VORWORT

Die Kommutative Algebra ist die Theorie der kommutativen Ringe und der Moduln über diesen.
Sie ist eine der wesentlichen Grundlagen der modernen Algebraischen Geometrie und spielt auch in der Komplexen Analysis eine wichtige Rolle. Ferner ist der "Durchschnitt" mit der algebraischen Zahlentheorie nicht leer.

Ziel des Buches ist es, interessierten Studenten eine gründliche, leicht zugängliche Einführung in dieses Gebiet zu geben.
Es werden nur relativ geringe algebraische Kenntnisse vorausgesetzt, nämlich so viel, wie man in etwa anderthalb Semestern einer normalen Algebra-Vorlesung über (kommutative) Ringe und Körper lernt. So wird z.B. der Modulbegriff, der den des Vektorraumes verallgemeinert, in unserem Buch eingeführt. Wir kommen bis zur Theorie der regulären und Cohen-Macaulay-Ringe und den Cohenschen Struktursätzen über komplette lokale Ringe. Der Zusammenhang mit der Algebraischen Geometrie wird in einem Paragraphen erläutert, ansonsten aber nicht besonders betont.
Wir haben nicht versucht, durch kunstvolle *ad-hoc*-Beweise Begriffe - wie etwa das Hilbert-Samuel-Polynom oder Ext und Tor - zu vermeiden. Unser Bestreben war es aber, den begrifflichen Rahmen in dosierter Weise im Laufe des Vorgehens zu erweitern. (Z.B. wird das Tensorprodukt erst etwa in der Mitte des Buches eingeführt.)

Unser Wunsch ist, der Leser möge Gefallen an der kommutativen Algebra, insbesondere an diesem Büchlein finden.

Wir widmen dieses Buch unserem Lehrer und Freund
Herrn Professor Dr. Hans-Joachim Nastold.

Münster, 13. Juli 1989

Rainer Brüske, Friedrich Ischebeck, Ferdinand Vogel

Zu den Voraussetzungen und zum Gebrauch des Buches

Vorausgesetzt werden grundlegende Kenntnisse über Gruppen, Ringe, Körper, Vektorräume, insbesondere:

Homomorphiesatz, Idealstruktur von Restklassenringen, Hauptidealringe, faktorielle Ringe (= ZPE-Ringe), Polynomringe in mehreren Unbestimmten (Satz von Gauß), eine gute Kenntnis über Körpererweiterungen.

In dem ansonsten vollständigen Aufbau des Buches haben wir uns eine Lücke erlaubt: Die Funktoren Ext^i und Tor_i werden "axiomatisch" eingeführt. Der Leser erhält Hinweise, wo er ihre Konstruktion nachlesen bzw. wie er sie anhand der Lösung von Übungsaufgaben selbst nachvollziehen kann.

In diesem Buch sollen folgende Festlegungen gelten:

Ein Ring ist (wenn nicht ausdrücklich anders vermerkt) kommutativ und hat ein Einselement.
Das Einselement des Ringes A *wird in der Regel mit* 1, *wenn erfoderlich, mit* 1_A *bezeichnet. (Man unterscheide den Buchstaben* $l = \ell$ *von* 1.*)*

Jeder Ringhomomorphismus $f: A \longrightarrow B$ *erfüllt* $f(1_A) = 1_B$. *Jeder Unterring eines Ringes* A *enthält* 1_A.

Ein Hauptidealring ist immer nullteilerfrei.

Ein minimales Primideal ist minimal in der Menge aller (nicht notwendig von (0) *verschiedenen) Primideale eines Ringes. (Nicht immer ist* (0) *ein Primideal!)*

Jedem Paragraphen folgen "Aufgaben und Hinweise". Diese geben Beispiele, Ergänzungen und Ausblicke. Sie sind nicht als "Intelligenztests" gedacht (z.B. variiert ihre Schwierigkeit sehr stark). Sie sollen auf keinen Fall ein Hindernis beim Lesen des "Haupttextes" sein. Dieser ist von den "Aufgaben und Hinweisen" unabhängig. (Manche Begriffe werden deshalb in dem Buch zweimal definiert.)

An mehreren Stellen weisen wir ausdrücklich auf die Möglichkeit hin, Teile des Textes (beim ersten Lesen) zu überschlagen. Eine erste Lektüre wird auch dadurch vereinfacht, daß man von allen betrachteten Ringen annimmt, sie seien noethersch, und von den Moduln, sie seien endlich erzeugt.

Zur Notation:

$\overline{a}$:= Restklasse von a

$Q(A)$:= Quotientenkörper von A

$\mathbb{N} := \{0,1,2,3,\ldots\}$, $\mathbb{N}_1 := \{1,2,3,\ldots\}$

$(a_1,\ldots,a_n)$ bezeichnet je nach Zusammenhang ein n-Tupel oder das von $a_1,\ldots,a_n$ erzeugte Ideal $a_1A+\ldots+a_nA$ eines Ringes A, insbesondere ist $(a) := aA$.

Nullring und Nullmodul werden mit 0 bezeichnet, der Nulluntermodul eines Moduls mit $\{0\}$, das Nullideal eines Ringes mit (0).

Das Inklusionszeichen "$\subset$" schließt die Gleichheit nicht aus. Andernfalls schreiben wir "$\subsetneq$" oder "$\subsetneqq$".

Wir danken Frau Bernadette Bourscheid für die sorgfältige Erstellung des Typoskripts.

INHALT

§1 RINGELEMENTE UND PRIMIDEALE

1. Klassifikation der Elemente eines Ringes

In einem Ring A betrachten wir folgende Teilmengen:
$A^* := \{a \in A \mid \exists\, b \in A: ab = 1\}$ =: Menge der Einheiten in A. A^* ist eine Gruppe bzgl. der Multiplikation.

$$\begin{aligned} NNT(A) &:= \left\{a \in A \mid \forall\, b \in A \text{ gilt: } (ab = 0 \Rightarrow b = 0)\right\} \\ &= \left\{a \in A \mid \forall\, b \in A - \{0\} \text{ gilt } ab \neq 0\right\} \end{aligned}$$

=: Menge der Nichtnullteiler in A.

$NNT(A)$ ist offensichtlich eine Halbgruppe bzgl. der Multiplikation mit $NNT(A) \supset A^*$.
Ist $a \in A$ ein Nichtnullteiler in A und gilt $ab = ab'$, so wegen $a(b-b') = 0$ auch $b-b' = 0$, also $b = b'$ ("Kürzungsregel"),

$NT(A) := \left\{a \in A \mid \exists\, b \in A - \{0\}: ab = 0\right\}$ =: Menge der Nullteiler in A.

Insbesondere ist 0 Nullteiler, wenn $1 \neq 0$ gilt. Ein Element a eines Ringes A heißt nilpotent, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 0$. Die nilpotenten Elemente eines Ringes A bilden ein Ideal in A. Ist nämlich $a^n = 0 = b^m$, so auch nach dem Binomialsatz $(a+b)^{n+m} = 0$, und die Implikation "a nilpotent, $b \in A \Rightarrow ab$ nilpotent" ist trivial.

$Nil(A) := \left\{a \in A \mid \exists\, n \in \mathbb{N}: a^n = 0\right\}$. Nilpotente Elemente eines Ringes $A \neq 0$ sind insbesondere Nullteiler: Ist n_0 minimal gewählt, so daß $a^{n_0} = 0$, so gilt $a \cdot a^{n_0-1} = 0$ mit $a^{n_0-1} \neq 0$. Das einzige nilpotente Element von $A_{red} := A/Nil(A)$ ist die Null.

Für $A \neq 0$ gelten folgende Inklusionen von Mengen:

$$\{0\} \subset Nil(A) \subset NT(A) \subset A - A^* \subset A$$

$$\{1\} \subset A^* \subset NNT(A) \subset A - Nil(A) \subset A$$

Beispiele 1.1

a) $\mathbb{Z}$: $\mathbb{Z}^* = \{-1,+1\}$, $NNT(\mathbb{Z}) = \mathbb{Z} - \{0\}$, $NT(\mathbb{Z}) = \{0\}$, $Nil(\mathbb{Z}) = \{0\}$.

b) $\mathbb{Z}/6\mathbb{Z}$: $(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1},-\bar{1}\} = NNT(\mathbb{Z}/6\mathbb{Z})$
$NT(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0},\bar{2},\bar{3},\bar{4}\}$ $\quad (\bar{2}\cdot\bar{3} = \bar{3}\cdot\bar{4} = \bar{0})$
$Nil(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0}\}$ $\quad (6 \mid a^n \Rightarrow 2 \mid a^n \wedge 3 \mid a^n \Rightarrow 2 \mid a \wedge 3 \mid a \Rightarrow 6 \mid a)$

c) $\mathbb{Z}/4\mathbb{Z}$: $(\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1},-\overline{1}\}$, $\mathrm{Nil}(\mathbb{Z}/4\mathbb{Z}) = \{\overline{0},\overline{2}\} = \mathrm{NT}(\mathbb{Z}/4\mathbb{Z})$

d) $\mathbb{Z}/12\mathbb{Z}$: $(\mathbb{Z}/12\mathbb{Z})^* = \{\overline{1},\overline{5},\overline{7},\overline{11}\} = \mathrm{NNT}(\mathbb{Z}/12\mathbb{Z})$

$\mathrm{NT}(\mathbb{Z}/12\mathbb{Z}) = \{\overline{0},\overline{2},\overline{3},\overline{4},\overline{6},\overline{8},\overline{9},\overline{10}\}$

$\mathrm{Nil}(\mathbb{Z}/12\mathbb{Z}) = \{\overline{0},\overline{6}\}$

N.B.: Beispiel b) zeigt, daß $\mathrm{NT}(A)$ im allgemeinen kein Ideal ist.

2. Operationen auf der Menge der Ideale

Sind $\mathfrak{a},\mathfrak{b}$ Ideale in A , so ist ihre Summe $\mathfrak{a}+\mathfrak{b}$ definiert als die Menge aller $x+y$ mit $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Es ist das kleinste Ideal in A , welches $\mathfrak{a}$ und $\mathfrak{b}$ enthält. Allgemeiner: Sind $\mathfrak{a}_i$ $(i \in I$, I Indexmenge) Ideale in A , so definiert man $\sum\limits_{i\in I} \mathfrak{a}_i := \left\{ \sum\limits_{i\in I} x_i \mid x_i \in \mathfrak{a}_i \text{ für alle } i \text{ und } x_i = 0 \text{ für fast alle } i \in I \right\}$. Es ist das kleinste Ideal in A , welches alle $\mathfrak{a}_i$ $(i \in I)$ enthält.

Mit zwei Idealen $\mathfrak{a},\mathfrak{b}$ in A ist ihr Durchschnitt wieder ein Ideal in A. Dasselbe gilt für eine (endliche oder unendliche) Familie von Idealen.

Das Produkt $\mathfrak{a}\cdot\mathfrak{b}$ ist das Ideal in A , welches von allen Produkten xy mit $x \in \mathfrak{a}$, $y \in \mathfrak{b}$ <u>erzeugt</u> wird. Analog definieren wir das Produkt für eine <u>endliche</u> Familie von Idealen. Insbesondere ist $\mathfrak{a}^n = \mathfrak{a}\cdot\mathfrak{a}\cdot\ldots\cdot\mathfrak{a}$ erklärt $(\mathfrak{a}^0 := (1) = A)$. $\mathfrak{a}^n$ $(n > 0)$ ist das Ideal, welches von allen Produkten der Form $x_1\cdot x_2\cdot\ldots\cdot x_n$ mit $x_i \in \mathfrak{a}$ $(1 \le i \le n)$ erzeugt wird.

Die Operationen "Summe", "Durchschnitt" und "Produkt" sind kommutativ und assoziativ, und es gilt das Distributivgesetz $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

Ist $\mathfrak{a}$ ein Ideal in A , so ist $\sqrt{\mathfrak{a}} := \{a \in A \mid \exists\, n \in \mathbb{N} \text{ mit } a^n \in \mathfrak{a}\}$ wieder ein Ideal $(a^n \in \mathfrak{a},\ b^m \in \mathfrak{a} \Rightarrow (a+b)^{m+n} \in \mathfrak{a}$). Es heißt Wurzel oder Radikal von $\mathfrak{a}$. Im allgemeinen hat man für Ideale $\mathfrak{a},\mathfrak{b}$ lediglich $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.

<u>Definition 1.2</u> Sind $\mathfrak{a},\mathfrak{b} \subset A$ Ideale in A mit $\mathfrak{a}+\mathfrak{b} = A$, so heißen $\mathfrak{a}$ und $\mathfrak{b}$ coprim.

<u>Lemma 1.3</u> *Sind* $\mathfrak{a},\mathfrak{b} \subset A$ *coprim, so gilt* $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

Zum <u>Beweis</u> ist nur zu bemerken, daß $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$, also im Falle $(\mathfrak{a}+\mathfrak{b}) = A$, daß $\mathfrak{a} \cap \mathfrak{b}$ $\mathfrak{a}\mathfrak{b}$ gilt. –

<u>Lemma 1.4</u> *Sind* $\mathfrak{a},\mathfrak{b}$ *und* $\mathfrak{a},\mathfrak{c}$ *jeweils coprim, so auch* $\mathfrak{a},\mathfrak{b}\mathfrak{c}$.

Beweis: $\mathfrak{a},\mathfrak{b}$ coprim $\Rightarrow$ es gibt $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ mit $a+b = 1$; $\mathfrak{a},\mathfrak{c}$ coprim $\Rightarrow$ es gibt $a' \in \mathfrak{a}$, $c \in \mathfrak{c}$ mit $a'+c = 1$. Betrachte $bc = (1-a)(1-a') = 1-a'-a+aa'$. Für $a'' := a'+a-aa' \in \mathfrak{a}$ gilt also $bc+a'' = 1$. Der Rest folgt aus der trivialen

Bemerkung 1.5 $\mathfrak{a},\mathfrak{b}$ coprim $\Leftrightarrow$ $\exists\, a \in \mathfrak{a}$ und $\exists\, b \in \mathfrak{b}$ mit $a+b = 1$. —

Definition 1.6 Sind $A_1,\ldots,A_n$ Ringe, so definiert man das direkte Produkt $A = \prod_{i=1}^{n} A_i$ als die Menge aller n-Tupel $(a_1,\ldots,a_n)$ mit $a_i \in A_i$ $(1 \le i \le n)$ und komponentenweiser Addition und Multiplikation. (Es dürfte dem Leser nicht schwerfallen, zwischen einem Produkt von Idealen und einem direkten Produkt von Ringen trotz gleicher Notation zu unterscheiden.)

Bemerkung 1.7 In den Bezeichnungen von 1.6 ist A kommutativer Ring mit Einselement $(1,1,\ldots,1)$.

Bemerkung 1.8 In den Bezeichnungen von 1.6 sind die Projektionen p_j ,

$$p_j: A \longrightarrow A_j \qquad ((a_1,\ldots,a_n) \longmapsto a_j)$$

Ringhomomorphismen (dagegen die Einbettungen $i_j: A_j \longrightarrow A$ $(a \longmapsto (0,\ldots,\underset{\substack{\uparrow \\ j\text{-te Komponente}}}{a},0,\ldots))$ nicht, da $i_j(1) = (0,\ldots,0,1,0,\ldots)$ nicht die Eins in A ist! Es gilt allerdings $(i_j(1))^2 = i_j(1)$, d.h. $i_j(1)$ ist idempotent.)

Für einen Ring A und Ideale $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ von A definiere man einen Homomorphismus $\phi: A \longrightarrow \prod_{i=1}^{n} (A/\mathfrak{a}_i)$ durch $a \longmapsto (a+\mathfrak{a}_1,\ldots,a+\mathfrak{a}_n)$.

Satz 1.9 (*Chinesischer Restsatz*)

a) *Sind die* $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ *paarweise coprim, so gilt* $\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$.

b) ϕ *surjektiv* $\Leftrightarrow$ *die* $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ *sind paarweise coprim.*

c) $\operatorname{Ker} \phi = \bigcap_{i=1}^{n} \mathfrak{a}_i$. *Also:* ϕ *injektiv* $\Leftrightarrow$ $\bigcap_{i=1}^{n} \mathfrak{a}_i = (0)$.

Beweis: Zu a): Induktion über n. Der Fall $n = 2$ ist in Lemma 1.3 abgehandelt. Sei $n > 2$ und die Behauptung richtig für

$\mathfrak{a}_1,\ldots,\mathfrak{a}_{n-1}$ und $\mathfrak{c} := \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. Nach Lemma 1.4 sind $\mathfrak{a}_n$ und $\mathfrak{c}$ wieder coprim. Deshalb ist $\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{c}\mathfrak{a}_n = \mathfrak{c} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i$.

Zu b): "$\Rightarrow$" Wir zeigen o.E. nur: $\mathfrak{a}_1, \mathfrak{a}_2$ sind coprim.
$\exists\, a \in A$ mit $\phi(a) = (1,0,\ldots,0)$, also $1 = (1-a)+a \in \mathfrak{a}_1 + \mathfrak{a}_2$.

"$\Leftarrow$" Es ist keine Einschränkung, nur zu zeigen: $\exists\, a \in A$ mit $\phi(a) = (1,0,\ldots,0)$: Wegen der Symmetrie gilt die Aussage dann für alle Elemente der Gestalt $(0,\ldots,0,1,0,\ldots)$ und, da ϕ ein Homomorphismus ist, sogar für alle Elemente aus $\prod_{i=1}^{n} (A/\mathfrak{a}_i)$!
Wegen $\mathfrak{a}_1 + \mathfrak{a}_i = A$ $(i > 1)$ hat man Gleichungen $a_i+b_i = 1$ mit $a_i \in \mathfrak{a}_1$, $b_i \in \mathfrak{a}_i$ $(2 \le i \le n)$. Für $a = \prod_{i=2}^{n} b_i$ gilt $a = \prod_{i=2}^{n} (1-a_i) = 1+a'$ mit geeignetem $a' \in \mathfrak{a}_1$ und $a \in \mathfrak{a}_i$ $(i \ge 2)$. Also: $\phi(a) = (1,0,\ldots,0)$.

Zu c) ist nichts zu sagen. –

<u>Bemerkung 1.10</u> Der Teil b) "$\Leftarrow$" obigen Satzes läßt sich auch wie folgt formulieren: Wenn $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ paarweise coprim und $b_1,\ldots,b_n$ beliebige Elemente von A sind, so besitzt das Kongruenzsystem
$x \equiv b_1(\mathfrak{a}_1),\ldots,x \equiv b_n(\mathfrak{a}_n)$ eine Lösung.

3. <u>Primideale</u>

<u>Definition 1.11</u> Ein Ring A heißt Integritätsring (oder auch integer oder auch nullteilerfrei), wenn er nicht zum Nullring isomorph ist und außer der Null keine Nullteiler enthält.

Im Sinne der obigen Definition ist ein Ring A genau dann Integritätsring, wenn $NT(A) = \{0\}$ gilt.

<u>Definition 1.12</u> Eine Teilmenge S eines Ringes A heißt multiplikativ, wenn $1 \in S$ und mit $x,y \in S$ auch $xy \in S$ gilt.

<u>Definition 1.13</u> Ein Ideal eines Ringes A heißt maximal, wenn es (bzgl. "$\subset$") maximal in der Menge aller von A verschiedenen Ideale ist.

<u>Satz und Definition 1.14</u> *In einem Ring A sind für ein Ideal $\mathfrak{p}$ folgende Aussagen äquivalent:*

(i) $A/\mathfrak{p}$ *ist integer.*

(ii) a) $\mathfrak{p} \neq A$, b) $(a,b \in A\,,\ ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p})$.

(iii) a) $\mathfrak{p} \neq A$, b) ($\mathfrak{a},\mathfrak{b}$ *Ideale in* A *mit* $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \Rightarrow \mathfrak{a}\subset\mathfrak{p} \vee \mathfrak{b}\subset\mathfrak{p}$).

(iv) $A-\mathfrak{p}$ *ist multiplikativ.*

Ein Ideal $\mathfrak{p}$, welches eine (und damit alle) der vorstehenden Eigenschaften hat, heißt Primideal. Die Menge der Primideale von A heißt das Spektrum von A und wird mit $\operatorname{Spec} A$ bezeichnet.

Beweis: (i) $\Rightarrow$ (ii): $A/\mathfrak{p}$ integer $\Rightarrow A/\mathfrak{p} \neq 0 \Rightarrow \mathfrak{p} \neq A$.
Seien $a,b \in A$ mit $ab \in \mathfrak{p} \Rightarrow \bar{a}\cdot\bar{b} = \bar{0}$ in $A/\mathfrak{p} \Rightarrow \bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$ ($A/\mathfrak{p}$ integer!) $\Rightarrow a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

(ii) $\Rightarrow$ (iii): Gälte $\mathfrak{a} \not\subset \mathfrak{p}$, $\mathfrak{b} \not\subset \mathfrak{p}$, so gäbe es $x \in \mathfrak{a}-\mathfrak{p}$, $y \in \mathfrak{b}-\mathfrak{p}$ mit $xy \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, also nach (ii) $x \in \mathfrak{p} \vee y \in \mathfrak{p}$, im Widerspruch zur Wahl von x und y.

(iii) $\Rightarrow$ (ii): Seien $a,b \in A$ mit $ab \in \mathfrak{p}$. Mit $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ und $\mathfrak{a}\mathfrak{b} = (ab) \subset \mathfrak{p}$ folgt $(a) \subset \mathfrak{p}$ oder $(b) \subset \mathfrak{p}$.

(ii) $\Rightarrow$ (i): Seien $\bar{a},\bar{b} \in A/\mathfrak{p}$ mit $\bar{a}\bar{b} = \bar{0}$, d.h. $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, also $\bar{a} = 0$ oder $\bar{b} = 0$. Wegen $\mathfrak{p} \neq A$ ist $A/\mathfrak{p}$ nicht der Nullring.

(ii) $\Longleftrightarrow$ (iv): $\mathfrak{p} \neq A \Longleftrightarrow 1 \notin \mathfrak{p} \Longleftrightarrow 1 \in A-\mathfrak{p}$.
$(a,b \in A\,,\ ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}) \Longleftrightarrow (a,b \in A,\ a \notin \mathfrak{p} \wedge b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}) \Longleftrightarrow (a,b \in A-\mathfrak{p} \Rightarrow ab \in A-\mathfrak{p})$. –

Beispiele für Primideale sind etwa in $\mathbb{Z}$ die von einer Primzahl erzeugten Ideale und das Nullideal.

Satz 1.15 (*Existenz von Primidealen*)

Es seien A *ein Ring,* $S \subset A$ *multiplikativ,* $\mathfrak{a} \subset A$ *ein Ideal mit* $\mathfrak{a} \cap S = \emptyset$. *Dann gilt:*

a) *Die Menge* $\mathfrak{M}$ *der Ideale* $\mathfrak{b}$ *von* A *mit* $\mathfrak{a} \subset \mathfrak{b} \subset A-S$ *besitzt maximale Elemente.*

b) *Jedes solche ist ein Primideal.*

Beweis: a) $\mathfrak{M} \neq \emptyset$, denn $\mathfrak{a} \in \mathfrak{M}$. $\mathfrak{M}$ ist bezüglich der Inklusion "$\subset$" teilweise geordnet. Sei $\mathcal{K} \subset \mathfrak{M}$ eine "Kette", das ist eine total geordnete Teilmenge (d.h. $\mathfrak{b}_1,\mathfrak{b}_2 \in \mathcal{K} \Rightarrow \mathfrak{b}_1 \subset \mathfrak{b}_2$ oder $\mathfrak{b}_2 \subset \mathfrak{b}_1$).

Bilde $\mathfrak{b}_{\mathcal{K}} = \bigcup\limits_{\mathfrak{b}\in\mathcal{K}} \mathfrak{b}$. Es ist $\mathfrak{b}_{\mathcal{K}}$ ein Ideal: Seien nämlich $x,y \in \mathfrak{b}_{\mathcal{K}}$, $a \in A$, $x \in \mathfrak{b}_1 \in \mathcal{K}$, $y \in \mathfrak{b}_2 \in \mathcal{K}$. Da $\mathcal{K}$ eine Kette ist, gilt $\mathfrak{b}_1 \subset \mathfrak{b}_2$ oder $\mathfrak{b}_2 \subset \mathfrak{b}_1$, etwa $\mathfrak{b}_1 \subset \mathfrak{b}_2$, also $x+y \in \mathfrak{b}_2 \in \mathcal{K}$, somit $x+y \in \mathfrak{b}_{\mathcal{K}}$. Ferner $ax \in \mathfrak{b}_1 \in \mathcal{K}$, also $ax \in \mathfrak{b}_{\mathcal{K}}$. Weiter hat man

$\mathfrak{h}_K \cap S = (\bigcup_{\mathfrak{h}\in K} \mathfrak{h}) \cap S = \bigcup_{\mathfrak{h}\in K} (\mathfrak{h} \cap S) = \emptyset$, d.h. $\mathfrak{h}_K \in \mathfrak{M}$.
Für alle $\mathfrak{h} \in K$ gilt $\mathfrak{h} \subset \mathfrak{h}_K$. Jede Kette in $\mathfrak{M}$ besitzt also eine obere Schranke in $\mathfrak{M}$. Nach dem Lemma von Zorn besitzt $\mathfrak{M}$ ein maximales Element $\mathfrak{p}$.

b) $\mathfrak{p}$ ist prim: Seien $a_1, a_2 \in A$, $a_1a_2 \in \mathfrak{p}$. Gilt $a_i \notin \mathfrak{p}$ für $i = 1,2$, so bilde man $\mathfrak{a}_1 = \mathfrak{p}+a_1A$, $\mathfrak{a}_2 = \mathfrak{p}+a_2A$. Wegen $a_i \notin \mathfrak{p}$ $(i = 1,2)$ folgt $\mathfrak{a}_i \supsetneqq \mathfrak{p}$ $(i = 1,2)$ und, wegen der Maximalität von $\mathfrak{p}$, $\mathfrak{a}_i \cap S \neq \emptyset$ $(i = 1,2)$. Seien $u_i = p_i+a_iy_i \in \mathfrak{a}_i \cap S$ $(p_i \in \mathfrak{p}, y_i \in A)$ $(i = 1,2)$. Man hat $u_1u_2 \in S$, da S multiplikativ ist, andererseits $u_1u_2 = p_1p_2 + p_1a_2y_2 + p_2a_1y_1 + a_1a_2y_1y_2 \in \mathfrak{p}$ wegen $a_1a_2 \in \mathfrak{p}$, im Widerspruch zu $S \cap \mathfrak{p} = \emptyset$. Es folgt: $a_1 \in \mathfrak{p}$ oder $a_2 \in \mathfrak{p}$, d.h. $\mathfrak{p}$ ist prim. —

Aus Satz 1.15 folgen Beziehungen zwischen den Primidealen von A und den Elementeklassen, die in Abschnitt 1 betrachtet wurden.

Folgerung 1.16 *Jedes Ideal* $\mathfrak{a} \neq A$ *ist in einem maximalen Ideal von* A *enthalten. Ein solches ist prim.*

Beweis: Man wende 1.15 auf die Menge $S = \{1\}$ an. —

Folgerung 1.17 $A^* = A - \bigcup_{\mathfrak{m}\text{ maximal}} \mathfrak{m}$.

Beweis: "$\subset$": $u \in A^*$, d.h. es gibt u' mit $u'u = 1$. Gäbe es ein maximales Ideal $\mathfrak{m}$ in A mit $u \in \mathfrak{m}$, so wäre auch $1 = u'u \in \mathfrak{m}$ (wegen der Idealeigenschaft), im Widerspruch zu $\mathfrak{m} \neq A$.

"$\supset$": Ist $u \in A - \bigcup_{\mathfrak{m}\text{ maximal}} \mathfrak{m}$, so gilt $Au \not\subset \mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$ in A , nach Folgerung 1.16 also $Au = A$. Folglich gibt es $u' \in A$ mit $u'u = 1$. —

Folgerung 1.18

a) $\mathrm{Nil}(A) = \bigcap_{\mathfrak{p}\text{ prim}} \mathfrak{p}$

b) Für ein Ideal $\mathfrak{a}$ *von* A *gilt* $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\supset\mathfrak{a}\text{ prim}} \mathfrak{p}$.

Beweis: a) "$\subset$": Sei $a \in \mathrm{Nil}(A)$ mit $a^n = 0$ und $\mathfrak{p} \supset \{0\}$ Primideal. Wegen $a^n = 0 \in \mathfrak{p}$ folgt $a \in \mathfrak{p}$ (Induktion nach n).

"$\supset$": Das Element a liege in jedem Primideal. Betrachte

$S = \{1,a,a^2,a^3,\dots\}$. S ist multiplikativ. Wäre $a^n \neq 0$ für alle $n \in \mathbb{N}$, so gälte $(0) \cap S = \emptyset$. Es gäbe also nach 1.15 ein Primideal $\mathfrak{p}$ mit $\mathfrak{p} \cap S = \emptyset$, insbesondere $a \notin \mathfrak{p}$. Widerspruch!

b) Mit $\varphi\colon A \longrightarrow A/\mathfrak{a}$ gilt $\sqrt{\mathfrak{a}} = \varphi^{-1}(\mathrm{Nil}(A/\mathfrak{a}))$; wende nun a) an. —

Folgerung 1.19 *In einem Ring A ist die Menge der Nullteiler eine Vereinigung gewisser Primideale.*

Beweis: Sei o.E. $A \neq 0$ und S die Menge der Nichtnullteiler. S ist multiplikativ und $(0) \cap S = \emptyset$. Nach 1.15 gibt es Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap S = \emptyset$. Sei M die Menge aller dieser Primideale (oder auch nur der maximalen unter ihnen). Behauptung: $NT(A) = \bigcup_{\mathfrak{p}\in M} \mathfrak{p}$.

"$\supset$": Da $(\bigcup_{\mathfrak{p}\in M} \mathfrak{p}) \cap S = \emptyset$, folgt $\bigcup_{\mathfrak{p}\in M} \mathfrak{p} \subset A - S = A - NNT(A) = NT(A)$.

"$\subset$": Sei $a \in NT(A)$, $ab = 0$, $b \neq 0 \Rightarrow ax \in NT(A)\ \forall x \in A \Rightarrow$
$aA \subset NT(A) \Rightarrow aA \cap S = \emptyset \Rightarrow$ Es gibt ein Primideal
$\mathfrak{p} \supset aA$ mit $\mathfrak{p} \cap S = \emptyset$, also $\mathfrak{p} \in M$: $aA \subset \bigcup_{\mathfrak{p}\in M} \mathfrak{p}$. —

Satz 1.20 *Die Menge der Primideale eines Ringes $A \neq 0$ besitzt minimale Elemente. Jedes Primideal umfaßt ein solches.*

(Zur Terminologie: Das 0-Ideal, falls es prim ist, gilt in diesem Buch als minimales Primideal.)

Beweis: Nach 1.16 besitzt A Primideale. Sei $\mathfrak{p}$ ein solches und $\mathfrak{M}$ die Menge der in $\mathfrak{p}$ enthaltenen Primideale. Ist $\mathfrak{K}$ eine Kette in $\mathfrak{M}$, so ist $\bigcap_{\mathfrak{q}\in\mathfrak{K}} \mathfrak{q}$ ein Ideal und $A - \bigcap_{\mathfrak{q}\in\mathfrak{K}} \mathfrak{q} = \bigcup_{\mathfrak{q}\in\mathfrak{K}} (A-\mathfrak{q})$ multiplikativ als Vereinigung einer Kette multiplikativer Mengen (vgl. den Schluß im Beweis von 1.15 Teil a)). Also ist $\bigcap_{\mathfrak{q}\in\mathfrak{K}} \mathfrak{q}$ ein Primideal und somit untere Schranke von $\mathfrak{K}$ in $\mathfrak{M}$. Zorns Lemma - "umgekehrt" angewandt - liefert die Behauptung. —

Satz 1.21 *Seien $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ endlich viele Ideale eines Ringes A und $\mathfrak{p}_1,\dots,\mathfrak{p}_{n-2}$ prim. Die Teilmenge $\mathfrak{a}$ von A sei bzgl. "+" und "$\cdot$" abgeschlossen, und es gelte $\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$. Dann gibt es ein $j \in \{1,\dots,n\}$ mit $\mathfrak{a} \subset \mathfrak{p}_j$.*

Beweis: Vollständige Induktion nach n.
Der Induktionsanfang ist trivial.

$n-1 \longrightarrow n$:

$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i \iff \mathfrak{a} = \bigcup_{i=1}^{n} (\mathfrak{a} \cap \mathfrak{p}_i)$. Könnten wir zeigen:

"es gibt ein $j \in \{1,\ldots,n\}$ mit $\mathfrak{a} \cap \mathfrak{p}_j \subset \bigcup_{\substack{i \neq j \\ i=1}}^{n} \mathfrak{p}_i$ ", so würde folgen

$\mathfrak{a} = \bigcup_{i=1}^{n} (\mathfrak{a} \cap \mathfrak{p}_i) \subset \bigcup_{\substack{i \neq j \\ i=1}}^{n} \mathfrak{p}_i$, und Anwenden der Induktionsvoraussetzung würde den Satz liefern. Es genügt also, die Annahme

"$\mathfrak{a} \cap \mathfrak{p}_j \not\subset \bigcup_{\substack{i \neq j \\ i=1}}^{n} \mathfrak{p}_i$ für alle j" zum Widerspruch zu bringen.

Wäre diese Annahme richtig, so gäbe es $a_j \in (\mathfrak{a} \cap \mathfrak{p}_j) - \bigcup_{\substack{i \neq j \\ i=1}}^{n} \mathfrak{p}_i$ $(1 \leq j \leq n)$.

Betrachte $y = a_1 + \prod_{k=2}^{n} a_k$, $y \in \mathfrak{a}$. Dieses y liegt in keinem der $\mathfrak{p}_i$ $(1 \leq i \leq n)$: Im Falle $i = 1$ gilt wegen $a_2,\ldots,a_n \notin \mathfrak{p}_1$, also $\prod_{k=2}^{n} a_k \notin \mathfrak{p}_1$ ($\mathfrak{p}_1$ ist für $n > 2$ prim!), und $a_1 \in \mathfrak{p}_1$, daß $y \notin \mathfrak{p}_1$.
Im Falle $i > 1$ gilt $a_1 \notin \mathfrak{p}_i$, aber $\prod_{k=2}^{n} a_k \in \mathfrak{p}_i$, deshalb $y \notin \mathfrak{p}_i$.
Insgesamt ist $y \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$, aber $y \in \mathfrak{a}$. Widerspruch zur Voraussetzung! —

Definition 1.22 Das Jacobson-Radikal $\mathrm{Jac}(A)$ eines Ringes A ist der Durchschnitt seiner maximalen Ideale.

Feststellung 1.23 $x \in \mathrm{Jac}(A) \iff 1-xy \in A^*$ *für alle* $y \in A$.

Beweis: "$\Rightarrow$": Wäre $1-xy$ keine Einheit, so wäre $1-xy$ in einem maximalen Ideal $\mathfrak{m}$ enthalten (1.17), und wegen $x \in \mathrm{Jac}(A) \subset \mathfrak{m}$ gälte $1 = (1-xy) + xy \in \mathfrak{m}$. Widerspruch!

"$\Leftarrow$": Gälte $x \notin \mathfrak{m}$ für ein maximales Ideal $\mathfrak{m}$ von A, so hätte man $\mathfrak{m}+xA = A$, also gäbe es $y \in A$, $m \in \mathfrak{m}$ mit $m+xy = 1$. Es folgte $1-xy \in \mathfrak{m}$ im Widerspruch zu $1-xy \in A^*$. —

Feststellung 1.24 *Ist* $\varphi: A \longrightarrow B$ *ein Ringhomomorphismus und* $\mathfrak{p}$ *ein Primideal in* B, *so ist* $\varphi^{-1}(\mathfrak{p})$ *ein Primideal in* A.

Beweis: $\varphi^{-1}(\mathfrak{p})$ ist trivialerweise ein Ideal und φ induziert eine Einbettung von $A/\varphi^{-1}(\mathfrak{p})$ in den Integritätsring $B/\mathfrak{p}$. —

<u>Aufgaben und Hinweise</u>

1) Zeige:

a) $x \in NT(A)$, $a \in A \Rightarrow xa \in NT(A)$.

b) $u \in A^*$, $x \in Nil(A) \Rightarrow u + x \in A^*$.

c) $a \in NNT(A)$, $x \in Nil(A) \Rightarrow a + x \in NNT(A)$. (1.18, 1.19)

2) Zeige für den Polynomring:

a) $Nil(A[T]) = (Nil(A))[T]$.

b) $A[T]^* = A^* + (Nil(A))[T]$.

3) Sei C der Ring der stetigen reellwertigen Funktionen auf $[0,1]$.

a) Ordne jedem Punkt von $[0,1]$ auf kanonische Weise ein maximales Ideal von C zu.

b) Seien $f_1,\ldots,f_n \in C$ ohne gemeinsame Nullstelle. Zeige: $\Sigma f_i^2 \in C^*$.

c) Zeige: Die Funktionen eines Ideals $\mathfrak{a} \neq C$ von C besitzen (mindestens) eine gemeinsame Nullstelle. (Benutze b) und die Kompaktheit.)

d) Folgere: Jedes maximale Ideal von C gehört zu einem Punkt von $[0,1]$ gemäß a).

N.B.: a) bis d) bleiben richtig, wenn $[0,1]$ durch einen beliebigen kompakten topologischen Raum ersetzt wird.

e) Zeige: In C gibt es Primideale $\mathfrak{p} \subsetneq \mathfrak{q}$. (1.15)

4) Ein Ringhomomorphismus $\varphi\colon A \longrightarrow B$ induziert durch $\mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p})$ eine Abbildung $\varphi^*\colon \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ (1.24). Für ein Ideal $\mathfrak{a}$ von A sei $V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supset \mathfrak{a}\}$.
Zeige:

a) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$, $V(A) = \emptyset$.

b) $V(\sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$, $V((0)) = \operatorname{Spec} A$.

Spec A wird also zu einem topologischen Raum, wenn man die $V(\mathfrak{a})$ als die abgeschlossenen Mengen von Spec A definiert (Zariski-Topologie). Zeige:

c) φ^* , wie oben für einen Ringhomomorphismus φ definiert, ist stetig.

d) Die Teilmengen $D(f) := \operatorname{Spec} A - V(Af)$, $f \in A$, bilden eine Basis der Zariski-Topologie auf Spec A .

5) Zeige: Die Ideale eines endlichen direkten Produktes von Ringen $\prod_{i=1}^{n} A_i$ sind von der Form $\prod_{i=1}^{n} \mathfrak{a}_i$, wo $\mathfrak{a}_i$ jeweils ein Ideal von A_i ist. Die Primideale sind von der Form $\prod_{i=1}^{n} \mathfrak{a}_i$, derart daß es ein $j \in \{1,\ldots,n\}$ gibt mit $\mathfrak{a}_i = A_i$ für $i \neq j$ und $\mathfrak{a}_j$ prim in A_j.

6) a) Sei e ein idempotentes ($e^2 = e$) Element eines Ringes A. Zeige: Es gibt Ringe A_1, A_2 und einen Isomorphismus $f: A \longrightarrow A_1 \times A_2$ mit $f(e) = (1,0)$. Bis auf Isomorphie sind A_1 und A_2 eindeutig bestimmt. Was geschieht in den Fällen $e = 1$ bzw. $e = 0$?

b) Löse das Zahlenrätsel

CHINA • CHINA = ***** CHINA .

Wende dabei a) und den chinesischen Restsatz an!

§2 BRUCHRINGE

Dieser Paragraph behandelt eine wichtige Verallgemeinerung der Bildung des Quotientenkörpers.

1. Definition und universelle Eigenschaft

Sei A ein Ring, S eine multiplikative Teilmenge von A. Auf dem cartesischen Produkt $A \times S$ betrachten wir die Relation "$\sim$":
$(a_1,s_1) \sim (a_2,s_2) :\iff \exists\, t \in S$ mit $ta_2s_1 = ta_1s_2$.
Diese Relation ist eine Äquivalenzrelation: Die Reflexivität $((a,s) \sim (a,s))$ und die Symmetrie $((a_1,s_1) \sim (a_2,s_2) \Rightarrow (a_2,s_2) \sim (a_1,s_1))$ sind trivialerweise erfüllt. Zur Transitivität: Gelte $(a_1,s_1) \sim (a_2,s_2)$, d.h. $\exists\, t_1$ mit $t_1a_2s_1 = t_1a_1s_2$ und $(a_2,s_2) \sim (a_3,s_2)$, d.h. $\exists\, t_2$ mit $t_2a_3s_2 = t_2a_2s_3$. Dann ist $(t_1t_2s_2)a_3s_1 = t_1s_1t_2a_2s_3 = t_2s_3t_1a_1s_2 = (t_1t_2s_2)a_1s_3$, also $(a_1,s_1) \sim (a_3,s_3)$.

Bemerkung 2.1 Enthält S keine Nullteiler, so gilt $(a,s) \sim (a',s')$ $\Longleftrightarrow$ $as' = a's$, wie man es bei der Quotientenkörperbildung gewohnt ist. Im allgemeinen definiert aber diese Regel keine Äquivalenzrelation! Immer gilt $(a,s) \sim (at,st)$ für $t \in S$.

Definition und Satz 2.2 $S^{-1}A := (A \times S)/\sim$ *ist auf naheliegende Weise ein Ring. Er heißt Bruch- oder Quotientenring von* A *nach der Nennermenge* S. *Mit* $\frac{a}{s}$ *wird die Äquivalenzklasse von* (a,s) *bezeichnet.*

Beweis: Auf $S^{-1}A$ definiert man die Addition wie folgt:

$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1s_2+a_2s_1}{s_1s_2}$. Sie ist wohldefiniert, denn sind $(a_1,s_1) \sim (A_1,S_1), (a_2,s_2) \sim (A_2,S_2)$, so gibt es $t_1,t_2 \in S$ mit $t_1s_1A_1 = t_1S_1a_1$, $t_2s_2A_2 = t_2S_2a_2$, also $S_1S_2t_1t_2(a_1s_2+a_2s_1)$

$= S_1S_2t_1t_2s_2a_1 + S_1S_2t_1t_2s_1a_2 = t_1s_1A_1S_2s_2t_2 + s_1t_1S_1t_2s_2A_2$

$= s_1s_2t_1t_2(A_1S_2+A_2S_1)$, d.h. wegen $t_1t_2 \in S$:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{A_1}{S_1} + \frac{A_2}{S_2} .$$

Die Kommutativität der Addition ist offensichtlich, die Assoziativität leicht zu verifizieren. Ferner sieht man sofort, daß $\frac{0}{1} = \frac{0}{s}$ (für jedes $s \in S$) das neutrale Element und daß $\frac{-a}{s}$ das zu $\frac{a}{s}$ inverse Element bzgl. der Addition ist. Die Multiplikation wird durch

$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}$ definiert. Ihre Wohldefiniertheit ist noch leichter einzusehen als die der Addition. Kommutativität und Assoziativität sind klar. Das Element $\frac{1}{1} = \frac{s}{s}$ (für jedes $s \in S$) ist neutral.
Die Distributivität ist so leicht zu verifizieren wie alles andere. –

Die Abbildung $i_{A,S}: A \longrightarrow S^{-1}A$, definiert durch $a \longmapsto \frac{a}{1}$, ist offensichtlich ein Ringhomomorphismus. Sie ist im allgemeinen weder injektiv noch surjektiv. Letzteres kennt man von der Quotientenkörperbildung. Bezüglich der Injektivität gilt genauer:

Bemerkung 2.3 Der Homomorphismus $i_{A,S}$ ist genau dann injektiv, wenn S aus lauter Nichtnullteilern besteht.

<u>Beweis:</u> Sei $s \in S$ ein Nullteiler und $a \in A - \{0\}$ mit $sa = 0$. Dann ist $i_{A,S}(a) = \frac{a}{1} = \frac{as}{s} = \frac{0}{s} = 0$. Wenn umgekehrt $S \subset \mathrm{NNT}(A)$ gilt und $i_{A,S}(a) = 0$, d.h. $\frac{a}{1} = \frac{0}{1}$ ist, gibt es $t \in S$ mit $t \cdot 1 \cdot a = t \cdot 0 \cdot 1 = 0$; also folgt $a = 0$, da t ein Nichtnullteiler ist. –

Offensichtlich gilt $i_{A,S}(S) \subset (S^{-1}A)^*$.

$S^{-1}A$ hat folgende universelle Eigenschaft:

<u>Satz 2.4</u> *Für jeden Ringhomomorphismus* $\varphi\colon A \longrightarrow B$ *mit* $\varphi(S) \subset B^*$ *gibt es genau einen Ringhomomorphismus* $\psi\colon S^{-1}A \longrightarrow B$ *mit* $\varphi = \psi \circ i_{A,S}$. *D.h. das Diagramm*

$$\begin{tikzcd} A \arrow[r, "i_{A,S}"] \arrow[dr, "\varphi"'] & S^{-1}A \arrow[d, dashed, "(!)\psi"] \\ & B \end{tikzcd}$$

ist auf genau eine Weise kommutativ ergänzbar.

Zum <u>Beweis</u> definiere man $\psi(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$. Die Wohldefiniertheit sieht man so: $\frac{a_1}{s_1} = \frac{a_2}{s_2} \Rightarrow \exists\, t \in S: \ ts_2a_1 = ts_1a_2 \Rightarrow \varphi(t)\varphi(s_2)\varphi(a_1)$
$= \varphi(t)\varphi(s_1)\varphi(a_2) \Rightarrow \varphi(s_2)\varphi(a_1) = \varphi(s_1)\varphi(a_2)$ $(\varphi(t) \in B^* \subset \mathrm{NNT}(B)!)$
$\Rightarrow \varphi(a_1)\varphi(s_1)^{-1} = \varphi(a_2)\varphi(s_2)^{-1}$. Wir zeigen, daß ψ ein Homomorphismus ist: $\psi(\frac{1}{1}) = \varphi(1)\varphi(1)^{-1}$, also $\psi(\frac{1}{1}) = 1$. Ferner $\psi(\frac{a_1}{s_1}\frac{a_2}{s_2}) = \psi(\frac{a_1a_2}{s_1s_2})$
$= \varphi(a_1a_2)\varphi(s_1s_2)^{-1} = \varphi(a_1)\varphi(a_2)(\varphi(s_1)\varphi(s_2))^{-1}$
$= \varphi(a_1)\varphi(s_1)^{-1}\varphi(a_2)\varphi(s_2)^{-1} = \psi(\frac{a_1}{s_1})\psi(\frac{a_2}{s_2})$. Und $\psi(\frac{a_1}{s_1} + \frac{a_2}{s_2}) = \psi(\frac{a_1s_2+a_2s_1}{s_1s_2})$
$= \varphi(a_1s_2+a_2s_1)\varphi(s_1s_2)^{-1} = (\varphi(a_1)\varphi(s_2) + \varphi(a_2)\varphi(s_1))\varphi(s_1)^{-1}\varphi(s_2)^{-1}$
$= \varphi(a_1)\varphi(s_1)^{-1} + \varphi(a_2)\varphi(s_2)^{-1} = \psi(\frac{a_1}{s_1}) + \psi(\frac{a_2}{s_1})$. Schließlich gilt
$\psi \circ i_{A,S}(a) = \psi(\frac{a}{1}) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$.

Ist Φ irgendein Ringhomomorphismus mit $\Phi \circ i_{A,S} = \varphi$, so gilt notwendig
$\Phi(\frac{a}{s}) = \Phi(\frac{a}{1}\cdot\frac{1}{s}) = \Phi(\frac{a}{1})\Phi(\frac{1}{s}) = \Phi(i_{A,S}(a))(\Phi(\frac{s}{1}))^{-1} = \Phi(i_{A,S}(a))(\Phi(i_{A,S}(s)))^{-1}$
$= \varphi(a)\varphi(s)^{-1}$. –

Korollar 2.5 *Seien* S,T *multiplikative Teilmengen eines Ringes* A *mit* $S \subset T$ *, so gibt es einen kanonischen Homomorphismus* $i_{S,T}: S^{-1}A \longrightarrow T^{-1}A$ *, der das Dreieck*

$$\begin{tikzcd} & A \arrow[dl, "i_{A,S}"'] \arrow[dr, "i_{A,T}"] & \\ S^{-1}A \arrow[rr, "i_{S,T}"] & & T^{-1}A \end{tikzcd}$$

kommutativ macht. –

Bemerkung 2.6 In der Situation von 2.5 kann $\frac{a}{s}$ mit $a \in A$, $s \in S$ verschiedene Bedeutungen haben, je nachdem ob man es als Element von $S^{-1}A$ oder von $T^{-1}A$ auffaßt: $i_{S,T}$ ist nicht immer injektiv. Wenn aber T aus Nichtnullteilern besteht, kann man $S^{-1}A$ (natürlich auch A) als Unterring von $T^{-1}A$ betrachten. Insbesondere ist für einen Integritätsring A jeder Bruchring $S^{-1}A$ mit $0 \notin S$ auf kanonische Weise ein Unterring des Quotientenkörpers $Q(A)$.
Genaueres zum Wechsel der Nennermenge findet man in [Bourbaki], chap. II, §2, no. 3.

Beispiele 2.7

(a) Wenn $S \subset A^*$, so ist $i_{A,S}$ ein Isomorphismus:
$\frac{a}{s} = \frac{as^{-1}}{1} \Rightarrow i_{A,S}$ ist surjektiv. $i_{A,S}$ ist injektiv, da S nur aus Nichtnullteilern besteht.

(b) Wenn $0 \in S$, folgt $S^{-1}A \simeq 0$: Für jedes (a,s) gilt $0\cdot(a\cdot 1-0\cdot s) = 0$ mit $0 \in S$. (Die Umkehrung gilt auch.)

(c) Ist A integer, $S = A - (0)$, so ist $S^{-1}A = Q(A)$ der Quotientenkörper von A und $A \xhookrightarrow[i_{A,S}]{} S^{-1}A$ injektiv.
(Beispiel: $\mathbb{Z} \hookrightarrow \mathbb{Q}$).

(d) Sei $\mathfrak{p}$ ein Primideal in A , $S = A-\mathfrak{p}$. Wir definieren $A_{\mathfrak{p}} := S^{-1}A$. $A_{\mathfrak{p}}$ heißt Lokalisierung von A in $\mathfrak{p}$.

Das letzte Beispiel soll genauer untersucht werden in

2. Idealstruktur in Bruchringen

Zunächst eine einfache

Bemerkung 2.8 In einem Ring A ist $A\text{-}A^*$ dann und nur dann ein Ideal, wenn A genau ein maximales Ideal besitzt.

Beweis: Sei $\mathfrak{n}$ ein maximales Ideal. Da $\mathfrak{n} \subset A\text{-}A^*$ und $A\text{-}A^*$ ein Ideal ist, folgt $\mathfrak{n} = A\text{-}A^*$. Die Umkehrung hatten wir schon in Folgerung 1.17 gezeigt. –

Definition 2.9 Ein Ring mit genau einem maximalen Ideal heißt lokaler Ring (oder auch Stellenring); einer mit nur endlich vielen maximalen Idealen heißt semilokal.

Beispiele für lokale Ringe liefert

Satz 2.10 *Sei* A *ein Ring und* $\mathfrak{p} \subset A$ *ein Primideal. Dann gilt:* $A_{\mathfrak{p}}$ *ist lokal mit dem maximalen Ideal* $\mathfrak{p}A_{\mathfrak{p}} := \{\frac{p}{s} \mid p \in \mathfrak{p}\ ,\ s \in A\text{-}\mathfrak{p}\}$.

Beweis: Nach 2.8 genügt es, zu zeigen: $\mathfrak{p}A_{\mathfrak{p}}$ ist ein Ideal und besteht aus allen Nichteinheiten von $A_{\mathfrak{p}}$. Sei $\frac{a}{s}$ eine Einheit in $A_{\mathfrak{p}}$, d.h. es gebe $\frac{a'}{s'} \in A_{\mathfrak{p}}$ mit $\frac{a}{s}\frac{a'}{s'} = \frac{1}{1}$. Dann gibt es ein $t \in A\text{-}\mathfrak{p}$ mit $taa' = tss' \in A\text{-}\mathfrak{p}$, also $a \in A\text{-}\mathfrak{p}$, da $\mathfrak{p}$ ein Ideal ist und sonst $taa' \in \mathfrak{p}$ gälte. Wir haben gezeigt: $(A_{\mathfrak{p}})^* \subset A_{\mathfrak{p}}\text{-}\mathfrak{p}A_{\mathfrak{p}}$. Die umgekehrte Inklusion $A_{\mathfrak{p}}\text{-}\mathfrak{p}A_{\mathfrak{p}} \subset (A_{\mathfrak{p}})^*$ ist klar, da aus $\frac{a}{s} \in A_{\mathfrak{p}}\text{-}\mathfrak{p}A_{\mathfrak{p}}$ folgt, daß $a,s \notin \mathfrak{p}$, somit $\frac{a}{1},\frac{1}{s} \in (A_{\mathfrak{p}})^*$ und also $\frac{a}{s} \in (A_{\mathfrak{p}})^*$ ist.

Daß $\mathfrak{p}A_{\mathfrak{p}}$ ein Ideal in $A_{\mathfrak{p}}$ ist, verifiziert man, wie folgt:
Sei $\frac{a}{t} \in A_{\mathfrak{p}}$, $\frac{p_1}{s_1}, \frac{p_2}{s_2} \in \mathfrak{p}A_{\mathfrak{p}}$. Dann ist $\frac{a}{t} \cdot \frac{p_1}{s_1} = \frac{ap_1}{ts_1}$ mit $ap_1 \in \mathfrak{p}$, $ts_1 \in S$ und $\frac{p_1}{s_1} + \frac{p_2}{s_2} = \frac{p_1s_2+p_2s_1}{s_1s_2}$ mit $s_1s_2 \in S$ und $p_1s_2+p_2s_1 \in \mathfrak{p}$. –

Bemerkung 2.11 $\mathfrak{p}A_{\mathfrak{p}}$ ist das von $i_{A,\mathfrak{p}}(\mathfrak{p})$ in $A_{\mathfrak{p}}$ erzeugte Ideal $(i_{A,\mathfrak{p}} := i_{A,A\text{-}\mathfrak{p}})$.

Beispiel: $A = \mathbb{Z}$, $\mathfrak{p} = \mathbb{Z}p$, p Primzahl.
$\mathbb{Z}_{\mathfrak{p}} = \mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} \mid m,n \in \mathbb{Z} \wedge p \nmid n\}$.
Wir werden später sehen: $\mathbb{Z}_{(p)}$ ist ein Hauptidealring mit im wesentlichen nur einem Primelement.

Welche Beziehungen bestehen nun zwischen den Idealen von A und $S^{-1}A$?

Definition 2.12 Sei $\mathfrak{a} \subset A$ ein Ideal. $S^{-1}\mathfrak{a} := \{\frac{a}{s} \mid a \in \mathfrak{a}, s \in S\}$.

Satz 2.13

a) $S^{-1}\mathfrak{a}$ *ist ein Ideal von* $S^{-1}A$. *Wenn* $\mathfrak{a} \cap S \neq \emptyset$, *folgt* $S^{-1}\mathfrak{a} = S^{-1}A$.

b) *Sei* $\mathfrak{b}$ *ein Ideal von* $S^{-1}A$ *und* $\mathfrak{a} = i^{-1}_{A,S}(\mathfrak{b})$. *Dann ist* $\mathfrak{b} = S^{-1}\mathfrak{a}$. *Insbesondere hat jedes Primideal von* $S^{-1}A$ *die Form* $S^{-1}\mathfrak{p}$, *wo* $\mathfrak{p}$ *ein Primideal von* A *ist*.

c) *Wenn* $\mathfrak{p}$ *ein Primideal von* A *ist mit* $\mathfrak{p} \cap S = \emptyset$, *so ist* $S^{-1}\mathfrak{p}$ *ein solches von* $S^{-1}A$.

d) *Unter der Voraussetzung von c) gilt* $i^{-1}_{A,S}(S^{-1}\mathfrak{p}) = \mathfrak{p}$.

Beweis: a) Daß $S^{-1}\mathfrak{a}$ ein Ideal ist, zeigt man wie im Beweis von 2.10 für $\mathfrak{p}A_{\mathfrak{p}}$. Falls $\mathfrak{a} \cap S \neq \emptyset$ ist, enthält $S^{-1}\mathfrak{a}$ eine Einheit des Ringes $S^{-1}A$.

b) "$\supset$": Sei $a \in \mathfrak{a}$, $s \in S$. $a \in \mathfrak{a} \iff \frac{a}{1} \in \mathfrak{b} \Rightarrow \frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} \in \mathfrak{b}$.

"$\subset$": $\frac{b}{s} \in \mathfrak{b} \Rightarrow \frac{b}{1} = \frac{s}{1} \cdot \frac{b}{s} \in \mathfrak{b} \Rightarrow b \in \mathfrak{a} \Rightarrow \frac{b}{s} \in S^{-1}\mathfrak{a}$.

Ist $\mathfrak{b}$ ein Primideal in $S^{-1}A$, so $i^{-1}_{A,S}(\mathfrak{b}) =: \mathfrak{p}$ ein Primideal in A (1.24) und $S^{-1}\mathfrak{p} = \mathfrak{b}$.

c) Sei $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in S^{-1}\mathfrak{p}$, also $\frac{a_1a_2}{s_1s_2} = \frac{p}{s_3}$ für ein $p \in \mathfrak{p}$, $s_3 \in S$. Dann gibt es ein $t \in S$ mit $ts_3a_1a_2 = ts_1s_2p \in \mathfrak{p}$, also (da $t, s_3 \notin \mathfrak{p}$) ist $a_1 \in \mathfrak{p} \vee a_2 \in \mathfrak{p}$. Folglich $\frac{a_1}{s_1} \in S^{-1}\mathfrak{p} \vee \frac{a_2}{s_2} \in S^{-1}\mathfrak{p}$.

d) "$\supset$" ist klar. "$\subset$": Sei $x \in A$, $i_{A,S}(x) \in S^{-1}\mathfrak{p}$, also $\frac{x}{1} = \frac{p}{s}$ mit gewissen $p \in \mathfrak{p}$, $s \in S$. Es gibt dann ein $t \in S$ mit $tsx = p$. Es folgt $x \in \mathfrak{p}$, da $st \in S$ und deshalb $st \notin \mathfrak{p}$. —

Satz 2.13 hat folgende Konsequenzen:

Folgerung 2.14 *Die Primideale von* $S^{-1}A$ *entsprechen bijektiv und ordnungserhaltend denjenigen Primidealen von* A, *die mit* S *leeren Durchschnitt haben. Insbesondere sehen wir nochmals, daß* $A_{\mathfrak{p}}$ *ein lokaler Ring ist.* —

Folgerung 2.15 *Ein minimales Primideal besteht aus lauter Nullteilern.*

Beweis: Sei $\mathfrak{p}$ ein minimales Primideal in A, und $0 \neq a \in \mathfrak{p}$. In $A_\mathfrak{p}$ ist $\mathfrak{p}A_\mathfrak{p}$ das einzige maximale Ideal und ein minimales Primideal, also das einzige Primideal. Wegen 1.18 sind alle Elemente von $\mathfrak{p}A_\mathfrak{p}$ nilpotent. Insbesondere gilt $(\frac{a}{1})^n = 0$ für ein minimal gewähltes n. Es gibt ein $t \in A-\mathfrak{p}$ mit $ta^n = 0$. Dann ist $(ta^{n-1})a = 0$ und $ta^{n-1} \neq 0$, da sonst $\frac{a^{n-1}}{1} = 0$ wäre. —

Definition 2.16 Ein Ring A heißt reduziert, wenn er keine nilpotenten Elemente $\neq 0$ hat.

Folgerung 2.17 *Für einen reduzierten Ring A gilt*

$$NT(A) = \bigcup_{\substack{\mathfrak{p} \text{ min.} \\ \text{Primideal}}} \mathfrak{p} .$$

Beweis: "$\supset$" ist wegen 2.15 offensichtlich. "$\subset$": Sei $a \notin \bigcup_{\substack{\mathfrak{p} \text{ min.} \\ \text{Primideal}}} \mathfrak{p}$ und $ab = 0$. Da 0 in jedem minimalen Primideal und a in keinem solchen liegt, liegt b in jedem minimalen Primideal, d.h. $b \in \mathrm{Nil}(A) = (0)$ nach 1.18. —

Satz 2.18 *A sei ein Hauptidealring. Dann gilt:*

a) *Wenn $S \subset A - \{0\}$ multiplikativ ist, ist $S^{-1}A$ ein Hauptidealring.*

b) *Wenn p ein Primelement in A ist und $\mathfrak{p} = Ap$, so ist $A_\mathfrak{p}$ ein Hauptidealring mit im wesentlichen genau einem Primelement.*

Beweis: Natürlich ist $S^{-1}A$ wieder integer. Sei $\mathfrak{a}$ ein Ideal von $S^{-1}A$. Nach 2.13 gibt es ein Ideal $\mathfrak{b}$ von A mit $\mathfrak{a} = S^{-1}\mathfrak{b}$. Sei $\mathfrak{b} = bA$. Dann gilt $\mathfrak{a} = \frac{b}{1} \cdot S^{-1}A$. $A_\mathfrak{p}$ hat genau ein Primideal, das nicht das Nullideal ist, nämlich $\frac{p}{1}A_\mathfrak{p}$. —

Satz 2.19 a) *Wenn $\varphi: A \longrightarrow B$ ein Ringhomomorphismus und $S \subset A$ multiplikativ ist, ist $\varphi(S) \subset B$ multiplikativ.*

b) *Seien $\mathfrak{a} \subset A$ ein Ideal, $S \subset A$ multiplikativ und $p: A \longrightarrow A/\mathfrak{a}$ die kanonische Projektion. Dann gilt $(S^{-1}A)/(S^{-1}\mathfrak{a}) \simeq p(S)^{-1}(A/\mathfrak{a})$. Genauer: Der nach Satz 2.4 existierende kanonische Homomorphismus $S^{-1}A \longrightarrow p(S)^{-1}(A/\mathfrak{a})$ ist surjektiv und hat den Kern $S^{-1}\mathfrak{a}$.*

Beweis: Nur b) ist nicht trivial. Wir haben Homomorphismen

$A \xrightarrow{p} A/\mathfrak{a} \xrightarrow{i_{A/\mathfrak{a},p(S)}} p(S)^{-1}(A/\mathfrak{a})$. Wende Satz 2.4 an mit $\varphi = i_{A/\mathfrak{a},p(S)} \circ p$. Jedes Element von $p(S)^{-1}(A/\mathfrak{a})$ hat die Form $\frac{p(a)}{p(s)}$ mit $a \in A$, $s \in S$, ist also Bild von $\frac{a}{s}$. Ferner $\frac{p(a)}{p(s)} = 0 \iff \exists\, t \in S$ mit $p(t)p(a) = 0 \iff p(ta) = 0 \iff ta \in \mathfrak{a} \iff \frac{a}{s} = \frac{at}{st} \in S^{-1}\mathfrak{a}$.—

Folgerung 2.20 $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq Q(A/\mathfrak{p})$. —

Aufgabe und Hinweis

1) Sei A ein reduzierter Ring, der nur endlich viele minimale Primideale, nämlich $\mathfrak{p}_1,\dots,\mathfrak{p}_n$, besitzt, und S die Menge seiner Nichtnullteiler, also $S = A - \bigcup_{i=1}^{n} \mathfrak{p}_i$. Zeige: $S^{-1}A \simeq \prod_{i=1}^{n} Q(A/\mathfrak{p}_i)$.

2) Wenn $S = \mathbb{Z} - (2)$ ist, ist $S^{-1}(2) = S^{-1}(6)$ in $S^{-1}\mathbb{Z}$.
Vgl. mit 2.12 und 2.13.

§3 MODULN

1. Definitionen, grundlegende Eigenschaften

Definition 3.1 Sei A ein Ring. Ein A-Modul M ist eine (additiv geschriebene) abelsche Gruppe, auf der A linear operiert. Genauer: Ein A-Modul M ist ein Paar (M,φ), wobei M eine abelsche Gruppe ist und $\varphi: A\times M \longrightarrow M$ eine Abbildung, so daß, wenn wir abkürzend $\varphi(a,m) =: am$ schreiben, folgendes gilt:

(i) $a(m_1+m_2) = am_1+am_2$ für $a \in A$, $m_1,m_2 \in M$,

(ii) $(a_1+a_2)m = a_1m+a_2m$ für $a_1,a_2 \in A$, $m \in M$,

(iii) $(a_1a_2)m = a_1(a_2m)$ für $a_1,a_2 \in A$, $m \in M$,

(iv) $1 \cdot m = m$ für $m \in M$.

Äquivalent zu Definition 3.1 ist ein A-Modul M eine abelsche Gruppe M zusammen mit einem Ringhomomorphismus von A in den (nicht notwendig kommutativen) Endomorphismenring der abelschen Gruppe M. Wenn A ein Körper ist, nennt man einen A-Modul bekanntlich auch einen A-Vektorraum.

<u>Bemerkungen 3.2</u> a) Wenn $f: A \longrightarrow B$ ein Ringhomomorphismus und M ein B-Modul ist, so ist M vermöge $(a,m) \longmapsto f(a)m$ auch ein A-Modul. Insbesondere ist auf diese Weise B selbst ein A-Modul.

b) Ist M ein A-Modul und $\mathfrak{a}$ ein Ideal von A, so daß $ax = 0$ ist für alle $a \in \mathfrak{a}$ und $x \in M$, so gilt $bx = cx$, wenn immer $b \equiv c \pmod{\mathfrak{a}}$ ist. In diesem Falle ist M also auf kanonische Weise ein $A/\mathfrak{a}$-Modul.

<u>Definition 3.3</u> Seien M_1, M_2 A-Moduln. Eine Abbildung $\varphi: M_1 \longrightarrow M_2$ heißt A-Modulhomomorphismus oder auch A-linear, wenn gilt:

(i) $\varphi(m+m') = \varphi(m)+\varphi(m')$ für $m,m' \in M_1$,

(ii) $\varphi(am) = a\varphi(m)$ für $m \in M_1$, $a \in A$.

Die Definition von "Isomorphismus", "isomorph", "$\simeq$" ist dann klar!

Mit $\mathrm{Hom}_A(M_1,M_2)$ bezeichnen wir die Menge aller A-linearen Abbildungen von M_1 in M_2. Mit $(a\varphi_1)(m) := a\varphi_1(m)$, $(\varphi_1+\varphi_2)(m) := \varphi_1(m) + \varphi_2(m)$ wird $\mathrm{Hom}_A(M_1,M_2)$ u.a. wegen $(\varphi_1+\varphi_2)(m_1+m_2) = \varphi_1(m_1+m_2) + \varphi_2(m_1+m_2) = \varphi_1(m_1) + \varphi_1(m_2) + \varphi_2(m_1) + \varphi_2(m_2) = (\varphi_1+\varphi_2)(m_1) + (\varphi_1+\varphi_2)(m_2)$ wieder zu einem A-Modul. (Die Kommutativität von A wird hierbei benötigt!)
Die Verkettung (= Hintereinanderschaltung) von A-linearen Abbildungen ist wieder A-linear.
Ein Untermodul N von M ist eine Untergruppe von M, die abgeschlossen unter der Multiplikation mit Elementen aus A ist. Die abelsche Faktorgruppe M/N trägt vermöge $a(m+N) := am+N$ eine A-Modulstruktur. Mit dieser heißt sie Faktormodul.

Die natürliche Projektion $M \xrightarrow{\varphi} M/N$ ist A-linear (und surjektiv).

<u>Bemerkung 3.4</u> Ist N ein Untermodul von M, so gibt es eine ordnungserhaltende Bijektion zwischen den Untermoduln E von M, die N enthalten, und den Untermoduln F von M/N, gegeben durch $E \longmapsto E/N$ bzw. $F \longmapsto \varphi^{-1}(F)$.

