass für jede R-bilineare Abbildung $\psi : M \times N \to P$ in einem R-Modul P ein eindeutig bestimmter R-Modul-Homomorphismus $\widetilde{\psi} : M \otimes_R N \to P$ existiert mit $\psi = \widetilde{\psi} \circ \psi_{univ}$, d.h., so dass das Diagramm:

(5.1.1)
$$\begin{array}{ccc} M \times N & \xrightarrow{\psi_{univ}} & M \otimes_R N \\ & {\scriptstyle \psi} \searrow \quad \swarrow {\scriptstyle \exists! \, \widetilde{\psi}} & \\ & P & \end{array}$$

kommutativ ist. Das Element $\psi_{univ}((m,n))$ wird mit $m \otimes n$ bezeichnet.

(b) Jedes Element in $M \otimes_R N$ ist von der Form

$$\sum_{i=1}^{k} m_i \otimes n_i$$

für ein $k \in \mathbb{N}$ und $m_1, \ldots, m_k \in M, n_1, \ldots, n_k \in N$.

(c) Es gilt:

(5.1.2)
$$\begin{array}{rcl} (m+m') \otimes n & = & m \otimes n + m' \otimes n \\ m \otimes (n+n') & = & m \otimes n + m \otimes n' \\ rm \otimes n & = & r(m \otimes n) = m \otimes rn \end{array}$$

Zum Beweis: Man kann $M \otimes_R N$ durch "Erzeugende und Relationen" definieren, nämlich durch

$$M \otimes_R N \; = \; F_R(M \times N)/U \; ,$$

wobei $F_R(M \times N)$ der freie R-Modul auf $M \times N$ ist (siehe 2.5) und

$$U = \langle (rm + r'm', n) - r(m,n) - r'(m',n), (m, sn + s'n') - s(m,n) - s'(m,n') \rangle$$

der von den angegebenen Elementen (mit $m, m' \in M, n,\ n' \in N$ und $r, r', s, s' \in R$) erzeugte Untermodul. Wir schreiben hier zur Vereinfachung auch (m,n) für das zu (m,n) gehörige Basiselement von $F_R(M \times N)$. Durch das Herausdividieren von U, also der richtigen "Relationen", wird gerade erreicht, dass die Abbildung

$$\begin{array}{rcccl} \psi_{univ} : M \times N & \to & F_R(M \times N) & \to & F_R(M \times N)/U \\ (m,n) & \mapsto & (m,n) & \mapsto & m \otimes n := \text{Klasse von}(m,n) \end{array}$$

bilinear ist, und die universelle Eigenschaft ergibt sich aus der universellen Eigenschaft von $F_R(M \times N)$. Die Aussage in (b) folgt aus der Konstruktion, und (c) ist gerade die Bilinearität von ψ_{univ}. Die Details seien dem Leser überlassen.

Im Folgenden braucht man nur die in 5.1 stehenden Eigenschaften, nicht die Konstruktion des Tensorproduktes! Dies gilt zum Beispiel für den Beweis von

Proposition 5.2 Es gibt kanonische Isomorphismen für R-Moduln M, N, P:

(a) $R \otimes_R M \cong M$

(b) $M \otimes_R N \cong N \otimes_R M$

(c) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$.

Beweis von (b): Wir haben eine Abbildung

$$\begin{array}{rcl} M \otimes_R N & \to & N \otimes_R M \\ m \otimes n & \mapsto & n \otimes m \quad \text{für } m \in M, n \in N. \end{array}$$

Dies soll heißen: diese Abbildung ist wohldefiniert, weil sie aufgrund der universellen Eigenschaft von der bilinearen (folgt mit 5.1 (c)!) Abbildung

$$\begin{array}{rcl} M \times N & \to & M \otimes_R N \\ (m, n) & \mapsto & n \otimes m \end{array}$$

induziert wird. Die Umkehrabbildung ist dann die analoge Abbildung

$$\begin{array}{rcl} N \otimes_R M & \to & M \otimes_R N \\ n \otimes m & \mapsto & m \otimes n\,. \end{array}$$

Um dies nachzurechnen, braucht man nur die Verknüpfung auf den Erzeugenden $m \otimes n$ auszurechnen, wo die Behauptung trivial ist.

Entsprechend werden die Isomorphismen in (a) und (c) "gegeben" durch

$$r \otimes m \mapsto rm$$

(mit Umkehrabbildung $m \mapsto 1 \otimes m$) beziehungsweise

$$(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$$

(mit Umkehrabbildung $m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p$).

Lemma 5.3 Für R-Moduln M, N werden die Mengen

$$Abb(M, N) := \text{ Menge aller Abbildungen } f : M \to N$$

$$Hom_R(M, N := \{f : M \to N \mid f \ R\text{-Modul-Homomorphismus}\}$$

zu R-Moduln vermöge der Definition

$$\begin{array}{rcl} (f + g)(m) & = & f(m) + g(m) \\ (rf)(m) & = & r(f(m)) \end{array}$$

$Hom_R(M, N)$ ist ein Untermodul von $Abb(M, N)$.

Beweis selbst.

Satz 5.4 Für R-Moduln M,N,P gibt es einen kanonischen R-Modul-Isomorphismus

$$Hom_R(M, Hom_R(N,P)) \cong Hom_R(M \otimes_R N, P)$$

Beweis: Sei $Bil_R(M,N,P)$ die Menge der R-bilinearen Abbildungen von $M \times N$ nach P. Dies ist ein Untermodul von $Abb(M \times N, P)$ (nachrechnen!) und man erhält eine Bijektion

$$\begin{array}{rcl} \Psi : Hom_R(M, Hom_R(N,P)) & \tilde{\to} & Bil_R(M,N,P) \\ \phi & \mapsto & (\psi_\phi : (m,n) \mapsto \phi(m)(n)) \end{array}$$

(ψ_ϕ ist offenbar bilinear!). Die Umkehrabbildung ist nämlich

$$(\phi_\psi : m \mapsto (n \mapsto \psi(m,n))) \leftarrow\!\shortmid \qquad \psi$$

($n \mapsto \psi(m,n)$ und ϕ_ψ sind R-linear!).

Weiter ist die Bijektion Ψ R-linear: $r\phi + r'\phi'$ wird auf die Abbildung

$$\begin{array}{rcl} (m,n) & \mapsto & (r\phi + r'\phi')(m)(n) \\ & = & (r\phi(m) + r'\phi'(m))(n) \\ & = & r(\phi(m)(n)) + r'(\phi'(m))(n) \end{array}$$

abgebildet, also auf $r\psi_\phi + r'\psi_{\phi'}$.

Durch Verknüpfung mit der Bijektion (universelle Eigenschaft des Tensorproduktes)

$$Bil_R(M,N,P) \tilde{\longrightarrow} Hom_R(M \otimes_R N, P)\,, \qquad \psi \mapsto \tilde{\psi}\,,$$

die ebenfalls R-linear ist (mit der universellen Eigenschaft nachrechnen!) erhält man den gewünschten Isomorphismus von R-Moduln.

Wir betrachten im Folgenden immer kommutative Ringe mit Eins.

Bemerkung 5.5 Sei $\varphi : A \to B$ ein Ringhomomorphismus. Dann wird B zu einem A-Modul durch die Verknüpfung

$$ab \;:=\; \varphi(a) \cdot b \quad \text{für } a \in A, b \in B\,.$$

Die Schreibweise ab bedeutet im folgenden immer diese Verknüpfung. Genauer gesagt wird B hierdurch zu einer A-Algebra, d.h., einem Ring mit einer A-Modul-Struktur derart, dass die Addition im Ring B und A-Modul B übereinstimmt und dass

$$(ab) \cdot b' = a(b \cdot b') \quad (aa')b = a(a'b)$$

für alle $a, a' \in A$ und $b, b' \in B$, wobei hier der Punkt für die Ringmultiplikation in B steht, aber im Folgenden auch meist weggelassen wird. Hat man umgekehrt eine A-Algebra B, so erhält man einen Ringhomomorphismus (von Ringen mit Eins)

$$\varphi : A \to B, \quad a \mapsto a1_B$$

und die Konstruktionen sind zueinander invers.

Lemma/Definition 5.6 Sei $\varphi : A \to B$ ein Ringhomomorphismus und M ein A-Modul. Dann wird

$$B \otimes_A M$$

in eindeutiger Weise zu einem B-Modul, so dass gilt:

$$b' \cdot (b \otimes m) := b'b \otimes m \quad (\text{für } b, b' \in B, m \in M)\,. \tag{5.6.1}$$

$B \otimes_A M$ mit dieser Struktur heißt die **Skalarerweiterung** von M (mit φ oder zu B).

Beweis: Wohldefiniertheit: Zu b' definiere die Abb.

$$\begin{array}{rccc} \psi_{b'} & : & B \times M & \to & B \otimes_A M \\ & & (b, m) & \mapsto & b'b \otimes m \end{array}$$

Diese ist A-bilinear und definiert also eine A-lineare Abb.

$$\begin{array}{rccc} \widetilde{\psi}_{b'} & : & B \otimes_A M & \to & B \otimes_A M \\ & \text{mit} & b \otimes m & \mapsto & b'b \otimes m\,, \end{array}$$

die wir als die Multiplikation mit b' definieren; es sei also $b'y = \widetilde{\psi}_{b'}(y)$ für $y \in B \otimes_A M$. Die Modulaxiome sind neben der Additivität von $\widetilde{\psi}_{b'}$ die Eigenschaften

$$\widetilde{\psi}_1 = id, \quad \widetilde{\psi}_{(b'+b'')} = \widetilde{\psi}_{b'} + \widetilde{\psi}_{b''} \quad \text{und} \quad \widetilde{\psi}_{(b''.b')} = \widetilde{\psi}_{b''} \circ \widetilde{\psi}_{b'}$$

und diese gelten, weil sie für die ψ's gelten. Die Eigenschaft (5.6.1) macht die Verknüpfung eindeutig, weil die $b \otimes m$ Erzeugende von $B \otimes_A M$ sind.

Proposition 5.7 Seien $\varphi : A \to B$ und $\psi : A \to C$ Ringhomomorphismen. Dann hat $B \otimes_A C$ eine eindeutig bestimmte A-Algebren-Struktur, für die gilt:

$$b \otimes c \cdot b' \otimes c' \quad = \quad b\,b' \otimes c\,c' \tag{5.7.1}$$

Beweis: Nur die Wohldefiniertheit ist zu zeigen! Nach Konstruktion ist $B \otimes_A C$ ein A-Modul.

Nach 5.6 wird $B \otimes_A C$ ein B-Modul mit $b(b' \otimes c') = b\,b' \otimes c'$ für $b, b' \in B$ und $c' \in C$.

Analog wird $B \otimes_A C$ ein C-Modul (Operation rechts geschrieben), wobei $(b' \otimes c') \cdot c = b' \otimes c'c$. Weiter ist

$$\begin{array}{ccc} B \times C & \to & Hom_A(B \otimes_A C, B \otimes_A C) \\ (b, c) & \mapsto & (\alpha \mapsto b\alpha c) \end{array}$$

A-bilinear, induziert also nach Satz 5.1 (a) eine A-lineare Abbildung

$$\psi : B \otimes_A C \to Hom_A(B \otimes_A C, B \otimes_A C)\,,$$

nach (dem Beweis von) Satz 5.4 also eine A-bilineare Verknüpfung

$$\begin{array}{ccccc} B \otimes_A C & \times & B \otimes_A C & \to & B \otimes_A C\,. \\ & (\alpha, \beta) & & \mapsto & \alpha \cdot \beta := \psi(\alpha)(\beta) \end{array}$$

für die (5.7.1) gilt:

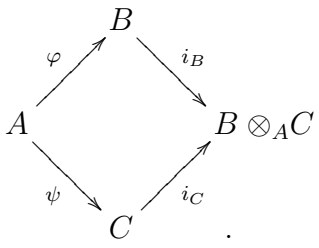
$$(b \otimes c) \cdot (b' \otimes c') = \psi(b \otimes c)(b' \otimes c') = b\,b' \otimes c\,c'$$

Hieraus folgt, dass $B \otimes_A C$ ein kommutativer Ring mit eins 1 wird (nachrechnen!).

Satz 5.8 (a) Die Abbildungen

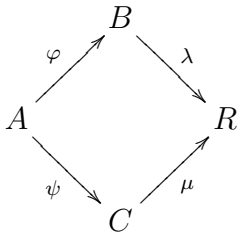
$$\begin{array}{lcll} i_B : B & \to & B \otimes_A C & b \mapsto b \otimes 1 \\ i_C : C & \to & B \otimes_A C & c \mapsto 1 \otimes c \end{array}$$

sind Ringhomomorphismen, und das folgende Diagramm ist kommutativ:



.

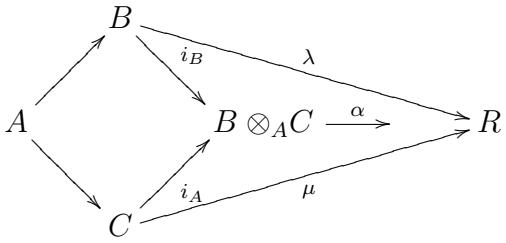
(b) (universelle Eigenschaft) Ist



ein kommutatives Diagramm von Ringhomomorphismen, so gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\alpha : B \otimes_A C \to R$$

der das Diagramm



kommutativ macht.

Beweis: (a): klar.

(b) Die Abbildung

$$\begin{array}{rccc} \lambda \cdot \mu : & B \times C & \to & R \\ & (b, c) & \mapsto & \lambda(b) \cdot \mu(c) \end{array}$$

ist A-bilinear und induziert daher nach 2.4. einen eindeutig bestimmten Morphismus von A-Moduln

$$\alpha : B \otimes_A C \longrightarrow R\,,$$

der $b \otimes c$ auf $\gamma(b) \cdot \mu(c)$ abbildet. Dieser leistet das Gewünschte (nachrechnen!).

Eine weitere nützliche Eigenschaft für das Tensorprodukt ist:

Lemma 5.9 Ist $(M_i)_{i\in I}$ eine Familie von R-Moduln und N ein weiterer R-Modul, so gibt es einen kanonischen R-Modul-Isomorphismus

$$\begin{array}{rccc} & \left(\bigoplus_{i\in I} M_i\right)\otimes N & \xrightarrow{\sim} & \bigoplus_{i\in I}(M_i\otimes N)\,, \\ \text{mit} & (m_i)\otimes n & \mapsto & (m_i\otimes n)\,. \end{array}$$

Beweis Die Abbildung ergibt sich mittels der universellen Eigenschaft des Tensorprodukts aus der R-bilinearen Abbildung

$$((m_i)_{i\in I}, n)\mapsto (m_i\otimes n)_{i\in I}\,.$$

Die Umkehrabbildung ist definiert durch die universelle Eigenschaft der direkten Summe und die Abbildungen

$$M_i\otimes N\to (\bigoplus_{i\in I} M_i)\otimes N\,,$$

die durch $m_i\otimes n\mapsto \varphi_i(m_i)\oplus n$ "definiert sind", wobei $\varphi_j : M_j\hookrightarrow \bigoplus_{i\in I} M_i$ der kanonische Monomorphismus ist, mit $\varphi_j(m_j)=(n_i)_{i\in I}$, wobei $n_j=m_j$ and $n_i=0$ für $i\neq j$.

Corollar 5.10 Sei I eine Menge und $R\to S$ ein Ringhomomorphismus. Für die Skalarerweiterung zu S des freien R-Moduls $F_R(I)$ über I gibt es einen kanonischen Isomorphismus von S-Moduln

$$\begin{array}{rccc} & S\otimes_R F_R(I) & \xrightarrow{\sim} & F_S(I) \\ \text{mit} & s\otimes e_i & \mapsto & se_i \end{array}$$

für die kanonische Basis $(e_i)_{i\in I}$ von $F_R(I)$ bzw. $F_S(I)$.

Beweis Wir haben die Isomorphismen

$$S\otimes_R F_R(I)=S\otimes_R\left(\bigoplus_{i\in I} Re_i\right)\overset{5.9}{\underset{\sim}{\to}}\bigoplus_{i\in I} S\otimes_R Re_i\overset{5.2\,(a)}{\underset{\sim}{\to}}\bigoplus_{i\in I} Se_i=F_S(I)\,.$$

Wir zeigen nun eine Exaktheitsaussage für das Tensorprodukt. Wenn der Grundring R klar ist, schreiben wir auch nur $\otimes$ für $\otimes_R$.

Vorbemerkung 5.11 Für Morphismen von R-Moduln $f : M_1\to M_2$ und $g : N_1\to N_2$ hat man einen kanonischen Morphismus von R-Moduln

$$\begin{array}{rccc} f\otimes g : M_1\otimes N_1 & \to & M_2\otimes N_2 \\ m_1\otimes n_1 & \mapsto & f(m_1)\otimes g(n_1)\,, \end{array}$$

entsprechend der bilinearen Abbildung $(m_1,n_1)\mapsto f(m_1)\otimes g(n_1)$.

Insbesondere hat man für jeden R-Modul N eine kanonische Abbildung

$$f\otimes id = f\otimes id_N : M_1\otimes N\to M_2\otimes N$$

(Man sagt hierzu, das Tensorprodukt ist "funktoriell").

Der folgende Satz ist extrem nützlich für das Rechnen mit Tensorprodukten.

Satz 5.12 (Rechtsexaktheit des Tensorproduktes) Ist

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

eine exakte Sequenz von R-Moduln, so ist für jeden R-Modul N auch die Sequenz

$$M_1 \otimes_R N \xrightarrow{f\otimes id} M_2 \otimes_R N \xrightarrow{g\otimes id} M_3 \otimes_R N \to 0$$

exakt, wobei $f \otimes id = f \otimes id_N$ und $g \otimes id = g \otimes id_N$ wie in 5.11.

Beweis: (1) $g \otimes id$ ist surjektiv: $M_3 \otimes_R N$ wird erzeugt von Elementen $m_3 \otimes n$ mit $m_3 \in M, n \in N$. Für m_3 existiert $m_2 \in M_2$, mit $g(m_2) = m_3$. Dann ist $m_3 \otimes n = (g \otimes id)(m_2 \otimes n)$.

(2) im $(f \otimes id) \subseteq ker\ (g \otimes id)$: Es ist $(g \otimes id) \circ (f \otimes id) = (g \circ f) \otimes id = 0$, da $g \circ f = 0$.

(3) im $(f \otimes id) \supseteq ker\ (g \otimes id)$: Sei $\varphi : M_2 \otimes_R N \twoheadrightarrow coker\,(f \otimes id)$ die kanonische (surjektive) Abbildung. Wir konstruieren nun eine Abbildung $\psi : M_3 \otimes N \to coker\,(f \otimes id)$, die das Diagramm

$$\begin{array}{ccc} M_2 \otimes N & \xrightarrow{\varphi} & coker\,(f \otimes id) \\ & \searrow^{g\otimes id} & \uparrow \psi \\ & & M_3 \otimes N \end{array}$$

kommutativ macht $(\psi \circ (g \otimes id) = \varphi)$. Dann folgt $\ker(g \otimes id) \subseteq \ker \varphi = im\,(f \otimes id)$.

Nach Definition ist $\varphi \circ (f \otimes id) = 0$. Definiere nun eine bilineare Abbildung

$$b : M_3 \times N \to coker\ (f \otimes id),\ (m_3, n) \mapsto \varphi(m_2 \otimes n)\ ,$$

wobei $m_2 \in M_2$ mit $g(m_2) = m_3$. Ein solches m_2 existiert, da g surjektiv ist. Weiter ist b wohldefiniert: Ist $m_2' \in M_2$ mit $g(m_2') = m_3 = g(m_2)$, so ist $m_2 - m_2' \in \ker g = im\, f$, also $m_2 - m_2' = f(m_1)$ für ein $m_1 \in M_1$. Es folgt

$$m_2 \otimes n - m_2' \otimes n = f(m_1) \otimes n = (f \otimes id)(m_1 \otimes n)\,,$$

also $\varphi(m_2 \otimes n) = \varphi(m_2' \otimes n)$ wegen $\varphi \circ (f \otimes id) = 0$.

Die bilineare Abbildung b induziert nun einen R-Modul-Homomorphismus

$$\psi : M_3 \otimes_R N \to coker\ (f \otimes id)\ .$$

Nach Konstruktion gilt dabei für $m_2 \in M_2$ und $n \in N$

$$(\psi \circ (g \otimes id))(m_2 \otimes n) = \psi(g(m_2) \otimes n) = b(g(m_2), n) = \varphi(m_2 \otimes n)\ .$$

Also ist $\psi \circ (g \otimes id) = \varphi$.

Bemerkung 5.13 Ist $0 \to M_1 \to M \to M_2 \to 0$ exakt, so ist die Sequenz

$$0 \to M_1 \otimes_R N \to M_2 \otimes_R N \to M_3 \otimes {}_R N \to 0$$

ist im Allgemeinen nicht an der Stelle $M_1 \otimes_R N$ exakt (das Tensorprodukt ist nur rechtsexakt und nicht exakt). Ein Gegenbeispiel ist das Folgende: Wir haben eine exakte Sequenz von $\mathbb{Z}$-Moduln

$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0\ ,$$

wobei $\cdot n$ die Multiplikation mit der natürlichen Zahl n bedeutet. Tensorieren wir dies mit $\mathbb{Z}/n\mathbb{Z}$, so erhalten wir vermöge der Isomorphien $\mathbb{Z}\otimes\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}\otimes\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ die exakte Sequenz

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

wobei $\cdot n$ die Nullabbildung, also nicht injektiv für $n \neq 1$ ist.

Die Rechtsexaktheit reicht aber für folgende Anwendung:

Corollar 5.14 Sei M ein R-Modul, und $\mathfrak{a} \subseteq R$ ein Ideal. Dann gibt es einen kanonischen Isomorphismus (von R- bzw. auch von $R/\mathfrak{a}$-Moduln)

$$R/\mathfrak{a} \otimes_R M \cong M/\mathfrak{a}M \,,$$

wobei $\mathfrak{a}M = \{\sum_{i=1}^{n} a_i m_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, m_i \in M\}$.

Beweis: Nach Definition ist

$$0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$$

exakt. Daher ist

$$\mathfrak{a} \otimes_R M \to R \otimes_R M \to R/\mathfrak{a} \otimes M \to 0$$

exakt. Vermöge der Isomorphie $R \otimes_R M \cong M$ erhalten wir ein exakte Sequenz

$$\mathfrak{a} \otimes_R M \xrightarrow{\psi} M \to R/\mathfrak{a} \otimes M \to 0$$

$$a \otimes m \mapsto a \cdot m, m \mapsto 1 \otimes m \,,$$

die die Behauptung zeigt: Offenbar ist $im\,\psi = \mathfrak{a}M$.

Bemerkungen 5.15 (a) Mit 5.10 und 5.12 kann man wie folgt Tensorprodukte "verstehen". Für jeden R-Modul M hat durch die Wahl von Erzeugenden $m_i\,(i \in I)$ eine Surjektion $F_R(I) \xrightarrow{\varphi} M$, $e_i \mapsto m_i$. Wendet man dies nochmals auf $\ker\varphi$ an, so erhält man durch Wahl von Erzeugenden $(n_j)_{j\in J}$ von $\ker\varphi$ eine Surjektion $F_R(J) \twoheadrightarrow \ker\varphi, e_j \mapsto n_j$, und damit eine exakte Sequenz

$$F_R(J) \to F_R(I) \xrightarrow{\varphi} M \to 0\,.$$

Dies nennt man eine **Präsentation** des Moduls M; man beschreibt M durch Erzeugende (die m_i) und Relationen (die Erzeugenden von $\ker\varphi$). Ist nun $R \to S$ ein Ringhomomorphismus, so ist nach 5.12

$$S \otimes_R F_R(J) \to S \otimes_R F_R(J) \to S \otimes_R M \to 0$$

exakt, und dies lässt sich nach 5.10 ($S \otimes_R F_R(I) \cong F_S(I)$, analog für $F_R(J)$) schreiben als

$$F_S(I) \to F_S(J) \to S \otimes_R M \to 0\,.$$

$S\otimes_R M$ hat also "dieselben Erzeugenden und Relationen", allerdings nun in freien S-Moduln, d.h., wir bilden die auftretenden Koeffizienten $a_i \in R$, $b_j \in R$ durch $R \to S$ in S ab.