Bemerkung 3.5 Ist $\varphi: M \longrightarrow N$ eine A-lineare Abbildung, so ist der Kern $\mathrm{Ker}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ ein Untermodul von M, ferner $\mathrm{Im}(\varphi) := \varphi(M)$, das Bild von φ, ein Untermodul von N. Der Cokern $\mathrm{Coker}(\varphi) := N/\mathrm{Im}(\varphi)$ ist ein Faktormodul von N.

Bemerkung 3.6 Ist $\varphi: M \longrightarrow N$ eine A-lineare Abbildung, M' ein Untermodul von M mit $M' \subset \mathrm{Ker}\,\varphi$, dann liefert φ eine A-lineare Abbildung $\overline{\varphi}: M/M' \longrightarrow N$, die folgendermaßen definiert wird: Ist $\overline{m} \in M/M'$ das Bild von m unter der natürlichen Projektion $M \xrightarrow{p} M/M'$, so sei $\overline{\varphi}(\overline{m}) := \varphi(m)$. Es ist $\mathrm{Ker}(\overline{\varphi}) = \mathrm{Ker}(\varphi)/M'$. Man nennt $\overline{\varphi}$ den von φ induzierten Homomorphismus. (Homomorphiesatz)

Speziell für $M' = \mathrm{Ker}(\varphi)$ gilt:

Bemerkung 3.7 $M/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$.

Beispiele 3.8

a) Ein Ideal $\mathfrak{a}$ eines Ringes A ist ein A-Modul.

b) Ist M abelsche Gruppe, so kann man M als $\mathbb{Z}$-Modul auffassen vermöge $n \cdot m := \underbrace{m+m+\ldots+m}_{n\text{-mal}}$ $(n \in \mathbb{N})$, $(-n)m := -(nm)$.

c) Ist I eine Indexmenge, so ist die Menge $A^{(I)}$ aller Abbildungen $f: I \longrightarrow A$ mit $f(i) = 0$ für fast alle $i \in I$ vermöge $(af)(i) := a(f(i))$, $(f+g)(i) := f(i)+g(i)$ ein A-Modul. Moduln dieser Gestalt heißen frei. Wenn $I = \{1,2,\ldots,n\}$, ist $A^{(I)} = A^n$, der Menge aller n-Tupel von Elementen aus A.

Ist M ein A-Modul und ist $(M_i)_{i\in I}$ eine Familie von Untermoduln von M, so ist $\sum\limits_{i\in I} M_i = \left\{\sum\limits_{i\in I} m_i \mid m_i \in M_i,\text{ mit } m_i = 0 \text{ für fast alle } i\right\}$ der kleinste Untermodul von M, der alle M_i, $i \in I$, enthält. Der Durchschnitt $\bigcap\limits_{i\in I} M_i$ ist Untermodul von M.

Satz 3.9 *a) Sind* $M \supset M_1 \supset M_2$ *A-Moduln, so ist auf kanonische Weise* $(M/M_2)/(M_1/M_2) \simeq M/M_1$.

b) Sind M_1, M_2 *Untermoduln von* M, *so ist auf kanonische Weise* $(M_1+M_2)/M_1 \simeq M_2/(M_1 \cap M_2)$ *(Noetherscher Isomorphiesatz).*

Beweis: a) Definiere $\varphi\colon M/M_2 \longrightarrow M/M_1$ durch $\varphi(m+M_2) = m+M_1$. Wegen $M_2 \subset M_1$ ist φ wohldefiniert. Es ist $\operatorname{Ker}\varphi = M_1/M_2$ und $\operatorname{Im}\varphi = M/M_1$. Wende 3.7 an!

b) Die Abbildung $p\colon M_2 \longrightarrow (M_1+M_2)/M_1$, definiert durch $p(m) = m+M_1$, hat den Kern $M_1 \cap M_2$. Wende 3.7 an! —

Ist m ein Element aus M, so ist die Menge aller Vielfachen am $(a \in A)$ ein Untermodul von M, bezeichnet mit Am. Moduln der Gestalt Am heißen monogen.

Bemerkung 3.10 M ist ein monogener A-Modul genau dann, wenn es ein Ideal $\mathfrak{a}$ von A gibt mit $M \simeq A/\mathfrak{a}$.

Denn gilt $M = Am$ für ein $m \in M$, so betrachte man $\varphi\colon A \longrightarrow M$, $a \longmapsto am$. Wende 3.6 an! Umgekehrt ist $A/\mathfrak{a} = A\cdot\bar{1}$, wo $\bar{1} = 1+\mathfrak{a}$ ist. —

Definition 3.11 Sei M ein A-Modul.

a) Eine Familie $(x_i,\ i \in I)$ mit $x_i \in M$ heißt ein Erzeugendensystem von M, wenn $M = \sum_{i\in I} Ax_i$ gilt (I Indexmenge).

b) $(x_i,\ i \in I)$ heißt eine Basis von M, wenn $(x_i,\ i \in I)$ ein Erzeugendensystem von M ist und folgendes gilt:
$\left(\sum_{i\in I} a_i x_i = \sum_{i\in I} \tilde{a}_i x_i \Rightarrow a_i = \tilde{a}_i \quad (i \in I) \right)$.

c) Besitzt M ein Erzeugendensystem $(m_i,\ i \in I)$ mit $|I| = n < \infty$, so heißt M ein endlicher (auch endlich erzeugter) A-Modul.

Bemerkung 3.12 M ist genau dann frei (3.8c)), wenn er eine Basis besitzt.

Denn für einen Modul M mit der Basis $(m_i)_{i\in I}$ ist die Abbildung $M \longrightarrow A^{(I)}$, definiert durch $m = \sum_{i\in I} a_i m_i \longmapsto (i \longmapsto a_i)$ wohldefiniert und bijektiv. Andererseits ist für einen Modul $M \simeq A^{(I)}$ die Menge der f_i, $i \in I$, mit $f_i(j) = 0$ für $j \neq i$, $f_i(i) = 1$ eine Basis von M. —

Bemerkung 3.13 a) Die A-Modulhomomorphismen $A \xrightarrow{\varphi} M$ entsprechen bijektiv den Elementen $m \in M$ vermöge $\varphi \longmapsto \varphi(1)$.

b) Allgemeiner: Sei F frei, $B \subset F$ eine Basis. Dann gehört zu jeder Abbildung $\varphi\colon B \longrightarrow M$ genau ein Homomorphismus $\Phi\colon F \longrightarrow M$ mit $\Phi|_B = \varphi$.

Zu a) bemerke man, daß wegen $\varphi(a) = a\varphi(1)$ eine A-lineare Abbildung $\varphi\colon A \longrightarrow M$ eindeutig durch den Wert $\varphi(1)$ charakterisiert ist.

Zu b): Die Abbildung $(f := \sum_{b\in B} a_b b \overset{\Phi}{\longmapsto} m = \sum_{b\in B} a_b\varphi(b))$ für $f \in F$ ist, da B Basis von F, wohldefiniert, A-linear und durch $b \longmapsto \varphi(b)$ charakterisiert. —

Satz 3.14

a) *Jeder Modul ist Faktormodul eines freien Moduls.*

b) M *ist ein endlicher* A-*Modul* $\iff M \simeq A^n/U$, *für ein* $n \in \mathbb{N}$ *und einen Untermodul* U *von* A^n.

c) *Jeder Faktormodul eines endlichen Moduls ist endlich.*

d) *Wenn* U *ein Untermodul des* A-*Moduls* M *ist und* M/U *sowie* U *endlich sind, so ist auch* M *endlich.*

Beweis: a) Es sei E ein Erzeugendensystem von M. Man betrachte $\Phi: A^{(E)} \longrightarrow M$, definiert durch $\Phi(f_e) = e$ (f_e wie im Beweis zu Bemerkung 3.12 definiert: $f_e(e') = 0$ für $e \neq e'$, $f_e(e) = 1$). (Die f_e, $e \in E$, bilden eine A-Basis von $A^{(E)}$.) Bemerkung 3.13 liefert die Existenz von Φ. Für $m \in M$, $m = \sum_{e\in E} a_e e$ gilt

$$\Phi(\sum_{e\in E} a_e f_e) = \sum_{e\in E} \phi(a_e f_e) = \sum_{e\in E} a_e\Phi(f_e) = \sum_{e\in E} a_e e = m .$$

Φ ist surjektiv. Bemerkung 3.7 liefert die Behauptung.

b) unmittelbar: Für $|E| = n < \infty$ gilt $A^{(E)} \simeq A^n$.

c) Restklassen eines Erzeugendensystems bilden ein Erzeugendensystem des Faktormoduls.

d) Ist $\overline{m}_1,\ldots,\overline{m}_n$ ein Erzeugendensystem des A-Moduls M/U, $u_1,\ldots,u_k$ ein solches des A-Moduls U, $m \in M$ beliebig, so gilt $\overline{m} = \sum a_i\overline{m}_i$, d.h.

$$m = \sum_{i=1}^{n} a_i m_i + u , \quad \text{mit geeigneten } u \in U,\ a_i \in A, \text{ also}$$

$$m = \sum_{i=1}^{n} a_i m_i + \sum_{j=1}^{k} b_j u_j \quad \text{mit geeigneten } a_i, b_j \in A . \text{ —}$$

Definition 3.15 Sind M_i, $i \in I$ (I Indexmenge), A-Moduln, so ist $\bigoplus_{i\in I} M_i := \left\{(m_i)_{i\in I} \mid m_i \in M_i,\ \text{für fast alle } i \in I\colon m_i = 0\right\}$ vermöge

$a\cdot(m_i)_{i\in I} := (am_i)_{i\in I}$, $(m_i)_{i\in I} + (n_i)_{i\in I} := (m_i+n_i)_{i\in I}$ wieder ein A-Modul. Man nennt $\bigoplus_{i\in I} M_i$ die direkte Summe der M_i.

Gilt $M_i = A$ für alle $i \in I$, so ist $\bigoplus_{i\in I} M_i = A^{(I)}$. Endliche direkte Summen werden auch mit $M \oplus N$, $M_1 \oplus \ldots \oplus M_n$ etc. bezeichnet.

Bemerkung 3.16 Für jedes $j \in I$ kann man M_j auf naheliegende Weise als Untermodul von $\bigoplus_{i\in I} M_i$ auffassen, indem man $x \in M_j$ mit der Familie $(m_i)_{i\in I}$ identifiziert, die durch $m_j = x$ und $m_i = 0$ für $i \neq j$ definiert ist.
Bei dieser Identifikation gilt

$$\sum_{i\in I} M_i = \bigoplus_{i\in I} M_i \quad \text{und}$$

$$M_j \cap \sum_{i\in I-\{j\}} M_i = \{0\} \quad \text{für jedes } j \in I .$$

Umgekehrt, wenn ein Modul E eine Familie $(M_i)_{i\in I}$ von Untermoduln besitzt, für die $\Sigma M_i = E$ und $M_j \cap \sum_{i\in I-\{j\}} M_i = 0$ für jedes $i \in I$ gilt, so ist die naheliegende Abbildung $\bigoplus_{i\in I} M_i \longrightarrow E$, $(m_i)_{i\in I} \longmapsto \sum_{i\in I} m_i$ ein Isomorphismus.
Die A-Linearität und Surjektivität ist klar. Zur Injektivität: Wenn $\sum_{i\in I} m_i = 0$, so gilt für jedes $j \in I$, daß $m_j \in M_j$ und $m_j = -\sum_{i\in I-\{j\}} m_i \in \sum_{i\in I-\{j\}} M_i$, mithin $m_j = 0$ ist.

Wenn E zusammen mit einer Familie $(M_i)_{i\in I}$ von Untermoduln obige Bedingungen erfüllt, schreibt man - etwas ungenau - $E = \bigoplus_{i\in I} M_i$.

Lemma 3.17 *Seien* $f\colon M \longrightarrow N$ *und* $g\colon N \longrightarrow M$ *Modulhomomorphismen mit* $f\circ g = id_N$, *so ist* f *surjektiv,* g *injektiv und* $M = g(N) \oplus Ker(f) \simeq N \oplus Ker(f)$.

Beweis: f ist surjektiv und g ist injektiv, da $f\circ g$ surjektiv und injektiv ist. Für $x \in N$ ist $f\circ g(x) = x$, also $x = 0$, wenn $g(x) \in Ker(f)$. Es folgt $g(N) \cap Ker(f) = \{0\}$. Für $y \in M$ gilt $y = (y-g\circ f(y)) + g(f(y)) \in Ker(f) + g(N)$, da $f(y-g\circ f(y)) = f(y)-id_N\circ f(y) = 0$. Also $g(N) + Ker(f) = M$. Beachte 3.16. –

Satz 3.18 *a) (Verallgemeinerung von 3.13)*
Seien $(M_i)_{i\in I}$ *(I Indexmenge) und* N *A-Moduln. Zu Homomorphismen* $f_i\colon M_i \longrightarrow N$ $(i \in I)$ *gibt es genau eine A-lineare Abbildung* $f\colon \bigoplus_{i\in I} M_i \longrightarrow N$ *mit* $f|_{M_i} = f_i$.
b) Zu A-Moduln M_i, $i \in I$ *(I Indexmenge),* N *und Homomorphismen* $g_i\colon N \longrightarrow M_i$ *mit* $(\forall\, n \in N$ *gilt* $g_i(n) = 0$ *für fast alle* $i)$ *gibt es genau ein* $g\colon N \longrightarrow \bigoplus_{i\in I} M_i$ *mit* $p_i\circ g = g_i$, *wobei* $p_i\colon \bigoplus_{j\in I} M_j \longrightarrow M_i$ *durch* $(m_j)_{j\in I} \longmapsto m_i$ *definiert ist.*

Beweis: a) Wenn es ein solches f geben soll, muß notwendig $f((m_i)_{i\in I}) = \sum_{i\in I} f(m_i) = \sum_{i\in I} f_i(m_i)$ gelten (f ist A-linear). Diese Definition liefert andererseits einen A-Modulhomomorphismus $\bigoplus_{i\in I} M_i \xrightarrow{f} N$ mit $f|_{M_i} = f_i$.

b) $g: N \longrightarrow \bigoplus_{i\in I} M_i$, $n \longmapsto (g_i(n))_{i\in I}$ ist wegen der Endlichkeitsvoraussetzung sinnvoll, A-linear mit $p_i \circ g(n) = p_i((g_j(n))_{j\in I}) = g_i(n)$. —

Satz 3.19 (*Lemma von Nakayama*): *Für ein Ideal* $\mathfrak{a} \subset A$ *sind äquivalent:*

(*i*) $\mathfrak{a} \subset \mathrm{Jac}(A)$;

(*ii*) *Für jeden endlichen* A-*Modul* M *mit* $\mathfrak{a}M = M$ *gilt* $M = 0$. Dabei bezeichnet $\mathfrak{a}M$ den von allen am, $a \in \mathfrak{a}$, $m \in M$ erzeugten Untermodul von M .

Beweis: (i) $\Rightarrow$ (ii): Sei $m_1,\ldots,m_n$ ein Erzeugendensystem von M mit minimalem n. Wenn $M \neq 0$ ist, ist $n > 0$. Aus $M = \mathfrak{a}M$ folgt: Es gibt $a_1,\ldots,a_n \in \mathfrak{a}$ mit $m_1 = a_1m_1 + \ldots + a_nm_n$, also $m_1 = (1-a_1)^{-1}(a_2m_2+\ldots+a_nm_n)$, da $1-a_1 \in A^*$ nach 1.23 gilt. Dann ist aber bereits $m_2,\ldots,m_n$ ein Erzeugendensystem.

(ii) $\Rightarrow$ (i): Gälte $\mathfrak{a} \not\subset \mathrm{Jac}(A)$, so gäbe es ein maximales Ideal $\mathfrak{m} \not\supset \mathfrak{a}$. Für $M := A/\mathfrak{m} \neq 0$ gilt aber $\mathfrak{a}M = M$. —

Folgerung 3.20 $N \subset M$ *seien* A-*Moduln,* M/N *endlich erzeugt. Gilt für ein Ideal* $\mathfrak{a} \subset \mathrm{Jac}(A)$, *daß* $N+\mathfrak{a}M = M$ *ist, so folgt* $M = N$.

Beweis: $\mathfrak{a}(M/N) = (N+\mathfrak{a}M)/N = M/N \Rightarrow M/N = 0$. —

Folgerung 3.21 *Sei* $\varphi: M \longrightarrow N$ A-*linear mit endlichem Cokern. Gilt für ein Ideal* $\mathfrak{a} \subset \mathrm{Jac}(A)$, *daß die "induzierte" Abbildung* $M/\mathfrak{a}M \longrightarrow N/\mathfrak{a}N$ (*die durch Anwendung von 3.6 auf die Verkettung der Abbildungen* $M \xrightarrow{\varphi} N \xrightarrow{\text{kan.}} N/\mathfrak{a}N$ *entsteht*) *surjektiv ist, so ist auch* φ *surjektiv.*

Beweis: $N = \varphi(M) + \mathfrak{a}N \Rightarrow N = \varphi(M)$ nach 3.20. —

2. Noethersche Moduln und Ringe

Eine wichtige Klasse von A-Moduln sind die endlichen Moduln. Im allgemeinen ist diese Klasse nicht stabil bei Bildung von Untermoduln: Der Polynomring $\mathbb{R}[X_i]_{i\in\mathbb{N}}$ in unendlich vielen Unbestimmten $X_1,X_2,\ldots$ ist

als Modul über sich selbst sogar monogen, aber das Ideal (= $\mathbb{R}[X_i]_{i\in\mathbb{N}}$-Untermodul) $(X_1,X_2,X_3,\dots)$ ist zum Beispiel nicht endlich erzeugbar: Sonst müßte die Kette $(X_1) \subset (X_1,X_2) \subset (X_1,X_2,X_3) \subset \dots$ stationär werden, was, wie man leicht nachprüft, nicht der Fall ist:
$X_{i+1} \notin (X_1,\dots,X_i)$!
Wir suchen nach Bedingungen für den A-Modul M, die dieses Phänomen ausschließen.

Feststellung 3.22 *Ist $\mathfrak{M}$ eine durch eine Relation "$\leq$" teilweise geordnete Menge, so sind folgende Bedingungen für $\mathfrak{M}$ äquivalent:*

(*i*) *Jede aufsteigende Folge $M_1 \leq M_2 \leq \dots$ von Elementen aus $\mathfrak{M}$ wird stationär (i.e. $\exists\, n \in \mathbb{N}$ mit $M_n = M_{n+1} = \dots$).*

(*ii*) *Jede nicht-leere Teilmenge von $\mathfrak{M}$ hat ein maximales Element.*

Beweis: (i) $\Rightarrow$ (ii): Ist (ii) falsch, so gibt es eine nicht-leere Teilmenge $\mathfrak{T}$ von $\mathfrak{M}$ ohne maximales Element, und man konstruiert induktiv, von einem beliebigen $M_1 \in \mathfrak{T}$ ausgehend, eine nichtendende, strikt wachsende Folge $M_1 \leq M_2 \leq \dots$ in $\mathfrak{T}$.
(ii) $\Rightarrow$ (i): Die Folge $M_1 \leq M_2 \leq \dots$ hat ein maximales Element, etwa M_n.

Definition 3.23 Ein A-Modul M, dessen Untermodulmenge bzgl. "$\subset$" (i) oder (ii) von 3.22 erfüllt, heißt noetherscher A-Modul. Ein Ring heißt noethersch, wenn er als Modul über sich selbst noethersch ist.

Beispiel: Wie sich sofort aus folgendem Satz ergibt, ist jeder Hauptidealring noethersch.

Satz 3.24 M *ist ein noetherscher* A-Modul $\iff$ *Jeder Untermodul von* M *(insbesondere* M *selbst) ist endlich.*

Beweis: "$\Rightarrow$": Sei N ein Untermodul von M und $\mathfrak{M}$ die Menge aller endlich erzeugten Untermoduln von N. Da $\{0\} \in \mathfrak{M}$, ist $\mathfrak{M} \neq \emptyset$.
Sei N_0 maximal in $\mathfrak{M}$ (3.22 (ii)). Wäre $N_0 \neq N$, so wäre für $x \in N - N_0$ der Untermodul $N_0 + Ax$ von N endlich und echt größer als N_0; Widerspruch.
"$\Leftarrow$": Sei $M_1 \subset M_2 \subset \dots$ eine aufsteigende Kette von Untermoduln von M.
$N = \bigcup_{n=1}^{\infty} M_n$ ist Untermodul von M, also endlich erzeugt, etwa durch $m_1,\dots,m_k$. Da $m_i \in \bigcup_{n=1}^{\infty} M_n$, gibt es n_i mit $m_i \in M_{n_i}$.

Sei $\ell \geq \max\{n_1,\ldots,n_k\}$. Dann gilt $m_i \in M_\ell$ für $1 \leq i \leq k$; also ist $N = M_\ell$ für alle $\ell \geq \max\{n_1,\ldots,n_k\}$. —

Satz 3.25 *Sei* U *ein Untermodul eines Moduls* M. *Dann gilt:*
M *ist noethersch* $\iff$ M/U *und* U *sind noethersch.*

Beweis: "$\Rightarrow$": Jeder Untermodul von U ist ein solcher von M, also endlich. Jeder Untermodul von M/U ist von der Form N/U, wo N ein Untermodul von M mit $U \subset N \subset M$ ist. Da N nach Voraussetzung endlich ist, gilt dies auch für N/U nach 3.14 c).
"$\Leftarrow$": Sei N ein Untermodul von M. Dann ist $N \cap U$ nach Voraussetzung endlich; dies gilt auch für $N/(N\cap U) \simeq (N+U)/U$. Mithin ist N endlich nach 3.14 d). —

Folgerung 3.26 *Sind* M_i $(1 \leq i \leq n)$ *noethersche A-Moduln, so ist auch* $\bigoplus_{i=1}^{n} M_i$ *noethersch. Insbesondere ist* A^n *noethersch, wenn* A *ein noetherscher Ring ist.*

Beweis: Induktion nach n. Es ist $\left(\bigoplus_{i=1}^{n} M_i\right)/M_n \simeq \bigoplus_{i=1}^{n-1} M_i$, und man kann Satz 3.25 auf $M_n \subset \bigoplus_{i=1}^{n} M_i$ anwenden. —

Satz 3.27 *Ist* A *ein noetherscher Ring, so ist jeder endliche A-Modul* M *noethersch.*

Beweis: $M \simeq A^n/U$ (3.14 b)). A^n ist noethersch nach 3.26, also M nach 3.25. —

Folgerung 3.28 *Ist* A *ein noetherscher Ring,* $\mathfrak{a}$ *ein Ideal von* A, *so ist* $A/\mathfrak{a}$ *ein noetherscher Ring.*

Beweis: Nach 3.27 ist $A/\mathfrak{a}$ noetherscher A-Modul, deswegen auch noetherscher $A/\mathfrak{a}$-Modul. —

Tiefer liegt der folgende

Satz 3.29 (*Hilbertscher Basissatz*): *Wenn* A *ein noetherscher Ring ist, so ist auch der Polynomring* A[X] *noethersch.*

Zum Beweis zeigen wir: Ist A[X] nicht noethersch, so auch A nicht. Sei nämlich $\mathfrak{a}$ ein Ideal in A[X], welches nicht endlich erzeugt ist,

und $f_1 \in \mathfrak{a} - (0)$ ein Element niedrigsten Grades. Da $\mathfrak{a}$ nicht endlich erzeugt ist, folgt $\mathfrak{a}-f_1A[X] \neq \emptyset$. Sei $f_2 \in \mathfrak{a} - f_1A[X]$ wieder vom niedrigsten Grad, usw.:
Sind $f_1,\dots,f_n \in A[X]$ auf diese Weise gewählt, ist
$\mathfrak{a} - (f_1A[X] + \dots + f_nA[X]) \neq \emptyset$, da $\mathfrak{a}$ nicht endlich erzeugt ist.
Wähle f_{n+1} aus $\mathfrak{a} - (f_1A[X] + \dots + f_nA[X])$ von niedrigstem Grad. Wir erhalten eine Folge $f_1,f_2,\dots,f_{n+1},\dots$ in $\mathfrak{a}$. Sei $n_i := \text{grad } f_i$ und a_i der höchste Koeffizient von f_i. Nach Konstruktion der Folge gilt $n_1 \le n_2 \le \dots$.
Behauptung: $Aa_1 \subsetneqq Aa_1 + Aa_2 \subsetneqq Aa_1 + Aa_2 + Aa_3 \subsetneqq \dots$ ist eine nicht stationär werdende Kette von Idealen in A. Wäre nämlich
$Aa_1 + \dots + Aa_r = Aa_1 + \dots + Aa_r + Aa_{r+1}$, so $a_{r+1} = \sum_{i=1}^{n} b_ia_i$, $b_i \in A$.
Betrachte nun $g = f_{r+1} - \sum_{i=1}^{r} b_if_iX^{n_{r+1}-n_i}$ $(n_{r+1} \ge n_i\ (1 \le i \le r)!)$.
Es wäre $g \in \mathfrak{a}$, aber $g \notin \sum_{i=1}^{r} f_iA[X]$, da $f_{r+1} \notin f_1A[X]+\dots+f_rA[X]$.
Ferner wäre $\text{grad } g \le n_{r+1}$ und wegen $a_{r+1} - \sum_{i=1}^{r} b_ia_i = 0$ sogar $\text{grad } g < n_{r+1}$ im Widerspruch zur Wahl von f_{r+1} (minimaler Grad!). –

Folgerung 3.30 *Ist* A *noethersch,* $\mathfrak{a}$ *ein Ideal in* $A[X_1,\dots,X_n]$ *so ist* $B = A[X_1,\dots,X_n]/\mathfrak{a}$ *noethersch. D.h. wenn* $\varphi: A \longrightarrow B$ *ein Ringhomomorphismus ist, derart daß* B *von* $\varphi(A)$ *und einer endlichen Menge erzeugt ist, dann ist mit* A *auch* B *noethersch.*
Beweis: Induktion über die Zahl der Unbestimmten, dann 3.28. –
3.31 (Weitere) Beispiele für nicht-noethersche Ringe:

a) Ring der ganzen Funktionen $\mathbb{C} \longrightarrow \mathbb{C}$. Die Ideale
$\mathfrak{a}_n = \{f \text{ ganz} \mid f(z) = 0 \ \forall z \in \mathbb{N},\ z > n\}$ bilden eine strikt aufsteigende Folge von Idealen (Weierstraßscher Produktsatz). Dieser Ring ist ein Beispiel für einen nicht noetherschen Unterring eines noetherschen Ringes, nämlich seines Quotientenkörpers.

b) Ring der auf $[0,1]$ stetigen reellwertigen Funktionen; betrachte
$\mathfrak{a}_n = \{f \mid f \text{ stetig auf } [0,1],\ f(x) = 0 \ \forall x \in [0,\frac{1}{n}]\}$.

3. Brüche in Moduln

Es seien A ein Ring, $S \subset A$ multiplikativ, und M ein A-Modul.
In $S\times M = \{(s,m) \mid s \in S,\ m \in M\}$ betrachte man die Relation
"$\sim$": $(s,m) \sim (s',m') :\iff \exists\, t \in S$ mit $ts'm = tsm'$. Man zeigt, wie in §2, daß "$\sim$" eine Äquivalenzrelation ist.

Definition und Satz 3.32 $S^{-1}M := S\times M/\sim$ *heißt Bruch- oder Quotientenmodul von* M *nach der Menge* S. *Mit* $\frac{m}{s}$ *bezeichnet man die Äquivalenzklasse von* (s,m). *Vermöge* $\frac{a}{s}\cdot\frac{m}{t} := \frac{am}{st}$, $\frac{m}{s}+\frac{m'}{s'} := \frac{ms'+m's}{ss'}$ *ist* $S^{-1}M$ *ein* $S^{-1}A$*-Modul.*

Daß die Definitionen sinnvoll sind (also unabhängig von der Wahl der Repräsentanten), zeigt man wie in 2.2. –
Analog wie in §2 definiert man $i_{M,S}: M \longrightarrow S^{-1}M$ und für Primideale $\mathfrak{p}$ von A den $A_{\mathfrak{p}}$-Modul $M_{\mathfrak{p}}$.

Bemerkungen 3.33 a) $S^{-1}M$ ist natürlich vermöge $A \xrightarrow{i_{A,S}} S^{-1}A$ auch ein A-Modul.

b) $S^{-1}\left(\bigoplus_{i\in I} M_i\right) \simeq \bigoplus_{i\in I} S^{-1}M_i$. (Hauptnenner!)

Satz 3.34 *Sei* $\varphi: M \longrightarrow N$ A*-linear,* $S \subset A$ *multiplikativ. Dann gibt es genau eine* $S^{-1}A$*-lineare Abbildung* $S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$, *so daß das Diagramm*

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "i_{M,S}"'] & N \arrow[d, "i_{N,S}"] \\ S^{-1}M \arrow[r, dashed, "S^{-1}\varphi"'] & S^{-1}N \end{tikzcd}$$

kommutativ wird, d.h. $S^{-1}\varphi\circ i_{M,S} = i_{N,S}\circ\varphi$ *gilt.*

Zum Beweis setze man $S^{-1}\varphi(\frac{m}{s}) := \frac{\varphi(m)}{s}$. Wegen der Forderung der $S^{-1}A$-Linearität und der Kommutativität des Diagramms muß man das tun:
$S^{-1}\varphi(\frac{m}{s}) = S^{-1}\varphi(\frac{1}{s}\cdot\frac{m}{1}) = \frac{1}{s}S^{-1}\varphi(\frac{m}{1}) = \frac{1}{s}(S^{-1}\varphi\circ i_{M,S})(m) = \frac{1}{s}(i_{N,S}\circ\varphi)(m) =$
$\frac{1}{s}\frac{\varphi(m)}{1} = \frac{\varphi(m)}{s}$. Ferner ist $S^{-1}\varphi$ wohldefiniert: Ist $(s,m)\sim(s',m')$, so gibt es $t\in S$ mit $ts'm = tsm'$, also $ts'\varphi(m) = ts\varphi(m')$. Es folgt $S^{-1}\varphi(\frac{m}{s}) = \frac{\varphi(m)}{s} = \frac{\varphi(m')}{s'} = S^{-1}\varphi(\frac{m'}{s'})$. Schließlich ist $S^{-1}\varphi$ eine $S^{-1}A$-lineare Abbildung: $\frac{a}{s'}\cdot S^{-1}\varphi(\frac{m}{s}) = \frac{a}{s'}\cdot\frac{\varphi(m)}{s} = \frac{a\varphi(m)}{ss'} = \frac{\varphi(am)}{ss'} = S^{-1}\varphi(\frac{am}{ss'})$.
$S^{-1}\varphi(\frac{m_1}{s_1}+\frac{m_2}{s_2}) = S^{-1}\varphi(\frac{s_2m_1+s_1m_2}{s_1s_2}) = \frac{\varphi(s_2m_1+s_1m_2)}{s_1s_2} = \frac{s_2\varphi(m_1)+s_1\varphi(m_2)}{s_1s_2} =$
$= \frac{\varphi(m_1)}{s_1}+\frac{\varphi(m_2)}{s_2} = S^{-1}\varphi(\frac{m_1}{s_1}) + S^{-1}\varphi(\frac{m_2}{s_2})$. Das Diagramm kommutiert:

$(S^{-1}\varphi)\circ i_{M,S}(m) = (S^{-1}\varphi)(\frac{m}{1}) = \frac{\varphi(m)}{1} = i_{N,S}(\varphi(m)) = (i_{N,S}\circ\varphi)(m)$. –

Bemerkung 3.35 a) $S^{-1}(id_M) = id_{S^{-1}M}$.

b) $S^{-1}(\varphi\circ\psi) = S^{-1}(\varphi)\circ S^{-1}(\psi)$.

Die Aussagen a) und b) besagen, daß die Abbildung, die jedem A-Modul M den $S^{-1}A$-Modul $S^{-1}M$ und jeder A-linearen Abbildung φ die $S^{-1}A$-lineare Abbildung $S^{-1}\varphi$ zuordnet, ein sogenannter Funktor ist.
Weitere Beispiele von Funktoren folgen in späteren Paragraphen.

Definition 3.36 Sei $\ldots \longrightarrow M_n \xrightarrow{\varphi_n} M_{n+1} \xrightarrow{\varphi_{n+1}} M_{n+2} \longrightarrow \ldots$ eine (endliche oder unendliche) Folge von A-Modulhomomorphismen. Sie heißt exakt, wenn $\operatorname{Im}\varphi_n = \operatorname{Ker}\varphi_{n+1}$ für alle (vorkommenden) n ist.

Bemerkungen 3.37 (Mit 0 sei der Nullmodul bezeichnet.) Es gilt:

a) $0 \longrightarrow M \xrightarrow{f} N$ ist exakt $\Longleftrightarrow$ f ist injektiv.

b) $M \xrightarrow{f} N \longrightarrow 0$ ist exakt $\Longleftrightarrow$ f ist surjektiv.

c) $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ ist exakt $\Longleftrightarrow$ f ist ein Isomorphismus.

d) $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ ist exakt $\Longleftrightarrow$ f ist injektiv, g surjektiv und g induziert einen Isomorphismus von $M/f(M')$ mit M''. D.h. M' kann mit einem Untermodul von M und M'' mit dem Faktormodul nach diesem identifiziert werden. Umgekehrt: Ist U ein Untermodul von M , so bilden die kanonischen Homomorphismen $0 \longrightarrow U \longrightarrow M \longrightarrow M/U \longrightarrow 0$ eine exakte Folge.

Satz 3.38 *Sei* S *eine multiplikative Teilmenge des Ringes* A *und* $M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ *eine exakte Folge von A-Modulhomomorphismen, so ist auch* $S^{-1}M_1 \xrightarrow{S^{-1}\alpha} S^{-1}M_2 \xrightarrow{S^{-1}\beta} S^{-1}M_3$ *exakt.*

Beweis: (1) $S^{-1}\beta\circ S^{-1}\alpha = S^{-1}(\beta\circ\alpha) = S^{-1}(0) = 0$, also $\operatorname{Im} S^{-1}\alpha \subset \operatorname{Ker} S^{-1}\beta$.

(2) Sei $\frac{m}{s} \in \operatorname{Ker}(S^{-1}\beta)$, d.h. es gibt ein $t \in S$ mit $t\beta(m) = 0$, also $\beta(tm) = 0$. Nach Voraussetzung existiert ein $n \in M_1$ mit $\alpha(n) = tm$. Dann ist $S^{-1}\alpha\,(\frac{n}{st}) = \frac{\alpha(n)}{st} = \frac{tm}{st} = \frac{m}{s}$, d.h. $\frac{m}{s} \in \operatorname{Im}(S^{-1}\alpha)$. –

Folgerung 3.39 *Wenn* U *ein A-Untermodul von* M *ist, so kann man auf kanonische Weise* $S^{-1}U$ *als* $S^{-1}A$*-Untermodul von* $S^{-1}M$ *auffassen. Man hat dann einen kanonischen Isomorphismus* $S^{-1}(M/U) \simeq S^{-1}M/S^{-1}U$. –

Beachte: Wenn $\mathfrak{a}$ ein Ideal von A ist, stimmt die hier gegebene Definition von $S^{-1}\mathfrak{a}$ mit der Definition 2.12 überein.

Satz 3.40 *Wenn* M *ein endlicher (bzw. noetherscher)* A-*Modul ist, so ist* $S^{-1}M$ *ein endlicher (bzw. noetherscher)* $S^{-1}A$-*Modul. Insbesondere ist* $S^{-1}A$ *ein noetherscher Ring, wenn* A *ein solcher ist.*

Beweis: Wenn M von $x_1,\dots,x_n$ über A erzeugt wird, so ist $\frac{x_1}{1},\dots,\frac{x_n}{1}$ offenbar ein Erzeugendensystem von $S^{-1}M$ über $S^{-1}A$. Zum Beweis, daß mit M auch $S^{-1}M$ noethersch ist, genügt es daher, folgendes zu zeigen:

Lemma 3.41 *Jeder* $S^{-1}A$-*Untermodul* N *von* $S^{-1}M$ *ist von der Form* $S^{-1}U$ *mit einem* A-*Untermodul* U *von* M.

Beweis hierfür: Wähle $U = i_{M,S}^{-1}(N)$. Wenn $x \in U$, ist $\frac{x}{1} \in N$, also $\frac{x}{s} = \frac{1}{s}\cdot\frac{x}{1} \in N$. Mithin ist $S^{-1}U \subset N$. Wenn $\frac{x}{s} \in N$, ist $\frac{x}{1} = \frac{s}{1}\cdot\frac{x}{s} \in N$, also $x \in U$ und $\frac{x}{s} \in S^{-1}U$. Somit ist $N \subset S^{-1}U$. –

Definition 3.42 Ein Element $a \in A$ heißt ein Nichtnullteiler für den A-Modul M, wenn $am \neq 0$ für alle $m \in M - \{0\}$ ist. Andernfalls heißt a ein Nullteiler für M.

Bemerkung 3.43 Wenn S aus lauter Nichtnullteilern für den A-Modul M besteht, ist $i_{M,S}\colon M \longrightarrow S^{-1}M$ injektiv (und umgekehrt).

Beweis: $i_{M,S}(m) = \frac{m}{1} = 0 \iff \exists\, t \in S$ mit $tm = 0$. Da t Nichtnullteiler für M ist, folgt $m = 0$. –

Satz 3.44 *Für einen* A-*Modul* M *sind äquivalent:*

(i) $M = 0$,

(ii) $M_{\mathfrak{m}} = 0$ *für jedes maximale Ideal* $\mathfrak{m}$ *von* A.

Beweis: "$\Rightarrow$" ist trivial. "$\Leftarrow$": Annahme: $M \neq 0$. Dann ist zu zeigen: Für mindestens ein maximales Ideal $\mathfrak{m}$ von A gilt $M_{\mathfrak{m}} \neq 0$. Sei also $m \in M - \{0\}$. $N := Am \subset M$. Es genügt, zu zeigen: $N_{\mathfrak{m}} \neq 0$ für mindestens ein maximales Ideal $\mathfrak{m}$ von A (Folgerung 3.39). N ist monogen, also $N \simeq A/\mathfrak{a}$ (Bemerkung 3.10). Sei $\mathfrak{m}$ ein maximales Ideal von A mit $\mathfrak{a} \subset \mathfrak{m}$ (Folgerung 1.16). Man hat einen surjektiven Homomorphismus

$A/\mathfrak{a} \longrightarrow A/\mathfrak{m} =: P$. Es genügt, zu zeigen: $P_\mathfrak{m} \neq 0$, da nach 3.38 $N_\mathfrak{m} \longrightarrow P_\mathfrak{m}$ surjektiv ist. Alle Elemente aus $S = A-\mathfrak{m}$ sind Nichtnullteiler für $A/\mathfrak{m} = P$, da $A/\mathfrak{m}$ ein Körper ist. Deshalb ist $i_{P,S}: P \longrightarrow P_\mathfrak{m}$ injektiv (3.43), und $P \neq 0$ impliziert $P_\mathfrak{m} \neq 0$.

Folgerung 3.45 *Eine A-lineare Abbildung* $\varphi: M \longrightarrow N$ *von A-Moduln ist genau dann injektiv (bzw. surjektiv, bzw. bijektiv, bzw. Null), wenn* $\varphi_\mathfrak{m}$ *es ist für jedes maximale Ideal* $\mathfrak{m}$ *in* A. ($\varphi_\mathfrak{m} := S^{-1}\varphi$ für $S = A-\mathfrak{m}$.)

Beweis: "$\Rightarrow$" 3.38. Beachte: $\varphi = 0 \iff M \xrightarrow{\varphi} N \xrightarrow{id} N$ exakt.

"$\Leftarrow$" Injektivität: Setze $K := \operatorname{Ker}(\varphi)$. Man erhält die exakte Folge $0 \longrightarrow K \longrightarrow M \xrightarrow{\varphi} N$. Nach 3.38 ist dann $0 \longrightarrow K_\mathfrak{m} \longrightarrow M_\mathfrak{m} \xrightarrow{\varphi_\mathfrak{m}} N_\mathfrak{m}$ exakt. Da $\varphi_\mathfrak{m}$ für jedes maximale Ideal $\mathfrak{m}$ von A injektiv ist, ist $K_\mathfrak{m} = 0$ für jedes solche $\mathfrak{m}$. Aus dem Satz folgt $K = 0$, d.h. φ injektiv. Surjektivität: Setze $K := \operatorname{Coker} \varphi$ und schließe mit der exakten Folge $M \xrightarrow{\varphi} N \longrightarrow K \longrightarrow 0$ wie oben. Um $\varphi = 0$ zu zeigen, setze wieder $K = \operatorname{Ker} \varphi$. Die Exaktheit von $0 \longrightarrow K_\mathfrak{m} \longrightarrow M_\mathfrak{m} \xrightarrow{\varphi_\mathfrak{m}} N_\mathfrak{m}$ besagt, daß $K_\mathfrak{m}$ auf kanonische Weise mit $\operatorname{Ker} \varphi_\mathfrak{m}$ identifiziert werden kann. Da $\varphi_\mathfrak{m} = 0$ ist, ist $K_\mathfrak{m} = M_\mathfrak{m}$, d.h. $(M/K)_\mathfrak{m} \simeq M_\mathfrak{m}/K_\mathfrak{m} = 0$ - und das für alle maximalen Ideale $\mathfrak{m}$. Es folgt $M/K = 0$, d.h. $M = \operatorname{Ker} \varphi$, also $\varphi = 0$. –

Folgerung 3.46 *Sei* U *ein Untermodul von* M *und* $x \in M$. *Dann gilt:*
$x \in U \iff i_{M,\mathfrak{m}}(x) \in U_\mathfrak{m}$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* A.

Beweis: Definiere $\varphi: A \longrightarrow M/U$ durch $\varphi(1) := x+U$. Dann gilt: $\varphi = 0 \iff x \in U$. Wende 3.45 an. –

Das sogenannte "Lokal-Global-Prinzip" der kommutativen Algebra ist im wesentlichen der Inhalt des Satzes 3.44 und der beiden obigen Folgerungen.

Folgerung 3.47 *Sei* A *ein Integritätsring,* K *sein Quotientenkörper. Wenn man* A *und die Lokalisierungen* $A_\mathfrak{m}$ *gemäß 2.6 als Unterringe von* K *auffaßt, ist* $A = \bigcap_{\substack{\mathfrak{m}\ \text{max.} \\ \text{Ideal}}} A_\mathfrak{m}$.

Beweis: Sei $x \in K$. Wenn man $A_\mathfrak{m}$ als Unterring von K auffaßt, bedeutet $i_{A,\mathfrak{m}}(x) \in A_\mathfrak{m}$ nichts anderes als $x \in A_\mathfrak{m}$. Die Behauptung folgt also aus 3.46. –

Aufgaben und Hinweise

Im folgenden sei A ein Ring.

1) a) Seien $\mathfrak{a},\mathfrak{b}$ Ideale von A und $A/\mathfrak{a} \simeq A/\mathfrak{b}$ als A-Moduln. Zeige: $\mathfrak{a} = \mathfrak{b}$. (N.B.: Dies gilt i.a. nicht für Linksideale $\mathfrak{a},\mathfrak{b}$ eines nichtkommutativen Ringes, z.B. eines Matrizenringes.)

b) Sei k ein unendlicher Körper. Zeige: Über dem Ring $k[X,Y]/(X^2,XY,Y^2)$ gibt es unendlich viele paarweise nicht-isomorphe monogene Moduln.

2) $A \neq 0$ und $A^r \simeq A^s$ (als A-Moduln) $\Rightarrow$ $r = s$.

(Hinweis: Für ein maximales Ideal $\mathfrak{m}$ schließe $(A/\mathfrak{m})^r \simeq A^r/\mathfrak{m}A^r \simeq A^s/\mathfrak{m}A^s \simeq (A/\mathfrak{m})^s$.)
(N.B.: Auch dies gilt i.a. nicht für nichtkommutative Ringe, z.B. nicht für den Endomorphismenring eines unendlich-dimensionalen Vektorraumes.)

3) Sei F ein freier A-Modul und $f\colon M \longrightarrow F$ ein surjektiver A-Modulhomomorphismus. Zeige: Es gibt eine A-lineare Abbildung $g\colon F \longrightarrow M$ mit $f \circ g = \mathrm{id}_F$; d.h. $M \simeq F \oplus \operatorname{Ker}(f)$.

4) A sei ein Hauptidealring und $n \in \mathbb{N}$. Zeige: Jeder Untermodul von A^n ist frei. (Hinweis: Induktion nach n. Sei $p\colon A^n \longrightarrow A$ die Projektion auf den letzten Summanden. Für einen Untermodul U von A^n ist $p(U) \simeq A$ oder 0. Nach Induktionsannahme ist $\operatorname{Ker} p$ frei. Wende Aufgabe 3) an.)
(Für freie A-Moduln mit unendlicher Basis ist obige Behauptung auch richtig. Siehe 10.26.)

5) Seien U, E_1, E_2 Untermoduln eines Moduls M. Es gelte:

a) $E_1 \subset E_2$, b) $E_1 \cap U = E_2 \cap U$, c) $E_1 + U = E_2 + U$.
Zeige: $E_1 = E_2$.

6) Ein Modul heißt artinsch, wenn jede absteigende Folge von Untermoduln stationär wird.

a) Sei U ein Untermodul eines Moduls M. Zeige (mit Aufgabe 5): M artinsch $\iff$ M/U und U artinsch.
(N.B.: Satz 3.25 läßt sich natürlich ebenfalls mit Hilfe der Aufgabe 5) beweisen.)

b) Sei p eine Primzahl. Die Menge $\left\{e^{2m\pi i/p^n} \mid m,n \in \mathbb{N}\right\}$ ist eine (multiplikativ geschriebene) artinsche Gruppe ($\mathbb{Z}$-Modul).

7) Für eine Familie $(M_i)_{i\in I}$ von A-Moduln definiert man das direkte Produkt $\prod_{i\in I} M_i$ als $\{(m_i)_{i\in I} \mid m_i \in M_i\}$. Für eine endliche Indexmenge I stimmt das direkte Produkt mit der direkten Summe überein. Im allgemeinen gilt $\bigoplus_{i\in I} M_i \subset \prod_{i\in I} M_i$.

   a) Zeige (analog zu 3.18): Zu Homomorphismen $N \longrightarrow M_i$ gehört auf naheliegende Weise ein Homomorphismus $N \longrightarrow \prod_{i\in I} M_i$.

   b) Sei P die Menge der Primzahlen. Betrachte den $\mathbb{Z}$-Modul $M := \prod_{p\in P} (\mathbb{Z}/(p)) / \bigoplus_{p\in P} (\mathbb{Z}/(p))$. Zeige: Jedes $n \in \mathbb{Z} - \{0\}$ operiert $(x \longmapsto nx)$ bijektiv auf M. Mit anderen Worten: M ist ein $\mathbb{Q}$-Vektorraum (übrigens von überabzählbarer Dimension).

   c) Gib (mit Hilfe von a)) einen kanonischen Homomorphismus $S^{-1}(\prod M_i) \longrightarrow \prod(S^{-1}M_i)$ an. Dieser ist im allgemeinen weder injektiv (b)), noch surjektiv.

8) Im allgemeinen sind Moduln schwer, wenn nicht unmöglich zu klassifizieren. Eine zufriedenstellende Theorie gibt es für endlich erzeugte Moduln über Hauptidealringen. Siehe [Lang], Chap XV, §2.

9) Wenn A ein noetherscher Ring ist, ist auch der Ring $A[\![X]\!]$ der formalen Potenzreihen über A noethersch. (18.32) u. [Bourbaki], Chap. III, §2, no. 10. (Eine formale Potenzreihe ist eine - i.a. nicht endliche - formale Summe $\sum_{i=0}^{\infty} a_i X^i$. Das Produkt zweier solcher ist das Cauchy-Produkt.) Gleiches gilt für gewisse Ringe holomorpher Funktionen (siehe: [Langmann], [Grauert-Remmert] §2, Satz 1).

10) Ein Ring, in dem sämtliche Primideale endlich erzeugt sind, ist noethersch. Siehe [Cohen] oder [Kaplansky, 1-1, Thm. 8]. Für eine Verfeinerung siehe [Lafon. 2, Thm II. 2].

11) Jeder Ring A ist eine filtrierte Vereinigung noetherscher Unterringe. D.h. es gibt eine Menge $\mathfrak{M}$ von noetherschen Unterringen von A mit den Eigenschaften:

   a) $\bigcup_{B\in\mathfrak{M}} B = A$;

   b) $B_1, B_2 \in \mathfrak{M} \Rightarrow \exists\, B_3 \in \mathfrak{M}$ mit $B_1 \cup B_2 \subset B_3$.

(Sei B_0 der Primring in A, d.h. das Bild des einzig möglichen Ringhomomorphismus $\mathbb{Z} \longrightarrow A$.
Wähle $\mathfrak{M} = \{B_0[E] \mid E$ endliche Teilmenge von $A\}$.)

12) Seien U_1, U_2 Untermoduln eines A-Moduls M. Zeige: Wenn M/U_1 und M/U_2 (bzw. U_1 und U_2) noethersch sind, so ist dies auch $M/(U_1 \cap U_2)$ (bzw. U_1+U_2). Insbesondere gilt also: Wenn zwei Faktorringe $A/\mathfrak{a}_1$ und $A/\mathfrak{a}_2$ noethersch sind, gilt dies auch für $A/(\mathfrak{a}_1 \cap \mathfrak{a}_2)$.

13) Auch über nichtkommutativen Ringen kann man Moduln definieren. Wenn man Definition 3.1 formal überträgt, spricht man von Linksmoduln. Wenn man in der Definition 3.1 die Regel (iii) durch

$$\text{(iii')} \qquad (a_1a_2)m = a_2(a_1m)$$

ersetzt, spricht man von Rechtsmoduln. In diesem Falle schreibt man in der Regel "ma" statt "am", damit (iii') wieder die Form eines Assoziativgesetzes bekommt:

$$m(a_1a_2) = (ma_1)a_2 .$$

Man kann einen Ring A sowohl als Links- wie als Rechtsmodul über sich betrachten. Schreibweise ${}_AA$ bzw. A_A. Die Untermoduln von ${}_AA$ (bzw. A_A) heißen Links- (bzw. Rechts-) Ideale.
Die Kerne von Ringhomomorphismen sind sowohl Links- wie Rechts-Ideale (sogenannte zweiseitige Ideale). Die Sätze der ersten beiden Abschnitte lassen sich auf nichtkommutative Ringe übertragen. Satz 3.27 z.B. bekommt die Form: Ist A ein linksnoetherscher Ring (d.h. ${}_AA$ ein noetherscher Modul), so ist jeder endliche Links-A-Modul M noethersch. Zu 3.19 beachte: Der Durchschnitt aller maximalen Linksideale ist gleich dem aller maximalen Rechtsideale und gleich dem aller maximalen zweiseitigen Ideale. Vgl. [Bourbaki: A], chap. VIII, §6.3.

§4 ASSOZIIERTE PRIMIDEALE, TRÄGER, PRIMÄRZERLEGUNG, MODULN VON ENDLICHER LÄNGE

1. $\mathrm{Ass}_A(M)$ und $\mathrm{Supp}_A(M)$

Definition 4.1 Es sei M ein A-Modul.
$\mathrm{Ann}_A(M) := \{a \in A \mid am = 0 \ \ \forall\, m \in M\}$ heißt der Annullator von M.
Für ein $m \in M$ heißt $\mathrm{Ann}_A(m) = \{a \in A \mid am = 0\}$ der Annullator von m.
(Man schreibt auch $\mathrm{Ann}(M)$ bzw. $\mathrm{Ann}(m)$.)

Im Sinne dieser Definition bestehen die Nichtnullteiler eines A-Moduls M aus $A - \bigcup\limits_{\substack{m\in M\\ m\neq 0}} \mathrm{Ann}(m)$.

Satz 4.2 *a)* $\mathrm{Ann}_A(M)$ *und* $\mathrm{Ann}_A(m)$ *sind Ideale.*
b) Maximale Elemente der Menge $\{\mathrm{Ann}(m) \mid m \in M - \{0\}\}$ *sind Primideale.*

Beweis: Nur bei b) ist etwas zu zeigen. Sei also $\mathfrak{p} = \mathrm{Ann}(m)$ maximal, $a,b \in A$ mit $ab \in \mathfrak{p}$, $b \notin \mathfrak{p}$. Da $b \notin \mathfrak{p}$, gilt $bm \neq 0$. Man betrachte nun $\mathfrak{a} := \mathrm{Ann}(bm)$. Für $p \in \mathfrak{p}$ gilt $p(bm) = b(pm) = 0$; somit ist $\mathfrak{p} \subset \mathfrak{a}$. Wegen der Maximalität von $\mathfrak{p}$ hat man $\mathfrak{p} = \mathfrak{a}$. Da $abm = 0$, folgt $a \in \mathfrak{a} = \mathfrak{p}$. –

Definition 4.3 $\mathrm{Ass}_A(M) := \left\{\mathfrak{p} \mid \mathfrak{p} \subset A \text{ prim}, \exists\, m \in M \text{ mit } \mathfrak{p} = \mathrm{Ann}(m)\right\}$.
Die Elemente von $\mathrm{Ass}_A(M)$ heißen die zu M assoziierten Primideale.
(Man schreibt auch $\mathrm{Ass}(M)$.)

Bemerkungen 4.4 a) $Am \simeq A/\mathrm{Ann}(m)$ (als A-Moduln!).
Deshalb liegt ein Primideal $\mathfrak{p}$ genau dann in $\mathrm{Ass}_A(M)$, wenn es eine injektive A-lineare Abbildung $A/\mathfrak{p} \hookrightarrow M$ gibt.

b) $\mathrm{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$. Es gilt sogar $\mathrm{Ass}_A U = \{\mathfrak{p}\}$, wenn U ein von 0 verschiedener Untermodul von $A/\mathfrak{p}$ ist. (Für $x \in A/\mathfrak{p}-\{\overline{0}\}$ ist $\mathrm{Ann}_A(x) = \mathfrak{p}$.)

Folgerung 4.5 *Sei* A *noethersch,* M *ein* A*-Modul. Dann sind äquivalent:*
(i) $M = 0$.
(ii) $\mathrm{Ass}_A(M) = \emptyset$.

Beweis: Nur die Richtung (ii) $\Rightarrow$ (i) ist nicht unmittelbar klar. Ist M nicht der Nullmodul, so ist die Menge $\mathfrak{M} := \{\mathrm{Ann}(m) \mid m \in M - \{0\}\}$ von

Idealen in A nicht leer. Da A noethersch ist, besitzt $\mathfrak{M}$ maximale Elemente, die nach Satz 4.2 prim und deshalb Elemente von $Ass_A(M)$ sind. –

Folgerung 4.6 *Sei A noethersch, M ein A-Modul. Dann ist die Menge der Nullteiler für M die Vereinigung seiner assoziierten Primideale.*

Beweis: Für ein $a \in \mathfrak{p} \in Ass_A(M)$ mit $\mathfrak{p} = Ann_A(m)$ gilt $am = 0$, also ist a Nullteiler. Andererseits, für einen Nullteiler a für M gibt es ein $m \in M$, $m \neq 0$ mit $am = 0$. Nach 4.2 b) gibt es ein $\mathfrak{p} \in Ass_A(M)$ mit $Ann_A(m) \subset \mathfrak{p}$. –

Folgerung 4.7 *Sei A noethersch, M ein endlicher A-Modul. Dann gibt es eine "Kompositionsreihe"*

$$0 = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_{n-1} \subset M_n = M \quad \textit{mit} \quad M_i/M_{i-1} \simeq A/\mathfrak{p}_i \ ,$$

wobei $\mathfrak{p}_i$ gewisse Primideale von A sind.

Zum Beweis darf man $M \neq 0$ annehmen. Nach 4.5 b) gibt es ein Primideal $\mathfrak{p}_1 \in Ass_A(M)$, also ein $m \in M$ mit $Ann_A(m) = \mathfrak{p}_1$. Setze $M_1 := Am \simeq A/\mathfrak{p}_1$. Wenn $M \neq M_1$ ist, findet man auf dieselbe Weise einen Untermodul M_2/M_1 von M/M_1, der isomorph zu $A/\mathfrak{p}_2$ mit einem Primideal $\mathfrak{p}_2$ ist, usw. Da M noethersch ist, bricht dieses Verfahren nach endlich vielen Schritten mit $M_n = M$ ab. –

Beispiel 4.8 Für den $\mathbb{Z}$-Modul $\mathbb{Z}$ ist $0 \subset 6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$ ist eine Kompositionsreihe der obigen Art, aber auch $0 \subset \mathbb{Z}$.
I.a. liegt also keine Eindeutigkeit vor!

Satz 4.9 *Seien $N \subset M$ A-Moduln. Dann gilt:*

$$Ass_A(N) \subset Ass_A(M) \subset Ass_A(N) \cup Ass_A(M/N) \ .$$

Beweis: $Ass_A(N) \subset Ass_A(M)$ ist nach Definition unmittelbar klar.
Sei $\mathfrak{p} \in Ass_A(M)$ und E ein Untermodul von M, isomorph zu $A/\mathfrak{p}$. Im Falle $E \cap N \neq \{0\}$ ist $\{\mathfrak{p}\} \overset{(4.4)}{=} Ass(E \cap N) \subset Ass\, N$. Wenn aber $E \cap N = \{0\}$ ist, ist E isomorph zum Untermodul $(E+N)/N$ von M/N, also $\mathfrak{p} \in Ass(M/N)$. –

Folgerung 4.10 *Seien M ein A-Modul und*
$0 = M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n = 0$ eine Kompositionsreihe, für die $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ mit Primidealen $\mathfrak{p}_i$ ist. Dann gilt $Ass_A(M) \subset \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$.

Beweis: Nach 4.4 b) und 4.9 hat man die Inklusionskette
$\mathrm{Ass}_A(M) \subset \mathrm{Ass}_A(M_{n-1}) \cup \mathrm{Ass}_A(M_n/M_{n-1}) =$
$\mathrm{Ass}_A(M_{n-1}) \cup \{\mathfrak{p}_n\} \subset \mathrm{Ass}_A(M_{n-2}) \cup \mathrm{Ass}_A(M_{n-1}/M_{n-2}) \cup \{\mathfrak{p}_n\} =$
$\mathrm{Ass}_A(M_{n-2}) \cup \{\mathfrak{p}_{n-1}\} \cup \{\mathfrak{p}_n\} \subset \ldots \subset \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$. –

Ist M ein endlicher Modul über dem noetherschen Ring A, so ist also $\mathrm{Ass}_A(M)$ nach Folgerung 4.10 endlich.

Satz 4.11 *Ist* A *noethersch,* $S \subset A$ *multiplikativ und* M *ein* A*-Modul, so gilt*

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}M) = \left\{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}_A M\ ,\ \mathfrak{p} \cap S = \emptyset\right\} .$$

Beweis: "$\supset$": Sei $\mathfrak{p} \in \mathrm{Ass}_A(M)$, $\mathfrak{p} = \mathrm{Ann}_A(m)$, $\mathfrak{p} \cap S = \emptyset$. Setze $\mathfrak{a} := \mathrm{Ann}_{S^{-1}A}(\frac{m}{1})$. Dann gilt $\mathfrak{a} = S^{-1}\mathfrak{p}$, denn man hat die Äquivalenzen:
$\frac{a}{s} \cdot \frac{m}{1} = \frac{0}{1} \iff \exists\, t \in S\colon tam = 0 \iff \exists\, t \in S\colon ta \in \mathfrak{p} \iff a \in \mathfrak{p}$, letzteres, da $\mathfrak{p}$ prim ist.

"$\subset$": Sei $\mathfrak{q} = \mathrm{Ann}_{S^{-1}A}(\frac{m}{s})$ $(s \in S)$. Nach 2.13 gilt $\mathfrak{q} = S^{-1}\mathfrak{p}$ für ein Primideal $\mathfrak{p}$ von A mit $\mathfrak{p} \cap S = \emptyset$. Da A noethersch ist, gibt es $p_1,\ldots,p_r \in \mathfrak{p}$ mit $\mathfrak{p} = Ap_1 + \ldots + Ap_r$, und es gilt $\frac{p_i}{1} \cdot \frac{m}{s} = 0$ $(1 \le i \le r)$. Es gibt also $t_i \in S$ $(1 \le i \le r)$ mit $t_i p_i m = 0$, also mit $t := \prod_{i=1}^{r} t_i \in S$ folgt $tp_i m = 0$. Man hat $\mathfrak{p} \subset \mathrm{Ann}_A(tm)$. Ist andererseits $atm = 0$, mithin $\frac{a}{1}\frac{tm}{ts} = 0$, also $\frac{a}{1} \in S^{-1}\mathfrak{p}$, so gibt es eine Darstellung $\frac{a}{1} = \frac{p}{s'}$ mit $p \in \mathfrak{p}$, $s' \in S$. Deshalb gibt es ein $s'' \in S$ mit $s's''a = s''p \in \mathfrak{p}$, und es folgt wegen $S \cap \mathfrak{p} = \emptyset$, daß a in $\mathfrak{p}$ liegt und damit $\mathrm{Ann}_A(tm) \subset \mathfrak{p}$ gilt. Insgesamt haben wir $\mathfrak{p} = \mathrm{Ann}_A(tm)$ mit $S^{-1}\mathfrak{p} = \mathfrak{q}$ gezeigt. –

Definition 4.12 $\mathrm{Supp}_A(M) := \{\mathfrak{p} \mid \mathfrak{p}$ Primideal in A , $M_\mathfrak{p} \neq 0\}$.
$\mathrm{Supp}_A(M)$ heißt der Träger von M . (Man schreibt auch $\mathrm{Supp}(M)$.)

Bemerkung 4.13 $\mathrm{Supp}_A(A) = \mathrm{Spec}\, A = \{\mathfrak{p} \mid \mathfrak{p} \subset A$ Primideal$\}$. Denn für jedes Primideal $\mathfrak{p}$ besitzt $A_\mathfrak{p}$ das maximale Ideal $\mathfrak{p}A_\mathfrak{p} \neq A_\mathfrak{p}$. Also ist $A_\mathfrak{p} \neq 0$.

Satz 4.14 *Für einen endlichen A-Modul M gilt*

$$\mathrm{Supp}_A M = \{\mathfrak{p} \mid \mathfrak{p} \text{ prim},\ \mathfrak{p} \supset \mathrm{Ann}_A M\} \quad (\text{i.a. nur } "\subset"!)$$

Beweis: "$\subset$": Angenommen, es gäbe $\mathfrak{p} \in \mathrm{Supp}_A(M)$ mit $\mathfrak{p} \not\supset \mathrm{Ann}_A(M)$. Sei dann $t \in \mathrm{Ann}_A(M)-\mathfrak{p}$, $\frac{m}{s} \in M_\mathfrak{p}$ beliebig. Es gälte $\frac{m}{s} = \frac{tm}{st} = \frac{0}{st} = 0$, also $M_\mathfrak{p} = 0$ im Widerspruch zu $\mathfrak{p} \in \mathrm{Supp}_A(M)$.

"$\supset$": Ist $M = Am_1 + \ldots + Am_r$, so gilt $\mathrm{Ann}_A(M) = \mathrm{Ann}_A(m_1) \cap \ldots \cap \mathrm{Ann}_A(m_r) \supset \mathrm{Ann}_A(m_1)\cdot\ldots\cdot\mathrm{Ann}_A(m_r)$.

Ist $\mathfrak{p} \supset \mathrm{Ann}_A(M)$, so folgt nach 1.14 (iii), daß $\mathfrak{p} \supset \mathrm{Ann}_A(m_i)$ für ein $i \in \{1,\ldots,r\}$ ist. Mit $\bar{\mathfrak{p}} = \mathfrak{p}/\mathrm{Ann}(m_i)$ folgt $\left(A/\mathrm{Ann}_A(m_i)\right)_\mathfrak{p} \simeq \left(A/\mathrm{Ann}_A(m_i)\right)_{\bar{\mathfrak{p}}} \neq 0$ wegen 4.13; also ist $\left(A/\mathrm{Ann}_A(m_i)\right)_\mathfrak{p} \simeq (Am_i)_\mathfrak{p}$ nach 3.39 ein nichttrivialer Untermodul von $M_\mathfrak{p}$, deshalb auch $M_\mathfrak{p} \neq 0$! —

Satz 4.15 *Sei* A *noethersch,* M *ein* A-*Modul.* M *besitze eine Kompositionsreihe* $0 = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_{n-1} \subset M_n = M$ *mit* $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ *für Primideale* $\mathfrak{p}_i$ *in* A. *Dann gilt:* $\mathrm{Ass}_A(M) \subset \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\} \subset \mathrm{Supp}_A(M)$. *Diese drei Mengen besitzen dieselben minimalen Elemente.*

Beweis: $\mathrm{Ass}_A(M) \subset \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$ gilt nach 4.10.

Wegen $A/\mathfrak{p}_i \simeq M_i/M_{i-1}$ hat man $0 \neq (A/\mathfrak{p}_i)_{\mathfrak{p}_i} \simeq (M_i/M_{i-1})_{\mathfrak{p}_i}$, also wegen (3.39) $(M_i)_{\mathfrak{p}_i} \neq 0$ und damit $M_{\mathfrak{p}_i} \neq 0$. Wir haben $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\} \subset \mathrm{Supp}_A(M)$ gezeigt. Es bleibt zu zeigen: Die minimalen Elemente von $\mathrm{Supp}_A(M)$ liegen in $\mathrm{Ass}_A(M)$. Sei $\mathfrak{p}$ ein solches. Dann ist $\mathrm{Supp}_{A_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}A_\mathfrak{p}\}$ $\left((M_\mathfrak{p})_{\mathfrak{q}_\mathfrak{p}} \simeq M_\mathfrak{q}\right)$. Da $\mathrm{Ass}_{A_\mathfrak{p}} M_\mathfrak{p} \neq \emptyset$, folgt $\mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \{\mathfrak{p}A_\mathfrak{p}\}$, also mit 4.11, daß $\mathfrak{p} \in \mathrm{Ass}_A(M)$ gilt. —

Bemerkung 4.16 Die minimalen Elemente von $\mathrm{Ass}_A(A/\mathfrak{a})$ sind also genau die minimalen Primoberideale von $\mathfrak{a}$. (A noethersch)

Folgerung 4.17 *Ein noetherscher Ring* A *besitzt nur endlich viele minimale Primideale.*

Beweis: Ist nämlich $\mathfrak{p}$ ein minimales Primideal in A, so heißt das: $\mathfrak{p}$ ist minimal in $\mathrm{Supp}_A A$. Also ist $\mathfrak{p}$ minimal in $\mathrm{Ass}_A A$, und $\mathrm{Ass}_A A$ ist nach der Bemerkung im Anschluß an den Beweis von 4.10 endlich. —

2. Primärzerlegung

Dieser Abschnitt wird - von Aufgaben abgesehen - im weiteren Verlauf des Buches nicht benötigt. (Ausnahme: 4.25 wird in §17 verwendet.)

Lemma 4.18 *Es seien* A *ein noetherscher Ring,* M *ein endlicher* A*-Modul und* $a \in A$. *Dann sind äquivalent:*

(*i*) *Die Homothetie* $h_a: M \longrightarrow M$ $(m \longmapsto am)$ *ist nilpotent.*

(*ii*) $a \in \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}$.