(b) Für Polynome $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$ ist also zum Beispiel

$$S \otimes_R (R[X_1, \ldots, X_n]/\langle f_1, \ldots, f_m\rangle) \cong S[X_1, \ldots, X_n]/\langle f_1, \ldots, f_m\rangle \,,$$

wobei die Polynome rechts in $S[X_1, \ldots, X_n]$ aufgefasst sind.

Wir beschließen diesen Abschnitt mit der folgenden Beobachtung.

Satz 5.16 Sei A ein Ring, $S \subseteq A$ eine multiplikative Teilmenge und M ein A-Modul. Dann ist der Homomorphismus von A_S-Moduln

$$\begin{array}{rccc} & A_S \otimes_A M & \to & M_S \\ \text{mit} & \alpha \otimes m & \mapsto & \alpha \cdot \frac{m}{1} \end{array}$$

ein Isomorphismus.

Beweis Die Umkehrabbildung ist

$$\frac{1}{s} \otimes m \leftarrow\!\shortmid \frac{m}{s}\,.$$

Beispiel 5.17 Für eine abelsche Gruppe A ist der $\mathbb{Q}$-Vektorraum $A_{\mathbb{Q}}$ aus Beispiel 5.11 (b) also gleich $\mathbb{Q} \otimes_{\mathbb{Z}} A$. Entsprechend ist für jeden Integritätsring R mit Quotientenkörper K und für jeden R-Modul M

$$M_{\langle 0 \rangle} = K \otimes_R M =: M_K$$

(und $rg\, M = \dim_K M_K$).

6 Symmetrische und äußere Produkte, und die Determinante über Ringen

Sei A ein kommutativer Ring mit Eins.

Lemma/Definition 6.1 Sei M ein A-Modul.

(a) Setze $T^0(M) = A$, und für $n > 0$

$$T^n(M) = M^{\otimes n} = M \otimes_A \ldots \otimes_A M \qquad (m\text{-mal}).$$

Dann wird

$$T(M) = \bigoplus_{n \geq 0} T^n(M)$$

durch das Tensorprodukt, d.h., die Abbildungen

$$T^m(M) \times T^n(M) \to T^{m+n}(M) \qquad \text{mit}$$

$$(a_1 \otimes \ldots \otimes a_m, b_1 \otimes \ldots \otimes b_n) \mapsto a_1 \otimes \ldots \otimes a_m \otimes b_1 \otimes \ldots \otimes b_n$$

zu einer assoziativen (nicht kommutativen) graduierten A-Algebra, die die **Tensoralgebra** von M heißt.

(b) Sei I_1 das (zweiseitige, graduierte) Ideal, welches durch die Elemente $x \otimes y - y \otimes x$ erzeugt wird. Dann ist

$$S(M) = T(M)/I_1 = \bigoplus_{n \geq 0} S^n(M)$$

eine kommutative graduierte A-Algebra und heißt die symmetrische Algebra von M, und $S^n(M)$ heißt die **n-te symmetrische Potenz** von M (andere Bezeichnung: $Sym^n(M)$).

(c) Sei I_2 das Ideal, welches durch die Elemente $x \otimes x$ für $x \in M$ erzeugt wird. Dann ist

$$\Lambda(M) = T(M)/I_2 = \bigoplus_{n \geq 0} \Lambda^n(M)$$

eine graduierte A-Algebra und heißt die äußere Algebra von M, und $\Lambda^n(M)$ heißt die **n-te äußere Potenz** von M (andere Bezeichnung $Alt^n(M)$).

Wir erklären zunächst die Begriffe.

Bemerkung 6.2 Eine graduierte A-**Algebra** ist eine A-Algebra B zusammen mit einer Zerlegung

$$B = \bigoplus_{n \in \mathbb{Z}} B_n \tag{6.2.1}$$

in eine direkte Summe von A-Untermoduln B_n, so dass gilt

$$B_m \cdot B_n \subseteq B_{m+n}\,. \tag{6.2.2}$$

Ein Ideal $\mathfrak{a} \subseteq B$ heißt **graduiert**, wenn

$$\mathfrak{a} = \bigoplus_{n \in \mathbb{Z}} \mathfrak{a}_n\,, \tag{6.2.3}$$

wobei $\mathfrak{a}_n \subseteq B_n$ ein A-Untermodul ist. Es ist dann $\mathfrak{a} = \mathfrak{a} \cap B_n$, und der Quotient $B/\mathfrak{a}$ ist wieder eine graduierte A-Algebra vermöge der Isomorphie

$$B/\mathfrak{a} \cong \bigoplus_{n\in\mathbb{Z}} B_n/\mathfrak{a}_n \tag{6.2.4}$$

(vergleiche Lemma 3.17, welches auch für unendliche Summen gilt).

Damit zeigen wir nun die Behauptung aus 6.1. Dass $T(M)$ wie beschrieben zu einer assoziativen graduierten A-Algebra wird, ist aus den Definitionen klar. Weiter ist das Ideal I_1 graduiert, weil es durch die Elemente $x \otimes y - y \otimes x$ erzeugt wird, die rein vom Grad 2 sind. Ist nun z ein Element in $T(M)$, so ist $z = \sum_{n\in\mathbb{Z}} z_n$ mit $z_n = 0$ für fast alle n und damit $z \otimes (x \otimes y - y \otimes x) = \sum_{n\in\mathbb{Z}} z_n \otimes (x \otimes y - y \otimes x)$, wobei nun jeder Summand rein vom Grad $n+2$ ist, und Entsprechendes gilt für $(x \otimes y - y \otimes x) \otimes z$. Dies zeigt, dass $I_1 = \bigoplus_{n\in\mathbb{Z}} I_1 \cap T^n(M)$ ist, also graduiertes Ideal ist.

Analog folgt, dass I_2 ein graduiertes Ideal ist, und nach Bemerkung 6.2 ist $S(M)$ graduiert mit $S^n(M) = T^n(M)/I_1 \cap T^n(M)$, und $\Lambda(M)$ graduiert mit $\Lambda^n(M) = T^n(M)/I_2 \cap T^n(M)$.

Lemma 6.3 (universelle Eigenschaften) Seien M und N zwei A-Moduln.

(a) Man hat eine kanonische Isomorphie von A-Moduln

$$Hom_A(S^n(M), N) \cong Sym_A(M^n, N)\,,$$

wobei rechts der A-Modul der symmetrischen A-multilinearen Abbildungen $M^n \to N$ steht.

(b) Man hat die kanonische Isomorphie von A-Moduln

$$Hom_A(\Lambda^n(M), N) \cong Alt_A(M^n, N)\,,$$

wobei rechts der Modul der alternierenden A-multilinearen Abbildungen $M^n \to N$ steht.

Hierzu definieren wir:

Definition 6.4 (a) Eine Abbildung

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

heißt **multilinear** (oder n-**linear**), wenn φ linear in jedem Argument ist (bei festgehaltenen anderen Argumenten), d.h., es ist

$$\varphi(m_1, \ldots, m_{i-1}, am_i, m_{i+1}, \ldots, m_n) = a\varphi(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n)$$

für alle $a \in A$ und alle i, sowie

$$\begin{aligned} & \varphi(m_1, \ldots, m_{i-1}, m_i + m_i', m_{i+1}, \ldots, m_n) \\ = \; & \varphi(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n) + \varphi(m_1, \ldots, m_{i-1}, m_i', m_{i+1}, \ldots, m_n) \end{aligned}$$

(b) Eine multilineare Abbildung $\varphi : M^n \to N$ heißt **symmetrisch**, wenn

$$\varphi(m_1, \ldots, m_i, m_{i+1}, \ldots, m_n) = \varphi(m_1, \ldots, m_{i+1}, m_i, \ldots, m_n)$$

für alle i, und **alternierend**, wenn

$$\varphi(m_1, \ldots, m_n) = 0 \text{ falls } m_i = m_j \text{ für } (i,j) \text{ mit } i \neq j\,.$$

Hiermit folgen nun die Behauptungen in Lemma 6.3: Erstens folgt aus der universellen Eigenschaft des Tensorproduktes, dass $Hom_A(M^{\otimes n}, N)$ isomorph zum A-Modul

$$Mult_A(M^n, N)(\subseteq Hom_A(M^n, N))$$

der multilinearen Abbildungen $\varphi : M^n \to N$ ist. Weiter ist eine solche Abbildung genau dann symmetrisch, wenn sie über $I_1 \cap M^{\otimes n}$ faktorisiert, und alternierend, wenn sie über $I_2 \cap M^{\otimes n}$ faktorisiert.

Satz 6.5 (Berechnung für freie A-Moduln) (a) Für $m_1, \ldots, m_n \in M$ sei $m_1 \ldots m_n$ das Bild von $m_1 \otimes \ldots \otimes m_n$ in $S^n M$. Ist M freier A-Modul mit Basis $e_1, \ldots, e_d$, so hat man einen Isomorphismus von graduierten kommutativen A-Algebren

$$\begin{array}{rcl} A[X_1, \ldots, X_d] & \tilde{\to} & S(M) \\ X_i & \mapsto & e_i \in M = S^1(M)\,. \end{array} \tag{6.5.1}$$

Insbesondere ist $S^n(M)$ ein freier A-Modul mit Basis

$$\{e_1^{n_1} \ldots e_d^{n_d} \mid n_1 + n_2 + \ldots + n_d = n\}\,, \tag{6.5.2}$$

also vom Rang

$$rg(A[X_1, \ldots, X_d]_n) = \begin{pmatrix} n+d-1 \\ n \end{pmatrix}\,.$$

(b) Für $m_1, \ldots, m_n \in M$ sei $m_1 \wedge \ldots \wedge m_n$ das Bild von $m_1 \otimes \ldots \otimes m_n$ in $\Lambda^n(M)$. Ist M freier A-Modul mit Basis $e_1, \ldots, e_d$, so ist $\Lambda^n(M)$ ein freier A-Modul von Rang $\binom{d}{n}$, mit Basis

$$\{e_{i_1} \wedge \ldots \wedge e_{i_n} \mid i_1 < i_2 < \ldots < i_n\}\,. \tag{6.5.2}$$

Insbesondere ist $\Lambda^n(M) = 0$ für $n > d$, und $\Lambda^d(M)$ ist frei vom Rang 1 mit Basis $e_1 \wedge e_2 \wedge \ldots \wedge e_d$.

Beweis: (a) Per Definition ist $m \cdot m' = m' \cdot m$, also $S(M)$ eine kommutative A-Algebra. Der Morphismus von A-Algebren (6.5.1) existiert also nach der universellen Eigenschaft des Polynomrings. Er bildet

$$X^{n_1} X_2^{n_2} \ldots X_d^{n_d} \quad \text{auf} \quad e_1^{n_1} e_2^{n_2} \ldots e_d^{n_d}$$

ab. Umgekehrt folgt aus Lemma 7.9 sofort:

Lemma 6.6 Ist M frei mit Basis $e_1, \ldots, e_r$ und N frei mit Basis $f_1, \ldots, f_s$, so ist $M \otimes_A N$ frei mit Basis $\{e_i \otimes f_j \mid i = 1, \ldots, r, j = 1, \ldots, s\}$.

Induktiv folgt hieraus, dass $T^n(M)$ frei mit Basis

$$\{e_{i_1} \otimes e_{i_2} \otimes \ldots \otimes e_{i_n} \mid (i_1, i_2, \ldots, i_n) \in \{1, \ldots, d\}^n\}$$

ist. Wir erhalten hieraus einen surjektiven A-Modul-Homomorphismus

$$\begin{array}{rcl} T^n(M) & \twoheadrightarrow & A[X_1, \ldots, X_d]_n \\ e_{i_1} \otimes \ldots \otimes e_{i_n} & \mapsto & X_{i_1} \ldots X_{i_n} \,. \end{array}$$

Dieser faktorisiert über $S^n(M)$, da $A[X_1, \ldots, X_d]$ kommutativ ist, und induziert einen A-Modul Epimorphismus

$$S^n(M) \twoheadrightarrow A[X_1, \ldots, X_d]_n$$

mit

$$e_{i_1} \ldots e_{i_n} \mapsto X_{i_1} \ldots X_{i_n} \,.$$

Dieser induziert einen A-Modul Epimorphismus

$$S(M) \twoheadrightarrow A[X_1, \ldots, X_d] \,,$$

mit

$$e_1^{n_1} e_2^{n_2} \ldots e_d^{n_d} \mapsto X_1^{n_1} \ldots X_d^{n_d} \,, ,$$

der offenbar invers zu (6.5.1) ist.

Für (b) benutzen wir

Lemma 6.7 Für eine direkte Summe $M \oplus N$ von A-Moduln und jedes $k \in \mathbb{N}_0$ hat man einen kanonischen Isomorphismus von A-Moduln

$$\begin{array}{rcl} \alpha : \bigoplus_{i=0}^{k} \Lambda^i(M) \oplus_A \Lambda^{k-i}(N) & \tilde{\to} & \Lambda^k(M \oplus N) \\ m_1 \wedge \ldots \wedge m_i \otimes n_{i+1} \wedge \ldots \wedge n_k & \mapsto & m_1 \wedge \ldots \wedge m_i \wedge n_{i+1} \wedge \ldots \wedge n_k \,, \end{array}$$

wobei wir $m \in M$ mit $(m, 0) \in M \oplus N$ und $n \in N$ mit $(0, n) \in M \oplus N$ identifizieren, so dass jedes Element in $M \oplus N$ eine eindeutige Darstellung $m + n$ mit $m \in M$ und $n \in N$ besitzt.

Beweis Die Abbildung ist offenbar ein wohldefinierter Homomorphismus, da die Zuordnung $(m_1 \wedge \ldots \wedge m_i, n_{i+1} \wedge \ldots \wedge n_k) \mapsto m_1 \wedge \ldots \wedge m_i \wedge n_{i+1} \wedge \ldots \wedge n_k$ bilinear ist.

Betrachte umgekehrt für jede geordnete Teilmenge $I = \{j_1 < j_2 < \ldots < j_i\} \subseteq K = \{1, \ldots, k\}$ der Mächtigkeit i $(0 \leq i \leq k)$ die Abbildung, die ein Element

$$(m_1 + n_1, m_2 + n_2, \ldots, m_k + n_k) \in (M \oplus N)^k$$

auf

$$\varepsilon(I) \cdot m_{j_1} \wedge \ldots \wedge m_{j_k} \otimes n_{\ell_1} \wedge \ldots \wedge n_{\ell_{k-i}} \in \Lambda^i(M) \otimes \Lambda^{k-i}(N)$$

abbildet, wobei $\ell_1 < \ldots < l_{k-i}$ die Elemente in $J = K \smallsetminus I$ sind, und $\epsilon(I) \in \{\pm 1\}$ das eindeutig bestimmte Vorzeichen mit

$$x_1 \wedge x_2 \wedge \ldots \wedge x_k = \varepsilon(I) m_{j_1} \wedge \ldots \wedge m_{j_i} \wedge n_{\ell_1} \wedge \ldots \wedge n_{\ell_{k-i}}$$

für

$$x_i = \begin{cases} m_i & , \quad i \in I, \\ n_i & , \quad i \in J. \end{cases}$$

(Dies ist das Vorzeichen der Permutation $(1,\dots k) \mapsto (j_1,\dots,j_i,\ell_1,\dots,\ell_{k-i})$). Dann ist diese Abbildung alternierend multilinear und induziert daher einen Homomorphismus

$$\beta_i : \Lambda^k(M \oplus N) \to \Lambda^i(M) \otimes \Lambda^{k-i}(N)\,.$$

Weiter sieht man, dass der Homomorphismus

$$\beta : \Lambda^k(M \oplus N) \to \bigoplus_{i=1}^{k} \Lambda^i(M) \otimes \Lambda^{k-i}(M)$$

mit Komponenten β_i ein Inverses für α ist.

Damit beweisen wir nun 6.5 (b) durch Induktion über den Rang d des freien A-Moduls $M = Ae_1 \oplus \ldots \oplus Ae_d$. Ist $d = 0$, also $M = 0$, so ist $\Lambda^0 M = A$ frei vom Rang $1 = \binom{0}{0}$ und $\Lambda^i M = 0$ für $i > 0$. Ist $d = 1$, also $M = Ae_1$, so ust $\Lambda^0 M = A$ und $\Lambda^1 M = M = Ae_1$, sowie $\Lambda^i M = 0$ für $i > 1$, da $e_1 \wedge e_1 = 0$.

Ist die Aussage nun für $d-1$ bewiesen und $M = \bigoplus_{i=1}^{d} Ae_i$, so $M = M' \oplus Ae_d$ mit $M' = \bigoplus_{i=1}^{d-1} Ae_i$. Nach 6.7 haben wir einen Isomorphismus

$$\begin{array}{rcl} \bigoplus_{i=0}^{k} \Lambda^i(M') \otimes \Lambda^{k-i}(Ae_d) & \tilde{\to} & \Lambda^k(M) \\ x \otimes y & \mapsto & x \wedge y\,. \end{array}$$

Nach der Induktionsvoraussetung, der obigen Berechnung für $\Lambda^\nu Ae_d$ und 6.6 erhalten wir die Basis von $\Lambda^k(M)$ aus

$$e_{i_1} \wedge \ldots \wedge e_{i_k} \quad \text{für} \quad 1 \le i_1 < i_2 < \ldots < i_k \le d-1$$

und

$$e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_d \quad \text{für} \quad 1 \le i_1 < i_2 < \ldots < i_{k-1} < d\,,$$

zusammen also alle $e_{i_1} \wedge \ldots \wedge e_{i_k}$ mit $1 \le i_1 < \ldots < i_k \le d$.

Damit ist nun auch 6.5 (c) klar.

Lemma/Definition 6.8 Jeder A-Modul-Homomorphismus $\varphi : M \to N$ induziert kanonische Homomorphismen von A-Moduln

(a) $T^n(\varphi) : T^n(M) \to T^n(N), m_1 \otimes \ldots \otimes m_n \mapsto \varphi(m_1) \otimes \ldots \otimes \varphi(m_n)\,,$

(b) $S^n(\varphi) : S^n(M) \to S^n(N), m_1 \ldots m_n \mapsto \varphi(m_1) \ldots \varphi(m_n)\,,$

(c) $\Lambda^n(\varphi) : \Lambda^n(M) \to \Lambda^n(N), m_1 \wedge \ldots \wedge m_n \mapsto \varphi(m_1) \wedge \ldots \wedge \varphi(m_n)\,.$

Diese induzieren Homomorphismen von graduierten A-Algebren

$$T(\varphi) : T(M) \to T(N), S(\varphi) : S(M) \to S(N), \Lambda(\varphi) : \Lambda(M) \to \Lambda(N)\,.$$

Beweis der Wohldefiniertheit: (a): Die Abbildung

$$\begin{array}{rcl} M^n & \to & N^{\otimes n} \\ (m_1,\dots,m_n) & \mapsto & \varphi(m_1) \otimes \ldots \otimes \varphi(m_n) \end{array}$$

ist n-linear und induziert deswegen einen R-Modul-Homomorphismus mit

$$m_1 \otimes \ldots \otimes m_n \mapsto \varphi(m_1) \otimes \ldots \otimes \varphi(m_n)\,.$$

Der Beweis der Fälle (b) und (c) ist analog, mit den universellen Eigenschaften aus 6.3.

Die letzte Behauptung ist klar.

Lemma/Definition 6.9 (Die Determinante über Ringen) Sei M ein freier A-Modul mit Basis $e_1, \ldots, e_d$, und sei

$$\varphi : M \to M$$

ein Endomorphismus von A-Moduln. Dann ist die Determinante von φ (Bezeichnung $\det(\varphi)$) definiert als das eindeutig bestimmte Element $a \in A$ mit

$$\Lambda^d(\varphi)(e_1 \wedge \ldots \wedge e_d) = a \cdot e_1 \wedge \ldots \wedge e_d\,, \tag{6.9.1}$$

also $\varphi(e_1) \wedge \ldots \wedge \varphi(e_d) = ae_1 \wedge \ldots \wedge e_n$.

Beweis dass dies wohldefiniert ist: Da $e_1 \wedge \ldots \wedge e_d$ eine Basis von $\Lambda^d(M)$ ist, gibt es ein eindeutig bestimmtes Element $a \in A$ mit (6.9.1). Aber dies hängt auch nicht von der Wahl der Basis ab: Ist nämlich $f_1, \ldots, f_d$ eine andere Basis von M, so ist $f_1 \wedge \ldots \wedge f_d$ wieder eine Basis von $\Lambda^d(M)$, also $f_1 \wedge \ldots \wedge f_d = b \cdot e_1 \wedge \ldots \wedge e_d$, wobei b eine Einheit in A sein muss (es ist auch $e_1 \wedge \ldots \wedge e_d = cf_1 \wedge \ldots \wedge f_d$ und es folgt $cb = 1$). Es folgt

$$\Lambda^d(\varphi)(f_1 \wedge \ldots \wedge f_d) = \Lambda^d(\varphi)(be_1 \wedge \ldots \wedge e_d) = b\Lambda^d(\varphi)(e_1 \wedge \ldots \wedge e_d) = bae_1 \wedge \ldots \wedge e_d = af_1 \wedge \ldots \wedge f_d\,.$$

Lemma 6.10 (Funktorialität der Determinante) Ist $\varphi : M \to M$ ein Endomorphismus eines endlich erzeugten freien A-Moduls, ist $A \to B$ ein Ringhomomorphismus (von kommutativen Ringen mit Eins) und

$$\varphi_B : M \otimes_A B \to M \otimes_A B$$

der induzierte Endomorphismus von freien B-Moduln, so ist $\det(\varphi_B)$ das Bild von $\det(\varphi)$ unter $A \to B$.

Beweis Allgemein ist das Diagramm

$$\begin{array}{lll} \Lambda^d(\varphi): & \Lambda^d_A M & \longrightarrow \Lambda^d_A M \\ & \downarrow & \downarrow \\ \Lambda^d(id_B \otimes \varphi): & \Lambda^d_B(B \otimes_A M) & \longrightarrow \Lambda^d_B(B \otimes_A M) \end{array}$$

kommutativ, $e_1, \ldots, e_d$ wieder eine B-Basis von $B \otimes_A M$ und daher auch $e_1 \wedge \ldots \wedge e_d$ eine B-Basis von $\Lambda^d_B(B \otimes_A M)$. Schließlich verwenden wir die Isomorphie $B \otimes_A A \cong B$.

Lemma 6.11 Sei M ein freier A-Modul mit Basis $e_1, \ldots, e_d$ und $\varphi : M \to M$ ein Endomorphismus von A-Moduln. Ist $D = (a_{ij}) \in M(d \times d, A)$ die darstellende Matrix bezüglich $e_1, \ldots, e_d$, definiert durch

$$\varphi(e_j) = \sum_{i=1}^{d} a_{ij} e_i \qquad (j = 1, \ldots, d)\,,$$

so gilt die Leibnizformel

$$\det(\varphi) = \sum_{\sigma \in S_d} sgn(\sigma) a_{\sigma(1),1} \dots a_{\sigma(d),d} \,.$$

Beweis: Nach unserer Definition ist $\det(\varphi)$ das Element $a \in A$ mit

$$\varphi(e_1) \wedge \ldots \wedge \varphi(e_d) = a \cdot e_1 \wedge \ldots \wedge e_d \,. \tag{6.11.1}$$

Dabei hängt $\varphi(e_j)$ nur von der j-ten Spalte

$$D_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{dj} \end{pmatrix}$$

ab. Weiter ist die linke Seite von (6.11.1) eine multilineare alternierende Form in den Spalten und für $\varphi = id$, also die Einheitsmatrix E, erhalten wir $e_1 \wedge \ldots \wedge e_d$, also $a = 1$. Die Zuordnung $\varphi \mapsto \det(\varphi)$ entspricht also einer Abbildung

$$\bigwedge^d M \to A \,,$$

die $e_1 \wedge \ldots \wedge e_d$ auf 1 abbildet, und ist dadurch eindeutig bestimmt, da $e_1 \wedge \ldots \wedge e_d$ eine Basis von $\bigwedge^d M$ ist.

Da die Leibnizformel ebenfalls multilinear und alternierend in den Spalten ist und die Einheitsmatrix auf 1 abbildet (wie man leicht nachrechnet), erhalten wir die Übereinstimmung.

Beispiel: Sei $M = Ae_1 + Ae_2$ und

$$\varphi : M \to M$$

durch die Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

gegeben. Dann ist

$$\begin{aligned} \bigwedge^2 \varphi(e_1 \wedge e_2) &= \varphi(e_1) \wedge \varphi(e_2) \\ &= (ae_1 + ce_2) \wedge (be_1 + de_2) \\ &= ae_1 \wedge be_1 + ae_1 \wedge de_2 + ce_2 \wedge be_1 + ce_2 \wedge ce_2 \\ &= ad\, e_1 \wedge e_2 + cb\, e_2 \wedge e_1 \quad (\text{da } e_i \wedge e_i = 0) \\ &= (ad - cb) \cdot e_1 \wedge e_2 \quad (\text{da } e_2 \wedge e_1 = -e_1 \wedge e_2) \,. \end{aligned}$$

Es ist also $\det(\varphi) = ad - cb$ wie gewohnt.

Corollar 6.12 Die bekannten Rechenregeln für Determinanten, also z.B. die Entwicklung nach Zeilen oder Spalten, gelten auch über Ringen.

Corollar 6.13 (Cramersche Regel) Sei A ein beliebiger kommutativer Ring mit Eins, sei $D = (a_{ij})$ eine $n \times n$-Matrix über A und sei $\tilde{D} = (\widetilde{a_{ij}})$ die komplementäre $n \times n$-Matrix, definiert durch

$$\widetilde{a_{ij}} = (-1)^{i+j} \det A_{ji}$$

wobei $A_{ji} \in M(n-1 \times n-1, A)$ die Streichmatrix ist, die durch Streichen der j-ten Zeile und der i-ten Spalte entsteht. Dann ist

$$D \cdot \tilde{D} = \det(D) \cdot E\,, \tag{6.13.1}$$

mit der Einheitsmatrix E.

Beweis Nachrechnen.

Corollar 6.14 Eine $(n \times n)$-Matrix D über A ist genau dann invertierbar, wenn $\det(D)$ eine Einheit in A ist.

Beweis Dies folgt sofort aus (6.13.1): Ist $\det(D)$ eine Einheit, so ist $\det(D)^{-1} \cdot \tilde{D}$ ein Inverses von D. Ist umgekehrt $B \cdot C = E$ für $(n \times n)$-Matrizen B, C, so ist $\det(B) \cdot \det(C) = \det(E) = 1$, denn für beliebige B, C gilt $\det(BC) = \det(B) \cdot \det(C)$ (nach 6.12).

Als letzte Anwendung erhalten wir:

Satz 6.15 (Satz von Caley-Hamilton) Sei M ein durch n Elemente erzeugbarer A-Modul und $\varphi : M \to M$ ein Endomorphismus. Dann gibt es ein normiertes Polynom

$$P(X) = X^n + a_{n-1}X^{n+1} + \ldots + a_1 X + a_0$$

in $A[X]$ mit $P(\varphi) = 0$ in $End(M)$.

Beweis: Wähle $m_1, \ldots, m_n \in M$ mit $M = \sum_{i=1}^{n} Am_i$. Dann gibt es Elemente $a_{ij} \in A$ (für $i, j = 1, \ldots, n$) mit

$$f(x_i) = \sum_{j=1}^{n} a_{ij} m_j\,.$$

Für die Matrix

$$D(X) = (\delta_{ij} X - a_{ij})_{1 \le i,j \le n} \in M(n \times n, A[X])$$

gilt dann

$$D(\varphi) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0\,.$$

Nach 6.13 gilt dann mit der adjungierten Matrix $\widetilde{D(\varphi)}$ über dem kommutativen Ring

$$A[\varphi] = im(A[X] \xrightarrow{x \mapsto \varphi} End_A(M))$$

$$\det D(\varphi) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \widetilde{D(\varphi)} D(\varphi) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0\,,$$

also $\det D(\varphi) = 0$, da $m_1, \ldots, m_n$ Erzeugende von M sind. Damit ist $P(x) = \det D(x) \in A[X]$ ein normiertes Polynom vom Grad n mit $P(\varphi) = 0$.

7 Kategorien und Funktoren

Die Sprache der Kategorien und Funktoren ist unabdingbar für viele Aussagen in der heutigen Mathematik. Sie ist formal und weniger als Selbstzweck anzusehen, sondern eher als ein nützliches Mittel zum Formulieren und Einordnen von mathematischen Resultaten.

Wir diskutieren im Folgenden keine mengentheoretischen Fragen wie das Problem der 'Menge aller Mengen'. Wir sprechen von Klassen, wenn wir 'Mengen höherer Stufe' behandeln; ein formaler Rahmen wurde durch die sogenannten 'Universen' nach Bourbaki geliefert. Bei der Bildung der 'Klasse aller Mengen', die selbst keine Menge (derselben Stufe) ist, wird also die obige Russell'sche Antinomie vermieden.

Definition 7.1 Eine Kategorie $\mathcal{C}$ besteht aus

(i) einer Klasse $ob(\mathcal{C})$ von Objekten,

(ii) einer Menge $Hom_{\mathcal{C}}(A, B)$ für je zwei Objekte A, B, deren Elemente **Pfeile** oder **Morphismen** von A nach B genannt werden,

(iii) sowie einer Verknüpfung für alle Objekte A, B, C

$$\begin{array}{ccc} Hom_{\mathcal{C}}(B,C) \times Hom_{\mathcal{C}}(A,B) & \to & Hom_{\mathcal{C}}(A,C) \\ (g,f) & \mapsto & g \circ f \quad (\text{oder } gf)\,. \end{array}$$

Dabei soll gelten

(a) Zu jedem $A \in ob(\mathcal{C})$ gibt es ein Element $1_A \in Hom_{\mathcal{C}}(A, A)$ (genannt **Identität** von A) mit

$$f1_A \;=\; f \;=\; 1_B f$$

für $f \in Hom_{\mathcal{C}}(A, B)$.

(b) (Assoziativität) Für f, g wie oben und $h \in Hom_{\mathcal{C}}(C, D)$ gilt

$$h(gf) = (hg)f$$

in $Hom_{\mathcal{C}}(A, D)$.

Dies ist der üblichen Situation von Hom-Mengen nachempfunden. Tatsächlich bekommen wir so die meisten Beispiele:

Beispiele 7.2 (a) Die Kategorie $\underline{Sets}$ aller Mengen wird definiert durch

$$\begin{array}{lcl} ob(\underline{Sets}) & = & \text{Klasse aller Mengen} \\ Hom_{\underline{Sets}}(A,B) & = & \text{Menge aller Abbildungen } f : A \to B\ . \end{array}$$

Die Verknüpfung ist die übliche Komposition von Abbildungen, und $1_A \in Hom_{\underline{Sets}}(A, A)$ ist die Identität $id_A : A \to A$.

(b) Entsprechend werden viele Kategorien gebildet:

(1) Kategorie $\underline{Gr}$ der Gruppen: Objekte: Gruppen, $Hom_{\underline{Gr}}(G, H)$ = Menge der Gruppenhomomorphismen von G nach H, Verknüpfung: Komposition.

(2) Kategorie Mod_R der Moduln über einem Ring: Morphismen= R-Modulhomomorphismen, Verknüpfung=Komposition.

(3) Kategorie $\underline{Top}$ der topologischen Räume, Morphismen =stetige Abbildungen, mit der Komposition als Verknüpfung.

(4) Kategorie der topologischen Gruppen: Morphismen=stetige Gruppenhomomorphismen, mit der Komposition als Verknüpfung.

(c) Es gibt aber auch andere Kategorien. Sei $(I, \leq)$ eine geordnete Menge. Definiere die Kategorie $\underline{I}$ durch $ob(\underline{I}) = I$ (die Objekte sind also die *Elemente* von I!),

$$Hom_{\underline{I}}(i,j) = \begin{cases} \{*\} & , \quad i \leq j\,, \\ \emptyset & , \quad \text{sonst} \end{cases}$$

(Im ersten Fall besteht die Morphismenmenge also aus genau einem Element, das wir mit $*$ bezeichnen). Die Verknüpfung ist die einzig mögliche: der einzige Fall, wo beide Mengen nicht leer sind, ist

$$Hom_{\underline{I}}(j,k) \times Hom_{\underline{I}}(i,j) \to Hom_{\underline{I}}(i,k)$$

für $i \leq j \leq k$, wo $(*,*)$ auf $*$ abgebildet wird.

(d) Die kleinste Kategorie der Welt: $\mathcal{C}_0$: $\mathcal{C}_0$ hat nur ein Objekt $*$ und es ist $Hom_{\mathcal{C}_0}(*,*) = \{id_*\}$.

(e) Sei G eine Gruppe. Definiere die Kategorie $\underline{G}$ wie folgt: $\underline{G}$ hat nur ein Objekt $*$ und es ist $Hom_{\underline{G}}(*.*) = G$ mit der Verknüpfung $G \times G \to G$, die durch das Gruppengesetz gegeben ist.

Definition 7.3 Ein Morphismus $f : A \to B$ in einer Kategorie $\mathcal{C}$ heißt

(a) **Monomorphismus**, wenn für alle Objekte X in $\mathcal{C}$ und alle Morphismen $g_1, g_2 : X \to A$ gilt

$$fg_1 = fg_2 \quad \Rightarrow \quad g_1 = g_2$$

(d.h., f ist links kürzbar),

(b) **Epimorphismus**, wenn für alle Objekte X in $\mathcal{C}$ und alle Morphismen $h_1, h_2 : B \to X$ gilt

$$h_1 f = h_2 f \quad \Rightarrow \quad h_1 = h_2$$

(d.h., f ist rechts kürzbar), und

(c) **Isomorphismus**, wenn es einen Morphismus $g : B \to A$ in $\mathcal{C}$ gibt mit

$$gf = 1_A \quad \text{und} \quad fg = 1_B$$

(Das g ist dann eindeutig bestimmt und heißt das Inverse von f).

Bemerkungen 7.4 (a) Sei $f : A \to B$ ein Morphismus in einer Kategorie $\mathcal{C}$. Für alle Objekte X in $\mathcal{C}$ induziert f eine Abbildung

$$\begin{array}{rccc} f_* : & Hom_{\mathcal{C}}(X,A) & \to & Hom_{\mathcal{C}}(X,B) \\ & g & \mapsto & fg \end{array}$$

und eine Abbildung

$$\begin{array}{rccc} f^* : & Hom_{\mathcal{C}}(B,X) & \to & Hom_{\mathcal{C}}(A,X) \\ & h & \mapsto & hf\,. \end{array}$$

(b) Offenbar ist f genau dann ein Monomorphismus, wenn f_* injektiv ist für alle X, und ein Epimorphismus, wenn f^* injektiv (!) für alle X ist.

Beispiele 7.5 (a) In den Kategorien $\underline{Sets}$, $\underline{Gr}$, $\underline{Mod}_R$ sind Morphismen genau dann Monomorphismen (bzw. Epimorphismen), wenn sie injektiv (bzw. surjektiv) sind, und genau dann Isomorphismus, wenn sie Monomorphismus und Epimorphismus sind.

(b) In $\underline{Top}$ ist eine stetige Abbildung $f : X \to Y$ genau dann Monomorphimus, wenn sie injektiv ist und genau dann Epimorphismus, wenn sie dichtes Bild hat. Eine bijektive stetige Abbildung ist kein Isomorphimus; Isomorphismen sind per Definition die Homöomorphismen.

(c) Für eine geordnete Menge $(I, \leq)$ ist in der Kategorie $\underline{I}$ aus Beispiel 7.2 (c) jeder Morphismus Monomorphismus und Epimorphismus, aber die einzigen Isomorphismen sind die Identitäten.

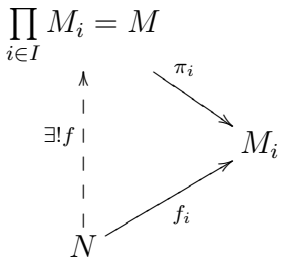
Definition 7.6 Eine Kategorie $\mathcal{C}$ heißt balanciert, wenn ein Morphismus genau dann ein Isomorphismus ist, wenn er ein Monomorphismus und ein Epimorphismus ist.

Definition 7.7 Sei $\mathcal{C}$ eine Kategorie. Dann ist die **duale Kategorie** $\mathcal{C}^{op}$ durch 'Umdrehen der Pfeile' definiert: $ob(\mathbb{C}^{op}) = ob(\mathcal{C})$ und $Hom_{\mathcal{C}^{op}}(A, B) = Hom_{\mathcal{C}}(B, A)$ mit den von $\mathcal{C}$ induzierten Kompositionen.

Bemerkungen 7.8 Ein Morphismus $f : A \to B$ in $\mathcal{C}$ ist genau dann ein Monomorphismus (Epimorphismus, Isomorphismus), wenn er ein Epimorphismus (Monomorphismus, Isomorphismus) in $\mathcal{C}^{op}$ ist.

Wir diskutieren noch einige kategorielle Begriffe – Stichwort Limiten.

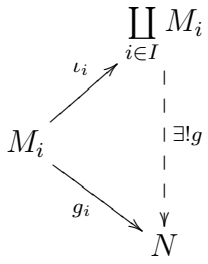
Definition 7.9 Sei $(M_i)_{i\in I}$ eine Familie von Objekten in einer Kategorie $\mathcal{C}$. Ein Objekt M in $\mathcal{C}$ zusammen mit Morphismen $\pi_i : M \to M_i$ für alle $i \in I$ heißt **Produkt der** M_i (Bez.: $M = \prod_{i\in I} M_i$), wenn es folgende universelle Eigenschaft erfüllt:
Ist N ein Objekt in $\mathcal{C}$ und sind $f_i : N \to M_i$ Morphismen für alle $i \in I$, so gibt es einen eindeutig bestimmtem Morphismus $f : N \to M$, der das Diagramm



kommutativ macht. $(M = \prod_{i\in I} M_i, \pi_i)$ ist also universell für Morphismen in die M_i, für alle $i \in I$.

Definition 7.10 Die **Summe** einer Familie $(M_i)_{i\in I}$ von Objekten in $\mathcal{C}$ wird dual erklärt, also (vergleiche 7.7) durch Umdrehen der Pfeile: Ein Objekt $\coprod_{i\in I} M_i$ in $\mathcal{C}$ mit Morphismen

$\iota_i : M_i \to \coprod_{i\in I} M_i$ für alle $i \in I$ heißt Summe der M_i, wenn es für jedes weitere Objekt N und Morphismen $g_i : M_i \to N$ einen eindeutig bestimmten Morphismus $g : \coprod_{i\in I} M_i \to N$ gibt, der



kommutativ macht. $(\coprod_{i\in I} M_i, \iota_i)$ ist also universelles Ziel für Morphismen von allen M_i.

Bemerkungen 7.11 Produkte und Summen müssen nicht existieren, aber wenn sie existieren, sind sie bis auf kanonische Isomorphie eindeutig (dies folgt leicht aus den universellen Eigenschaften).

Beispiele 7.12 (a) In $\underline{Sets}$, $\underline{Gr}$, $\underline{Ab}$ (=Kategorie der abelschen Gruppen) und $\underline{Top}$ existieren beliebige Produkte, gegeben jeweils durch das kartesische Produkt der unterliegenden Mengen. Dies gilt auch für **Top**, man muss aber die Produkttopologie geeignet definieren.

(b) In $\underline{Sets}$ existieren auch beliebige Summen; die Summe der Familie $(M_i)_{i\in I}$ ist dabei gegeben durch die disjunkte Vereinigung $\coprod_{i\in I} M_i (= \bigcup_{i\in I} M_i)$.

(c) In $\underline{Ab}$ und $\underline{Mod_R}$ existieren ebenfalls beliebige Summen, sie sind gegeben durch die bereits früher eingeführten direkten Summen

$$\bigoplus_{i\in I} M_i = \{(x_i)_{i\in I} \in \prod_{i\in I} M_i \mid x_i = 0 \text{ für fast alle } i \in I\}\,.$$

(d) In $\underline{Gr}$ existieren ebenfalls beliebige Summen (im Sinne von Kategorien); für eine Familie $(G_i)_{i\in I}$ von Gruppen ist dies gegeben durch das sogenannte 'freie Produkt' $\underset{i\in I}{*} G_i$, das sogar bei abelschen G_i im Allgemeinen nicht-kommutativ ist (man betrachtet beliebige 'Worte' $g_{i_1} g_{i_2} \dots g_{i_n}$ mit Elementen $g_{i_\nu} \in G_{i_\nu}$, die nur vereinfacht werden können, wenn zwei benachbarte g_i aus derselben Gruppe G_i sind, so dass man sie multiplizieren kann).

Bemerkung 7.13 Mit der expliziten Beschreibung von *Produkten* in $\underline{Sets}$ lassen sich die universellen (und damit charakterisierenden!) Eigenschaften von Produkt und Summe ganz kurz hinschreiben (Bezeichnungen wie in 7.9 und 7.10)

$$(1) \qquad \begin{array}{rcl} \prod_{i\in I} Hom_{\mathcal{C}}(N, M_i) & \xrightarrow{\sim} & Hom_{\mathcal{C}}(N, \prod_{i\in I} M_i) \\ (f_i) & \mapsto & f \end{array}$$

$$(2) \qquad \begin{array}{rcl} \prod_{i\in I} Hom_{\mathcal{C}}(M_i, N) & \xrightarrow{\sim} & Hom_{\mathcal{C}}(\coprod_{i\in I} M_i, N) \\ (g_i) & \mapsto & g \end{array}$$

Wir kommen nun zu "Abbildungen zwischen Kategorien":

Definition 7.14 Seien $\mathcal{A}, \mathcal{B}$ zwei Kategorien. Ein **kovarianter Funktor** $F : \mathcal{A} \to \mathcal{B}$ von $\mathcal{A}$ nach $\mathcal{B}$ ist eine Zuordnung, die
(i) jedem Objekt A in $\mathcal{A}$ ein Objekt $F(A)$ in $\mathcal{B}$ zuordnet, und
(ii) jedem Morphismus $f : A \to B$ in $\mathcal{A}$ einen Morphismus $F(f) : F(A) \to F(B)$ in $\mathcal{B}$ zuordnet.

Dabei muss gelten

(a) $F(1_A) = 1_{F(A)}$ für alle $A \in ob(\mathcal{A})$.

(b) Für Morphismen $f : A \to B$, $g : B \to V$ in $\mathcal{A}$ gilt $F(gf) = F(g)F(f) : F(A) \to F(C)$,

Definition 7.15 Ein **kontravarianter Funktor** $G : \mathcal{A} \to \mathcal{B}$ wird als ein kovarianter Funktor $\mathcal{A} \to \mathcal{B}^{op}$ (oder, äquivalent: $\mathcal{A}^{op} \to \mathcal{B}$) definiert, d.h., G "dreht Pfeile um": Für $f : A \to B$ haben wir also (i) und (a), sowie
(ii') $G(f) : G(B) \to G(A)$,
und entsprechend
(b') $G(gf) = G(f)G(g)$ für $A \xrightarrow{f} B \xrightarrow{g} C$.

Beispiele 7.16 (a) Wir haben den **Vergissfunktor**

$$\begin{array}{rccl} V: & \underline{Gr} & \to & \underline{Sets} \\ & G & \mapsto & G \\ & f & \mapsto & f\,, \end{array}$$

der nur die Gruppenstruktur vergisst.

(b) Entsprechend haben wir einen Vergissfunktor

$$V : \underline{Ringe} \to \underline{Ab}$$

auf der Kategorie der Ringe (mit Ringhomomorphismen), der einen Ring R auf die abelsche Gruppe $(R, +)$ abbildet, sowie weitere Vergissfunktoren

$$\underline{Mod}_R \to \underline{Ab} \quad , \quad \underline{Top} \to \underline{Sets}\,.$$

(c) Sei $\varphi : A \to B$ ein Ringhomomorphismus. Dann haben wir einen Restriktionsfunktor

$$\begin{array}{rccll} Res_{B/A}: & \underline{Mod}_B & \to & \underline{Mod}_A & \\ & M & \mapsto & M & \text{mit Operation von } A \text{ via } \varphi \\ & f & \mapsto & f\,. & \end{array}$$

Weiter ist die Skalarerweiterung (siehe Definition 7.6) ein Funktor

$$\begin{array}{rccl} B\otimes_A: & \underline{Mod}_A & \to & \underline{Mod}_B \\ & M & \mapsto & B \otimes_A M \\ & f : M_1 \to M_2 & \mapsto & f_* : B \otimes_A M_1 \to B \otimes_A M_2\,, \end{array}$$

mit $f_*(b \otimes m_1) = b \otimes f(m_1)$; dies folgt wie in 7.11.

(d) Sei R ein Ring. Die Bildung des freien Moduls gibt einen Funktor

$$\begin{array}{rccl} F_R: & \underline{Sets} & \to & \underline{Mod}_R \\ & I & \mapsto & F_R(I) \\ & (f: I \to J) & \mapsto & (f_*: F_R(I) \to F_R(J))\,. \end{array}$$

Hierbei ist f_* der R-Modul-Homomorphismus, der das kanonische Basiselement $e_i\,(i \in I)$ von $F_R(I)$ auf das Basiselement $e_{f(i)} \in F_R(J)$ abbildet – aufgrund der universellen Eigenschaft des freien Moduls gibt es genau einen R-Modul-Homomorphismus f_* mit dieser Eigenschaft. Man rechnet leicht nach, dass F_R ein Funktor ist, d.h., dass

$$\begin{array}{rrcl} & (gf)_* & = & g_* f_* \quad \text{für } I \xrightarrow{f} J \xrightarrow{g} K \\ \text{und} & (id_I)_* & = & id_{F_R(I)} \quad \text{für alle } I\,. \end{array}$$

Definition 7.17 Seien $F: \mathcal{A} \to \mathcal{B}$ und $G: \mathcal{B} \to \mathcal{C}$ Funktoren. Dann ist die Komposition $G \circ F: A \to \mathcal{C}$ definiert durch

$$\begin{array}{rcll} (G \circ F)(A) & = & G(F(A)) & \text{für} \quad A \in ob(\mathcal{C})\,, \\ (G \circ F)(f) & = & G(F(f)) & \text{für} \quad f: A \to B \text{ in } \mathcal{C}\,. \end{array}$$

Man sieht leicht, dass dies wieder ein Funktor ist. Dieser ist kovariant, wenn F und G beide kovariant oder beide kontravariant sind, und kontravariant sonst.