Beweis: Da die minimalen Elemente von $\mathrm{Ass}M$ und $\mathrm{Supp}M$ gemäß 4.15 übereinstimmen und diese gleichzeitig die minimalen Primoberideale von $\mathrm{Ann}M$ sind (4.14), gilt $\bigcap_{\mathfrak{p} \in \mathrm{Ass}M} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Supp}M} \mathfrak{p} = \sqrt{\mathrm{Ann}M}$. D.h. $a \in \bigcap_{\mathfrak{p} \in \mathrm{Ass}M} \mathfrak{p}$ ist äquivalent zu $a^n \in \mathrm{Ann}M$ für ein $n \in \mathbb{N}$. –

Satz 4.19 *Es seien* A *ein noetherscher Ring,* M *ein endlicher* A*-Modul. Dann sind äquivalent:*

(*i*) *Für alle* $a \in A$ *ist die Homothetie* $h_a: M \longrightarrow M$ $(m \longmapsto am)$ *entweder injektiv oder nilpotent.*

(*ii*) $\mathrm{Ass}_A M$ *besteht aus genau einem Element.*

Beweis: (i) ist genau dann erfüllt, wenn

$A = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p} \cup \left(A - \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}\right)$ gilt (4.18 und 4.6); das ist genau der Fall, wenn $\bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}$ gilt, und das stimmt genau dann, wenn $\mathrm{Ass}_A(M)$ aus genau einem Element besteht. –

Zusatz 4.20 *Sind* (*i*) *und* (*ii*) *erfüllt, ist*
$\mathrm{Ass}_A(M) = \{\{a \in A \mid h_a \text{ nilpotent}\}\}$.

Beweis: (4.18). –

Definition 4.21 Sind A ein noetherscher Ring, E ein endlicher A-Modul, $U \subset E$ ein Untermodul, so heißt U primär in E, wenn $M = E/U$ die Bedingungen (i), (ii) von 4.19 erfüllt. Ist $\mathrm{Ass}_A(E/U) = \{\mathfrak{p}\}$, so heißt U (genauer) $\mathfrak{p}$-primär in E.

Satz 4.22 *Sei A ein noetherscher Ring.*

a) Für jedes Primideal $\mathfrak{p}$ *von A gilt:* $\mathfrak{p}$ *ist* $\mathfrak{p}$*-primär in A.*
b) Ist $\mathfrak{q}$ $\mathfrak{p}$*-primär in A, so gibt es ein n mit* $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Beweis: a) $\mathrm{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$ (4.4b).

b) $\mathfrak{q}$ $\mathfrak{p}$-primär $\iff \mathrm{Ass}_A(A/\mathfrak{q}) = \{\mathfrak{p}\}$. Nach 4.16 ist $\mathfrak{p}$ ein minimales Primoberideal von $\mathfrak{q}$, und zwar das einzige. Also $\mathrm{Nil}(A/\mathfrak{q}) = \mathfrak{p}/\mathfrak{q}$.
Sei $\mathfrak{p} = Ap_1 + \ldots + Ap_r$ mit $p_i^{n_i} \in \mathfrak{q}$ für geeignete n_i. Mit $N := \max\{n_1,\ldots,n_r\}$ gilt $\mathfrak{p}^{Nr} \subset \mathfrak{q}$. –

Bemerkung 4.23 Die Umkehrung von 4.22b) ist im allgemeinen falsch, aber

Feststellung 4.24 *Ist* $\mathfrak{m} \subset A$ *maximal und A noethersch, so gilt:*
$\mathfrak{q}$ ist $\mathfrak{m}$*-primär* $\iff \exists\, n: \mathfrak{m} \supset \mathfrak{q} \supset \mathfrak{m}^n$.

Beweis: "$\Leftarrow$": Ist $\mathfrak{p}$ ein Primideal mit $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{m}^n$, so gilt

$\mathfrak{p} \supset \mathfrak{m}$, also $\mathfrak{p} = \mathfrak{m}$ (1.14). Somit ist $\mathfrak{m}$ das einzige Primideal mit $\mathfrak{m} \supset \mathfrak{q}$. Dann folgt $\mathrm{Ass}(A/\mathfrak{q}) = \{\mathfrak{m}\}$ mit 4.16. –

Satz 4.25 *Seien A ein noetherscher Ring, M ein A-Modul,* $\Phi \subset \mathrm{Ass}_A(M)$ *eine Teilmenge. Dann gibt es einen Untermodul N von M mit* $\mathrm{Ass}_A(M/N) = \Phi$ *und* $\mathrm{Ass}_A(N) = \mathrm{Ass}_A(M) - \Phi$.

Beweis: Sei $\mathfrak{M} = \left\{P \mid P \subset M \text{ Untermodul}, \mathrm{Ass}_A(P) \subset \mathrm{Ass}_A(M) - \Phi\right\}$ und

$\mathbb{K}$ eine Kette in $\mathfrak{M}$, also $P_0 = \bigcup_{P \in \mathbb{K}} P$ ein Untermodul von M. Wenn $\mathfrak{p} \in \mathrm{Ass}_A P_0$, so $\mathfrak{p} = \mathrm{Ann}_A(m)$ für ein $m \in P_0$, also für ein $m \in P$ mit $P \in \mathbb{K}$, daher $\mathfrak{p} \in \mathrm{Ass}_A(M) - \Phi$ und $P_0 \in \mathfrak{M}$. Da $\{0\} \in \mathfrak{M}$, ist $\mathfrak{M} \neq \emptyset$.
Nach dem Zornschen Lemma gibt es ein maximales Element in $\mathfrak{M}$. Dies heiße N.

Behauptung: $\mathrm{Ass}_A(M/N) \subset \Phi$. (Dann hat man wegen $\mathrm{Ass}_A M \overset{4.9}{\subset} \mathrm{Ass}_A N \cup \mathrm{Ass}_A(M/N)$, $\mathrm{Ass}_A(N) \subset \mathrm{Ass}_A(M) - \Phi$ und $\mathrm{Ass}_A(M/N) \subset \Phi$, daß der Satz gilt.)
Sei also $\mathfrak{p} \in \mathrm{Ass}_A(M/N)$. Es gibt eine Injektion $A/\mathfrak{p} \xhookrightarrow{\varphi} M/N$ nach 4.4a). Sei $N' \subset M$ ein Untermodul, so daß $\varphi(A/\mathfrak{p}) = N'/N$ gilt. Wegen $\mathrm{Ass}_A(N'/N) = \{\mathfrak{p}\}$ folgt $\mathrm{Ass}_A(N') \subset \mathrm{Ass}_A(N) \cup \{\mathfrak{p}\}$ gemäß 4.9.

Gälte $\mathrm{Ass}_A(N') \subset \mathrm{Ass}_A(M) - \Phi$, wäre N nicht maximal in $\mathfrak{M}$. Es folgt $\mathfrak{p} \in \mathrm{Ass}_A(N') \subset \mathrm{Ass}_A M$. Deshalb muß $\mathfrak{p} \in \Phi$ sein. —

Definition 4.26 Seien A ein noetherscher Ring, M ein A-Modul, N ein Untermodul von M.
Eine endliche Familie $(Q_i)_{i\in I}$ von Untermoduln von M, die in M primär sind, so daß $N = \bigcap_{i\in I} Q_i$ gilt, heißt Primärzerlegung von N in M.

Beispiel 4.27 Sei A ein Hauptidealring, $M = A$ und $N = xA$ mit $x \in A - \{0\}$, ferner $x = u\cdot p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r}$ Primfaktorzerlegung von x in A (wobei $u \in A^*$ und die $p_1,\ldots,p_r$ paarweise nicht assoziiert sind), so ist $xA = (p_1^{\alpha_1}A) \cap \ldots \cap (p_r^{\alpha_r}A)$ eine Primärzerlegung von N in A.

Beweis: Die Ideale $(p_i^{\alpha_i})$ sind paarweise coprim zueinander, denn $\mathrm{ggT}\,(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ für $i \neq j$. Deswegen folgt mit 1.9a), daß $Ax = Ap_1^{\alpha_1}\cdot\ldots\cdot Ap_r^{\alpha_r} = Ap_1^{\alpha_1} \cap \ldots \cap Ap_r^{\alpha_r}$ ist. Betrachte nun für $a \in A$ und ein Primelement p die Homothetie $h_a\colon A/Ap^{\alpha} \longrightarrow A/Ap^{\alpha}$, $\bar{y} \longmapsto \overline{ay}$.
Im Fall $p \nmid a$ ist a eine Einheit modulo p und h_a bijektiv, insbesondere injektiv. Gilt hingegen $p \mid a$, so ist $(h_a)^{\alpha} = h_{a^{\alpha}} = 0$, also h_a nilpotent. Wir haben gezeigt: $N = xA = \bigcap_{i=1}^{r} p_i^{\alpha_i}A$, und die $p_i^{\alpha_i}A$ sind primär in $M = A$. —

Satz 4.28 (*Existenz von Primärzerlegungen*) *Seien A ein noetherscher Ring, M ein endlicher A-Modul und N ein Untermodul von M. Dann gibt es endlich viele Untermoduln $Q_1,\ldots,Q_r$ von M, so daß folgendes gilt:*

a) Die Q_i sind $\mathfrak{p}_i$-primär in M mit paarweise verschiedenen Primidealen in $\mathfrak{p}_i$.

b) $N = Q_1 \cap \ldots \cap Q_r$.

c) $\mathrm{Ass}_A(M/N) = \{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$.

Zum Beweis genügt es, den Fall $N = 0$ zu betrachten, denn $N = \cap\, Q_i$ ist genau dann eine Primärzerlegung von N in M, wenn $\{\bar{0}\} = \cap\,(Q_i/N)$ eine solche von $\{\bar{0}\}$ in M/N ist.
Sei $\mathrm{Ass}_A(M) = \{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$. Nach 4.25 gibt es $Q_i \subset M$ mit $\mathrm{Ass}_A(M/Q_i) = \{\mathfrak{p}_i\}$ $(1 \le i \le r)$ und $\mathrm{Ass}_A Q_i = \{\mathfrak{p}_1,\ldots,\mathfrak{p}_{i-1},\mathfrak{p}_{i+1},\ldots,\mathfrak{p}_r\}$. Nach 4.21 ist jedes Q_i primär in M. Sei $U = Q_1 \cap \ldots \cap Q_r$.

Es ist $U = 0$, (wegen 4.5) also $\mathrm{Ass}_A U = \emptyset$ zu zeigen. Nach 4.9 gilt $\mathrm{Ass}_A U \subset \mathrm{Ass}_A Q_i \subset \mathrm{Ass}_A M$. Aus $\mathfrak{p}_i \in \mathrm{Ass}_A U$ folgte $\mathfrak{p}_i \in \mathrm{Ass} Q_i$. Widerspruch. —

<u>Bemerkung 4.29</u> Ist $\bigcap_{i=1}^{r} Q_i = N$ eine Primärzerlegung von N in M mit Q_i $\mathfrak{p}_i$-primär, so gilt $\mathrm{Ass}_A(M/N) \subset \{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$.

<u>Beweis:</u> Es gibt eine Injektion $M/N \hookrightarrow \bigoplus_{i=1}^{r} M/Q_i$, also $\mathrm{Ass}_A(M/N) \subset \bigcup_{i=1}^{r} \mathrm{Ass}_A(M/Q_i) = \{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$, denn 4.9 liefert für eine direkte Summe $M = \bigoplus_{i=1}^{n} M_i$, daß $\mathrm{Ass}_A\left(\bigoplus_{i=1}^{n} M_i\right) \subset \mathrm{Ass}_A\left(\bigoplus_{i=1}^{n-1} M_i\right) \cup$

$$\cup\, \mathrm{Ass}_A\left(\bigoplus_{i=1}^{n} M_i \Big/ \bigoplus_{i=1}^{n-1} M_i\right) = \mathrm{Ass}_A\left(\bigoplus_{i=1}^{n-1} M_i\right) \cup \mathrm{Ass}_A(M_n) \subset \dots \subset \bigcup_{i=1}^{n} \mathrm{Ass}(M_i) \quad ! \text{ —}$$

Wie steht es mit der Eindeutigkeit einer Primärzerlegung?

Ist $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$ eine Primärzerlegung eines Ideals $\mathfrak{a}$ im Ring A, und ist $\mathfrak{m} \supset \mathfrak{a}$ ein maximales Ideal in A, so folgt, daß $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r \cap \mathfrak{m}$ auch eine Primärzerlegung ist, und oft gibt es unendlich viele maximale Ideale $\mathfrak{m} \supset \mathfrak{a}$. Ferner auch

<u>Feststellung 4.30</u> *Sind* $Q_1,\dots,Q_n$ *in* M *$\mathfrak{p}$-primär (für dasselbe $\mathfrak{p}$), so ist* $Q_1 \cap \dots \cap Q_n$ *ebenfalls $\mathfrak{p}$-primär in* M, falls A noethersch.

<u>Beweis:</u> Man hat eine Injektion $M/(Q_1 \cap \dots \cap Q_n) \hookrightarrow \bigoplus_{i=1}^{n} (M/Q_i)$, also gilt $\mathrm{Ass}\big(M/(Q_1 \cap \dots \cap Q_n)\big) \subset \bigcup_{i=1}^{n} \mathrm{Ass}(M/Q_i) = \{\mathfrak{p}\}$ (vgl. Beweis von 4.29).

Wenn man also in Richtung Eindeutigkeit etwas erreichen will, muß man zumindest fordern, daß die Zerlegung im Sinne der folgenden Definition unverkürzbar ist:

<u>Definition 4.31</u> Seien A ein noetherscher Ring, $N \subset M$ A-Moduln. Die Primärzerlegung $N = \bigcap_{i \in I} Q_i$ von N in M heißt unverkürzbar, wenn gilt:

(a) Es gibt kein $i \in I$ mit $\bigcap_{j \neq i} Q_j \subset Q_i$.

(b) Wenn $\mathrm{Ass}_A(M/Q_i) = \{\mathfrak{p}_i\}$, sind die $\mathfrak{p}_i$, $i \in I$, paarweise verschieden.

<u>Feststellung 4.32</u> *Ist* $N = \bigcap_{i \in I} Q_i$ *eine unverkürzbare Primärzerlegung von* N *in* M *mit einer endlichen Indexmenge* I, *so gilt:*

a) $\mathrm{Ass}_A(Q_i/N) = \bigcup_{j\neq i} \mathrm{Ass}_A(M/Q_j)$,

b) $\mathrm{Ass}_A(M/N) = \bigcup_{i\in I} \mathrm{Ass}_A(M/Q_i)$.

Beweis: a) "$\subset$": Wegen $N = \bigcap_{j\neq i} (Q_j \cap Q_i)$ gilt

$\mathrm{Ass}_A(Q_i/N) \subset \bigcup_{j\neq i} \mathrm{Ass}_A\Big(Q_i \,/\, (Q_j\cap Q_i)\Big)$, da man eine Injektion

$Q_i/N \hookrightarrow \bigoplus_{j\neq i} \Big(Q_i \,/\, (Q_j\cap Q_i)\Big)$ hat. Ferner ist

$Q_i \,/\, (Q_j\cap Q_i) \simeq (Q_i+Q_j) \,/\, Q_j \subset M/Q_j$, also $\mathrm{Ass}_A(Q_i/N) \subset \bigcup_{j\neq i} \mathrm{Ass}_A(M/Q_j)$.

"$\supset$" ist mit b) klar, da dann mit 4.9 nämlich

$\bigcup_{j\in I} \{\mathfrak{p}_j\} \subset \mathrm{Ass}_A(Q_i/N) \cup \mathrm{Ass}_A(M/Q_i) = \mathrm{Ass}_A(Q_i/N) \cup \{\mathfrak{p}_i\}$ gilt.

b) $\mathrm{Ass}(M/N) \subset \bigcup_{i\in I} \{\mathfrak{p}_i\}$ nach 4.29. Andererseits setze $P_i := \bigcap_{j\neq i} Q_j$. Dann gilt $P_i \cap Q_i = N$ und $P_i \neq N$ (da die Primärzerlegung unverkürzbar sein sollte). Man hat $0 \neq P_i/N \subset (P_i+Q_i) \,/\, Q_i \subset M/Q_i$. Mit 4.9 gilt $\mathrm{Ass}_A(P_i/N) = \{\mathfrak{p}_i\}$, und wegen $P_i/N \subset M/N$ folgt $\mathfrak{p}_i \in \mathrm{Ass}(M/N)$. —

Folgerung 4.33 *Seien* A *ein noetherscher Ring,* M *ein endlicher* A*-Modul und* $N \subset M$ *ein Untermodul. Es gibt Primärzerlegungen von* N *in* M *, also auch unverkürzbare. Wenn* $N = \bigcap_{i=1}^{r} Q_i$ *eine unverkürzbare Primärzerlegung von* N *in* M *ist mit* Q_i $\mathfrak{p}_i$*-primär, so sind die* $\mathfrak{p}_i$ *eindeutig bestimmt - und zwar sind sie die* $\mathfrak{p} \in \mathrm{Ass}(M/N)$ *, jedes genau einmal.* —

Sind die Q_i eindeutig bestimmt? Im allgemeinen nicht, aber

Satz 4.34 *Seien* A,M,N *wie oben und* $N = Q_1 \cap \ldots \cap Q_r$ *eine unverkürzbare Primärzerlegung. Sei* $\mathfrak{p}$ *minimal in* $\mathrm{Ass}_A(M/N)$ *, und* Q_j *sei* $\mathfrak{p}$*-primär. Dann ist* $Q_j = i^{-1}_{M,\mathfrak{p}}(N_{\mathfrak{p}})$ *. Also sind die zu den minimalen* $\mathfrak{p} \in \mathrm{Ass}(M/N)$ *gehörenden* Q_j *eindeutig bestimmt.*

Beweis: Schreibe $Q = Q_j$. O.E. sei $N = 0$. Zu zeigen: $Q = i^{-1}_{M,\mathfrak{p}}(0)$. Mit $S := A-\mathfrak{p}$ hat man

$$\mathrm{Ass}_{A_\mathfrak{p}}(Q_\mathfrak{p}) \overset{4.11}{=} \left\{S^{-1}\mathfrak{q} \mid \mathfrak{q} \in \mathrm{Ass}_A Q\,,\ \mathfrak{q} \subset \mathfrak{p}\right\} = \emptyset\,, \text{ da } \mathfrak{p} \in \mathrm{Ass}_A M$$

minimal und "$\mathfrak{q} \in \mathrm{Ass}_A Q \iff \mathfrak{q} = \mathfrak{p}_i$ für ein $i \neq j$" nach 4.32a).
Es folgt $Q_\mathfrak{p} = 0$, also $Q \subset i^{-1}_{M,\mathfrak{p}}(0)$.

Wenn andererseits ein $U \supsetneqq Q$ existierte mit $i_{M,\mathfrak{p}}(U) = 0$, so gälte $S^{-1}(U/Q) = 0$, aber $\emptyset \neq \mathrm{Ass}_A(U/Q) \subset \mathrm{Ass}_A(M/Q) = \{\mathfrak{p}\}$, und wegen 4.6 bestünde S aus lauter Nichtnullteilern für U/Q . Mit 3.43 folgte $S^{-1}(U/Q) \neq 0$. Widerspruch! —

Satz 4.35 *Sei* A *ein noetherscher Ring,* $\mathfrak{a} \subset A$ *ein Ideal derart, daß* $\mathrm{Ass}_A(A/\mathfrak{a})$ *nur aus maximalen Idealen von* A *besteht. Ist dann* $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ *eine unverkürzbare Primärzerlegung, sind die* $\mathfrak{q}_i$ *eindeutig bestimmt, und der kanonische Homomorphismus* $A/\mathfrak{a} \longrightarrow \prod_{i=1}^{r} (A/\mathfrak{q}_i)$ *ist ein Isomorphismus. Jedes* $A/\mathfrak{q}_i$ *besitzt genau ein Primideal.*

Beweis: Seien $\{\mathfrak{m}_i\} = \mathrm{Ass}(A/\mathfrak{q}_i)$, also $\mathrm{Ass}(A/\mathfrak{a}) = \{\mathfrak{m}_1,\ldots,\mathfrak{m}_r\}$ (4.32b)). Da alle $\mathfrak{m}_i$ nach Voraussetzung in A maximal sind, sind sie auch alle minimal in $\mathrm{Ass}_A(A/\mathfrak{a})$, deshalb sind nach 4.34 die $\mathfrak{q}_i$ eindeutig bestimmt. Da $\mathfrak{m}_i$ das einzige minimale unter den $\mathfrak{q}_i$ enthaltenden Primidealen ist und gleichzeitig maximal ist, ist $\mathfrak{m}_i$ das einzige Primideal von A , welches $\mathfrak{q}_i$ umfaßt. Insbesondere gilt $\mathfrak{m}_i \supset \mathfrak{q}_i \supset \mathfrak{m}_i^{r_i}$ gemäß 4.24. Nach Lemma 1.4 sind $\mathfrak{m}_i^{r_i}, \mathfrak{m}_j^{r_j}$ für $i \neq j$ coprim und deshalb erst recht $\mathfrak{q}_i, \mathfrak{q}_j$ coprim. Die Abbildung $A/\cap\mathfrak{q}_i \longrightarrow\!\!\!\!\to \prod_{i=1}^{r}(A/\mathfrak{q}_i)$ ist nach dem Chinesischen Restsatz 1.9 ein Isomorphismus. —

3. Moduln von endlicher Länge

Zunächst einige Vorbereitungen:

Lemma 4.36 *Seien* F,E,U *Untermoduln eines Moduls* M, *und es gelte* $F \subset E$. *Dann ist* $(E \cap U) + F = E \cap (U+F)$. *(Modulares Gesetz)*

Beweis: "$\subset$": $E \cap U \subset E$, $F \subset E$, also $(E \cap U) + F \subset E$;
$E \cap U \subset U$, $F \subset F$, also $(E \cap U) + F \subset U+F$.

"$\supset$": Sei $e \in E \cap (U+F)$. Dann besitzt e eine Darstellung $e = u+f$ mit $e \in E$, $u \in U$, $f \in F \subset E$, und es folgt $u = e-f \in E$ sowie $u \in U$. Daher liegt $e = u+f$ in $(E \cap U) + F$.

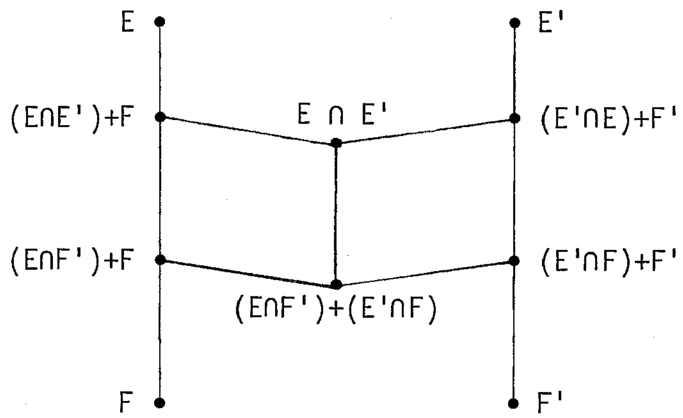
Bemerkung 4.37 Mit den Voraussetzungen von 4.36 gilt $F \subset (E \cap U) + F = E \cap (U+F) \subset E$. Man nennt $(E \cap U) + F$ die Einschiebung von U zwischen E und F .

Lemma 4.38 *(Schmetterlingslemma von Zassenhaus): Seien* F,E,F',E' *Untermoduln von* M, $F \subset E$, $F' \subset E'$. *Dann ist*

$$\big((E \cap E')+F\big) \,/\, \big((E \cap F')+F\big) \simeq \big((E' \cap E)+F'\big) \,/\, \big((E' \cap F)+F'\big) .$$

D.h. die Einschiebungen von E' *und* F' *zwischen* E *und* F *haben bis auf Isomorphie denselben "Quotienten" wie die von* E *und* F *zwischen* E' *und* F' .

Beweis: Betrachte



Aus Symmetriegründen genügt es, die Isomorphie
$\big((E \cap E')+F\big) \,/\, \big((E \cap F')+F\big) \simeq (E \cap E')/\big((E \cap F')+(E' \cap F)\big)$ zu zeigen

(linker "Schmetterlingsflügel"). Um hierfür den Noetherschen Isomorphiesatz (3.9) anwenden zu können, ist zweierlei nachzuweisen:
(1) $(E \cap E') + \big((E \cap F')+F\big) = (E \cap E')+F$ und
(2) $(E \cap E') \cap \big(F+(E \cap F')\big) = (E' \cap F) + (E \cap F')$. Da aber $F' \subset E'$ und deshalb $E \cap F' \subset E \cap E'$ ist, folgt (1) sofort und (2) mit Hilfe von 4.36 und $E' \cap F = E \cap E' \cap F$ $(F \subset E)$. —

Definition 4.39 Zwei Kompositionsreihen
$\{0\} = M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n = M$, $\{0\} = N_0 \subset N_1 \subset \ldots \subset N_{r-1} \subset N_r = M$ eines A-Moduls M heißen äquivalent, wenn $n = r$ und eine Permutation der Indizes $i \longmapsto i'$ existiert mit $M_i/M_{i-1} \simeq N_{i'}/N_{i'-1}$ für $1 \le i \le r$.
Die Faktormoduln M_i/M_{i-1} heißen (Kompositions-) Faktoren der Kompositionsreihe.
Die Kompositionsreihe $\{0\} = P_0 \subset P_1 \subset \ldots \subset P_{s-1} \subset P_s = M$ heißt Verfeinerung der Kompositionsreihe $\{0\} = M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n = M$, wenn alle M_j $(0 \le j \le n)$ unter den P_i $(0 \le i \le s)$ vorkommen.

Satz 4.40 (*Schreier*): *Sei* M *ein* A-*Modul. Dann haben zwei Kompositionsreihen von* M *zueinander äquivalente Verfeinerungen.*

Beweis: Seien $\{0\} = M_0 \subset M_1 \subset \ldots \subset M_{r-1} \subset M_r = M$ und
$\{0\} = N_0 \subset N_1 \subset \ldots \subset N_{s-1} \subset N_s = M$ zwei Kompositionsreihen für M.
Für $i = 1,\ldots,r$, für $j = 0,\ldots,s$ definiere man $P_{ij} = M_{i-1} + (N_j \cap M_i)$.
Dann gilt $P_{i0} = M_{i-1}$, $P_{is} = M_i$, und wir haben eine Verfeinerung der ersten Kompositionsreihe $\{0\} = M_0 = P_{10} \subset P_{11} \subset \ldots \subset P_{1s} = M_1 = P_{20} \subset \ldots \subset M_{r-1} = P_{r0} \subset P_{r1} \subset \ldots \subset P_{rs} = M_r = M$. (Diese Verfeinerung entsteht also durch Einschiebung der N_j zwischen M_{i-1} und M_i für jedes i.)
Analog definiere man $Q_{ji} = N_{j-1} + (M_i \cap N_j)$ für $j = 1,\ldots,s$ und für $i = 0,\ldots,r$. Dies liefert eine Verfeinerung der zweiten Kompositionsreihe.
Nach dem Schmetterlingslemma 4.38 gilt

$$P_{ij} / P_{i,j-1} \simeq M_{i-1}+(N_j \cap M_i) / M_{i-1}+(N_{j-1} \cap M_i)$$

$$\simeq N_{j-1}+(N_j \cap M_i) / N_{j-1}+(N_j \cap M_{i-1}) \simeq Q_{ji} / Q_{j,i-1}$$

(ersetze dort F durch M_{i-1}, E durch M_i,
F' durch N_{j-1}, E' durch N_j)

$(1 \le i \le r,\ 1 \le j \le s)$. Beide Verfeinerungen haben dieselbe Anzahl von

Elementen, nämlich $rs+1$: Die P_{ij} $(1 \le i \le r,\ 1 \le j \le s)$ und $\{0\}$ im ersten Fall, die Q_{ij} $(1 \le i \le r,\ 1 \le j \le s)$ und $\{0\}$ im zweiten Fall. Der obige Isomorphismus für jedes Paar von Indizes (i,j) zeigt, daß diese beiden Verfeinerungen äquivalent sind. –

Definition 4.41 Ein Modul M heißt einfach, wenn $M \neq \{0\}$ ist und $\{0\}$ und M seine einzigen Untermoduln sind.

N.B.: Ein Faktormodul M/U ist demgemäß genau dann einfach, wenn $M \neq U$ ist und für jeden Untermodul N mit $U \subset N \subset M$ gilt: $N = U$ oder $N = M$.

Definitionen 4.42 a) Eine Kompositionsreihe $\{0\} = M_0 \subset \ldots \subset M_{r-1} \subset M_r = M$ heißt Jordan-Hölder-Reihe, wenn ihre Kompositionsfaktoren sämtlich einfach sind (d.h. die Reihe nicht echt verfeinerbar ist).
b) Ein A-Modul heißt von endlicher Länge, wenn er eine Jordan-Hölder-Reihe besitzt: $\{0\} = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_{r-1} \subset M_r = M$. Man nennt r die Länge der Jordan-Hölder-Reihe.

Folgerung 4.43 *Es sei M ein Modul von endlicher Länge. Dann läßt sich jede Kompositionsreihe zu einer Jordan-Hölder-Reihe verfeinern. Je zwei Jordan-Hölder-Reihen sind äquivalent, also insbesondere von gleicher Länge.*

Beweis: Sei (*) $\{0\} = M_0 \subset M_1 \subset \ldots \subset M_r = M$ eine beliebige Kompositionsreihe für M und (**) $\{0\} = N_0 \subset N_1 \subset N_2 \subset \ldots \subset N_s = M$ eine nach Voraussetzung existierende Jordan-Hölder-Reihe für M.
Nach Satz 4.40 haben wir zueinander äquivalente Verfeinerungen der beiden Reihen. Eine Jordan-Hölder-Reihe kann man aber nur verfeinern, indem man gewisse Terme wiederholt. Dabei entsteht eine Kompositionsreihe, deren Faktoren $\simeq 0$ oder einfach sind. Dies gilt dann auch für die äquivalente Verfeinerung der ersten Reihe. Indem man aus beiden Verfeinerungen die überflüssigen Terme streicht (d.h. jeweils jeden vorkommenden Term genau einmal zählt), erhält man einerseits eine Jordan-Hölder-Reihe (*'), welche die erste Kompositionsreihe verfeinert, und andererseits die Kompositionsreihe (**) (welche schon eine Jordan-Hölder-Reihe war) zurück. Da man aus äquivalenten Kompositionsreihen nur die zu 0 isomorphen Faktoren weggelassen hat, sind (*') und (**) äquivalent. Wenn (*) bereits eine Jordan-Hölder-Reihe ist, ist (*) = (*'), also (**) zu (*) äquivalent. –

Definition 4.44 Besitzt der A-Modul M eine Jordan-Hölder-Reihe $\{0\} = M_0 \subset M_1 \subset \ldots \subset M_{r-1} \subset M_r = M$, so heißt r die Länge von M. Man schreibt $l_A(M) := r$. Besitzt M keine Jordan-Hölder-Reihe, so setzt man $l_A(M) := \infty$. (Man schreibt auch $l(M)$ statt $l_A(M)$.)

Feststellung 4.45 *Es seien* $U \subset M$ *A-Moduln. Dann gilt:*

a) $l_A(U) + l_A(M/U) = l_A(M)$ *(auch im Falle* $l_A(M) = \infty$ *!)* .

b) $l_A(M) < \infty$, $U \neq M \Rightarrow l_A(U) < l_A(M)$;

$l_A(M) < \infty$, $U \neq \{0\} \Rightarrow l_A(M/U) < l_A(M)$.

c) $l_A(U) < \infty$, $l_A(M/U) < \infty \iff l_A(M) < \infty$.

Zum Beweis betrachte man die Kompositionsreihe $\{0\} = M_0 \subset M_1 = U \subset M_2 = M$. Ist M von endlicher Länge, so läßt sich diese Kompositionsreihe zu einer Jordan-Hölder-Reihe $\{0\} = M_0' \subset M_1' \subset \ldots \subset M_s' = U = M_0'' \subset M_1'' \subset \ldots \subset M_t'' = M$ verfeinern (4.43). Dabei ist $\{0\} = M_0' \subset M_1' \subset \ldots \subset M_s' = U$ trivialerweise eine Jordan-Hölder-Reihe von U, und mit $\overline{M}_i := M_i'' / U$ $(0 \leq i \leq t)$ ist $\{0\} = \overline{M}_0 \subset \ldots \subset \overline{M}_t = M/U$, da $\overline{M}_i/\overline{M}_{i-1} \simeq M_i''/M_{i-1}''$ einfach ist, eine solche von M/U. Mit 4.43 folgt a) im Falle $l_A(M) < \infty$, ferner c) "$\Leftarrow$" und b), da im Falle $U \neq M$ gilt: $l_A(M/U) \neq 0$, und im Falle $U \neq 0$, daß $l_A(U) \neq 0$ ist. Ist $l_A(U) =: r < \infty$, $l_A(M/U) =: s < \infty$ und $\{0\} = U_0 \subset U_1 \subset \ldots \subset U_r = U$ eine Jordan-Hölder-Reihe von U, $\{0\} = \overline{V}_0 \subset \overline{V}_1 \subset \ldots \subset \overline{V}_s = M/U$ eine Jordan-Hölder-Reihe von M/U, so betrachte man mit der natürlichen Projektion $\varphi\colon M \twoheadrightarrow M/U$ die A-Moduln $V_i = \varphi^{-1}(\overline{V}_i)$ $(0 \leq i \leq s)$. Dann gilt $V_i/V_{i-1} \simeq (V_i/U) / (V_{i-1}/U) = \overline{V}_i/\overline{V}_{i-1}$ für $1 \leq i \leq s$. Die Faktoren sind also einfach, und $\{0\} = U_0 \subset U_1 \subset U_r = U \subset V_1 \subset \ldots \subset V_s = M$ ist eine Jordan-Hölder-Reihe von M, insbesondere ist M von endlicher Länge. Wir haben c) "$\Rightarrow$" gezeigt und damit auch a) im Falle $l_A(M) = \infty$. —

Bemerkung 4.46 Man kann 4.45a) auch folgendermaßen ausdrücken: Sei $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ eine exakte Folge von A-Moduln, so gilt $l_A(M) = l_A(M') + l_A(M'')$.

Feststellung 4.47 *Ein A-Modul M ist genau dann von endlicher Länge, wenn jede aufsteigende und jede absteigende Folge von Untermoduln stationär wird.*

Beweis: "$\Leftarrow$": Wähle in M einen maximalen echten Untermodul M_1, in M_1 einen maximalen echten Untermodul M_2, usw. Dies ist nach 3.22 möglich, da aufsteigende Folgen stationär werden. Da absteigende Folgen stationär werden, bricht die Folge $M \supset M_1 \supset M_2 \supset \dots$ ab, und zwar mit $\{0\}$. Sie ist nach Konstruktion nicht mehr verfeinerbar.
"$\Rightarrow$": Jede echt aufsteigende (bzw. absteigende) Folge hat höchstens $l_A(M)+1$ Glieder. —

Definition 4.48 Ein A-Modul M, in dem jede absteigende Kette von Untermoduln abbricht, heißt artinsch. Ist der A-Modul ${}_AA$ artinsch, so heißt A artinscher Ring.

Satz 4.49 *In einem artinschen Ring A ist jedes Primideal maximal.*

Beweis: Sei $\mathfrak{p} \subsetneqq A$ prim. Dann ist $B = A/\mathfrak{p}$ artinsch und integer. Sei $x \in B$, $0 \neq x$. Wegen $(x^n) \supset (x^{n+1}) \supset \dots$ gilt $x^r = yx^{r+1}$ für ein $r \in \mathbb{N}$ (B artinsch!). Da $0 \neq x$ und B integer ist, gilt $xy = 1$. Also ist B ein Körper und $\mathfrak{p}$ maximal in A. —

Feststellung 4.50 *Ein A-Modul E ist genau dann einfach, wenn es ein maximales Ideal $\mathfrak{m} \subset A$ gibt mit $E \simeq A/\mathfrak{m}$.*

Beweis: Natürlich ist $A/\mathfrak{m}$ ein einfacher A-Modul. Wenn umgekehrt E einfach ist, wähle $x \in E - \{0\}$. Der Untermodul Ax von M ist dann $\neq \{0\}$, also $Ax = M$ und deshalb $M \simeq A/\mathfrak{a}$ mit $\mathfrak{a} = \operatorname{Ann} x$. Wenn $\mathfrak{a}$ nicht maximal ist, ist $A/\mathfrak{a}$ nicht einfach. —

Satz 4.51 *Für einen Ring A sind äquivalent:*

(i) A *ist noethersch, und jedes Primideal von* A *ist ein maximales Ideal;*

(ii) A *ist noethersch und artinsch, d.h. als* A*-Modul von endlicher Länge;*

(iii) jeder endliche A*-Modul ist noethersch und artinsch, d.h. von endlicher Länge;*

(iv) es gibt einen A*-Modul* M *von endlicher Länge mit* $\operatorname{Ann} M = (0)$.

Beweis: (i) $\Rightarrow$ (iii) folgt aus 4.7.
(iii) $\Rightarrow$ (ii) ist trivial.

(ii) $\Rightarrow$ (i) folgt aus 4.49.
(ii) $\Rightarrow$ (iv) ist trivial.
(iv) $\Rightarrow$ (ii): M ist noethersch, also endlich erzeugt: $M = Ax_1 + \ldots + Ax_n$. Die A-lineare Abbildung $A \longrightarrow M^n$, $a \longmapsto (ax_1,\ldots,ax_n)$ ist injektiv, da $\operatorname{Ann} M = (0)$ gilt. A ist somit als Untermodul eines Moduls endlicher Länge selbst ein solcher (4.45). –

Bemerkungen 4.52 a) Die Bedingungen (i) bis (iv) sind sogar äquivalent zu "(v) A ist artinsch". D.h. ein artinscher Ring ist auch noethersch. (Zum Beweis siehe 4.A5.)
Beachte aber, daß ein artinscher Modul nicht noethersch zu sein braucht (3.A6).
b) Nach 4.35 ist ein Ring A, der den äquivalenten Bedingungen von 4.51 genügt, isomorph zu einem direkten Produkt endlich vieler Ringe von endlicher Länge, die jeweils nur ein einziges Primideal besitzen. Dies läßt sich verhältnismäßig einfach auch ohne die Theorie der Primärzerlegung zeigen. (Übungsaufgabe)

Folgerung 4.53 *Es sind für einen Integritätsring* A *äquivalent:*
(i) A *ist noethersch, und jedes Primideal* $\mathfrak{p} \neq (0)$ *ist maximal.*
(ii) Für jedes Ideal $\mathfrak{a} \neq (0)$ *hat* $A/\mathfrak{a}$ *endliche Länge.*

Fast unmittelbare Folgerung aus 4.51 ! –

Der folgende Satz wird im weiteren Verlauf des Buches nicht benötigt.

Satz 4.54 *(Krull-Akizuki): Sei* A *ein noetherscher Integritätsring, in dem jedes Primideal* $\mathfrak{p} \neq (0)$ *maximal ist.* $L \supset Q(A)$ *sei eine endliche Körpererweiterung,* B *ein beliebiger Zwischenring:* $L \supset B \supset A$. *Dann gilt:* B *ist noethersch, und in* B *ist jedes Primideal* $\mathfrak{p}' \neq (0)$ *maximal.*

Zum Beweis benötigen wir folgende Lemmata:

Lemma 4.55 *Sei* A *wie in 4.54 und* M *ein endlicher* A*-Modul mit* $\operatorname{Ann}_A(M) \neq (0)$. *Dann ist* $l_A(M) < \infty$.

Lemma 4.56 *Sei* A *wie in 4.54,* V *ein* $Q(A)$*-Vektorraum der Dimension* $s < \infty$, $M \subset V$ *ein* A*-Untermodul,* $a \in A - \{0\}$. *Dann gilt* $l_A(M/aM) \leq s\, l_A(A/aA)$.

Beweis des Satzes: Es sei $\mathfrak{b} \neq (0)$ ein Ideal in B, $b \in \mathfrak{b} - (0)$ beliebig. Da $b \in L$ algebraisch über $Q(A)$ ist, gibt es eine Gleichung $a_0 + a_1 b + \ldots + a_r b^r = 0$ mit gewissen $a_i \in A$ und $a_0 \neq 0$. Es folgt $a_0 \in Ab \subset Bb \subset \mathfrak{b}$ und mit 4.56, daß $l_B(B/\mathfrak{b}) \leq l_A(B/\mathfrak{b}) \leq l_A(B/a_0B) \leq s l_A(A/a_0A) \overset{4.53}{<} \infty$ ist. Wende nun 4.53 (ii) $\Rightarrow$ (i) an. –

Beweis von 4.55 Der Ring $C = A/\mathrm{Ann}M$ ist noethersch, und seine Primideale sind maximal. Wende 4.53 (i) $\Rightarrow$ (ii) und 4.51 (i) $\Rightarrow$ (iii) an. –

Beweis von 4.56 O.E. sei der von M erzeugte $Q(A)$-Vektorraum ganz V.

a) Zunächst sei M ein endlicher A-Modul: $M = Am_1 + \ldots + Am_t$. Dann gilt o.E. für ein $s \leq t$, daß $m_1, \ldots, m_s$ eine $Q(A)$-Basis von V ist. Sei $F := Am_1 + \ldots + Am_s \subset M$. Betrachte $\varphi\colon A^s \longrightarrow F$
$(a_1, \ldots, a_s) \longmapsto a_1 m_1 + \ldots + a_s m_s$. Trivialerweise ist φ surjektiv. φ ist auch injektiv: Ist $\varphi(a_1, \ldots, a_s) = 0$, also $\sum_{i=1}^{s} a_i m_i = 0$, so folgt $a_i = 0$ $(1 \leq i \leq s)$, da die $m_1, \ldots, m_s$ über $Q(A)$ linear unabhängig sind. Also $F \simeq A^s$ $(*)$.
Es gibt Koeffizienten $\lambda_{ij} \in Q(A)$ $(1 \leq i \leq t,\ 1 \leq j \leq s)$ mit
$m_i = \sum_{j=1}^{s} \lambda_{ij} m_j$. Ist c ein Hauptnenner aller λ_{ij}, so gilt: $cm_i \in F$ $(1 \leq i \leq t)$, mithin $cM \subset F$ und somit $l_A(M/F) < \infty$ wegen 4.55.
Sei nun $a \in A - \{0\}$ beliebig. Für $n \geq 1$ gilt

$$l_A(M/a^nM) \leq l_A(M/a^nF) \overset{4.45}{=} l_A(M/F) + l_A(F/a^nF) \qquad (**) .$$

Wegen $M \subset V \simeq Q(A)^s$ gilt $M \xrightarrow[\simeq]{\cdot a} aM$, also
$M/aM \simeq aM/a^2M \simeq \ldots \simeq a^{n-1}M \,/\, a^nM$, analog
$F/aF \simeq aF/a^2F \simeq \ldots \simeq a^{n-1}F \,/\, a^nF$. Wegen 4.45 hat man deshalb
$l_A(M/a^nM) = n l_A(M/aM)$, $l_A(F/a^nF) = n l_A(F/aF)$. Durch Grenzübergang $n \longrightarrow \infty$ folgt aus $(**)$ schließlich

$$l_A(M/aM) \leq l_A(F/aF) \overset{(*)}{=} l_A\Big((A/aA)^s\Big) = s l_A(A/aA) .$$

b) Sei nun M ein nicht notwendig endlicher A-Modul und $\{M_\tau\}_{\tau \in T}$ – T Indexmenge – die Menge aller endlichen A-Untermoduln von M.

Es gilt $l_A(M_\tau/aM_\tau) \leq s l_A(A/aA)$ für alle $\tau \in T$ und deshalb
$l_A(M_\tau + aM/aM) = l_A(M_\tau/M_\tau \cap aM) \leq s l_A(A/aA)$ wegen $aM_\tau \subset aM \cap M_\tau$. Sei $\tau_0 \in T$ so, daß $l_A\Big((M_{\tau_0} + aM) \,/\, aM\Big)$ maximal ist. Wäre $M_{\tau_0} + aM \subsetneqq M$, so wäre für

$z \in M - (M_{\tau_0} + \mathfrak{a}M)$ auch $M_{\tau_1} := M_{\tau_0} + Az$ ein endlicher A-Untermodul von M, $M_{\tau_1} + \mathfrak{a}M = M_{\tau_0} + Az + \mathfrak{a}M \supsetneqq M_{\tau_0} + \mathfrak{a}M$, also $\left(M_{\tau_1} + \mathfrak{a}M\right) / \mathfrak{a}M \supsetneqq \left(M_{\tau_0} + \mathfrak{a}M\right) / \mathfrak{a}M$, und deswegen $l_A\left(M_{\tau_1} + \mathfrak{a}M / \mathfrak{a}M\right) > l_A\left(M_{\tau_0} + \mathfrak{a}M / \mathfrak{a}M\right)$ im Widerspruch zur Maximalität von $l_A\left(M_{\tau_0} + \mathfrak{a}M / \mathfrak{a}M\right)$! Also: $l_A(M/\mathfrak{a}M) = l_A\left(M_{\tau_0} + \mathfrak{a}M / \mathfrak{a}M\right) \leq sl(A/\mathfrak{a}A)$. —

Aufgaben und Hinweise

1) Für nicht noethersche Ringe bleiben 4.5 und 4.6 nicht richtig. Hier ist der Begriff "schwach assoziiertes Primideal" adäquater. Siehe dazu [Bourbaki] chap. IV §1 Exerc. 17.

2) Sei k ein Körper, $A = k[X,Y]$ und $\mathfrak{a} = (X^2, XY)$. Bestimme $\mathrm{Ass}(A/\mathfrak{a})$ und gib mehrere unverkürzbare Primärzerlegungen von $\mathfrak{a}$ in A an.

3) a) Die Theorie der Kompositions- und Jordan-Hölder-Reihen gilt auch für Moduln über nichtkommutativen Ringen - mit identischen Beweisen -, ferner für nicht notwendig abelsche Gruppen - mit fast identischen Beweisen (vgl. [Lang] IV, §4) - usw.

b) Beachte, daß aus 4.43 die Invarianz der Dimension endlich-dimensionaler Vektorräume und die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{N}$ folgt.

4) Sei $(\mathfrak{p}_i)_{i \in \mathbb{N}}$ eine Folge von Primidealen mit $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ für $i < j$. Setze $\mathfrak{a}_n := \bigcap_{i \leq n} \mathfrak{p}_i$. Zeige: Die $\mathfrak{a}_n$ bilden eine <u>echt</u> absteigende Folge.

5) Sei A ein artinscher Ring. Zeige: a) A besitzt nur endlich viele maximale Ideale (A4). Mit $J = \mathrm{Jac}A$ ist also A/J ein endliches direktes Produkt von Körpern.
b) Für jedes r ist J^r/J^{r+1} ein (A/J)-Modul endlicher Länge. (Wenn $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ die maximalen Ideale von A sind, gilt für jeden A/J-Modul E, daß die kanonische Abbildung $E \longrightarrow \bigoplus_{i=1}^{n} E/\mathfrak{m}_i E$ bijektiv ist. Die $E/\mathfrak{m}_i E$ haben als artinsche $A/\mathfrak{m}_i$-Vektorräume endliche Dimension.)
c) Es gibt ein n mit $J^n = 0$. (Für ein n ist $J^n = J^{n+1} = \ldots$. Sei $\mathfrak{a}$ ein minimales Ideal mit $J^n\mathfrak{a} \neq (0)$. (Existenz?) Da $J^n(J\mathfrak{a}) = J^{n+1}\mathfrak{a} = J^n\mathfrak{a} \neq (0)$ und $J\mathfrak{a} \subset \mathfrak{a}$, ist $J\mathfrak{a} = \mathfrak{a}$ aus Gründen der Minimalität. $\mathfrak{a}$ ist aber auch ein Hauptideal, insbesondere endlich erzeugt. Wende Nakayama an.)

d) A ist von endlicher Länge.

N.B.: Mit i.w. denselben Schlüssen zeigt man, daß auch ein nichtkommutativer artinscher Ring als Linksmodul von endlicher Länge ist. [Bourbaki: A] chap. VIII, § 6.5.

6) Es gibt zu "Ass" und "Primärzerlegung" die dualen Begriffe "Att" ("attached") und "secondary representation", die für artinsche Moduln die gleiche Rolle spielen wie "Ass" und "Primärzerlegung" für die noetherschen. Siehe [Matsumura: R] Appendix to §6.

§5 DAS HILBERT-SAMUEL-POLYNOM

Hier wird ein wichtiges Hilfsmittel für die Dimensionstheorie im nächsten Paragraphen bereitgestellt. Es ist allerdings auch möglich, einen großen Teil der Dimensionstheorie viel schneller als in diesem Buch herzuleiten. Wer mag, kann [Kunz] V. 3.1-3.4, 4.1-4.8 lesen, hat damit unsere Sätze 6.20 und 6.19, woraus 6.10 ff auch folgt.

Das Hilbert-Samuel-Polynom ist allerdings auch außerhalb der Dimensionstheorie wichtig, und Theorem 6.9 geht wesentlich weiter als Satz 6.19.

1. Graduierte und filtrierte Ringe und Moduln

Definition 5.1 Ein graduierter Ring ist ein Ring A, zusammen mit einer direkten Zerlegung seiner unterliegenden additiven Gruppe: $A = \bigoplus_{n\geq 0} A_n$, so daß $A_n A_m \subset A_{n+m}$ für $n,m \in \mathbb{N}$ gilt. (A_0 ist ein Unterring von A und jedes A_n ein A_0-Modul.) Ein graduierter A-Modul ist ein A-Modul M über einem graduierten Ring A, zusammen mit einer direkten Zerlegung als Gruppe: $M = \bigoplus_{n\geq 0} M_n$ mit $A_n M_m \subset M_{n+m}$ für alle $n,m \in \mathbb{N}$. Elemente von A_n bzw. M_n heißen homogen vom Grad n. Ein Untermodul N des graduierten Moduls M heißt graduierter Untermodul von M, wenn $N = \bigoplus_{n\geq 0} (N \cap M_n)$ gilt.

Lemma 5.2 *Es sei* M *ein graduierter* A-*Modul*, N *ein Untermodul.*
Es sind äquivalent:

(*i*) N *ist ein graduierter Untermodul von* M.

(*ii*) N *wird von homogenen Elementen erzeugt.*

(*iii*) *In* N *gilt:*
$$\left(n = m_0+m_1+\ldots+m_s \in N,\ m_i \in M_i \text{ für } i \le s \Rightarrow m_i \in N \text{ für } i \le s\right).$$

Beweis: (i) $\Rightarrow$ (ii) wegen $N = \bigoplus_{n\ge 0} (N \cap M_n)$ trivial.

(i) $\Leftrightarrow$ (iii) trivial.

(ii) $\Rightarrow$ (i) Nach (ii) gibt es $a_j \in A$ und homogene $n_j \in N$, so daß $n = \sum_j a_j n_j$ gilt. Jedes a_j wiederum läßt sich schreiben als $a_j = \sum_{k\ge 0} a_{jk}$ mit $a_{jk} \in A_k$. Da $a_{jk}n_j \in N$ und homogen ist, ist n Summe homogener Elemente aus N. Es folgt (i). —

Ist N ein graduierter Untermodul von M, so ist M/N vermöge $M/N = \oplus\, (M_n / N \cap M_n)$ ein graduierter A-Modul. Ein Ideal $\mathfrak{a}$ heißt graduiert, wenn es als A-Modul ein graduierter Untermodul von A ist, d.h. $\mathfrak{a} = \sum_{n\ge 0} (\mathfrak{a} \cap A_n)$ gilt, wenn $A = \bigoplus_{n\ge 0} A_n$ die Graduierung von A ist.
$A/\mathfrak{a} = \bigoplus_{n\ge 0} A_n \,/ \bigoplus_{n\ge 0} (\mathfrak{a} \cap A_n) \simeq \bigoplus_{n\ge 0} \left(A_n / \mathfrak{a} \cap A_n\right)$ ist dann sogar ein graduierter Ring!

Eine Filtrierung eines Ringes A ist eine absteigende Folge von Idealen $A = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots$, die $\mathfrak{a}_n\mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ für $n,m \in \mathbb{N}$ erfüllt. Ist eine solche Filtrierung gegeben, so definieren wir einen graduierten Ring $gr_{(\mathfrak{a}_n)}(A)$ wie folgt: Die unterliegende additive Gruppe sei $\bigoplus_{n\ge 0} \mathfrak{a}_n/\mathfrak{a}_{n+1}$, und wenn $\alpha \in gr^n_{(\mathfrak{a}_n)}(A) := \mathfrak{a}_n / \mathfrak{a}_{n+1}$ und $\beta \in gr^m_{(\mathfrak{a}_n)}(A) := \mathfrak{a}_m / \mathfrak{a}_{m+1}$, so wähle Repräsentanten $a \in \mathfrak{a}_n$, $b \in \mathfrak{a}_m$ mit $\overline{a} = \alpha$, $\overline{b} = \beta$ und setze $\alpha\beta = \overline{ab}$ in $\mathfrak{a}_{n+m} / \mathfrak{a}_{n+m+1}$. Diese Multiplikation ist wohldefiniert und macht $gr_{(\mathfrak{a}_n)}(A)$ zu einem graduierten Ring.
Speziell: Ist $\mathfrak{a} \subset A$ ein Ideal und setzt man $\mathfrak{a}_n := \mathfrak{a}^n$, so liefert die "$\mathfrak{a}$-adische" Filtrierung $A = \mathfrak{a}^0 \supset \mathfrak{a}^1 \supset \mathfrak{a}^2 \supset \ldots$ den zu ihr "assoziierten" graduierten Ring $gr_{\mathfrak{a}}(A)$.

Feststellung 5.3 *Ist* A *noethersch und* $\mathfrak{a} \subset A$ *ein Ideal, so ist* $gr_{\mathfrak{a}}(A)$ *noethersch.*

Beweis: Sei $\mathfrak{a} = (a_1,\ldots,a_n)$. Aus der kanonischen Abbildung $A \longrightarrow A/\mathfrak{a}$ erhält man durch die Vorschrift $X_i \longmapsto \bar{a}_i \in \mathfrak{a}/\mathfrak{a}^2$ einen surjektiven Ringhomomorphismus $A[X_1,\ldots,X_n] \longrightarrow gr_{\mathfrak{a}}(A)$. Wende nun 3.30 (Hilbertscher Basissatz) an. –

Eine Filtrierung eines A-Moduls M ist eine absteigende Folge von Untermoduln $M = M_0 \supset M_1 \supset M_2 \supset \ldots$. Ist $\mathfrak{a} \subset A$ ein Ideal, so heißt die Filtrierung $\mathfrak{a}$-zulässig, wenn $\mathfrak{a}M_n \subset M_{n+1}$ für alle $n \in \mathbb{N}$ gilt, $\mathfrak{a}$-adisch, falls $M_n = \mathfrak{a}^n M$ für alle $n \in \mathbb{N}$ gilt, im wesentlichen $\mathfrak{a}$-adisch, wenn sie $\mathfrak{a}$-zulässig ist und $\mathfrak{a}M_n = M_{n+1}$ für fast alle n gilt.

Feststellung 5.4 *Seien* A *ein Ring,* $\mathfrak{a} \subset A$ *ein Ideal und* M *ein* A*-Modul.* $M = M_0 \supset M_1 \supset M_2 \supset \ldots$ *sei eine* $\mathfrak{a}$*-zulässige Filtrierung von* M*, bestehend aus endlichen* A*-Moduln* M_n $(n \in \mathbb{N})$. *Betrachte den Ring* $A' = \oplus\, \mathfrak{a}^n$ *und den* A'*-Modul* $M' = \oplus M_n$. *Dann sind äquivalent:*

(*i*) *Die Filtrierung ist i.w.* $\mathfrak{a}$*-adisch.*

(*ii*) M' *ist ein endlicher* A'*-Modul.*

Beweis: Man rechnet sofort nach: M' ist ein graduierter Modul über dem graduierten Ring A'.

(ii) ⇒ (i): Aus einem endlichen Erzeugendensystem $x_1,\ldots,x_s$ von M' erhält man sofort ein solches, das aus endlich vielen homogenen Elementen besteht. Wenn nämlich $x_j = \sum_{k=1}^{t_j} m_{jk}$ mit homogenen m_{jk} ist, so erzeugen die endlich vielen m_{jk} den Modul M'. Sei also $M' = A'm_1 + \ldots + A'm_r$ mit gewissen $m_i \in M'_{n_i}$. Für $n \geq \max\{n_1,\ldots,n_r\}$ gilt dann

$$M'_{n+1} = \left\{ \sum_{i=1}^{r} a_i m_i \mid a_i \in A'_{n+1-n_i} \right\} = \mathfrak{a}M'_n \quad , \text{ da } A'_{n+1-n_i} = \mathfrak{a}\cdot\mathfrak{a}^{n-n_i} \text{ ist.}$$

(i) ⇒ (ii): Hat man umgekehrt $M_{n+1} = \mathfrak{a}M_n$ für $n \geq n_0$, so ist M' über A' durch $M_0 \oplus M_1 \oplus \ldots \oplus M_{n_0}$ erzeugt, welches ein endlicher A'-Modul ist. –

Satz 5.5 (*Artin-Rees*) *Seien* A *ein noetherscher Ring,* $\mathfrak{a} \subset A$ *ein Ideal,* M *ein endlicher* A*-Modul,* $N \subset M$ *ein Untermodul. Dann ist die Filtrierung* $(\mathfrak{a}^n M \cap N)_{n=0,1,\ldots}$ *von* N *im wesentlichen* $\mathfrak{a}$*-adisch, in Formeln:* $\exists\, n_0 \in \mathbb{N}$ *mit* $\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-n_0}\cdot(\mathfrak{a}^{n_0} M \cap N)$ *für alle* $n \geq n_0$.

Beweis: Wegen $\mathfrak{a}(\mathfrak{a}^n M \cap N) \subset \mathfrak{a}^{n+1} M \cap N$ ist die Filtrierung $\mathfrak{a}$-zulässig, und $N' = \bigoplus_{n\geq 0} (\mathfrak{a}^n M \cap N)$ ist ein graduierter Untermodul des A'-Moduls $M' = \bigoplus_{n\geq 0} \mathfrak{a}^n M$. Letzterer ist ein endlicher A'-Modul; denn aus $M = Am_1 + \ldots + Am_r$ folgt $M' = A'm_1 + \ldots + A'm_r$. Wenn $\mathfrak{a} = (a_1,\ldots,a_s)$ ist, erhält man einen surjektiven Ringhomomorphismus $A[X_1,\ldots,X_s] \rightarrow A'$ durch die Vorschrift $X_i \longmapsto a_i \in A_1' = \mathfrak{a}$. Also ist A' nach dem Hilbertschen Basissatz (3.30) noethersch, und N' ist mit M' ein endlicher A'-Modul. Nun wende 5.4 an! –

Folgerung 5.6 (*Krullscher Durchschnittssatz*): *Seien* A *ein noetherscher Ring,* $\mathfrak{a} \subset A$ *ein Ideal,* M *ein endlicher* A*-Modul und* $N := \bigcap_{n\geq 0} \mathfrak{a}^n M$. *Dann ist* $\mathfrak{a}N = N$.

Beweis: Für genügend großes n gilt $N = \mathfrak{a}^n M \cap N \overset{5.5}{=} \mathfrak{a}(\mathfrak{a}^{n-1} M \cap N) = \mathfrak{a}N$. –

Folgerung 5.7 *Seien* $A, \mathfrak{a}, M$ *wie oben und zusätzlich* $\mathfrak{a} \subset \mathrm{Jac}(A)$, *so ist* $\bigcap_{i\geq 0} \mathfrak{a}^n M = 0$.

Beweis: Lemma von Nakayama (3.19) zusammen mit 5.6. –

Folgerung 5.8 *Seien* A *noethersch,* $\mathfrak{a} \subset \mathrm{Jac}(A)$ *ein Ideal. Dann ist* $\bigcap_{n\geq 0} \mathfrak{a}^n = (0)$. –

2. Existenz und einfache Eigenschaften des Hilbert-Samuel-Polynoms

Lemma 5.9 *Sei* $f(X) \in \mathbb{Q}[X]$, $f(n) \geq 0$ *für fast alle* $n \in \mathbb{N}$. *Dann ist der höchste Koeffizient* > 0.

Beweis: Mit $f(X) = a_r X^r + a_{r-1} X^{r-1} + \ldots + a_0$ gilt
$\frac{f(X)}{X^r} = a_r + a_{r-1}\frac{1}{X} + \ldots + a_0 \frac{1}{X^r}$, also $0 \leq \lim_{n\to\infty} \frac{f(n)}{n^r} = a_r$. –

Folgerung 5.10 *Seien* $f(X), g(X) \in \mathbb{Q}[X]$ *mit positiven höchsten Koeffizienten,* $f(n) \geq g(n)$ *für fast alle* $n \in \mathbb{N}$. *Dann gilt* $\operatorname{grad} f \geq \operatorname{grad} g$. *Ist außerdem* $\operatorname{grad} f = \operatorname{grad} g$, *so ist der höchste Koeffizient von* f $\geq$ *dem höchsten Koeffizienten von* g.

Beweis: Wäre $\operatorname{grad} g > \operatorname{grad} f$, $f = a_r X^r + \ldots + a_0$, $g = b_s X^s + \ldots + b_0$ $(a_r, b_s > 0)$, so $0 \geq \lim_{n\to\infty} \frac{1}{n^s}(g(n) - f(n)) = b_s$. Widerspruch!

Ist $\operatorname{grad} g = \operatorname{grad} f$, so $0 \le \lim\limits_{n\to\infty} \frac{1}{n^s}(f(n)-g(n)) = a_r - b_r$. —

Bemerkung 5.11 Ist $f \in \mathbb{Q}[X]$, $n_0 \in \mathbb{Z}$, $g(X) := f(X+n_0)$, so haben f und g gleichen Grad und gleichen höchsten Koeffizienten.

Lemma 5.12 *Für* $r \ge -1$ *und eine Abbildung* $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ *sind die folgenden Aussagen äquivalent:*

(*i*) *Es gibt ein Polynom* $P(X) \in \mathbb{Q}[X]$ *mit* $\operatorname{grad} P \le r+1$ *und* $f(n) = P(n)$ *für fast alle* n.

(*ii*) *Es gibt ein Polynom* $Q(X) \in \mathbb{Q}[X]$ *mit* $\operatorname{grad} Q \le r$ *und* $f(n+1)-f(n) = Q(n)$ *für fast alle* n.

Beweis: (i) ⇒ (ii) folgt wegen 5.11 sofort.
(ii) ⇒ (i): Definiere Polynome $\binom{X}{i}$ vom Grad i in $\mathbb{Q}[X]$ wie folgt: $\binom{X}{0} = 1$, $\binom{X}{i} = \frac{1}{i!}X(X-1)\cdot\ldots\cdot(X-i+1)$ für $i > 0$. Diese bilden offenbar eine Basis von $\mathbb{Q}[X]$ über $\mathbb{Q}$. Sei $Q(X) = \sum\limits_{k=0}^{r} a_k\binom{X}{k}$ und $f(n+1)-f(n) = Q(n)$ für $n > n_0$. Man erhält: $f(n+1) = Q(n)+f(n) = Q(n)+Q(n-1)+f(n-1) = \ldots$

$$= \sum_{p=0}^{n-n_0} Q(n-p)+f(n_0) = \sum_{k=0}^{r} a_k \sum_{p=0}^{n-n_0}\binom{n-p}{k} + f(n_0)$$

$$= \sum_{k=0}^{r} a_k\left(\sum_{\sigma=0}^{n}\binom{\sigma}{k} - \sum_{\sigma=0}^{n_0-1}\binom{\sigma}{k}\right) + f(n_0) = \sum_{k=0}^{r} a_k\binom{n+1}{k+1} + c\,.$$

Dabei wurde die bekannte (durch Induktion leicht zu beweisende) Identität $\sum\limits_{\sigma=0}^{n}\binom{\sigma}{k} = \sum\limits_{\sigma=k}^{n}\binom{\sigma}{k} = \binom{n+1}{k+1}$ benutzt und $c = -\sum\limits_{k=0}^{r} a_k\binom{n_0}{k+1} + f(n_0)$ gesetzt. Das gesuchte Polynom ist $P = \sum\limits_{k=0}^{r} a_k\binom{X+1}{k+1} + c$. —

Im folgenden sei $A = \bigoplus\limits_{n\ge 0} A_n$ ein graduierter Ring mit folgenden Eigenschaften:

(1) A_0 ist von endlicher Länge (als A_0-Modul).

(2) A wird als Ring von $A_0 \cup \{x_1,\ldots,x_r\}$ erzeugt, wobei alle $x_i \in A_1$ sind.

Bemerkung 5.13 Unter diesen Bedingungen hat man einen surjektiven Ringhomomorphismus

$$A_0[X_1,\ldots,X_r] \longrightarrow A\,,$$

definiert durch $X_i \longmapsto x_i$. Daraus erhält man:

a) A ist noethersch, da A_0 (nach 4.47) noethersch ist;

b) $l_{A_0}(A_i) \le l_{A_0}(A_0) \cdot \binom{r+i-1}{r-1}$, da $\binom{r+i-1}{r-1}$ die Anzahl der unitären Monome vom Grade i in r Unbestimmten ist. (Dies ist bekannt und durch Induktion nach i leicht zu beweisen.) Infolgedessen ist
$l_{A_0}\left(\bigoplus_{i=0}^{n-1} A_i\right) \le l_{A_0}(A_0)\binom{r+n-1}{r}$.

Sei $M = \bigoplus_{n\le 0} M_n$ ein graduierter endlicher A-Modul. Dann gibt es ein endliches Erzeugendensystem, bestehend aus homogenen Elementen. (Siehe Beweis von 5.4). Sei also $m_1,\dots,m_r$ mit $m_i \in M_{j_i}$ ein Erzeugendensystem von M. Dann gilt $M_n = \sum_{i=1}^{r} A_{n-j_i}m_i$, wobei $A_s := 0$ für $s < 0$ gesetzt wird. Da die A_{n-j_i} endliche A_0-Moduln sind, ist auch M_n ein endlicher A_0-Modul, daher mit A_0 von endlicher Länge (4.51).

Beispiel 5.14 Sei A ein noetherscher Ring, $\mathfrak{a}$ ein Ideal, derart daß $A/\mathfrak{a}$ von endlicher Länge ist. Betrachte $gr^n_{\mathfrak{a}}(A) = \mathfrak{a}^n/\mathfrak{a}^{n+1}$. Wenn $a_1,\dots,a_r$ ein Erzeugendensystem von $\mathfrak{a}$ ist, wird $\mathfrak{a}^n$ von den Produkten der Form $a_1^{j_1}\cdot\ldots\cdot a_r^{j_r}$ mit $\sum_{k=1}^{r} j_k = n$ erzeugt. Also wird der graduierte Ring $gr_{\mathfrak{a}}(A)$ von A_0 und den Restklassen $\bar a_1,\dots,\bar a_r \in \mathfrak{a}/\mathfrak{a}^2 = A_1$ erzeugt.

Satz 5.15 *(Hilbert) Sei* $A = \bigoplus_{n\ge 0} A_n$ *ein graduierter Ring, der (wie oben) folgende Eigenschaften hat:*

(1) A_0 *ist ein* A_0*-Modul endlicher Länge,*

(2) A *wird als Ring von* A_0 *und endlich vielen Elementen* $x_1,\dots,x_r \in A_1$ *erzeugt.*

Ferner sei M *ein graduierter endlicher* A*-Modul. Dann ist*
$f(n) := l_{A_0}\left(\bigoplus_{i=0}^{n-1} M_i\right)$ *für große* n *ein Polynom aus* $\mathbb{Q}[X]$. *Mit anderen Worten: Es gibt ein Polynom* $P \in \mathbb{Q}[X]$ *mit* $f(n) = P(n)$ *für fast alle* $n \in \mathbb{N}$. *Es ist* $\operatorname{grad} P \le r$ *und der höchste Koeffizient von* P *positiv.*

P heißt Hilbert-Samuel-Polynom von M.

Beweis: Induktion über r: Für $r = 0$ ist $A = A_0$ von endlicher Länge, also $l_{A_0}(M) < \infty$ (4.51) und deshalb $l_{A_0}(M_n) = 0$ für fast alle n.