Definition 7.18 Sei $\mathcal{C}$ eine Kategorie. Für jedes Objekt A in $\mathcal{C}$ ist der **kovariante Hom-Funktor**

$$h^A = Hom_{\mathcal{C}}(A, -): \mathcal{C} \to \underline{Sets}$$

definiert durch

$$\begin{array}{rcll} h^A(X) & = & Hom_{\mathcal{C}}(A, X)\,, & \text{für } X \in ob(\mathcal{C}), \\ h^A(f) & = & f_*: Hom_{\mathcal{C}}(A, X) \to Hom_{\mathcal{C}}(A, Y), & \text{für } f: X \to Y \text{ in } \mathcal{C}\,. \end{array}$$

siehe 7.4. Der **kontravariante Hom-Funktor**

$$h_A = Hom_{\mathcal{C}}(-, A): \mathcal{C} \to \underline{Sets}$$

ist definiert durch

$$\begin{array}{rcll} h_A(X) & = & Hom_{\mathcal{C}}(X, A)\,, & \text{für } X \in ob(\mathcal{C}), \\ h_A(f) & = & f^*: Hom_{\mathcal{C}}(Y, A) \to Hom_{\mathcal{C}}(X, A), & \text{für } f: X \to Y \text{ in } \mathcal{C}\,, \end{array}$$

siehe 7.4.

Wichtig sind auch "Abbildungen zwischen Funktoren":

Definition 7.19 Seien $\mathcal{A}$ und $\mathcal{B}$ Kategorien und $F, G: \mathcal{A} \to \mathcal{B}$ zwei Funktoren von $\mathcal{A}$ nach $\mathcal{B}$. Ein **Morphismus von Funktoren** (oder auch **natürliche Transformation**)

$$u: F \to G$$

von F nach G besteht aus Morphismen in $\mathcal{B}$

$$u_A : F(A) \to G(A)$$

für alle Objekte A in $\mathcal{A}$. Dabei soll gelten, dass für alle Morphismen $f : A \to A'$ das Diagramm

$$\begin{array}{ccc} F(A) & \xrightarrow{u_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(A') & \xrightarrow{u_{A'}} & G(A') \end{array}$$

kommutativ ist (Hierfür sagt man auch, dass die durch die u_A gegebene Zuordnung "natürlich" ist).

Beispiel 7.20 Sei R ein kommutativer Ring mit Eins.

(a) Für jedes $n \in \mathbb{N}$ haben wir dann den Funktor

$$\begin{array}{rccc} T^n : & Mod_R & \to & Mod_R \\ & M & \mapsto & T^n(M) = M^{\otimes n}\,, \end{array}$$

denn wir haben gesehen (siehe Lemma/Definition 8.8), dass jeder Morphismus $\varphi : M \to N$ in Mod_R einen Morphismus

$$\begin{array}{rccc} & T^n(\varphi) : T^n(M) = M^{\otimes n} & \to & N^{\otimes n} = T^n(N) \\ \text{mit} & m_1 \otimes \ldots \otimes m_n & \mapsto & \varphi(m_1) \otimes \ldots \otimes \varphi(m_n) \end{array}$$

induziert, und man sieht sofort, dass für einen Morphismus $\psi : N \to P$ in Mod_R gilt

$$T^n(\psi \circ \varphi) = T^n(\varphi) \circ T^n(\varphi)\,,$$

also die Eigenschaft 7.14 (b). Ebenfalls gilt 7.14 (a):

$$T^n(id_M) = id_{T^n(M)}\,.$$

(b) Entsprechend haben wir Funktoren

$$\begin{array}{rccc} S^n : & Mod_R & \to & Mod_R \\ & M & \mapsto & S^n(M) \end{array}$$

und

$$\begin{array}{rccc} \Lambda^n : & Mod_R & \to & Mod_R \\ & M & \mapsto & \Lambda^n(M)\,. \end{array}$$

(c) Schließlich haben wir Morphismen von Funktoren

$$u : T^n \to S^n\,,$$

wobei

$$\begin{array}{rccc} u_M : & T^n(M) & \to & S^n(M) \\ & m_1 \otimes \ldots \otimes m_n & \mapsto & m_1 \ldots m_n \end{array}$$

die kanonische Surjektion ist, sowie

$$v : T^n \to \Lambda^n \,,$$

wobei

$$\begin{array}{rccc} v_M : & T^n(M) & \to & \Lambda^n(M) \\ & m_1 \otimes \ldots \otimes m_n & \mapsto & m_1 \wedge \ldots \wedge m_n \end{array}$$

die kanonische Surjektion ist (Nachrechnen, dass u und v Morphismen von Funktoren sind!).

Beispiel 7.21 (a) Sei $\mathcal{C}$ eine Kategorie, A ein Objekt in $\mathcal{C}$ und

$$\begin{array}{rccc} h^A = Hom_{\mathcal{C}}(A,-) : & \mathcal{C} & \to & \underline{Sets} \\ & X & \mapsto & Hom_{\mathcal{C}}(A,X) \end{array}$$

der kovariante Hom-Funktor. Jeder Morphismus $g : B \to A$ liefert einen Morphismus von Funktoren

$$g^* : h^A \to h^B \,,$$

wobei für $C \in \mathcal{C}$

$$g^*_C : h^A(C) = Hom_{\mathcal{C}}(A,C) \to Hom_{\mathcal{C}}(B,C) = h^B(C)$$

die Abbildung g^* aus 7.4 (a) ist, also $f : A \to C$ auf $fg : B \to C$ abbildet.

(b) Entsprechend erhält man für den kontravarianten Hom-Funktor $h_B = Hom_C(-,B)$ und einen Morphismus $g : B \to A$ einen Morphismus von Funktoren

$$g_* : h_B \to h_A$$

(Beweis selbst).

Definition 7.22 Ein Morphismus von Funktoren

$$u : F \to G$$

$(F, G : \mathcal{A} \to \mathcal{B})$ heißt **Isomorphismus von Funktoren** (oder **natürliche Äquivalenz**), wenn alle Morphismen

$$u_A : F(A) \xrightarrow{\sim} G(A)$$

Isomorphismen sind.

Offenbar bilden dann die Inversen u_A^{-1} einen Morphismus von Funktoren $u^{-1} : G \to F$ und es gilt $u^{-1} \circ u = Id_{\mathcal{A}}$ und $u \circ u^{-1} = Id_{\mathcal{B}}$, wobei die Komposition von Morphismen von Funktoren in offensichtlicher Weise definiert ist und $Id_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ der identische Funktor einer Kategorie $\mathcal{A}$ ist $(Id_{\mathcal{A}}(A) = A;\ Id_{\mathcal{A}}(f) = f)$.

Man schreibt $F \simeq G$, wenn es einen Isomorphismus $u : F \to G$ von Funktoren gibt.

Definition 7.23 Ein Funktor $F : \mathcal{A} \to \mathcal{B}$ heißt Äquivalenz von Kategorien, wenn es einen Funktor $G : \mathcal{B} \to \mathcal{A}$ gibt mit

$$G \circ F \simeq Id_{\mathcal{A}} \quad , \quad F \circ G \simeq Id_{\mathcal{B}} \,.$$

$\mathcal{A}$ und $\mathcal{B}$ heißen dann äquivalente Kategorien und G heißt ein Quasi-Inverses von F.

Es kommt selten vor, dass man ein echtes Inverses findet, d.h., ein G mit $G \circ F = Id_{\mathcal{A}}$ und $F \circ G = Id_{\mathcal{B}}$.

Beispiel 7.24 Sei k ein Körper und $n \in \mathbb{N}$ und sei $\underline{Vek}_k$ die Kategorie der endlichdimensionalen k-Vektorräume. Sei $M_0 = k^n$, aufgefasst als $M_n(k)$-Modul. Nach Sätzen von Wedderburn hat man eine Kategorienäquivalenz

$$\begin{array}{rccc} F: & \underline{Vek}_k & \to & \underline{Mod}_{M_n(k)} \\ & V & \mapsto & M_0 \otimes_k V \end{array}$$

mit Quasi-Inversem

$$M \mapsto Hom_{M_n(k)}(M_0, M)\,.$$

Definition 7.25 Seien $F : \mathcal{A} \to \mathcal{B}$ und $G : \mathcal{B} \to \mathcal{A}$ Funktoren zwischen Kategorien $\mathcal{A}$ und $\mathcal{B}$. Dann heißt G **linksadjungiert** zu F (und F **rechtsadjungiert** zu G), wenn es für alle Objekte A in $\mathcal{A}$ und Objekte B in $\mathcal{B}$ Isomorphismen

$$\varphi_{A,B} : Hom_{\mathcal{A}}(GB, A) \xrightarrow{\sim} Hom_{\mathcal{B}}(B, FA)$$

gibt, die in folgender Weise funktoriell in A und B sind:
(i) Für jeden Morphismus $f : A \to A'$ ist das Diagramm

$$\begin{array}{ccc} Hom_{\mathcal{A}}(GB, A) & \xrightarrow{\sim} & Hom_{\mathcal{B}}(B, FA) \\ {\scriptstyle f_*}\downarrow & & \downarrow{\scriptstyle F(f)_*} \\ Hom_{\mathcal{A}}(GB, A') & \xrightarrow{\sim} & Hom_{\mathcal{B}}(B, FA') \end{array}$$

kommutativ.
(ii) Für jeden Morphismus $g : B \to B'$ in $\mathcal{B}$ ist das Diagramm

$$\begin{array}{ccc} Hom_{\mathcal{A}}(GB, A) & \xrightarrow{\sim} & Hom_{\mathcal{B}}(B, FA) \\ {\scriptstyle G(g)^*}\uparrow & & \uparrow{\scriptstyle g^*} \\ Hom_{\mathcal{A}}(GB', A) & \xrightarrow{\sim} & Hom_{\mathcal{B}}(B', FA) \end{array}$$

kommutativ.

Satz 7.26 Ist $G : \mathcal{B} \to \mathcal{A}$ linksadjungiert zu $F : \mathcal{A} \to \mathcal{B}$, so gibt es für alle $B \in ob(\mathcal{B})$ kanonische Adjunktionsmorphismen

$$ad_B : B \to FGB$$

und für alle $A \in ob(\mathcal{A})$ kanonische Koadjunktionsmorphismen

$$Ad_A : GFA \to A\,,$$

die Morphismen von Funktorem

$$id_{\mathcal{B}} \to FG$$

$$GF \to id_{\mathcal{A}}$$

liefern.

Dabei sind beide Kompositionen

$$GB \xrightarrow{G(ad_B)} GFGB \xrightarrow{Ad_{GB}} GB$$

$$FA \xrightarrow{ad_{FA}} FGFB \xrightarrow{F(Ad_A)} FA$$

die Identitäten.

Beweis Konstruktion:
(i) Setze $A = GB$ und erhalte ad_B wie folgt:

$$Hom_{\mathcal{A}}(GB, GB) \xrightarrow{\sim} Hom_{\mathcal{B}}(B, FGB)$$

$$id_{GB} \longmapsto ad_B$$

(ii) Setze $B = FA$ und erhalte Ad_A wie folgt:

$$Hom_{\mathcal{B}}(GFA, A) \xrightarrow{\sim} Hom_{\mathcal{B}}(FA, FA)$$

$$Ad_A \longmapsfrom id_{FA}\,.$$

Beweis der Behauptung: selbst!

Beispiele (a) Der Vergissfunktor $V : \underline{Mod}_R \to \underline{Sets}$ besitzt den Linksadjungierten $F_R : \underline{Sets} \to \underline{Mod}_R$, $I \mapsto F_R(I)$. Denn es ist gerade

$$\begin{array}{rcl} Hom_R(F_R(I), M) & \tilde{\to} & Hom_{\underline{Sets}}(I, M) \\ \varphi & \mapsto & (i \mapsto \varphi(i)) \\ \text{eindeutiges } \varphi \text{ mit } \varphi(e_i) = f(i) & \leftarrow\!\shortmid & f : I \to M\,. \end{array}$$

(b) Sei R ein kommutativer Ring mit Eins. Der Vergissfunktor

$$(\text{kommutative } R\text{-Algebren mit Eins}) \to \underline{Sets}$$

besitzt das Linksadjungierte $I \mapsto R[X_i | i \in I]$, denn es ist

$$\begin{array}{rcl} Hom_{R-Alg}(R[X_i | i \in I], A) & \tilde{\to} & Hom_{\underline{Sets}}(I, A) \\ \varphi & \mapsto & (i \mapsto \varphi(X_i)) \\ \text{eindeutiges } \varphi \text{ mit } \varphi(X_i) = f(i) & \leftarrow\!\shortmid & f : I \to A \end{array}$$

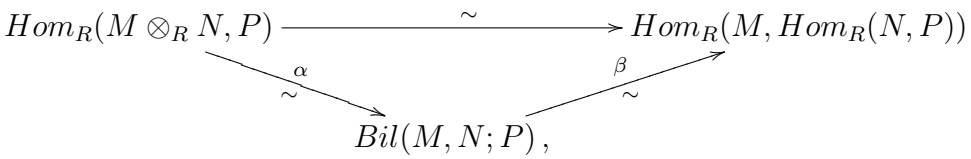
(c) Sei R ein kommutativer Ring mit Eins. Für jeden R-Modul N hat der kovariante Hom-Funktor

$$Hom_R(N, -) : \underline{Mod}_R \to \underline{Mod}_R$$

den Linksadjungierten

$$- \otimes_R N : \underline{Mod}_R \to \underline{Mod}_R \,,$$

denn man hat kanonische Isomorphismen, funktoriell in M und P



wobei $Bil(M, N; P)$ die Menge der bilinearen Abbildungen $\varphi : M \times N \to P$ ist. Hier ist α der kanonische Isomorphismus aus der universellen Eigenschaft des Tensorprodukts, und β bildet eine bilineare Abbildung φ auf den Homomorphismus (!)

$$m \mapsto (n \mapsto \varphi(m, n))$$

ab.

(d) Ist $F : \mathcal{A} \xrightarrow{\sim} \mathcal{B}$ eine Kategorienäquivalenz mit Quasi-Inversem $G : B \xrightarrow{\sim} \mathcal{A}$, so sind F und G adjungiert zueinander.

8 Endliche und ganze Ringerweiterungen

Die Begriffe und Ergebnisse in diesem Paragraphen sind nützlich für die Zahlentheorie und die Algebraische Geometrie. Im Folgenden betrachten wir immer kommutative Ringe mit Eins.

Definition 8.1 Sei A ein Ring und B eine A-Algebra. B heißt endliche A-Algebra, wenn B als A-Modul endlich erzeugt ist. Wir sagen auch, dass der Ringhomomorphismus $A \to B$ endlich ist.

Für eine A-Algebra B und ein Element $b \in B$ sei $A[b]$ die kleinste A-Unteralgebra von B, die b enthält. Offenbar besteht $A[b]$ aus allen A-Linearkombinationen der Elemente $b^n, n \geq 0$.

Lemma/Definition 8.2 Sei A ein Ring und B eine A-Algebra.

(a) Ein Element $b \in B$ heißt ganz über A, wenn die folgenden äquivalenten Bedingungen erfüllt sind.

(i) Es gibt ein normiertes Polynom

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in A[x]\,,$$

so dass $f(b) = 0$ in B, d.h., es gibt eine sogenannte *Ganzheitsgleichung*

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1b + a_0 \quad \text{mit } a_i \in A\,. \tag{8.2.1}$$

(ii) $A[b] \subseteq B$ ist eine endliche A-Algebra.

(iii) Es gibt einen Unterring $B' \subseteq B$ mit $A[b] \subseteq B'$, der eine endliche A-Algebra ist.

(b) B heißt ganz über A, wenn jedes $b \in B$ ganz über A ist.

Beweis der Äquivalenzen in (a):

(i) $\Rightarrow$ (ii): Nach Definition wird $A[b]$ als A-Modul von allen b^m ($m \in \mathbb{N}$) erzeugt. Aus (8.2.1) folgt aber per Induktion, dass $A[b]$ von $1, b \ldots, b^{n-1}$ erzeugt wird.

(ii) $\Rightarrow$ (iii): Setze $B = A[b]$.

(iii) $\Rightarrow$ (i): Die Multiplikation mit b ist ein Endomorphismus φ_b von B'. Da B' ein endlich erzeugter A-Modul ist, gibt es nach Satz 8.15 (Cayley-Hamilton) ein normiertes Polynom $f(x) \in A[x]$ mit $f(\varphi_b) = 0$. Angewandt auf das Element $1 \in B'$ folgt $f(b) = 0$.

Corollar 8.3 (a) Eine endliche A-Algebra B ist ganz über A.

(b) $b_1, \ldots, b_n \in B$ sind genau dann ganz über A, wenn $A[b_1, \ldots, b_n]$ eine endliche A-Algebra ist.

(c) Die Menge $\overline{A}$ aller Elemente $b \in B$, die ganz über A sind, bildet eine A-Unteralgebra von B und heißt der ganze Abschluss von A in B.

Beweis (a) folgt mit Kriterium (iii), (b) folgt durch Induktion über n mit Kriterium (ii) und (c) folgt aus (b).

Satz 8.4 (going-up-Theorem von Krull-Cohen-Seidenberg) Sei B/A eine ganze Ring-Erweiterung, d.h., $A \subseteq B$ ist ein Unterring, und B ist ganz über A. Dann gilt:

(a) Ist $\mathfrak{P} \subseteq B$ ein Primideal über $\mathfrak{p} \subseteq A$ (d.h., $\mathfrak{P} \cap A = \mathfrak{p}$), so ist $\mathfrak{P}$ genau dann maximal, wenn $\mathfrak{p}$ maximal ist.

(b) Sind $\mathfrak{P} \subseteq \mathfrak{P}' \subseteq B$ Primideale über demselben Primideal $\mathfrak{p} \subseteq B$, so ist $\mathfrak{P} = \mathfrak{P}'$.

(c) Über jedem Primideal $\mathfrak{p} \subseteq A$ liegt ein Primideal $\mathfrak{P} \subseteq B$, d.h., die Abbildung $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ ist surjektiv.

(d) (going-up) Sei $\mathfrak{P} \subseteq B$ ein Primideal und $\mathfrak{p} \subseteq A$ das darunterliegende Primideal. Ist $\mathfrak{p}' \subseteq A$ ein weiteres Primideal mit $\mathfrak{p} \subseteq \mathfrak{p}'$, so gibt es ein Primideal $\mathfrak{P}' \subseteq B$ über $\mathfrak{p}'$ mit $\mathfrak{P} \subseteq \mathfrak{P}'$.

Beweis (b): Angenommen $\mathfrak{P} \subsetneqq \mathfrak{P}'$. Sei $f \in \mathfrak{P}' \smallsetminus \mathfrak{P}$. Sei $p(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ normiert mit $n \geq 1$ und

$$p(f) = f^n + a_{n-1}f^{n-1} + \ldots + a_1 f + a_0 \in \mathfrak{P}\,. \tag{8.4.1}$$

Ein solches $p(X)$ gibt es immer, da f ganz über A ist (so dass wir sogar $p(f) = 0$ erreichen). Sei $p(x)$ mit minimalen Grad gewählt. Aus der Gleichung (8.4.1) folgt $a_0 \in \mathfrak{P}' \cap A = \mathfrak{p}$, also auch $a_0 \in \mathfrak{P}$.

Wegen $f \notin \mathfrak{P}$ ist $n > 1$. Dann haben wir

$$f \cdot (f^{n-1} + a_{n-1}f^{n-1} + \ldots + a_1) \in \mathfrak{P}\,.$$

Da $\mathfrak{P}$ ein Primideal ist, und $f \notin \mathfrak{P}$, folgt

$$f^{n-1} + a_{n-1}f^{n-1} + \ldots + a_2 f + a_1 \in \mathfrak{P}$$

im Widerspruch dazu, dass der Grad von $p(X)$ minimal war.

(a): Ist $\mathfrak{p}$ maximal, so auch $\mathfrak{P}$. Wäre nämlich $\mathfrak{P}' \supsetneqq \mathfrak{P}$ ein echt größeres Primideal, so wäre nach (b) $\mathfrak{p}' = \mathfrak{P} \cap A \supsetneqq \mathfrak{p}$ – Widerspruch.

Sei umgekehrt $\mathfrak{P}$ maximal. Dann ist $B/\mathfrak{P}$ ein Körper und $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$ wieder eine ganze Ringerweiterung. Es genügt also zu zeigen: Ist B ein Körper, so auch A. Sei B ein Körper, und $a \in A \smallsetminus \{0\}$. Für $b = \frac{1}{a} \in B$ gibt es dann eine Gleichung

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

mit $a_0, \ldots, a_{n-1} \in A$. Durch Multiplikation mit a^{n-1} folgt

$$\frac{1}{a} = -(a_{n-1} + a a_{n-2} + \ldots + a^{n-1}a_0) \in A\,.$$

Für (c) betrachte das kommutative Diagramm

$$\begin{array}{ccc} B & \xrightarrow{\psi} & B_{\mathfrak{p}} \\ \uparrow{\scriptstyle \subseteq} & & \uparrow{\scriptstyle \subseteq} \\ A & \xrightarrow{\varphi} & A_{\mathfrak{p}}\,, \end{array}$$

wobei $B_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1}B$ die Lokalisierung von B nach $A \setminus \mathfrak{p}$ ist.

Dann ist $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$ injektiv (wegen der Exaktheit der Lokalisierung, siehe 5.10) und eine ganze Ringerweiterung: Sei nämlich $\frac{b}{f} \in B_\mathfrak{p}$, mit $b \in B$ und $f \in A \setminus \mathfrak{p}$, und sei

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

(mit $a_0, \ldots a_{n-1} \in A$) eine Ganzheitsgleichung für b. Teilt man diese Gleichung durch f^n, so erhält man eine Ganzheitsgleichung für $\frac{b}{f}$ über $A_\mathfrak{p}$.

Da $A_\mathfrak{p} \neq 0$, ist auch $B_\mathfrak{p} \neq 0$, besitzt also ein maximales Ideal $\tilde{\mathfrak{P}}$. Nach (a) ist $\tilde{\mathfrak{p}} = \tilde{\mathfrak{P}} \cap A_\mathfrak{p}$ ein maximales Ideal von $A_\mathfrak{p}$, also gleich dem eindeutig bestimmten maximalen Ideal $\mathfrak{p}A_\mathfrak{p}$ des lokalen Rings $A_\mathfrak{p}$. Weiter gilt $\varphi^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$ (vergleiche (5.14.2) für $s = 1$). Deswegen gilt für $\mathfrak{P} = \psi^{-1}(\tilde{\mathfrak{P}})$ die Gleichheit $\mathfrak{P} \cap A = \mathfrak{p}$ wie gewünscht.

Für (d) betrachten wir die Ringerweiterung $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$, die wieder ganz ist. Dann ist $\mathfrak{p}'/\mathfrak{p} \subseteq A/\mathfrak{p}$ ein Primideal, und nach (c) gibt es ein Primideal $\tilde{\mathfrak{P}} \subseteq B/\mathfrak{P}$ über $\mathfrak{p}'/\mathfrak{p}$. Dann ist $\tilde{\mathfrak{P}} = \mathfrak{P}'/\mathfrak{P}$ für ein Primideal $\mathfrak{P}' \subseteq B$ mit $\mathfrak{P}' \supseteq \mathfrak{P}$ (vergleiche Übungsaufgabe 1), und für dieses gilt $\mathfrak{P}' \cap A = \mathfrak{p}'$.

9 Die Dimension von Ringen und endlich erzeugten k-Algebren

In diesem Kapitel betrachten wir immer kommutative Ringe mit Eins. Für diese hat man eine Dimensionstheorie.

Definition 9.1 Die (Krull-)**Dimension** eines Ringes R ist definiert als

$$\dim R \;=\; \sup\{r \in \mathbb{N}_0 \mid \text{es existiert eine Kette der Länge } r: \; \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_{r-1} \subsetneqq \mathfrak{p}_r \text{ von Primidealen } \mathfrak{p}_i \subseteq R\}.$$

Beispiele 9.2 (a) Für einen Körper K ist $\dim K = 0$, da K nur das Primideal $\{0\}$ hat.