Sei jetzt $r > 0$. Der Ring $B = A/Ax_r$ ist ein graduierter Ring, da Ax_r nach 5.2 ein graduiertes Ideal ist. B erfüllt (1), (2) mit $r-1$ anstelle von r: Es ist $B_0 = A_0$, und B wird als Ring von $B_0 \cup \{\bar{x}_1,\dots,\bar{x}_{r-1}\}$ erzeugt ($\bar{x}_i$ = Restklasse von x_i in $A_1/Ax_r \cap A_1$). Nach Induktionsvoraussetzung ist die Behauptung des Satzes für B richtig. Betrachte nun $\varphi\colon M_n \longrightarrow M_{n+1}$ $(m \longmapsto x_r m)$. Setze $N_n := \operatorname{Ker}(\varphi)$ und $R_{n+1} := M_{n+1} / x_r M_n$, $R_0 := M_0$. Man hat eine exakte Folge $0 \longrightarrow N_n \longrightarrow M_n \longrightarrow M_{n+1} \longrightarrow R_{n+1} \longrightarrow 0$, also $l_{A_0}(M_{n+1}) - l_{A_0}(M_n) = l_{A_0}(R_{n+1}) - l_{A_0}(N_n)$ (sofortige Verallgemeinerung von 4.46). $N = \bigoplus_{i\geq 0} N_i$, $R = \bigoplus_{i\geq 0} R_i$ sind graduierte endliche A-Moduln. Da $x_r N = 0$, $x_r R = 0$, sind N und R graduierte B-Moduln. Nach Induktionsvoraussetzung und 5.12 gibt es also Polynome f, g vom Grade $\leq r-2$ mit $l_{A_0}(N_n) = f(n)$ und $l_{A_0}(R_n) = g(n)$ für große n. (Beachte $A_0 = B_0$.) Also gibt es auch ein Polynom Q_1 vom Grade $\leq r-2$ mit $l_{A_0}(M_{n+1}) - l_{A_0}(M_n) = l_{A_0}(R_{n+1}) - l_{A_0}(N_n) = Q_1(n)$ für fast alle $n \in \mathbb{N}$. Also gibt es nach 5.12 ein Polynom Q_2 vom Grade $\leq r-1$ mit $l_{A_0}(M_n) = Q_2(n)$ für große n und schließlich wieder mit 5.12 ein Polynom P vom Grade $\leq r$ mit $l_{A_0}\left(\bigoplus_{i=0}^{n-1} M_i\right) = P(n)$ für große n.

Daß sein höchster Koeffizient positiv ist, folgt aus 5.9. –

<u>Definition 5.16</u> Sei A ein semilokaler noetherscher Ring. Ein Ideal $\mathfrak{a} \subset A$ heißt Definitionsideal für A, wenn es ein $n \in \mathbb{N}$ gibt mit

$$\operatorname{Jac}(A)^n \subset \mathfrak{a} \subset \operatorname{Jac}(A) .$$

<u>Feststellung 5.17</u> *Sei A ein semilokaler noetherscher Ring. Für ein Ideal $\mathfrak{a} \subset A$ sind äquivalent:*

(*i*) $\mathfrak{a}$ *ist ein Definitionsideal für* A.

(*ii*) $\mathfrak{a} \subset \operatorname{Jac}(A)$ *und* $A/\mathfrak{a}$ *ist artinsch, d.h. von endlicher Länge.*

(*iii*) $\operatorname{Supp}_A(A/\mathfrak{a}) = \{\mathfrak{m} \mid \mathfrak{m} \subset A$ *maximales Ideal*$\}$.

Dies folgt sofort aus 4.51. –

<u>Bemerkung 5.18</u> Ist A lokal, noethersch mit dem maximalen Ideal $\mathfrak{m}$, so ist (i) - (iii) aus 5.17 äquivalent zu

(iv) $\mathfrak{a}$ ist $\mathfrak{m}$-primär. (4.24)

Lemma 5.19 *Seien* A *ein noetherscher Ring,* $\mathfrak{a} \subset A$ *ein Ideal,* M *ein endlicher* A*-Modul, versehen mit einer i.w.* $\mathfrak{a}$*-adischen Filtrierung* $F: M = M_0 \supset M_1 \supset \dots$. *Dann ist der graduierte Modul* $gr_F(M) := \bigoplus_{n\geq 0}(M_n/M_{n+1})$ *über dem graduierten Ring* $gr_{\mathfrak{a}}(A) = \bigoplus_{n\geq 0}(\mathfrak{a}^n/\mathfrak{a}^{n+1})$ *endlich.*

Beweis: Sei $M_{n+1} = \mathfrak{a}M_n$ für $n \geq n_0$. Dann wird $gr_F(M)$ über A offenbar von $N := M_0/M_1 \oplus \dots \oplus M_{n_0}/M_{n_0+1}$ erzeugt. Da A noethersch ist, besitzt der A-Modul N ein endliches Erzeugendensystem. Dies ist auch ein Erzeugendensystem des $gr_{\mathfrak{a}}(A)$-Moduls $gr_F(M)$. —

Satz 5.20 *Seien* A *ein semilokaler noetherscher Ring,* $\mathfrak{a} \subset A$ *ein Definitionsideal,* M *ein endlicher* A*-Modul und* $M = M_0 \supset M_1 \supset \dots$ *.eine i.w.* $\mathfrak{a}$*-adische Filtrierung* F. *Dann sind* $l_A(M/M_n)$ *und* $l_A(M/\mathfrak{a}^nM)$ *endlich und für große* n *Polynome* $P_F(M,n)$ *bzw.* $P_{\mathfrak{a}}(M,n)$ *in* n.

Beweis: M_i/M_{i+1} und $\mathfrak{a}^iM/\mathfrak{a}^{i+1}M$ sind endliche Moduln über dem Ring endlicher Länge $A/\mathfrak{a}$ (5.17, siehe auch 3.2b)). Wegen 5.14 und 5.19 sind die Voraussetzungen des Satzes 5.15 für den Ring $gr_{\mathfrak{a}}(A)$ und die beiden Moduln $gr_F(M)$ und $gr_{\mathfrak{a}}(M) := \bigoplus_{n\geq 0}(\mathfrak{a}^iM/\mathfrak{a}^{i+1}M)$ erfüllt. Deshalb sind $l_A(M/M_n) = l_{A/\mathfrak{a}}\left(\bigoplus_{i=0}^{n-1}(M_i/M_{i+1})\right)$ und $l_A(M/\mathfrak{a}^nM) = l_{A/\mathfrak{a}}\left(\bigoplus_{i=0}^{n-1}(\mathfrak{a}^iM/\mathfrak{a}^{i+1}M)\right)$ für große n Polynome $P_F(M,n)$ bzw. $P_{\mathfrak{a}}(M,n)$ in n.

Satz 5.21 $P_F(M,n)$ *und* $P_{\mathfrak{a}}(M,n)$ *haben denselben Grad und denselben höchsten Koeffizienten.*

Beweis: $M_{n+n_0} = \mathfrak{a}^nM_{n_0} \subset \mathfrak{a}^nM \subset M_n$ für ein n_0 und alle $n \geq 0$. Für große n ist folglich $P_F(M,n+n_0) \geq P_{\mathfrak{a}}(M,n) \geq P_F(M,n)$, also $\mathrm{grad}_n P_F(M,n+n_0) \geq \mathrm{grad}_n P_{\mathfrak{a}}(M,n) \geq \mathrm{grad}_n P_F(M,n)$ nach 5.10. Da $\mathrm{grad}_n P_F(M,n+n_0) = \mathrm{grad}_n P_F(M,n)$ nach 5.11, folgt $\mathrm{grad}_n P_F(M,n) = \mathrm{grad}_n P_{\mathfrak{a}}(M,n)$, und wegen 5.10 und 5.11 auf analoge Weise: P_F und $P_{\mathfrak{a}}$ haben denselben höchsten Koeffizienten. —

Satz 5.22 *Sei* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *eine exakte Folge von endlichen* A*-Moduln. Dann gilt:*

a) $P_{\mathfrak{a}}(M',n)$ *und* $P_{\mathfrak{a}}(M,n) - P_{\mathfrak{a}}(M'',n)$ *haben denselben Grad und denselben höchsten Koeffizienten.*

b) $\mathrm{grad}\, P_{\mathfrak{a}}(M',n) \leq \mathrm{grad}\, P_{\mathfrak{a}}(M,n)$.

Beweis: Betrachte auf $M' \subset M$ die Filtrierung F': $M'_n := M' \cap \mathfrak{a}^n M$. Sie ist nach 5.5 (Artin-Rees) i.w. $\mathfrak{a}$-adisch. Mittels 4.45 und 3.9 erhält man $l(M/\mathfrak{a}^n M) = l(M/\mathfrak{a}^n M+M') + l(\mathfrak{a}^n M+M' / \mathfrak{a}^n M) = l(M''/\mathfrak{a}^n M'') + l(M'/\mathfrak{a}^n M \cap M')$ $= l(M''/\mathfrak{a}^n M'') + l(M'/M'_n)$. Also ist $P_\mathfrak{a}(M,n) = P_\mathfrak{a}(M'',n) + P_{F'}(M',n)$. Mit 5.21 folgt a) und, da die höchsten Koeffizienten der Polynome positiv sind, auch b). –

Folgerung 5.23 *Sei* $a \in A$ *ein Nichtnullteiler für den endlichen* A-*Modul* M *und* $M'' = M/aM$. *Dann ist* $\operatorname{grad}(P_\mathfrak{a}(M'',n)) < \operatorname{grad} P_\mathfrak{a}(M,n)$.

Beweis: $0 \longrightarrow M \xrightarrow{\varphi} M \longrightarrow M'' \longrightarrow 0$ mit $\varphi(m) := am$ ist exakt. $P_\mathfrak{a}(M,n)$ hat den gleichen Grad und höchsten Koeffizienten wie $P_\mathfrak{a}(M,n) - P_\mathfrak{a}(M'',n)$. –

Aufgaben und Hinweis

1) Sei $P \in \mathbb{Q}[X]$. Zeige: Es sind äquivalent: (i) $P(\mathbb{Z}) \subset \mathbb{Z}$; (ii) $P(n) \in \mathbb{Z}$ für fast alle $n \in \mathbb{N}$; (iii) $P = \sum_{i \geq 0} a_i \binom{X}{i}$ mit $a_i \in \mathbb{Z}$ ($a_i = 0$ für fast alle i).

2) Zeige: Der Ring der Polynome P, die obige Bedingungen erfüllen, ist nicht noethersch.

3) In diesem Buch spielt nur der Grad des Hilbert-Samuel-Polynoms eine Rolle. In anderen Zusammenhängen sind auch die Koeffizienten wichtig, insbesondere der höchste. Vgl. [Hartshorne] I. 7 und [Northcott].

§ 6 DIMENSIONSTHEORIE

Definition 6.1 a) Es sei A ein Ring. Eine endliche Kette von $n+1$ verschiedenen Primidealen $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_n$ heißt Primidealkette der Länge n in A.

b) Ist $\mathfrak{p}$ ein Primideal in A, so heißt das Supremum der Längen von Primidealketten mit $\mathfrak{p}_0 = \mathfrak{p}$ die Höhe von $\mathfrak{p}$, bezeichnet mit $\mathrm{ht}(\mathfrak{p})$.

c) Ist $\mathfrak{a} \subset A$ ein Ideal in A, so heißt die Höhe von $\mathfrak{a}$ das Infimum der Höhen der Primideale $\mathfrak{p}$ in A, die $\mathfrak{a}$ umfassen:
$\mathrm{ht}(\mathfrak{a}) = \inf\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \supset \mathfrak{a}\}$.

d) Die (Krull-) Dimension eines Ringes A, bezeichnet mit $\dim(A)$, ist das Supremum der Höhen aller Primideale in A, also $\dim(A) := \sup\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p}$ Primideal in $A\}$.

e) Ist M ein endlicher A-Modul, so definiert man die Dimension von M durch $\dim_A(M) := \dim(A/\mathrm{Ann}_A(M))$.

<u>Bemerkungen 6.2</u> a) $\mathrm{ht}\,\mathfrak{p} = \dim A_{\mathfrak{p}}$.

b) Die Dimension eines Körpers ist 0, die eines Hauptidealringes 1, wenn er kein Körper ist.

c) Nullring und Nullmodul haben die Dimension $-\infty$.

<u>Feststellung 6.3</u> *Ist* A *noethersch,* $M \neq 0$ *ein endlicher* A-*Modul, so sind äquivalent:*

(i) M *ist ein* A-*Modul endlicher Länge;*

(ii) $A/\mathrm{Ann}(M)$ *ist artinsch, d.h. (nach 4.47) von endlicher Länge;*

(iii) $\dim_A(M) = 0$.

<u>Beweis:</u> Da $\dim(A/\mathrm{Ann}(M)) = 0$ bedeutet, daß jedes Primideal von $A/\mathrm{Ann}(M)$ maximal ist, ist dies eine unmittelbare Folgerung aus 4.51. —

<u>Definition 6.4</u> Seien A noethersch, semilokal, $M \neq 0$ ein endlicher A-Modul. Definiere

$$s_A(M) := \inf\left\{n \in \mathbb{N} \mid \exists\, a_1,\dots,a_n \in \mathrm{Jac}(A) \text{ mit } l_A(M/a_1M+\dots+a_nM) < \infty\right\}.$$

<u>Bemerkung 6.5</u> $s_A(M) < \infty$. Wenn nämlich $\mathrm{Jac}(A) = (a_1,\dots,a_r)$ ist, so ist $s(M) \le r$. $(l(A/\mathrm{Jac}(A)) < \infty$ (5.17) $\Rightarrow l(M/\mathrm{Jac}(A)\cdot M) < \infty$ (6.3).)

<u>Definition 6.6</u> Seien A noethersch, semilokal, $M \neq 0$ ein endlicher A-Modul und $\mathfrak{a}$ ein Definitionsideal. Nach 5.20 gibt es ein Polynom $P_{\mathfrak{a}}(M,X) \in \mathbb{Q}[X]$ mit $l(M/\mathfrak{a}^nM) = P_{\mathfrak{a}}(M,n)$ für große n.

Definiere: $d_A(M) := \mathrm{grad}\, P_{\mathfrak{a}}(M,X)$.

Bemerkung 6.7 a) $d_A(M)$ ist von der Wahl des Definitionsideals $\mathfrak{a}$ unabhängig. Ist nämlich $\mathfrak{b}$ ein anderes Definitionsideal, so gilt: $\exists\, r,s$: $\mathrm{Jac}(A)^r \subset \mathfrak{a} \subset \mathrm{Jac}(A)$, $\mathrm{Jac}(A)^s \subset \mathfrak{b} \subset \mathrm{Jac}(A)$, also $\mathfrak{b}^r \subset \mathfrak{a}$, $\mathfrak{a}^s \subset \mathfrak{b}$, somit $P_{\mathfrak{a}}(M,n) \le P_{\mathfrak{b}}(M,nr) \le P_{\mathfrak{a}}(M,nsr)$, folglich grad $P_{\mathfrak{a}}$ = grad $P_{\mathfrak{b}}$, da grad $P_{\mathfrak{a}}(M,X)$ = grad $P_{\mathfrak{a}}(M,srX)$.

b) Wenn es ein Definitionsideal $\mathfrak{a}$ mit s Erzeugenden gibt, ist $\mathfrak{a}/\mathfrak{a}^2$ als $A/\mathfrak{a}$-Modul von s Elementen erzeugt, also $d_A(M) \le s$ nach 5.15.

Lemma 6.8 *Sei A semilokal, noethersch,* $M \neq 0$ *ein endlicher A-Modul. Dann gilt:*

a) Für $a \in \mathrm{Jac}(A)$ *ist* $s_A(M/aM) \ge s_A(M)-1$.

b) Wenn $a \in \mathrm{Jac}(A)$ *in keinem der Primideale* $\mathfrak{p}$ *von* $\mathrm{Supp}_A(M)$ *mit* $\dim A/\mathfrak{p} = \dim M$ *liegt, dann ist* $\dim_A(M/aM) \le \dim_A(M)-1$.

Beweis: a) Seien $a_1,\dots,a_s$ mit $s = s_A(\overline{M})$ gewählt,
$\overline{M} := M/aM \Rightarrow l_A(\overline{M}/(a_1,\dots,a_s)\overline{M}) = l_A(M/(a,a_1,\dots,a_s)M)$
$\Rightarrow s_A(M/aM) + 1 \ge s_A(M)$.

b) Der Fall $\dim M = \infty$ (der übrigens nicht vorkommt, s.u.) ist trivial. Sei also $\dim M = n < \infty$. Wäre $\dim_A(M/aM) \ge n$, so gäbe es eine Primidealkette $\mathfrak{p}_0 \supsetneqq \dots \supsetneqq \mathfrak{p}_n$ mit $\mathfrak{p}_n \supset \mathrm{Ann}(M/aM) \supset \mathrm{Ann}(M) + (a) \supset \mathrm{Ann}(M)$. Es wäre $\dim A/\mathfrak{p}_n \ge n$, also $\dim A/\mathfrak{p}_n = n$ und deshalb nach Voraussetzung $a \notin \mathfrak{p}_n$. Widerspruch. –
(N.B.: Sei $\mathfrak{p} \in \mathrm{Supp}\, M$. Wenn $\dim A/\mathfrak{p} = \dim M < \infty$ ist, dann ist $\mathfrak{p}$ minimal in $\mathrm{Supp}\, M$, aber nicht immer umgekehrt! Vgl. A6.)

Theorem 6.9 *Mit den obigen Voraussetzungen und Bezeichnungen gilt:*
$\dim_A(M) = d_A(M) = s_A(M)$.

Beweis: Ohne Einschränkung ist $\mathrm{Ann}_A(M) = 0$.

a) $\dim_A(M) \le d_A(M)$: Induktion nach $d_A(M)$. Wenn $d_A(M) = 0$, ist $l_A(M/\mathrm{Jac}(A)^n M)$ konstant für große n. D.h. es gibt ein n mit $\mathrm{Jac}(A)^{n+1}M = \mathrm{Jac}(A)^n M$. Nach 3.19 (Nakayama) ist $\mathrm{Jac}(A)^n M = 0$, also $\dim_A(M) \le \dim(A/\mathrm{Jac}(A)^n) = 0$. Sei jetzt $d_A(M) \ge 1$ und $\mathfrak{p}_0$ ein minimales Primideal in A mit $\dim(A/\mathfrak{p}_0) = \dim_A(M) = \dim A$. Auch wenn $\dim A = \infty$ sein sollte, gibt es ein solches, da die Anzahl der minimalen Primideale endlich ist (4.17). Nach 4.15 ist $\mathfrak{p}_0 \in \mathrm{Ass}\, M$. Also besitzt M einen Untermodul $N \simeq A/\mathfrak{p}_0$. Nach 5.22 b) ist $d_A(N) \le d_A(M)$. Da $\dim_A(N) = \dim(A/\mathfrak{p}_0) = \dim_A(M)$ ist, genügt es also, $\dim_A(N) \le d_A(N)$ zu zeigen. Wenn also $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \dots \subsetneqq \mathfrak{p}_n$ eine Primidealkette ist, müssen

wir $n \leq d_A(N)$ nachweisen. Für $n = 0$ ist das klar. Sonst wähle $a \in \mathfrak{p}_1 - \mathfrak{p}_0$. Da a ein Nichtnullteiler für $N \simeq A/\mathfrak{p}_0$ ist, gilt $d_A(N/aN) \leq d_A(N) - 1$ nach 5.23. Nach Induktionsvoraussetzung ist $\dim_A(N/aN) \leq d_A(N/aN)$. Andererseits ist $\dim_A(N/aN) \geq n-1$, da $\mathrm{Ann}_A(N/aN) = \mathfrak{p}_0 + (a) \subset \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n$ gilt. Insgesamt erhält man $n-1 \leq \dim_A(N/aN) \leq d_A(N/aN) \leq d_A(N)-1$, somit $n \leq d_A(N)$.
Beachte: a) impliziert $\dim_A(M) < \infty$.

b) $d_A(M) \leq s_A(M)$: Für $s = s_A(M)$ gibt es $a_1,\ldots,a_s \in \mathrm{Jac}(A)$ mit $l_A(M/(a_1,\ldots,a_s)M) < \infty$. Nach 6.3 und 5.17 ist $(a_1,\ldots,a_s)$ ein Definitionsideal. Wegen 6.7 b) folgt hieraus $d_A(M) \leq s_A(M)$.

c) $s_A(M) \leq \dim_A(M)$: Induktion nach $\dim_A(M)$. (Nach a) ist $\dim_A(M) < \infty$.) Im Falle $\dim_A(M) = 0$ ist $l_A(M) < \infty$, also $s_A(M) = 0$ nach Definition von $s_A(M)$. Sei nun $\dim_A(M) > 0$. Wir betrachten die Primideale $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ mit $\dim A/\mathfrak{p}_i = \dim_A(M) = \dim A$. Sie sind minimal, also von endlicher Anzahl. Keines ist maximal, da $\dim_A(M) > 0$. Weil A semilokal, d.h. $\mathrm{Jac}(A) = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t$ mit maximalen Idealen $\mathfrak{m}_j$ ist, würde aus $\mathfrak{p}_i \supset \mathrm{Jac}(A)$ folgen $\mathfrak{p}_i = \mathfrak{m}_j$ für ein j. Wir erhalten $\mathfrak{p}_i \not\supset \mathrm{Jac}(A)$ und deshalb $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r \not\supset \mathrm{Jac}(A)$ nach 1.21. Wähle $a \in \mathrm{Jac}(A) - (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r)$. Nach 6.8 gilt $s_A(M/aM) \geq s_A(M)-1$ und $\dim_A(M/aM) \leq \dim_A(M)-1$, also mit der Induktionsvoraussetzung $s_A(M)-1 \leq s_A(M/aM) \leq \dim_A(M/aM) \leq \dim_A(M)-1$ und deshalb $s_A(M) \leq \dim_A(M)$. —

Folgerung 6.10 *Ist* A *ein semilokaler noetherscher Ring, so ist* $\dim A$ *gleich der kleinstmöglichen Erzeugendenzahl eines Definitionsideals, insbesondere ist* $\dim A < \infty$. —

Bemerkung 6.11 Es gibt noethersche Ringe unendlicher Dimension. Siehe [Nagata] Appendix 1, Example 1.

Folgerung 6.12 *In einem noetherschen Ring hat jedes Primideal endliche Höhe. Absteigende Ketten von Primidealen werden stationär.*

Zum Beweis beachte: $\mathrm{ht}\,\mathfrak{p} = \dim A_{\mathfrak{p}}$. —

Folgerung 6.13 *Seien* A *semilokal, noethersch,* M *ein endlicher* A-*Modul, ferner* $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ *die Primideale in* $\mathrm{Supp} M$ *mit* $\dim A/\mathfrak{p}_i = \dim_A M$. *Dann gilt für* $a \in \mathrm{Jac}(A)$

$$\dim_A(M/aM) \geq \dim_A(M)-1 .$$

Das Gleichheitszeichen gilt genau dann, wenn $a \notin \bigcup_{i=1}^{r} \mathfrak{p}_i$.

Beweis: 6.8 und $\dim_A(M) = s_A(M)$. —

Definition 6.14 Ist A ein semilokaler noetherscher Ring, M ein endlicher A-Modul mit $\dim_A(M) = n$, so heißt $(a_1,\ldots,a_n)$ Parametersystem für M , wenn $M/(a_1,\ldots,a_n)M$ von endlicher Länge ist und $a_1,\ldots,a_n \in \mathrm{Jac}(A)$ gilt.

Definition 6.15 Ist A ein Ring, M ein endlicher A-Modul, so

$$\mu_A(M) := \mathrm{Min}\left\{s \mid \exists\, m_i \in M,\ 1 \leq i \leq s \ \text{ mit } \ M = Am_1 + \ldots + Am_s\right\} .$$

Ist k ein Körper, V ein k-Vektorraum, so ist $\mu_k(V)$ die k-Vektorraumdimension von V über k , die wir hier nicht mit "dim" bezeichnen wollen. In diesem Fall ist auch die Bezeichnung $\mathrm{rg}_k(V)$ ("Rang") üblich.

Feststellung 6.16 *Ist* A *lokal mit maximalem Ideal* $\mathfrak{m}$ *und Restklassenkörper* k *und* M *ein endlicher* A*-Modul, so ist*

$$\mu_A(M) = \mu_k(M/\mathfrak{m}M) .$$

Beweis: "$\geq$" ist trivial.
"$\leq$": Sei $\overline{m}_1,\ldots,\overline{m}_r$ eine Basis von $M/\mathfrak{m}M$ über $k = A/\mathfrak{m}$ und $N = Am_1 + \ldots + Am_r$, so ist $N+\mathfrak{m}M = M$, also $M = N$ nach 3.20 (Nakayama). —

Folgerung 6.17 $\dim(A) \leq \mu_k(\mathfrak{m}/\mathfrak{m}^2)$.

Beweis mittels 6.10 und $\mu_A(\mathfrak{m}) = \mu_k(\mathfrak{m}/\mathfrak{m}^2)$ nach 6.16. —

Bemerkung 6.18 Lokale, noethersche Ringe A , für die $\dim A = \mu_k(\mathfrak{m}/\mathfrak{m}^2)$ gilt, heißen regulär und werden später (§§ 14,16) genauer untersucht.

Satz 6.19 *Seien* A *ein noetherscher Ring,* $\mathfrak{p} \subset A$ *ein Primideal und* $n \in \mathbb{N}$. *Dann sind äquivalent:*

(*i*) $\mathrm{ht}\,\mathfrak{p} \leq n$.

(*ii*) $\exists\, a_1,\ldots,a_n \in A$, *so daß* $\mathfrak{p}$ *minimal ist unter den Primidealen, die* $(a_1,\ldots,a_n)$ *umfassen.*

Beweis: Setze $\mathfrak{a} := (a_1,\dots,a_n)$.
(ii) $\Rightarrow$ (i): In dem lokalen Ring $A_\mathfrak{p}$ ist das maximale Ideal $\mathfrak{p}A_\mathfrak{p}$ minimal unter allen Primidealen, die $\mathfrak{a}A_\mathfrak{p}$ umfassen. (Beachte: Für ein Primideal $\mathfrak{q} \subset \mathfrak{p}$ von A mit $\mathfrak{q}A_\mathfrak{p} \supset \mathfrak{a}A_\mathfrak{p}$ gilt $\mathfrak{q} = i^{-1}_{A,\mathfrak{p}}(\mathfrak{q}A_\mathfrak{p}) \supset i^{-1}_{A,\mathfrak{p}}(\mathfrak{a}A_\mathfrak{p}) \supset \mathfrak{a}$ nach 2.13, also $\mathfrak{q} = \mathfrak{p}$.) Somit ist
$\mathfrak{a}A_\mathfrak{p} = (\frac{a_1}{1},\dots,\frac{a_n}{1})A_\mathfrak{p}$ ein Definitionsideal von $A_\mathfrak{p}$. Wende nun 6.10 an.
(i) $\Rightarrow$ (ii): Nach 6.10 gibt es $\frac{a_1}{s_1},\dots,\frac{a_n}{s_n} \in \mathfrak{p}A_\mathfrak{p}$, so daß $\left(\frac{a_1}{s_1},\dots,\frac{a_n}{s_n}\right) A_\mathfrak{p}$ ein Definitionsideal für $A_\mathfrak{p}$ ist. $\mathfrak{p}A_\mathfrak{p}$ ist also minimal unter allen Primidealen, die $\left(\frac{a_1}{s_1},\dots,\frac{a_n}{s_n}\right) A_\mathfrak{p}$ umfassen. Da die $\frac{s_i}{1}$ Einheiten in $A_\mathfrak{p}$ sind, ist $\mathfrak{p}A_\mathfrak{p} \supset (a_1,\dots,a_n)A_\mathfrak{p}$ ein minimales Primoberideal, also $\mathfrak{p} \supset (a_1,\dots,a_n)$ minimales Primoberideal in A (2.13). –

Folgerung 6.20 *Seien* $a \in A\text{-}A^*$ *und* $\mathfrak{p}$ *minimal unter den Primidealen, die* a *enthalten. Dann ist* $\mathrm{ht}(\mathfrak{p}) \le 1$. *(Krulls Hauptidealsatz)* –

Folgerung 6.21 *Seien* $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2$ *Primideale in* A. *Dann gibt es unendlich viele Primideale* $\mathfrak{q}$ *mit* $\mathfrak{p}_0 \subset \mathfrak{q} \subset \mathfrak{p}_2$.

Beweis: O.E. sei $\mathfrak{p}_0 = (0)$ und A lokal mit maximalem Ideal $\mathfrak{p}_2$. (Bilde sonst $A_{\mathfrak{p}_2}/\mathfrak{p}_0A_{\mathfrak{p}_2}$.) Sei $a \in \mathfrak{p}_2$. Nach 6.20 gibt es ein Primideal $\mathfrak{q}$ der Höhe ≤ 1 mit $a \in \mathfrak{q}$. Also ist $\mathfrak{p}_2 = \bigcup_{\substack{\mathfrak{q}\ \text{Primideal} \\ \mathrm{ht}(\mathfrak{q}) \le 1}} \mathfrak{q}$. Gäbe es nur endlich viele solche $\mathfrak{q}$, so wäre $\mathfrak{q} = \mathfrak{p}_2$ für ein solches $\mathfrak{q}$ nach 1.21 im Widerspruch zu $\mathrm{ht}(\mathfrak{p}_2) \ge 2$. –

Satz 6.22 *Sei* A *ein noetherscher Ring,* $A[X_1,\dots,X_n]$ *der Polynomring über* A *in* n *Unbestimmten. Dann gilt:* $\dim A[X_1,\dots,X_n] = \dim A + n$.

Zum Beweis benötigen wir mehrere Lemmata.

Lemma 6.23 *Ist* $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \dots \subsetneqq \mathfrak{p}_r$ *eine Primidealkette in* A, *so ist* $\mathfrak{p}_0A[X] \subsetneqq \mathfrak{p}_1A[X] \subsetneqq \dots \subsetneqq \mathfrak{p}_rA[X] \subsetneqq \mathfrak{p}_rA[X] + XA[X]$ *eine solche in* $A[X]$.

Beweis: Es ist $A[X] / (\mathfrak{p}_rA[X]+XA[X]) \simeq (A[X]/\mathfrak{p}_rA[X]) / (XA[X]+\mathfrak{p}_rA[X]/\mathfrak{p}_rA[X])$ $\simeq (A/\mathfrak{p}_r)[X] / (X) \simeq A/\mathfrak{p}_r$ integer. Der Rest ist klar. –

Folgerung 6.24 $\dim A[X] \ge \dim A + 1$.

Lemma 6.25 *Seien* $\mathfrak{p}' \subsetneqq \mathfrak{p}''$ *Primideale in* $A[X]$ *mit* $\mathfrak{p}' \cap A = \mathfrak{p}'' \cap A$. *Dann gilt* $\mathfrak{p}' = (\mathfrak{p}' \cap A)A[X]$.

Beweis: Schreibe $\mathfrak{p} := \mathfrak{p}' \cap A$. Die Inklusion $\mathfrak{p}' \supset \mathfrak{p}A[X]$ ist klar. Gälte $\mathfrak{p}' \supsetneqq \mathfrak{p}A[X]$, so wäre $\mathfrak{p}A[X] \subsetneqq \mathfrak{p}' \subsetneqq \mathfrak{p}''$ eine Primidealkette.

Man kann $\mathfrak{p} = (0)$ annehmen, da man für $A/\mathfrak{p} \subset (A/\mathfrak{p})[X] = A[X]/\mathfrak{p}[X]$ dieselben Verhältnisse hat. Setze nun $S := A - \{0\}$. Aus der Voraussetzung $\mathfrak{p}' \cap A = \mathfrak{p}'' \cap A = (0)$ folgt $\mathfrak{p}' \cap S = \mathfrak{p}'' \cap S = \emptyset$. Man gewänne also aus obiger Primidealkette der Länge 2 in $A[X]$ eine solche in $S^{-1}(A[X]) = (S^{-1}A)[X]$. Da aber $S^{-1}A$ ein Körper und deshalb $S^{-1}A[X]$ ein Hauptidealring ist, geht dies nicht. –

Lemma 6.26 *Seien* $\mathfrak{a} \subset A$ *ein Ideal,* $\mathfrak{p} \subset A$ *ein Primideal, minimal über* $\mathfrak{a}$. *Dann ist* $\mathfrak{p}A[X]$ *minimal über* $\mathfrak{a}A[X]$.

Beweis: Angenommen, es gäbe ein Primideal $\mathfrak{p}'$ in $A[X]$ mit $\mathfrak{p}A[X] \supsetneqq \mathfrak{p}' \supset \mathfrak{a}A[X]$. Da $\mathfrak{p}$ minimal, gälte wegen $\mathfrak{p} = \mathfrak{p}A[X] \cap A \supset \mathfrak{p}' \cap A \supset \mathfrak{a}$. daß $\mathfrak{p}' \cap A = \mathfrak{p}$, also wegen 6.25 $\mathfrak{p}' = \mathfrak{p}A[X]$ wäre. Widerspruch! –

Lemma 6.27 A *sei noethersch,* $\mathfrak{p}$ *ein Primideal in* A. *Dann ist* $ht_A(\mathfrak{p}) = ht_{A[X]}(\mathfrak{p}A[X])$.

Beweis: Setze $n = ht_A(\mathfrak{p})$. Es gibt $a_1, \ldots, a_n$, so daß $\mathfrak{p}$ minimal über $\mathfrak{a} := Aa_1 + \ldots + Aa_n$ ist (6.19). Nach 6.26 ist $\mathfrak{p}A[X]$ minimal unter den Primidealen, die $\mathfrak{a}A[X] = a_1A[X] + \ldots + a_nA[X]$ umfassen, also $ht_{A[X]}(\mathfrak{p}A[X]) \le n$ wiederum nach 6.19.

Ist umgekehrt $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n = \mathfrak{p}$ eine Primidealkette in A, so ist $\mathfrak{p}_0A[X] \subsetneqq \mathfrak{p}_1A[X] \subsetneqq \ldots \subsetneqq \mathfrak{p}_nA[X] = \mathfrak{p}A[X]$ eine solche in $A[X]$, also $ht_{A[X]}(\mathfrak{p}A[X]) \ge n$. –

Beweis von 6.22: Wegen 6.24 genügt es, $\dim A[X] \le \dim A + 1$ zu beweisen.

Sei $\mathfrak{p}'_0 \subsetneqq \mathfrak{p}'_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}'_r$ eine Primidealkette in $A[X]$. Zu zeigen ist: $\dim A \ge r-1$. Setze $\mathfrak{p}_i = \mathfrak{p}'_i \cap A$. Wenn $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r$, ist sogar $\dim A \ge r$. Sonst sei j maximal mit $\mathfrak{p}_j = \mathfrak{p}_{j+1}$. Dann gilt nach Lemma 6.25 $\mathfrak{p}_jA[X] = \mathfrak{p}'_j$, also $ht_A(\mathfrak{p}_j) = ht_{A[X]}(\mathfrak{p}'_j) \ge j$ gemäß 6.27. Wegen der Maximalität von j gilt $\mathfrak{p}_j = \mathfrak{p}_{j+1} \subsetneqq \mathfrak{p}_{j+2} \subsetneqq \ldots \subsetneqq \mathfrak{p}_r$. Es folgt $\dim A \ge ht_A(\mathfrak{p}_r) \ge r-(j+1)+ht_A(\mathfrak{p}_j) \ge r-j-1+j \ge r-1$. Damit ist 6.22 bewiesen. –

Folgerung 6.28 *Ist* k *ein Körper, dann ist* $\dim k[X_1,\ldots,X_n] = n$. —

Aufgaben und Hinweise

1) Sei A integer. Zeige: Das Ideal $(X_1,\ldots,X_r)$ im Polynomring $A[X_1,\ldots,X_n]$ ist ein Primideal der Höhe r.

2) Sei A ein Ring, $n \in \mathbb{N}$, so daß jedes Ideal von A von $\leq n$ Elementen erzeugt wird. (Dann ist A natürlich noethersch.) Zeige: $\dim A \leq 1$.
(Reduziere die Behauptung auf den Fall: A lokal, mit maximalem Ideal $\mathfrak{m}$. Jedes $\mathfrak{m}^r$ ist dann von $\leq n$ Elementen erzeugt, d.h. $l_A(\mathfrak{m}^r/\mathfrak{m}^{r+1}) \leq n$. Wende $\dim A = d_A(A)$ an.)

3) Zeige: In einem faktoriellen Ring sind die Primideale der Höhe 1 genau die von den Primelementen erzeugten Hauptideale.

4) Sei A faktoriell, $a \in A - \{0\}$ und $a = up_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_r}$ eine Primfaktorzerlegung mit $u \in A^*$ und paarweise nicht assoziierten Primelementen p_i. Zeige: $(a) = (p_1^{\alpha_1}) \cap \ldots \cap (p_r^{\alpha_r})$, und dies ist eine Primärzerlegung.

5) Sei A ein Hauptidealring mit genau einem maximalen Ideal $(p) \neq (0)$. Zeige: In $A[X]$ gibt es maximale Ideale sowohl der Höhe 1 als auch der Höhe 2.

6) Sei k ein Körper, $\mathfrak{m} = (X,Y,Z)$ in $k[X,Y,Z]$. Ferner sei A der lokale Ring $k[X,Y,Z]_{(X,Y,Z)}$. In dem lokalen Ring $B = A/((AX+AY) \cap AZ)$ gibt es minimale Primideale $\mathfrak{p}$ und $\mathfrak{q}$ mit $\dim(B/\mathfrak{p}) = 1$ und $\dim(B/\mathfrak{q}) = 2$.

7) Es gibt Ringe, in denen folgendes Phänomen auftritt: Zwischen zwei Primidealen $\mathfrak{p} \subset \mathfrak{q}$ gibt es verschieden lange, nicht verfeinerbare Primidealketten. Siehe [Nagata] A1 Example 2. Dieses Beispiel benötigt Begriffe des folgenden Paragraphen. Vergleiche deshalb 7.A5.

8) Für nichtnoethersche Ringe gilt Lemma 6.27 nicht mehr. Die Lemmata 6.23 und 6.25 geben für die Dimension des Polynomringes die Grenzen $\dim A+1 \leq \dim A[X] \leq 2 \dim A + 1$. Tatsächlich kann jeder danach mögliche Wert angenommen werden. Vgl. [Jaffard] .

§ 7 GANZE RINGERWEITERUNGEN

1. Grundlagen

Definition 7.1 $A \subset B$ sei eine Ringerweiterung.

a) B heißt endlich über A, wenn B als A-Modul endlich ist.

b) B heißt von endlichem Typ über A, wenn B als A-Algebra (9.27) endlich erzeugt ist (d.h. $B \simeq A[X_1,\dots,X_n]/\mathfrak{a}$ mit einem Ideal $\mathfrak{a} \subset A[X_1,\dots,X_n]$).

c) i) $b \in B$ heißt ganz über A, wenn (der von $A \cup \{b\}$ erzeugte Ring) $A[b]$ endlich über A ist,

ii) B heißt ganz über A, wenn alle $b \in B$ ganz über A sind.

(Man sagt auch, die Erweiterung $A \subset B$ ist endlich, von endlichem Typ, bzw. ganz, wenn a), b), bzw. c) ii) erfüllt sind.)

Satz 7.2 *Sei* $A \subset B$ *eine Ringerweiterung,* $b \in B$.
Folgende Aussagen sind äquivalent:

(*i*) b *ist ganz über* A.

(*ii*) *Es gibt ein* $n \in \mathbb{N}$ *und* $a_1,\dots,a_n \in A$ *mit*
(*) $b^n + a_1b^{n-1} + \dots + a_n = 0$
(*die Gleichung* (*) *heißt auch Ganzheitsgleichung für* b).

(*iii*) *Es gibt einen Zwischenring* $A \subset B_1 \subset B$, *so daß* $b \in B_1$ *und* B_1 *endlich über* A *ist.*

(*iv*) *Es gibt einen* $A[b]$*-Modul* M *mit* $\operatorname{Ann}_{A[b]}M = (0)$, *der als A-Modul endlich ist.*

(N.B.: In (ii) ist wesentlich, daß der Koeffizient von b^n gleich 1 ist.)

Beweis: (i) $\Rightarrow$ (iii): Der Ring $A[b]$ hat die gewünschten Eigenschaften.
(iii) $\Rightarrow$ (iv): $M := B_1$ leistet das Verlangte: Wenn $aB_1 = 0$, folgt $a = 0$, da $1 \in B_1$, also $\operatorname{Ann}_{A[b]}B_1 = (0)$.
(iv) $\Rightarrow$ (ii): Sei $m_1,\dots,m_n$ ein Erzeugendensystem von M über A, da $bM \subset M$, gibt es $a_{ij} \in A$ mit $bm_i = \sum_{j=1}^n a_{ij}m_j$, d.h. $\sum_{j=1}^n (a_{ij}-b\delta_{ij})m_j = 0$ für $1 \le i \le n$.
Sei σ die Matrix $(a_{ij}-b\delta_{ij})_{i,j}$ mit Komponenten in $A[b]$, $\sigma^\#$ die Adjungierte zu σ. Dann gilt
$0 = \sigma^\#\sigma \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \det(\sigma) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$. Da $\det(\sigma)$ also aus $\operatorname{Ann}_{A[b]}M$, folgt

$\det(\sigma) = 0$. Entwickeln von $\det(\sigma)$ liefert eine Gleichung von der Form
(*): $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ mit $a_i \in A$.
(ii) $\Rightarrow$ (i): $1, b, \ldots, b^{n-1}$ ist ein Erzeugendensystem von $A[b]$ über A:
Ist $c \in A[b]$ beliebig, $c = \sum_{j=0}^{\infty} \tilde{a}_j b^j$ ($\tilde{a}_j \in A$ fast alle Null), so betrachte das Polynom $h(X) = \sum_{j=0}^{\infty} \tilde{a}_j X^j$. Es ist $h(X) = g(X)f(X) + r(X)$ mit $\operatorname{grad} r < \operatorname{grad} f$, wobei $f(X) = \sum_{i=0}^{n} a_i X^{n-i}$, $a_0 = 1$ gesetzt wurde.
Es folgt $c = h(b) = r(b) \in A\cdot 1 + A\cdot b + \ldots + Ab^{n-1}$, da $f(b) = (0)$ nach (*) gilt.–

7.3 Wenn $A \subset B$ eine Körpererweiterung ist, bedeutet "ganz" dasselbe wie "algebraisch".

Folgerung 7.4 *a)* $A \subset B$ *sei eine endliche Ringerweiterung. Dann ist* B *ganz über* A.
b) $A \subset B \subset C$, $c \in C$ *ganz über* $A \Rightarrow c$ *ganz über* B.

Beweis: a) 7.2 (iii) $\Rightarrow$ (i) wähle $B_1 = B$.
b) 7.2 (i) $\Leftrightarrow$ (ii). –

Beispiel 7.5 $\mathbb{Z} \subset \mathbb{Z} + i\mathbb{Z}$ ist ganz.

Feststellung 7.6 *Seien* $A \subset B$ *und* $B \subset C$ *endliche Ringerweiterungen. Dann ist* C *endlich über* A.

Beweis: Seien $b_1, \ldots, b_r$ ein Erzeugendensystem des A-Moduls B und $c_1, \ldots, c_s$ ein Erzeugendensystem des B-Moduls C, schließlich $c \in C$ beliebig. Es gibt $\beta_1, \ldots, \beta_s \in B$ mit $c = \sum_{j=1}^{s} \beta_j c_j$. Dann gibt es $\alpha_{ij} \in A$ mit $\beta_j = \sum_{i=1}^{r} \alpha_{ij} b_i$ für $1 \le j \le s$. Mithin ist $c = \sum_{j=1}^{s} \sum_{i=1}^{r} \alpha_{ij} b_i c_j$. Die $(b_i c_j)$ $(1 \le i \le r,\ 1 \le j \le s)$ erzeugen C als A-Modul. (Vgl. den Beweis des Gradsatzes für Körpererweiterungen.) –

Folgerung 7.7 *Sei* $A \subset B$ *eine Ringerweiterung. Die Elemente von* B, *die ganz sind über* A, *bilden einen Unterring* $\bar{A}$ *von* B *mit* $\bar{A} \supset A$.

Beweis: Zu zeigen ist: Wenn $x, y \in B$ ganz über A sind, so sind dies auch $x \pm y$ und xy. Nach 7.4 und 7.6 ist $A[x,y] = (A[x])[y]$ endlich über A. Da $x \pm y$, $xy \in A[x,y]$, sind $x \pm y$ und $x \cdot y$ ganz über A nach 7.2 (iii) $\Rightarrow$ (i). –

Definition 7.8 a) $A \subset B$ sei eine Ringerweiterung.
$\overline{A} := \{b \in B \mid b$ ganz über $A\}$ heißt der ganze Abschluß von A in B.

b) Ist A integer, $B = Q(A)$, so heißt der ganze Abschluß von A in $Q(A)$ einfach der ganze Abschluß von A.
c) Ist A integer, so heißt A ganz abgeschlossen, wenn A mit seinem ganzen Abschluß übereinstimmt.

Satz 7.9 *Jeder faktorielle Ring A ist ganz abgeschlossen.*

Beweis: Sei $x \in Q(A)$ ganz über A. Es gilt also eine Gleichung $x^n + a_1x^{n-1} + \ldots + a_n = 0$ mit $a_i \in A$. Sei $x = \frac{b}{c}$ mit $b,c \in A$, b und c teilerfremd. Es folgt $b^n = -a_1cb^{n-1} - a_2c^2b^{n-2} - \ldots - a_nc^n$. Sei p ein Primteiler von $c \Rightarrow p|b^n \Rightarrow p|b$. Widerspruch!
Also ist $c \in A^*$, d.h. $x \in A$. —

Satz 7.10 *Seien $A \subset B \subset C$ Ringerweiterungen. Dann sind äquivalent:*

(i) $A \subset B$ und $B \subset C$ sind ganze Ringerweiterungen.
(ii) C ist ganz über A.

Beweis: (ii) $\Rightarrow$ (i): Siehe 7.4 b).
(i) $\Rightarrow$ (ii) Für jedes $x \in C$ gibt es eine Gleichung der Art $x^n + b_1x^{n-1} + \ldots + b_n = 0$ mit $b_i \in B$. Indem man 7.6 mehrfach anwendet, erkennt man, daß $A[b_1,\ldots,b_n,x]$ endlich über A ist. Also ist x ganz über A nach 7.2 (i) $\Longleftrightarrow$ (iii). —

Folgerung 7.11 *Sei $A \subset B$ eine Ringerweiterung und C der ganze Abschluß von A in B. Dann ist C ganz abgeschlossen in B.* —

Beispiele 7.12

a) $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[X_1,\ldots,X_n]$, $k[X_1,\ldots,X_n]$ sind faktoriell, also ganz abgeschlossen. (Natürlich soll k einen Körper bezeichnen.)
b) $\mathbb{Z}[i]$ ist der ganze Abschluß von $\mathbb{Z}$ in $\mathbb{Q}(i)$. Denn $\mathbb{Z}[i]$ ist ganz über $\mathbb{Z}$ (7.4a), 7.5); andererseits ist $\mathbb{Z}[i]$ ganz abgeschlossen in $Q(\mathbb{Z}[i]) = \mathbb{Q}(i)$.
c) $\mathbb{Z}[i]$ ist auch der ganze Abschluß von $\mathbb{Z} + 2i\mathbb{Z}$ in $\mathbb{Q}(i) = Q(\mathbb{Z}+2i\mathbb{Z})$.

Satz 7.13 *Sei $A \subset B$ eine Ringerweiterung.*
a) Wenn B ganz über A ist, so gilt:

1. *Ist* $\mathfrak{b}$ *ein Ideal von* B *und* $\mathfrak{a} = A \cap \mathfrak{b}$, *so ist* $B/\mathfrak{b}$ *ganz über* $A/\mathfrak{a}$.
2. *Ist* $S \subset A$ *multiplikativ, so ist* $S^{-1}B$ *ganz über* $S^{-1}A$.

b) *Ist* A *ganz abgeschlossen in* B, *so auch* $S^{-1}A$ *in* $S^{-1}B$.

Beweis: a)1.: Man hat einen injektiven Homomorphismus $A/\mathfrak{a} \longrightarrow B/\mathfrak{b}$, da $\mathfrak{b} \cap A = \operatorname{Ker}[A \longrightarrow B/\mathfrak{b}]$. Eine Ganzheitsgleichung von $b \in B$ über A wird zu einer Ganzheitsgleichung der Restklasse $\bar{b}$ über $A/\mathfrak{a}$.

a)2.: Sei $b \in B$, $s \in S$. Wir haben für b eine Ganzheitsgleichung $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ über A . Hieraus bekommen wir (durch Multiplikation mit s^{-n}) die Ganzheitsgleichung $(\frac{b}{s})^n + \frac{a_1}{s}(\frac{b}{s})^{n-1} + \ldots + \frac{a_n}{s^n} = 0$ von $\frac{b}{s}$ über $S^{-1}A$. (Beachte $S^{-1}A \subset S^{-1}B$ nach 3.39.)

b) Seien $b \in B$, $s \in S$ und $\frac{b}{s}$ ganz über $S^{-1}A$. Zu zeigen ist: $\frac{b}{s} \in S^{-1}A$. Aus einer Ganzheitsgleichung $(\frac{b}{s})^n + \alpha_1(\frac{b}{s})^{n-1} + \ldots + \alpha_n = 0$ mit $\alpha_i \in S^{-1}A$ erhält man $b^n + \alpha_1 s b^{n-1} + \ldots + \alpha_n s^n = 0$. Dabei ist $\alpha_i s^i = \frac{a_i'}{t_i}$ mit gewissen $a_i' \in A$, $t_i \in S$ (für $1 \le i \le n$) . Setze $t := t_1 \cdot \ldots \cdot t_n$. Man bekommt in $S^{-1}B$ eine Gleichung $\frac{tb^n + a_1'' b^{n-1} + \ldots + a_n''}{t} = 0$ mit $a_i'' \in A$. Hieraus folgt: Es gibt $s_0 \in S$ mit $s_0(tb^n + a_1'' b^{n-1} + \ldots + a_n'') = 0$ in B . Durch Multiplikation mit $(s_0 t)^{n-1}$ erhält man $(s_0 tb)^n + s_0 a_1''(s_0 tb)^{n-1} + \ldots + s_0^n t^{n-1} a_n'' = 0$. Also ist $s_0 tb$ ganz über A, d.h. $s_0 tb \in A$ und somit $\frac{b}{s} = \frac{bs_0 t}{ss_0 t} \in S^{-1}A$. —

Folgerung 7.14 *A sei integer, ganz abgeschlossen, $S \subset A - \{0\}$ multiplikativ. Dann ist $S^{-1}A$ ganz abgeschlossen.* —

Folgerung 7.15 *Ein Integritätsring A ist ganz abgeschlossen genau dann, wenn $A_{\mathfrak{m}}$ ganz abgeschlossen ist für jedes maximale Ideal $\mathfrak{m}$.*

Beweis: "$\Rightarrow$" 7.14.
"$\Leftarrow$": Nach 3.47 ist $A = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$. Wenn $x \in Q(A)$ ganz über A ist, ist x auch ganz über $A_{\mathfrak{m}}$, also nach Voraussetzung $x \in A_{\mathfrak{m}}$ - und dies für alle $\mathfrak{m}$. Es folgt $x \in A$. —

Satz 7.16 *Seien A ein ganz abgeschlossener Integritätsring, $K = Q(A)$, $K \subset L$ eine Körpererweiterung und $\alpha \in L$. Dann sind äquivalent:*

(*i*) α *ist ganz über* A.

(*ii*) α *ist algebraisch über* K *und* $\mathrm{Mipo}(\alpha,K) \in A[X]$.

(Mipo = Minimalpolynom. Dieses ist nach Definition normiert.)

Beweis: (ii) $\Rightarrow$ (i): trivial (mit 7.2).
(i) $\Rightarrow$ (ii): Natürlich ist α algebraisch über K. Seien $\alpha_1,\ldots,\alpha_n$ die Konjugierten von α, d.h. alle Nullstellen von $\mathrm{Mipo}(\alpha,K)$ in einem algebraischen Abschluß $\overline{K}$ von K. Man hat K-Isomorphismen $K[\alpha] \longrightarrow K[\alpha_i]$ mit $\alpha \longmapsto \alpha_i$. Also hat man Isomorphismen $A[\alpha] \longrightarrow A[\alpha_i]$, die auf A die Identität sind. Es folgt, daß mit α auch sämtliche α_i ganz über A sind. Die Koeffizienten von $\mathrm{Mipo}(\alpha,K)$ sind als elementarsymmetrische Funktionen in den α_i nach 7.7 ebenfalls ganz über A, andererseits in K, also in A, da A ganz abgeschlossen. –

7.17 Zusatz: *Wenn zusätzlich* L *endlich über* K *ist, sind* (*i*), (*ii*) *äquivalent zu*

(*iii*) $\chi_{L/K}(\alpha) \in A[X]$.

($\chi_{L/K}(\alpha)$ = charakteristisches Polynom der K-linearen Abbildung $L \longrightarrow L$, $1 \longmapsto \alpha 1$.)

Zum Beweis beachte man nur, daß die Nullstellen von $\chi_{L/K}(\alpha)$ auch Nullstellen von $\mathrm{Mipo}(\alpha,K)$ sind. –

2. Ganzheit und Dimension

Lemma 7.18 *Ist* $A \subset B$ *eine ganze Ringerweiterung und* B *integer, so gilt:* A *ist genau dann ein Körper, wenn* B *einer ist.*

Beweis: "$\Rightarrow$": Sei $b \in B - \{0\}$. Dann ist $b \in Q(B)$ algebraisch über dem Körper A und deshalb $A[b]$ ein Körper. Es folgt $b^{-1} \in A[b] \subset B$. Somit ist jedes Element $b \in B - \{0\}$ in B invertierbar.
"$\Leftarrow$": Sei $a \in A - \{0\}$. Da B ein Körper ist, gilt $a^{-1} \in B$. Wir haben nach Voraussetzung eine Ganzheitsgleichung $(a^{-1})^n + a_1(a^{-1})^{n-1}+\ldots+a_n = 0$ mit $a_i \in A$, also $a^{-1} = -a_1 - a_2a - \ldots - a_na^{n-1} \in A$. –

Definition 7.19 Sei $A \subset B$ eine Ringerweiterung. Man sagt, ein Primideal $\mathfrak{p} \subset B$ liege über dem Primideal $\mathfrak{p}' \subset A$, wenn $\mathfrak{p}' = \mathfrak{p} \cap A$ gilt.

Satz 7.20 *Es sei $A \subset B$ eine ganze Ringerweiterung. Dann gilt:*

a) *"lying over": Zu jedem Primideal $\mathfrak{p}' \subset A$ gibt es ein Primideal $\mathfrak{p} \subset B$ welches über $\mathfrak{p}'$ liegt.*

b) *Sind $\mathfrak{p} \subset \mathfrak{q}$ Primideale in B, die über demselben Primideal $\mathfrak{p}'$ in A liegen, so gilt $\mathfrak{p} = \mathfrak{q}$.*

c) *Das Primideal $\mathfrak{p}$ von B liege über dem Primideal $\mathfrak{p}'$ von A. Dann gilt: $\mathfrak{p}$ ist ein maximales Ideal genau dann, wenn $\mathfrak{p}'$ ein solches ist.*

Beweis: Zu c): Die Erweiterung $A/\mathfrak{p}' \hookrightarrow B/\mathfrak{p}$ ist nach 7.13 a)1., wegen $\mathfrak{p}' = \mathfrak{p} \cap A$, ganz. c) folgt aus 7.18.
Zu b): Sei $S = A - \mathfrak{p}' \subset B - \mathfrak{q}$. Betrachte die Injektion $S^{-1}A \hookrightarrow S^{-1}B$. Die Primideale $S^{-1}\mathfrak{p}$ und $S^{-1}\mathfrak{q}$ liegen über dem maximalen Ideal $S^{-1}\mathfrak{p}'$ von $S^{-1}A = A_{\mathfrak{p}'}$. (Denn $S^{-1}\mathfrak{q} \supset S^{-1}\mathfrak{p} \supset S^{-1}\mathfrak{p}'$, aber $1 \notin S^{-1}\mathfrak{q}$.) Nach c) ist $S^{-1}\mathfrak{p}$ maximal, also $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}$. Wende nun Satz 2.13 an.

Zu a): Man hat folgendes kommutative Diagramm:

$$\begin{array}{ccc} B & \xrightarrow{i_{B,S}} & B_{\mathfrak{p}'} \\ \uparrow & & \uparrow \\ \mathfrak{p}' \subset A & \xrightarrow[i_{A,S}]{} & A_{\mathfrak{p}'} \end{array} \qquad (S := A - \mathfrak{p}')$$

mit ganzen Erweiterungen $A \subset B$, $A_{\mathfrak{p}'} \subset B_{\mathfrak{p}'}$ (vgl. 7.13). Sei $\mathfrak{m}$ ein maximales Ideal von $B_{\mathfrak{p}'}$. Dann ist $\mathfrak{m}' = \mathfrak{m} \cap A_{\mathfrak{p}'}$ ein maximales Ideal in $A_{\mathfrak{p}'}$ nach c), also das einzige maximale Ideal des lokalen Ringes $A_{\mathfrak{p}'}$. Das Ideal $\mathfrak{p} := i_{B,S}^{-1}(\mathfrak{m})$ ist prim (1.24), und $\mathfrak{p} \cap A = i_{A,S}^{-1}(\mathfrak{m}') = \mathfrak{p}'$. –

In den Folgerungen sei $A \subset B$ eine ganze Ringerweiterung.

Folgerung 7.21 *Sei $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \dots \subsetneqq \mathfrak{p}_r$ eine Primidealkette in B. $\mathfrak{p}_i' := \mathfrak{p}_i \cap A$. Dann ist $\mathfrak{p}_0' \subsetneqq \mathfrak{p}_1' \subsetneqq \dots \subsetneqq \mathfrak{p}_r'$ eine Primidealkette in A.*

Beweis: 7.20 b). –

Folgerung 7.22 ("*going up*") *Ist $\mathfrak{p}_0' \subsetneqq \mathfrak{p}_1' \subsetneqq \dots \subsetneqq \mathfrak{p}_r'$ eine Primidealkette in A, und das Primideal $\mathfrak{p}_0$ von B liege über $\mathfrak{p}_0'$. Dann gibt es in B eine Primidealkette $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \dots \subsetneqq \mathfrak{p}_r$ mit $\mathfrak{p}_i \cap A = \mathfrak{p}_i'$ für alle i.*

Beweis: Induktion nach r, wobei der Fall $r = 0$ trivial ist. Sei $r > 0$ und $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_{r-1}$ bereits konstruiert. Die Ringerweiterung $A/\mathfrak{p}'_{r-1} \longrightarrow B/\mathfrak{p}_{r-1}$ ist nach 7.13 ganz. Über dem Primideal $\mathfrak{p}'_r/\mathfrak{p}'_{r-1}$ von $A/\mathfrak{p}'_{r-1}$ liegt nach 7.20a) also ein Primideal $\mathfrak{p}_r/\mathfrak{p}_{r-1}$ von $B/\mathfrak{p}_{r-1}$. Dabei ist $\mathfrak{p}_r$ ein Primideal von B mit $\mathfrak{p}_r \supset \mathfrak{p}_{r-1}$. Um $\mathfrak{p}_r \cap A = \mathfrak{p}'_r$ zu erkennen, betrachte das kommutative Diagramm mit offensichtlichen Homomorphismen:

$$\begin{tikzcd} A \arrow[r, hook, "i"] \arrow[d, "\varphi_A"'] & B \arrow[d, "\varphi_B"] \\ A/\mathfrak{p}'_{r-1} \arrow[r, hook, "j"] & B/\mathfrak{p}_{r-1} \end{tikzcd}$$

Es ist $\mathfrak{p}_r \cap A = i^{-1}(\mathfrak{p}_r) = i^{-1}(\varphi_B^{-1}(\mathfrak{p}_r/\mathfrak{p}_{r-1})) = \varphi_A^{-1}(j^{-1}(\mathfrak{p}_r/\mathfrak{p}_{r-1})) =$

$\varphi_A^{-1}(\mathfrak{p}'_r/\mathfrak{p}'_{r-1}) = \mathfrak{p}'_r$. —

Folgerung 7.23 *a) Es ist* $\dim A = \dim B$.

b) Sei $\mathfrak{p}'$ *ein Primideal in* A . *Es gilt:*

1. *Für jedes Primideal* $\mathfrak{p}$ *von* B *über* $\mathfrak{p}'$ *ist* $\dim A/\mathfrak{p}' = \dim B/\mathfrak{p}$ *und* $\operatorname{ht} \mathfrak{p} \le \operatorname{ht} \mathfrak{p}'$.
2. *Wenn* $\operatorname{ht} \mathfrak{p}' < \infty$ *ist, gibt es ein Primideal* $\mathfrak{p}$ *von* B *über* $\mathfrak{p}'$ *mit* $\operatorname{ht} \mathfrak{p} = \operatorname{ht} \mathfrak{p}'$.

Beweis: a) Aus 7.21 folgt $\dim A \ge \dim B$. Aus 7.22 folgt $\dim A \le \dim B$.

b) Da $\mathfrak{p} = A \cap \mathfrak{p}'$ ist, folgt $\dim A/\mathfrak{p}' = \dim B/\mathfrak{p}$ mit 7.13 aus a). Die Ungleichung $\operatorname{ht} \mathfrak{p} \le \operatorname{ht} \mathfrak{p}'$ folgt aus 7.21.

Zu 2. Sei $\operatorname{ht} \mathfrak{p}' = r$ und $\mathfrak{p}'_0 \subsetneqq \mathfrak{p}'_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}'_r$ mit $\mathfrak{p}'_r = \mathfrak{p}'$ eine Primidealkette in A . Nach 7.22 existieren $\mathfrak{p}_i$ über $\mathfrak{p}'_i$, so daß $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r$, also $\operatorname{ht} \mathfrak{p}_r \ge r$ gilt. Da nach 1. aber auch $\operatorname{ht} \mathfrak{p}_r \le r$ gilt, ist $\mathfrak{p} = \mathfrak{p}_r$ das gesuchte Primideal. —

Bemerkung 7.24 Die Gleichheit $\operatorname{ht} \mathfrak{p} = \operatorname{ht} \mathfrak{p}'$ gilt i.a. nicht für jedes Primideal $\mathfrak{p}$ über $\mathfrak{p}'$. Siehe A5, aber auch A6.

3. Zur Endlichkeit des ganzen Abschlusses

Wir betrachten die folgende Situation: Sei A ein Integritätsring, $K = Q(A)$ und $K \subset L$ eine endliche Körpererweiterung. Der ganze Abschluß B von A in L braucht i.a. nicht endlich über A zu sein. Wir werden hier, in §9 und auch in §18 wichtige Spezialfälle angeben, in denen B endlich über A ist.

Feststellung 7.25 *In obiger Situation ist* $L = \left\{\frac{b}{a} \mid b \in B,\ a \in A - \{0\}\right\}$. *Es gibt eine Basis von* L *über* K, *bestehend aus Elementen von* B.

Beweis: Sei $x \in L$. Da x algebraisch über K ist, gilt eine Gleichung $x^n + c_1 x^{n-1} + \ldots + c_n = 0$ mit gewissen $c_i \in K$. Dabei ist $c_i = \frac{a_i}{a}$ mit geeigneten $a, a_i \in A$, $a \neq 0$. Somit ist $(ax)^n + a_1(ax)^{n-1} + aa_2(ax)^{n-2} + \ldots + a^{n-1}a_0 = 0$, d.h. ax ist ganz über A. Nach Voraussetzung ist also $ax \in B$, d.h. $x = \frac{b}{a}$ mit einem $b \in B$. Der Rest ist dann klar. –

Mit $S_{L/K} : L \longrightarrow K$ bezeichnen wir die Spur. Diese ist K-linear. Aus der Theorie der endlichen Körpererweiterungen zitieren wir den Satz:

Wenn L *über* K *separabel ist, ist* $S_{L/K} \neq 0$.

Siehe [Lorenz] §13.3 F6, S. 158, oder [Lang] VIII §5 Theorem 9, S. 211. –

N.B.: Im Falle $\operatorname{char} K=0$ ist dieses trivial, da $S_{L/K}(1) = [L:K]$ ist.

Satz 7.26 *In obiger Situation sei* A *noethersch und ganz abgeschlossen und* L *separabel über* K. *Dann ist* B *endlich über* A, *insbesondere auch noethersch.*

Beweis: Wir schreiben $S := S_{L/K}$. Es gilt $S(B) \subset A$, denn für $b \in B$ ist $S(b)$ offenbar ganz über A und in K gelegen. Ferner ist $S \neq 0$ nach dem zitierten Satz.

Wenn M ein A-Untermodul von L ist, sei $\widetilde{M} := \{x \in L \mid S(xM) \subset A\}$. Dann ist $\widetilde{M}$ auch ein A-Untermodul von L; denn S ist A-linear. Ferner folgt aus $M_1 \subset M_2$, daß $\widetilde{M}_1 \supset \widetilde{M}_2$ gilt. Da $S(B) \subset A$ und $BB \subset B$, ist $B \subset \widetilde{B}$.

Sei nun $b_1,\dots,b_n$ eine Basis von L über K mit $b_i \in B$ und $M := Ab_1 + \dots + Ab_n$. Dann ist $M \subset B$, also $\widetilde{B} \subset \widetilde{M}$. Betrachte die Abbildung $\varphi\colon \widetilde{M} \longrightarrow A^n$, $x \longmapsto (S(xb_1),\dots\dots,S(xb_n))$. (Nach Definition von $\widetilde{M}$ ist $S(xb_i) \in A$ für $x \in \widetilde{M}$.) Die Abbildung φ ist A-linear. Sie ist aber auch injektiv. Denn $\varphi(x) = 0$ bedeutet $S(xb_i) = 0$ für jedes i, und deshalb $S(xy) = 0$ für jedes $y \in L$, da S linear über K und $b_1,\dots,b_n$ eine K-Basis von L ist. Da $S \neq 0$ ist, folgt $x = 0$.

Insgesamt haben wir $B \subset \widetilde{B} \subset \widetilde{M}$ und $\widetilde{M}$ isomorph zu einem Untermodul des endlichen A-Moduls A^n. Da A noethersch ist, ist B ein endlicher A-Modul. —

Aufgaben und Hinweise

1) Satz 7.2 läßt sich im Falle, daß A noethersch ist, einfacher beweisen. (i)$\Leftrightarrow$(ii) ist einfach, (i) $\Rightarrow$ (iii) $\Rightarrow$ (iv) ist trivial. Es gelte (iv) und M sei über $A[b]$ von r Elementen erzeugt. Man erhält eine Injektion $A[b] \hookrightarrow M^r$. Da M^r ein endlicher A-Modul und A noethersch ist, ist $A[b]$ ein endlicher A-Modul, also gilt (i).

   Wenn man die nicht so wichtige Aussage (iv) ausläßt, wird es noch einfacher, da der Schluß von (iii) auf (i) bei noetherschem A unmittelbar klar ist. Beachte, daß man für den Beweis von 7.4 und 7.7 auf die Äquivalenz (i) $\Leftrightarrow$ (iii) nicht ohne weiteres verzichten kann.

2) Sei $d \in \mathbb{Z} - \{1\}$ quadratfrei, d.h. d sei nicht durch das Quadrat einer Primzahl teilbar. Dann ist $\sqrt{d} \notin \mathbb{Z}$, also nach 7.9 auch $\sqrt{d} \notin \mathbb{Q}$. Zeige: Der ganze Abschluß von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ ist:

   $\mathbb{Z} + \mathbb{Z}\sqrt{d}$, falls $d \equiv 2$ oder $d \equiv 3 \bmod 4$,

   $\mathbb{Z} + \mathbb{Z}\cdot \frac{1}{2}(1+\sqrt{d})$, falls $d \equiv 1 \bmod 4$ ist.

3) (Verallgemeinerung von 2)): Sei A ein faktorieller Ring, $\operatorname{char} Q(A) \neq 2$, ferner $d \in A$ quadratfrei und auch nicht das Quadrat einer Einheit. B sei der ganze Abschluß von A in $Q(A)(\sqrt{d})$. Zeige:

   a) $B = \{\frac{1}{2}(a + b\sqrt{d}) \mid a,b \in A,\ a^2 \equiv b^2 d \bmod 4A\}$.

b) $B = A + A\sqrt{d}$, falls $2|d$ (insbesondere, wenn $2 \in A^*$).

c) Wenn es ein $\delta \in A$ mit $d \equiv \delta^2 \bmod 4A$ gibt, ist $\frac{1}{2}(\delta + \sqrt{d}) \in B$, also $B \supsetneqq A + A\sqrt{d}$ - vorausgesetzt, $2 \notin A^*$.

d) Zusätzlich zu der Voraussetzung von c) sei 2 quadratfrei in A. Dann ist $B = A + A \cdot \frac{1}{2}(\delta + \sqrt{d})$.

e) Wenn $A/2A$ ein Körper und d in A kein Quadrat modulo $4A$ ist, gilt $B = A + A\sqrt{d}$.

4) Keineswegs trivial ist folgender Satz: Sei $w \in \mathbb{C}$ eine Einheitswurzel, dann ist $\mathbb{Z}[w]$ der ganze Abschluß von $\mathbb{Z}$ in $\mathbb{Q}(w)$. Siehe in den Büchern über Algebraische Zahlentheorie, etwa [Marcus], Cor. 2 of Thm. 12. In letzterem Buch finden sich weitere Bestimmungen ganzer Abschlüsse von $\mathbb{Z}$ in Körpern, die über $\mathbb{Q}$ endlich sind.

5) Ein Beispiel zu 7.24 findet sich in [Nagata] A1., Example 2, das schon in 6.A7 genannt wurde. Hinweise: "local" = "lokal und noethersch", "derived normal ring" = "ganzer Abschluß", "$\subset$" = "$\subsetneqq$"; das "theorem of Cohen" ist die Aussage in 3.A10.

$K[[x]]$ ist der formale Potenzreihenring (vgl. 3.A9). Wenn K etwa abzählbar ist, ist der algebraische Abschluß von K in $Q(K[[x]])$ ebenfalls abzählbar. Andererseits ist $K[[x]]$ überabzählbar, also der Transzendenzgrad von $Q(K[[x]])$ über K unendlich. Man findet deshalb in $K[[x]]$ unendlich viele über K algebraisch unabhängige Elemente.

6) "Going down" oder Krullsches Abstiegslemma. Sei $A \subset B$ eine ganze Erweiterung von Integritätsringen und A ganz abgeschlossen. Zu einer Primidealkette $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_n$ in A und zu einem Primideal $\mathfrak{p}_n$ von B über $\mathfrak{p}'_n$ gibt es eine Primidealkette $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ in B mit $\mathfrak{p}_i \cap A = \mathfrak{p}'_i$. Siehe [Serre] III.3 oder [Lorenz] Anh. 19.6. Insbesondere ist in dieser Situation $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}')$ für jedes $\mathfrak{p}$ über $\mathfrak{p}'$.

7) Wenn ein Integritätsring A ganz abgeschlossen ist, so gilt dies auch für den Polynomring $A[X]$ und umgekehrt. Siehe [Bourbaki] chap. V, § 1.3.

8) Sei $A \subset B$ eine Erweiterung von Integritätsringen derart, daß $Q(B)$ algebraisch über $Q(A)$ ist.
   a) Zeige: Zu $b \in B$ gibt es $b' \in B - \{0\}$ mit $bb' \in A$.
      (Zeige $Bb \cap A \neq (0)$ wie im Beweis von 4.54.)
   b) Folgere: $Q(B) = \{\frac{b}{a} \mid b \in B,\ a \in A - \{0\}\}$.

   Man sieht, daß von 7.25 nach dieser Aufgabe nur die Aussage $L = Q(B)$ "übrigbleibt". Und diese braucht man streng genommen nicht, um 7.26 zu zeigen, da ja $Q(B)$ auch endlich und separabel über K wäre.

9) Zu einem Beispiel, wo B bei einer inseparablen Erweiterung $K \subset L$ nicht endlich über A ist, siehe [Schmidt] oder 8. A5.

§8 DISKRETE BEWERTUNGSRINGE, DEDEKINDRINGE

Definition 8.1 Es sei K ein Körper.
Eine diskrete Bewertung von K ist eine Abbildung $v: K \longrightarrow \mathbb{Z} \cup \{\infty\}$, die folgenden Bedingungen genügt:
(a) $v(x) = \infty \iff x = 0$.
(b) $v(xy) = v(x)+v(y)$ (d.h. $v|K^*: K^* \longrightarrow \mathbb{Z}$ ist ein Gruppenhomomorphismus).
(c) $v(x+y) \geq \min\{v(x),v(y)\}$.
(Konvention: $n + \infty = \infty$, $n \leq \infty$ für alle $n \in \mathbb{Z} \cup \{\infty\}$.)

Die Bewertung heißt trivial, wenn $v(K) = \{0,\infty\}$, sie heißt normiert, wenn $v(K) = \mathbb{Z} \cup \{\infty\}$ ist, d.h. ein $x \in K$ mit $v(x) = 1$ existiert.

Bemerkungen 8.2
a) Es gibt einen allgemeineren Bewertungsbegriff, wo $\mathbb{Z}$ durch eine beliebige geordnete kommutative Gruppe (z.B. $(\mathbb{R},+)$) ersetzt werden darf. Vgl. [Bourbaki] chap. VI.

b) Ist k ein Unterkörper von K, so ist $v|_k$ eine diskrete Bewertung von k. Sie kann natürlich trivial (bzw. nicht normiert) sein, auch wenn v selbst nichttrivial (bzw. normiert) ist.

c) $v(K^*)$ ist eine Untergruppe von $\mathbb{Z}$, also $v(K^*) = m\mathbb{Z}$ mit einem $m \in \mathbb{Z}$. Die Bewertung v ist genau dann trivial, wenn $m = 0$ gilt. Wenn v nicht trivial ist, kann man durch $v'(x) := \frac{1}{m}v(x)$ $(x \in K^*)$, $v'(0) := \infty$ eine normierte diskrete Bewertung auf K definieren. D.h. es bedeutet häufig keine Einschränkung, wenn man von einer diskreten Bewertung voraussetzt, sie sei normiert.

Beispiel 8.3 Es sei p Primelement in einem faktoriellen Ring A. Dann definiert man für $a \in Q(A)-\{0\}$ von der Form $a = p^n \frac{a_1}{a_2}$ mit $p \nmid a_1 a_2$, $n \in \mathbb{Z}$, eine normierte diskrete Bewertung durch $v_p(a) = n$.

Satz 8.4 *Sei* K *ein Körper,* v *eine diskrete Bewertung auf* K.
Dann gilt:

a) $\mathfrak{O}_v := \{x \in K \mid v(x) \geq 0\}$ *ist ein Ring.*

b) $\mathfrak{O}_v^* = \{x \in K \mid v(x) = 0\}$.

c) $\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$ *ist das einzige maximale Ideal von* $\mathfrak{O}_v$.
Also: $\mathfrak{O}_v$ *ist lokal mit maximalem Ideal* $\mathfrak{m}_v$.

d) $\mathfrak{O}_v$ *ist ein Hauptidealring (also insbesondere ganz abgeschlossen), und zwar genau dann kein Körper, wenn* v *nicht trivial ist.*

e) Wenn v *normiert ist, sind die (zueinander assoziierten) Primelemente von* $\mathfrak{O}_v$ *genau die* p *mit* $v(p) = 1$. *(Jedes solche* p *erzeugt dann* $\mathfrak{m}_v$.*)*

Zum Beweis:

a) $x \in \mathfrak{O}_v$, $y \in \mathfrak{O}_v \Rightarrow v(x) \geq 0$, $v(y) \geq 0 \Rightarrow v(xy) = v(x)+v(y) \geq 0$.
$v(x+y) \geq \min(v(x),v(y)) \geq 0$. $v(1) = v(1\cdot 1) = v(1)+v(1) \Rightarrow v(1) = 0 \Rightarrow$ $1 \in \mathfrak{O}_v$. $0 = v(1) = v((-1)(-1)) = v(-1)+v(-1) \Rightarrow v(-1) = 0 \Rightarrow$ $v(-x) = v(x)+v(-1) = v(x) \geq 0$.

b) $x \in K$ in $\mathfrak{O}_v$ invertierbar $\Leftrightarrow v(x) \geq 0 \wedge v(x^{-1}) \geq 0$:
Gilt $v(x) \geq 0$, so wegen $0 = v(1) = v(x)+v(x^{-1})$: $v(x^{-1}) = -v(x) \leq 0$.
Also: $x \in K$ in $\mathfrak{O}_v$ invertierbar $\Leftrightarrow v(x) = 0$.

c) $\mathfrak{m}_v$ ist ein Ideal: $x \in \mathfrak{m}_v$, $y \in \mathfrak{O}_v \Rightarrow v(xy) = v(x)+v(y) > 0$!
$x \in \mathfrak{m}_v$, $y \in \mathfrak{m}_v \Rightarrow v(x) > 0$, $v(y) > 0 \Rightarrow v(x+y) \geq \min\{v(x),v(y)\} > 0$.
$\mathfrak{O}_v - \mathfrak{m}_v = \mathfrak{O}_v^* \Rightarrow \mathfrak{O}_v$ hat genau ein maximales Ideal, nämlich $\mathfrak{m}_v$ nach 2.8.

d) Sei $\mathfrak{a} \subset \mathfrak{O}_v$ ein Ideal $\neq (0)$. Sei $a \in \mathfrak{a}$ so gewählt, daß $v(a)$ minimal unter allen $v(x)$ mit $x \in \mathfrak{a}$ ist. (Dies ist sinnvoll, da $v(x) \in \mathbb{N}$.) Dann gilt $\mathfrak{a} = (a)$: Sei nämlich $b \in \mathfrak{a}$ beliebig. Dann ist $b = a\cdot\frac{b}{a}$ mit $a \in \mathfrak{a}$ und $v(\frac{b}{a}) = v(b)-v(a) \geq 0$, also $\frac{b}{a} \in \mathfrak{O}_v$, somit $b \in (a)$.

e) Nach der Theorie der Hauptidealringe ist $p \in \mathcal{O}_v$ ein Primelement genau dann, wenn p das einzige maximale Ideal $\mathfrak{m}_v$ von $\mathcal{O}_v$ erzeugt. Nach dem Beweis von d) tut dies sicher jedes $p \in K$ mit $v(p) = 1$. Wenn $v(q) = n > 1$ und $v(p) = 1$ ist (v ist normiert!), gilt $v(qp^{-n}) = n-n = 0$, also $qp^{-n} \in \mathcal{O}_v$ und deshalb $p^n | q$. Dann kann q nicht prim sein.

Definition 8.5 Ein lokaler Hauptidealring A, der kein Körper ist, heißt diskreter Bewertungsring (DBR).

Satz 8.6 *Sei* A *ein diskreter Bewertungsring,* p *ein Primelement von* A.

a) Jedes Element $x \in Q(A)^*$ *hat die Gestalt* $x = up^n$ *mit einem* $u \in A^*$, $n \in \mathbb{Z}$. *Dabei ist* n *unabhängig von der Wahl von* p.

b) Die Abbildung $v = v_A\colon Q(A) \longrightarrow \mathbb{Z} \cup \{\infty\}$ *mit* $v(0) = \infty$, $v(x) = n$, *wenn* $x = up^n$ *gemäß a) gewählt, ist eine normierte diskrete Bewertung von* $Q(A)$ *mit* $A = \mathcal{O}_v$.

Beweis: Nach der Theorie der Hauptidealringe weiß man a) zumindest dann, wenn $x \in A - \{0\}$ ist. Für allgemeine $x \in Q(A)^*$ folgt die Aussage sofort.

Zu b): Daß v eine normierte diskrete Bewertung ist, ist ein Spezialfall von 8.3. Da wir dort den Beweis dem Leser überlassen haben, sei hier wenigstens die Eigenschaft 8.1 (c) nachgeprüft: Für $n \geq m$ in $\mathbb{Z}$ und $u,u' \in A^*$ gilt $p^n u + p^m u' = p^m(p^{n-m}u+u') = p^m a$ mit einem $a \in A$. D.h. $v(p^n u+p^m u') = m+v(a) \geq m = \min(n,m)$. Noch zu zeigen ist $A = \mathcal{O}_v$. Nun ist up^n (mit $u \in A^*$ und $n \in \mathbb{Z}$) genau dann ein Element von A, wenn $n \geq 0$ ist. –

Folgerung 8.7 *Sei* K *ein Körper. Die Zuordnung* $v \longmapsto \mathcal{O}_v$ *definiert eine Bijektion*

$$\{\textit{normierte diskrete Bewertungen von } K\}$$
$$\longrightarrow \{A \textit{ Unterring von } K \mid A \textit{ ist ein DBR, } Q(A) = K\}.$$

Die inverse Abbildung wird durch $A \longmapsto v_A$ *gegeben.*

Beweis: a) Es gilt: $v_{(\mathcal{O}_v)} = v$. Sei nämlich $u \in \mathcal{O}_v^*$ und p prim in $\mathcal{O}_v$, so ist $v(up^n) = n \cdot v(p) = n$ nach 8.4 e).

b) $\mathcal{O}_{v_A} = A$ steht in 8.6 b).

Satz 8.8 *(Charakterisierung diskreter Bewertungsringe nach Emmy Noether)*

Sei A *integer, noethersch, lokal mit dem maximalen Ideal* $\mathfrak{m}$.
Es sind äquivalent:

(*i*) A *ist ein diskreter Bewertungsring.*

(*ii*) $\dim A = 1$ *und* A *ist ganz abgeschlossen.*

(*iii*) A *ist ganz abgeschlossen, und es gibt ein* $a \in A - \{0\}$, *so daß* $\mathfrak{m} \in \mathrm{Ass}_A(A/aA)$.

(*iv*) $\mathfrak{m}$ *ist ein Hauptideal* $\neq (0)$;

(*v*) A *ist faktoriell und besitzt im wesentlichen genau ein Primelement.*

Beweis: (i) $\Rightarrow$ (ii): A ist ein Hauptidealring. Also ist $\dim A = 1$ und A ganz abgeschlossen nach 7.9.
(ii) $\Rightarrow$ (iii): Sei $a \in \mathfrak{m} - \{0\}$ beliebig. Wegen $\{\mathfrak{m}\} \overset{4.14}{=\!=} \mathrm{Supp}_A(A/aA)$ (also $\mathfrak{m}$ minimal in $\mathrm{Supp}_A(A/aA)$) ist $\mathfrak{m} \in \mathrm{Ass}_A(A/aA)$ nach 4.15.

(iii) $\Rightarrow$ (iv): Es gibt ein $\overline{b} \in A/aA$, so daß $\mathfrak{m} = \mathrm{Ann}_A(\overline{b})$, $\overline{b} = b+aA$. Da $\mathrm{Ann}_A(\overline{b}) \neq A$, gilt $\overline{b} \neq 0$, d.h. $b \notin aA$. Andererseits ist $\mathfrak{m}b \subset aA$, d.h. $\mathfrak{m}ba^{-1} \subset A$ (mit $a^{-1} \in Q(A)$). Darum ist $\mathfrak{m}ba^{-1}$ ein Ideal in A .

Behauptung: Es gilt sogar $\mathfrak{m}ba^{-1} = A$! Beweis: Sonst wäre $\mathfrak{m}ba^{-1} \subset \mathfrak{m}$, $\mathfrak{m}(ba^{-1})^2 \subset \mathfrak{m}(ba^{-1}) \subset \mathfrak{m}, \ldots$ also $\mathfrak{m}(ba^{-1})^n \subset \mathfrak{m}$ für alle $n \in \mathbb{N}$. Insbesondere gälte $a(ba^{-1})^n \in A$, d.h. $(ba^{-1})^n \in a^{-1}A$ für alle n . Somit ist $A[ba^{-1}] \subset a^{-1}A$ und deshalb ba^{-1} ganz über A . Denn A ist noethersch und $Aa^{-1} \simeq A$ als A-Modul, somit $A[ba^{-1}]$ ein endlicher A-Modul. Daraus folgt $ba^{-1} \in A$, d.h. $b \in aA$. Widerspruch!
Mit $\mathfrak{m}ba^{-1} = A$ ist $\mathfrak{m} = Aab^{-1}$ ein Hauptideal.

(iv) $\Rightarrow$ (v): Sei $\mathfrak{m} = Ap$ und $a \in A - \{0\}$ beliebig.
Behauptung: Es gibt ein $n \in \mathbb{N}$, so daß $p^{n+1} \nmid a$.
Beweis: Sonst gäbe es für jedes $n \in \mathbb{N}$ ein a_n mit $a = p^n a_n$ ($a_0 := a$) , also: $pa_{n+1} = a_n$. Man hätte $Aa_n \subset Aa_{n+1}$ für jedes n . Da A noethersch ist, gälte $Aa_n = Aa_{n+1}$ für ein n . Somit wäre $a_{n+1} = ba_n = bpa_{n+1}$ für ein geeignetes $b \in A$, also $bp = 1$, deshalb p eine Einheit. Widerspruch!
Für $a \in A - \{0\}$ gibt es also ein $n \in \mathbb{N}$ mit $p^n | a$, aber $p^{n+1} \nmid a$. Es gibt also ein $u \in A$ mit $a = p^n u$, $p \nmid u$. Wegen $p \nmid u$ gilt $u \notin \mathfrak{m}$, deshalb $u \in A^*$. Wenn nun auch $a = p^j b$, so gilt wegen $p^{n+1} \nmid a$, daß $j \leq n$. Ist $j < n$, $k = n-j$, so hat man $a = p^{j+k}u = p^j b$, also $p^k u = b$, deswegen $p \mid b$ und $b \notin A^*$. Es folgt also die Eindeutigkeit der Primfaktorzerlegung.

(v) $\Rightarrow$ (i): Sei $\mathfrak{a} \neq (0)$ ein Ideal. Wähle $a \in \mathfrak{a} - \{0\}$ so, daß bei der Darstellung $a = up^n$, $u \in A^*$, n minimal ist. Dann gilt $\mathfrak{a} = Aa$; denn für $b \in \mathfrak{a}$ ist $b = p^m v$ mit einem $v \in A^*$ und einem $m \geq n$, also $b = p^{m-n}vu^{-1}(p^n u) = p^{m-n}vu^{-1}a \in Aa$. Nach Definition ist A ein DBR. —

Definition 8.9 Ein Dedekindring ist ein ganz-abgeschlossener noetherscher Integritätsring der Dimension ≤ 1.

N.B.: Jeder Hauptidealring ist also ein Dedekindring. (7.9.)

Folgerung 8.10: *Ein noetherscher Integritätsring ist genau dann ein Dedekindring, wenn für jedes Primideal* $\mathfrak{p} \neq (0)$ *in* A *der Ring* $A_{\mathfrak{p}}$ *ein diskreter Bewertungsring ist.*

Beweis: 8.8 (i) $\Leftrightarrow$ (ii) und 7.15. —

Satz 8.11 *Es sei* A *ein Dedekindring. Dann gilt:*
a) Jedes Ideal $\mathfrak{a} \neq (0)$ *von* A *läßt sich bis auf die Reihenfolge eindeutig darstellen als Produkt von endlich vielen maximalen Idealen.*

b) Zu jedem Ideal $\mathfrak{a}$ *gibt es ein Ideal* $\mathfrak{b}$*, so daß* $\mathfrak{a}\mathfrak{b}$ *ein Hauptideal ist.*

Beweis: a) Nach 8.10 sind die $A_{\mathfrak{m}}$ für maximale $\mathfrak{m} \subset A$ diskrete Bewertungsringe. Bezeichne die zugehörige normierte Bewertung von $Q(A_{\mathfrak{m}}) = Q(A)$ mit $v_{\mathfrak{m}}$. Für ein Ideal $\mathfrak{a}$ definiere
$v_{\mathfrak{m}}(\mathfrak{a}) := \min\{v_{\mathfrak{m}}(a) \mid a \in \mathfrak{a}\}$.

Behauptung 1): $\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow v_{\mathfrak{m}}(\mathfrak{a}) \geq v_{\mathfrak{m}}(\mathfrak{b})$ für alle maximalen Ideale $\mathfrak{m}$.
Beweis: "$\Rightarrow$" ist klar. "$\Leftarrow$": Sei $a \in \mathfrak{a}$. Für jedes $\mathfrak{m}$ gibt es ein $b_{\mathfrak{m}} \in \mathfrak{b}$ mit $v_{\mathfrak{m}}(a) \geq v_{\mathfrak{m}}(b_{\mathfrak{m}})$, also $a \in b_{\mathfrak{m}}A_{\mathfrak{m}} \subset \mathfrak{b}_{\mathfrak{m}}$. Nach 3.46 folgt $a \in \mathfrak{b}$.

Behauptung 2): $v_{\mathfrak{m}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{m}}(\mathfrak{a}) + v_{\mathfrak{m}}(\mathfrak{b})$.
Beweis: Seien $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ so gewählt, daß $v_{\mathfrak{m}}(a) = v_{\mathfrak{m}}(\mathfrak{a})$, $v_{\mathfrak{m}}(b) = v_{\mathfrak{m}}(\mathfrak{b})$. Dann ist $v_{\mathfrak{b}}(\mathfrak{a}\mathfrak{b}) \leq v_{\mathfrak{m}}(ab) = v_{\mathfrak{m}}(a)+v_{\mathfrak{m}}(b) = v_{\mathfrak{m}}(\mathfrak{a}) + v_{\mathfrak{m}}(\mathfrak{b})$, da $ab \in \mathfrak{a}\mathfrak{b}$. Andererseits $v_{\mathfrak{m}}\left(\sum_{i=1}^{r} a_i b_i\right) \geq \min\{v_{\mathfrak{m}}(a_i b_i) \mid 1 \leq i \leq r\} \geq v_{\mathfrak{m}}(\mathfrak{a}) + v_{\mathfrak{m}}(\mathfrak{b})$, falls $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$, d.h. $\Sigma a_i b_i \in \mathfrak{a}\mathfrak{b}$ beliebig.

Behauptung 3): Wenn ein Ideal $\mathfrak{a} \neq (0)$ ist, gilt $v_{\mathfrak{m}}(\mathfrak{a}) > 0$ nur für endlich viele maximale Ideale $\mathfrak{m}$.
Beweis: $v_{\mathfrak{m}}(\mathfrak{a}) > 0 \Leftrightarrow \mathfrak{m} \supset \mathfrak{a}$. Da dann $\mathfrak{m}/\mathfrak{a}$ ein minimales Primideal in $A/\mathfrak{a}$ ist, liefert 4.17 die Behauptung.

Behauptung 4): $\mathfrak{a} = \prod_{\mathfrak{m}} \mathfrak{m}^{v_{\mathfrak{m}}(\mathfrak{a})}$.

Beweis: Auf der rechten Seite steht ein endliches Produkt nach Behauptung 3). Sei nun $\mathfrak{n}$ ein beliebiges maximales Ideal in A. Aufgrund der Behauptung 1) ist nur noch $v_{\mathfrak{n}}(\mathfrak{a}) = v_{\mathfrak{n}}\left(\prod_{\mathfrak{m}} \mathfrak{m}^{v_{\mathfrak{m}}(\mathfrak{a})}\right)$ zu zeigen. Es gilt aber $v_{\mathfrak{n}}(\mathfrak{n}) = 1$, da $v_{\mathfrak{n}}$ normiert ist, und $v_{\mathfrak{n}}(\mathfrak{m}) = 0$ für $\mathfrak{m} \neq \mathfrak{n}$, da $v_{\mathfrak{n}}(\mathfrak{m}) = \min\{v_{\mathfrak{n}}(a) \mid a \in \mathfrak{m}\}$ und wegen $\mathfrak{m} \not\subset \mathfrak{n}$ ein $a \in \mathfrak{m} \cap (A - \mathfrak{n})$ existiert. Deshalb ist

$$(*) \qquad v_{\mathfrak{n}}\left(\prod_{\mathfrak{m}} \mathfrak{m}^{v_{\mathfrak{m}}(\mathfrak{a})}\right) = \sum_{\mathfrak{m}} v_{\mathfrak{n}}\left(\mathfrak{m}^{v_{\mathfrak{m}}(\mathfrak{a})}\right) = \sum_{\mathfrak{m}} v_{\mathfrak{m}}(\mathfrak{a}) v_{\mathfrak{n}}(\mathfrak{m}) = v_{\mathfrak{n}}(\mathfrak{a}) .$$

Damit ist die Existenz der Zerlegung bewiesen; die Eindeutigkeit folgt ebenfalls aus (*).

b) O.E. ist $\mathfrak{a} \neq (0)$. Sei $x \in \mathfrak{a} - \{0\}$, also $(x) \subset \mathfrak{a}$. Sei ferner $\mathfrak{a} = \prod \mathfrak{m}_i^{n_i}$ und $(x) = \prod \mathfrak{m}_i^{r_i}$. Dann ist $r_i - n_i \geq 0$ nach (*) und Behauptung 1). Definiere $\mathfrak{b} := \prod \mathfrak{m}_i^{r_i - n_i}$. Es ist $\mathfrak{a}\mathfrak{b} = (x)$. —

Bemerkung 8.12 Ein Integritätsring, der a) oder b) aus 8.11 erfüllt, ist ein Dedekindring. Siehe 12.28.

Bemerkung 8.13 Ist A ein noetherscher Integritätsring der Dimension 1 und B der ganze Abschluß von A in einem endlichen Erweiterungskörper von $Q(A)$, dann ist B ein Dedekindring nach Satz 4.54 (Krull-Akizuki). Aber B ist nicht immer endlich über A. (Siehe A5.)

Satz 8.14 *(Serresches Kriterium) Sei* A *ein noetherscher Integritätsring. Mit* P *sei die Menge seiner Primideale der Höhe* 1 *bezeichnet. Dann sind äquivalent:*

(i) A *ist ganz abgeschlossen.*

(ii) *(a) Für jedes* $\mathfrak{p} \in P$ *ist* $A_{\mathfrak{p}}$ *ein diskreter Bewertungsring,*
(b) für jedes $a \in A - \{0\}$ *ist* $\operatorname{Ass}(A/aA) \subset P$.

(iii) *(a) Für jedes* $\mathfrak{p} \in P$ *ist* $A_{\mathfrak{p}}$ *ein diskreter Bewertungsring,*
(b) $A = \bigcap_{\mathfrak{p} \in P} A_{\mathfrak{p}}$.

Beweis: (i) ⇒ (ii): Da A ganz abgeschlossen ist, gilt dies auch für $A_{\mathfrak{p}}$ nach 7.14. Ist $\operatorname{ht}(\mathfrak{p}) = 1$, so ist $A_{\mathfrak{p}}$ nach 8.8 (i) ⟺ (ii) ein diskreter Bewertungsring. Das ist (a).

Nun zu (b): Sei $a \in A - \{0\}$, $\mathfrak{p} \in \operatorname{Ass}(A/aA)$. Nach 4.11 ist dann

$\mathfrak{p}A_{\mathfrak{p}} \in \mathrm{Ass}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}/aA_{\mathfrak{p}})$, vermöge 8.8 (iii) $\Longleftrightarrow$ (i) also $A_{\mathfrak{p}}$ ein diskreter Bewertungsring und deshalb $\mathrm{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}} = 1$.

(ii) $\Rightarrow$ (iii): Wegen (ii) (b) genügt es, folgendes Lemma zu zeigen:

Lemma 8.15 *Sei* A *ein noetherscher Integritätsring und* $Q = \bigcup_{a \in A-\{0\}} \mathrm{Ass}(A/aA)$. *Dann ist* $A = \bigcap_{\mathfrak{p} \in Q} A_{\mathfrak{p}}$.

Beweis hierfür: Sei $x = \frac{b}{a} \in Q(A)$ mit $b,a \in A$ und $x \in A_{\mathfrak{p}}$ für alle $\mathfrak{p} \in Q$. Wir müssen zeigen, daß $b \in aA$, d.h. $(bA+aA)/aA = 0$, d.h. $\mathrm{Ass}_A((bA+aA)/aA) = \emptyset$ ist (4.5). Sei deshalb $\mathfrak{q} \in \mathrm{Ass}_A((bA+aA)/aA)$, also insbesondere $\mathfrak{q} \in \mathrm{Ass}_A(A/aA)$ gemäß 4.9 und somit $\mathfrak{q} \in Q$. Mit $x \in A_{\mathfrak{q}}$ ist $b \in aA_{\mathfrak{q}}$ und darum $((bA+aA)/aA)_{\mathfrak{q}} = 0$, d.h. $\mathfrak{q} \notin \mathrm{Supp}((bA+aA)/aA)$. Dies widerspricht aber der Beziehung "Ass $\subset$ Supp" (4.15). —

Zurück zu 8.14 (iii) $\Rightarrow$ (i): A ist Durchschnitt von diskreten Bewertungsringen. Diese sind nach 8.8 (i) $\Longleftrightarrow$ (ii) ganz abgeschlossen. Also gilt dies auch für A. —

Aufgaben und Hinweise

1) Der reduzierte Ring A besitze nur endlich viele minimale Primideale $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$. Ferner sei $S = A - \bigcup_{i=1}^{n} \mathfrak{p}_i$ die Menge seiner Nichtnullteiler (2.17). Dann ist auf kanonische Weise $S^{-1}A \simeq \prod_{i=1}^{n} Q(A/\mathfrak{p}_i)$ (2. A1). Sei B der ganze Abschluß von A in $S^{-1}A$. Zeige: Dann ist $B \simeq \prod_{i=1}^{n} B_i$, wobei B_i isomorph zum ganzen Abschluß von $A/\mathfrak{p}_i$ in $Q(A/\mathfrak{p}_i)$ ist - und alles ist kanonisch. (Hinweis: Für ein idempotentes Element e hat man die Ganzheitsgleichung $e^2-e = 0$ über jedem Unterring.)

2) Sei $A \subset B$ eine Ringerweiterung und $\mathfrak{c} := \{c \in A \mid cB \subset A\} = \mathrm{Ann}_A(B/A)$ der sogenannte Führer dieser Erweiterung. Zeige:
   a) $\mathfrak{c}$ ist ein gemeinsames Ideal von A und B, d.h. ein in A enthaltenes Ideal von B, und zwar das größte unter all diesen.
   b) Sei $\mathfrak{p} \in \mathrm{Spec}\, A$. Aus $\mathfrak{p} \not\supset \mathfrak{c}$ folgt $A_{\mathfrak{p}} = B_{\mathfrak{p}}$. ($B_{\mathfrak{p}} := (A-\mathfrak{p})^{-1}B$.) Wenn B endlich über A ist, so folgt aus $A_{\mathfrak{p}} = B_{\mathfrak{p}}$, daß $\mathfrak{p} \not\supset \mathfrak{c}$ gilt (4.14 und 3.39).

c) Sei zusätzlich A integer, B der ganze Abschluß von A und $A \subset B$ endlich. Dann ist $\mathfrak{c} \neq (0)$. (Betrachte die "Nenner" eines Erzeugendensystems des A-Moduls B.) Für $\mathfrak{p} \in \operatorname{Spec} A$ gilt die Äquivalenz: $A_{\mathfrak{p}}$ ist ganz abgeschlossen $\Leftrightarrow$ $\mathfrak{p} \not\supset \mathfrak{c}$. (Beachte 7.13, 7.14.) Also ist $\{\mathfrak{p} \in \operatorname{Spec} A \mid A_{\mathfrak{p}}$ ganz abgeschlossen$\}$ offen und dicht in $\operatorname{Spec} A$ im Sinne der Zariski-Topologie (1. A4).

3) Ganz abgeschlossene noethersche Integritätsringe haben nach 8.14 eine recht angenehme Struktur. Der Übergang von einem noetherschen Integritätsring A (bzw. noetherschen reduzierten Ring A) zu seinem ganzen Abschluß $\bar{A}$ in $Q(A)$ (bzw. in $S^{-1}A$, $S := \{\text{Nichtnullteiler}\}$, vgl. A1) bedeutet also eine gewisse Glättung, zumindest, wenn $\bar{A}$ wieder noethersch ist. Dies ist jedenfalls dann der Fall, wenn $\bar{A}$ endlich über A ist. Wenn letzteres gilt, kann man ferner A2 c) anwenden. Die Eigenschaft, einen endlichen ganzen Abschluß zu haben, ist also sehr wichtig.

4) Sei k ein Körper. Zeige:

a) $k[\![X]\!]$, der formale Potenzreihenring in einer Unbestimmten, ist ein diskreter Bewertungsring.

b) Die "formalen Laurentreihen mit endlichem Hauptteil": $\sum\limits_{i=n}^{\infty} a_i X^i$, $n \in \mathbb{Z}$, bilden einen Körper $k(\!(X)\!)$; dieser ist "der" Quotientenkörper von $k[\![X]\!]$. Wie sieht die zum Bewertungsring $k[\![X]\!]$ gehörige Bewertung aus?

5) a) Sei $K \subset L$ eine radizielle (d.i. rein-inseparable) Körpererweiterung vom Grade $p = \operatorname{char} K$ (> 0). Zeige: Für $\alpha \in L - K$ ist dann $\operatorname{Mipo}(\alpha, K) = X^p - \alpha^p$. Wenn A ein ganz abgeschlossener Ring mit $Q(A) = K$ ist, ist also $B = \{\alpha \in L \mid \alpha^p \in A\}$ der ganze Abschluß von A in L.

b) Konstruiere ein Beispiel, so daß - mit obigen Voraussetzungen und Bezeichnungen - B nicht endlich über A ist, wie folgt (E. Artin und - unabhängig - O. Zariski, [Artin]): Sei k ein Körper der Charakteristik $p \geq 0$. Alles spielt sich ab im Körper $k(\!(X)\!)$. Sei $\eta = \sum\limits_{i \geq 0} c_i X^i \in k[\![X]\!]$ (mit $c_i \in k$) transzendent über $k(X)$, und $Y = \eta^p = \sum\limits_{i \geq 0} c_i^p X^{pi}$. Setze $K := k(X,Y)$, $L := k(X,\eta) = K(\sqrt[p]{Y})$ und $A = k[\![X]\!] \cap K$. Dann ist A ein diskreter Bewertungsring mit Primelement X. Für jedes $n \in \mathbb{N}$ kann man $Y \overset{(*)}{=} f_n^p + X^{pn} Y_n$ schreiben, wobei f_n ein Polynom in X und $Y_n \in k[\![X]\!]$ ist. Dann ist aber auch

$Y_n \in k(X,Y)$, also $Y_n \in A$. Aus (*) folgt $X^{-n}\eta - X^{-n}f_n = \sqrt[p]{Y_n} \in B$ (siehe oben). Wäre B endlich über A, so gäbe es ein $d \in A$, so daß $db \in A + A\eta + A\eta^2 + \ldots + A\eta^{p-1}$ für alle $b \in B$ gälte. Dieses d müßte durch X^n teilbar sein, und zwar für alle n.

6) Sei A ein diskreter Bewertungsring, $K = Q(A)$. Zeige:
a) Für alle $x \in K^*$ gilt: $x \in A$ oder $x^{-1} \in A$.
b) Sei B ein Ring zwischen A und K. Dann gilt $B = A$ oder $B = K$.
Bemerkung: Durch die Eigenschaft a) definiert man allgemeinere Bewertungsringe. Man kann dies auch durch eine Verschärfung von b) tun:
b') Sei B ein lokaler Ring zwischen A und K, dessen maximales Ideal das von A umfaßt. Dann gilt $A = B$.
Die Äquivalenz von a) und b') ist nicht trivial. ([Bourbaki] chap.VI.)

7) Bestimme die (normierten) diskreten Bewertungen von $\mathbb{Q}$.
(Wenn A ein DBR mit $Q(A) = \mathbb{Q}$ ist, ist $A \supset \mathbb{Z}$.
Bestimme $\mathfrak{m} \cap \mathbb{Z}$, wenn $\mathfrak{m}$ das maximale Ideal von A ist.)

8) Sei k ein Körper. Bestimme die (normierten) diskreten Bewertungen von $k(X)$, die auf k trivial sind. (Wenn A ein DBR mit $Q(A)=k(X)$ ist, gilt $A \supset k$, ferner $X \in A$ oder $X^{-1} \in A$. Beachte: Es gibt nur ein solches A mit $A \supset k[X^{-1}]$, aber $A \not\supset k[X]$.)

9) Welcher Zusammenhang besteht zwischen Primärzerlegung eines Ideals und seiner Darstellung als Produkt maximaler Ideale in einem Dedekindring?

10) Seien A ein Dedekindring, $\mathfrak{m}_1,\ldots,\mathfrak{m}_r$ endlich viele maximale Ideale von A, $n_1,\ldots,n_r \in \mathbb{Z}$, $a_1,\ldots,a_r \in Q(A)$. Zeige:
a) Es gibt ein $x \in Q(A)$ mit $v_{\mathfrak{m}_i}(x-a_i) \geq n_i$ und $v_{\mathfrak{n}}(x) \geq 0$ für alle von den $\mathfrak{m}_1,\ldots,\mathfrak{m}_r$ verschiedenen maximalen Ideale $\mathfrak{n}$ von A.
b) Es gibt ein $x \in Q(A)$ mit $v_{\mathfrak{m}_i}(x) = n_i$, $v_{\mathfrak{n}}(x) \geq 0$ für alle maximalen Ideale $\mathfrak{n}$ von A, die verschieden von den $\mathfrak{m}_1,\ldots,\mathfrak{m}_r$ sind.
(Für $a_i \in A$ folgt a) aus dem chinesischen Restsatz 1.9, 1.10.
b) folgt aus a).)

11) Zeige: In einem Dedekindring wird jedes Ideal $\mathfrak{a} \neq (0)$ von 2 Elementen erzeugt, von denen eines beliebig in $\mathfrak{a} - \{0\}$ gewählt werden kann.

12) Eine Verallgemeinerung von Lemma 8.15 ist Satz 1.6 in [Ischebeck]. (N.B.: In der zitierten Arbeit ist Lemma 3.9 falsch und deshalb Satz 3.7 nicht bewiesen. Diesen Hinweis verdanken wir Herrn H. Krämer (Hamburg).)

13) Krull-Ringe. Ein (nicht notwendig noetherscher) Ring A heißt Krull-Ring (oder krullsch), wenn er ein Integritätsring ist, der die Aussage (iii) aus Satz 8.14 und zusätzlich folgende Bedingung erfüllt: Jedes $a \in A - \{0\}$ liegt in nur endlich vielen $\mathfrak{p} \in P$. Die Klasse der Krullringe umfaßt also die der noetherschen ganz abgeschlossenen Integritätsringe, besitzt aber - meist im Gegensatz zu letzterer - folgende Eigenschaften:

a) Jeder (nicht notwendig noethersche) faktorielle Ring ist krullsch.

b) Wenn A krullsch und $Q(A) \subset L$ eine endliche Körpererweiterung ist, so ist der ganze Abschluß von A in L wieder krullsch.

c) Der Durchschnitt zweier krullscher Unterringe eines Ringes ist krullsch. (Insbesondere gilt dies für $k \cap A$, wenn A krullsch und k ein Unterkörper von $Q(A)$ ist.)

d) Jeder Polynomring - auch in unendlich vielen Unbestimmten - über einem Krull-Ring ist krullsch.

e) Mit A ist jeder Bruchring $S^{-1}A$ krullsch.

f) Der ganze Abschluß eines noetherschen Integritätsringes ist krullsch.

Zu a) bis e) siehe [Bourbaki], chap. VII, zu d) insbesondere Exerc. 1.8. Zu f) siehe [Fossum] Chap. I, Theorem 4.3, [Nagata 2] oder [Nagata], 33.10.

14) Sei A ein noetherscher Integritätsring der Dimension ≤ 2. Dann ist der ganze Abschluß von A ebenfalls noethersch. Der Fall $\dim A = 1$ ist wegen 4.54 (Krull-Akizuki) klar. Zum Fall $\dim A = 2$ siehe [Nagata 2] oder [Nagata] , 33.12. Für $\dim A = 3$ findet sich ein Gegenbeispiel in [Nagata] A1 Ex. 5. Schon im Fall $\dim A = 1$ braucht der ganze Abschluß nicht endlich über A zu sein. S.loc.cit. Ex. 3.

Beachte, daß im Falle $\dim A \leq 2$ aus obigem Ergebnis sich auch sofort ergibt, daß der ganze Abschluß B von A in einem endlichen Erweiterungskörper L von $Q(A)$ noethersch ist. Es läßt sich nämlich leicht ein Unterring B' von B finden, der endlich über A ist und $Q(B') = Q(B)$ erfüllt.

Vgl. zu dieser Thematik Satz 9.40 und Hinweise zu §18.

15) In der Literatur wird häufig folgende Terminologie benutzt: Seien A,B wie in A1. Dann heißt B die Normalisierung von A. Ferner heißt A normal, wenn es die Voraussetzungen von A1 erfüllt und $A = B$ ist.

16) Zu einer "schwachen" Art von Normalisierung eines reduzierten Ringes A, der sogenannten Seminormalisierung ${}^+A$ siehe [Swan]. Unter der Voraussetzung von A1 gilt $A \subset {}^+A \subset B$.

§9 ANFANGSGRÜNDE DER ALGEBRAISCHEN GEOMETRIE

1. Algebren von endlichem Typ über einem Körper

Definition 9.1 Sei B ein Ring.

a) Eine B-Algebra ist ein Ring A zusammen mit einem Ringhomomorphismus $B \longrightarrow A$. Letzterer wird auch als Strukturhomomorphismus bezeichnet.

b) A_1, A_2 seien B-Algebren mit Strukturhomomorphismen $B \xrightarrow{\alpha_i} A_i$.
Ein B-Algebrenhomomorphismus $f\colon A_1 \longrightarrow A_2$ ist ein Ringhomomorphismus, für den das Dreieck

$$\begin{tikzcd} A_1 \arrow[rr, "f"] & & A_2 \\ & B \arrow[ul, "\alpha_1"] \arrow[ur, "\alpha_2"'] & \end{tikzcd}$$

kommutativ ist, d.h. $\alpha_2 = f \circ \alpha_1$ gilt.

c) Es ist klar, was man eine Unteralgebra nennen soll, und deshalb auch, was ein Erzeugendensystem einer Algebra bedeutet.

d) Eine B-Algebra A heißt von endlichem Typ, wenn sie als B-Algebra endlich erzeugt ist, d.h. wenn es einen surjektiven B-Algebrenhomomorphismus $B[X_1,\dots,X_n] \longrightarrow A$ gibt.

e) Eine B-Algebra A heißt endlich, wenn sie als B-Modul endlich ist.

(Im Unterschied zu 7.1 werden in obigen Definitionen nicht nur injektive Ringhomomorphismen betrachtet.)

Satz 9.2 (*Noethersches Normalisierungslemma*):
Seien k *ein Körper,* A *eine integre* k*-Algebra von endlichem Typ und* $n = \mathrm{trgd}_k Q(A)$. *Dann gibt es* n *über* k *algebraisch unabhängige Elemente* $x_1,\dots,x_n \in A$, *so daß* A *endlich über* $k[x_1,\dots,x_n]$ *ist. Insbesondere ist dann* $\dim A = n$.

(Für eine Körpererweiterung $k \subset K$ bezeichnet $\mathrm{trgd}_k K$ ihren Transzendenzgrad.)
Zunächst ein Lemma, welches für $d = 10$ jedermann und für $d = 2$ jedem Computer vertraut ist:

Seien $d, n, a_0,\dots,a_n, a'_0,\dots,a'_n$ *natürliche Zahlen mit* $0 \le a_i < d$, $0 \le a'_i < d$ *und* $\sum_{i=0}^{n} a_i d^i = \sum_{i=0}^{n} a'_i d^i$. *So folgt* $a_i = a'_i$ *für* $i = 0,\dots,n$. —

Beweis von Satz 9.2: Sei $A = k[Y_1,\dots,Y_m]/\mathfrak{p}$ mit Unbestimmten Y_i und einem Primideal $\mathfrak{p}$. Mit y_i bezeichne die Restklasse von Y_i modulo $\mathfrak{p}$.

Induktion nach m mit Induktionsanfang $m \le n$: Da die Menge $\{y_1,\dots, y_m\}$ eine Transzendenzbasis von $Q(A)$ über k enthält, muß sie im Falle "$m \le n$" schon selber eine Transzendenzbasis sein. (D.h. es ist $m = n$ und $\mathfrak{p} = (0)$.) Wähle $x_i = y_i$.
Sei jetzt $m > n$, insbesondere $\mathfrak{p} \neq (0)$. Es genügt, einen Ring B zwischen k und A zu finden, der von $m-1$ Elementen erzeugt wird, und über welchem A endlich ist. Denn dann ist $\mathrm{trgd}_k Q(B) = \mathrm{trgd}_k Q(A)$. Also existieren nach Induktionsvoraussetzung $x_1,\dots,x_n \in B$, algebraisch unabhängig, derart daß B, mithin nach 7.6 auch A, endlich über $k[x_1,\dots,x_n]$ ist.

Zur Konstruktion von B sei

$$(*) \qquad f = \sum_{J \in \mathbb{N}^m} a_J Y^J \in \mathfrak{p} - (0),$$

wo $Y^J := Y_1^{j_1} \cdot \ldots \cdot Y_m^{j_m}$ für $J = (j_1,\dots,j_m)$ geschrieben wurde. Sei $d > \mathrm{grad}\, f$ eine natürliche Zahl. (Es genügt, $d > \operatorname{Max}_i \mathrm{grad}_{Y_i} f$ zu wählen.) Wir definieren $J^* := j_1 + j_2 d + \ldots + j_m d^{m-1}$ für $J = (j_1,\dots,j_m)$.
Setze nun $Z_i := Y_i - Y_1^{d^{i-1}}$ für $2 \le i \le m$. Aus $(*)$ erhalten wir dann

$f = f\left(Y_1, Z_2 + Y_1^{d}, \ldots, Z_m + Y_1^{d^{m-1}}\right) = \sum_{J \in \mathbb{N}^m} \left(a_J Y_1^{J^*} + g_J(Y_1, Z_2, \ldots, Z_m)\right)$ mit

$\operatorname{grad}_{Y_1} g_J < J^*$. Da aber nach dem Lemma und der Wahl von d diejenigen J^*, für die $a_J \neq 0$ ist, paarweise verschieden sind, ist

$f = a_{J_0} Y_1^{J_0^*} + h(Y_1, Z_2, \ldots, Z_m)$ mit $a_{J_0} \in k^*$ und $\operatorname{grad}_{Y_1} h < J_0^*$.

Da $f \in \mathfrak{p}$ ist, bedeutet dies, daß Y_1 ganz über $B := k[z_2, \ldots, z_m]$ ist, wenn mit z_i die Restklasse von Z_i modulo $\mathfrak{p}$ bezeichnet wird. –

Lemma 9.3 *a) Sei* A *ein noetherscher Integritätsring.*

1. Wenn P *eine unendliche Menge von Primidealen der Höhe* 1 *ist, gilt* $\bigcap_{\mathfrak{p} \in P} \mathfrak{p} = (0)$.

2. Wenn $\dim A > 1$ *ist, besitzt* A *unendlich viele Primideale der Höhe* 1.

b) k *sei ein Körper. Dann hat* $k[X]$ *unendlich viele maximale Ideale.*

Beweis: Zu a): 1. Läge $a \in A - (0)$ in unendlich vielen Primidealen der Höhe 1, so hätte der noethersche Ring A/Aa unendlich viele minimale Primideale im Widerspruch zu 4.17.

2. 6.21.

Zu b): Euklid: Gäbe es nur endlich viele irreduzible normierte Polynome $f_1, \ldots, f_r$, so bilde $F = \prod_{i=1}^{r} f_i + 1$. Offenbar ist $\prod_{i=1}^{r} f_i + 1 \notin k$, also $\prod_{i=1}^{r} f_i + 1 \notin (k[X])^*$, aber $f_i \nmid F$. Somit gibt es unendlich viele Primpolynome, also unendlich viele maximale Ideale, da $k[X]$ ein Hauptidealring ist. –

Satz 9.4 *(Hilbertscher Nullstellensatz, algebraische Form): Sei* k *ein Körper,* A *eine* k*-Algebra von endlichem Typ. Dann gilt:*

a) Für jedes maximale Ideal $\mathfrak{m}$ *ist* $k \subset A/\mathfrak{m}$ *eine endliche Körpererweiterung.*

b) Jedes Ideal $\mathfrak{a} \subset A$ *mit* $\sqrt{\mathfrak{a}} = \mathfrak{a}$ *ist Durchschnitt von maximalen Idealen von* A.

Beweis: a) $A/\mathfrak{m}$ ist wie A von endlichem Typ über k. Nach 9.2 gilt also $\operatorname{trgd}_k(A/\mathfrak{m}) = \dim(A/\mathfrak{m}) = 0$; d.h. $A/\mathfrak{m}$ ist algebraisch über k, somit - da von endlichem Typ - auch endlich über k.

b) Nach 1.18 ist $\mathfrak{a} = \sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \supset \mathfrak{a} \\ \text{prim}}} \mathfrak{p}$. Deshalb genügt es, den Fall, daß $\mathfrak{a}$ prim ist, zu betrachten. Sei $\mathfrak{p}$ maximal in der Menge aller Primideale, die nicht Durchschnitt maximaler Ideale sind. Insbesondere ist $\mathfrak{p}$ selbst nicht maximal, also $\dim(A/\mathfrak{p}) > 0$.

Gilt $\dim(A/\mathfrak{p}) = 1$, so gibt es nach 9.2 ein $x \in A/\mathfrak{p}$, transzendent über k, derart daß $A/\mathfrak{p}$ über $k[x]$ ganz ist. Mit $k[x]$ hat $A/\mathfrak{p}$ unendlich viele maximale Ideale (9.3b) und 7.20). Deren Durchschnitt ist (0) in $A/\mathfrak{p}$ nach 9.3a)1. Also ist $\mathfrak{p}$ in A Durchschnitt maximaler Ideale. Widerspruch!

Gilt $\dim A/\mathfrak{p} > 1$, so hat $A/\mathfrak{p}$ unendlich viele Primideale der Höhe 1 nach 9.3a)2. Mit 9.3a)1. folgt, daß $\mathfrak{p}$ Durchschnitt von Primidealen ist, die $\mathfrak{p}$ echt umfassen, die also (nach Wahl von $\mathfrak{p}$) selber Durchschnitt maximaler Ideale sind. Widerspruch! –

Folgerung 9.5 *Sei* $f: A_1 \longrightarrow A_2$ *ein Homomorphismus von* k-*Algebren endlichen Typs und* $\mathfrak{m}$ *ein maximales Ideal von* A_2. *Dann ist* $f^{-1}(\mathfrak{m})$ *ein maximales Ideal von* A_1.

Beweis: Man hat injektive Ringhomomorphismen $k \hookrightarrow A_1/F^{-1}(\mathfrak{m}) \hookrightarrow A_2/\mathfrak{m}$. Da $A_2/\mathfrak{m}$ nach 9.4a) endlich über k ist, ist es erst recht endlich über dem Integritätsring $A_1/f^{-1}(\mathfrak{m})$. Dieser ist also nach 7.18 ein Körper. –

N.B.: Für beliebige Ringhomomorphismen ist die Folgerung nicht richtig. Beispiel: $\mathbb{Z} \longrightarrow \mathbb{Q}$.

Der Inhalt der nächsten beiden Abschnitte wird im folgenden kaum gebraucht. Man darf ihn deshalb beim ersten Lesen überschlagen. Dazu ist allerdings zu bemerken, daß die Wichtigkeit der kommutativen Algebra großenteils auf ihren Anwendungen in der Algebraischen Geometrie beruht.

2. Affine algebraische Varietäten

In diesem Abschnitt bezeichne k *einen algebraisch abgeschlossenen Körper und* $A = k[X_1,\dots,X_n]$ *den Polynomring in* n *Unbestimmten.*
Unter $(a_1,\dots,a_n)$ *mit* $a_i \in k$ *verstehen wir hier ein* n-*Tupel (in* k^n*) – nicht ein Ideal. Das von* $f_1,\dots,f_r$ *in* A *erzeugte Ideal wird hier mit* $(f_1,\dots,f_r)A$ *bezeichnet.*

Definition 9.6 Für $F \subset A$ sei definiert
$V(F) := \{(a_1,\ldots,a_n) \in k^n \mid f(a_1,\ldots,a_n) = 0$ für alle $f \in F\}$. $V(F)$ heißt die affine Varietät von F und ist die Lösungsmenge von $f(x) = 0$, $f \in F$. Die $V(F)$ heißen auch algebraische Mengen (in k^n).

Feststellung 9.7 *a) Ist* $\mathfrak{a} \subset A$ *das von* F *erzeugte Ideal in* A, *so gilt* $V(\mathfrak{a}) = V(F)$.
b) $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.

Beweis: a) $F \subset \mathfrak{a} \Rightarrow V(F) \supset V(\mathfrak{a})$. Sind $f_i \in F$, $h_i \in A$ beliebig, so ist $(\Sigma h_i f_i)(a) = \Sigma h_i(a) f_i(a) = 0$ für alle $a \in V(F)$. Es folgt $a \in V(\mathfrak{a})$.
b) Wegen $\sqrt{\mathfrak{a}} \supset \mathfrak{a}$ gilt $V(\sqrt{\mathfrak{a}}) \subset V(\mathfrak{a})$. Wenn $a \in V(\mathfrak{a})$ und $f \in \sqrt{\mathfrak{a}}$ ist, gilt $f^m \in \mathfrak{a}$ für ein m, also $(f(a))^n = 0$ in k und somit $f(a) = 0$. Es folgt $a \in V(\sqrt{\mathfrak{a}})$. –

Die algebraischen Teilmengen eines k^n sind die ersten Objekte der algebraischen Geometrie. Jede solche ist nach 9.7 von der Form $V(\mathfrak{a})$, wobei $\mathfrak{a}$ ein Ideal mit $\mathfrak{a} = \sqrt{\mathfrak{a}}$ ist. Andererseits ist jede algebraische Menge auch von der Form $V(F)$, wobei F eine endliche Menge von Polynomen ist. Denn A ist noethersch und $V(\mathfrak{a}) = V(f_1,\ldots,f_r)$, falls $\mathfrak{a}$ von $f_1,\ldots,f_r$ erzeugt. (Wie üblich wurde hier $V(f_1,\ldots,f_r)$ statt $V(\{f_1,\ldots,f_r\})$ geschrieben.)

Definition 9.8 a) Ein Ideal $\mathfrak{a}$ heißt reduziert oder Radikalideal, wenn $\mathfrak{a} = \sqrt{\mathfrak{a}}$ gilt.
b) $\operatorname{Spmax} B$ = Menge der maximalen Ideale des Ringes B.

Definition 9.9 Sei $M \subset k^n$ eine beliebige Teilmenge.
$I(M) := \{f \in A \mid f(a) = 0$ für alle $a \in M\}$ heißt das Verschwindungsideal von M.

Bemerkung 9.10 $I(M)$ ist ein reduziertes Ideal. Dies sieht man wie 9.7.

Satz 9.11 *a) Die maximalen Ideale von* A *sind diejenigen von der Form* $(X_1-a_1,\ldots,X_n-a_n)A$ *mit* $a_i \in k$. *Die Abbildung* $\varphi\colon k^n \longrightarrow \operatorname{Spmax} A$, *definiert durch* $a = (a_1,\ldots,a_n) \longmapsto \mathfrak{m}_a := (X_1-a_1,\ldots,X_n-a_n)A$, *ist bijektiv. Die Umkehrabbildung* ψ *ordnet jedem maximalen Ideal* $\mathfrak{m}$ *von* A *das einzige Element von* $V(\mathfrak{m})$ *zu.*

b) *Für* $f \in A$ *und* $a_i \in k$ *gilt:*

$f \in (X_1-a_1,\dots,X_n-a_n)A \iff f(a_1,\dots,a_n) = 0$.

Beweis: a) Die Zuordnung $X_i \mapsto X_i-a_i$ definiert einen k-Algebrenautomorphismus von A . Das maximale Ideal $(X_1,\dots,X_n)A$ wird dabei auf $(X_1-a_1,\dots,X_n-a_n)A$ abgebildet. Also ist letzteres ein maximales Ideal.

Sei umgekehrt $\mathfrak{m}$ ein solches. Die Erweiterung $k \subset A/\mathfrak{m}$ ist nach 9.4a) endlich, also trivial, da k algebraisch abgeschlossen ist. Es gibt also $a_i \in k$ mit $X_i \equiv a_i \bmod \mathfrak{m}$, d.h. $X_i-a_i \in \mathfrak{m}$. Demnach muß $\mathfrak{m}$ mit dem maximalen Ideal $(X_1-a_1,\dots,X_n-a_n)A$ übereinstimmen.
Wir haben gezeigt, daß φ surjektiv ist. Da aber offenbar $V(\mathfrak{m}_a) = V(X_1-a_1,\dots,X_n-a_n) = \{a\}$ ist, ist ψ wohldefiniert und $\psi\circ\varphi = \mathrm{id}_{k^n}$, somit φ auch injektiv und ψ invers zu φ .

b) Offenbar ist $f(X_1,\dots,X_n) \equiv f(a_1,\dots,a_n) \bmod (X_1-a_1,\dots,X_n-a_n)A$.
Deshalb gilt: $f(X_1,\dots,X_n) \in (X_1-a_1,\dots,X_n-a_n)A$
$\iff f(a_1,\dots,a_n) \in (X_1-a_1,\dots,X_n-a_n)A \cap k = (0)$.(b) folgt auch aus a).)—

Folgerung 9.12 *Sei* $F \subset A$ *und* $a \in k^n$. *Dann gilt:*
$a \in V(F) \iff F \subset \mathfrak{m}_a \iff I(V(F)) \subset \mathfrak{m}_a$.
(Dabei ist $\mathfrak{m}_a$ wie in Satz 9.11 definiert.)

Beweis: Aus 9.11b) erhält man "$a \in V(F) \iff F \subset \mathfrak{m}_a$" durch Anwendung auf die $f \in F$ und "$a \in V(I(V(F))) \iff I(V(F)) \subset \mathfrak{m}_a$" durch Anwendung auf die $f \in I(V(F))$. Es ist aber $V(I(V(F))) = V(F)$. —

Bei der in 9.11a) angegebenen Korrespondenz entsprechen die Punkte von $V(F)$ also umkehrbar den maximalen Idealen von A , die F bzw. $I(V(F))$ umfassen, d.h. den maximalen Idealen von $A/(F)A$ bzw. $A/I(V(F))$. (Dabei ist $(F)A$ das von F in A erzeugte Ideal.) Da ein Ring genau dann maximale Ideale besitzt, wenn er nicht isomorph zu 0 ist, erhalten wir:

Folgerung 9.13 $V(F) \neq \emptyset \iff (F)A \neq A$. —

Schärfer gilt:

Satz 9.14 (*Hilbertscher Nullstellensatz, geometrische Form*):
Sei $F \subset A$, $\mathfrak{a} = (F)A$. *Dann ist* $I(V(F)) = \sqrt{\mathfrak{a}}$.

Beweis: $f \in I(V(F)) \iff f(a) = 0$ für alle $a \in V(F) \iff f \in \mathfrak{m}_a$ für alle $a \in V(F) \iff f \in \mathfrak{m}$ für alle $\mathfrak{m}$ mit $\mathfrak{m} \supset F$. Wegen 9.4b) ist letzteres äquivalent zu $f \in \sqrt{\mathfrak{a}}$. —

N.B.: Der Satz ist in der Tat eine wesentliche Verschärfung von 9.13. Denn er besagt nicht nur, daß ein echtes Ideal $\mathfrak{a}$ von A Nullstellen hat, sondern sogar, daß seine Nullstellenmenge so groß ist, daß nur die modulo $\mathfrak{a}$ nilpotenten Polynome auf ihr verschwinden.

Folgerung 9.15 *Die Abbildung* V *bildet die Menge der reduzierten Ideale in* $k[X_1,\ldots,X_n]$ *bijektiv und ordnungsumkehrend auf die Menge der algebraischen Mengen in* k^n *ab.* I, *eingeschränkt auf die algebraischen Mengen, ist die (ebenfalls ordnungsumkehrende) Umkehrabbildung.* —

Folgerung 9.16 *Für* $f,g \in A$ *gilt:* $V(f) \supset V(g) \iff$ *Jeder Primfaktor von* g *ist einer von* f.

Beweis: Sei $f = \prod_{i=1}^{r} p_i^{\;i}$ die Primfaktorzerlegung von f, $g = \prod_{i=1}^{s} q_i^{\;i}$ die von g. Nach 9.14 gilt: $I(V(f)) = \sqrt{(f)} = (p_1\cdot\ldots\cdot p_r)$ und $I(V(g)) = \sqrt{(g)} = (q_1\cdot\ldots\cdot q_s)$. Also: $V(f) \supset V(g) \iff I(V(f)) \subset I(V(g))$ $\iff (p_1\cdot\ldots\cdot p_r) \subset (q_1\cdot\ldots\cdot q_s) \iff f = hq_1\cdot\ldots\cdot q_s$ mit einem $h \in A$. —

Feststellung 9.17 a) *Für Ideale* $\mathfrak{a}_i$, $i \in I$, *in* A *gilt* $\bigcap_{i\in I} V(\mathfrak{a}_i) = V(\sum_{i\in I}\mathfrak{a}_i)$. *Es ist* $V(0) = k^n$.
b) *Für Ideale* $\mathfrak{a}_1,\ldots,\mathfrak{a}_r$ *in* A *gilt* $V(\mathfrak{a}_1\cdot\ldots\cdot\mathfrak{a}_r) = V(\mathfrak{a}_1\cap\ldots\cap\mathfrak{a}_r) = \bigcup_{i=1}^{r} V(\mathfrak{a}_i)$. *Es ist* $V(A) = \emptyset$.

Beweis: a) $V(\mathfrak{a}_j) \supset V(\sum_{i\in I}\mathfrak{a}_i)$ für $j \in I \Rightarrow \bigcap_{j\in I} V(\mathfrak{a}_j) \supset V(\sum_{i\in I}\mathfrak{a}_i)$.

$x \in \bigcap_{j\in I} V(\mathfrak{a}_j) \Rightarrow f(x) = 0$ für alle $f \in \mathfrak{a}_j$ und alle $j \in I \Rightarrow f(x) = 0$ für alle $f \in \bigcup_{j\in I}\mathfrak{a}_j \Rightarrow f(x) = 0$ für alle $f \in (\bigcup_{j\in I}\mathfrak{a}_j)A = \sum_{i\in I}\mathfrak{a}_i \Rightarrow$ $x \in V(\sum_{i\in I}\mathfrak{a}_i)$.

b) $\mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{a}$, $\mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{b} \Rightarrow V(\mathfrak{a}\cap\mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b}) \Rightarrow$ $V(\mathfrak{a}\mathfrak{b}) \supset V(\mathfrak{a}\cap\mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b})$. Ist $x \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$, so gibt es $f \in \mathfrak{a}$, $g \in \mathfrak{b}$ mit $f(x) \neq 0 \neq g(x)$, also $f\cdot g(x) \neq 0$, und deshalb $x \notin V(\mathfrak{a}\mathfrak{b})$. —

Definition 9.18 Eine algebraische Menge $M \subset k^n$ heißt irreduzibel, wenn $M \neq \emptyset$ ist und für je zwei algebraische Mengen $N_1, N_2 \subset k^n$ aus $N_1 \cup N_2 = M$ folgt: $M = N_1$ oder $M = N_2$.

<u>Satz 9.19</u> *Für eine algebraische Menge* M *gilt:*
M *ist irreduzibel* $\iff$ $I(M)$ *ist prim.*

<u>Beweis:</u> "$\Rightarrow$": Seien $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ die paarweise verschiedenen minimalen Primoberideale von $I(M)$. (Wegen 4.17 ist $r < \infty$.) Da $I(M)$ reduziert ist, ist $I(M) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$. Wäre $I(M)$ nicht prim, so $r > 1$. Setze $N_1 = V(\mathfrak{p}_1)$, $N_2 = V(\mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r)$, $N_1 \cup N_2 = M$, da
$M = V(I(M)) = V(\bigcap_{i=1}^{r} \mathfrak{p}_i) = V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r)$. Wäre $N_1 = M$, dann $\mathfrak{p}_1 = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$ (nach 9.15). Wäre $N_2 = M$, dann $\mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$. Beides steht (für $r > 1$) im Widerspruch zu

<u>Lemma 9.20</u> *Seien* $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ *und* $\mathfrak{q}_1,\dots,\mathfrak{q}_s$ *Primideale (eines beliebigen Ringes) mit* $\mathfrak{p}_i \not\supset \mathfrak{p}_j$ *und* $\mathfrak{q}_i \not\supset \mathfrak{q}_j$ *für* $i \neq j$. *Aus* $\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s$ *folgt dann* $\{\mathfrak{p}_1,\dots,\mathfrak{p}_r\} = \{\mathfrak{q}_1,\dots,\mathfrak{q}_s\}$.

<u>Beweis</u> hierfür: Für $1 \le i \le r$ gilt $\mathfrak{p}_i \supset \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s$. Also gibt es ein j mit $\mathfrak{p}_i \supset \mathfrak{q}_j$ (1.14). Zu diesem j gibt es ein l mit $\mathfrak{q}_j \supset \mathfrak{p}_l$. Es folgt $\mathfrak{p}_i \supset \mathfrak{p}_l$ und deshalb $i = l$ und $\mathfrak{p}_i = \mathfrak{q}_j$. Symmetrie liefert den Rest. —

Zurück zu 9.19. "$\Leftarrow$": $I(M) = \mathfrak{p}$. Sei $M = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$, also $\mathfrak{p} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$. Es folgt $\mathfrak{p} \supset \mathfrak{a} \cap \mathfrak{b}$, also $\mathfrak{p} \supset \mathfrak{a}$ oder $\mathfrak{p} \supset \mathfrak{b}$ nach 1.14. D.h. es ist $M \subset V(\mathfrak{a})$ oder $M \subset V(\mathfrak{b})$, also $M = V(\mathfrak{a})$ oder $V = V(\mathfrak{b})$. —

<u>Satz 9.21</u> *Eine algebraische Menge* M *ist Vereinigung endlich vieler irreduzibler algebraischer Mengen, die paarweise einander nicht umfassen:* $M = M_1 \cup \dots \cup M_r$ *Die Menge* $\{M_1,\dots,M_r\}$ *ist eindeutig bestimmt. Wenn* $I(M) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_s$ *mit den (paarweise verschiedenen) minimalen Primoberidealen* $\mathfrak{p}_i$ *von* $I(M)$ *ist, gilt* $r = s$ *und (nach Umnumerierung)* $M_i = V(\mathfrak{p}_i)$.

<u>Beweis:</u> Aus der o.a. Darstellung $I(M) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_s$ ergibt sich $M = V(I(M)) = V(\mathfrak{p}_1) \cup \dots \cup V(\mathfrak{p}_s)$ mit $V(\mathfrak{p}_i) \not\subset V(\mathfrak{p}_j)$ für $i \neq j$, da die $\mathfrak{p}_i$ reduziert sind und $\mathfrak{p}_i \not\supset \mathfrak{p}_i$ gilt. Ist $M = M_1 \cup \dots \cup M_r$ irgendeine solche Darstellung, so ist $M_j = V(\mathfrak{q}_j)$ mit Primidealen $\mathfrak{q}_j$ nach 9.19 und $\mathfrak{q}_i \not\subset \mathfrak{q}_j$, da $M_i \not\supset M_j$, für $i \neq j$. Wir erhalten $M = V(\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r)$, also $\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_s = I(M) = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$. Wende Lemma 9.20 an. —

Definition 9.22 Die M_i in Satz 9.21 heißen die irreduziblen Komponenten der algebraischen Menge M.