(b) Sei k ein Körper. Es ist $\dim k[x] = 1$, denn die Primideale in $k[x]$ sind $< 0 >$ und die Ideale $< f >$ für $f \in k[x]$ irreduzibel. Die maximalen Ketten sind also von der Form $\{0\} \subsetneqq < f >$, denn für ein irreduzibles g mit $< f > \neq < g >$ sind f und g nicht assoziiert, also teilerfremd; also kann es keine Inklusion zwischen $< f >$ und $< g >$ geben. Entsprechend ist $\dim R = 1$ für jeden (integren) Hauptidealring, z.B. ist $\dim \mathbb{Z} = 1$. Weiter ist $\dim(R) = 1$ für jeden diskreten Bewertungsring.

(c) $\dim k[x_n \mid n \in \mathbb{N}] = \infty$.

(d) Es gibt noethersche Ringe unendlicher Dimension.

Aus den Ergebnissen von Kapitel 9 folgern wir:

Satz 9.3 Ist $A \hookrightarrow B$ eine ganze Ringerweiterung, so gilt

$$\dim A \;=\; \dim B\,.$$

Beweis Ist

$$\mathfrak{P}_0 \subsetneqq \mathfrak{P}_1 \subsetneqq \ldots \subsetneqq \mathfrak{P}_r \tag{9.3.1}$$

eine Primidealkette in B, und ist $\mathfrak{p}_i = \mathfrak{P}_i \cap A \;\; (i = 1, \ldots, r)$, so ist nach Satz 9.4 (b)

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r \tag{9.3.2}$$

eine Primidealkette in A. Es ist also $\dim A \geq \dim B$. Ist umgekehrt (9.3.2) eine Primidealkette in A, so gibt es nach 9.4 (c) ein $\mathfrak{P}_0 \in \mathrm{Spec}(B)$ über $\mathfrak{p}_0$, und aus 9.4 (d) und (b) folgt induktiv die Existenz einer Primidealkette (9.3.1) in B mit $\mathfrak{P}_i \cap A = \mathfrak{p}_i$. Also ist $\dim B \geq \dim A$.

Wir werden nun zeigen, dass $\dim k[X_1, \ldots, X_n] = n$ für einen Körper k ist, und wie man hieraus die Dimension von endlich erzeugten k-Algebren A berechnet.

Hierzu definieren wir:

Lemma/Definition 9.4 Sei R ein Ring. Eine R-Algebra A heißt endlich erzeugt (oder von endlichem Typ über R), wenn die folgenden äquivalenten Bedingungen gelten.

(a) A wird als R-Algebra von endlich vielen Elementen $a_1, \ldots, a_n$ erzeugt.

(b) Es gibt einen surjektiven Homomorphismus von R-Algebren $R[X_1, \ldots, X_n] \twoheadrightarrow A$ (d.h., A ist Quotient eines Polynomrings über R in endlich vielen Variablen).

Beweis der Äquivalenz: Sei $R[a_1, \ldots, a_n]$ die von $a_1, \ldots, a_n$ erzeugte R-Unteralgebra von A, d.h., die kleinste R-Unteralgebra, die $a_1, \ldots, a_n$ enthält. Dann besteht $R[a_1, \ldots, a_n]$ aus allen polynomialen Ausdrücken in den a_i, d.h., ist das Bild von

$$\begin{array}{rcl} R[X_1, \ldots, X_n] & \to & A \\ f & \mapsto & f(a_1, \ldots, a_n)\,. \end{array}$$

Definition 9.5 Sei A ein Ring und B eine A-Algebra. Elemente $b_1, \ldots, b_n \in B$ heißen *algebraisch unabhängig über* A, wenn es kein Polynom $f \in A[x_1, \ldots, x_n] \smallsetminus \{0\}$ gibt mit $f(b_1, \ldots, b_n) = 0$ ($\Leftrightarrow$ die verschiedenen Potenzen $b_1^{i_1} \ldots b_n^{i_n}$ sind *linear unabhängig* über A, d.h., es gibt keine nicht-triviale A-Linearkombination zu 0 $\Leftrightarrow$ der Einsetzungshomomorphismus $A[x_1, \ldots, x_n] \to B$, $x_i \mapsto b_i$, ist injektiv).

Satz 9.6 (Noether-Normalisierung) Sei A eine endlich erzeugte k-Algebra, k ein Körper, und sei $I \subseteq A$ ein Ideal, $I \neq A$. Dann gibt es $i, d, \in \mathbb{N}_0$, $i \leq d$, und Elemente $y_1, \ldots, y_d \in A$, so dass gilt:

(a) $y_1, \ldots, y_d$ sind algebraisch unabhängig über k.

(b) A ist endliche $k[y_1, \ldots, y_d]$-Algebra (d.h., als $k[y_1, \ldots, y_d]$-Modul endlich erzeugt).

(c) $I \cap k[y_1, \ldots, y_d] =< y_{i+1}, \ldots, y_d >$.

1. Zusatz: Ist $A = k[x_1, \ldots, x_n]$, so kann $d = n$ gewählt werden.

2. Zusatz: Für unendliches k können dabei $y_1, \ldots, y_i$ als Linearkombinationen der $x_1, \ldots, x_n$ gewählt werden.

Bevor wir den Satz beweisen, ziehen wir einige Schlussfolgerungen.

Corollar 9.7 (a) $\dim k[x_1, \ldots, x_n] = n$.

(b) Ist $k[y_1, \ldots, y_n] \subseteq A$ eine Noether-Normalisierung (d.h., wie im Satz eine Injektion eines Polynomrings in A so, dass A endlich erzeugt als $k[y_1, \ldots, y_n]$-Modul ist), so ist $\dim A = n$.

Beweis Nach Satz 9.3 ist $\dim A = \dim k[y_1, \ldots, y_n]$, und es genügt (a) zu zeigen. Die Primidealkette

$$\langle 0 \rangle \subsetneqq < x_1 > \subsetneqq < x_1, x_2 > \subsetneqq \ldots \subsetneqq < x_1, \ldots, x_n > \subseteq k[x_1, \ldots, x_n] =: B$$

zeigt, dass $\dim B \geqslant n$ ist. Es ist also zu zeigen: Für eine Primidealkette der Länge r in B

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r$$

ist $r \leq n$. Wir beweisen dies durch Induktion über n. Für $n = 0$ ist nichts zu zeigen; sei $n > 0$, und die Behauptung und damit auch (b) für weniger Variablen als n schon bewiesen. Nach 9.6, 1. Zusatz gibt es eine Noether-Normalisierung

$$k[t_1, \ldots, t_n] \subseteq k[x_1, \ldots, x_n]$$

mit

$$\mathfrak{p}_1' := \mathfrak{p}_1 \cap k[t_1, \ldots, t_n] =< t_{i+1}, \ldots, t_n >$$

für ein $i \leq n$. Nach 9.4 (b) ist für $\mathfrak{p}_0' = \mathfrak{p}_0 \cap k[t_1, \ldots, t_n]$ wegen $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1$ auch $\mathfrak{p}_0' \subsetneqq \mathfrak{p}_1'$, also insbesondere $\mathfrak{p}_1' \neq 0$ und damit $i < n$.

Nun ist

$$\begin{array}{ccc} k[t_1, \ldots, t_n]/ < t_{i+1}, \ldots, t_n > & \hookrightarrow & B/\mathfrak{p}_1 \\ \| \wr & & \\ k[t_1, \ldots, t_i] & & \end{array}$$

wieder eine Noether-Normalisierung. Für die Primidealkette

$$\{0\} = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneqq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r/\mathfrak{p}_1$$

der Länge $r - 1$ in $B/\mathfrak{p}_1$ gilt also nach (b) und der Induktionsvoraussetzung $r - 1 \leq i < n$. Es folgt $r \leq n$.

Beweis von Satz 9.6

1. Fall $A = k[x_1, \ldots x_n]$ und $I =< f >$ ist ein Hauptideal, $f \neq 0$.

Lemma 9.8 (a) Durch eine Substitution der Form

$$x_i = y_i + x_n^{r_i} \qquad (i = 1, \ldots, n-1) \tag{9.8.1}$$

mit geeigneten $r_i \in \mathbb{N}_0$ geht f über in ein Element der Form

$$a\, x_n^m + g_{m-1}\, x_n^{m-1} + \ldots + g_1\, x_n + g_0$$

mit $a \in k$ und $g_i \in k[y_1, \ldots, y_{n-1}]$.

(b) Ist k unendlich, so ist dies auch möglich mit einer Substitution

$$x_i = y_i + a_i\, x_n \tag{9.8.2}$$

mit geeigneten $a_i \in k \quad (i = 1, \ldots, n-1)$.

Beweis Sei $f = \sum a_{i_1,\ldots,i_n} x^{i_1} \ldots x^{i_n} \neq 0$. Im Fall (a) ist nach der Substitution

$$\begin{aligned} f &= \sum a_{i_1,\ldots,i_n} (x_n^{r_1} + y_1)^{i_1} \ldots (x_n^{r_{n-1}} + y_{n-1})^{i_{n-1}} x_n^{i_n} \\ &= \sum a_{i_1,\ldots,i_n} (x_n^{i_1 r_1 + i_2 r_2 + \ldots + i_{n-1} r_{n-1} + i_n} + \ldots)\ , \end{aligned}$$

wobei die Punkte Terme bedeuten, in denen x_n mit niedrigerer Potenz auftritt.

Sei $k = \max\{i \mid \exists\, (i_1, \ldots, i_n) \text{ mit } a_{i_1,\ldots,i_n} \neq 0 \text{ und } i \in \{i_1, \ldots, i_n\}\} + 1$. Die Zahlen

$$i_n + i_1 k + \ldots + i_{n-1} k^{n-1} \quad (a_{i_1,\ldots,i_n} \neq 0) \tag{9.8.3}$$

sind dann für verschiedene n-Tupel $(i_1, \ldots, i_n)$ mit $a_{i_1,\ldots,i_n} \neq 0$ verschieden. Setzt man $r_i := k^i \quad (i = 1, \ldots, n-1)$, so erhält man die Darstellung in (a) mit $m =$ Maximum der Zahlen (9.8.3).

(b): Sei

$$f = f_0 + f_1 + \ldots f_m$$

die Zerlegung von f in homogene Komponenten f_i, mit $\deg(f_i) = i$, wobei $f_m \neq 0$ sei. Nach der Substitution in (b) ist

$$f = f_m(a_1, \ldots, a_{n-1}, 1)x_n^m + \ldots$$

wobei die Punkte Terme bedeuten, in denen x_n in niedrigerer Potenz als m vorkommt. Ist k unendlich, so gibt es ein Tupel $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ mit $f_m(a_1, \ldots, a_{n-1}, 1) \neq 0$ (Ist f_m homogen, $\neq 0$ so ist $f(x_1, \ldots, x_{n-1}, 1) \neq 0$), und die Behauptung folgt.

Wir beweisen damit Satz 9.6 im ersten Fall: Wähle

$$y_n = f \tag{41}$$

und y_i wie in Lemma 9.8 $(i = 1, \ldots, n-1)$ (Für unendliches k seien die y_i wie in (9.8.2) gewählt). Dann sind $y_1, \ldots y_{n-1}$ algebraisch unabhängig über k (rechne modulo x_n !). Es sind auch $y_1, \ldots, y_n$ algebraisch unabhängig über k. Denn: Es ist von der Form der Substitution klar, dass mit $x_1, \ldots, x_n$ auch $y_1, \ldots, y_{n-1}, x_n$ algebraisch unabhängig sind: Ist $g \in k[x_1, \ldots, x_n] \setminus \{0\}$ mit $0 = g(y_1, \ldots, y_{n-1}, x_n) = g(x_1 - x_n^{k_1}, \ldots, x_{n-1} - x_n^{k_{n-1}}, x_n)$ so ist durch erneute Substitution $x_i \mapsto x_i + x_n^{k_i}$ $(i = 1, \ldots, n-1)$ und $x_n \mapsto x_n$ auch $0 = g(x_1, \ldots, x_n)$. Wäre nun

$$\sum_{i=0}^{r} g_i(y_1, \ldots, y_{n-1}) y_n^i = 0 \,,$$

mit $g_r(y_1, \ldots, y_{n-1}) \neq 0$, so folgte mit $y_n = f = a\, x_n^m + \ldots$

$$0 = a^r\, g_r(y_1, \ldots y_{n-1}) x_n^{m \cdot r} + \ldots$$

wobei $\ldots$ Terme bedeutet, in denen x_n mit kleinerem Grad vorkommt. Widerspruch zur algebraischen Unabhängigkeit von $y_1, \ldots, y_{n-1}, x_n$!

Weiter ist $A = k[y_1, \ldots, y_{n-1}][x_n]$ und daher endlich über $k[y_1, \ldots, y_n]$; denn mit den Bezeichnungen von 9.8 ist

$$0 \;=\; f - y_n \;= a\; x_n^m + g_{m-1}(y_1, \ldots, y_{n-1}) x_n^{m-1} + \ldots + (g_0\,(y_1, \ldots, y_{n-1}) - y_n) \,,$$

also ist x_n ganz über $k[y_1, \ldots, y_n]$ (da $a \in k^\times$). Damit gilt der 1. Zusatz.

Es bleibt zu zeigen: $I \cap k[y_1, \ldots, y_n] =< y_n >$, wobei "$\supseteq$" nach Definition gilt. Sei umgekehrt $g \in I \cap k[y_1 \ldots, y_n]$. Dann ist $g = h \cdot y_n$ mit $h \in A$. Es gibt dann eine Gleichung

$$h^s + a_{s-1} h^{s-1} + \ldots + a_1 h + a_0 = 0$$

mit $s > 0$ und $a_0, \ldots, a_{s-1} \in k[y_1, \ldots, y_n]$. Es folgt (durch Multiplikation mit y_n^s)

$$g^s + a_{s-1}\, y_n\, g^{s-1} + \ldots + a_1\, y_n^{s-1}\, g + a_0\, y_n^s = 0 \,,$$

also $g^s \in < y_n > \subseteq k[y_1, \ldots, y_n]$ und daher auch $g \in < y_n >$, da dies ein Primideal ist. Für unendliches k ist nach Wahl von $y_1, \ldots, y_{n-1}$ auch der 2. Zusatz erfüllt.

2. Fall $A = k[x_1, \ldots, x_n]$, und $I \subsetneqq A$ ist ein beliebiges Ideal.

Für $I = < 0 >$ ist nichts zu zeigen; sei also $0 \neq f \in I$ nicht konstant. Für $n = 1$ sind wir ebenfalls fertig: dann ist I ein Hauptideal und wir sind im 1. Fall. Sei also $n > 1$, und sei $k[y_1, \ldots, y_n] \subseteq A$ mit $y_n = f$ wie im 1. Fall konstruiert (Insbesondere sei $x_i = y_i + a_i x_n \quad (i = 1, \ldots, n-1)$ für unendliches k). Durch Induktion über n können wir annehmen, dass die Behauptung für $k[y_1, \ldots, y_{n-1}]$ und das Ideal $I \cap k[y_1, \ldots, y_{n-1}]$ schon gilt; es gibt also eine Noether-Normalisierung (1. Zusatz!)

$$k[t_1, \ldots, t_{n-1}] \subseteq k[y_1, \ldots, y_{n-1}]$$

$$\text{mit} \quad I \cap k[t_1, \ldots, t_{n-1}] = < t_{i+1}, \ldots, t_{n-1} >$$

für ein $i \leq n-1$. Für unendliches k können wir dabei annehmen, dass $t_1, \ldots, t_i$ Linearkombinationen der $y_1, \ldots, y_{n-1}$ sind, also auch der $x_1, \ldots, x_n$. Mit $k[t_1, \ldots, t_{n-1}] \hookrightarrow k[y_1, \ldots, y_{n-1}]$ ist auch $k[t_1, \ldots, t_{n-1}, y_n] \hookrightarrow k[y_1, \ldots, y_n]$ eine endliche Ringerweiterung, also gilt dies auch für $k[t_1, \ldots, t_{n-1}, y_n] \hookrightarrow A$. Die algebraische Unabhängigkeit von $t_1, \ldots t_{n-1}$, y_n in A ist nun offensichtlich (selbst!).

Jedes $g \in I \cap k[t_1, \ldots, t_{n-1}, y_n]$ schreibt sich wegen $y_n \in I$ als

$$g = g^* + h \cdot y_n$$

mit $g^* \in I \cap k[t_1, \ldots, t_{n-1}] = < t_{i+1}, \ldots, t_{n-1} >$ und $h \in k[t_1, \ldots, t_{n-1}, y_n]$. Es folgt $I \cap k[t_1, \ldots, t_{n-1}, y_n] = < t_{i+1}, \ldots, t_{n-1}, y_n >$.

3. Fall =allgemeiner Fall:

Schreibe $A = k[x_1, \ldots x_n]/J$ und bestimme nach dem 2. Fall eine Noether-Normalisierung

$$k[y_1, \ldots, y_n] \subseteq k[x_1, \ldots, x_n]$$

mit $J \cap k[y_1, \ldots, y_n] = < y_{i+1}, \ldots, y_n >, \quad i \leq n$. Dies liefert eine Noether-Normalisierung

$$\begin{array}{ccc} k[y_1, \ldots, y_n]/ < y_{i+1}, \ldots, y_n > & \hookrightarrow & A \\ \| \wr & & \\ k[y_1, \ldots, y_i] & & \end{array}$$

Wenden wir den 2. Fall noch einmal an, auf $k[y_1, \ldots, y_i]$ und $I' = I \cap k[y_1, \ldots, y_i]$, so erhalten wir eine Noether-Normalisierung

$$k[t_1, \ldots, t_i] \hookrightarrow k[y_1, \ldots, y_i]$$

$$\text{mit } I' \cap k[t_1, \ldots, t_i] = < t_{j+1}, \ldots, t_i > \qquad j \leq i \, .$$

Dann ist

$$k[t_1, \ldots, t_i] \hookrightarrow A$$

die gewünschte Noether-Normalisierung für A und I. Für unendliches k sind dabei ohne Einschränkung $y_1, \ldots, y_i$ Linearkombinationen der $x_1, \ldots, x_n$ und $t_1, \ldots, t_j$ Linearkombinationen der $y_1, \ldots, y_i$, also auch der $x_1, \ldots, x_n$.

Bemerkung 9.9 Der Beweis zeigt: Ist A eine endlich erzeugte k-Algebra und $I_0 \subseteq I_1 \subseteq \dots I_r$ eine Kette von Idealen, so gibt es eine Noether-Normalisierung

$$k[y_1, \dots, y_n] \subseteq A$$

$$\text{mit } I_\nu \cap k[y_1, \dots, y_n] =< y_{i_\nu+1}, \dots, y_n >$$

für $\nu = 0, \dots, r$ (und $i_0 \geqslant i_1 \geqslant \dots \geqslant i_r$).

Corollar 9.10 Sei k ein Körper. Für eine endlich erzeugte k-Algebra A sind äquivalent
(i) $\dim A = 0$
(ii) $\dim_k A < \infty$ (A ist als k-Vektorraum endlich-dimensional).

Beweis Sei $k[X_1, \dots, X_d] \hookrightarrow A$ eine Noether-Normalisierung ($d = \dim A$). Dann gilt $d = 0$ genau dann, wenn A endlich-dimensional ist.

Corollar 9.11 Sei k ein algebraisch abgeschlossener Körper. Ein polynomiales Gleichungssystem

$$\begin{aligned} f_1(X_1, \dots, X_n) &= 0 \\ &\vdots \\ f_m(X_1, \dots, X_n) &= 0 \end{aligned}$$

hat genau dann endlich viele Lösungen in k, wenn die Dimension des Rings

$$A = k[X_1, \dots, X_n]/ < f_1, \dots, f_m >$$

gleich null ist, also wenn diese k-Algebra endliche k-Dimension hat.

Beweis Sei $k[x_1, \dots, x_d] \hookrightarrow A$ eine Noether-Normalisierung mit $d \geq 1$. Ist $a = (a_1, \dots, a_d) \in k^d$, so ist der Kern $\mathfrak{m}_a$ des Einsetzungsmorphismus

$$\begin{array}{rcccc} \varphi_0 & = & k[x_1, \dots, x_d] & \to & k \\ & & x_i & \mapsto & a_i \end{array}$$

ein maximales Ideal. Für $a' = (a'_1, \dots, a'_d) \neq a$ ist $\mathfrak{m}_a \neq \mathfrak{m}_{a'}$, denn für $a_i \neq a'_i$ ist $x_i - a_i$ im Kern $\mathfrak{m}_a$ aber nicht im Kern $\mathfrak{m}_{a'}$. Es gibt also unendlich viele verschiedene solche Ideale $\mathfrak{m}_a$.

Nach dem going-up-Theorem 9.4 liegt aber über jedem $\mathfrak{m}_a$ ein maximales Ideal $\mathfrak{n}_a$ von A; diese sind also alle verschieden. Da A endlich über $k[x_1, \dots, x_d]$ ist, ist auch

$$k \cong k[x_1, \dots, x_d]/\mathfrak{m}_a \hookrightarrow A/\mathfrak{n}_a$$

eine endliche Körpererweiterung. Da k algebraisch abgeschlossen ist, ist also $k \xrightarrow{\sim} A/\mathfrak{n}_a$. Dies liefert eine Surjektion von k-Algebren.

$$\varphi : k[x_1, \dots, x_n] \twoheadrightarrow k[x_1, \dots, x_n]/\langle f_1, \dots, f_m \rangle = A \twoheadrightarrow k\,.$$

Sind $a_1, \dots a_n \in k$ die Bilder von $x_1, \dots, x_n$ in k, so muss also gelten

$$f_i(a_1, \dots, a_n) = 0 \quad \text{für alle} \quad i = 1, \dots, m$$

(da $\langle f_1, \ldots, f_n \rangle \subseteq \ker(\varphi)$). Für jedes $\mathfrak{n}_a$ erhalten wir also eine Lösung des Gleichungssystems, also unendlich viele.

Ist aber $d = 0$, so ist A endlich-dimensional über k. Sei $b_1, \ldots, b_r$ eine k-Basis. Für jedes i haben wir eine Surjektion

$$\begin{array}{rccc} \varphi_i & : & k[x] & \twoheadrightarrow & k[b_i] \\ & & x & \mapsto & b_i \,, \end{array}$$

wobei $k[b_i]$ die von b_i erzeugte Unteralgebra von A ist. Der Kern von φ_i ist ein Hauptideal $\langle g_i \rangle$ mit einem Polynom $g_i \neq 0$. Ist nun $(a_1, \ldots, a_n) \in k^n$ eine Lösung des Gleichungssystems, so erhalten wir einen k-Homomorphismus

$$\begin{array}{rccc} \psi_i : k[x]/\langle g_i \rangle \xrightarrow{\sim} k[b_i] \hookrightarrow A & \twoheadrightarrow & k \,. \\ \overline{x_i} & \mapsto & a_i \end{array}$$

Für diesen muss $g_i(x)$ auf null abgebildet werden, also x (und damit b_i) auf eine Nullstelle von g_i. Dies gibt nur endlich viele Möglichkeiten, um b_i abzubilden, für $i = 1, \ldots, r$, also nur endlich viele Möglichkeiten für $\varphi : A \twoheadrightarrow k$, da die b_i A erzeugen, also nur endlich viele Lösungen des Gleichungssystems.

Beispiel 9.12 (a) Sei k ein Körper. Dann hat

$$A = k[x, y, z]/ < x^2 + y^3, y^4 + z^5 >$$

die Dimension 1, denn

$$\begin{array}{rccc} S = k[y] & \hookrightarrow & A = S[x, z] \\ y & \mapsto & y \end{array}$$

ist offenbar eine Noether-Normalisierung.