Beispiele 9.23 a) Für $f \in A$ gilt: $V(f)$ ist irreduzibel $\Leftrightarrow$ $f = p^N$ mit einem irreduziblen $p \in A$.
b) Sei $f = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$, p_i irreduzibel und paarweise verschieden. Dann ist $V(f) = V(p_1) \cup \ldots \cup V(p_s)$, und die $M_i := V(p_i)$ $(1 \leq i \leq s)$ sind die irreduziblen Komponenten von M.

Bemerkung 9.24 Ketten von irreduziblen algebraischen Teilmengen in $V(\mathfrak{a})$ entsprechen Ketten von Primidealen von $A/\mathfrak{a}$ und umgekehrt (vermöge I bzw. V).

Definition 9.25 Ist $M = V(\mathfrak{a})$ eine algebraische Menge des k^n, so setze man $\dim M := \dim A/I(M) = \dim A/\sqrt{\mathfrak{a}} = \dim A/\mathfrak{a}$.

Bemerkungen 9.26 a) Die irreduziblen nulldimensionalen algebraischen Teilmengen des k^n sind von der Form $V(\mathfrak{m})$, wo $\mathfrak{m}$ ein maximales Ideal von A ist, also einpunktig.
b) Die nulldimensionalen algebraischen Teilmengen von k^n sind genau die endlichen Teilmengen.
c) Eine irreduzible algebraische Teilmenge M von K^n hat genau dann die Dimension 1, wenn gilt:
1. M ist unendlich,
2. jede echte algebraische Teilmenge ist endlich.

Solche Mengen heißen irreduzible (affine algebraische) Kurven.

d) Eine (nicht notwendig irreduzible) algebraische Teilmenge M von k^n hat die Dimension 1 genau dann, wenn sie eine endliche Vereinigung irreduzibler Kurven, vereinigt mit einer endlichen Menge ist.
e) Die Dimension einer (nichtleeren) algebraischen Menge ist das Maximum der Dimensionen ihrer irreduziblen Komponenten.
Eine irreduzible algebraische Menge M hat die Dimension d genau dann, wenn M eine echte algebraische Teilmenge der Dimension $d-1$ besitzt und jede echte algebraische Teilmenge eine Dimension $\leq d-1$ hat.

N.B.: Man kann die Dimension einer algebraischen Menge induktiv durch die Aussagen b) und e) definieren.

Satz 9.27 *Sei* V *eine irreduzible algebraische Teilmenge von* k^n. *Dann ist* $\dim V = \mathrm{trgd}_k Q(A/I(V))$.

Beweis: Nach 9.2 gibt es über k algebraisch unabhängige $x_1,\dots,x_r$ in $A/I(V)$, derart, daß $A/I(V)$ ganz über $k[x_1,\dots,x_r]$ und $r = \mathrm{trgd}_k Q(A/I(V))$ ist. Es ist $\dim V = \dim A/I(V) \underset{7.23a)}{=} \dim k[x_1,\dots,x_r] \underset{6.28}{=} r$. —

Bemerkung 9.28 Seien $V \subset k^n$ und $W \subset k^m$ algebraische Mengen. Dann ist auch $V \times W \subset k^n \times k^m = k^{n+m}$ eine algebraische Menge. Nämlich: $X_1,\dots,X_n$, $Y_1,\dots,Y_m$ seien $n+m$ Unbestimmte und $F \subset k[X_1,\dots,X_n]$, $G \subset k[Y_1,\dots,Y_m]$ Teilmengen mit $V = V(F)$, $W = V(G)$. Betrachte $k[X_1,\dots,X_n]$ und $k[Y_1,\dots,Y_m]$ auf naheliegende Weise als Unterringe von $k[X_1,\dots,X_n, Y_1,\dots,Y_m]$. Dann ist offenbar $V \times W = V(F \cup G)$.

3. Morphismen

Weiterhin sei mit k ein algebraisch abgeschlossener Körper bezeichnet.

Definition 9.29 Seien $V \subset k^n$, $W \subset k^m$ algebraische Mengen. Eine Abbildung $f\colon V \longrightarrow W$ heißt Morphismus algebraischer Mengen, wenn es Polynome $f_1,\dots,f_m$ in n Variablen gibt, so daß für die Abbildung $F : k^n \longrightarrow k^m$, definiert durch $(x_1,\dots,x_n) \longmapsto (f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n))$ gilt: $F|V = f$. Ein Isomorphismus (algebraischer Mengen) ist ein Morphismus $f\colon V \longrightarrow W$, für den es einen Morphismus $g\colon W \longrightarrow V$ gibt mit $g \circ f = \mathrm{id}_V$ und $f \circ g = \mathrm{id}_W$.

Bemerkungen 9.30 a) Morphismen $V \longrightarrow W$ mit $W \subset k^m$ werden also durch m-Tupel von Polynomen gegeben. Dabei können verschiedene m-Tupel denselben Morphismus beschreiben. Genauer: $(f_1,\dots,f_m)$ und $(g_1,\dots,g_m)$ beschreiben denselben Morphismus $V \longrightarrow W$ dann und nur dann, wenn $f_i|V = g_i|V$, d.h. $f_i - g_i \in I(V)$ für $1 \le i \le m$ gilt.

b) id_V ist ein Morphismus. Desgleichen sind konstante Abbildungen Morphismen. Mit $\alpha\colon V_1 \longrightarrow V_2$ und $\beta\colon V_2 \longrightarrow V_3$ ist $\beta \circ \alpha$ ein Morphismus.

c) Eine Abbildung $\alpha\colon V \longrightarrow W$ ist ein Isomorphismus, wenn α bijektiv ist und α sowie α^{-1} Morphismen sind.

N.B.: Es gibt bijektive Morphismen, die keine Isomorphismen sind. Siehe A.9.

d) $V \subset k^n$ sei eine algebraische Menge. Die Morphismen $V \longrightarrow k$ bilden auf naheliegende Weise ein k-Algebra. Diese wird mit $k[V]$ bezeichnet. ("+" und "•" werden wie üblich, etwa wie bei stetigen Funktionen, definiert. Der Strukturhomomorphismus ordnet jedem $c \in k$ den entsprechenden konstanten Morphismus zu.) Im Falle $V = \emptyset$ erhält man den Nullring mit trivialem Strukturhomomorphismus.

Satz 9.31 *Für eine algebraische Teilmenge* V *des* k^n *hat man einen kanonischen* k-*Algebrenisomorphismus:*

$$k[X_1,\ldots,X_n]/I(V) \longrightarrow k[V].$$

Beweis: Für $f \in k[X_1,\ldots,X_n]$ sei mit $f|V$ der zugehörige Morphismus $V \longrightarrow k$ bezeichnet. Nach Definition ist jeder Morphismus $V \longrightarrow k$ von der Form $f|V$. Man erhält also eine surjektive Abbildung $k[X_1,\ldots,X_n] \longrightarrow k[V]$ durch $f \longmapsto f|V$. Diese Abbildung ist offenbar ein k-Algebrenhomomorphismus und hat den Kern $I(V)$. —

Definition 9.32 Zu einem Morphismus $\alpha\colon V \longrightarrow W$ algebraischer Mengen gehört ein k-Algebrenhomomorphismus $\alpha^*\colon k[W] \longrightarrow k[V]$, definiert durch $\alpha^*(f) = f \circ \alpha$ für Morphismen $f\colon W \longrightarrow k$.
(Beachte die "Pfeilumkehrung": $V \xrightarrow{\alpha} W$, $k[V] \xleftarrow{\alpha^*} k[W]$. Es ist hier so wie bei dualen Vektorräumen.)

Bemerkung 9.33 Es gilt $id_V^* = id_{k[V]}$, $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$. Die Zuordnung $V \longmapsto k[V]$, $\alpha \longmapsto \alpha^*$ ist ein "kontravarianter" Funktor von der "Kategorie" der (affinen) algebraischen Mengen in die "Kategorie" der reduzierten k-Algebren von endlichem Typ. Jede reduzierte k-Algebra von endlichem Typ ist isomorph zu einem $k[V]$. Denn sie ist von der Gestalt $k[X_1,\ldots,X_n]/\mathfrak{a}$ mit $\mathfrak{a} = \sqrt{\mathfrak{a}}$. Wegen 9.14 kann man $V = V(\mathfrak{a})$ wählen.

Den Punkten aus V entsprechen bijektiv die maximalen Ideale von $k[X_1,\ldots,X_n]$, die $I(V)$ umfassen, d.h. wegen 9.31 den maximalen Idealen von $k[V]$. Mit $\mathfrak{m}_{p,V}$ bezeichnen wir das zu $p \in V$ gehörige maximale Ideal von $k[V]$. (Für $V = k^n$ ist $\mathfrak{m}_{p,V} = \mathfrak{m}_p$ mit der Bezeichnung von 9.11.)

Satz 9.34 *Sei* $\alpha\colon V \longrightarrow W$ *ein Morphismus algebraischer Mengen und* $p \in V$. *Dann ist*

$$(\alpha^*)^{-1}(\mathfrak{m}_{p,V}) = \mathfrak{m}_{\alpha(p),W} \quad .$$

D.h. wenn man V *bzw.* W *(wie oben angegeben) mit* $\operatorname{Spmax} k[V]$ *bzw.* $\operatorname{Spmax} k[W]$ *identifiziert, induziert* $\alpha^*: k[W] \longrightarrow k[V]$ *die Abbildung* $\alpha: \operatorname{Spmax} k[V] \longrightarrow \operatorname{Spmax} k[W]$.

Beweis: a) Zunächst betrachten wir den Fall $V = k^n$, $W = k^m$. Sei $\alpha: k^n \longrightarrow k^m$ durch $f_1,\dots,f_m \in k[X_1,\dots,X_n]$ gegeben. Dann ist $\alpha^*: k[Y_1,\dots,Y_m] \longrightarrow k[X_1,\dots,X_n]$ als k-Algebrenhomomorphismus durch $Y_i \longmapsto f_i$ gegeben. Denn durch das Polynom Y_i wird als Abbildung $k^m \longrightarrow k$ die Projektion auf den i-ten Faktor (d.h. die i-te Koordinate) definiert. Verknüpft mit α ergibt sich f_i .

Also ist $\alpha^*(Y_i - f_i(p)) = f_i(X_1,\dots,X_n) - f_i(a_1,\dots,a_n) \in \mathfrak{m}_p$, wo $p := (a_1,\dots,a_n)$ sei. Somit ist $\alpha^*(\mathfrak{m}_{\alpha(p)}) \subset \mathfrak{m}_p$, mithin $\mathfrak{m}_{\alpha(p)} \subset (\alpha^*)^{-1}(\mathfrak{m}_p)$. Da $\mathfrak{m}_{\alpha(p)}$ ein maximales Ideal (und $1 \notin \mathfrak{m}_p$) ist, folgt der Satz in diesem Falle.

b) Sei jetzt $V \subset k^n$ eine algebraische Menge, $W = k^n$ und $\alpha: V \longrightarrow k^n$ die Inklusionsabbildung $(\alpha(p) = p)$. Diese ist ein Morphismus - nämlich durch das n-Tupel $X_1,\dots,X_n$ von Polynomen aus $k[X_1,\dots,X_n]$ definiert. Der Homomorphismus $\alpha^*: k[X_1,\dots,X_n] \longrightarrow k[V] = k[X_1,\dots,X_n]/I(V)$ ist die kanonische Restklassenabbildung. Offensichtlich ist $(\alpha^*)^{-1}(\mathfrak{m}_{p,V}) = (\alpha^*)^{-1}(\mathfrak{m}_p/I(V)) = \mathfrak{m}_p = \mathfrak{m}_{\alpha(p)}$ und damit der Satz auch in diesem Falle bewiesen.

c) Zuletzt betrachten wir den allgemeinen Fall. Seien V in k^n und W in k^m algebraische Mengen, $I(V) \subset k[X_1,\dots,X_n]$, $I(W) \subset k[Y_1,\dots,Y_m]$ und $i_1: V \longrightarrow k^n$, $i_2: W \longrightarrow k^m$ die Einbettungsabbildungen. Der Morphismus α sei durch $f_1,\dots,f_m \in k[X_1,\dots,X_n]$ gegeben. $F: k^n \longrightarrow k^m$ sei ebenfalls durch $f_1,\dots,f_m$ gegeben. Man hat also ein kommutatives Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & W \\ {\scriptstyle i_1}\downarrow & & \downarrow{\scriptstyle i_2} \\ k^n & \xrightarrow{F} & k^m \end{array} .$$

Das hieraus entstehende Diagramm

$$\begin{array}{ccc} k[V] & \xleftarrow{\alpha^*} & k[W] \\ {\scriptstyle i_1^*}\uparrow & & \uparrow{\scriptstyle i_2^*} \\ k[X_1,\dots,X_n] & \xleftarrow{F^*} & k[Y_1,\dots,Y_m] \end{array}$$

ist wegen der Funktoreigenschaft (9.33) ebenfalls kommutativ. Sei $p \in V$ und

$\mathfrak{n}/I(W) = (\alpha^*)^{-1}\mathfrak{m}_{p,V}$. Dann ist $\mathfrak{n} \overset{b)}{=} (i_2^*)^{-1}(\alpha^*)^{-1}\mathfrak{m}_{p,V} = (F^*)^{-1}(i_1^*)^{-1}\mathfrak{m}_{p,V}$ $\overset{b)}{=} (F^*)^{-1}\mathfrak{m}_p \overset{a)}{=} \mathfrak{m}_{F(p)} = \mathfrak{m}_{\alpha(p)}$, also $\mathfrak{n}/I(W) = \mathfrak{m}_{\alpha(p)}/I(W) \overset{b)}{=} \mathfrak{m}_{\alpha(p),W}$.

<u>Definition 9.35</u> $\mathrm{Mor}(V,W)$ bezeichnet die Menge der Morphismen $V \longrightarrow W$ und $\mathrm{Hom}_{k\text{-Alg}}(A,B)$ die Menge der k-Algebrenhomomorphismen $A \longrightarrow B$.

<u>Satz 9.36</u> *Die durch* $\alpha \longrightarrow \alpha^*$ *definierte Abbildung*

$$\mathrm{Mor}(V,W) \longrightarrow \mathrm{Hom}_{k\text{-Alg}}(k[W],k[V])$$

ist bijektiv.

<u>Beweis:</u> Injektivität: Wenn $\alpha \neq \beta$ ist, gibt es ein $p \in V$ mit $\alpha(p) \neq \beta(p)$, also $(\alpha^*)^{-1}(\mathfrak{m}) \neq (\beta^*)^{-1}(\mathfrak{m})$, wo $\mathfrak{m}$ das zu p gehörige maximale Ideal von $k[V]$ ist. Dann muß aber $\alpha^* \neq \beta^*$ sein.
Surjektivität: Sei $\varphi\colon k[W] \longrightarrow k[V]$ ein Homomorphismus, $k[V] = k[X_1,\ldots,X_n]/I(V)$, $k[W] = k[Y_1,\ldots,Y_m]/I(W)$. Betrachte

$$\begin{tikzcd}
k[X_1,\ldots,X_n] \arrow[d, "\kappa_1"] & k[Y_1,\ldots,Y_m] \arrow[l, dashed, "\Phi"'] \arrow[d, "\kappa_2"] \\
k[V] & k[W] \arrow[l, "\varphi"']
\end{tikzcd}$$

mit kanonischen κ_i. Wähle $f_1,\ldots,f_m \in k[X_1,\ldots,X_n]$ so, daß $\kappa_1(f_i) = \varphi\circ\kappa_2(Y_i)$ ist. Definiere Φ durch $Y_i \longmapsto f_i$. Dann wird obiges Diagramm kommutativ und deshalb $\Phi(I(W)) = \Phi(\mathrm{Ker}\,\kappa_2) \subset \mathrm{Ker}\,\kappa_1 = I(V)$. Wenn also $\mathfrak{m}_p$ ein maximales Ideal von $k[X_1,\ldots,X_n]$ mit $p \in V$, d.h. $\mathfrak{m}_p \supset I(V)$, ist, gilt $\Phi^{-1}(\mathfrak{m}_p) \supset \Phi^{-1}(I(V)) \supset I(W)$. Es ist aber $\Phi = F^*$, wo $F\colon k^n \longrightarrow k^m$ durch $f_1,\ldots,f_m$ gegeben ist. Also ist $\Phi^{-1}(\mathfrak{m}_p)$ nach 9.34 das maximale Ideal $\mathfrak{m}_{F(p)}$ von $k[Y_1,\ldots,Y_m]$. Aus $\mathfrak{m}_{F(p)} \supset I(W)$ folgt $F(p) \in W$. Der Morphismus $F\colon k^n \longrightarrow k^m$ induziert also durch Einschränkung einen Morphismus $\alpha\colon V \longrightarrow W$ mit $\alpha^* = \varphi$. —

<u>Definition 9.37</u> Ein Morphismus $\varphi\colon V \longrightarrow W$ algebraischer Mengen heißt endlich, wenn $k[V]$ vermöge des Strukturhomomorphismus $\varphi^*\colon k[W] \longrightarrow k[V]$ eine endliche $k[W]$-Algebra ist.

<u>Satz 9.38</u> *Die Fasern eines endlichen Morphismus* $\varphi\colon V \longrightarrow W$ *sind endlich. (D.h.* $\varphi^{-1}(p)$ *ist eine endliche Menge für jedes* $p \in W$*.)*

<u>Beweis:</u> Wenn man Punkte von W bzw. V mit maximalen Idealen von $k[W]$

bzw. $k[V]$ identifiziert und 9.34 beachtet, hat man folgendes zu zeigen: Zu jedem maximalen Ideal $\mathfrak{n}$ von $k[W]$ gibt es nur endlich viele maximale Ideale $\mathfrak{m}$ von $k[V]$ mit $(\varphi^*)^{-1}(\mathfrak{m}) = \mathfrak{n}$. Es gilt aber sogar das

Lemma 9.39 *Sei $A \subset B$ eine endliche Ringerweiterung. Über jedem Primideal $\mathfrak{p}$ von A liegen nur endlich viele Primideale von B.*

Beweis hierfür: Sei $\mathfrak{h}$ der Durchschnitt aller Primideale von B, die über $\mathfrak{p}$ liegen. Setze $A' := A/\mathfrak{p}$ und $B' = B/\mathfrak{h}$. Man kann dann A' als Unterring von B' auffassen, und die Primideale von B, die über $\mathfrak{p}$ liegen, entsprechen den Primidealen von B', die über (0) in A' liegen, d.h. den Primidealen von B', die mit $S = A' - (0)$ leeren Durchschnitt haben, d.h. den Primidealen von $S^{-1}B'$. Da B endlich über A ist, ist $S^{-1}B'$ endlich über $S^{-1}A'$, d.h. ein endlich dimensionaler $S^{-1}A'$-Vektorraum. $S^{-1}B'$ ist deshalb als $S^{-1}A'$-Modul von endlicher Länge, also erst recht als $S^{-1}B'$-Modul. Nach Satz 4.51 ist jedes Primideal von $S^{-1}B'$ maximal, also auch ein minimales Primideal. Deshalb folgt aus 4.17, daß $S^{-1}B'$ nur endlich viele Primideale hat. –

Die Bildung des ganzen Abschlusses einer integren k-Algebra endlichen Typs liefert einen endlichen Morphismus. Dies liegt an folgendem

Satz 9.40 *Sei k ein nicht notwendig algebraisch abgeschlossener Körper, A eine integre k-Algebra endlichen Typs, $L \supset Q(A)$ eine endliche Körpererweiterung. Dann ist der ganze Abschluß von A in L endlich über A.*

Beweis: Sei B dieser ganze Abschluß. Nach 9.2 gibt es algebraisch unabhängige $x_1,\dots,x_n$ in A, derart daß A endlich über $k[x_1,\dots,x_n]$ ist. B ist dann auch der ganze Abschluß von $k[x_1,\dots,x_n]$ in L, und L ist endlich über $k(x_1,\dots,x_n)$. Wir dürfen also $A = k[x_1,\dots,x_n]$ annehmen. Wenn L' die normale Hülle von L über $Q(A)$ ist und der ganze Abschluß B' von A in L' endlich über A ist, so gilt dies auch für B. Wir dürfen also annehmen, daß L über $Q(A)$ normal ist. Nach [Lang] VII §7 Proposition 12 gibt es dann einen Körper E zwischen $Q(A)$ und L, derart daß L über E separabel und E über $Q(A)$ radiziell (d.h. rein inseparabel) ist. Wir sind fertig, wenn wir wissen, daß der ganze Abschluß C von A in E endlich über A ist. Denn dann ist C noethersch und ganz abgeschlossen, $Q(C) = E$ und $L \supset E$ eine endliche, separable Körpererweiterung, so daß man Satz 7.26 anwenden kann.

Es genügt also, den Satz in folgendem Fall zu beweisen: Es ist $A = k[X_1,\dots,X_n]$ (der Polynomring) $\operatorname{char} k = p > 0$ und L radiziell über $Q(A)$. Dazu konstruieren wir eine $Q(A)$-lineare Abbildung $S\colon L \longrightarrow Q(A)$ mit $\{0\} \neq S(B) \subset A$. Dann kann man nämlich den Beweis von 7.26 wörtlich übertragen. Da L über $Q(A)$ radiziell und endlich ist, gibt es eine Potenz q von p mit $L \subset Q(A)^{1/q}$. Dann ist $k^{1/q}[X_1^{1/q},\dots,X_n^{1/q}]$ ganz abgeschlossen (7.9) und ganz über A, also der ganze Abschluß von A in $Q(A)^{1/q}$. Demnach ist $B = L \cap k^{1/q}[X_1^{1/q},\dots,X_n^{1/q}]$. Nun ist $k[X_1^{1/q},\dots,X_n^{1/q}]$ ein freier A-Modul. Eine Basis besteht aus den Elementen $(X_1^{1/q})^{\alpha_1} \cdot \ldots \cdot (X_n^{1/q})^{\alpha_n}$ mit $0 \le \alpha_i < q$.
Und $k^{1/q}[X_1^{1/q},\dots,X_n^{1/q}]$ ist frei (aber nicht notwendig endlich) über $k[X_1^{1/q},\dots,X_n^{1/q}]$. Eine Basis wird durch eine Basis der Körpererweiterung $k \subset k^{1/q}$ gegeben. Insgesamt ist $k^{1/q}[X_1^{1/q},\dots,X_n^{1/q}]$ ein freier A-Modul. Deshalb gibt es zu einem (beliebig gewählten) Element $b_0 \in B - (0)$ $\subset k^{1/q}[X_1^{1/q},\dots,X_n^{1/q}] - (0)$ eine A-lineare Abbildung:
$s\colon k^{1/q}[X_1^{1/q},\dots,X_n^{1/q}] \longrightarrow A$ mit $s(b_0) \neq 0$. Da $L = \left\{\frac{b}{a} \mid b \in B,\ a \in A - (0)\right\}$ ist, wird durch $S(\frac{b}{a}) := \frac{s(b)}{a}$ eine Abbildung $S\colon L \longrightarrow Q(A)$ der gesuchten Art definiert. — (Vgl. Lemma 18.71.)

Sei V eine irreduzible algebraische Menge über einem algebraisch abgeschlossenen Körper k. Dann ist $k[V]$ eine integre k-Algebra endlichen Typs. Nach obigem Satz ist ihr ganzer Abschluß $\overline{k[V]}$ endlich über $k[V]$, also wieder eine k-Algebra endlichen Typs. Demnach gibt es eine algebraische Menge $\overline{V}$ mit $k[\overline{V}] = \overline{k[V]}$. Und der Einbettung $k[V] \subset \overline{k[V]}$ entspricht ein endlicher Morphismus $\overline{V} \longrightarrow V$.

Aufgaben und Hinweise

1) Eine Verschärfung des Noetherschen Normalisierungslemmas findet sich in [Serre] II-20,Thm. 2 und in [Bourbaki] Chap. V, §3, Thm. 1.

2) Sei $A \subset B$ eine Erweiterung endlichen Typs von Integritätsringen. Zeige (mittels 9.2): Es gibt ein $s \in A - (0)$ und über A algebraisch unabhängige Elemente $x_1,\dots,x_n \in B$, derart daß B_s ganz über $A_s[x_1,\dots,x_n]$ ist. (Die algebraische Unabhängigkeit der $x_1,\dots,x_n$ soll bedeuten, daß der Einsetzungshomomorphismus $A[X_1,\dots,X_n] \longrightarrow A[x_1,\dots,x_n]$, $X_i \longmapsto x_i$, ein Isomorphismus ist. $A_s = S^{-1}A$ mit $S = \{1,s,s^2,\dots\}$.)

3) Sei $A \subset K$ eine Ringerweiterung von endlichem Typ und K ein Körper (also A integer). Zeige:
a) Es gibt ein $s \in A - (0)$ mit $Q(A) = A_s$;
b) $[K:Q(A)] < \infty$;
c) (0) in A ist nicht Durchschnitt aller übrigen Primideale von A.
(Verwende A2 und 7.18 für a) und b) und 2.14 für c).)

4) Sei A ein noetherscher Integritätsring. Zeige: Genau dann gibt es ein $x \in Q(A)$ mit $Q(A) = A[x]$, wenn A semilokal und $\dim A \leq 1$ ist.

5) Eine Verallgemeinerung von Satz 9.4. Ein Ring heißt jacobsonsch (oder hilbertsch), wenn in ihm jedes Primideal (also auch jedes Ideal $\mathfrak{a}$ mit $\mathfrak{a} = \sqrt{\mathfrak{a}}$) Durchschnitt maximaler Ideale ist. Gemäß 9.4 ist jede Algebra endlichen Typs über einem Körper jacobsonsch.
Sei A ein jacobsonscher Ring und B eine A-Algebra endlichen Typs. Zeige:
a) B ist jacobsonsch.
b) Wenn $\varphi: A \longrightarrow B$ den Strukturhomomorphismus bezeichnet, so gilt für jedes maximale Ideal $\mathfrak{n}$ von B, daß $\mathfrak{m} = \varphi^{-1}(\mathfrak{n})$ maximal in A und die induzierte Körpererweiterung $A/\mathfrak{m} \longrightarrow B/\mathfrak{n}$ endlich ist.
(Beweise zunächst b) mit Hilfe von A3. Sei dann $\mathfrak{p} \in \operatorname{Spec} B$, $s \in B-\mathfrak{p}$ und $\mathfrak{q} \supset \mathfrak{p}$ ein Primideal von B, so daß $\mathfrak{q}_s$ ein maximales Ideal von B_s ist. Beachte $(B/\mathfrak{p})_s \neq 0$. Da B_s von endlichem Typ über A ist, ist $\varphi^{-1}(\mathfrak{q})$ maximal in A, und deshalb $B/\mathfrak{q}$ jacobsonsch gemäß 9.4. Somit ist $\mathfrak{q}$ Durchschnitt maximaler Ideale und $s \notin \mathfrak{q}$. Kein $s \in B-\mathfrak{p}$ liegt in allen maximalen Idealen, die $\mathfrak{p}$ umfassen.)

6) Mit "going down" (7.A6) und dem noetherschen Normalisierungslemma kann man zeigen, daß alle maximalen Primidealketten in integren k-Algebren endlichen Typs von gleicher Länge sind. Vgl. [Lorenz], §19, Satz 6. Siehe auch §17 in diesem Buch.

7) Sei im folgenden k algebraisch abgeschlossen, V eine affine k-Varietät, $p \in V$ und $\mathfrak{m}$ das zu p gehörige maximale Ideal von $k[V]$. Man nennt $k[V]_{\mathfrak{m}}$ den lokalen Ring von V in p.
Sei $f \in k[X,Y]$ ein quadratfreies (s. 7.A2) Polynom, $C := V(f)$ die durch f definierte (ebene) Kurve und $p \in C$. Zeige: Der lokale Ring von C in p ist genau dann ein DBR, wenn $\frac{\partial f}{\partial X}(p) \neq 0$ oder $\frac{\partial f}{\partial Y}(p) \neq 0$ ist. (Vgl. den Satz über implizite Funktionen.) (Hinweis:

Man kann annehmen, daß $p = (0,0) \in k^2$ ist, da Translationen Automorphismen des k^2 (natürlich auch allgemein des k^n) sind. In diesem Falle ist f von der Form $aX + bY +$ Glieder höheren Grades.)

8) Sei $f \in k[X]$ ein beliebiges Polynom. Zeige: $V(Y-f(X))$ ist isomorph zu k^1.

9) Sei $V(X^2-Y^3) \subset k^2$ die Neilsche Parabel. Zeige: Die Abbildung $k^1 \longrightarrow V(X^2-Y^3)$, $t \longmapsto (t^3,t^2)$ ist ein bijektiver Morphismus, aber kein Isomorphismus.

10) Satz 9.38 läßt sich nicht ohne weiteres umkehren. Beispiel: $V := V(XY-1) \subset k^2$; $V \longrightarrow k^1$, $(x,y) \longmapsto x$. Die "richtige Umkehrung" von 9.38 ist "Zariski's Main Theorem". Siehe [Iversen], IV. 2.

11) Sei k ein algebraisch abgeschlossener Körper. Aus der Feststellung 9.17 folgt: Wenn man die algebraischen Teilmengen einer algebraischen Menge V als die abgeschlossenen Mengen in V definiert, wird V zu einem topologischen Raum. Die so definierte Topologie heißt Zariski-Topologie. Überlege:

a) Die abgeschlossenen Teilmengen einer irreduziblen Kurve C (etwa des k^1) sind, bis auf C selbst, genau die endlichen Teilmengen von C. Vgl. 9.26.

b) Für $n > 1$ ist die Zariski-Topologie auf k^n echt feiner als die Produkttopologie der Zariski-Topologien auf k^{n-1} und k^1.

c) Bei der Identifizierung von V mit $\operatorname{Spmax} k[V]$ ist die Zariski-Topologie auf $\operatorname{Spmax} k[V]$ die Einschränkung der Zariski-Topologie auf $\operatorname{Spec} k[V]$, die in 1.A4 definiert wurde.

d) Die "übliche" Topologie auf $\mathbb{C}^n$ ist echt feiner als die Zariski-Topologie (für $n > 0$).

e) Die Dimension von V hängt nur von der Zariski-Topologie auf V ab.

Durch Betrachtung der Zariski-Topologie auf $\operatorname{Spec} A$ kann man Sätze der kommutativen Algebra mit Mitteln der allgemeinen Topologie beweisen; z.B. 4.17. Vgl. [Bourbaki], Chap. II, §4 und [Kunz], Kap. VI, 4.2 und die dort angegebene Literatur.

12) Die Theorie der affinen Varietäten, von der ein Anfang in unserem Buch gemacht wurde, ist wegen 9.33 und 9.36 im wesentlichen äquivalent zur Theorie der reduzierten Algebren endlichen Typs über einem

Körper, einem Teilgebiet der kommutativen Algebra. Man darf allerdings nicht übersehen, daß die geometrische "Anschauung", was die Motivation und Heuristik von Begriffen, Sätzen und Beweisen betrifft, dem rein algebraischen Denken eine zusätzliche Komponente hinzufügt. Darüber hinaus erweist es sich als unumgänglich, neben den affinen auch sogenannte projektive Varietäten, das sind algebraisch definierte (irreduzible) Teilmengen projektiver Räume, zu betrachten. (Dies hat man schon lange vor der "Erfindung" der kommutativen Algebra getan.) Die projektiven Varietäten bilden keine Kategorie, die zu einer Kategorie von gewissen Ringen oder Algebren äquivalent wäre.
So gesehen sind kommutative Algebra und die klassische algebraische Geometrie zwei verschiedene Gebiete mit einem beachtlichen "Durchschnitt". Eine Theorie, die beide umfaßt, ist die Theorie der Schemata. Diese wird heute als "die" moderne algebraische Geometrie angesehen. Sie wurde konzipiert in der Hoffnung, mit ihrer Hilfe außer geometrischen auch tiefe zahlentheoretische Sätze beweisen zu können - eine Hoffnung, die nicht getrogen hat: In der Tat, mit ihrer Hilfe wurden Beweise der Weilschen und der Mordellschen Vermutung ([Deligne], [Faltings]) erbracht. Eine schöne Einführung in die algebraische Geometrie ist [Hartshorne]. In [Kunz] findet sich - auf elementarem Niveau - mancherlei zum Zusammenspiel von geometrischen und algebraischen Fragen und Methoden.

§10 HOM, $\otimes$; INJEKTIVE, PROJEKTIVE UND FLACHE MODULN

1. Kategorien und Funktoren

Definition 10.1 Folgende Gegebenheiten machen eine Kategorie $\mathcal{C}$ aus:

1. eine Klasse (s. nachfolgende Bemerkung a)) von "Objekten", die mit $\mathrm{Ob}\mathcal{C}$ (oder einfach mit $\mathcal{C}$) bezeichnet wird;
2. zu jedem Paar $(A,B) \in (\mathrm{Ob}\mathcal{C})^2$ eine Menge von "Morphismen" $\mathrm{Mor}_{\mathcal{C}}(A,B)$ (auch mit $\mathrm{Hom}_{\mathcal{C}}(A,B)$ oder $\mathcal{C}(A,B)$ bezeichnet), wobei $\mathrm{Mor}_{\mathcal{C}}(A,B)$ und $\mathrm{Mor}_{\mathcal{C}}(A',B')$ disjunkt sind, wenn $A \neq A'$ oder $B \neq B'$ gilt;
3. zu jedem $A \in \mathrm{Ob}\mathcal{C}$ ein ausgezeichnetes Element $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A,A)$;
4. zu jedem Tripel $(A,A',A'') \in (\mathrm{Ob}\mathcal{C})^3$ eine Verknüpfung
$\mathrm{Mor}_{\mathcal{C}}(A,A') \times \mathrm{Mor}_{\mathcal{C}}(A',A'') \longrightarrow \mathrm{Mor}_{\mathcal{C}}(A,A'')$, $(\alpha,\beta) \longmapsto \beta \circ \alpha$.
Diese Verknüpfung unterliegt folgenden Regeln:
K1) $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$, wenn immer eine der beiden Seiten - und damit auch die andere - definiert ist;
K2) $\alpha \circ \mathrm{id}_A = \alpha$ und $\mathrm{id}_B \circ \alpha = \alpha$ für $\alpha \in \mathrm{Mor}_{\mathcal{C}}(A,B)$.

Bemerkungen: a) Man verwendet ein anderes Wort als "Menge", um widerspruchsträchtige Begriffe wie "Menge aller Mengen", "Menge aller Ringe" o.ä. zu vermeiden.
b) Man schreibt auch $\alpha: A \longrightarrow B$ für $\alpha \in \mathrm{Mor}_{\mathcal{C}}(A,B)$.

Beispiele 10.2 a) Mengen und Abbildungen,
b) Ringe und Homomorphismen,
c) A-Moduln und A-lineare Abbildungen, Bezeichnung dieser Kategorie: A-Mod ,
d) topologische Räume und stetige Abbildungen,
e) k-Varietäten und Morphismen.

Bemerkung: Man betrachtet in der Mathematik auch kompliziertere Kategorien, in denen die Objekte nicht einfach Mengen mit gewissen Zusatzstrukturen und die Morphismen gewisse Abbildungen dieser Mengen sind.

Definition 10.3 Ein Isomorphismus in einer Kategorie $\mathcal{C}$ ist ein Morphismus $\alpha \in \mathrm{Mor}_{\mathcal{C}}(A,B)$, zu dem es ein $\beta \in \mathrm{Mor}_{\mathcal{C}}(B,A)$ mit $\beta \circ \alpha = \mathrm{id}_A$ und $\alpha \circ \beta = \mathrm{id}_B$ gibt.

<u>Definition 10.4</u> Seien $\mathcal{C},\mathcal{C}'$ Kategorien. Ein kovarianter (bzw. kontravarianter) Funktor $t\colon \mathcal{C} \longrightarrow \mathcal{C}'$ besteht aus

1. einer Abbildung $\mathrm{Ob}\mathcal{C} \longrightarrow \mathrm{Ob}\mathcal{C}'$, $A \longmapsto tA$;
2. für jedes Paar $(A,B) \in (\mathrm{Ob}\mathcal{C})^2$ einer Abbildung
   $\mathrm{Mor}_{\mathcal{C}}(A,B) \xrightarrow{t} \mathrm{Mor}_{\mathcal{C}'}(tA,tB)$ (bzw. $\mathrm{Mor}_{\mathcal{C}}(A,B) \longrightarrow \mathrm{Mor}_{\mathcal{C}'}(tB,tA)$) ,

so daß gilt:

$$t(\mathrm{id}_A) = \mathrm{id}_{tA}\,, \quad t(\alpha \circ \beta) = (t\alpha) \circ (t\beta)$$

$$(\text{bzw. } t(\alpha \circ \beta) = (t\beta) \circ (t\alpha)\ ,$$

wenn immer $\alpha \circ \beta$ definiert ist.

<u>Bemerkungen 10.5</u> a) Ein Funktor bildet Isomorphismen auf Isomorphismen ab.

b) Ein Funktor führt kommutative Diagramme in solche über.

<u>Beispiele 10.6</u> a) $A\text{-Mod} \longrightarrow S^{-1}A\text{-Mod}$, $M \longrightarrow S^{-1}M$, $\alpha \longmapsto S^{-1}\alpha$.

b) $\{\text{Ringe}\} \longrightarrow \{\text{Mengen}\}$ (bzw. $\longrightarrow \{\text{topologische Räume}\}$),
$A \longmapsto \mathrm{Spec}\, A$, $(f\colon A \longrightarrow B) \longmapsto (\mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A,\ \mathfrak{p} \longmapsto f^{-1}(\mathfrak{p}))$.
Vgl. 1.24 und 1.A4.

<u>Definition 10.7</u> Seien $\mathcal{C},\mathcal{C}'$ Kategorien, für welche die $\mathrm{Mor}_{\mathcal{C}}(A,B)$ und $\mathrm{Mor}_{\mathcal{C}'}(A',B')$ mit der Struktur von abelschen Gruppen (bzw. R-Moduln) versehen sind. Ein Funktor $t\colon \mathcal{C} \longrightarrow \mathcal{C}'$ heißt additiv (bzw. R-linear), wenn die Abbildungen $\mathrm{Mor}_{\mathcal{C}}(A,B) \xrightarrow{t} \mathrm{Mor}_{\mathcal{C}'}(tA,tB)$ ($\mathrm{Mor}_{\mathcal{C}}(A,B) \xrightarrow{t} \mathrm{Mor}_{\mathcal{C}'}(tB,tA)$ im kontravarianten Fall) Gruppenhomomorphismen (bzw. R-linear) sind.

<u>Definition 10.8</u> Seien $t_1,t_2\colon \mathcal{C} \longrightarrow \mathcal{C}'$ Funktoren (beide kovariant oder beide kontravariant). Eine natürliche Transformation von t_1 nach t_2, geschrieben $\varphi\colon t_1 \longrightarrow t_2$, ist eine Familie $(\varphi_A)_{A \in \mathrm{Ob}\mathcal{C}}$ von Morphismen $\varphi_A \in \mathrm{Mor}_{\mathcal{C}'}(t_1A,t_2A)$, so daß für alle $A,B \in \mathrm{Ob}\mathcal{C}$ und jedes $\alpha \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ folgendes Diagramm kommutativ ist:

$$\begin{tikzcd}
t_1A \arrow[r, "\varphi_A"] \arrow[d, "t_1\alpha"'] & t_2A \arrow[d, "t_2\alpha"'] \\
t_1B \arrow[r, "\varphi_B"] \arrow[u, dashed, bend right] & t_2B \arrow[u, dashed, bend right]
\end{tikzcd}$$

(Die gestrichelten Pfeile gelten im kontravarianten Fall.) Man sagt auch: "Ein" Morphismus $\varphi_A\colon t_1A \longrightarrow t_2A$ ist natürlich (in A), wenn die Familie

$(\varphi_A)_{A \in \mathrm{Ob}C}$ eine natürliche Transformation $\varphi\colon t_1 \longrightarrow t_2$ ist.

Für einen Funktor t ist die Familie $(\mathrm{id}_{tA})_{A \in \mathrm{Ob}}$ eine natürliche Transformation $t \longrightarrow t$, die mit id_t bezeichnet wird.

Beachte, daß für natürliche Transformationen $\varphi\colon t_1 \longrightarrow t_2$, $\psi\colon t_2 \longrightarrow t_3$ auf naheliegende Weise eine natürliche Transformation $\psi \circ \varphi\colon t_1 \longrightarrow t_3$ zu definieren ist.

Ein natürlicher Isomorphismus ist eine natürliche Transformation $\varphi\colon t_1 \longrightarrow t_2$, zu der es eine natürliche Transformation $\psi\colon t_2 \longrightarrow t_1$ gibt, so daß $\varphi \circ \psi = \mathrm{id}_{t_2}$ und $\psi \circ \varphi = \mathrm{id}_{t_1}$ ist.

N.B.: Eine natürliche Transformation $\varphi\colon t_1 \longrightarrow t_2$ ist genau dann ein natürlicher Isomorphismus, wenn $\varphi_A\colon t_1A \longrightarrow t_2A$ für jedes A ein Isomorphismus ist.

Beispiele 10.9 a) Seien A ein Ring und $S \subset A$ multiplikativ. Für jeden A-Modul M fasse $S^{-1}M$ wieder als A-Modul auf. Die Abbildung $i_{M,S}\colon M \longrightarrow S^{-1}M$ ist natürlich; d.h. die Familie $(i_{M,S})_{M \in A\text{-Mod}}$ bildet eine natürliche Transformation $\mathrm{id}_{A\text{-Mod}} \longrightarrow S^{-1}$, wobei $\mathrm{id}_{A\text{-Mod}}$ der "identische" Funktor und S^{-1} als Funktor $A\text{-Mod} \longrightarrow A\text{-Mod}$ aufgefaßt wird. (Vgl. 3.34.)
b) Sei k ein Körper, k-Mod also die Kategorie der k-Vektorräume. Die kanonische Abbildung $V \longrightarrow V^{**}$ (Bidual) ist natürlich. Auf der Kategorie der endlich-dimensionalen Vektorräume hat man einen natürlichen Isomorphismus.
c) Sei k ein Körper und A eine k-Algebra von endlichem Typ. Die Einbettung $\mathrm{Spmax}\, A \hookrightarrow \mathrm{Spec}\, A$ ist natürlich, d.h. man hat eine natürliche Transformation der beiden kontravarianten Funktoren
$\mathrm{Spmax}, \mathrm{Spec}\colon \{k\text{-Algebren}\} \longrightarrow \{\text{Mengen}\}$.

N.B.: Ein kanonischer Morphismus ist häufig natürlich - wobei "kanonisch" ein vager, "natürlich" hingegen ein definierter Begriff ist.

Definition 10.10 Zwei Kategorien C, C' heißen äquivalent, wenn es Funktoren $t\colon C \longrightarrow C'$ und $t'\colon C' \longrightarrow C$ gibt, so daß $t' \circ t$ natürlich isomorph zu id_C und $t \circ t'$ natürlich isomorph zu $\mathrm{id}_{C'}$ ist.

2. Der Funktor Hom

Im folgenden sei A *ein Ring,* M,N *seien* A-*Moduln.*

Definition 10.11 $\mathrm{Hom}_A(M,N)$ bezeichne die Menge der A-Modulhomomorphismen von M nach N (d.h. $\mathrm{Mor}_{A\text{-Mod}}(M,N)$), versehen mit der elementweisen Addition als innerer Verknüpfung.

Bemerkungen 10.12 a) $\mathrm{Hom}_A(M,N)$ ist ein A-Modul. (Vgl. die Bemerkung im Anschluß an Def. 3.3. Für nicht-kommutatives A ist $\mathrm{Hom}_A(M,N)$ eine abelsche Gruppe.)

b) Man hat einen natürlichen Isomorphismus $\mathrm{Hom}_A(A,N) \simeq N$, gegeben durch $f \longmapsto f(1)$.

c) Für $n,m \in \mathbb{N}$ gilt: $\mathrm{Hom}_A(A^n,A^m) \simeq A^{nm}$. (Den Homomorphismen entsprechen Matrizen auf bijektive Weise.)

Definition 10.13 Ein A-Modulhomomorphismus $N \xrightarrow{\alpha} N'$ induziert einen A-Modulhomomorphismus

$$\begin{aligned} \mathrm{Hom}_A(M,N) &\xrightarrow{\mathrm{Hom}(M,\alpha)} \mathrm{Hom}_A(M,N') \\ f &\longmapsto \alpha \circ f \end{aligned} .$$

Man bezeichnet $\mathrm{Hom}(M,\alpha)$ auch mit α_*.

Feststellungen 10.14 *a)* $\mathrm{Hom}(M,\mathrm{id}_N) = \mathrm{id}_{\mathrm{Hom}(M,N)}$.

b) Für eine Folge $N_1 \xrightarrow{\beta} N_2 \xrightarrow{\alpha} N_3$ *von* A-*linearen Abbildungen gilt* $\mathrm{Hom}_A(M,\alpha\circ\beta) = \mathrm{Hom}_A(M,\alpha) \circ \mathrm{Hom}_A(M,\beta)$.

c) Somit ist $\mathrm{Hom}_A(M,-)$ *ein (kovarianter) Funktor von der Kategorie der* A-*Moduln in die Kategorie der* A-*Moduln (bzw. abelschen Gruppen bei nicht-kommutativem* A).

d) $\mathrm{Hom}_A(M,-)$ *ist* A-*linear (bei nichtkommutativem* A *noch additiv).*

Definition 10.15 Ein A-Modulhomomorphismus $\alpha\colon M \longrightarrow M'$ induziert einen Homomorphismus

$$\begin{aligned} \mathrm{Hom}_A(M',N) &\xrightarrow{\mathrm{Hom}(\alpha,N)} \mathrm{Hom}(M,N) \\ f &\longmapsto f\circ\alpha \end{aligned} .$$

Man bezeichnet $\mathrm{Hom}(\alpha,N)$ auch mit α^*.

Feststellungen 10.16 *a)* $\mathrm{Hom}(\mathrm{id}_M,N) = \mathrm{id}_{\mathrm{Hom}(M,N)}$.

b) $\mathrm{Hom}(\alpha\circ\beta,N) = \mathrm{Hom}(\beta,N) \circ \mathrm{Hom}(\alpha,N)$.

c) *Somit ist* Hom(–,N) *ein kontravarianter Funktor von der Kategorie der* A-*Moduln in die Kategorie der* A-*Moduln (bzw. abelschen Gruppen bei nichtkommutativem* A).

d) Hom(–,N) *ist* A-*linear (bzw. additiv bei nichtkommutativem* A).

<u>Satz 10.17</u> (*Linksexaktheit von* Hom)

a) *Sei* $0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N''$ *exakt, dann ist*

$$0 \longrightarrow \mathrm{Hom}(M,N') \xrightarrow{\alpha_*} \mathrm{Hom}(M,N) \xrightarrow{\beta_*} \mathrm{Hom}(M,N'')$$

exakt.

b) *Sei* $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *exakt, dann ist*

$$0 \longrightarrow \mathrm{Hom}(M'',N) \xrightarrow{\beta^*} \mathrm{Hom}(M,N) \xrightarrow{\alpha^*} \mathrm{Hom}(M',N)$$

exakt.

<u>Beweis:</u> a) Die Injektivität von α_* ist trivial.
Zur Exaktheit bei Hom(M,N):
Sei zunächst $\beta\circ\alpha = 0$. Dann ist $\beta_* \circ \alpha_* \overset{10.14b)}{=} (\beta\circ\alpha)_* \overset{10.14d)}{=} 0_* = 0$, also $\mathrm{Im}\,\alpha_* \subset \mathrm{Ker}\,\beta_*$.
Es bleibt zu zeigen: $\mathrm{Ker}\,\beta_* \subset \mathrm{Im}\,\alpha_*$.
Sei $f \in \ker\beta_*$, d.h. $f\colon M \longrightarrow N$ und $\beta\circ f = 0$. Somit ist $f(M) \subset \mathrm{Ker}\,\beta = \mathrm{Im}\,\alpha \simeq N'$. Folglich gibt es ein A-lineares $f'\colon M \longrightarrow N'$ mit $\alpha\circ f' = f$, d.h. $\alpha_*(f') = f$.

b) Injektivität von β^*:
Für $f\colon M'' \longrightarrow N$ gelte $f\circ\beta = \beta^*(f) = 0$. Dann ist $f(M'') = f(\beta(M)) = 0$ (β surjektiv), d.h. $f = 0$.
Exaktheit bei Hom(M,N): Aus $\beta\circ\alpha = 0$ folgt $\alpha^*\circ\beta^* = (\beta\circ\alpha)^* = 0^* = 0$, also $\mathrm{Im}\,\beta^* \subset \mathrm{Ker}\,\alpha^*$.
Es bleibt "$\mathrm{Ker}\,\alpha^* \subset \mathrm{Im}\,\beta^*$" zu zeigen: Sei $f\colon M \longrightarrow N$ mit $0 = \alpha^*(f) = f\circ\alpha$.

$$\begin{tikzcd} M' \arrow[r, "\alpha"] & M \arrow[r, "\beta"] \arrow[d, "f"] & M'' \arrow[r] & 0 \\ & N & & \end{tikzcd}.$$

Aus $f\circ\alpha = 0$ folgt $0 = f(\mathrm{Im}\,\alpha) = f(\ker\beta)$.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\beta"'] & N \\ M'' \simeq M/\ker\beta \arrow[ur, dashed, "f''"'] & \end{tikzcd}$$

Der Homomorphiesatz liefert die Existenz eines Homomorphismus $f''\colon M'' \longrightarrow N$ mit $\beta^*(f'') = f''\circ\beta = f$. —

Bemerkungen 10.18 a) Für eine exakte Sequenz von A-Modulhomomorphismen $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ gilt i.a. nicht, daß $0 \longrightarrow \mathrm{Hom}(M'',N) \xrightarrow{\beta^*} \mathrm{Hom}(M,N) \xrightarrow{\alpha^*} \mathrm{Hom}(M',N) \longrightarrow 0$ exakt ist.
D.h. nicht, jeder Homomorphismus $M' \longrightarrow N$ läßt sich zu einem Homomorphismus $M \longrightarrow N$ fortsetzen.

Beispiel: $A = \mathbb{Z}$, $h_2(n) := 2n$,

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "h_2"] \arrow[d, "id_{\mathbb{Z}}"'] & \mathbb{Z} \arrow[r] \arrow[dl, "\varphi"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\ & \mathbb{Z} & & & \end{tikzcd}$$

Für jeden Homomorphismus $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}$ gilt: Mit $x \in \mathbb{Z}$ ist $\varphi(h_2(x)) = \varphi(2x) = 2\varphi(x) \in 2\mathbb{Z}$, also $\varphi \circ h_2 \neq id_{\mathbb{Z}}$.

b) Für eine exakte Sequenz von A-Modulhomomorphismen $0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$ gilt i.a. nicht, daß $0 \longrightarrow \mathrm{Hom}(M,N') \xrightarrow{\alpha^*} \mathrm{Hom}(M,N) \xrightarrow{\beta^*} \mathrm{Hom}(M,N'') \longrightarrow 0$ exakt ist.
D.h. nicht jeder Homomorphismus $M \longrightarrow N''$ faktorisiert über N.

Beispiel: $A = \mathbb{Z}$.

$$\begin{tikzcd} & & & \mathbb{Z}/2\mathbb{Z} \arrow[dl, "\varphi"'] \arrow[d, "id_{\mathbb{Z}/2\mathbb{Z}}"] & \\ 0 \arrow[r] & \mathbb{Z} \arrow[r, "h_2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$.

Für jeden Homomorphismus $\varphi: \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}$ gilt: $0 = \varphi(0) = \varphi(z \cdot \overline{2}) = 2\varphi(\overline{1})$, also auch $\varphi(\overline{1}) = 0$, d.h. $\varphi = 0$. –

Allgemeiner machen wir folgende 2 Feststellungen:

Feststellung 10.19 *Es sei* $N \xrightarrow{\beta} N''$ *ein Homomorphismus, so daß* $\mathrm{Hom}(N'',N) \xrightarrow{\beta_*} \mathrm{Hom}(N'',N'') \longrightarrow 0$ *exakt ist. Dann existiert ein* $f: N'' \longrightarrow N$ *mit* $\beta \circ f = id_{N''}$, *d.h.* N'' *ist nach 3.17 ein direkter Summand von* N.

Beweis: Da $id_{N''} \in \mathrm{Im}\, \beta_*$ ist, gibt es $f: N'' \longrightarrow N$ mit $\beta \circ f = \beta_*(f) = id_{N''}$. –

Feststellung 10.19' *Es sei* $M' \xrightarrow{\alpha} M$ *ein Homomorphismus, so daß* $\mathrm{Hom}(M,M') \xrightarrow{\alpha^*} \mathrm{Hom}(M',M') \longrightarrow 0$ *exakt ist. Dann existiert ein* $g: M \longrightarrow M'$, *so daß* $g \circ \alpha = id_{M'}$ *gilt, d.h.* M' *direkter Summand von* M *ist.*

Analoger Beweis. –

Definition 10.20 a) Ein A-Modul P heißt projektiv, falls für jede exakte Sequenz $N \xrightarrow{\beta} N'' \longrightarrow 0$ gilt: $\mathrm{Hom}(P,N) \xrightarrow{\beta_*} \mathrm{Hom}(P,N'') \longrightarrow 0$ ist exakt.

b) Ein A-Modul I heißt injektiv, falls für jede exakte Sequenz $0 \longrightarrow M' \xrightarrow{\alpha} M$ gilt: $\mathrm{Hom}(M,I) \xrightarrow{\alpha^*} \mathrm{Hom}(M',I) \longrightarrow 0$ ist exakt.

Definition 10.21 a) Für eine Familie $(M_i)_{i\in I}$ von Moduln definiert man das direkte Produkt $\prod_{i\in I} M_i$ als $\{(m_i)_{i\in I} \mid m_i \in M_i\}$ - ohne die Endlichkeitsbedingung der direkten Summe - mit naheliegender Modulstruktur.

Beachte: $\bigoplus_{i\in I} M_i$ ist ein Untermodul von $\prod_{i\in I} M_i$ - und zwar genau dann ein echter Untermodul, wenn I unendlich ist.

Schreibe: $M^I = \prod_{i\in I} M$. (Vgl. 3.A7.)

b) Wenn $(\alpha_i\colon M_i \longrightarrow N_i)_{i\in I}$ eine Familie von Modulhomomorphismen ist, bekommt man auf kanonische Weise Homomorphismen:

$$\bigoplus_{i\in I} \alpha_i : \bigoplus_{i\in I} M_i \longrightarrow \bigoplus_{i\in I} N_i \quad \text{und}$$

$$\prod_{i\in I} \alpha_i : \prod_{i\in I} M_i \longrightarrow \prod_{i\in I} N_i .$$

Satz 10.22 *a)* $\mathrm{Hom}(\bigoplus_{i\in I} M_i, N) \simeq \prod_{i\in I} \mathrm{Hom}(M_i,N)$.

b) $\mathrm{Hom}(M, \prod_{i\in I} N_i) \simeq \prod_{i\in I} \mathrm{Hom}(M,N_i)$.

c) Wenn M *endlich ist, so ist* $\mathrm{Hom}(M, \bigoplus_{i\in I} N_i) \simeq \bigoplus_{i\in I} \mathrm{Hom}(M,N_i)$.

Diese Isomorphismen sind natürlich, d.h.:

a') Sei $\alpha\colon N \longrightarrow N'$ *ein Homomorphismus von A-Moduln. Dann kommutiert folgendes Diagramm:*

$$\begin{tikzcd}
\mathrm{Hom}(\bigoplus_{i\in I} M_i, N) \arrow[r, "\sim"] \arrow[d, "\alpha_*"] & \prod_{i\in I} \mathrm{Hom}(M_i,N) \arrow[d, "\prod_{i\in I}\mathrm{Hom}(M_i,\alpha)"] \\
\mathrm{Hom}(\bigoplus_{i\in I} M_i, N') \arrow[r, "\sim"] & \prod_{i\in I} \mathrm{Hom}(M_i,N')
\end{tikzcd}$$

b') Sei $\alpha\colon M \longrightarrow M'$ *ein Homomorphismus von A-Moduln. Dann kommutiert folgendes Diagramm:*

$$\begin{array}{ccc}
\mathrm{Hom}(M', \prod\limits_{i\in I} N_i) & \xrightarrow{\sim} & \prod\limits_{i\in I} \mathrm{Hom}(M',N_i) \\
\downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \prod\limits_{i\in I} \mathrm{Hom}(\alpha,N_i)} \\
\mathrm{Hom}(M, \prod\limits_{i\in I} N_i) & \xrightarrow{\sim} & \prod\limits_{i\in I} \mathrm{Hom}(M,N_i)
\end{array} \quad .$$

c') *Sei* $\alpha: M \longrightarrow M'$ *ein Homomorphismus von endlichen* A-*Moduln. Dann kommutiert folgendes Diagramm:*

$$\begin{array}{ccc}
\mathrm{Hom}(M', \bigoplus\limits_{i\in I} N_i) & \xrightarrow{\sim} & \bigoplus\limits_{i\in I} \mathrm{Hom}(M',N_i) \\
\downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \bigoplus\limits_{i\in I} \mathrm{Hom}(\alpha,N_i)} \\
\mathrm{Hom}(M, \bigoplus\limits_{i\in I} N_i) & \xrightarrow{\sim} & \bigoplus\limits_{i\in I} \mathrm{Hom}(M,N_i)
\end{array} \quad .$$

Beweis: Die Aussagen verifiziert man leicht. Man beachte nur, daß für endliches M das Bild eines jeden Homomorphismus $f: M \longrightarrow \bigoplus\limits_{i\in I} N_i$ in einer endlichen "Teilsumme" liegt. —

Folgerung 10.24 *Ein direkter Summand eines freien Moduls ist projektiv.*

Beweis: Für jeden A-Modul N hat man einen natürlichen Isomorphismus $\mathrm{Hom}_A(A,N) \xrightarrow{\sim} N$. Also ist $\mathrm{Hom}_A(A,-)$ ein exakter Funktor, d.h. er führt exakte Folgen in solche über. Dies gilt daher auch für $\mathrm{Hom}_A(A^{(I)},-)$, denn $\mathrm{Hom}(A^{(I)},N) \xrightarrow{\sim} N^{(I)}$. Falls nun $P \oplus Q = A^{(I)}$, dann ist $\mathrm{Hom}(P,N) \oplus \mathrm{Hom}(Q,N) \xrightarrow{\sim} \mathrm{Hom}(A^{(I)},N) \xrightarrow{\sim} N^{(I)}$.

Für eine exakte Sequenz von A-Moduln $N \xrightarrow{\beta} N'' \longrightarrow 0$ ist die nach Definition 10.21 induzierte Folge $N^{(I)} \longrightarrow N''^{(I)} \longrightarrow 0$ exakt, folglich ist $\mathrm{Hom}(P,N) \oplus \mathrm{Hom}(Q,N) \xrightarrow{\varphi} \mathrm{Hom}(P,N'') \oplus \mathrm{Hom}(Q,N'')$ surjektiv, wobei $\varphi = \mathrm{Hom}(P,\beta) \oplus \mathrm{Hom}(Q,\beta)$. Das ist genau dann der Fall, wenn $\mathrm{Hom}(P,\beta)$ und $\mathrm{Hom}(Q,\beta)$ surjektiv sind. —

Satz 10.25 a) *Ein* A-*Modul* P *ist projektiv* $\Longleftrightarrow$ P *ist isomorph zu einem direkten Summanden eines freien Moduls.*

b) P *ist projektiv und endlich erzeugt* $\Longleftrightarrow$ P *ist isomorph zu einem direkten Summanden eines endlich erzeugten freien Moduls.*

c) P *ist projektiv* $\Longleftrightarrow$ *Jeder surjektive Homomorphismus* $M \xrightarrow{f} P$ *splittet, d.h. es gibt einen Homomorphismus* $g\colon P \longrightarrow M$ *mit* $f \circ g = \mathrm{id}_P$.

Beweis: a) "$\Rightarrow$": Wende 10.19 auf einen surjektiven Homomorphismus $A^{(I)} \longrightarrow P$ an.
"$\Leftarrow$": Folgerung 10.24.

b) ist nach a) klar.

c) "$\Rightarrow$": 10.19.
"$\Leftarrow$": Wähle M als freien A-Modul. —

Satz 10.26 *Sei* A *ein Hauptidealring. Dann ist jeder Untermodul eines freien* A*-Moduls frei.*

Beweis: Sei B eine Basis des freien A-Moduls F, U ein Untermodul von F. Mit $\mathfrak{M}$ bezeichnen wir die Menge der Paare (C,X) mit folgenden Eigenschaften:

(1) $C \subset B$,
(2) X ist eine Menge von Untermoduln $V \simeq A$ von F,
(3) $U \cap \sum_{b\in C} Ab = \bigoplus_{V\in X} V$.

Wegen $(\emptyset,\emptyset) \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$. Durch $((C,X) \leq (C',X') :\Longleftrightarrow C \subset C' \wedge X \subset X')$ wird $\mathfrak{M}$ teilweise geordnet - und zwar induktiv. Denn für eine Kette $((C_k,X_k))_{k\in\mathbb{K}}$ ist $(\bigcup_{k\in\mathbb{K}} C_k, \bigcup_{k\in\mathbb{K}} X_k)$ eine obere Schranke in $\mathfrak{M}$:
(1) und (2) und die Inklusion "$\supset$" aus (3) sind trivialerweise erfüllt. Wenn aber $u \in U \cap \sum_{b\in \cup C_k} Ab$ ist, gibt es ein $k \in \mathbb{K}$ mit $u \in U \cap \sum_{b\in C_k} Ab$, da u, wie jedes Element von F, eine Linearkombination endlich vieler $b \in B$ ist. Also ist $u \in \bigoplus_{V\in X_k} V \subset \bigoplus_{V\in \cup X_k} V$.

Nach dem Zornschen Lemma gibt es ein maximales (C_0,X_0) in $\mathfrak{M}$. Wenn $C_0 = B$ ist, ist $U = \bigoplus_{V\in X_0} V \simeq A^{(X_0)}$ frei. Wäre aber $C_0 \neq B$, so gäbe es $b_1 \in B - C_0$. Schreibe $F_0 = \sum_{b\in C_0} Ab$ und betrachte die Projektion $p\colon F_0 \oplus Ab_1 \longrightarrow Ab_1$. Dann ist $p(U \cap (F_0 \oplus Ab_1))$ isomorph einem Ideal von A, also entweder 0 oder isomorph zu A. Im ersten Falle ist $(C_0 \cup \{b_1\}, X_0) \in \mathfrak{M}$ - im Widerspruch zur Maximalität von (C_0,X_0).
Im zweiten Fall hat man eine exakte Folge
$0 \longrightarrow U \cap F_0 \longrightarrow U \cap (F_0 \oplus Ab_1) \xrightarrow{p'} A \longrightarrow 0$, wo p' durch p induziert ist.

Also gibt es nach 10.25 einen Untermodul $V_1 \subset U \cap (F_0 \oplus Ab_1)$ mit $U \cap (F_0 \oplus Ab_1) = (U \cap F_0) \oplus V_1 = (\bigoplus_{V \in X_0} V) \oplus V_1$, und man erhält durch $(C_0 \cup \{b_1\}, X_0 \cup \{V_1\}) \in \mathfrak{M}$ wieder einen Widerspruch. —

Folgerung 10.27 *Über einem Hauptidealring ist jeder projektive Modul frei.* —

3. Das Tensorprodukt

Definition 10.28 Seien M,N,R A-Moduln. Eine Abbildung $\varphi\colon M \times N \longrightarrow R$ heißt bilinear, falls für jedes $m \in M$ die Abbildung $N \longrightarrow R$, $n \longmapsto \varphi(m,n)$ und für jedes $n \in N$ die Abbildung $M \longrightarrow R$, $m \longmapsto \varphi(m,n)$ A-linear sind.

Definition 10.29 Seien M,N A-Moduln. Ein Tensorprodukt von M und N ist ein A-Modul $M \otimes_A N$ zusammen mit einer bilinearen Abbildung (genannt universell) $\tau\colon M \times N \longrightarrow M \otimes_A N$ derart, daß folgende "universelle" Eigenschaft gilt: Für jede bilineare Abbildung $\varphi\colon M \times N \longrightarrow R$ gibt es genau einen Homomorphismus $\alpha\colon M \otimes_A N \longrightarrow R$, so daß $\alpha \circ \tau = \varphi$ ist.

Satz 10.30 *Seien* $M \otimes N$ *und* $M \otimes' N$ *zwei Tensorprodukte mit universellen bilinearen Abbildungen* $\tau\colon M \times N \longrightarrow M \otimes N$ *und* $\tau'\colon M \times N \longrightarrow M \otimes' N$. *Dann gibt es genau einen Homomorphismus* $\alpha\colon M \otimes N \longrightarrow M \otimes' N$ *mit* $\alpha \circ \tau = \tau'$. *Diese Abbildung* α *ist ein Isomorphismus. Das Tensorprodukt ist damit eindeutig bestimmt bis auf einen eindeutigen Isomorphismus.*

Beweis: Nach Definition des Tensorprodukts existiert genau ein Homomorphismus $\alpha\colon M \otimes N \longrightarrow M \otimes' N$ und genau ein Homomorphismus $\beta\colon M \otimes' N \longrightarrow M \otimes N$, so daß $\alpha \circ \tau = \tau'$ und $\beta \circ \tau' = \tau$ gilt. Also $\beta \circ \alpha \circ \tau = \beta \circ \tau' = \tau = id_{M \otimes N} \circ \tau$ und $\alpha \circ \beta \circ \tau' = \alpha \circ \tau = \tau' = id_{M \otimes' N} \circ \tau'$. Nach Definition des Tensorprodukts existiert jeweils genau ein Homomorphismus mit dieser Eigenschaft, also $\beta \circ \alpha = id_{M \otimes N}$ und $\alpha \circ \beta = id_{M \otimes' N}$.

10.31 Konstruktion "des" Tensorprodukts

Seien M und N A-Moduln. $A^{(M \times N)}$ sei der freie A-Modul mit Basis $M \times N$, U sei der Untermodul von $A^{(M \times N)}$, der von allen Elementen folgender Gestalten erzeugt wird:

$(m+m',n) - (m,n) - (m',n)$, $(m,n+n') - (m,n) - (m,n')$, $(am,n) - a(m,n)$, $(m,an) - a(m,n)$, wobei $m,m' \in M$, $n,n' \in N$ und $a \in A$ sind. τ sei die Verkettung folgender Abbildungen: $M \times N \xhookrightarrow{i} A^{(M\times N)} \xrightarrow{p} A^{(M\times N)}/U$, wobei i die kanonische Injektion und p die kanonische Projektion sei.

Satz 10.32 *Der A-Modul* $A^{(M\times N)}/U$ *zusammen mit der Abbildung* τ *bilden ein Tensorprodukt für* M *und* N.

Beweis: Man sieht sofort, daß τ bilinear ist. Ist nun eine bilineare Abbildung $\varphi: M \times N \longrightarrow R$ gegeben, so setzt sich φ fort zu einer eindeutig bestimmten linearen Abbildung α auf $A^{(M\times N)}$:

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[d, hook] & R \\ A^{(M\times N)} \arrow[ur, "\alpha"'] & \end{tikzcd}$$

Da φ bilinear ist, ist $\alpha(U) = 0$ und liefert daher $\bar{\alpha}: A^{(M\times N)}/U \longrightarrow R$, so daß $\bar{\alpha} \circ \tau = \varphi$. $\bar{\alpha}$ ist durch diese Bedingung eindeutig bestimmt. —

Bemerkung 10.33 In $M \otimes N = A^{(M\times N)}/U$ definiert man für $m \in M$ und $n \in N$: $m \otimes n := \tau(m,n)$. Jedes Element von $A^{(M\times N)}$ hat die Gestalt $\sum_{i=1}^{r} a_i\,(m_i,n_i)$. Daher hat jedes Element von $M \otimes N$ die Gestalt

$\sum_{i=1}^{r} a_i(m_i \otimes n_i) = \sum_{i=1}^{r} (a_i m_i) \otimes n_i = \sum_{i=1}^{r} m_i \otimes (a_i n_i)$, also die Gestalt

$\sum_{i=1}^{r} m_i \otimes n_i$. Aber diese Darstellung ist, wie man sieht, nicht eindeutig!