(b) Die k-Algebra

$$B = k[x, y, z]/ < x^2 + y^3, y^4 + z^5, z^6 + x^7 >$$

hat die Dimension 0, denn in B gilt

$$x^2 = -y^3 \quad , \quad z^5 = -y^4 \quad , \quad z^6 = -x^7 \,,$$

also

$$y^{48} = z^{60} = x^{70} = -y^{105} \,,$$

d.h.,

$$y^{48}(1 + y^{57}) = 0 \,,$$

Dies liefert einen endlichen Ringhomomorphismus (Definition 9.1)

$$k \to k[y]/ < y^{48}(1 + y^{57}) \rangle \to B$$

(Siehe Corollar 9.3 (b): $A = k[y]/\langle y^{18}(1+y^{37}) \rangle$ ist endlich über k, da von dem ganzen Element y erzeugt, B ist endlich über A, da über A von den ganzen Elementen x und z erzeugt).

Also ist B endlich erzeugter k-Modul, d.h., $\dim_k B < \infty$, d.h., $\dim B = 0$. Tatsächlich erhalten wir z.B. für $k = \mathbb{C}$ die Lösungen des Gleichungssystems

$$\begin{array}{c} x^2 + y^3 = 0 \\ y^4 + z^5 = 0 \\ z^6 + x^7 = 0 \end{array}$$

wie folgt: es muss $y^{48}(1 + y^{57}) = 0$ gelten. Es ist also $y = 0$ oder $y = \zeta$ mit $\zeta^{57} = -1$ (eine 114te Einheitswurzel), und dann $x = z = 0$ (im ersten Fall), oder $x^2 = -\zeta^3$ und $z^5 = -\zeta^4$. Das Gleichungssystem hat also nur endlich viele Lösungen.

10 Der Transzendenzgrad

Erinnerung: Eine Körpererweiterung L/K heißt transzendent, wenn sie nicht algebraisch ist.

Definition 10.1 Sei L/K eine Körpererweiterung.

(a) Eine Familie $(x_1, \ldots, x_n)$ von Elementen aus L heißt **algebraisch unabhängig** (oder **transzendent**) über K, wenn für jedes Polynom $f \in K[X_1, \ldots, X_n]$ mit $f(x_1, \ldots, x_n) = 0$ notwendigerweise $f = 0$ ist, d.h., wenn der Einsetzungshomomorphismus

$$\begin{array}{rcl} K[X_1, \ldots, X_n] & \to & L \\ f(X_1, \ldots, X_n) = \sum c_{\nu_1,\ldots,\nu_n} X_1^{\nu_1} \ldots X_n^{\nu_n} & \mapsto & f(x_1, \ldots, x_n) = \sum c_{\nu_1,\ldots,\nu_n} x_1^{\nu_1} \ldots x_n^{\nu_n} \end{array}$$

injektiv ist (Hier ist $K[X_1, \ldots, X_n]$ der Polynomring in den n Variablen $X_1, \ldots, X_n$).

(b) Eine beliebige Familie $(x_i)_{i \in I}$ von Elementen $x_i \in L$ heißt algebraisch unabhängig (oder transzendent) über K, wenn dies für jede endliche Teilfamilie $(x_{i_1}, \ldots, x_{i_r})$ gilt.

Bemerkungen 10.2 (a) Offenbar ist L/K genau dann transzendent, wenn es ein transzendentes Element $x \in K$ gibt.

(b) 10.1(b) bedeutet ebenfalls, dass der Einsetzungshomomorphismus

$$\begin{array}{rcl} K[X_i \mid i \in I] & \to & L \\ f & \mapsto & f(x_i) \end{array}$$

injektiv ist. Insbesondere erhalten wir dann eine Isomorphie

$$K(X_i \mid i \in I) \xrightarrow{\sim} K(x_i \mid i \in I)\,,$$

wobei $K(X_i \mid i \in I) = Quot(K[X_i \mid i \in I])$ der sogenannte (rationale) **Funktionenkörper in den Variablen** X_i ist und $K(x_i \mid i \in I) \subseteq L$ der von den $x_i\,(i \in I)$ erzeugte Teilkörper von L.

Definition 10.3 Sei L/K eine Körpererweiterung. Eine Familie $(x_i)_{i \in I}$ von Elementen $x_i \in L$ heißt **Transzendenzbasis von L über K**, wenn sie algebraisch unabhängig über K ist und L algebraisch über $K(x_i \mid i \in I)$ ist.

Genauso können wir auch für Teilmengen $\mathcal{X} \subseteq L$ definieren, wann sie algebraisch unabhängig über K sind oder eine Transzendenzbasis von L/K (durch Betrachtung der Familie $(x)_{x \in \mathcal{X}}$).

Sei L/K eine Körpererweiterung.

Lemma 10.4 Sei $\mathcal{X} \subseteq L$ algebraisch unabhängig über K, und sei $x \in L \setminus \mathcal{X}$. Dann ist x genau dann transzendent über $K(\mathcal{X}) := K(x \mid x \in \mathcal{X})$, wenn $\mathcal{X} \dot\cup \{x\}$ algebraisch unabhängig über K ist.

Beweis (1) Sei x transzendent über $K(\mathcal{X})$. Angenommen $\mathcal{X} \dot\cup \{x\}$ ist nicht algebraisch unabhängig über K. Dann gibt es $x_1, \ldots, x_n \in \mathcal{X}$ und ein nicht-triviales Polynom$f \in K[X_1, \ldots, X_{n+1}]$ mit $f(x_1, \ldots, x_n, x) = 0$. Da $(x_1, \ldots, x_n)$ algebraisch unabhängig über K

sind, kommt X_{n+1} in f in nicht-trivialer Potenz vor, und es folgt, dass x algebraisch über $k(x_1, \ldots, x_n)$, also auch über $k(\mathcal{X})$ ist – Widerspruch!

(2) Sei $\mathcal{X} \bigcup \{x\}$ algebraisch unabhängig über K. Angenommen, x ist algebraisch über $K(\mathcal{X})$. Dann gibt es ein nicht-triviales Polynom $f \in K(\mathcal{X})[X]$ mit $f(x) = 0$. Ist

$$f(x) = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0$$

mit $a_i \in K(\mathcal{X})$, so gibt es endlich viele $x_1, \ldots, x_n \in \mathcal{X}$, so dass $a_0, \ldots, a_m \in K(x_1, \ldots, x_n)$. Schreiben wir die a_i als Brüche

$$a_i = \frac{p_i(x_1, \ldots, x_n)}{q_i(x_1, \ldots, x_n)}$$

mit Polynomen $p_i, q_i \in K[X_1, \ldots, X_n], q_i \neq 0$, so erhalten wir durch Multiplikation mit $\prod_i q_i(x_1, \ldots, x_n)$ eine Gleichung

$$b_m(x_1, \ldots, x_n)x^m + \ldots + b_1(x_1, \ldots, x_n)x + b_0(x_1, \ldots, x_n) = 0$$

mit Polynomen $b_i(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, nicht alle gleich null. Dann ist

$$g(X_1, \ldots, X_n, X_{n+1}) = \sum_{i=0}^{m} b_i(X_1, \ldots, X_n) X_{n+1}^i$$

ein nicht-triviales Polynom in $K[X_1, \ldots, X_{n+1}]$ mit $g(x_1, \ldots, x_n, x) = 0$ – Widerspruch zur algebraischen Unabhängigkeit von $\mathcal{X} \bigcup \{x\}$.

Corollar 10.5 Eine Teilmenge $\mathcal{X} \subseteq L$ ist genau dann eine Transzendenzbasis von L/K, wenn sie eine maximale über K algebraisch unabhängige Teilmenge ist.

Beweis Gilt die letztere Bedingung, so ist nach 10.4 jedes $x \in L$ algebraisch über $k(\mathcal{X})$. Ist umgekehrt $\mathcal{X}$ eine Transzendenzbasis von L/K, so gibt es nach 10.4 keine echt größere Teilmenge, die algebraisch unabhängig über K ist.

Corollar 10.6 Jede Körpererweiterung L/K besitzt eine (möglicherweise leere) Transzendenzbasis.

Beweis Ist L/K algebraisch, so ist nichts zu zeigen. Andernfalls ist die Menge $\mathcal{M}$ der über K algebraisch unabhängigen Teilmengen $\mathcal{X} \subseteq L$ nicht leer und induktiv geordnet: Für eine Kette (total geordnete Teilmenge) $\mathcal{N} \subseteq \mathcal{M}$ ist nämlich

$$\bigcup_{\mathcal{X} \in \mathcal{N}} \mathcal{X}$$

algebraisch unabhängig über K, also eine obere Schranke von $\mathcal{N}$ in $\mathcal{M}$. Nach dem Zornschen Lemma besitzt $\mathcal{M}$ also mindestens ein maximales Element; dies ist nach 10.5 eine Transzendenzbasis von L/K.

Sei weiter L/K eine Körpererweiterung.

Proposition 10.7 (Ergänzungssatz) Seien $\mathcal{X}', \mathcal{Y} \subseteq L$ Teilmengen. Ist $\mathcal{X}'$ algebraisch unabhängig über K und L algebraisch über $K(\mathcal{Y})$, so lässt sich $\mathcal{X}'$ durch Hinzunahme von Elementen aus $\mathcal{Y}$ zu einer Transzendenzbasis $\mathcal{X}$ von L/K vergrößern.

Beweis: Wieder mit dem Zornschen Lemma sieht man, dass es eine maximale Teilmenge $\mathcal{X}'' \subseteq \mathcal{Y}$ gibt, für die $\mathcal{X}' \cup \mathcal{X}''$ algebraisch unabhängig über K ist. Nach Lemma 10.4 ist dann jedes Element $y \in \mathcal{Y}$ algebraisch über $K(\mathcal{X} \cup \mathcal{X}'')$. Dann ist $K(\mathcal{Y})$ algebraisch über $K(\mathcal{X}' \cup \mathcal{X}'')$. Nach Voraussetzung gilt dies dann auch für L, und damit ist $\mathcal{X}' \cup \mathcal{X}''$ eine Transzendenzbasis von L/K.

Bemerkungen 10.8 (a) Insbesondere enthält $\mathcal{Y}$ eine Transzendenzbasis für L/K (Fall $\mathcal{X} = \emptyset$).

(b) In 10.7 können wir für $\mathcal{Y}$ ein Erzeugendensystem von L über K nehmen (Fall $K(\mathcal{Y}) = L$).

Beispiel 10.9 Sei $L = \mathbb{R}(x, y \mid x^2 + y^2 = 0)$ der Funktionenkörper der Quadrik $x^2 + y^2 = 0$. Dies ist so zu verstehen: Das Polynom $X^2 + Y^2 \in \mathbb{R}[X, Y]$ ist irreduzibel, denn sonst könnten wir es in zwei Linearfaktoren $(X - \alpha) \cdot (X - \beta)$ mit $\alpha, \beta \in \mathbb{R}[Y]$ aufspalten. (Fasse $\mathbb{R}[X, Y]$ als Polynomring $\mathbb{R}[Y][X]$ auf), was auf $\alpha^2 = -Y^2$ führen würde – Widerspruch. Daher ist

$$A = \mathbb{R}[X, Y]/(X^2 + Y^2)$$

integer, und wir setzen $L = Quot(A)$ (Quotientenkörper von A), wobei wir mit x und y die Bilder von X und Y in A (und L) bezeichnen. Dann ist $\{x, y\}$ ein Erzeugendensystem von L über $\mathbb{R}$ (klar) und sowohl x als auch y liefert eine Transzendenzbasis von $L/\mathbb{R}$: Die Inklusion $\mathbb{R}[X] \hookrightarrow \mathbb{R}[X, Y]$ induziert einen injektiven Ringhomomorphismus von integren Ringen

$$\mathbb{R}[X] \hookrightarrow \mathbb{R}[X, Y]/(X^2 + Y^2) = A\,,$$

da offenbar $\mathbb{R}[X] \cap (X^2 + Y^2) = 0$. Dieser induziert wiederum eine Einbettung

$$\mathbb{R}(X) \hookrightarrow L$$

der Quotientenkörper (warum?) mit Bild $\mathbb{R}(x)$. Also ist x transzendent über $\mathbb{R}$; andererseits ist y wegen der Gleichung $y^2 + x^2 = 0$ algebraisch über $\mathbb{R}(x)$, also auch L. Der Fall von y ist symmetrisch.

Satz 10.10 Zwei Transzendenzbasen $\mathcal{X}, \mathcal{Y}$ einer Körpererweiterung L/K haben diesselbe Mächtigkeit.

Beweis von Satz 10.10 für den Fall, dass $\mathcal{X}$ endlich ist: Sei etwa $\mathcal{X} = \{x_1, \ldots, x_n\}$. Wir zeigen durch Induktion über n, dass $|\mathcal{Y}| \leq n = |\mathcal{X}|$. Durch Symmetrie folgt dann auch $|\mathcal{X}| \leq |\mathcal{Y}|$, also $|\mathcal{X}| = |\mathcal{Y}|$. Für $n = 0$ ist L/K algebraisch, also auch $\mathcal{Y} = \emptyset$. Sei also $n > 0$. Dann ist L/K nicht algebraisch, also $\mathcal{Y} \neq \emptyset$, etwa $y \in \mathcal{Y}$. Nach Proposition 10.7 können wir y durch eine Teilmenge aus $\mathcal{X}$ zu einer Transzendenzbasis $\mathcal{Z}$ von L/K ergänzen. Dann gilt $|\mathcal{Z}| \leq n$, denn sonst wäre $\mathcal{Z} = \{y\} \bigcup \mathcal{X}$, aber $\mathcal{X}$ ist maximal algebraisch unabhängig. Man sieht leicht, dass $\mathcal{Y} \setminus \{y\}$ und $\mathcal{Z} \setminus \{y\}$ beides Transzendenzbasen von $L/K(y)$ sind (ähnliche Schlüsse wie für Lemma 10.4 – Übungsaufgabe!), wobei $|\mathcal{Z} \setminus \{y\}| < n$. Nach Induktionsvoraussetzung ist dann $|\mathcal{Y} \setminus \{y\}| \leq |\mathcal{Z} \setminus \{y\}|$, also $|\mathcal{Y}| \leq |\mathcal{Z}| \leq n$.

Der Fall, wo $\mathcal{X}$ und $\mathcal{Y}$ beide unendlich sind, wird im Anhang 10.A bewiesen.

Definition 10.11 Der **Transzendenzgrad** einer Körpererweiterung L/K wird definiert als

$$tr.\deg(L/K) = |\mathcal{X}|\,,$$

wobei $\mathcal{X}$ eine Transzendenzbasis von L/K ist.

Nach Satz 10.10 hängt diese Mächtigkeit nur von L/K ab.

Beispiel 10.12 Für den Körper $L = \mathbb{R}(x, y \mid x^2+y^2 = 0)$ aus Beispiel 10.9 gilt $tr.\deg(L/\mathbb{R}) = 1$.

Der Transzendenzgrad ist additiv in Körpererweiterungen:

Satz 10.13 Für eine Kette $K \subseteq L \subseteq M$ von Körpererweiterungen gilt

$$tr.deg(M/K) = tr.deg(L/K) + tr.deg(M/L)\,.$$

(Sind die Transzendenzgrade unendlich, so benutzt man die Addition von Kardinalzahlen: $|M| + |N| = |M \cup N|$).

Beweis: Dies folgt leicht mit den oben entwickelten Methoden – Übungsaufgabe! (Tipp: zeigen Sie: Ist $\mathcal{X}$ eine Transzendenzbasis für L/K und $\mathcal{Y}$ eine Transzendenzbasis von M/L, so ist $\mathcal{X} \cap Y = \emptyset$, und $\mathcal{X} \cup Y$ ist eine Transzendenzbasis für M/K).

Wir haben die folgende Beziehung zur Dimensionstheorie von endlich erzeugten k-Algebren in Kapitel 9.

Satz 10.14 Sei k ein Körper und A eine integre endlich erzeugte k-Algebra mit Quotientenkörper $K = Quot(A)$. Dann gilt

$$\dim(A) = tr.deg(K/k)\,.$$

Beweis Sei $\varphi : k[x_1, \ldots, x_d] \hookrightarrow A$ eine Noether-Normalisierung (siehe Satz 9.6). Dann ist $d = \dim(A)$. Andererseits induziert φ eine Inklusion $k(x_1, \ldots, x_d) = Quot(k[x_1, \ldots, x_d]) \subseteq Quot(A) = K$. Da A ganz über $k[x_1, \ldots, x_d]$ ist, ist K ganz, also algebraisch, über $k(x_1, \ldots, x_d)$. Es folgt $tr.deg_k(K) = d$, da $x_1, \ldots, x_d$ algebraisch unabhängig über k sind.

10.A Anhang: Beweis von Satz 10.10 im allgemeinen Fall

Der Fall, wo $\mathcal{X}$ und $\mathcal{Y}$ beide unendlich sind, brauchen wir für den Beweis von Satz 10.10 einige mengentheoretische Vorbereitungen.

Satz 10.A.1 (Schröder-Bernstein) Seien M und N Mengen. Gibt es Injektionen $\sigma : M \hookrightarrow N$ und $\tau : N \hookrightarrow M$, so existiert eine Bijektion $\rho : M \to N$, d.h., M und N sind gleichmächtig ($|M| = |N|$).

Beweis: Sei $M' \subseteq M$ die Menge aller Elemente $x \in M$, so dass für alle $b \in \mathbb{N}_0$ gilt

$$x \in (\tau\sigma)^n(M) \Rightarrow x \in (\tau\sigma)^n\tau(N)$$

(mit $(\tau\sigma)^0 = id$). Ein $x \in M$ gehört also genau dann zu M', wenn eine fortwährende Bildung von Urbildern (eindeutig falls existent!)

$$\begin{array}{cccccc} x, & \tau^{-1}(x), & \sigma^{-1}\tau^{-1}(x), & \tau^{-1}\sigma^{-1}\tau^{-1}(x), & \ldots \\ \cap & \cap & \cap & \cap & \\ M & N & M & N & \end{array}$$

entweder unendlich oft möglich ist oder bei einem Element aus N (nach einer ungeraden Anzahl von Schritten) endet. Erkläre nun $\rho : M \to N$ durch

$$\rho(x) = \begin{cases} \tau^{-1}(x) & , \quad x \in M', \\ \sigma(x) & , \quad x \notin M'. \end{cases}$$

Dann ist ρ injektiv: Die Einschränkungen $\rho_{|M'}$ und $\rho_{|M \smallsetminus M'}$ sind injektiv, und für $x \in M'$ und $y \in M \smallsetminus M'$ mit $\rho(x) = \rho(y)$ folgt $\sigma(y) = \tau^{-1}(x)$, d.h., $\tau\sigma(y) = x$ und damit $y \in M'$ – Widerspruch! Weiter ist ρ surjektiv: Sei $z \in N$ und $x = \tau(z)$. Für $x \in M'$ gilt dann $\rho(x) = \tau^{-1}(x) = z$. Für $x \notin M'$ besitzt $z \in N$ ein Urbild $y = \sigma^{-1}(z) = \sigma^{-1}\tau^{-1}(z)$, da sonst $x \in M'$ nach Definition von M'. Wegen $x \notin M'$ gilt auch $y \notin M'$ und daher, nach Definition, $\rho(y) = \sigma(y) = z$.

Für Mengen M und N schreibe $|M| \leq |N|$ wenn, es eine Injektion $M \hookrightarrow N$ gibt. Der obige Satz lautet damit: $|M| \leq |N|$ und $|N| \leq |M| \Rightarrow |M| = |N|$.

Bemerkungen 10.A.2 Unter Benutzung des Auswahlaxioms ($\Leftrightarrow$ Zornsches Lemma) folgt

$$|M| \leq |N| \Leftrightarrow \text{ Es gibt eine Surjektion } f : N \to M\,.$$

Sei nämlich $f : N \twoheadrightarrow M$ eine Surjektion, so gibt es nach dem Auswahlaxiom einen Schnitt $s : M \to N$ von f ($f \circ s = id_M$), und s ist notwendigerweise injektiv. Ist umgekehrt $i : M \hookrightarrow N$ eine Injektion und $\overline{M} = N \smallsetminus i(M)$, $M \neq \emptyset$ (sonst ist nichts zu zeigen), so wähle $m \in M$ und definiere eine Surjektion $f : N \to M$ durch

$$f(n) = \begin{cases} i^{-1}(n) & , \quad n \in i(M), \\ m & , \quad \text{sonst}\,. \end{cases}$$

Lemma 10.A.3 Ist $(M_i)_{i\in I}$ eine Familie von *endlichen* Mengen und ist die Indexmenge *unendlich*, so gilt für die disjunkte Vereinigung $\coprod_{i\in I} M_i$

$$|\coprod_{i\in I} M_i| = |I|\,.$$

Beweis: Ist I abzählbar unendlich, so ist dies klar (durch einfaches "Abzählen"). Im Allgemeinen betrachte die Menge $\mathcal{P}$ aller Paare

$$P = (I_P, f_P)$$

wobei $I_P \subseteq I$ eine unendliche Teilmenge ist und $f : \coprod_{i\in I_P} M_i \to I_P$ eine Bijektion. Dann ist $\mathcal{P}$ nicht leer, denn I enthält eine abzählbar unendliche Teilmenge I' und nach der Vorbemerkung gibt es ein Paar $(I', f) \in \mathcal{P}$. Definiere eine Ordnung $\leq$ auf P durch

$$P \leq P' \text{ wenn } I_P \subseteq I_{P'} \text{ und } f_P = f_{P'} \mid \coprod_{i\in I_P} M_i$$

(insbesondere gilt dann $f_{P'}(\coprod_{i\in I_P} M_i) = I_P$!). Diese Ordnung ist induktiv, denn für eine Kette $(P_\alpha)_{\alpha\in A}$ mit $P_\alpha = (I_\alpha, f_\alpha) \in \mathcal{P}$ definiere $P = (I_P, f_P) \in \mathcal{P}$ durch

$$\begin{aligned} I_P &= \bigcup_{\alpha\in A} I_\alpha \\ f_P &: \coprod_{i\in I_P} M_i \to I_P\,,\ f_P \mid \coprod_{i\in I_\alpha} M_i = f_\alpha\,. \end{aligned}$$

Dann ist P wohldefiniert und eine obere Schranke für die Kette. Nach dem Zornschen Lemma besitzt $\mathcal{P}$ also ein maximales Element (I_0, f_0). Für dieses ist aber $I \smallsetminus I_0$ endlich, denn sonst können wir eine abzählbare Menge $I_1 \subseteq I \smallsetminus I_0$ und eine Bijektion $f_1 : \coprod_{i\in I_1} M_i \to I_1$ finden. Dann ist aber $(I_0 \bigcup I_1, f) \in \mathcal{P}$ mit

$$f_{|\coprod_{i\in I_0} M_i} = f_0\ ,\ f_{|\coprod_{i\in I_1} M_i} = f_1,$$

im Widerspruch zur Maximalität von (I_0, f_0). Es bleibt zu zeigen:

Behauptung: Ist M eine unendliche Menge und N eine endliche Menge, so gilt $|M| = |M \coprod N|$.

Damit folgt dann nämlich wegen der Endlichkeit von $I \smallsetminus I_0$

$$|\coprod_{i\in I} M_i| = |\coprod_{i\in I_0} M_i| = |I_0| = |I|\,.$$

Beweis der Behauptung: Die Behauptung ist klar falls M abzählbar unendlich ist. Im Allgemeinen sei $J \subseteq M$ eine abzählbar unendliche Teilmenge und $f : J \to J \coprod N$ eine Bijektion. Dann erhalten wir eine offensichtliche Bijektion $g : M \to M \coprod N$ durch

$$g(x) = \begin{cases} x & ,\ x \notin J, \\ f(x) & ,\ x \in J\,. \end{cases}$$

Beweis von Satz 10.10 für den Fall, dass $\mathcal{X}$ und $\mathcal{Y}$ unendlich sind: Seien $\mathcal{X}$ und $\mathcal{Y}$ zwei unendliche Transzendenzbasen von L/K. Jedes $x \in \mathcal{X}$ ist algebraisch über $K(\mathcal{Y})$. Es gibt also zu x eine endliche Teilmenge $\mathcal{Y}_x \subseteq \mathcal{Y}$, so dass x algebraisch über $K(\mathcal{Y}_x)$ ist. Da L für eine echte Teilmenge $\mathcal{Y}' \subsetneq \mathcal{Y}$ nicht algebraisch über $K(\mathcal{Y}')$ sein kann (Corollar 10.5), ist $\bigcup_{x\in\mathcal{X}} \mathcal{Y}_x = \mathcal{Y}$. Die Inklusionen $\mathcal{Y}_x \hookrightarrow \mathcal{Y}$ definieren daher eine surjektive Abbildung

$$\coprod_{x\in\mathcal{X}} \mathcal{Y}_x \twoheadrightarrow \mathcal{Y}\,.$$

Mit Bemerkung 10.14 und Lemma 10.15 folgt

$$|\mathcal{Y}| \leq |\coprod_{x\in\mathcal{X}} \mathcal{Y}_x| = |\mathcal{X}|\,.$$

Aus Symmetriegründen gilt auch $|\mathcal{X}| \leq |\mathcal{Y}|$, und aus Satz 10.A.1 folgt $|\mathcal{X}| = |\mathcal{Y}|$ q.e.d.

11 Homologische Algebra für Moduln

Dieses Kapitel kann als eine Fortführung des Kapitels 2 über Komplexe von Moduln angesehen werden. Sei R ein nicht notwendig kommutativer Ring mit Eins. Wir betrachten ohne Einschränkung Links-Moduln über R (Rechts-Moduln sind Links-Moduln über dem Opposit-Ring R^* mit der Multiplikation $a * b := ba$).

Für R-Linksmoduln M, N ist $Hom_R(M, N)$ im Allgemeinen nur eine abelsche Gruppe; ist R kommutativ, so ist $Hom_R(M, N)$ auch ein R-Modul (siehe Lemma 5.3).

Proposition 11.1 (a) Für jeden R-Modul M ist der kovariante Funktor $Hom_R(M; -)$ **linksexakt**, d.h., ist

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

eine exakte Sequenz von R-Moduln, so ist

$$0 \to Hom_R(M, A) \xrightarrow{i_*} Hom_R(M, B) \xrightarrow{p_*} Hom_R(M, C) \tag{1}$$

exakt.

(b) Für jeden R-Modul N ist der kontravariante Funktor $Hom_R(-, N)$ **linksexakt**, d.h., ist

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

eine exakte Sequenz von R-Moduln, so ist

$$0 \to Hom_R(C, N) \xrightarrow{p^*} Hom_R(B, N) \xrightarrow{i^*} Hom_R(A, N) \tag{2}$$

exakt.

Beweis (a): Es ist klar, dass (1) ein Komplex ist: Da $pi = 0$, gilt $p_*i_* = (pi)_* = 0_* = 0$. Da i injektiv ist, also ein Monomorphismus, ist i_* auch injektiv (siehe 7.4 (b)). Die Exaktheit bei $Hom_R(M, B)$ folgt nun aus der Tatsache, dass A sich mit dem Kern von p identifiziert: Ist $f \in Hom_B(M, B)$ mit $p_*(f) = pf = 0$, so hat f Bild in $\ker(p) = im(i)$, also $f(m) = i(a)$ für ein eindeutig bestimmtes Element $a \in A$, und wir erhalten so ein $g : M \to A$ ($m \mapsto a$ mit $i(a) = f(m)$) mit $f = ig = i_*(g)$.

(b): Dies wird analog gezeigt, indem man benutzt, dass sich C mit dem Kokern von i identifiziert.

Lemma/Definition 11.2 Ein R-Modul P heißt **projektiv**, wenn die folgenden äquivalenten Bedingungen gelten.

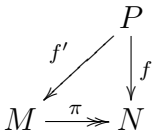
(a) Der Funktor $Hom_R(P, -)$ ist exakt, d.h., überführt exakte Sequenzen in exakte Sequenzen.

(b) Jeder Epimorphismus $M \overset{\pi}{\twoheadrightarrow} P$ besitzt einen Schnitt, d.h., einen Homomorphismus $\iota : P \to M$ mit $\pi\iota = id_P$.

(c) Für jedes Diagramm von R-Modul-Homomorphismen

$$\begin{array}{ccc} & & P \\ & & \downarrow f \\ M & \xrightarrow{\pi} & N \end{array}$$

mit einem Epimorphismus π gibt es einen Homomorphismus $f' : P \to M$, der das Diagramm



kommutativ macht (man sagt auch, dass f' ein Lift von f zu M ist).

Beweis der Äquivalenzen:

(a) $\Leftrightarrow$ (c): Die Bedingung (c) besagt gerade, dass

$$\begin{array}{rcl} Hom_R(P,M) & \stackrel{\pi_*}{\to} & Hom_R(P,N) \\ f' & \mapsto & f = \pi f' \end{array}$$

surjektiv ist. Für eine exakte Sequenz wie in 11.1 (a) erhalten wir also eine exakte Sequenz

$$0 \to Hom_R(P,A) \to Hom_R(P,B) \to Hom_R(P,C) \to 0\,.$$

Hieraus folgt leicht, dass der Funktor $F = Hom_R(P,-)$ beliebige exakte Sequenzen von R-Moduln in exakte Sequenzen überführt: Ist nämlich

$$\ldots \to M^{n-1} \stackrel{d^{n-1}}{\to} M^n \stackrel{d^n}{\to} M^{n+1} \to \ldots$$

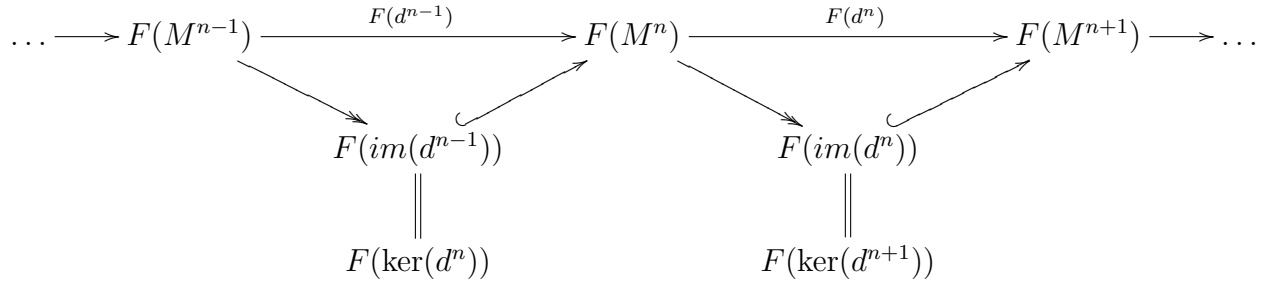
eine beliebige exakte Sequenz von R-Moduln, so haben wir lauter kurze exakte Sequenzen

$$0 \to im(d^{n-1}) \to M^n \to im(d^n) \to 0$$

mit $im(d^{n-1}) = \ker(d^n)$ für alle n. Hieraus erhält man exakte Sequenzen

$$0 \to F(im(d^{n-1})) \to F(M^n) \to F(im(d^n)) \to 0$$

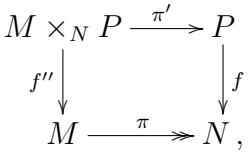
für alle n, und damit ein kommutatives Diagramm



in dem die obige Sequenz nun offenbar exakt ist.

(c) $\Rightarrow$ (b) ist trivial: Wende (a) auf $f = id_P$ an.

(b) $\Rightarrow$ (c): betrachte für (c) das kommutative Diagramm



wobei

$$M \times_N P = \{(m,p) \in M \times P \mid \pi(m) = f(p)\}$$

das sogenannte Faserprodukt von M und P über N ist. Dies ist offenbar ein Untermodul von $M \times P$. Da π surjektiv ist, ist auch π' surjektiv, wie man leicht sieht. Gilt nun (b), so besitzt π' einen Schnitt $\iota' : P \to M \times_N P$ mit $\pi'\iota' = id_P$. Dann gilt mit $f' = f''\iota'$:

$$\pi f' = \pi f''i' = f\pi'i' = f\,,$$

also (a).

Analog hat man

Lemma/Definition 11.3 Ein R-Modul I heißt **injektiv**, wenn die folgenden äquivalenten Bedingungen gelten.

(a) Der Funktor $Hom_R(-, I)$ ist exakt.

(b) Jeder Monomorphismus $I \overset{\iota}{\hookrightarrow} M$ besitzt eine Retraktion, d.h., einen Morphismus $r : M \to N$ mit $r\iota = id_I$.

(c) Für jedes Diagramm von R-Moduln

$$\begin{array}{ccc} & & I \\ & & \uparrow{\scriptstyle g} \\ M & \overset{\iota}{\hookrightarrow} & N \end{array}$$

mit einem Monomorphismus ι gibt es einen Morphismus $g' : N \to I$, der

$$\begin{array}{ccc} & & I \\ & \nwarrow^{g'} & \uparrow{\scriptstyle g} \\ M & \overset{\iota}{\hookrightarrow} & N \end{array}$$

kommutativ macht.

Wir untersuchen nun die Existenz von projektiven und injektiven Moduln.

Satz 11.4 (a) Jeder freie Modul ist projektiv.

(b) Ein Modul ist genau dann projektiv, wenn er direkter Faktor eines freien Moduls ist.

Beweis (a) Sei $F = F_R(I)$ der freie Modul über der Menge I, und sei

$$\begin{array}{ccc} & & F \\ & & \downarrow{\scriptstyle f} \\ M & \overset{\pi}{\twoheadrightarrow} & N \end{array}$$

gegeben, mit surjektivem π. Sei $(e_i)_{i\in I}$ die Basis von F, und sei $n_i = f(e_i) \in N$. Sei $m_i \in M$ ein Urbild von n_i unter π für alle i (existiert, da π surjektiv ist). Dann können wir für $f' : F \to M$ den Homomorphismus nehmen, der $e_i \in F$ auf $m_i \in M$ abbildet (existiert in eindeutiger Weise und macht offenbar das Diagramm kommutativ).

(b) Ist P projektiv, so gibt es durch eine Wahl von Erzeugenden $(p_i)_{i\in I}$ einen Epimorphismus

$$\begin{array}{rcl} \pi : F(I) & \twoheadrightarrow & P \\ e_i & \mapsto & p_i\,. \end{array}$$

Da P projektiv ist, existiert nach 11.2 (b) ein Schnitt $\iota : P \to F(I)$ von π, also mit $\pi\iota = id_p$. Dies bedeutet aber, dass P ein direkter Faktor von $F(I)$ ist (siehe Übungsblatt 2, Aufgabe 4).

Satz 11.5 Sei R ein Ring mit Eins (nicht notwendig kommutativ) und sei Mod_R die Kategorie der R-Linksmoduln.

(a) Für jeden Modul M in Mod_R gibt es einen Epimorphismus

$$P \twoheadrightarrow M$$

mit einem projektiven R-Modul P (Man sagt auch Mod_R besitzt genügend viele Projektive).

(b) Für jeden Modul M in Mod_R gibt es einen Monomorphismus

$$M \hookrightarrow I$$

mit einem injektiven R-Modul I (Man sagt auch Mod_R besitzt genügend viele Injektive).

Beweis: (a) Die Existenz von genügend vielen Projektiven ist nach Satz 11.4 (a) klar, da jeder R-Modul M eine Surjektion $F \twoheadrightarrow M$ mit einem freien R-Modul F besitzt.

(b) Die Existenz von genügend vielen Injektiven erfordert mehr Vorarbeit.

Satz 11.6 (Kriterium von Baer) Ein R-Modul M ist genau dann injektiv, wenn für jedes Ideal $\mathfrak{a} \subseteq R$ und jeden R-Modul-Homomorphismus $\mathfrak{a} \to M$ eine Erweiterung $R \to M$ existiert.

Beweis Es gelte die Bedingung, und es sei

$$\begin{array}{ccc} & & M \\ & & \uparrow{\scriptstyle f} \\ N & \overset{g}{\hookrightarrow} & N' \end{array}$$

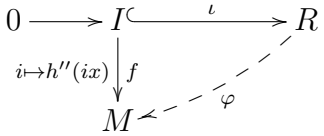
ein Diagramm von Moduln mit injektivem g. Wir suchen einen R-Modul-Homomorphismus $h : N' \to M$ mit $hg = f$. Betrachte die Menge $\mathcal{N}$ der Paare (N'', h) mit $N \hookrightarrow N'' \hookrightarrow N'$ und $h : N'' \to M$ welches f fortsetzt. Definiere eine Ordnung auf $\mathcal{N}$ durch

$$(N_1, h_1) \leq (N_2, h_2) \quad :\Leftrightarrow \quad N_1 \subseteq N_2 \text{ und } h_1 = h_2|_{N_1}\,.$$

Dann hat jede nicht-leere Kette in $\mathcal{N}$ eine obere Schranke, gegeben durch die Vereinigung V der Teilmengen N_i und $h : V \to M$ mit $h|_{N_i} = h_i$. Nach dem Lemma von Zorn gibt es also ein maximales Element (N'', h'') in $\mathcal{N}$. Wir behaupten, dass $N'' = N'$. Sei nämlich $N'' \subsetneqq N'$ und $x \in N' \smallsetminus N''$. Sei dann

$$I = \{r \in R \mid rx \in N''\}\,.$$

Dies ist ein Ideal von R. Betrachte das Diagramm (zunächst ohne φ)



Für $i \in I$ ist $ix \in N''$ und deswegen $h''(ix)$ definiert, weiter ist f R-linear. Nach Annahme erhalten wir also einen R-Modul-Homomorphismus $\varphi : R \to M$ mit $\varphi\iota = f$. Wir behaupten, dass sich $g : N \to M$ auf $Rx + N''$ fortsetzen lässt, was einen Widerspruch zur Maximalität von N'' gibt, da $x \notin N''$.

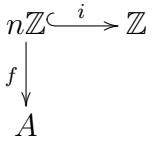
Hierzu definieren wir

$$\begin{array}{rccc} \varphi' : & Rx + N'' & \to & M \\ & rx + n'' & \mapsto & r\varphi(1) + h(n'') \end{array}$$

für $r \in R$ und $n'' \in N''$. Dies ist wohldefiniert: Ist nämlich $rx = n \in Rx \cap N''$, mit $r \in R$ und $n \in N''$, so ist $r\varphi(1) = \varphi(r) = h''(rx)$.

Lemma 11.7 Die Kategorie $\underline{Ab}$ aller abelschen Gruppen besitzt genügend viele Injektive.

Beweis (1) Jede divisible Gruppe ist injektiv: Wir benutzen Baer's Kriterium für $\underline{Ab} = \underline{Mod}_{\mathbb{Z}}$. Sei $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal und

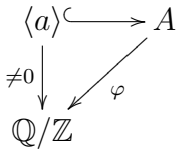


gegeben. Sei $f(n) = a$. Da A divisibel ist, gibt es ein $b \in A$ mit $a = n \cdot b$. Definiere nun $g : \mathbb{Z} \to A$ durch $g(1) = b$; dann ist $gi = f$.

(2) Sei A ein $\mathbb{Z}$-Modul; dann gibt es einen Monomorphismus $A \hookrightarrow I$ mit I injektiv: Für jeden $\mathbb{Z}$-Modul B setze $B^\vee = Hom(B, \mathbb{Q}/\mathbb{Z})$. Dann haben wir einen natürlichen Homomorphismus

$$\begin{array}{rccc} \psi : & A & \to & A^{\vee\vee} \\ & a & \mapsto & (\varphi \mapsto \varphi(a)) \,. \end{array}$$

i) ψ ist injektiv: Sei $0 \neq a \in A$, und sei $\langle a \rangle$ die von a erzeugte zyklische Untergruppe. Dann gibt es eine natürliche Zahl $n > 0$ und einen nicht-trivialen Homomorphismus $\langle a \rangle \to \mathbb{Q}/\mathbb{Z}$ (Hat a unendliche Ordnung, also $\langle a \rangle = \mathbb{Z}$, so bilde a auf irgendein Element $0 \neq b \in \mathbb{Q}/\mathbb{Z}$ ab; ist $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}, n > 0$, so bilde a auf $\frac{1}{n} \mod \mathbb{Z}$ ab). Nach Voraussetzung finden wir ein kommutatives Diagramm



also ein $\varphi \in A^\vee$ mit $\varphi(a) \neq 0$.

ii) Sei

$$\bigoplus_{j \in J} \mathbb{Z} \to A^\vee$$

eine Surjektion (von $\mathbb{Z}$-Moduln). Dann erhalten wir eine Einbettung

$$A^{\vee\vee} = Hom(A^{\vee}, \mathbb{Q}/\mathbb{Z}) \hookrightarrow Hom(\bigoplus_{j\in J} \mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong (\mathbb{Q}/\mathbb{Z})^J .$$

Nach (1) ist $(\mathbb{Q}/J)^J$ injektiver Modul, und wir haben die Injektion

$$A \overset{\psi}{\hookrightarrow} A^{\vee\vee} \hookrightarrow (\mathbb{Q}/\mathbb{Z})^J .$$

Lemma 11.8 Sei A ein kommutativer Ring mit Eins und sei B eine A-Algebra mit Eins. Sei I ein injektiver A-Modul und P ein projektiver B-Modul. Dann ist $Hom_A(P, I)$ ein injektiver B-Modul (Dies gilt auch für einen nicht-kommutativen Ring B; für B-Linksmoduln sei dabei P ein B-Rechtsmodul, so dass $Hom_A(P, I)$ ein B-Linksmodul wird; entsprechend für B-Rechtsmoduln).

Beweis Wir haben zu zeigen, dass $Hom_B(-, Hom_A(P, I))$ exakt ist. Es gilt aber

$$Hom_B(-, Hom_A(P, I)) \cong Hom_A(P \otimes_B -; I)$$

nach der universellen Eigenschaft des Tensorprodukts. Aber $P\otimes_B -$ ist exakt, da P projektiv ist, und $Hom_A(-, I)$ ist exakt, da I injektiv ist. Daher ist die Komposition $Hom_A(P\otimes_B -, I)$ exakt.

Beweis von Satz 11.5 für Injektive: Sei M ein R-Modul. Dann ist M auch ein $\mathbb{Z}$-Modul, und nach Satz 11.7 gibt es einen injektiven $\mathbb{Z}$-Modul I_1 und einen Monomorphismus $\varphi_1 : M \hookrightarrow I_1$. Nach Lemma 11.8 ist der R-Modul $Hom_{\mathbb{Z}}(R, I_1)$ injektiv. Weiter ist die folgende Abbildung

$$\begin{array}{rccc} \varphi: & M & \to & Hom_{\mathbb{Z}}(R, I_1) \\ & m & \mapsto & (r \mapsto \varphi_1(rm)) \end{array}$$

R-linear. Schließlich ist φ injektiv: Ist $\varphi(m) = 0$, so ist $\varphi_1(m) = 0$, also $m = 0$, da φ_1 injektiv ist.

Wir kommen jetzt zur eigentlichen homologischen Algebra.

Definition 11.9 Sei M ein R-Modul.

(a) Eine **projektive Auflösung** von M ist eine exakte Sequenz

$$\ldots \to P_2 \to P_1 \to P_0 \to M \to 0$$

mit projektiven R-Moduln P_i.

(b) Eine **injektive Auflösung** von M ist eine exakte Sequenz

$$0 \to M \to I^0 \to I^1 \to I^2 \to \ldots$$

mit injektiven R-Moduln I^j.

Aus 11.5. erhalten wir:

Proposition 11.10 (a) Jeder R-Modul besitzt eine projektive Auflösung.

(b) Jeder R-Modul besitzt eine injektive Auflösung.

Beweis (a): Sei M ein R-Modul. Wir konstruieren die Sequenz induktiv. Sei

$$P_0 \twoheadrightarrow M$$

ein Epimorphismus mit projektivem P_0. Dann ist

$$P_0 \to M \to 0$$

exakt. Ist nun bereits eine exakte Sequenz

$$P_n \xrightarrow{d_n} P_{n-1} \to \ldots \to P_0 \to M \to 0$$

mit projektivem P_i konstruiert, so sei $K_n = \ker(d_n) \subseteq P_n$. Wählen wir einen Epimorphismus $P_{n+1} \twoheadrightarrow K_n$ mit projektivem P_{n+1}, so ist mit $d_{n+1} \twoheadrightarrow K_n \hookrightarrow P_n$ die Sequenz

$$P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_1} P_0 \to M \to 0$$

exakt, wegen $im(d_{n+1}) = K_n = \ker(d_n)$.

(b): Der Beweis ist analog (dual).

Die oben konstruierten Komplexe

$$P_\cdot: \quad \ldots \to P_n \to P_{n-1} \to \ldots \to P_0$$

$$I_\cdot: \quad I^0 \to I^1 \to \ldots \to I^n \to \ldots$$

sind natürlich nicht eindeutig. Aber sie sind eindeutig bis auf Homotopie:

Definition 11.11 (a) Ein Morphismus

$$f = (f^n) : (C^n, d_C^n) \to (D^n, d_D^n)$$

von Komplexen von R-Moduln heißt nullhomotop (Bez. $f \sim 0$), wenn es eine Familie (k^n) von Morphismen $k^n : C^n \to D^{n-1}$ gibt mit

$$f^n = d^{n-1}k^n + k^{n+1}d^n$$

für alle $n \in \mathbb{Z}$:

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & D^{n-1} & \xrightarrow{d_D^{n-1}} & D^n & \xrightarrow{d_D^n} & D^{n+1} & \longrightarrow & \ldots \\
 & & \uparrow{\scriptstyle f^{n-1}} & \nwarrow{\scriptstyle k^n} & \uparrow{\scriptstyle f^n} & \nwarrow{\scriptstyle k^{n+1}} & \uparrow{\scriptstyle f^{n+1}} & & \\
\ldots & \longrightarrow & C^{n-1} & \xrightarrow{d_C^{n-1}} & C^n & \xrightarrow{d_D^n} & C^{n+1} & \longrightarrow & \ldots
\end{array}$$

(b) Zwei Morphismen $f, g : C^\cdot \to D^\cdot$ heißen homotop (Bez. $f \sim g$), wenn $f - g$ nullhomotop ist.

Es sei daran erinnert, dass ein Morphismus von Komplexen $f : C^\cdot \to D^\cdot$ Homomorphismen

$$f_* = H^n(f) : H^n(C^\cdot) \to H^n(D^\cdot)$$

für alle n induziert (siehe Lemma 2.23).

Genauer erhalten wir einen Funktor

$$\begin{array}{rcl} ((\text{Komplexe von } R\text{-Moduln}) & \stackrel{H^n}{\to} & Mod_R \\ C^{\cdot} & \mapsto & H^n(C^{\cdot}) \\ f : C^{\cdot} \to D^{\cdot} & \mapsto & H^n(f) : H^n(C^{\cdot}) \to H^n(D^{\cdot}) \,, \end{array}$$

den n-ten Kohomologiefunktor (Beweis: Übungsaufgabe!)

Homotope Morphismen induzieren *denselben* Morphismus in der Homologie:

Lemma 11.12 Ist $f \sim g : C^{\cdot} \to D^{\cdot}$, so ist $H^n(f) = H^n(g) : H^n(C^{\cdot}) \to H^n(D^{\cdot})$ für alle $n \in \mathbb{Z}$.

Beweis Es genügt zu zeigen:

$$f \sim 0 \quad \Rightarrow \quad H^n(f) = 0 \,.$$

Sei (k^n) wie in der Definition,

$$d_D^{n-1} k^n + k^{n+1} d_C^n = f^n \,.$$

Dann ist $f|_{\ker(d_C^n)} = d_C^{n-1} k^n$, hat also Bild in $im(d_D^{n-1})$, und die Behauptung folgt.

$$\begin{array}{ccc} & & im(d_D^{n-1}) \\ & \nearrow & \downarrow \\ \ker(d_C^n) & \xrightarrow{f^n} & \ker(d_D^n) \\ \downarrow & & \downarrow \\ H^n(C^{\cdot}) & \xrightarrow{H^n(f)} & H^n(D^{\cdot}) \,. \end{array}$$

Lemma 11.13 (a) Homotopie ist eine Äquivalenzrelation.