Frage: Wie kann man für zwei Darstellungen die Gleichheit $\sum_{i=1}^{r} m_i \otimes n_i = \sum_{j=1}^{s} m'_j \otimes n'_j$ zeigen? Nützlich hierbei sind folgende Rechenregeln:

i) $(m+m') \otimes n = m \otimes n + m' \otimes n$,

ii) $m \otimes (n+n') = m \otimes n + m \otimes n'$,

iii) $am \otimes n = m \otimes an$.

Beispiele: a) $\forall\, m \in M$, $\forall\, n \in N$: $0 = m \otimes 0 = 0 \otimes n$.

Beweis: Sei $n \in N$, dann $0 \otimes n + 0 \otimes n = (0+0) \otimes n = 0 \otimes n$, also $0 \otimes n = 0$. Analog für $m \otimes 0$, $m \in M$.

b) $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

Beweis: $\forall\, q \in \mathbb{Q}/\mathbb{Z}:$ 1) $\exists\, n \in \mathbb{Z} - \{0\}: \; nq = 0$.
2) $\forall\, m \in \mathbb{Z} - \{0\} \; \exists\, q' \in \mathbb{Q}/\mathbb{Z}: \; mq' = q$.

Seien $a,b \in \mathbb{Q}/\mathbb{Z}$, $n \in \mathbb{Z} - \{0\}$ mit $na = 0$ und $b' \in \mathbb{Q}/\mathbb{Z}$ mit $nb' = b$. Dann ist $a \otimes b = a \otimes nb' = na \otimes b' = 0 \otimes b' = 0$.

Frage: Wie kann man hingegen eine Ungleichheit $\sum_{i=1}^{r} m_i \otimes n_i \neq \prod_{j=1}^{s} m_j' \otimes n_j'$ zeigen?
Man gebe eine bilineare Abbildung $\varphi: M \times N \longrightarrow R$ in einen geeigneten A-Modul R an, so daß $\Sigma\, \varphi(m_i,n_i) \neq \Sigma\, \varphi(m_j',n_j')$ ist.

Beispiel 10.34 $A \otimes_A M \simeq M$. Dieser Isomorphismus ist natürlich; d.h. jeder Modulhomomorphismus induziert ein kommutatives Diagramm.

Beweis: Man definiert einen Homomorphismus $M \xrightarrow{\psi} A \otimes_A M$, $m \longmapsto 1 \otimes m$.

Surjektivität: $\Sigma\, a_i \otimes m_i = \Sigma\, 1 \otimes a_i m_i = 1 \otimes \Sigma\, a_i m_i = \psi(\Sigma\, a_i m_i)$.

Injektivität: Es ist $1 \otimes m \neq 0$ für $m \neq 0$. Betrachte nämlich folgende bilineare Abbildung: $A \times M \xrightarrow{\varphi} M$, $(a,m) \longmapsto am$. Für $m \neq 0$ ist $\varphi(1,m) = m \neq 0$. —

Konstruktion 10.35 Es sei N ein A-Modul und $M' \xrightarrow{\alpha} M$ ein A-Modulmorphismus. Die induzierte Abbildung $M' \times N \longrightarrow M \times N$ hat eine eindeutige Fortsetzung α' auf $A^{(M' \times N)}$:

$$\begin{tikzcd}
M' \times N \arrow[r, "\alpha \times \mathrm{id}"] \arrow[d, hook] & M \times N \arrow[d, hook, "j"] \\
A^{(M' \times N)} \arrow[ur, "\alpha'"] \arrow[r, "\alpha'' = j \circ \alpha'"'] & A^{(M \times N)}
\end{tikzcd}$$
.

Gemäß Satz 10.32 ist $M' \otimes N \simeq A^{(M' \times N)}/U'$ und $M \otimes N \simeq A^{(M \times N)}/U$.
Es ist $\alpha''(U') \subset U$, so daß sich α'' fortsetzt zu einem Homomorphismus $\overline{\alpha}: M \otimes N \longrightarrow M' \otimes N$. Diesen Homomorphismus bezeichnet man mit $\alpha \otimes_A N := \overline{\alpha}$ oder mit α_*. Analog ist $M \otimes \beta$ für $\beta: N \longrightarrow N'$ definiert.

Satz 10.36 *Für einen A-Modul N bildet die Zuordnung*
$- \otimes_A N: \; (M' \xrightarrow{\alpha} M) \longmapsto (M' \otimes_A N \xrightarrow{\alpha \otimes_A N} M \otimes_A N)$ *einen A-linearen Funktor von der Kategorie der A-Moduln in die der A-Moduln.*

Beweis: Für jeden A-Modul M ist in der Konstruktion $(id_M)'' = id_{A^{(M\times N)}}$ und somit $id_M \otimes_A N = id_{M\otimes N}$. Für Homomorphismen $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ ist $(\beta\circ\alpha)'' = \beta''\circ\alpha''$, also auch $(\beta\circ\alpha)\otimes_A N = (\beta\otimes_A N)\circ(\alpha\otimes_A N)$.
Die A-Linearität ist klar. —

Bemerkung 10.37 Aufgrund der symmetrischen Definition hat man einen natürlichen Isomorphismus $M\otimes_A N \xrightarrow{\sim} N\otimes_A M$.

4. Der Zusammenhang zwischen Hom und dem Tensorprodukt; flache Moduln

Im folgenden seien E, F, G, M, N *A-Moduln.*

Satz 10.38) *Es gibt einen "kanonischen" Isomorphismus* $\mathrm{Hom}_A(E\otimes_A F,G) \xrightarrow{\sim} \mathrm{Hom}_A(E,\mathrm{Hom}_A(F,G))$. *Dieser ist natürlich in allen drei Variablen.*

Beweis: Es bezeichne $\mathrm{Bilin}_A(E\times F,G)$ die Menge der A-bilinearen Abbildungen von $E\times F$ nach G. $\mathrm{Bilin}_A(E\times F,G)$ ist in natürlicher Weise ein A-Modul. Nach Definition des Tensorprodukts ist
$\mathrm{Hom}_A(E\otimes_A F,G) \simeq \mathrm{Bilin}_A(E\times F,G)$, und diese Abbildung ist A-linear.

Sei $\Phi\colon \mathrm{Bilin}_A(E\times F,G) \longrightarrow \mathrm{Hom}(E,\mathrm{Hom}_A(F,G))$ definiert durch:

Für $\varphi\colon E\times F \longrightarrow G$ bilinear, $\Phi(\varphi)\colon E \longrightarrow \mathrm{Hom}_A(F,G)$

$$e \longrightarrow \Phi(\varphi)(e)\colon F \longrightarrow G$$
$$f \longmapsto \varphi(e,f)\ .$$

$\Phi(\varphi)$ ist offenbar A-linear.
Umgekehrt sei $\Psi\colon \mathrm{Hom}(E,\mathrm{Hom}(F,G)) \longrightarrow \mathrm{Bilin}(E\times F,G)$ definiert durch:

Für $\alpha\colon E \longrightarrow \mathrm{Hom}_A(F,G)$ sei $\Psi(\alpha)\colon E\times F \longrightarrow G$ definiert durch
$$(e,f) \longmapsto \alpha(e)(f)\ .$$

Offenbar ist $\Psi(\alpha)$ bilinear.
Φ und Ψ sind invers zueinander und A-linear, also ist
$\mathrm{Bilin}_A(E\times F,G) \simeq \mathrm{Hom}_A(E,\mathrm{Hom}_A(F,G))$. Insgesamt ist also
$\mathrm{Hom}_A(E\otimes_A F,G) \xrightarrow{\sim} \mathrm{Hom}_A(E,\mathrm{Hom}_A(F,G))$, und dieser Isomorphismus ist natürlich in allen drei Variablen. —

Lemma 10.39 *Sei* $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ *eine Folge von* A-*Moduln. Falls für alle* A-*Moduln* N *die Folge* $\mathrm{Hom}(M'',N) \xrightarrow{\beta^*} \mathrm{Hom}(M,N) \xrightarrow{\alpha^*} \mathrm{Hom}(M',N)$ *exakt ist, so ist* $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ *exakt.*

Beweis: i) Wähle $N = M''$. Dann gilt nach Voraussetzung
$0 = \alpha^* \circ \beta^* \,(\mathrm{id}_{M''}) = \mathrm{id}_{M''} \circ \beta \circ \alpha = \beta \circ \alpha$. Also ist $\mathrm{Im}\,\alpha \subset \mathrm{Ker}\,\beta$.

ii) Wähle $N = M/\mathrm{Im}\,\alpha$, und sei $f\colon M \longrightarrow M/\mathrm{Im}\,\alpha$ der kanonische Epimorphismus (= surjektiver Homomorphismus). Dann ist $\alpha^*(f) = f \circ \alpha = 0$. Nach Voraussetzung existiert ein Homomorphismus $g\colon M'' \longrightarrow N$ mit $g \circ \beta = \beta^*(g) = f$. Also ist $\mathrm{Im}\,\alpha = \ker f = \ker(g \circ \beta) \supset \ker \beta$. –

Satz 10.40 *Der Funktor* $\_ \otimes_A N$ *ist rechtsexakt. D.h. für eine exakte Folge von* A-*Moduln* $M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *ist die induzierte Folge* $M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0$ *exakt.*

Beweis: Für alle A-Moduln G ist aufgrund der Linksexaktheit des Funktors Hom die Sequenz $0 \longrightarrow \mathrm{Hom}(M'',\mathrm{Hom}(N,G)) \longrightarrow \mathrm{Hom}(M,\mathrm{Hom}(N,G)) \longrightarrow \mathrm{Hom}(M',\mathrm{Hom}(N,G))$ exakt. Diese Sequenz ist kanonisch isomorph zu $0 \longrightarrow \mathrm{Hom}(M'' \otimes N,G) \longrightarrow \mathrm{Hom}(M \otimes N,G) \longrightarrow \mathrm{Hom}(M' \otimes N,G)$. Nach obigem Lemma ist daher $M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0$ exakt. –

Folgerung 10.41 *Sei* $\mathfrak{a}$ *ein Ideal in* A, M *ein* A-*Modul. Dann ist* $(A/\mathfrak{a}) \otimes_A M \simeq M/\mathfrak{a}M$.

Beweis: Man betrachte $0 \longrightarrow \mathfrak{a} \xrightarrow{i} A \longrightarrow A/\mathfrak{a} \longrightarrow 0$. Nach 10.40 ist die obere Zeile des folgenden Diagramms exakt:

$$\begin{tikzcd}
 & \mathfrak{a} \otimes M \arrow[r, "i \otimes M"] \arrow[d, "\varepsilon"'] & A \otimes M \arrow[r] \arrow[d, "10.34"', "\wr"] & (A/\mathfrak{a}) \otimes M \arrow[r] & 0 \\
0 \arrow[r] & \mathfrak{a}M \arrow[r] & M \arrow[r] & M/\mathfrak{a}M \arrow[r] & 0
\end{tikzcd}$$

Hierbei ist $\varepsilon\colon \mathfrak{a} \otimes M \longrightarrow \mathfrak{a}M$ gegeben durch $\Sigma\, a_i \otimes m_i \longrightarrow \Sigma\, a_m m_i$ und ist offensichtlich surjektiv. Also ist
$M/\mathfrak{a}M \simeq A \otimes M/\,(i \otimes M)(\mathfrak{a} \otimes M) \simeq (A/\mathfrak{a}) \otimes M$. –

Bemerkung 10.42 Für eine exakte Sequenz $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ ist im allgemeinen die Sequenz $0 \longrightarrow M' \otimes N \longrightarrow M \otimes N \longrightarrow M'' \otimes N \longrightarrow 0$ nicht exakt.

Beispiel: Die exakte Sequenz von $\mathbb{Z}$-Moduln $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2 \longrightarrow 0$ hat nach Tensorieren mit $\mathbb{Z}/2$ die Gestalt

$(0 \longrightarrow)\ \mathbb{Z}/2 \xrightarrow{\alpha} \mathbb{Z}/2 \longrightarrow \mathbb{Z}/2 \longrightarrow 0$, wobei α, die Homothetie von 2 also, die Nullabbildung und deshalb nicht injektiv ist.

Definition 10.43 Ein A-Modul N heißt flach, falls für alle exakten Sequenzen von A-Moduln $0 \longrightarrow M' \longrightarrow M$ die induzierte Sequenz

$$0 \longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N$$

exakt ist.

Satz 10.44 *Seien* M_i, $i \in I$, *und* N *A-Moduln. Dann gilt:*

$$(\bigoplus_{i\in I} M_i) \otimes_A N \simeq \bigoplus_{i\in I} (M_i \otimes_A N)$$

Dieser Isomorphismus ist natürlich in N.

Beweis: Die bilineare Abbildung $(\bigoplus_{i\in I} M_i) \times N \longrightarrow \bigoplus_{i\in I} (M_i \otimes N)$, $((m_i)_{i\in I}, n) \longmapsto (m_i \otimes n)_{i\in I}$, faktorisiert über einen Homomorphismus $\varphi\colon (\bigoplus_{i\in I} M_i) \otimes N \longrightarrow \bigoplus_{i\in I} (M_i \otimes N)$.

Für $j \in I$ sei $\psi\colon M_j \longrightarrow \bigoplus_{i\in I} M_i$ die kanonische Einbettung. Die Homomorphismen $\psi_j \otimes N : M_j \otimes N \longrightarrow (\bigoplus_{i\in I} M_i) \otimes N$ induzieren einen Homomorphismus $\psi\colon \bigoplus_{i\in I} (M_i \otimes N) \longrightarrow (\oplus M_i) \otimes N$. Wie man leicht nachrechnet, sind φ und ψ invers zueinander und natürlich in N. —

Folgerung 10.45 *Projektive Moduln sind flach.*

Beweis: Seien P und N projektive A-Moduln mit $P \oplus N \simeq A^{(I)}$ und $0 \longrightarrow M' \longrightarrow M$ eine exakte Sequenz von A-Moduln. Dann ist $0 \longrightarrow A^{(I)} \otimes M' \longrightarrow A^{(I)} \otimes M$ nach 10.44 einerseits isomorph zu $0 \longrightarrow M'^{(I)} \longrightarrow M^{(I)}$, also exakt, andererseits isomorph zu $0 \longrightarrow (P \oplus N) \otimes M' \longrightarrow (P \oplus N) \otimes M$, und diese Sequenz ist isomorph zu $0 \longrightarrow (P \otimes M') \oplus (N \otimes M') \longrightarrow (P \otimes M) \oplus (N \otimes M)$. Also ist auch $0 \longrightarrow P \otimes M' \longrightarrow P \otimes M$ exakt.

(N.B.: Die Isomorphie von Sequenzen ist auf naheliegende Weise zu definieren.) —

Satz 10.46 *Sei* $S \subset A$ *eine multiplikative Teilmenge. Dann gilt:*

$$(S^{-1}A) \otimes_A M \simeq S^{-1}M .$$

Dieser Isomorphismus ist natürlich in M .

Beweis: Die Abbildung $S^{-1}A \times M \longrightarrow S^{-1}M$, $(\frac{a}{s},m) \longrightarrow \frac{am}{s}$ ist bilinear, induziert also einen Homomorphismus $f\colon S^{-1}A \otimes_A M \longrightarrow S^{-1}M$.
Umgekehrt definiert man $g\colon S^{-1}M \longrightarrow S^{-1}A \otimes_A M$, $\frac{m}{s} \longmapsto \frac{1}{s} \otimes m$.
Die Wohldefiniertheit von g sieht man so: Seien $\frac{m}{s} = \frac{m'}{s'} \in S^{-1}M$. Dann gibt es $t \in S$ mit $tsm' = ts'm$. Somit ist $\frac{1}{s} \otimes m = \frac{1}{tss'} \otimes ts'm = \frac{1}{tss'} \otimes tsm' = \frac{1}{s'} \otimes m'$.
Trivialerweise ist $f \circ g = \mathrm{id}_{S^{-1}M}$.
Die Elemente der Gestalt $\frac{a}{s} \otimes m$ in $S^{-1}A \otimes M$ bilden ein Erzeugendensystem von $S^{-1}A \otimes M$, und für diese gilt:

$$g \circ f(\tfrac{a}{s} \otimes m) = g(\tfrac{am}{s}) = \tfrac{1}{s} \otimes am = \tfrac{a}{s} \otimes m .$$

Daher ist $g \circ f = \mathrm{id}_{S^{-1}A \otimes M}$.

Man rechnet leicht nach, daß der Isomorphismus f natürlich in M ist. –

Folgerung 10.47 *Sei* S *eine multiplikative Teilmenge von* A . *Dann ist* $S^{-1}A$ *ein flacher* A-*Modul.*

Beweis: Sei $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ eine exakte Sequenz von A-Moduln. Dann ist $0 \longrightarrow S^{-1}M' \longrightarrow S^{-1}M \longrightarrow S^{-1}M'' \longrightarrow 0$ exakt, und diese Sequenz ist natürlich isomorph zu
$0 \longrightarrow S^{-1}A \otimes_A M' \longrightarrow S^{-1}A \otimes M \longrightarrow S^{-1}A \otimes M'' \longrightarrow 0$. –

Satz 10.48 *Seien* E, F, G *A-Moduln. Dann existiert ein Isomorphismus*

$$E \otimes_A (F \otimes_A G) \simeq (E \otimes_A F) \otimes_A G .$$

Dieser ist natürlich in allen drei Variablen.

Beweis: Für $g \in G$ sei $\alpha_g\colon E \times F \longrightarrow E \otimes (F \otimes G)$, definiert durch $(e,f) \longmapsto e \otimes (f \otimes g)$. α_g ist bilinear, induziert also einen Homomorphismus $\varphi_g\colon E \otimes F \longrightarrow E \otimes (F \otimes G)$ mit $\varphi_g(e \otimes f) = e \otimes (f \otimes g)$.
$\alpha\colon (E \otimes F) \times G \longrightarrow E \otimes (F \otimes G)$, $(x,g) \longmapsto \varphi_g(x)$ ist bilinear, induziert also einen Homomorphismus $\varphi\colon (E \otimes F) \otimes G \longrightarrow E \otimes (F \otimes G)$ mit $\varphi((e \otimes f) \otimes g) = e \otimes (f \otimes g)$.

Analog erhält man einen Morphismus $\psi\colon E \otimes (F \otimes G) \longrightarrow (E \otimes F) \otimes G$ mit $\psi(e \otimes (f \otimes g)) = \psi\,(e \otimes f) \otimes g$.
$\varphi \circ \psi = \mathrm{id}_{E \otimes (F \otimes G)}$ und $\psi \circ \varphi = \mathrm{id}_{(E \otimes F) \otimes G}$ und φ und ψ sind natürlich in allen drei Variablen. —

Folgerung 10.49 *Seien* E *und* F *flache* A-*Moduln.*
Dann ist $E \otimes_A F$ *flach.*

Beweis: Sei $0 \longrightarrow M' \longrightarrow M$ eine exakte Sequenz von A-Moduln. Da E flach ist, ist $0 \longrightarrow M' \otimes E \longrightarrow M \otimes E$ exakt. Da F flach ist, ist $0 \longrightarrow (M' \otimes E) \otimes F \longrightarrow (M \otimes E) \otimes F$ exakt. Diese Sequenz ist nach Satz 10.48 isomorph zu $0 \longrightarrow M' \otimes (E \otimes F) \longrightarrow M \otimes (E \otimes F)$.
Also ist $E \otimes F$ flach. —

Feststellung 10.50 (*Exaktheit von Funktoren*)

Sei $F\colon A\text{-Mod} \longrightarrow B\text{-Mod}$ *ein kovarianter additiver Funktor. Dann sind äquivalent:*

(i) *Für jede exakte Sequenz von* A-*Moduln* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *ist die Sequenz von* B-*Moduln* $0 \longrightarrow F(M') \longrightarrow F(M'') \longrightarrow F(M'') \longrightarrow 0$ *exakt.*

(ii) *Für jede exakte Sequenz von* A-*Moduln* $M' \longrightarrow M \longrightarrow M''$ *ist die Sequenz von* B-*Moduln* $F(M') \longrightarrow F(M) \longrightarrow F(M'')$ *exakt.*

Beweis: (ii) ⇒ (i) ist trivial.
(i) ⇒ (ii): Jede exakte Sequenz $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ läßt sich aufspalten in exakte Sequenzen:

$$0 \longrightarrow M_1' \longrightarrow M_1 \xrightarrow{\alpha} M_2' \longrightarrow 0$$
$$0 \longrightarrow M_2' \xrightarrow{\beta} M_2 \xrightarrow{\gamma} M_3' \longrightarrow 0$$
$$0 \longrightarrow M_3' \xrightarrow{\delta} M_3 \longrightarrow M_4' \longrightarrow 0\ ,$$

wobei $M_1' \simeq \operatorname{Ker} f,\ M_2' \simeq \operatorname{Ker} g = \operatorname{Im} f$
$M_3' \simeq \operatorname{Im} g\ ,\ M_4' \simeq \operatorname{Coker} g$.

Hat man umgekehrt drei solche exakte Sequenzen (von B-Moduln), gegeben mit $\beta\alpha = f$ und $\delta\gamma = g$, dann ist $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ exakt. —

Satz 10.51 *Sei* F *ein* A-*Modul. Dann sind äquivalent:*

(*i*) *Für jede Sequenz* $M' \xrightarrow{f} M \xrightarrow{g} M''$ *gilt:*
$M' \xrightarrow{f} M \xrightarrow{g} M''$ *ist exakt* ⟺ $F \otimes M' \xrightarrow{f_*} F \otimes M \xrightarrow{g_*} F \otimes M''$ *ist exakt.*

(ii) F *ist flach, und für alle maximalen Ideale* $\mathfrak{m}$ *von* A *ist* $F/\mathfrak{m}F \neq 0$.

(iii) F *ist flach, und für alle* A-*Moduln* M *gilt:*
$F \otimes M = 0 \Rightarrow M = 0$.

(iv) F *ist flach, und für alle* A-*Modulhomomorphismen* g *gilt:*
$F \otimes g = 0 \Rightarrow g = 0$.

Beweis: (i) ⇒ (ii): Die Flachheit von F ist trivial.
Sei $\mathfrak{m}$ ein maximales Ideal von A. $0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow A/\mathfrak{m} \longrightarrow 0$ (mit den kanonischen Abbildungen) ist exakt. Also ist

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F \otimes \mathfrak{m} & \longrightarrow & F \otimes A & \longrightarrow & F \otimes A/\mathfrak{m} & \longrightarrow & 0 \\ & & & & \wr\! \| & & \wr\! \| & & \\ & & & & F & & F/\mathfrak{m}F & & \end{array}$$

exakt. Es gilt: $F/\mathfrak{m}F \neq 0$; denn aus $F/\mathfrak{m}F = 0$ würde folgen, daß
$0 \longrightarrow F \otimes \mathfrak{m} \longrightarrow F \otimes A \longrightarrow 0$ und daher nach (i) auch
$0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow 0$ exakt ist.

(ii) ⇒ (iii): Es sei $M \neq 0$ ein A-Modul, $x \in M - \{0\}$.
$M \supset Ax \simeq A/\mathrm{Ann}\, x$ und $\mathrm{Ann}\, x \neq A$. Sei $\mathfrak{m} \supset \mathrm{Ann}\, x$ ein maximales Ideal von A. Man hat eine surjektive A-lineare Abbildung $f\colon Ax \longrightarrow A/\mathfrak{m}$.
Somit ist auch $f_*\colon F \otimes Ax \longrightarrow F \otimes A/\mathfrak{m} \simeq F/\mathfrak{m}F \neq 0$ surjektiv und deshalb $F \otimes Ax \neq 0$. Die naheliegende Folge $0 \longrightarrow Ax \longrightarrow M$ ist exakt, also ist $0 \longrightarrow F \otimes Ax \longrightarrow F \otimes M$ exakt. Da $F \otimes Ax \neq 0$, ist $F \otimes M \neq 0$.

(iii) ⇒ (iv): Es sei $M \xrightarrow{g} N$ A-linear mit $F \otimes g = 0$, $U := \mathrm{Im}\, g$ und $M \xrightarrow{\alpha} U \xrightarrow{\beta} N$, so daß $\beta \circ \alpha = g$. $F \otimes \alpha$ ist surjektiv, und da F flach ist, ist $F \otimes \beta$ injektiv, sowie $(F \otimes \beta) \circ (F \otimes \alpha) = F \otimes g = 0$.
Also ist $F \otimes U = 0$, und nach Voraussetzung folgt $U = 0$, d.h. $g = 0$.

(iv) ⇒ (iii): Sei M ein A-Modul mit $F \otimes M = 0$. Dann ist $F \otimes \mathrm{id}_M = 0$, folglich $\mathrm{id}_M = 0$.

(iii) und (iv) ⇒ (i): (i) "⇒" ist klar, da F flach ist.

(i) "⇐": Sei $U = \mathrm{Im}\, f$, $V = \mathrm{Ker}\, g$. $F \otimes (g \circ f) = (F \otimes g) \circ (F \otimes f) = 0$, nach (iv) ist $g \circ f = 0$, d.h. $U \subset V$.
Die Sequenzen

$$M' \xrightarrow{\alpha} U \longrightarrow 0$$
$$0 \longrightarrow U \xrightarrow{\beta} V \xrightarrow[\text{kanonisch}]{} V/U \longrightarrow 0$$
$$0 \longrightarrow V \xrightarrow{\gamma} M \xrightarrow{g} M''$$

sind exakt, und $f = \gamma \circ \beta \circ \alpha$. Es gilt

$\mathrm{Im}((F \otimes \gamma) \circ (F \otimes \beta) \circ (F \otimes \alpha)) = \mathrm{Im}(F \otimes f) = \ker(F \otimes g) = \mathrm{Im}(F \otimes \gamma)$,
da $F \otimes M' \longrightarrow F \otimes M \longrightarrow F \otimes M''$ exakt ist.
Weil $F \otimes \gamma$ injektiv ist, ist $(F \otimes \beta) \circ (F \otimes \alpha)$ surjektiv, und daher $F \otimes \beta$ surjektiv. Also ist $F \otimes (V/U) = 0$ und nach (iii) daher $V = U$, d.h. $M' \xrightarrow{f} M \xrightarrow{g} M''$ ist exakt. –

Definition 10.52 Ein A-Modul F, der die äquivalenten Bedingungen von 10.51 erfüllt, heißt treuflach.

Beispiele 10.53 a) Für eine Indexmenge $I \neq \emptyset$ ist der freie A-Modul $A^{(I)}$ treuflach. Insbesondere ist der Polynomring $A[X]$ ein treuflacher A-Modul.

b) $\bigoplus_{m \in I} A_m$, wo $I = \{$maximale Ideale von $A\}$ ist, ist ein treuflacher A-Modul.

Beweis: Nach 10.44 und 10.47 ist $\bigoplus_m A_m$ flach und $M \otimes (\bigoplus_m A_m) = \bigoplus_m M_m$. Mit 3.44 ist also die Bedingung (iii) in Satz 10.51 erfüllt.

c) $\mathbb{Q}$ ist ein flacher, aber kein treuflacher $\mathbb{Z}$-Modul (vgl. Bedingung (ii) in 10.51, $\mathbb{Q} \otimes (\mathbb{Z}/(n)) \simeq 0$ für $n > 0$!)

(N.B.: Ein Modul M mit $\mathrm{Ann}_A M = (0)$ heißt auch ein treuer A-Modul. $\mathbb{Q}$ ist also treu und flach, aber nicht treuflach über $\mathbb{Z}$.)

Bemerkungen 10.54 a) Es sei $A \longrightarrow B$ ein Ringhomomorphismus (insbesondere also B ein A-Modul) und N ein A-Modul. Dann ist $B \otimes_A N$ vermöge folgender Operation von B auf $B \otimes_A N$ ein B-Modul:

$$\varphi\colon B \times B \otimes_A N \longrightarrow B \otimes_A N$$
$$(b, \Sigma\, b_i \otimes n_i) \longmapsto \Sigma\, (bb_i) \otimes n_i \ .$$

b) Ist N ein projektiver A-Modul, so ist $B \otimes_A N$ ein projektiver B-Modul.

Beweis: Für $N = A$ gilt: $B \otimes_A N \simeq B$, also ist nach 10.44 auch: $B \otimes_A A^{(I)} \simeq B^{(I)}$, und schließlich gilt für $N \oplus N' \simeq A^{(I)}$
$B^{(I)} = B \otimes_A A^{(I)} \simeq B \otimes_A (N \oplus N') \simeq (B \otimes_A N) \oplus (B \otimes_A N')$. –

c) Seien B und C zwei A-Algebren, $f\colon A \longrightarrow B$, $g\colon A \longrightarrow C$ die Strukturhomomorphismen. Dann ist $D := B \otimes_A C$ ein A-Modul. Wir wollen auf D eine Multiplikation erklären. Dazu betrachten wir die Abbildung

$B \times C \times B \times C \longrightarrow D$, die durch $(b,c,\tilde{b},\tilde{c}) \longmapsto b\tilde{b} \otimes c\tilde{c}$ erklärt ist. Sie ist, wie man sofort nachrechnet, in jedem Faktor A-linear und induziert deshalb aufgrund der universellen Eigenschaft des Tensorproduktes einen A-Modulhomomorphismus $B \otimes_A C \otimes_A B \otimes_A C \simeq D \otimes_A D \longrightarrow D$, der wiederum wegen der universellen Eigenschaft des Tensorproduktes zu einer bilinearen Abbildung $m\colon D \times D \longrightarrow D$ mit $m(b \otimes c, \tilde{b} \otimes \tilde{c}) = b\tilde{b} \otimes c\tilde{c}$ korrespondiert. Auf diese Weise haben wir eine Multiplikation auf D definiert: Für Elemente der Form $b \otimes c$ ist sie gegeben durch $(b \otimes c)\cdot(\tilde{b} \otimes \tilde{c}) = b\tilde{b} \otimes c\tilde{c}$ und allgemein durch $(\sum_i b_i \otimes c_i)(\sum_j \tilde{b}_j \otimes \tilde{c}_j) = \sum_{i,j} (b_i\tilde{b}_j \otimes c_i\tilde{c}_j)$.

Man überprüft sofort, daß mit dieser Multiplikation D ein kommutativer Ring mit Einselement $1 \otimes 1$ ist. D ist sogar eine A-Algebra, denn die Abbildung $a \longrightarrow f(a) \otimes g(a)$ ist ein Ringhomomorphismus $A \longrightarrow D$: Man hat nämlich ein kommutatives Diagramm von Ringhomomorphismen

$$\begin{tikzcd} & B \arrow[dr, "\alpha"] & \\ A \arrow[ur, "f"] \arrow[dr, "g"'] & & D \\ & C \arrow[ur, "\beta"'] & \end{tikzcd},$$

in dem α und β durch $\alpha(b) = b \otimes 1$, $\beta(c) = 1 \otimes c$ definiert sind.

Beispiel: Sei B eine A-Algebra. Dann ist $A[X] \otimes_A B \xrightarrow{\sim} B[X]$.

Beweis: Nach Satz 10.44 ist $A[X] \otimes_A B \longrightarrow B[X]$, $\sum f_i \otimes b_i \longmapsto \sum f_i b_i$ ein A-Modulisomorphismus, der mit der oben erklärten Algebrenstruktur auf $A[X] \otimes_A B$ verträglich ist.

Aufgaben und Hinweise

1) Sei A ein nicht notwendig kommutativer Ring und $Z(A) := \{z \in A \mid za = az \ \ \forall\, a \in A\}$ sein Zentrum. Zeige:
   a) Für jedes $z \in Z(A)$ bilden die Homothetien $h_z\colon M \longrightarrow M$, $x \longmapsto zx$ für alle A-(Links-) Moduln eine natürliche Transformation des identischen Funktors von A-Mod.
   b) Die Abbildung $z \longmapsto h_z$ bildet $Z(A)$ bijektiv auf die Klasse aller natürlichen Transformationen von $\mathrm{id}_{A\text{-Mod}}$ ab.

   Ein kommutativer Ring A ist also durch A-Mod bestimmt.
   Zeige: c) Sei $M_n(A)$ der $n{\times}n$-Matrizenring über A. Dann sind die Kategorien A-Mod und $M_n(A)$-Mod zueinander äquivalent.

2) Hom und $\otimes$ sind nicht nur Funktoren von 2 Variablen, sondern sogar sogenannte Bifunktoren. D.h. die durch Homomorphismen $\alpha\colon M \longrightarrow M'$ und $\beta\colon N \longrightarrow N'$ induzierten Diagramme

$$\begin{array}{ccc} \mathrm{Hom}(M',N) & \xrightarrow{\mathrm{Hom}(\alpha,N)} & \mathrm{Hom}(M,N) \\ \downarrow{\scriptstyle \mathrm{Hom}(M',\beta)} & & \downarrow{\scriptstyle \mathrm{Hom}(M,\beta)} \\ \mathrm{Hom}(M',N') & \xrightarrow{\mathrm{Hom}(\alpha,N')} & \mathrm{Hom}(M,N') \end{array}$$

und

$$\begin{array}{ccc} M \otimes N & \xrightarrow{\alpha \otimes N} & M' \otimes N \\ \downarrow{\scriptstyle M\otimes\beta} & & \downarrow{\scriptstyle M'\otimes\beta} \\ M \otimes N' & \xrightarrow{\alpha \otimes N'} & M' \otimes N' \end{array}$$

sind kommutativ.

3) Sei A ein Ring, dessen Ideale projektive A-Moduln sind. Zeige: Jeder Untermodul eines freien A-Moduls ist isomorph einer direkten Summe, deren Summanden sämtlich zu Idealen von A isomorph sind. (Der Beweis von 10.26 läßt sich direkt übertragen.) Jeder Untermodul eines projektiven Moduls ist also wieder projektiv. Ein Ring A mit obiger Eigenschaft heißt hereditär. (Untermoduln projektiver Moduln "erben" die Eigenschaft, projektiv zu sein.) Wir werden später sehen, daß ein Integritätsring genau dann hereditär ist, wenn er ein Dedekindring ist. Vgl. jedoch hiermit die nächste Aufgabe.

4) Sei k ein Körper. Betrachte in der unendlichen direkten "Potenz" $k^{\mathbb{N}}$ den Unterring $A = \{(x_i)_{i\in\mathbb{N}} \mid \exists\, x \in k$ mit $x_i = x$ für fast alle $i\}$. Für $j \in \mathbb{N}$ sei $e_j := (\delta_{ij})_{i\in\mathbb{N}} \in A$. Für $J \subset \mathbb{N}$ sei

$$e_J := (x_i)_{i\in\mathbb{N}} \quad \text{mit} \quad x_i = \begin{cases} 1 & \text{für } i \in J \\ 0 & \text{für } i \notin J \end{cases}.$$

Sei $\mathfrak{a}$ ein Ideal von A. Zeige:

a) Wenn jedes Element von $\mathfrak{a}$ nur endlich viele nichtverschwindende Komponenten hat, ist $\mathfrak{a} = \bigoplus_{j\in J} Ae_j$ für eine geeignete Menge $J \subset \mathbb{N}$.

b) Wenn ein Element von $\mathfrak{a}$ nur endlich viele verschwindende Komponenten hat, ist $\mathfrak{a} = Ae_J$ für eine Menge $J \subset \mathbb{N}$ mit endlichem Komplement $\mathbb{N} - J$.

c) A ist hereditär.

5) a) Sei t ein kovarianter A-linearer Funktor von der Kategorie der A-Moduln in dieselbe und N ein A-Modul. Es gelte:

(i) t ist rechtsexakt; d.h. wenn $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ exakt ist, ist $t(M') \xrightarrow{t(\alpha)} t(M) \xrightarrow{t(\beta)} t(M'') \longrightarrow 0$ exakt.

(ii) Man hat einen natürlichen Isomorphismus: $t(\bigoplus_{i\in I} M_i) \simeq \bigoplus_{i\in I} t(M_i)$.

(iii) $t(A) = N$.

Zeige: Man hat einen natürlichen Isomorphismus $t(M) \simeq M \otimes_A N$.

b) Man überlege in diesem Zusammenhang, daß a) eine Methode zur Berechnung des Tensorproduktes liefert, die 10.41 verallgemeinert.

Sei $A^{(I)} \xrightarrow{\alpha} A^{(J)} \longrightarrow M \longrightarrow 0$ exakt, wobei α eine (möglicherweise unendliche) Matrix sei. Dann ist

$$N^{(I)} \xrightarrow{\alpha} N^{(J)} \xrightarrow{\varphi} M \otimes N \longrightarrow 0$$

mit der gleichen Matrix α und richtig gewähltem φ ebenfalls exakt. Falls man I und J endlich wählen kann, wird es besonders einfach. Insbesondere ist dann α eine endliche Matrix.

6) Sei t ein kontravarianter A-linearer Funktor von der Kategorie der A-Moduln in dieselbe und N ein A-Modul. Es gelte:

(i) t ist linksexakt, d.h. wenn $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ exakt ist, ist $0 \longrightarrow t(M'') \xrightarrow{t(\beta)} t(M) \xrightarrow{t(\alpha)} t(M')$ exakt;

(ii) man hat einen natürlichen Isomorphismus $t(\bigoplus_{i\in I} M_i) \simeq \prod_{i\in I} t(M_i)$;

(iii) $t(A) = N$.

Zeige: Man hat einen natürlichen Isomorphismus $t(M) \simeq \mathrm{Hom}_A(M,N)$.

7) Sei M ein Modul über einem Integritätsring A (bzw. reduzierten Ring A mit nur endlich vielen minimalen Primidealen). M heißt torsionsfrei, wenn für jedes $s \in A - \{0\}$ (bzw. jeden Nichtnullteiler s in A) die Homothetie $h_s\colon M \longrightarrow M$ injektiv ist. Sei $S = A - \{0\}$ (bzw. S die Menge der Nichtnullteiler von A). Zeige:

a) M ist genau dann torsionsfrei, wenn der Homomorphismus $i_{M,S}\colon M \longrightarrow S^{-1}M$ injektiv ist.

b) Ein endlich erzeugter A-Modul M ist genau dann torsionsfrei, wenn er zu einem Untermodul eines freien A-Moduls isomorph ist. ($S^{-1}M \subset (S^{-1}A)^n$; Hauptnenner.) Beachte aber: $\mathbb{Q} \not\subset \mathbb{Z}^{(I)}$.

8) Zeige: Ein A-Modul M ist genau dann flach, wenn für jedes (endlich erzeugte) Ideal $\mathfrak{a}$ von A die Inklusion $\mathfrak{a} \subset A$ einen injektiven Homomorphismus $\mathfrak{a} \otimes M \longrightarrow M$ induziert. (Vgl. 18.22.)

9) Zeige: a) Ein Modul über einem Hauptidealring ist genau dann flach, wenn er torsionsfrei ist.
b) Der Ring C_1 der stetigen Funktionen $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ ist treuflach über dem Polynomring $\mathbb{R}[X]$. (Naheliegende Einbettung $\mathbb{R}[X] \hookrightarrow C_1$.)

10) Sei k ein Körper. Zeige:
a) Wenn M ein flacher $k[X_1,\dots,X_n]$-Modul ist, ist X_i ein Nichtnullteiler für $M/X_1M + \dots + X_{i-1}M$ für jedes $i = 1,\dots,n$. (Für $i = 1$ ist $X_1M + \dots + X_{i-1}M := \{0\}$.)
b) Der Ring C_n der stetigen Funktionen $\mathbb{R}^n \longrightarrow \mathbb{R}$ ist für $n > 1$ nicht flach über $\mathbb{R}[X_1,\dots,X_n]$.

11) Man mache sich klar, daß es nicht sehr sinnvoll ist, bilineare Abbildungen über nichtkommutativen Ringen zu betrachten. (Seien M, N und E Linksmoduln über A und $x \in M$, $y \in N$, $a,b \in A$, ferner $\varphi\colon M \times N \longrightarrow E$ bilinear. Dann ist $(ab)\varphi(x,y) = a\varphi(bx,y) = \varphi(bx,ay) = (ba)\varphi(x,y)$.) Stattdessen betrachtet man für einen A-Rechtsmodul M, einen A-Linksmodul N und eine abelsche Gruppe E Abbildungen: $f\colon M \times N \longrightarrow E$, für die folgendes gilt:
$f(x+x',y) = f(x,y) + f(x',y)$,
$f(x,y+y') = f(x,y) + f(x,y')$,
$f(xa,y) = f(x,ay)$. In [MacLane] heißen sie mittellinear.
Definiere ein zugehöriges Tensorprodukt - vorläufig mit $\otimes'$ bezeichnet -: $M \otimes'_A N$ ist eine abelsche Gruppe, i.a. kein A-Modul. Zeige die Existenz. Für einen kommutativen Ring A zeige: $M \otimes'_A N$ ist auf kanonische Weise ein A-Modul und als solcher natürlich isomorph zu $M \otimes_A N$.

12) Seien $U_1,\dots,U_n$ endlich viele Untermoduln eines A-Moduls M und F ein flacher A-Modul. Zeige: Wenn man $F \otimes_A U_i$ auf kanonische Weise als Untermodul von $F \otimes_A M$ auffaßt, gilt:

$$\bigcap_{i=1}^{n} (F \otimes_A U_i) = F \otimes_A \Big(\bigcap_{i=1}^{n} U_i\Big).$$

Dies gilt nicht für unendliche Durchschnitte. (Beispiel?)
Wenn hingegen F sogar projektiv ist, gilt für unendliche Durchschnitte die analoge Aussage.

§ 11 HOM, TENSORPRODUKT UND BRÜCHE

1. Allgemeines

11.1 Sei S eine multiplikative Teilmenge eines Ringes A, und M,N seien A-Moduln. Dann hat man folgendes kommutative Diagramm:

$$\begin{tikzcd} \mathrm{Hom}_A(M,N) \arrow[rr, "\sigma"] \arrow[d, "i"'] & & \mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) \\ S^{-1}\mathrm{Hom}_A(M,N) \arrow[urr, "\varphi"'] & & \end{tikzcd}$$

$i\colon \mathrm{Hom}_A(M,N) \longrightarrow S^{-1}\mathrm{Hom}_A(M,N)$, $f \longmapsto \frac{f}{1}$,

$\sigma\colon \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$, $f \longmapsto S^{-1}f$,

$\varphi\colon S^{-1}\mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$, $\frac{f}{s} \longmapsto \frac{1}{s}S^{-1}f$

(φ ist wohldefiniert!).

Im allgemeinen ist φ weder injektiv noch surjektiv:

Beispiele: $A = \mathbb{Z}$, $S = \mathbb{Z} - \{0\}$.

a) Es sei $M = \mathbb{Q}$, $N = \mathbb{Z}$. Dann ist $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = 0$, aber $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q},\mathbb{Q}) \simeq \mathbb{Q}$.
φ ist also nicht surjektiv.

b) Es sei $M = N = \mathbb{Q}/\mathbb{Z}$. Dann ist $r \cdot \mathrm{id}_{\mathbb{Q}/\mathbb{Z}} \neq 0$ für alle $r \in \mathbb{Z} - \{0\}$.
Es folgt: $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \supset \mathbb{Z} \cdot \mathrm{id}_{\mathbb{Q}/\mathbb{Z}} \simeq \mathbb{Z}$, und daher ist
$S^{-1}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z},\mathbb{Q}/\mathbb{Z}) \neq 0$, aber $S^{-1}(\mathbb{Q}/\mathbb{Z}) = 0$, also $\mathrm{Hom}_{\mathbb{Q}}(S^{-1}(\mathbb{Q}/\mathbb{Z})\ S^{-1}(\mathbb{Q}/\mathbb{Z})) = 0$.
φ ist nicht injektiv.

Definition 11.2 Ein A-Modul M heißt endlich darstellbar (oder von endlicher Darstellung), wenn eine exakte Sequenz der Form
$A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$ existiert.

Bemerkungen 11.3 a) Ist A noethersch und M ein endlicher A-Modul, so ist M endlich darstellbar.

b) Ist P ein endlicher, projektiver A-Modul, so ist P endlich darstellbar.
Denn nach 10.25b) gibt es Q und $n \in \mathbb{N}$ mit $P \oplus Q \simeq A^n$. Man hat kanonische Homomorphismen $A^n \longrightarrow P$ und $A^n \longrightarrow Q \longrightarrow A^n$, aus denen die exakte Folge $A^n \longrightarrow A^n \longrightarrow P \longrightarrow 0$ entsteht. —

Satz 11.4 *Sei* M *ein endlich darstellbarer* A*-Modul,* S *eine multiplikative Teilmenge von* A. *Dann ist*

$$S^{-1}\mathrm{Hom}_A(M,N) \xrightarrow{\varphi} \mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$$

ein Isomorphismus.

Beweis: a) Sei zunächst M ein endlicher, freier A-Modul, also $M \simeq A^n$ für geeingetes $n \in \mathbb{N}$. Dann gilt $S^{-1}\mathrm{Hom}_A(M,N) \simeq S^{-1}N^n$, $\mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) \simeq \mathrm{Hom}_{S^{-1}A}((S^{-1}A)^m,S^{-1}N) \simeq (S^{-1}N)^n$.

b) Sei nun $A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$ eine exakte Sequenz von A-Moduln. Dann hat man folgendes kommutative Diagramm mit exakten Zeilen:

$$\begin{array}{ccccccc}
0 \longrightarrow & S^{-1}\mathrm{Hom}_A(M,N) & \longrightarrow & S^{-1}\mathrm{Hom}_A(A^n,N) & \longrightarrow & S^{-1}\mathrm{Hom}_A(A^m,N) \\
& \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\wr} & & \downarrow{\scriptstyle\wr} \\
0 \longrightarrow & \mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) & \longrightarrow & \mathrm{Hom}_{S^{-1}A}(S^{-1}A^n,S^{-1}N) & \longrightarrow & \mathrm{Hom}_{S^{-1}A}(S^{-1}A^m,S^{-1}N) .
\end{array}$$

Daher ist φ ein Isomorphismus. —

Bemerkung 11.5 Ist M lediglich ein endlich erzeugter A-Modul, so ist φ injektiv.

Folgerung 11.6 *Ein endlich darstellbarer* A*-Modul* P *ist projektiv genau dann, wenn* $P_{\mathfrak{m}}$ *ein projektiver* $A_{\mathfrak{m}}$*-Modul für jedes maximale Ideal* $\mathfrak{m}$ *von* A *ist.*

Beweis: "$\Rightarrow$": Für alle Ringhomomorphismen $A \longrightarrow B$ ist $B \otimes_A P$ projektiv gemäß 10.25 b).

"$\Leftarrow$": Sei $M \longrightarrow M' \longrightarrow 0$ exakt. Dann ist für alle maximalen Ideale $\mathfrak{m}$ von A auch $M_{\mathfrak{m}} \longrightarrow M'_{\mathfrak{m}} \longrightarrow 0$ exakt. Da $P_{\mathfrak{m}}$ projektiver $A_{\mathfrak{m}}$-Modul ist, ist $\mathrm{Hom}_{A_{\mathfrak{m}}}(P_{\mathfrak{m}},M_{\mathfrak{m}}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{m}}}(P_{\mathfrak{m}},M'_{\mathfrak{m}}) \longrightarrow 0$ exakt, und diese Sequenz ist nach Satz 11.4 isomorph zu $\mathrm{Hom}_A(P,M)_{\mathfrak{m}} \longrightarrow \mathrm{Hom}_A(P,M')_{\mathfrak{m}} \longrightarrow 0$. Man hat deshalb die exakte Sequenz $\bigoplus_{\mathfrak{m}} \mathrm{Hom}_A(P,M)_{\mathfrak{m}} \longrightarrow \bigoplus_{\mathfrak{m}} \mathrm{Hom}_A(P,M')_{\mathfrak{m}} \longrightarrow 0$, also ist auch $\bigoplus_{\mathfrak{m}} A_{\mathfrak{m}} \otimes \mathrm{Hom}_A(P,M) \longrightarrow \bigoplus_{\mathfrak{m}} A_{\mathfrak{m}} \otimes \mathrm{Hom}_A(P,M') \longrightarrow 0$ exakt (10.44,46). $\bigoplus_{\mathfrak{m}} A_{\mathfrak{m}}$ ist treuflach über A, also ist $\mathrm{Hom}_A(P,M) \longrightarrow \mathrm{Hom}_A(P,M') \longrightarrow 0$ exakt, d.h. P ist projektiv. —

Bemerkung 11.7 Sei A ein Ring, E ein A-Modul, B ein weiterer Ring, G ein B-Modul und F ein A-B-Bimodul. D.h. F ist sowohl ein

A- wie ein B-Modul, und für $a \in A$, $b \in B$, $x \in F$ ist $a(bx) = b(ax)$. Dann sind $F \otimes_B G$ und $E \otimes_A F$ auch A-B-Bimoduln, und man hat einen in E,F,G natürlichen Isomorphismus $E \otimes_A (F \otimes_B G) \simeq (E \otimes_A F) \otimes_B G$. Dies beweist man wie Satz 10.48.

Satz 11.8 *Es seien* M, N *A-Moduln,* S *eine multiplikative Teilmenge von* A. *Dann gilt:*

$$S^{-1}(M \otimes_A N) \simeq (S^{-1}M) \otimes_A N \simeq (S^{-1}M) \otimes_A (S^{-1}N) \simeq (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N).$$

Diese Isomorphismen sind natürlich in M *und* N.

Beweis: Gemäß 10.46, 10.48 und 11.7 gilt $S^{-1}(M \otimes_A N) \simeq S^{-1}A \otimes_A M \otimes_A N \simeq S^{-1}M \otimes_A N$ sowie $S^{-1}(M \otimes_A N) \simeq S^{-1}(S^{-1}(M \otimes_A N)) \simeq S^{-1}(S^{-1}M \otimes_A N) \simeq S^{-1}M \otimes_A S^{-1}N$. Weiterhin ist $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq M \otimes_A (S^{-1}A \otimes_{S^{-1}A} S^{-1}N) \simeq M \otimes_A S^{-1}N \simeq S^{-1}M \otimes_A S^{-1}N$. —

Folgerung 11.9 *Sei* F *ein* A-*Modul. Dann gilt:*

F *ist flach über* A. $\Longleftrightarrow$ *Für alle maximalen Ideale* $\mathfrak{m}$ *von* A *ist* $F_\mathfrak{m}$ *flach über* $A_\mathfrak{m}$ *(oder* A*).*

Beweis: "$\Rightarrow$" folgt direkt aus 11.8
"$\Leftarrow$": Sei $0 \longrightarrow N \longrightarrow M$ eine exakte Folge von A-Moduln. Für jedes maximale Ideal $\mathfrak{m}$ von A ist dann

$$0 \longrightarrow F_\mathfrak{m} \otimes_{A_\mathfrak{m}} N_\mathfrak{m} \longrightarrow F_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \quad \text{exakt,}$$

also auch $0 \longrightarrow A_\mathfrak{m} \otimes_A (F \otimes_A N) \longrightarrow A_\mathfrak{m} \otimes_A (F \otimes_A M)$ nach 11.8. Nach 10.44 ist dann auch $0 \longrightarrow (\bigoplus_\mathfrak{m} A_\mathfrak{m}) \otimes_A (F \otimes_A N) \longrightarrow (\bigoplus_\mathfrak{m} A_\mathfrak{m}) \otimes_A (F \otimes_A M)$ exakt, also $0 \longrightarrow F \otimes_A N \longrightarrow F \otimes_A M$ exakt nach 10.51, da $\bigoplus_\mathfrak{m} A_\mathfrak{m}$ gemäß 10.53 treuflach ist. —

2. Projektive Moduln und Lokalisierungen

Lemma 11.10 *Es sei* M *ein endlicher* A-*Modul,* $x_1,\dots,x_n \in M$, *so daß* $(\overline{x}_1,\dots,\overline{x}_n)$ *ein Erzeugendensystem von* $M/\mathrm{Jac}(A)\cdot M$ *ist. Dann wird* M *von* $x_1,\dots,x_n$ *erzeugt.* —

Beweis: Sei $U := Ax_1 + \dots + Ax_n \subset M$. Nach Voraussetzung ist $\mathrm{Jac}(A)\cdot M + U = M$, also nach 3.20 (Nakayama) $M = U$. —

Satz 11.11 *Es sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, M ein endlicher A-Modul. Dann existiert ein endlicher freier A-Modul F und ein surjektiver Homomorphismus $f: F \longrightarrow M$, so daß $\operatorname{Ker} f \subset \mathfrak{m}F$.*

Beweis: Sei $k = A/\mathfrak{m}$ der Restklassenkörper. Gemäß 3.2 ist $M/\mathfrak{m}M$ ein $A/\mathfrak{m}$-Modul, d.h. ein k-Vektorraum. Man wähle $x_1,\dots,x_n \in M$ so, daß $\overline{x}_1,\dots,\overline{x}_n$ eine Basis des k-Vektorraums $M/\mathfrak{m}M$ bilden. Nach Lemma 11.10 bilden $x_1,\dots,x_n$ ein Erzeugendensystem von M. Also ist der Homomorphismus $A^n \xrightarrow{f} M$, $e_i \longmapsto x_i$, surjektiv.
Sei nun $\Sigma a_i e_i \in \operatorname{Ker} f$, d.h. $\Sigma a_i x_i = 0$, also $\Sigma \overline{a_i}\, \overline{x_i} = 0$.
Da $\overline{x_1},\dots,\overline{x_n}$ linear unabhängig über k sind, ist $\overline{a_i} = 0$ und deshalb $a_i \in \mathfrak{m}$ für jedes i, d.h. $\operatorname{Ker} f \subset \mathfrak{m}\cdot A^n$. –

Folgerung 11.12 *Es sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Jeder endliche projektive A-Modul P ist frei.*

Beweis: Nach 11.11 existiert eine exakte Sequenz
$0 \longrightarrow K \xrightarrow{g} F \xrightarrow{f} P \longrightarrow 0$, wobei F frei und endlich und $g(K) \subset \mathfrak{m}F$ ist. K ist endlich wegen $K \oplus P \simeq F$. Für alle A-Moduln E ist
$0 \longrightarrow K \otimes E \xrightarrow{g \otimes E} F \otimes E \xrightarrow{f \otimes E} P \otimes E \longrightarrow 0$ exakt.
Denn, da P projektiv ist, existiert ein $h: F \longrightarrow K$ mit $h \circ g = \mathrm{id}_K$.
Dann ist $(h \otimes E) \circ (g \otimes E) = \mathrm{id}_{K \otimes E}$, und somit ist $g \otimes E$ injektiv.
Man betrachte nun $E = A/\mathfrak{m}$.

Da $0 \longrightarrow K/\mathfrak{m}K \xrightarrow{g \otimes (A/\mathfrak{m})} F/\mathfrak{m}F \xrightarrow{\sim} P/\mathfrak{m}P \longrightarrow 0$ exakt und $g \otimes (A/\mathfrak{m}) = 0$ ist, ist $K/\mathfrak{m}K = 0$, also $K = 0$ nach 3.19 (Nakayama). –

Lemma 11.13 *Folgendes Diagramm von A-Moduln sei kommutativ mit exakten Zeilen und Spalten:*

$$\begin{tikzcd}
 & & & 0 \arrow[d] \\
 & \bullet \arrow[r, "\alpha'"] \arrow[d, "f'"'] & \bullet \arrow[r, "\beta'"] \arrow[d, "f"'] & \bullet \arrow[d, "f''"'] \\
0 \arrow[r] & \bullet \arrow[r, "\alpha"] \arrow[d, "g'"'] & \bullet \arrow[r, "\beta"] \arrow[d, "g"'] & \bullet \\
 & \bullet \arrow[r, "\alpha''"] \arrow[d] & \bullet & \\
 & 0 & &
\end{tikzcd}$$

Dann ist α'' injektiv.

Beweis: Sei $\alpha''(x) = 0$. g' ist surjektiv. Folglich gibt es ein y mit $g'(y) = x$. Für dieses gilt $g(\alpha(y)) = \alpha''(g'(y)) = \alpha''(x) = 0$, also $\alpha(y) \in \operatorname{Im} f$. D.h. es gibt ein z mit $f(z) = \alpha(y)$. Für z gilt $f''(\beta'(z)) = \beta(f(z)) = \beta(\alpha(y)) = 0$, also $\beta'(z) = 0$, da f'' injektiv ist. Somit gibt es ein w mit $\alpha'(w) = z$. Dann ist $\alpha(f'(w)) = f(\alpha'(w)) = f(z) = \alpha(y)$, und deshalb $f'(w) = y$, da α injektiv ist. Es folgt $x = g'(y) = g'(f'(w)) = 0$. —

N.B.: Diese Art von Beweis heißt Diagrammjagd. Sie geschieht weitgehend mechanisch.

Satz 11.14 *Sei* $0 \longrightarrow M' \xrightarrow{f} M \longrightarrow F \longrightarrow 0$ *eine exakte Sequenz von A-Moduln, wobei* F *flach ist. Für alle A-Moduln* E *gilt dann:*

$$f \otimes E\colon M' \otimes E \longrightarrow M \otimes E \quad \textit{ist injektiv.}$$

Beweis: Es existiert eine exakte Folge $0 \longrightarrow K \longrightarrow P \longrightarrow E \longrightarrow 0$, wobei P projektiv, insbesondere also flach ist. Man erhält daher ein kommutatives Diagramm mit exakten Zeilen und Spalten:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & M' \otimes K & \longrightarrow & M \otimes K & \longrightarrow & F \otimes K & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' \otimes P & \longrightarrow & M \otimes P & \longrightarrow & F \otimes P & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & M' \otimes E & \xrightarrow{f \otimes E} & M \otimes E & \longrightarrow & F \otimes E & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Die dritte Spalte ist exakt, da F flach ist, und die zweite Zeile ist exakt, da P flach ist. Nach obigem Lemma ist $f \otimes E$ injektiv. —

Satz 11.15 *Es sei* A *ein lokaler Ring mit maximalem Ideal* $\mathfrak{m}$, M *ein endlich darstellbarer A-Modul und* N *ein endlicher A-Modul. Weiter sei* $f\colon N \longrightarrow M$ *ein Homomorphismus, der einen Isomorphismus* $N/\mathfrak{m}N \longrightarrow M/\mathfrak{m}N$ *induziert. Dann ist* $\operatorname{Ker} f$ *endlicher A-Modul.*

Beweis: Nach 3.21 ist $f\colon N \longrightarrow M$ surjektiv.
Sei $A^m \xrightarrow{\gamma} A^n \xrightarrow{g} M \longrightarrow 0$ exakt, und $\beta\colon A^n \longrightarrow N$ ein Homomorphismus, so daß das folgende Diagramm kommutiert (A^n ist projektiv):

$$\begin{tikzcd} A^m \arrow[r] & A^n \arrow[r, "g"] \arrow[d, "\beta"] & M \arrow[r] \arrow[d, "id_M"] & 0 \\ & N \arrow[r, "f"] & M \arrow[r] & 0 \end{tikzcd}$$

Es genügt, $\operatorname{Ker} f = \beta\circ\gamma(A^m)$ zu zeigen.

Da $f\otimes(A/\mathfrak{m})$ bijektiv ist, muß $\beta\otimes(A/\mathfrak{m})$ surjektiv sein. Es folgt: β ist surjektiv nach 3.21. Wegen $0 = g\circ\gamma(A^m) = f\circ\beta\circ\gamma(A^m)$ ist $\beta\circ\gamma(A^m)\subset\operatorname{Ker} f$. Umgekehrt sei $x\in N$ mit $f(x)=0$ und $y\in A^n$ mit $\beta(y)=x$. Dann ist $g(y) = f\beta(y) = 0$. Daher existiert ein $z\in A^m$ mit $\gamma(z)=y$. Also ist $\beta\gamma(z)=\beta(y)=x$. Somit haben wir $\ker f\subset\beta\gamma(A^m)$. —

Folgerung 11.16 *Sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper k. Dann ist jeder endlich darstellbare, flache A-Modul F frei.*

Beweis: Fast wie für 11.12.

Sei $\mu_k(F/\mathfrak{m}F) = n$. Nach 11.11 (Beweis) hat man eine exakte Sequenz $0\longrightarrow K\xrightarrow{g} A^n\xrightarrow{f} F\longrightarrow 0$, wobei $K = \operatorname{Ker} f\subset\mathfrak{m}A^n$. Nach 11.15 ist K endlich. Durch Tensorieren mit $k = A/\mathfrak{m}$ erhält man wegen 11.14 die exakte Sequenz $0\longrightarrow k\otimes K\xrightarrow{k\otimes g} k^n\longrightarrow F/\mathfrak{m}F\longrightarrow 0$. Es ist $k\otimes g = 0$, daher $k\otimes K = 0$. Da K endlich ist, folgt mit 3.19 (Nakayama): $K = 0$.— (Man hätte auf 11.12 verzichten können.)

Satz 11.17 *Für einen A-Modul P sind äquivalent:*

(*i*) *P ist endlich und projektiv.*

(*ii*) *P ist endlich darstellbar und flach.*

(*iii*) *P ist endlich darstellbar, und für jedes maximale Ideal $\mathfrak{m}$ von A ist $P_{\mathfrak{m}}$ ein freier $A_{\mathfrak{m}}$-Modul.*

Beweis: (i) ⇒ (ii) klar.

(ii) ⇒ (iii): Sei $A^m\longrightarrow A^n\longrightarrow P\longrightarrow 0$ exakt. Dann ist für alle maximalen Ideale $\mathfrak{m}$ von A die Folge $A^m_{\mathfrak{m}}\longrightarrow A^n_{\mathfrak{m}}\longrightarrow P_{\mathfrak{m}}\longrightarrow 0$ exakt.
Da P flach ist und für jeden $A_{\mathfrak{m}}$-Modul M ein natürlicher Isomorphismus $P_{\mathfrak{m}}\otimes_{A_{\mathfrak{m}}} M\simeq P\otimes_A M$ existiert (11.8), ist $P_{\mathfrak{m}}$ flach über $A_{\mathfrak{m}}$. Wende 11.16 an.

(iii) ⇒ (i): P ist natürlich endlich, und für alle maximalen Ideale $\mathfrak{m}$ ist $P_{\mathfrak{m}}$ projektiv über $A_{\mathfrak{m}}$, also ist P projektiv über A gemäß 11.6. —

Aufgaben und Hinweise

1) a) Sei $A = A_1 \times A_2$ ein direktes Produkt von zwei Ringen $A_i \neq 0$. Zeige: Für jede Indexmenge $I \neq \emptyset$ ist $A_1^{(I)}$ ein projektiver nicht freier A-Modul.
Beachte: Wenn ein Ring A lokal ist oder nur ein minimales Primideal besitzt (etwa integer ist), dann läßt A sich nicht (mit Faktoren $\neq 0$) direkt zerlegen.
b) Ein weniger banales Beispiel eines nichtfreien projektiven Moduls findet sich in 12.A 4.

2) a) Zu injektiven Moduln siehe 13.A 16 f.

b) Nichttriviale flache Moduln werden in 13. A 13 ff konstruiert.

3) Zeige: A ist genau dann nicht (nicht-trivial) direkt zerlegbar, wenn Spec A zusammenhängend ist. (Vgl. [Bourbaki] chap. II §4.3 prop. 15 und 1. A6.)

4) a) Wenn A nicht (nicht-trivial) direkt zerlegbar und noethersch ist, ist jeder nicht endliche projektive A-Modul frei. Siehe [Bass 1]. Beachte A 3.
b) Wenn A lokal (aber nicht notwendig noethersch) ist, gilt dies auch. D.h. jeder projektive A-Modul ist frei.
Siehe loc. cit. oder [Kaplansky] .

5) Sei S eine multiplikative Teilmenge eines Ringes A und M ein $S^{-1}A$-Modul. Zeige: M ist genau dann flach, wenn M als A-Modul flach ist.

6) Sei $\varphi\colon A \longrightarrow B$ ein Ringhomomorphismus und M ein B-Modul. Zeige: M ist genau dann als A-Modul flach, wenn $M_{\mathfrak{m}}$ ein flacher A-Modul ist für jedes maximale Ideal $\mathfrak{m}$ von B. (Nach A5 ist $M_{\mathfrak{m}}$ ein flacher A-Modul, wenn $M_{\mathfrak{m}}$ ein flacher $A_{\varphi^{-1}(\mathfrak{m})}$-Modul ist.)

§12 PROJEKTIVE MODULN VOM RANG 1 UND DIVISOREN

1. Projektive Moduln vom Rang 1

Feststellung 12.1 *Seien* A *ein lokaler Ring mit maximalem Ideal* $\mathfrak{m}$, $k := A/\mathfrak{m}$ *der Restklassenkörper von* A, M *ein endlicher* A-*Modul sowie* $x_1,\dots,x_n \in M$.
Dann sind folgende Aussagen äquivalent:

(i) $(x_1,\dots,x_n)$ *ist ein kürzestes Erzeugendensystem von* M *(d.h.* n *ist minimal gewählt).*

(ii) $(x_1,\dots,x_n)$ *ist ein minimales Erzeugendensystem (d.h. für* $1 \le i \le n$ *gilt:* $(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n)$ *erzeugt* M *nicht).*

(iii) $(\overline{x}_1,\dots,\overline{x}_n)$ *ist eine Basis von* $M/\mathfrak{m}M$ *als* k-*Vektorraum, wobei* $\overline{x}_i = x_i + \mathfrak{m}M$.

Beweis: (i) $\Rightarrow$ (ii) trivial.
(ii) $\Rightarrow$ (iii): $(\overline{x}_1,\dots,\overline{x}_n)$ ist trivialerweise ein Erzeugendensystem von $M/\mathfrak{m}M$. Sei $\Sigma\, \overline{a_i}\,\overline{x_i} = 0$ $(\overline{a_i} \in k,\ \overline{a_i} = a_i + \mathfrak{m})$ eine nichttriviale Linearkombination, oBdA $\overline{a_1} \neq 0$, d.h. $\Sigma\, a_i x_i \in \mathfrak{m}M$, aber $a_1 \notin \mathfrak{m}$. Dann ist $a_1 \in A^*$, da A lokal ist, also $x_1 \in Ax_2 + \dots + Ax_n + \mathfrak{m}M$. Somit ist nach dem Lemma von Nakayama M von $x_2,\dots,x_n$ erzeugt, im Widerspruch zu (ii).

(iii) $\Rightarrow$ (i): a) $(x_1,\dots,x_n)$ ist ein Erzeugendensystem von M, denn: Sei $N = Ax_1 + \dots + Ax_n \subset M$. Da $\overline{x_1},\dots,\overline{x_n}$ Erzeugendensystme von $M/\mathfrak{m}M$ $M/\mathfrak{m}M$ ist, gilt: $N + \mathfrak{m}M = M$. Mit dem Lemma von Nakayama folgt: $M = N$.

b) $(x_1,\dots,x_n)$ ist kürzestes Erzeugendensystem von M, denn: Wäre $y_1,\dots,y_m$ mit $m < n$ ein kürzestes Erzeugendensystem, so wäre nach "(i) $\Rightarrow$ (ii) $\Rightarrow$ (iii)" auch $\overline{y_1},\dots,\overline{y_m}$ eine Basis von $M/\mathfrak{m}M$. Widerspruch! –

Definition 12.2 Für einen A-Modul M definiert man den dualen Modul

$$M^\vee := \mathrm{Hom}_A(M,A)\ .$$

Bemerkung 12.3 $(A^n)^\vee \simeq A^n$.

Beispiel 12.4 Seien A integer, $a \in A - (A^* \cup \{0\})$ und $M := A/(a) \neq 0$. Dann gilt $M^\vee \simeq 0$. Denn aus der Exaktheit der Folge $0 \longrightarrow A \xrightarrow{\cdot a} A \longrightarrow M \longrightarrow 0$ folgt die von $0 \longrightarrow M^\vee \longrightarrow \underset{A^\vee}{\overset{A}{\wr\!\wr}} \xrightarrow{\cdot a} \underset{A^\vee}{\overset{A}{\wr\!\wr}}$.
Da $A \xrightarrow{\cdot a} A$ injektiv ist, ist $M^\vee \simeq 0$.