(b) Gilt $f \sim g$ und $f' \sim g'$ in $Hom(C^{\cdot}, D^{\cdot})$, so ist $f + f' \sim g + g'$.

(c) Gilt $f \sim g$ in $Hom(C^{\cdot}, D^{\cdot})$, so gilt $hf \sim hg$ und $fk \sim gk$ für $h \in Hom(D^{\cdot}, C^{\cdot})$ und $k \in Hom(D^{\cdot}, C^{\cdot})$.

Beweis selbst!

Definition 11.14 Ein Morphismus $f : C^{\cdot} \to D^{\cdot}$ von Komplexen heißt Quasiisomorphismus, wenn f Isomorphismen

$$H^n(f) : H^n(C^{\cdot}) \to H^n(D^{\cdot})$$

für alle n induziert.

Definition 11.15 Ein Morphismus $f : C^{\cdot} \to D^{\cdot}$ von Komplexen heißt **Homotopieäquivalenz**, wenn es einen Morphismus $g : D^{\cdot} \to C^{\cdot}$ gibt mit $gf \sim id_{C^{\cdot}}$ und $fg \sim id_{D^{\cdot}}$.

Corollar 11.16 Eine Homotopieäquivalenz ist ein Quasiisomorphismus.

Beweis In der Situation von 11.15 ist nach 11.12 $H^n(g)H^n(f) = H^n(id_{C^\cdot}) = id_{H^n(C^\cdot)}$ und entsprechend $H^n(f)H^n(g) = id_{H^n(D^\cdot)}$, also sind $H^n(f)$ und $H^n(g)$ zueinander inverse Isomorphismen.

Satz 11.17 Sei $f : M \to N$ ein Modulhomomorphismus.

(a) Sind $P_\cdot \to M$ und $Q_\cdot \to N$ projektive Auflösungen, so gibt es einen Homomorphismus von Komplexen $f_\cdot : P_\cdot \to Q_\cdot$, der das Diagramm

$$\begin{array}{ccc} P_\cdot & \longrightarrow & M \\ {\scriptstyle f_\cdot}\downarrow & & \downarrow{\scriptstyle f} \\ Q_\cdot & \longrightarrow & N \end{array}$$

kommutativ macht. Die Homotopieklasse $[f_\cdot]$ von $f_\cdot$ ist dabei eindeutig bestimmt.

(b) Sind $M \to I^\cdot$ und $N \to J^\cdot$ injektive Auflösungen, so gibt es einen Morphismus von Komplexen $f^\cdot : I^\cdot \to J^\cdot$, der das Diagramm

$$\begin{array}{ccc} N & \longrightarrow & I^\cdot \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle f^\cdot} \\ M & \longrightarrow & J^\cdot \end{array}$$

kommutativ macht. Die Homotopieklasse $[f^\cdot]$ von $f^\cdot$ ist dabei eindeutig bestimmt.

Beweis (a) (Der Beweis von 11.17 (b) ist analog/dual) Wir haben ein Diagramm

$$\begin{array}{ccc} P_0 & \xrightarrow{\alpha} & M \\ & & \downarrow{\scriptstyle f} \\ Q_0 & \xrightarrow{\beta} & N \end{array}$$

mit surjektiven Morphismen α und β. Nach der Eigenschaft von Projektiven, und wegen der Surjektivität von β, gibt es einen Morphismus $f_0 : P_0 \to Q_0$ mit $\beta f_0 = f\alpha$, so dass also

$$\begin{array}{ccc} P_0 & \xrightarrow{\alpha} & M \\ {\scriptstyle f_0}\downarrow & & \downarrow{\scriptstyle f} \\ Q_0 & \xrightarrow{\beta} & N \end{array}$$

kommutativ ist. Wir gehen nun induktiv vor. Angenommen, es existiert bereits ein kommutatives Diagramm

$$\begin{array}{ccccccccccc} P_n & \xrightarrow{d_n^P} & P_{n-1} & \longrightarrow & \cdots & \longrightarrow & P_0 & \xrightarrow{\alpha} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow & & \downarrow{\scriptstyle f_0} & & \downarrow & & \\ Q_n & \xrightarrow{d_n^Q} & Q_{n-1} & \longrightarrow & \cdots & \longrightarrow & Q_0 & \xrightarrow{\beta} & N & \longrightarrow & 0 \end{array}$$

(also Morphismus von Komplexen), und sei

$$\tilde{f}_n : K_n = \ker(d_n^P) \to \ker(d_n^Q) = L_n$$

der induzierte Morphismus. Dann erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccccc} P_{n+1} & \twoheadrightarrow & K_n & \hookrightarrow & P_n \\ & & (*)\downarrow \tilde{f}_n & & \downarrow f_n \\ Q_{n+1} & \twoheadrightarrow & L_n & \hookrightarrow & Q_n\,. \end{array}$$

Mit demselben Argument wie oben existiert dann ein Morphismus $f_{n+1} : P_{n+1} \to Q_{n+1}$ der das Quadrat $(*)$ kommutativ ergänzt, was der Induktionsschritt liefert.

Wir zeigen nun, dass $f^{\cdot}$ bis auf Homotopie eindeutig ist. Dafür genügt es zu zeigen:

$$f = 0 \quad \Rightarrow \quad f^{\cdot} \sim 0\,.$$

Im ersten Schritt erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccccccc} & & & & P_0 & \xrightarrow{\alpha} & M \\ & & & \swarrow^{k_0} & \downarrow f_0 & & \downarrow f=0 \\ Q_1 & \xrightarrow{\pi_0} & L_0 & \xrightarrow[i_0]{\tilde{f}_0} & Q_0 & \xrightarrow{\beta} & N \end{array}$$

mit $L_0 = \ker(\beta)$ und $d_1^Q = i_0\pi_0$: Wegen $0 = f\alpha = \beta f_0$ ist $im(f_0) \subseteq L_0$, d.h., f_0 funktioniert mittels $\tilde{f}_0$ über L_0. Wegen der Projektivität von P_0 gibt es den Lift k_0 von $\tilde{f}_0$ zu Q_1.

Setze nun $P_{-1} = 0$, $Q_{-1} = 0$ und $k_{-1} = 0 : P_{-1} \to N_0$. Dann ist

$$f_0 = d_1^Q k_0 + k_{-1} d_0^P\,.$$

Seien nur bereits $k_i : P_i \to Q_{i+1}$ konstruiert, $i = -1, \ldots, n-1$, mit

$$f_i = d_{i+1}^Q k_{i-1} d_i^P\,.$$

Dann erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccccccc} & & & & P_n & \xrightarrow{d_n^P} & P_{n-1} \\ & & & \swarrow^{k_n} \quad \swarrow^{\tilde{f}_n} & \downarrow f_n & \swarrow^{k_{n-1}} & \downarrow f_{n-1} \\ Q_{n+1} & \xrightarrow{\pi_n} & L_0 & \xrightarrow{i_n} & Q_n & \xrightarrow{d_n^N} & Q_{n-1} \end{array}$$

mit $L_n = \ker(d_n^Q)$ und $d_{n+1}^Q = i_n\pi_n$. Hier ist

$$\begin{aligned} d_n^Q(f_n - k_{n-1}d_n^P) &= d_n^Q f_n - d_n^Q k_{n-1} d_n^P \\ &= f_{n-1}d_n^P - d_n^Q k_{n-1} d_n^P \\ &= (f_{n-1} - d_n^Q k_{n-1}) d_n P \\ &= k_{n-2} d_{n-1}^P d_n^P = 0\,. \end{aligned}$$

Also faktorisiert $f_n - k_{n-1}d_n^P$ mittels eines Morphismus $\tilde{f}_n$ über L_n und, wegen der Projektivität von P_n, mittels eines Morphismus k_n über N_{n+1}. Es folgt $f_n - k_{n-1}d_n^P = d_{n+1}^Q k_n$, also

$$f_n = d_{n+1}^Q k_n + k_{n-1} d_n^P\,.$$

Wir erhalten also die gewünschte Homotopie $f_\cdot \sim 0$.

Damit definieren wir nun:

Satz/Definition 11.18 Sei für Ringe R und S

$$F : Mod_R \to Mod_S$$

ein kovarianter rechtsexakter Funktor, d.h., für jede kurze exakte Sequenz

$$0 \to A \to B \to C \to 0$$

ist

$$F(A) \to F(B) \to F(C) \to 0$$

exakt. Dann sind die **Linksableitungen** von F

$$L_nF : Mod_R \to Mod_S \qquad (n \geq 0)$$

wie folgt definiert:
(i) Für ein Objekt $M \in Mod_R$ wähle eine projektive Auflösung

$$P_\cdot \to M$$

und setze

$$(L_nF)(M) := H^n(F(P_\cdot))\,,$$

die n-te Kohomologie des Komplexes

$$F(P_\cdot): \quad \ldots \to F(P_2) \to F(P_1) \to F(P_0)\,.$$

(ii) Für einen Morphismus $f : M \to N$ von R-Moduln wähle ein kommutatives Diagramm

$$\begin{array}{ccc} P_\cdot & \longrightarrow & M \\ {\scriptstyle f_\cdot}\downarrow & & \downarrow{\scriptstyle f} \\ Q_\cdot & \longrightarrow & N \end{array}$$

von projektiven Auflösungen (vergleiche 11.18 (a)) und definiere

$$f_* = (L_nF)(f) \;:\quad L_nF(M) \to L_nF(N)$$

als die induzierte Abbildung

$$H^n(F(P_\cdot)) \xrightarrow{H^n(F(f_\cdot))} H^n(F(Q_\cdot))\,.$$

Analog können wir definieren:

Definition 11.19 Sei für Ringe R und S

$$G : Mod_R \to Mod_S$$

ein *kontravarianter* linksexakter Funktor, d.h., für jede kurze exakte Sequenz

$$0 \to A \to B \to C \to 0$$

ist

$$0 \to G(C) \to G(B) \to G(A)$$

exakt. Dann sind die **Rechtsableitungen** von G

$$R^nG : Mod_R \to Mod_S \qquad (n \geq 0)$$

wie folgt definiert:
(i) Für ein Objekt $M \in Mod_R$ wähle eine projektive Auflösung

$$P_\cdot \to M$$

und setze

$$(R^nG)(M) := H^n(G(P_\cdot))\,,$$

die n-te Kohomologie des Komplexes

$$G(P_\cdot) : G(P_0) \to G(P_1) \to G(P_2) \to \dots$$

(ii) Für einen Morphismus $f : M \to N$ von R-Moduln wähle ein kommutatives Diagramm

$$\begin{array}{ccc} P_\cdot & \longrightarrow & M \\ {\scriptstyle f_\cdot}\downarrow & & \downarrow{\scriptstyle f} \\ Q_\cdot & \longrightarrow & N \end{array}$$

wie oben und definiere

$$f^* = R^nG(f) : L^nG(N) \to L^nG(M)$$

als die induzierte Abbildung

$$H^n(G(Q_\cdot)) \xrightarrow{H^n(G(f_\cdot))} H^n(G(P_\cdot))\,.$$

Lemma 11.20 Die in 11.18 und 11.19 definierten Funktoren L_nF bzw. R^nG hängen bis auf kanonische Isomorphien nicht von den Wahlen ab.

Der Beweis ergibt sich aus den folgenden Betrachtungen.

Definition 11.21 Ein Funktor

$$H : Mod_R \to Mod_S$$

heißt **additiv**, wenn für alle Morphismen von R-Moduln $f, g : A \to B$ gilt:

$$H(f + g) = H(f) + H(g)\,.$$

Lemma 11.22 Ist $F : Mod_R \to Mod_S$ additiv, so gilt für einen Morphismus $f^\cdot : C^\cdot \to D^\cdot$ von Komplexen in Mod_R und den induzierten Morphismus $F(f^\cdot)$ zwischen $F(C^\cdot)$ und $F(D^\cdot)$

$$f^\cdot \sim 0 \quad \Rightarrow \quad F(f^\cdot) \sim 0\,.$$

Beweis für kovariantes F (der kontravariante Fall ist analog): Ist $(k^\cdot)$ eine Homotopie von $f^\cdot$ zu 0,

$$d_D^{n-1}k^n + k^{n+1}d_C^n = f^\cdot\,,$$

so gilt wegen Funktorialität und Additivität von F

$$F(d_D^{n-1})F(k^n) + F(k^{n+1})F(d_C^n) = F(f^\cdot)\,,$$

also $F(f^\cdot) \sim 0$.

Lemma 11.23 Ist F ein kovarianter rechtsexakter Funktor wie in 11.18 (bzw. G ein kontravarianter linksexakter Funktor wie in 11.19), so ist F (bzw. G) additiv.

Beweis später

Beweis von Lemma 11.20 für den kovarianten Fall (der andere Fall ist analog): Hat man für jeden Modul M eine projektive Auflösung wie oben gewählt, und ist $f. : P. \to Q.$ wie oben, so ist $f.$ nach 11.17 (a) bis auf Homotopie eindeutig. Nach 11.22 und 11.23 ist dann auch

$$F(f.) : F(P.) \to F(Q.)$$

bis auf Homotopie eindeutig, also eindeutig auf der Kohomologie nach 11.12.

Wählt man andere projektive Auflösungen

$$\tilde{P}. \to M\,,$$

so gibt es, wieder nach 11.17 (a), kommutative Diagramme

$$\begin{array}{ccc} P. & \longrightarrow & M \\ \downarrow{\scriptstyle g.} & & \| \\ \tilde{P}. & \longrightarrow & M \\ \downarrow{\scriptstyle h.} & & \| \\ P. & \longrightarrow & M \end{array}$$

wobei die Homotopieklassen von $g.$ und $h.$ eindeutig sind, und $h.g. \sim id_{P.}$ sowie $g.h. \sim id_{\tilde{P}.}$. Wir erhalten also nach 11.12 *kanonische*, zueinander inverse Isomorphismen

$$H^n(FP.) \to H^n(F\tilde{P}.) \to H^n(FP.)\,.$$

Lemma 11.24 (a) In der Situation von 11.18 gibt es eine kanonische Isomorphie von Fuktoren

$$L_0F \xrightarrow{\sim} F\,.$$

(b) In der Situation von 11.19 gibt es eine kanonische Isomorphie von Funktoren

$$R^0G \xrightarrow{\sim} G\,.$$

Beweis (a): Da der Funktor rechtsexakt ist, ist für die exakte Sequenz

$$P_1 \to P_0 \to M \to 0$$

auch

$$F(P_1) \to F(P_0) \to F(M) \to 0$$

exakt. Daher ist

$$L_0F(M) = coker(F(P_1) \to F(P_0)) \cong F(M)\,.$$

(b) ist analog.

Wir kommen nun zu Anwendungen. Sei R ein kommutativer Ring mit Eins.

Definition 11.25 Sei N ein R-Modul. Dann ist der kovariante Funktor

$$\begin{array}{rccc} F_N = - \otimes_R N : Mod_R & \to & Ab \\ M & \mapsto & M \otimes_R N \end{array}$$

rechtsexakt. Die n-te Linksableitung $L_nF_N = L_n(- \otimes_R N)$ wird mit $Tor_n^R(-, N)$ bezeichnet.

Bemerkung 11.26 Ist $P_\cdot \to M$ eine projektive Auflösung, so ist also $Tor_n^R(M, N)$ die n-te Homologie des Komplexes

$$\ldots \to P_1 \otimes_R N \to P_1 \otimes_R M \to P_0 \otimes_R M \to 0\,.$$

Außerdem gilt nach 11.24 (a):

$$Tor_0^R(M, N) \cong M \otimes_R N\,.$$

Definition 11.27 Ein R-Modul N heißt **flach**, wenn der Funktor $- \otimes_R N$ exakt ist, wenn also für jede kurze exakte Sequenz

$$0 \to A \to B \to C \to 0$$

von R-Moduln die Sequenz

$$0 \to A \otimes_R N \to B \otimes_R N \to C \otimes_R N \to 0$$

exakt ist.

Bemerkungen 11.28 (a) Da der Funktor $- \otimes_R N$ rechtsexakt ist, ist die Frage die Exaktheit bei $A \otimes_R N$.

(b) Analog zum Argument im Beweis von Satz 11.2 ist ein Funktor $Mod_R \to Ab$ genau dann exakt, wenn er beliebige exakte Sequenzen in exakte Sequenzen überführt.

Definition 11.29 Sei N ein R-Modul. Dann ist der kontavarianter Funktor

$$\begin{array}{rccc} G_M = Hom_R(-, N) : & Mod_R & \to & Ab \\ & M & \mapsto & Hom_R(M, N) \end{array}$$

linksexakt (siehe 11.1 (b)). Die n-te Rechtsableitung $R^nG_M = R^nHom_R(-,N)$ wird mit $Ext^n_R(-,N)$ bezeichnet.

Bemerkung 11.30 Ist $P_\cdot \to M$ eine projektive Auflösung von M, so ist also $Ext^n_R(M,N)$ die n-te Kohomologie der Komplexes

$$0 \to Hom_R(P_0,N) \to Hom_R(P_1,N) \to Hom_R(P_2,N) \to \dots .$$

Außerdem gilt nach 11.24 (b)

$$Ext^0_R(M,N) \cong Hom_R(M,N) .$$

Beweis von Lemma 11.23 für den kovarianten Fall (der kontravariante Fall ist analog):

Lemma 11.31 (Vergleiche 7.9, 7.10 und 7.12) Seien M_1 und M_2 zwei R-Moduln. Für den R-Modul $M_1 \oplus M_2$ gilt dann:

(a) $M_1 \oplus M_2$ ist die Summe der R-Moduln M_1 und M_2 bezüglich der Homomorphismen

$$\begin{array}{rccc} i_1: & M_1 & \hookrightarrow & M_1 \oplus M_2 \\ & m_1 & \mapsto & (m_1,0) \end{array} \quad \text{und} \quad \begin{array}{rccc} i_2: & M_2 & \hookrightarrow & M_1 \oplus M_2 \\ & m_2 & \mapsto & (0,m_2) , \end{array}$$

d.h., sind $f_1 : M_1 \to N$ und $f_2 : M_2 \to N$ zwei Modulhomomorphismen, so gibt es genau einen Homomorphismus $f : M_1 \oplus M_2 \to N$ mit $fi_1 = f_1$ und $fi_2 = f_2$. Bezeichne f mit $f_1 \dot{+} f_2$.

(b) $M_1 \oplus M_2$ ist das Produkt von M_1 und M_2 bezüglich der Homomorphismen

$$\begin{array}{rccc} p_1: & M_1 \oplus M_2 & \to & M_1 \\ & (m_1,m_2) & \mapsto & m_1 \end{array} , \quad \begin{array}{rccc} p_2: & M_1 \oplus M_2 & \to & M_2 \\ & (m_1+m_2) & \mapsto & m_2 , \end{array}$$

d.h., sind $g_1 : N \to M_1$ und $g_2 : N \to M_2$ zwei Homomorphismen, so gilt es genau einen Homomorphismus $g : N \to M_1 \oplus M_2$ mit $p_1g = g_1$ und $p_2g = g_2$. Bezeichne g mit (g_1, g_2).

(c) Es ist $p_1 = i_1 \dot{+} 0$, $p_2 = 0 \dot{+} i_2$, $i_1 = (i_1, 0)$ und $i_2 = (i_2, 0)$.

(d) Es ist $id_{M_1 \oplus M_2} = i_1p_1 + i_2p_2$.

Beweis (a) und (b) wurden in 7.9 – 7.12 behandelt.

(c): Es gilt offenbar

$$p_1i_1 = id_{M_1}, \quad p_1i_2 = 0, \quad p_2i_1 = 0, \quad p_2i_2 = id_{M_2} . \tag{11.31.1}$$

(d): Aus (11.31.1) folgt

$$(i_1p_1 + i_2p_2)i_1 = i_1 = id\, i_1, \quad (i_1p_1 + i_2p_2)i_2 = i_2 = id\, i_2 .$$

Lemma 11.32 Für einen kovarianten Funktor

$$F : Mod_R \to Mod_S$$

betrachte die folgenden Aussagen.

(a) F ist additiv.

(b) F respektiert Summen, d.h., ist $M = M_1 \oplus M_2$, mittels $i_1 : M_1 \hookrightarrow M$ und $i_2 : M_2 \hookrightarrow M$, so ist

$$F(i_1) \dot{+} F(i_2) : F(M_1) \oplus F(M_2) \xrightarrow{\sim} F(M)$$

ein Isomorphismus.

(c) F respektiert Produkte, d.h., ist $M = M_1 \oplus M_2$, als Produkt aufgefasst mittels $p_1 : M \to M_1$ und $p_2 : M \to M_2$, so ist

$$(F(p_1), F(p_2) : F(M) \xrightarrow{\sim} F(M_1) \oplus F(M_2)$$

ein Isomorphismus.

Dann gilt

(b) $\Leftrightarrow$ (c) $\Rightarrow$ (a).

Beweis (b) $\Rightarrow$ (c): F respektive Summen. Dies bedeutet, dass $F(M) = F(M_1) \oplus F(M_2)$ bezüglich $F(i_1)$ und $F(i_2)$. Für $f = f_1 \dot{+} f_2 : M_1 \oplus M_2 \to N$ gilt dann $F(f) = F(f_1) \dot{+} F(f_2) : F(M_1) \oplus F(M_2) \to F(M)$. Denn es ist $F(f)F(i_1) = F(fi_1) = F(f_1)$ und $F(f)F(i_2) = F(f_2)$.

(c) $\Rightarrow$ (b) ist analog; man zeigt $F((f_1, f_2)) = (F(f_1), F(f_2))$.

(b) $\Rightarrow$ (a): Wir bemerken:

Lemma 11.33 In Mod_R ist für zwei Homomorphismen $f, g : M \to N$ die Komposition

$$M \xrightarrow{(id,id)} M \oplus M \xrightarrow{f \dot{+} g} N$$

gleich $f + g$.

Beweis: $x \mapsto (x, x) \mapsto (f(x) + g(x)$.

Gilt nun (b), so gilt auch (c), und wir haben

$$\begin{aligned} F(f+g) &= F((f \dot{+} g) \circ (id, id)) \\ &= (F(f) \dot{+} F(g)) \circ (F(id), F(id) \\ &= (F(f) \dot{+} F(g)) \circ (id, id) = F(f) + F(g)\,. \end{aligned}$$

Der Beweis von Lemma 11.23 folgt nun aus 11.32 und dem folgenden Lemma.

Lemma 11.34 Ein kovarianter rechtsexakter Funktor wie in 11.18 respektiert Summen.

Beweis Für eine Summe $M_1 \oplus M_2$ haben wir eine exakte Sequenz

$$0 \longrightarrow M_1 \underset{p_1}{\overset{i_1}{\rightleftarrows}} M_1 \oplus M_2 \underset{i_2}{\overset{p_2}{\rightleftarrows}} M_2 \longrightarrow 0$$

mit $p_\nu i_\nu = id$ und $i_1 p_1 + i_2 p_2 = id_{M_1 \oplus M_2}$ (siehe Lemma 11.31). Die Sequenz ist daher exakt. Dann ist die induzierte Sequenz

$$0 \longrightarrow F(M_1) \xrightarrow{F(i_1)} F(M_1 \oplus M_2) \longrightarrow F(M_2) \longrightarrow 0$$

auch exakt: F ist rechtsexakt, und wegen $F(p_1)F(i_1) = F(p_1 i_1) = id$ ist $F(i_1)$ injektiv.