Bezeichnungen 12.5 Wir betrachten die folgenden kanonischen Isomorphismen: $\mathrm{Hom}_A(M^\vee,M^\vee) \xrightarrow[\varphi]{\sim} \mathrm{Hom}_A(M \otimes_A M^\vee,A) \xrightarrow[\psi]{\sim} \mathrm{Hom}_A(M, \underset{\substack{\parallel \\ M^{\vee\vee}}}{\mathrm{Hom}_A(M^\vee,A)})$ (10.38).

Ferner bezeichne ε den kanonischen Auswertungshomomorphismus:

$$\varepsilon := \varphi(\mathrm{id}_{M^\vee}) : \quad M \otimes_A M^\vee \longrightarrow A$$
$$(x \otimes \alpha) \longmapsto \alpha(x) \quad ,$$

und δ bezeichne den kanonischen Homomorphismus von M in das Bidual $M^{\vee\vee}$:

$$\delta := \psi(\varepsilon) \; : \quad M \longrightarrow M^{\vee\vee}$$
$$x \longmapsto \delta(x) : M^\vee \longrightarrow A$$
$$\alpha \longmapsto \alpha(x) \quad .$$

Die genannten Bezeichnungen gelten bis 12.9.

Bemerkung 12.6 Ist M ein endlicher, projektiver A-Modul, so ist δ ein Isomorphismus.

Die Aussage ist klar für einen endlich erzeugten, freien A-Modul und daher ebenso für einen direkten Summanden. –

Satz 12.7 *Sei* M *ein* A-*Modul von endlicher Darstellung.*
Dann sind äquivalent:

(*i*) $\varepsilon: M \otimes_A M^\vee \longrightarrow A$ *ist ein Isomorphismus.*
(*ii*) *Es existiert ein* A-*Modul* N *mit* $M \otimes N \simeq A$.
(*iii*) *Für alle maximalen Ideale* $\mathfrak{m}$ *gilt:* $M_\mathfrak{m} \simeq A_\mathfrak{m}$ *über* $A_\mathfrak{m}$.
(*iv*) *Für alle* $\mathfrak{p} \in \operatorname{Spec} A$ *gilt* $M_\mathfrak{p} \simeq A_\mathfrak{p}$ *über* $A_\mathfrak{p}$.
(*v*) M *ist projektiv, und* (*iii*) (*oder* (*iv*)) *gilt.*

Bemerkung: Der Satz gilt auch unter der Voraussetzung, daß M lediglich ein endlicher A-Modul ist. Vgl. Bourbaki chap. II §5 Thm. 2 und Thm 3.

Beweis von Satz 12.7: (i) $\Rightarrow$ (ii) trivial.

(ii) $\Rightarrow$ (iii): $M \otimes_A N \xrightarrow{\sim} A$. Für jedes maximale Ideal $\mathfrak{m}$ ist also $M_\mathfrak{m} \otimes_{A_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{\sim} A_\mathfrak{m}$. D.h. o.B.d.A. ist A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper k. Wir haben Isomorphismen
$k \simeq A \otimes_A k \simeq M \otimes_A N \otimes_A k \simeq M \otimes_A (N/\mathfrak{m}N) \simeq k \otimes_A M \otimes_A (N/\mathfrak{m}N) \simeq (M/\mathfrak{m}M) \otimes_A (N/\mathfrak{m}N)$.
Dann ist $1 = \mu_k((M/\mathfrak{m}M) \otimes_A (N/\mathfrak{m}N)) = \mu_k(M/\mathfrak{m}M) \cdot \mu_k(N/\mathfrak{m}N)$, mithin $M/\mathfrak{m}M \simeq k$.
Da M endlich ist, ist M monogen nach 12.1, d.h. $M \simeq A/\mathfrak{a}$, wobei $\mathfrak{a}$ der Annullator eines erzeugenden Elements von M ist. Es folgt:

$\mathfrak{a}$ annulliert $M \otimes_A N$. Aber es ist $M \otimes_A N \simeq A$, daher $\mathfrak{a} = (0)$, d.h. $M \simeq A$.

(iii) $\Rightarrow$ (iv) Sei $\mathfrak{p} \in \operatorname{Spec} A$ und $\mathfrak{m}$ ein maximales Ideal von A mit $\mathfrak{p} \subset \mathfrak{m}$. Dann hat man einen kanonischen Isomorphismus $M_{\mathfrak{p}} \xrightarrow{\sim} (M_{\mathfrak{m}})_{\mathfrak{p}_{\mathfrak{m}}}$ sowie $(M_{\mathfrak{m}})_{\mathfrak{p}_{\mathfrak{m}}} \xrightarrow{\sim} (A_{\mathfrak{m}})_{\mathfrak{p}_{\mathfrak{m}}} \xrightarrow{\sim} A_{\mathfrak{p}}$.

(iv) $\Rightarrow$ (iii) trivial.

(iii) (bzw. (iv)) $\Rightarrow$ (v): Da M endlich darstellbar und $M_{\mathfrak{m}}$ frei über $A_{\mathfrak{m}}$ für alle maximalen Ideale $\mathfrak{m}$ von A ist, folgt mit 11.6 daß M projektiv ist.

(v) $\Rightarrow$ (i) Nach 3.45, 11.4 und 11.8 gilt die Äquivalenz:
$M \otimes_A M^{\vee} \xrightarrow{\varepsilon} A$ ist ein Isomorphismus. $\Longleftrightarrow$ Für alle maximalen Ideale $\mathfrak{m}$ von A ist $M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}^{\vee} \longrightarrow A_{\mathfrak{m}}$ ein Isomorphismus.

Für $M_{\mathfrak{m}} \simeq A_{\mathfrak{m}}$ ist die zweite Aussage aber klar. —

<u>Definition 12.8</u> Ein A-Modul M heißt projektiv vom Rang 1, wenn er von endlicher Darstellung ist und die äquivalenten Bedingungen von Satz 12.7 erfüllt (d.h. M ist projektiv, und für jedes maximale Ideal $\mathfrak{m}$ in A gilt $M_{\mathfrak{m}} \simeq A_{\mathfrak{m}}$).

<u>Satz 12.9</u> *Seien* P, P' *projektive* A-*Moduln vom Rang* 1. *Dann sind auch* $P^{\vee}$ *und* $P \otimes_A P'$ *projektiv vom Rang* 1.

<u>Beweis:</u> a) Zu $P^{\vee}$: Wie man leicht nachrechnet, ist das Diagramm

$$\begin{tikzcd}
 & P \otimes_A P^{\vee} \arrow[dl, "\delta \otimes \mathrm{id}"'] \arrow[dr, "\varepsilon_P"] & \\
P^{\vee\vee} \otimes P^{\vee} \simeq P^{\vee} \otimes P^{\vee\vee} \arrow[rr, "\varepsilon_{P^{\vee}}"'] & & A
\end{tikzcd},$$

kommutativ, und nach 12.6, 12.7(i) sind $\delta \otimes \mathrm{id}$ und ε_P Isomorphismen.

b) Daß $P \otimes_A P'$ projektiv und endlich (also endlich darstellbar) ist, zeigt man wie folgt: Wähle Q, Q', n, m so, daß $P \oplus Q \simeq A^n$, $P' \oplus Q' \simeq A^m$ gilt. Dann ist
$$A^{nm} \simeq (P \oplus Q) \otimes_A (P' \oplus Q') \simeq (P \otimes_A P') \oplus ((P \otimes_A Q') \oplus (Q \otimes_A P') \oplus (Q \otimes_A Q')).$$

$P \otimes_A P'$ ist projektiv vom Rang 1, da für jedes maximale Ideal $\mathfrak{m}$ in A gilt: $(P \otimes_A P')_{\mathfrak{m}} \simeq P_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} P'_{\mathfrak{m}} \simeq A_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} A_{\mathfrak{m}} \simeq A_{\mathfrak{m}}$. —

<u>Folgerung 12.10</u> *Die Isomorphieklassen* $[P]$ *projektiver* A-*Moduln vom Rang* 1 *bilden bezüglich des Tensorproduktes eine abelsche Gruppe mit* $[A]$ *als Neutralelement und* $[P]^{-1} = [P^{\vee}]$.

Beweis: Die Isomorphieklassen projektiver A-Moduln vom Rang 1 bilden eine Menge, da jeder endliche Modul isomorph zu einem Faktormodul von $A^{(\mathbb{N})}$ ist. Die Kommutativität und Assoziativität von "$\otimes$" ist klar, die Abgeschlossenheit folgt mit Satz 12.9. Für alle projektiven A-Moduln P vom Rang 1 gilt: $A \otimes_A P \simeq P$ und nach 12.7 auch $P \otimes_A P^\vee \simeq A$. —

Definition 12.11 Die Gruppe der Isomorphieklassen [P] projektiver A-Moduln vom Rang 1 mit dem Tensorprodukt als innerer Verknüpfung bezeichnet man als die Picardgruppe Pic A von A.
(Die Verknüpfung in Pic A wird oft additiv geschrieben. Insbesondere schreibt man Pic A = 0, wenn Pic A die triviale Gruppe ist.
In Bourbaki chap. II §5 wird Pic A mit P(A) bezeichnet.)

Satz 12.12 *Es sei* $\varphi: A \longrightarrow B$ *ein Ringhomomorphismus und* P *ein projektiver* A-*Modul vom Rang* 1. *Dann ist* $P \otimes_A B$ *ein projektiver* B-*Modul vom Rang* 1.

Beweis: $P \otimes_A B$ ist nach 10.54 projektiv und endlich. Sei nun $\mathfrak{P} \in \operatorname{Spec} B$, $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$ und $A_\mathfrak{p} \longrightarrow B_\mathfrak{P}$ der induzierte Homomorphismus. Dann gilt:
$(P \otimes_A B) \otimes_B B_\mathfrak{P} \simeq P \otimes_A B_\mathfrak{P} \simeq (P \otimes_A A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} B_\mathfrak{P} \simeq A_\mathfrak{p} \otimes_{A_\mathfrak{p}} B_\mathfrak{P} \simeq B_\mathfrak{P}$. —

Folgerung 12.13: *Ein Ringhomomorphismus* $\varphi: A \longrightarrow B$ *induziert einen Gruppenhomomorphismus:* $\operatorname{Pic}(\varphi): \operatorname{Pic}(A) \longrightarrow \operatorname{Pic}(B)$, $[P] \longrightarrow [P \otimes_A B]$. *Ferner ist diese Zuordnung funktoriell, d.h.* Pic *ist ein kovarianter Funktor.*

Beweis: $(P \otimes_A P') \otimes_A B \simeq P \otimes_A B \otimes_B P' \otimes_A B$, also ist $\operatorname{Pic}(\varphi)$ ein Homomorphismus. Ferner gilt für Ringhomomorphismen $A \longrightarrow B \longrightarrow C$:
$(P \otimes_A B) \otimes_B C \xrightarrow{\sim} P \otimes_A C$ und $P \otimes_A A \xrightarrow{\sim} P$. —

2. Invertierbare Ideale

Definition 12.14 Sei im folgenden S eine multiplikative Menge von Nichtnullteilern eines Ringes A. Ein S-Ideal von A ist ein A-Untermodul $\mathfrak{a}$ von $S^{-1}A$, für den es ein $s \in S$ mit $sA \subset \mathfrak{a} \subset s^{-1}A$ gibt.
(Wir fassen A als Unterring von $S^{-1}A$ auf.)

Bemerkungen 12.15 a) Sei $\mathfrak{a}$ ein A-Untermodul von $S^{-1}A$, für den es $s,t \in S$ gibt mit $s \in \mathfrak{a}$, $t\mathfrak{a} \subset A$. Dann ist $stA \subset \mathfrak{a} \subset (st)^{-1}A$, also $\mathfrak{a}$ ein S-Ideal.

b) Wenn $\mathfrak{a}$ ein A-Untermodul von $s^{-1}A$ ist, heißt dies, daß $s\mathfrak{a}$ ein (ganzes) Ideal von A ist. D.h. die S-Ideale sind alle von der Form $s^{-1}\mathfrak{b}$, wobei $s \in S$ und $\mathfrak{b}$ ein (gewöhnliches) Ideal von A mit $\mathfrak{b} \cap S \neq \emptyset$ ist.

c) Ist A noethersch, so sind die S-Ideale von A genau die endlichen A-Untermoduln $\mathfrak{a}$ von $S^{-1}A$ mit $\mathfrak{a} \cap S \neq \emptyset$.

Definition 12.16 Seien $\mathfrak{a},\mathfrak{b}$ S-Ideale.

a) Man definiert wie für (gewöhnliche) Ideale das Produkt $\mathfrak{a}\mathfrak{b}$ als die von allen ab mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ erzeugte additive Untergruppe von $S^{-1}A$.

b) $\mathfrak{a}:\mathfrak{b} = \{x \in S^{-1}A \mid x\mathfrak{b} \subset \mathfrak{a}\}$.

Feststellungen 12.17 *a)* $\mathfrak{a}A = \mathfrak{a}$.

b) $\mathfrak{a}\cdot\mathfrak{b}$ *und* $\mathfrak{a}:\mathfrak{b}$ *sind ebenfalls S-Ideale.*

Beweis: a) ist klar.

b) $\mathfrak{a}\cdot\mathfrak{b}$ und $\mathfrak{a}:\mathfrak{b}$ sind natürlich A-Untermoduln von $S^{-1}A$.

Es sei $sA \subset \mathfrak{a} \subset s^{-1}A$ und $tA \subset \mathfrak{b} \subset t^{-1}A$. Dann ist $(st)A \subset \mathfrak{a}\mathfrak{b} \subset (st)^{-1}A$.
Weiterhin: Aus $t\mathfrak{b} \subset A$, $sA \subset \mathfrak{a}$ folgt $st\mathfrak{b} \subset \mathfrak{a}$, also $st \in \mathfrak{a}:\mathfrak{b}$.

Sei nun $x \in \mathfrak{a}:\mathfrak{b}$, d.h. $x\mathfrak{b} \subset \mathfrak{a} \subset s^{-1}A$. Da $tA \subset \mathfrak{b}$, folgt: $xtA \subset \mathfrak{a} \subset s^{-1}A$, mithin $x \in (st)^{-1}A$. —

Satz 12.18 *Für S-Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *von* A *ist folgende Abbildung*

$$\varphi\colon \mathfrak{a}:\mathfrak{b} \longrightarrow \operatorname{Hom}_A(\mathfrak{b},\mathfrak{a})$$
$$x \longmapsto (b \longmapsto xb)$$

ein Isomorphismus.

Beweis: Offensichtlich ist φ ein Homomorphismus von A-Moduln.
Da $\mathfrak{b}$ ein $s \in S \subset (S^{-1}A)^*$ enthält, ist φ injektiv.

Die Surjektivität folgt so:
Es sei $\alpha\colon \mathfrak{b} \longrightarrow \mathfrak{a}$ eine A-lineare Abbildung, $t \in S$ ein Element mit $tA \subset \mathfrak{b} \subset t^{-1}A$. Setze $x := t^{-1}\alpha(t) \in S^{-1}A$.

Für alle $b \in \mathfrak{b}$ ist nun $\alpha(b) = xb$.
Denn wegen $tb \in A$ gilt:

$\alpha(b) = t^{-2}(t^2\alpha(b)) = t^{-2}\alpha(t^2b) = t^{-2}\alpha((tb)\cdot t) = t^{-2}((tb)\alpha(t)) =$
$t^{-1}\alpha(t)\cdot b = x\cdot b$. —

Definition 12.19 Sei $\mathfrak{a}$ ein S-Ideal von A. Setze $\mathfrak{a}^{-1} := A:\mathfrak{a} \ (\underset{12.18}{\simeq} \mathfrak{a}^{\vee})$.

Feststellungen 12.20 *Seien* $\mathfrak{a},\mathfrak{b}$ *S-Ideale von* A.

a) $\mathfrak{a}\mathfrak{a}^{-1} \subset A$.
b) Aus $\mathfrak{a}\cdot\mathfrak{b} = A$ *folgt* $\mathfrak{b} = \mathfrak{a}^{-1}$.

Beweis: a) folgt direkt aus der Definition.
b) Offenbar ist $\mathfrak{b} \subset \mathfrak{a}^{-1}$, also $\mathfrak{a}\cdot\mathfrak{a}^{-1} = A$. Daher: $\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b} = \mathfrak{a}^{-1}$.

Definition 12.21 Ein S-Ideal $\mathfrak{a}$ von A heißt invertierbar, wenn es ein S-Ideal $\mathfrak{b}$ von A gibt mit $\mathfrak{a}\cdot\mathfrak{b} = A$, oder - äquivalent dazu - wenn $\mathfrak{a}\mathfrak{a}^{-1} = A$ ist.

Satz 12.22 *Sei* $\mathfrak{a}$ *ein S-Ideal von* A. *Dann sind äquivalent:*

(i) $\mathfrak{a}$ *ist invertierbar.*
(ii) $\mathfrak{a}$ *ist projektiv.*
(iii) $\mathfrak{a}$ *ist projektiv vom Rang 1 (insbesondere endlich).*

Beweis: (i) ⇒ (ii): Aus $\mathfrak{a}\mathfrak{a}^{-1} = A$ folgt $1 \in \mathfrak{a}\mathfrak{a}^{-1}$. Deshalb gibt es $a_1,\dots,a_n \in \mathfrak{a}$, $b_1,\dots,b_n \in \mathfrak{a}^{-1}$ (d.h. $b_i\mathfrak{a} \subset A$) mit: $\Sigma a_ib_i = 1$.
Man definiere Homomorphismen

$$\begin{array}{ccc} A^n \xrightarrow{f} \mathfrak{a} & & A^n \xleftarrow{g} \mathfrak{a} \\ e_i \longmapsto a_i & \text{und} & (b_1a,\dots,b_na) \longleftarrow\!\!\dashv a \end{array} .$$

(Dabei ist $e_1,\dots,e_n$ die kanonische Basis von A^n.)

Es ist $f\circ g(a) = \Sigma\, a_ib_ia = a$, d.h. $f\circ g = id_{\mathfrak{a}}$, und daher $\mathfrak{a}$ projektiv und endlich (10.25a)).
(ii) ⇒ (i): Es seien (vgl. 10.25a))

$$\begin{array}{ccc} A^{(I)} \xrightarrow{f} \mathfrak{a} & & A^{(I)} \xleftarrow{g} \mathfrak{a} \\ e_i \longmapsto a_i & \text{und} & \Sigma g_i(a)e_i \longleftarrow\!\!\dashv a \end{array}$$

Homomorphismen mit $f\circ g = id_{\mathfrak{a}}$. Für jedes $i \in I$ gibt es dann (12.18) ein $b_i\in\mathfrak{a}^{-1}\simeq\mathrm{Hom}(\mathfrak{a},A)$ mit $g_i(a) = b_ia$ für alle $a \in \mathfrak{a}$. Für jedes $a \in \mathfrak{a}$ ist aber für fast alle i $g_i(a) = 0$, mithin $b_ia = 0$. Da dies speziell für $a \in \mathfrak{a} \cap S \subset (S^{-1}A)^*$ gilt, folgt $b_i = 0$ für fast alle i.

Für $a \in \mathfrak{a}$ haben wir $a = f \circ g(a) = \Sigma a_i b_i a$. Wenn man speziell $a \in \mathfrak{a} \cap S$ wählt, kann man kürzen und erhält $\Sigma a_i b_i = 1$. Da $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{a}^{-1}$ gilt, folgt $1 \in \mathfrak{a}\mathfrak{a}^{-1}$, und somit $\mathfrak{a}\mathfrak{a}^{-1} = A$.

(i) $\Rightarrow$ (iii): Im Beweis für "(i) $\Rightarrow$ (ii)" wurde bereits gezeigt, daß projektiv und endlich ist. Nach 12.7 genügt es also, $\mathfrak{a} \otimes \mathfrak{a}^{-1} \simeq \mathfrak{a}\mathfrak{a}^{-1}$ zu zeigen; denn es ist $\mathfrak{a}\mathfrak{a}^{-1} = A$.
Da aber $\mathfrak{a}$ als A-Modul isomorph zu einem ganzen Ideal $\mathfrak{b} \subset A$ und $\mathfrak{a}^{-1}$ projektiv, also flach ist, folgt die Isomorphie aus:

Lemma 12.23 *Sei* $\mathfrak{b}$ *ein Ideal von* A *und* E *ein* A-*Modul.*
a) *Durch* $\Sigma b_i \otimes e_i \longrightarrow \Sigma b_i e_i$ *wird ein surjektiver Homomorphismus* $\varphi\colon \mathfrak{b} \otimes E \longrightarrow \mathfrak{b}E$ *definiert.*

b) *Wenn* E *flach ist, ist* φ *bijektiv.*

Beweis: a) ist klar.
b) Man hat das folgende kommutative Diagramm mit naheliegenden A-Modulhomomorphismen:

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{a} \otimes E \arrow[r] \arrow[d, "\varphi"] & A \otimes E \arrow[r] \arrow[d, "\varphi'", "\wr"'] & A/\mathfrak{a} \otimes E \arrow[r] \arrow[d, "\psi", "\wr"'] & 0 \\
0 \arrow[r] & \mathfrak{a}E \arrow[r] & E \arrow[r] & E/\mathfrak{a}E \arrow[r] & 0
\end{tikzcd}.$$

Die obere Zeile ist exakt, weil E flach ist; die untere ist es trivialerweise. Aus der Bijektivität von φ' und ψ folgt die von φ. —

Definition 12.24 Sei S eine multiplikative Menge von Nichtnullteilern in A. Dann bezeichne $\mathrm{Inv}(A,S)$ die Gruppe der invertierbaren S-Ideale, versehen mit der inneren Verknüpfung "$\cdot$".
In $\mathrm{Inv}(A,S)$ hat man die Untergruppe $H(A,S) = \{\mathfrak{a} \in \mathrm{Inv}(A,S) \mid \exists\, x \in S^{-1}A$ mit $\mathfrak{a} = Ax\}$ der invertierbaren S-Hauptideale.
$\mathrm{Inv}(A,S)\,/\,H(A,S)$ bezeichnet man als die S-Idealklassengruppe von A.

Bemerkung 12.25 Man hat nach 12.22 eine kanonische Abbildung

$$\alpha\colon \mathrm{Inv}(A,S) \longrightarrow \mathrm{Pic}(A)\ .$$

Indem man 12.23 auf $\mathfrak{b}, E \in \mathrm{Inv}(A,S)$ anwendet, sieht man, daß α ein Homomorphismus ist. Offenbar ist $\mathrm{Ker}\,\alpha = H(A,S)$. Durch α wird also eine Injektion

$$\mathrm{Inv}(A,S)\ /\ H(A,S) \hookrightarrow \mathrm{Pic}(A)$$

induziert.

Satz 12.26 *Sei* S *eine multiplikative Menge von Nichtnullteilern in* A. *Auf kanonische Weise hat man eine exakte Folge:*

$$0 \longrightarrow H(A,S) \xrightarrow{\text{Inkl.}} \mathrm{Inv}(A,S) \xrightarrow{\alpha} \mathrm{Pic}\, A \xrightarrow{\beta} \mathrm{Pic}\, S^{-1}A \quad \textit{mit} \quad \beta = \mathrm{Pic}(i_{A,S}).$$

Beweis: Zu zeigen bleibt die Exaktheit bei $\mathrm{Pic}\, A$.

$\mathrm{Im}\,\alpha \subset \mathrm{Ker}\,\beta$: Sei $\mathfrak{a} \in \mathrm{Inv}(A,S)$. Es gibt ein $s \in S$ mit $As \subset \mathfrak{a} \subset As^{-1}$. Folglich gilt $S^{-1}As \subset S^{-1}\mathfrak{a} \subset S^{-1}As^{-1}$, es ist aber $S^{-1}As = S^{-1}A = S^{-1}As^{-1}$. Es folgt $\mathfrak{a} \otimes_A S^{-1}A \simeq S^{-1}\mathfrak{a} = S^{-1}A$.

$\mathrm{Ker}\,\beta \subset \mathrm{Im}\,\alpha$: Sei $[P] \in \mathrm{Pic}\, A$ mit $\beta[P] = [S^{-1}P] = 0$. D.h. man hat einen Isomorphismus $g\colon S^{-1}P \xrightarrow{\sim} S^{-1}A$. Es gibt also $p \in P$, $s \in S$ mit $g(\frac{p}{s}) = 1$ in $S^{-1}A$.
Da P ein direkter Summand, also ein Untermodul eines freien Moduls ist, sind die Elemente von S auch Nichtnullteiler für P: Deshalb ist $i_{P,S}\colon P \longrightarrow S^{-1}P$ injektiv (3.43). Vermöge $P \xhookrightarrow{i_{P,S}} S^{-1}P \xrightarrow{g\,\sim} S^{-1}A$ ist also P isomorph zu einem A-Untermodul $\mathfrak{a}$ von $S^{-1}A$. Aus $g \circ i_{P,S}(p) = g(\frac{p}{1}) = \frac{s}{1}$ folgt $\mathfrak{a} \supset As$. Nach Definition 12.8 ist P, also $\mathfrak{a}$, endlich, und mit $\mathfrak{a} = \sum_{i=1}^{n} A\frac{a_i}{s_i}$ hat man $\mathfrak{a} \subset A(s_1 \cdot \ldots \cdot s_n)^{-1}$.
Somit ist $\mathfrak{a}$ ein S-Ideal von A, und $\mathfrak{a}$ ist invertierbar, da es projektiv ist. –

Frage: Wann kann man eine multiplikative Menge S von Nichtnullteilern in A finden, so daß $\mathrm{Pic}\, S^{-1}A = 0$ ist?

Satz 12.27 *Sei* B *ein* *semilokaler* *Ring,* P *ein endlicher, projektiver* B*-Modul. Es gebe ein* $r \in \mathbb{N}$ *mit* $P_{\mathfrak{m}} \simeq B_{\mathfrak{m}}^{r}$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* B. *Dann ist* P *frei.*

Beweis: Seien $\mathfrak{m}_1,\ldots,\mathfrak{m}_n$ die maximalen Ideale von B, $J = \mathrm{Jac}\, B = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ das Jacobsonradikal von B.

a) Spezialfall: $J = (0)$.
Nach dem Chinesischen Restsatz (1.9) hat man einen Ring-Isomorphismus $B \xrightarrow{\sim} B/\mathfrak{m}_1 \times \ldots \times B/\mathfrak{m}_n$. Diese Abbildung ist auch ein B-Modul-Isomorphismus $B \xrightarrow{\sim} \bigoplus_{i=1}^{n} (B/\mathfrak{m}_i)$. Es ist $B_{\mathfrak{m}_j} = \bigoplus_{i=1}^{n} (B/\mathfrak{m}_i)_{\mathfrak{m}_j} = B/\mathfrak{m}_j$.
Denn $B - \mathfrak{m}_j$ besteht aus Elementen, deren Homothetien auf $B/\mathfrak{m}_j$ bijektiv sind, und enthält für $i \neq j$ ein Element, das $B/\mathfrak{m}_i$ annulliert. Man hat also einen B-Modul-Isomorphismus $B \xrightarrow{\sim} \bigoplus_{i=1}^{n} B_{\mathfrak{m}_i}$. Hieraus folgt für P,

daß $P \simeq \bigoplus_{i=1}^{n} P_{\mathfrak{m}_i} \simeq \bigoplus_{i=1}^{n} B^r_{\mathfrak{m}_i} \simeq B^r$ gilt.

b) Allgemeiner Fall: Es ist $P/JP \simeq P \otimes B/J$ und nach a) frei vom Rang r über B/J. Seien $y_1,\dots,y_r \in P$, so daß $(\bar{y}_1,\dots,\bar{y}_r)$ eine Basis von B/JP ist. Wir erhalten die exakte Folge $0 \longrightarrow K \longrightarrow B^r \longrightarrow P \longrightarrow 0$.
$$e_i \longmapsto y_i$$
Da P projektiv, also flach ist, folgt die Exaktheit der induzierten Folge: $0 \longrightarrow K \otimes B/J \longrightarrow B^r \otimes B/J \xrightarrow{\sim} P \otimes B/J \longrightarrow 0$. Also ist $0 = K \otimes B/J \simeq K/JK$. Mit dem Lemma von Nakayama folgt $K = 0$. —

Folgerung 12.28 *Sei S eine multiplikative Menge von Nichtnullteilern in A. Falls $S^{-1}A$ semilokal ist, so ist die S-Idealklassengruppe von A isomorph zu* Pic A.

Beweis: Nach 12.27 ist $\mathrm{Pic}(S^{-1}A) = 0$. Wende 12.26 an. —

Beispiele 12.29 a) Für einen Integritätsring A wähle $S = A - \{0\}$.

b) Für einen reduzierten Ring mit nur endlich vielen minimalen Primidealen $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ wähle $S = A - \bigcup_{i=1}^{r} \mathfrak{p}_i$.

c) Für einen noetherschen Ring wähle $S = A - \bigcup_{\mathfrak{P} \in \mathrm{Ass}\, A} \mathfrak{P}$.

3. Divisoren und Krull-Ringe

Im folgenden sei A ein Integritätsring, K sein Quotientenkörper.

Wir übernehmen in diesem Abschnitt die folgenden allgemein üblichen Bezeichnungen:

Ein gebrochenes Ideal (sic!) ist entweder ein S-Ideal mit $S = A - (0)$ oder das Ideal (0). (D.h. ein gebrochenes Ideal ist ein A-Untermodul $\mathfrak{a}$ von K, für den es ein $x \in A - (0)$ mit $\mathfrak{a}x \subset A$ gibt.) Die gewöhnlichen Ideale werden als ganze Ideale bezeichnet.

Satz 12.30 *Folgende Aussagen (über den Integritätsring A) sind äquivalent:*

(i) *A ist ein Dedekindring.*

(ii) *Zu jedem ganzen Ideal $\mathfrak{a}$ von A gibt es ein ganzes Ideal $\mathfrak{b} \neq (0)$ von A, derart daß $\mathfrak{a}\mathfrak{b}$ ein Hauptideal ist.*

(iii) *Alle gebrochenen Ideale* $\neq (0)$ *von* A *sind invertierbar.*
(iv) *Alle ganzen Ideale* $\neq (0)$ *von* A *sind invertierbar.*
(v) *Jedes ganze Ideal* $\neq (0)$ *ist ein Produkt von maximalen Idealen.*

Beweis: "(i) $\Rightarrow$ (ii)" und "(i) $\Rightarrow$ (v)" sind unter 8.11 bewiesen.
(ii) $\Rightarrow$ (iii): Sei $\mathfrak{a}$ ein gebrochenes Ideal. Es gibt ein $x \in A - (0)$ so, daß $\mathfrak{a}x$ ganz ist, und ein ganzes Ideal $\mathfrak{b} \neq (0)$ so, daß $\mathfrak{a}x\mathfrak{b}$ ein Hauptideal $Ay \neq (0)$ ist. Dann ist $\mathfrak{a}(xy^{-1}\mathfrak{b}) = A$, also $\mathfrak{a}$ invertierbar.

(iii) $\Rightarrow$ (iv): trivial.

(iv) $\Rightarrow$ (i): Da die ganzen Ideale invertierbar sind, sind sie nach 12.22 endlich. Also ist A noethersch. Sei $\mathfrak{p} \neq (0)$ ein Primideal. Da $\mathfrak{p}$ invertierbar ist, ist $\mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$ nach 12.22 und 12.7 ein Hauptideal in $A_{\mathfrak{p}}$. Nach 8.8 ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring. Daraus folgt mit 8.10, daß A ein Dedekindring ist.
(v) $\Rightarrow$ (iv): Es genügt zu zeigen, daß jedes maximale Ideal $\mathfrak{m}$ invertierbar ist, da ein Produkt invertierbarer Ideale wieder invertierbar ist. Sei $x \in \mathfrak{m} - (0)$ und $Ax = \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_r$ mit maximalen Idealen $\mathfrak{m}_i$. Aus $\mathfrak{m} \supset \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_r$ folgt $\mathfrak{m} \supset \mathfrak{m}_i$, also $\mathfrak{m} = \mathfrak{m}_i$ für ein i. Es ist somit $\mathfrak{m} \cdot \prod_{j \neq i} \mathfrak{m}_j$ ein Hauptideal. Wie im Beweis von "(ii) $\Rightarrow$ (iii)" folgt, daß $\mathfrak{m}$ invertierbar ist. —

Folgerung 12.31 *Die gebrochenen Ideale* $\neq (0)$ *eines Dedekindringes bilden bzgl. der Multiplikation eine freie abelsche Gruppe. Eine Basis dieser Gruppe besteht aus den maximalen Idealen.*

Beweis: Die ganzen Ideale $\neq (0)$ bilden nach 8.11 eine "freie kommutative Halbgruppe" und die maximalen Ideale eine Basis derselben. Beachte: Jedes gebrochene Ideal ist Quotient zweier ganzer Ideale: Wenn $x\mathfrak{a} \subset A$ mit $x \in A - (0)$ gilt, ist $\mathfrak{a} = (x\mathfrak{a}) \cdot (Ax)^{-1}$. —

Feststellungen 12.32 *Seien* $\mathfrak{a}, \mathfrak{b}$ *nichttriviale gebrochene Ideale von* A, *ferner* $\mathfrak{a}^{-1} = A:\mathfrak{a} = \{x \in K \mid x\mathfrak{a} \subset A\}$ *(wie in Abschnitt 3).*
Dann gilt:
a) $\mathfrak{a} \subset \mathfrak{b} \Rightarrow \mathfrak{a}^{-1} \supset \mathfrak{b}^{-1}$.
b) *Für* $x \in K^*$ *ist* $(Ax)^{-1} = Ax^{-1}$.
c) *Für* $x \in K^*$ *gilt:* $\mathfrak{a} \subset Ax \Longleftrightarrow Ax^{-1} \subset \mathfrak{a}^{-1}$.
d) $\mathfrak{a}^{-1} = \{x^{-1} : \mathfrak{a} \subset Ax\} \cup \{0\}$.

Beweis: a) ist trivial.

b) Sei $y \in K$. Es gilt: $y \in (Ax)^{-1} \iff Axy \subset A \iff xy \in A \iff y \in Ax^{-1}$.

c) $\mathfrak{a} \subset Ax \iff x^{-1}\mathfrak{a} \subset A \iff x^{-1} \in \mathfrak{a}^{-1} \iff Ax^{-1} \subset \mathfrak{a}^{-1}$.

d) folgt aus c). –

Satz 12.33 *Für alle nichttrivialen gebrochenen Ideale* $\mathfrak{a}$ *gilt:*

$$(\mathfrak{a}^{-1})^{-1} = \bigcap_{\substack{x \in K \\ \mathfrak{a} \subset Ax}} Ax .$$

Beweis: "$\subset$": Sei $\mathfrak{a} \subset Ax$. Dann ist $Ax^{-1} \subset \mathfrak{a}^{-1}$, also $(\mathfrak{a}^{-1})^{-1} \subset Ax$. Es folgt $(\mathfrak{a}^{-1})^{-1} \subset \bigcap_{\mathfrak{a} \subset Ax} Ax$.

"$\supset$": Sei $y \in \bigcap_{\mathfrak{a} \subset Ax} Ax$. Für alle x mit $\mathfrak{a} \subset Ax$ gilt dann $Ax^{-1} \subset Ay^{-1}$. Da $\mathfrak{a} \subset Ax$ mit $x^{-1} \in \mathfrak{a}^{-1}$ gleichwertig ist, gilt $\mathfrak{a}^{-1} \subset Ay^{-1}$, und somit $y\mathfrak{a}^{-1} \subset A$, d.h. $y \in (\mathfrak{a}^{-1})^{-1}$. –

Bemerkung 12.34 $\mathfrak{a} \subset (\mathfrak{a}^{-1})^{-1}$.

Definition 12.35 Für ein nichttriviales gebrochenes Ideal $\mathfrak{a}$ von A definiert man:

a) $\tilde{\mathfrak{a}} := (\mathfrak{a}^{-1})^{-1} = \bigcap_{\mathfrak{a} \subset Ax} Ax$.

b) $\mathfrak{a}$ heißt divisoriell, wenn $\mathfrak{a} = \tilde{\mathfrak{a}}$ ist.

Bemerkung 12.36 $\tilde{\tilde{\mathfrak{a}}} = \tilde{\mathfrak{a}}$.

Satz 12.37 *Seien* $\mathfrak{a}, \mathfrak{b}$ *nichttriviale gebrochene Ideale in* A. *Dann sind äquivalent:*

(i) $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$

(ii) $\{x \mid \mathfrak{a} \subset Ax\} = \{x \mid \mathfrak{b} \subset Ax\}$.

(iii) $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$.

Beweis: (ii) $\iff$ (iii) gilt nach 12.33.

(i) $\Rightarrow$ (iii): $\mathfrak{a}^{-1} = \mathfrak{b}^{-1} \Rightarrow (\mathfrak{a}^{-1})^{-1} = (\mathfrak{b}^{-1})^{-1}$.

(ii) $\Rightarrow$ (i): Siehe 12.32d).

Definitionen 12.38 Seien $\mathfrak{a}, \mathfrak{b}$ nichttriviale gebrochene Ideale in A. Wir definieren eine Relation $\sim$ durch: $\mathfrak{a} \sim \mathfrak{b}$, wenn $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$.

$\mathfrak{a}$ und $\mathfrak{b}$ heißen dann quasigleich.

Die Quasigleichheit ist eine Äquivalenzrelation auf der Menge der nichttrivialen gebrochenen Ideale von A. Die Äquivalenzklasse, die ein gebrochenes Ideal $\mathfrak{a}$ enthält, bezeichnet man mit $\operatorname{div}(\mathfrak{a})$.
Die Menge der Äquivalenzklassen der nichttrivialen gebrochenen Ideale von A bezeichnet man mit $D(A)$.

Bemerkungen 12.39 a) Jede Klasse $\operatorname{div}(\mathfrak{a}) \in D(A)$ enthält genau ein divisorielles Ideal, nämlich $\tilde{\mathfrak{a}}$. Dieses ist das größte unter allen Idealen in $\operatorname{div}(\mathfrak{a})$.
b) Wenn $\mathfrak{a}$ ein invertierbares Ideal ist, ist $\mathfrak{a}$ divisoriell. Aus $\mathfrak{a}\mathfrak{a}^{-1} = A$ folgt nämlich $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$ nach 12.20. Quasigleiche invertierbare gebrochene Ideale sind also gleich. Für gebrochene Ideale von Dedekindringen (spezieller Hauptidealringen, noch spezieller diskreten Bewertungsringen) ist also Quasigleichheit dasselbe wie Gleichheit.

Satz 12.40 *Seien* $\mathfrak{a},\mathfrak{b},\mathfrak{b}'$ *nichttriviale gebrochene Ideale in* A *mit* $\operatorname{div}(\mathfrak{b}) = \operatorname{div}(\mathfrak{b}')$. *Dann gilt:*

$$\operatorname{div}(\mathfrak{a}\cdot\mathfrak{b}) = \operatorname{div}(\mathfrak{a}\cdot\mathfrak{b}').$$

Beweis: Sei $x \in K$. Dann gelten die Äquivalenzen: $\mathfrak{a}\mathfrak{b} \subset Ax$

$\Longleftrightarrow$ $a\mathfrak{b} \subset Ax$ für alle $a \in \mathfrak{a}$
$\Longleftrightarrow$ $\mathfrak{b} \subset Axa^{-1}$ für alle $a \in \mathfrak{a} - (0)$
$\Longleftrightarrow$ $\mathfrak{b}' \subset Axa^{-1}$ für alle $a \in \mathfrak{a} - (0)$
$\Longleftrightarrow$ $\mathfrak{a}\mathfrak{b}' \subset Ax$. —

Folgerung 12.41 $D(A)$ *bildet unter der Verknüpfung* $\operatorname{div}(\mathfrak{a}) + \operatorname{div}(\mathfrak{b}) := \operatorname{div}(\mathfrak{a}\cdot\mathfrak{b})$ *eine kommutative Halbgruppe mit Neutralelement* $\operatorname{div}(A)$.

Beweis: Satz 12.40 liefert die Wohldefiniertheit von "+". Alles andere ist trivial. —

Satz 12.42 *Sei* $T \subset A - (0)$ *eine multiplikative Menge, derart daß* $T^{-1}A$ *noethersch ist. Wenn* $\mathfrak{a}$ *und* $\mathfrak{b}$ *quasigleiche gebrochene Ideale von* A *sind, so sind* $T^{-1}\mathfrak{a}$ *und* $T^{-1}\mathfrak{b}$ *quasigleiche gebrochene Ideale von* $T^{-1}A$. *Durch* $\mathfrak{a} \longmapsto T^{-1}\mathfrak{a}$ *wird ein Homomorphismus* $D(A) \longrightarrow D(T^{-1}A)$ *induziert.*

Beweis: Sei $\mathfrak{a} \neq (0)$ ein gebrochenes Ideal in A mit $\mathfrak{a} \subset Ax$ für $x \in K = Q(A)$. $T^{-1}\mathfrak{a}$ ist ebenfalls ein A-Untermodul von $K = Q(A)$. Da $\mathfrak{a} \subseteq T^{-1}\mathfrak{a}$, ist $T^{-1}\mathfrak{a} \neq (0)$. Wegen $T^{-1}\mathfrak{a} \subset T^{-1}Ax$ ist $T^{-1}\mathfrak{a}$ ein gebrochenes Ideal von $T^{-1}A$. Seien $\mathfrak{a},\mathfrak{b}$ quasigleiche gebrochene Ideale und $T^{-1}\mathfrak{a} = (a_1,\ldots,a_n)T^{-1}A$. (Nach Voraussetzung ist $T^{-1}A$ noethersch.) Sei $T^{-1}\mathfrak{a} \subset T^{-1}Ax$, dann gibt es zu jedem $i = 1,\ldots,n$ ein $t_i \in T$ mit $a_i \in At_i^{-1}x$. Für $t = t_1 \ldots t_n$ gilt daher: $\mathfrak{a} \subset At^{-1}x$. Da $\mathfrak{a} \sim \mathfrak{b}$, folgt: $\mathfrak{b} \subset At^{-1}x$. Analog zeigt man: Ist $T^{-1}\mathfrak{b} \subset T^{-1}Ax$, so ist $T^{-1}\mathfrak{a} \subset T^{-1}Ax$. Also sind $T^{-1}\mathfrak{a}$ und $T^{-1}\mathfrak{b}$ quasigleich als gebrochene $T^{-1}A$-Ideale. Damit induziert die Zuordnung $\mathfrak{a} \longmapsto T^{-1}\mathfrak{a}$ eine wohldefinierte Abbildung $D(A) \longrightarrow D(T^{-1}A)$. Da offenbar $T^{-1}(\mathfrak{a}\cdot\mathfrak{b}) = (T^{-1}\mathfrak{a})\cdot(T^{-1}\mathfrak{b})$, ist die Abbildung ein Homomorphismus. —

Definition 12.43 a) Mit $P(A)$ sei die Menge der Primideale der Höhe 1 eines Ringes A bezeichnet.

b) Ein (nicht notwendig noetherscher) Ring A heißt krullsch (oder ein Krull-Ring), wenn folgendes gilt (vgl. 8.A13):

1) A ist integer;
2) $A_{\mathfrak{p}}$ ist ein diskreter Bewertungsring für jedes $\mathfrak{p} \in P(A)$;
3) jedes $a \in A - (0)$ liegt in nur endlich vielen $\mathfrak{p} \in P(A)$;
4) $\bigcap_{\mathfrak{p} \in P(A)} A_{\mathfrak{p}} = A$.

Bemerkungen 12.44 a) Ein noetherscher Integritätsring ist nach Serres Kriterium (8.14) genau dann krullsch, wenn er ganz abgeschlossen ist. Insbesondere ist jeder Dedekindring krullsch.

b) Ein Element a eines krullschen Ringes A, welches in keinem $\mathfrak{p} \in P(A)$ liegt, ist eine Einheit, da dann $a^{-1} \in A_{\mathfrak{p}}$ für alle $\mathfrak{p} \in P(A)$ und nach 4) deshalb $a^{-1} \in A$ gilt.

Bezeichnungen 12.45 Sei A ein Krull-Ring.

Zu $\mathfrak{p} \in P(A)$ gehört der diskrete Bewertungsring $A_{\mathfrak{p}}$ mit $Q(A_{\mathfrak{p}}) = Q(A)$ und deshalb eine normierte diskrete Bewertung $v_{\mathfrak{p}}$ von $Q(A)$ gemäß 8.7.

Wenn $\mathfrak{a} \neq (0)$ ein gebrochenes Ideal ist, definiere
$v_{\mathfrak{p}}(\mathfrak{a}) := \inf\{v_{\mathfrak{p}}(a) \mid a \in \mathfrak{a}\}$.

Bemerkung 12.46 Seien $A,\mathfrak{a}$ wie oben, $\mathfrak{p} \in P(A)$. Da $A_{\mathfrak{p}}$ (als DBR) ein Hauptidealring ist, gilt $\mathfrak{a}_{\mathfrak{p}} = xA_{\mathfrak{p}}$ für ein $x \in \mathfrak{a}_{\mathfrak{p}}$. In diesem Falle ist $v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(x)$. Sei nämlich $x = \frac{a}{s}$ mit $a \in \mathfrak{a}$, $s \in A - \mathfrak{p}$, so ist $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(\mathfrak{a})$. Für ein beliebiges $b \in \mathfrak{a}$ ist aber $bA_{\mathfrak{p}} \subset \mathfrak{a}_{\mathfrak{p}} = xA_{\mathfrak{p}}$, also $v_{\mathfrak{p}}(b) \geq v_{\mathfrak{p}}(x)$. Es folgt $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(\mathfrak{a})$.

Satz 12.47 *Für einen Krull-Ring* A *und von* (0) *verschiedenen gebrochene Ideale* $\mathfrak{a},\mathfrak{b}$ *von* A *gilt:*

a) *Für alle* $\mathfrak{p} \in P(A)$ *ist* $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$, *und für fast alle* $\mathfrak{p} \in P(A)$ *ist* $v_{\mathfrak{p}}(\mathfrak{a}) = 0$.

b) $\mathfrak{a}^{-1} = \{x \in Q(A) \mid \forall\, \mathfrak{p} \in P(A): v_{\mathfrak{p}}(x) \geq -v_{\mathfrak{p}}(\mathfrak{a})\}$.

c) $\mathfrak{a} \sim \mathfrak{b} \iff v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{b})$ *für alle* $\mathfrak{p} \in P(A)$.

d) *Die wegen a) und c) "⇒" wohldefinierte Abbildung*

$\varphi: D(A) \longrightarrow \mathbb{Z}^{(P(A))}$, $\operatorname{div}(\mathfrak{a}) \longmapsto (v_{\mathfrak{p}}(\mathfrak{a}))_{\mathfrak{p} \in P(A)}$

ist ein Isomorphismus. Insbesondere ist D(A) *eine Gruppe.*

Beweis: a) Es gibt ein $x \in Q(A)$ mit $Ax \subset \mathfrak{a} \subset Ax^{-1}$. Also ist $\infty > v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{a}) \geq v_{\mathfrak{p}}(x^{-1}) > -\infty$. Es gibt ein $y \in A - \{0\}$ mit $y\mathfrak{a} \subset A$. Für alle $\mathfrak{p} \in P(A)$ ist $A \subset A_{\mathfrak{p}}$, also $v_{\mathfrak{p}}(y\mathfrak{a}) \geq 0$ und $v_{\mathfrak{p}}(y) \geq 0$. Da für jedes $a \in A - (0)$ die Menge $\{\mathfrak{p} \in P(A) \mid v_{\mathfrak{p}}(a) > 0\}$ nach Definition 12.43.3) endlich ist, sind die Mengen $\{\mathfrak{p} \in P(A) \mid v_{\mathfrak{p}}(y) > 0\}$ und $\{\mathfrak{p} \in P(A) \mid v_{\mathfrak{p}}(\mathfrak{a}y) > 0\}$ endlich. Aus $v_{\mathfrak{p}}(y\mathfrak{a}) = v_{\mathfrak{p}}(y) + v_{\mathfrak{p}}(\mathfrak{a})$ folgt dann die Endlichkeit der Menge $\{\mathfrak{p} \in P(A) \mid v_{\mathfrak{p}}(\mathfrak{a}) \neq 0\}$.

b) Für ein gebrochenes Ideal $\mathfrak{b}$ gilt:
$\mathfrak{b} \subset A \iff \mathfrak{b} \subset A_{\mathfrak{p}}$ für alle $\mathfrak{p} \in P(A) \iff v_{\mathfrak{p}}(\mathfrak{b}) \geq 0$ für alle $\mathfrak{p} \in P(A)$.
Also ist $\mathfrak{a}^{-1} = \{x \in Q(A) \mid x\mathfrak{a} \subset A\} = \{x \in Q(A) \mid \forall\, \mathfrak{p} \in P(A): v_{\mathfrak{p}}(x\mathfrak{a}) \geq 0\}$
$= \{x \in Q(A) \mid \forall\, \mathfrak{p} \in P(A): v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\mathfrak{a}) \geq 0\}$.

c) "⇒": Aus $\mathfrak{a} \sim \mathfrak{b}$ folgt $\mathfrak{a}_{\mathfrak{p}} \sim \mathfrak{b}_{\mathfrak{p}}$ mit Satz 12.42, da $A_{\mathfrak{p}}$ noethersch ist. Hieraus folgt $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$, nach 12.39 b), denn $A_{\mathfrak{p}}$ ist ein DBR. Wegen 12.46 ist dann $v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{b})$.
"⇐": Da $v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{b})$ für alle $\mathfrak{p} \in P(A)$ gilt, ist $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$ nach b). D.h. es ist $\mathfrak{a} \sim \mathfrak{b}$.

d) Wie man sich etwa mittels 12.46 leicht überzeugt, gilt:
$v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$. Also ist φ ein Homomorphismus. Wegen c) "⇐" ist φ injektiv. Da für $\mathfrak{q} \in P(A)$ gilt:

$$v_{\mathfrak{p}}(\mathfrak{q}) = \begin{cases} 1 & \text{für } \mathfrak{p} = \mathfrak{q} \\ 0 & \text{sonst} \end{cases},$$

ist φ surjektiv. —

Folgerung 12.48 *Unter den Voraussetzungen des Satzes gilt:*

a) $\mathfrak{a}\mathfrak{a}^{-1} \sim A$, *d.h.* $\operatorname{div}(\mathfrak{a}^{-1}) = -\operatorname{div}(\mathfrak{a})$;

b) $v_{\mathfrak{p}}(\mathfrak{a}^{-1}) = -v_{\mathfrak{p}}(\mathfrak{a})$ *für alle* $\mathfrak{p} \in P(A)$;

c) $\tilde{\mathfrak{a}} = \{x \in Q(A) \mid \forall\, \mathfrak{p} \in P(A): v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{a})\}$.

Beweis: a) Da D(A) eine Gruppe ist, gibt es ein gebrochenes Ideal $\mathfrak{b}$ mit $\mathfrak{a}\mathfrak{b} \sim A$. Es folgt $(\mathfrak{a}\mathfrak{b})^{\sim} = A$, da A als Hauptideal divisoriell ist.

Insbesondere ist $\mathfrak{a}\mathfrak{b} \subset A$, also $\mathfrak{b} \subset \mathfrak{a}^{-1}$. Es folgt $(\mathfrak{a}\mathfrak{b})^{\sim} \subset (\mathfrak{a}\mathfrak{a}^{-1})^{\sim} \subset A$, und deshalb $(\mathfrak{a}\mathfrak{a}^{-1})^{\sim} = A$, d.h. a).
b) folgt aus a) und der Tatsache, daß φ ein Gruppenhomomorphismus ist.
c) folgt aus b) und 12.47 b). —

Bemerkungen 12.49 a) Quasigleichheit bedeutet nicht immer Gleichheit. Beispiel: Sei A ein ganz abgeschlossener noetherscher Integritätsring mit $\dim A > 1$. Dann gibt es ganze Ideale $\mathfrak{a} \neq A$ von A, die in keinem $\mathfrak{p} \in P(A)$ enthalten sind. Für solche $\mathfrak{a}$ gilt $\tilde{\mathfrak{a}} = A$ nach 12.47 c).

b) Satz 12.47 d) soll als eine Art Satz über eindeutige Primfaktorzerlegung verstanden werden. Er besagt nämlich: Jedes ganze Ideal $\neq (0)$ des Krull-Ringes A ist quasigleich einem (bis auf die Reihenfolge) eindeutigen Produkt gewisser $\mathfrak{p} \in P(A)$. Einzelheiten überlassen wir dem Leser.

c) Aus 12.47 folgt auch die Aussage: Aufsteigende Folgen ganzer divisorieller Ideale eines Krull-Ringes werden stationär. Sind nämlich $\mathfrak{a}, \mathfrak{b}$ divisoriell, so ist "$\mathfrak{a} \subset \mathfrak{b}$" nach 12.47 b) und d) äquivalent zu "$v_{\mathfrak{p}}(\mathfrak{a}) \geq v_{\mathfrak{p}}(\mathfrak{b})$ für alle $\mathfrak{p} \in P(A)$". Und genau dann ist $\mathfrak{a}$ ganz, wenn $v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ für alle $\mathfrak{p} \in P(A)$ ist.

Bemerkungen und Definition 12.50 a) Sei A integer und $H(A)$ die Gruppe der gebrochenen Hauptideale $\neq (0)$ von A. Da Hauptideale divisoriell sind (12.39 b)), ist die kanonische Abbildung $H(A) \longrightarrow D(A)$ ein injektiver Homomorphismus. Wir fassen $H(A)$ als Untergruppe von $D(A)$ auf und nennen die Restklassenhalbgruppe $D(A)/H(A)$ die Divisorenklassenhalbgruppe $C(A)$ von A.
Wenn A krullsch ist, hat man eine Divisorenklassengruppe.
b) Sei $\mathrm{Inv}(A) = \mathrm{Inv}(A, A-(0))$ die Gruppe der invertierbaren Ideale. Auch die kanonische Abbildung $\mathrm{Inv}(A) \longrightarrow D(A)$ ist ein injektiver Homomorphismus. Nach Identifizierung erhält man Inklusionen $H(A) \subset \mathrm{Inv}(A) \subset D(A)$ und deshalb eine Inklusion $\mathrm{Pic}\, A \subset C(A)$ wegen 12.29. Genauer: $\mathrm{Pic}\, A$ ist auf kanonische Weise eine Untergruppe der Divisorenklassenhalbgruppe (bzw. der Divisorenklassengruppe, wenn A krullsch ist).

Beachte: Für einen Dedekindring A gilt $\mathrm{Pic}\, A = C(A)$.

Satz 12.51: *Sei* A *ein Integritätsring. Dann sind äquivalent:*

(i) A *ist faktoriell.*

(ii) A *ist krullsch und* $C(A) = 0$.

(iii) (a) Jede aufsteigende Folge von ganzen Hauptidealen wird stationär;

(b) *jedes divisorielle Ideal ist ein Hauptideal.*

(iv) (a) *Jede aufsteigende Folge von ganzen Hauptidealen wird stationär;*

(b) *für alle* $a,b \in A$ *ist* $\widetilde{(a,b)}$ $(:= (Aa+Ab)^{\sim})$ *ein Hauptideal.*

Beweis: (i) ⇒ (ii): Jedes $\mathfrak{p} \in P(A)$ ist von einem Primelement von A erzeugt: Sei nämlich $a \in \mathfrak{p} - (0)$ und $a = up_1 \cdot \ldots \cdot p_r$ mit $u \in A^*$, p_i prim. Da $u \notin \mathfrak{p}$, gibt es ein $j \in \{1,\ldots,r\}$ mit $p_j \in \mathfrak{p}$. Da $\operatorname{ht}\mathfrak{p} = 1$ und (p_j) ein Primideal ist, folgt $\mathfrak{p} = (p_j)$. Wir zeigen jetzt, daß die Bedingungen aus Definition 12.43 b) erfüllt sind:
Nach Voraussetzung ist A integer, d.h. 1) gilt.
Sei $\mathfrak{p} = (p) \in P(A)$. Es ist klar, daß $A_{\mathfrak{p}}$ ein faktorieller Ring mit im wesentlichen nur einem Primideal ist. Wende nun Satz 8.8 "(v) ⇒ (i)" an, und beachte dabei, daß die Voraussetzung, daß A noethersch sei, für den Beweis der Implikation (v) ⇒ (i) nicht nötig ist. Es folgt 2).

Zu 3): $a \in (p) \iff p \mid a$. Jedes $a \in A - (0)$ hat aber nur endlich viele Primteiler.

Zu 4): Sei $x \in Q(A)$, $x = up_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$ mit $u \in A^*$, $n_i \in \mathbb{Z}$, p_i zu p_j mit $i \neq j$ nicht assoziiert. Nun bedeutet offenbar $x \in \bigcap_{\mathfrak{p} \in P(A)} A$, daß $n_i \geq 0$ für $i = 1,\ldots,r$, also $x \in A$ ist.

Wir haben gezeigt, daß A ein Krull-Ring ist.

Sei $\mathfrak{a}$ ein gebrochenes Ideal. Das Hauptideal $\prod_{\mathfrak{p} \in P(A)} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$ hat unter φ (aus 12.47 d)) das gleiche Bild wie $\mathfrak{a}$. Es folgt: Jedes $\operatorname{div}(\mathfrak{a}) \in D(A)$ liegt bereits in $H(A)$. Deshalb ist $C(A) = D(A)/H(A) = 0$.

(ii) ⇒ (iii): Zu (a): Hauptideale sind divisoriell, und aufsteigende Folgen ganzer divisorieller Ideale in Krull-Ringen werden stationär gemäß 12.49 c). Zu (b): $C(A) = 0 \iff H(A) = D(A) \iff$ (b).
(iii) ⇒ (iv) ist trivial.

(iv) ⇒ (i): Aus (iv) (a) folgt, daß sich jedes Element von $A - \{0\}$ als Produkt einer Einheit mit irreduziblen Elementen schreiben läßt.
Es genügt jetzt, noch folgendes zu zeigen:

Behauptung: Ist $p \in A$ irreduzibel, dann ist p ein Primelement.

Beweis hierfür: Es sei p irreduzibel, $a,b \in A$ mit: $p \mid ab$, $p \nmid a$.
Zu zeigen ist: $p \mid b$.

Sei $\widetilde{(a,p)} = dA$. Es ist $d \in A$, denn aus $\mathfrak{a} \subset A$ folgt $\tilde{\mathfrak{a}} \subset A$.

Wegen $(a,p) \subset (d)$ ist $d \mid a$ und $d \mid p$. Da p irreduzibel und kein Teiler von a ist, muß $d \in A^*$ gelten. Daher ist $(b) = bA = bdA = b\widetilde{(a,p)} = \widetilde{(ab,pb)}$. Also gilt für alle $x \in Q(A)$ mit $(ab,pb) \subset Ax$, daß $(x) \supset (b)$.
Nach Voraussetzung ist $p \mid ab$, ferner $p \mid pb$, also $Ap \supset (ab,pb)$.
Daher haben wir $Ap \supset Ab$, d.h. $p \mid b$. –

Folgerung 12.52 *Ist A faktoriell, so ist* $\operatorname{Pic} A = 0$.

Beweis: Nach 12.50 ist $\operatorname{Pic} A \subset C(A)$.

Aufgaben und Hinweise

1) Zeige: Ein freies Ideal in einem (kommutativen) Ring A ist immer ein Hauptideal (welches von einem Nichtnullteiler erzeugt wird). (N.B.: In nichtkommutativen Ringen gilt dies nicht immer.)

2) Zeige: In einem Krull-Ring A umfaßt jedes von (0) verschiedene Primideal $\mathfrak{q}$ ein $\mathfrak{p} \in P(A)$. (Sei $a \in \mathfrak{q}-(0)$. Dann ist $(a) \sim \prod_{i=1}^{m} \mathfrak{p}_i$ mit $\mathfrak{p}_i \in P(A)$. Es folgt $\mathfrak{q} \supset \prod_{i=1}^{m} \mathfrak{p}_i$.)

3) Zeige: Ein Krull-Ring A, in dem jedes Primideal $\neq (0)$ maximal ist (d.h. $P(A)$ aus lauter maximalen Idealen besteht), ist ein Dedekindring. ($\mathfrak{a}\mathfrak{a}^{-1} \sim A$, also $\mathfrak{a}\mathfrak{a}^{-1} \not\subset \mathfrak{p}$ für alle $\mathfrak{p} \subset P(A)$. Es folgt $\mathfrak{a}\mathfrak{a}^{-1} = A$.)

4) a) Sei $A = \mathbb{Z}$ oder $A = k[X]$ mit einem endlichen Körper k, $L \supset Q(A)$ eine endliche Körpererweiterung und B der ganze Abschluß von A in L. Dann ist $\operatorname{Pic} B$ endlich. Dieser (nichttriviale) Satz findet sich in vielen Büchern über Algebraische Zahlentheorie und Funktionenkörper. Wir verweisen auf [Swan-Evans] Theorem 3.9.

   b) Andererseits ist in dieser Situation meistens $\operatorname{Pic} B \neq 0$. Gewisse Ideale von B sind dann projektive nichtfreie B-Moduln. Ein explizites Beispiel erhält man wie folgt:

   Sei $A = \mathbb{Z}$ und $L = Q(\sqrt{-5})$. Nach 7.A2 ist $B = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{-5}$. Das Ideal $\mathfrak{a} := (3, 1+\sqrt{-5})$ von B ist invertierbar, also projektiv, da B ein Dedekindring ist, aber kein Hauptideal, also nach A1 nicht frei: Zeige - mit Hilfe der Norm -, daß 3 und $1+\sqrt{-5}$ in B irreduzibel sind. Folgere: $\mathfrak{a}$ ist in keinem echten ganzen Hauptideal enthalten. Es gilt aber $\mathfrak{a} \neq B$.

5) Sei A ein Krull-Ring; zu $\mathfrak{p} \in P(A)$ sei mit $v_{\mathfrak{p}}$ die zugehörige Bewertung von $Q(A)$ bezeichnet. Seien $\mathfrak{p}_1,\ldots,\mathfrak{p}_r \in P(A)$ und $n_1,\ldots,n_r \in \mathbb{Z}$ (mit $r < \infty$). Zeige: Es gibt ein $x \in Q(A)$ mit $v_{\mathfrak{p}_i}(x) = n_i$ für $i = 1,\ldots,r$ und $v_{\mathfrak{p}}(x) \geq 0$ für $\mathfrak{p} \in P(A) - \{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$. (Sei $S = A - \bigcup\limits_{i=1}^{r} \mathfrak{p}_i$. Wende 8.A10 auf $S^{-1}A$ an.)

6) Sei A krullsch. Zeige: Jedes gebrochene divisorielle Ideal $\mathfrak{a}$ von A ist Durchschnitt zweier gebrochener Hauptideale. (Nach Definition gibt es ein $y \in Q(A)$ mit $\mathfrak{a} \subset Ay$. Finde mit Hilfe von A5 ein $x \in Q(A)$ so, daß

"$a \in \mathfrak{a} \iff v_{\mathfrak{p}}(a) \geq \operatorname{Max}(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$ für alle $\mathfrak{p} \in P(A)$"

gilt.

7) Wenn A integer und M ein A-Modul ist, versteht man unter der Torsion von M den Untermodul $T(M) := \{x \in M \mid \exists\, a \in A - \{0\} \text{ mit } ax = 0\}$.

Seien A ein Krull-Ring, $\mathfrak{a}, \mathfrak{b}$ gebrochene Ideale. Zeige:

a) $\mathfrak{a}\mathfrak{b} \simeq (\mathfrak{a} \otimes \mathfrak{b})/T(\mathfrak{a} \otimes \mathfrak{b})$. (Es ist $(\mathfrak{a} \otimes \mathfrak{b})_{\mathfrak{p}} \simeq (\mathfrak{a}\mathfrak{b})_{\mathfrak{p}}$ für $\mathfrak{p} \in P(A)$.)

b) $\operatorname{div}(\mathfrak{a})$ und $\operatorname{div}(\mathfrak{b})$ haben in $C(A)$ dasselbe Bild genau dann, wenn $\tilde{\mathfrak{a}} \simeq \tilde{\mathfrak{b}}$ ist.

8) a) Sei $f: A \longrightarrow B$ ein Homomorphismus krullscher Ringe mit folgender Eigenschaft:

(*) Wenn $\mathfrak{p} \in P(B)$ und $\mathfrak{q} = f^{-1}(\mathfrak{p})$ ist, so ist $A_{\mathfrak{q}}$ faktoriell.

In diesem Fall kann man einen kanonischen Homomorphismus $C(f): C(A) \longrightarrow C(B)$ wie folgt angeben:

Repräsentiere $\alpha \in C(A)$ durch ein $\operatorname{div}(\mathfrak{a})$, wobei $\mathfrak{a}$ divisoriell und ganz sei. Dann ist $\mathfrak{a}$ bis auf Isomorphie eindeutig bestimmt (A7b)). Dann ist $\mathfrak{a} \otimes_A B / T_B(\mathfrak{a} \otimes B)$ (wo T_B die Torsion als B-Modul bezeichnet) isomorph zu einem Ideal $\neq (0)$ in B. (Aus der Inklusion $\mathfrak{a} \hookrightarrow A$ ergibt sich nämlich ein Homomorphismus: $\mathfrak{a} \otimes_A B \longrightarrow B$, dessen Kern $T_B(\mathfrak{a} \otimes_A B)$ ist. Wegen (*) ist $\mathfrak{a}_{\mathfrak{q}} \simeq A_{\mathfrak{q}}$ für $\mathfrak{q} = f^{-1}(\mathfrak{p})$ und $\mathfrak{p} \in P(B)$.) $C(f)(\alpha)$ sei die Klasse dieses Ideals. Wegen A7b) ist $C(f)$ wohldefiniert. Es bleibt noch zu zeigen,

daß $C(f)$ ein Homomorphismus ist: Seien $\mathfrak{a}, \mathfrak{b}$ divisorielle Ideale in A und $\mathfrak{p} \in P(B)$. Für $\mathfrak{p} \in P(B)$ und $\mathfrak{q} = f^{-1}(\mathfrak{p})$ ist $(\mathfrak{a} \otimes_A \mathfrak{b})_\mathfrak{q} \simeq (\mathfrak{a}\mathfrak{b})_\mathfrak{q}$.
(Mit Hilfe von A6 und 10.A12 sieht man, daß $\mathfrak{a}_\mathfrak{q}$ und $\mathfrak{b}_\mathfrak{q}$ divisoriell in $A_\mathfrak{q}$, also nach (*) Hauptideale sind.)
Es folgt $\mathfrak{a} \otimes_A \mathfrak{b} \otimes_A B_\mathfrak{p} \simeq (\mathfrak{a}\mathfrak{b}) \otimes_A B_\mathfrak{p}$ für $\mathfrak{p} \in P(B)$. Deshalb sind $(\mathfrak{a}\mathfrak{b}) \otimes_A B$ und $\mathfrak{a} \otimes_A \mathfrak{b} \otimes_A B \simeq \mathfrak{a} \otimes_A B \otimes_B \mathfrak{b} \otimes_A B$ bis auf Torsion isomorph. Mit A7a) erhält man, daß $C(f)$ ein Homomorphismus ist.

b) Wenn $g: B \longrightarrow C$ ein weiterer Homomorphismus krullscher Ringe ist und f, g und $g \circ f$ die Bedingung (*) erfüllen, gilt $C(g \circ f) = (C(g) \circ C(f)$.

c) Sei $f: A \hookrightarrow B$ ein injektiver Homomorphismus krullscher Ringe. Dann heißt f (eine Erweiterung) ohne Aufblasung, wenn für jedes $\mathfrak{p} \in P(B)$ gilt: $f^{-1}(\mathfrak{p}) \in P(A) \cup \{(0)\}$.
(Bedingung (PDE) in [Bourbaki] chap. VII §1 no. 10 und in [Fossum] §6.) Eine Erweiterung ohne Aufblasung erfüllt (*). Bei Erweiterungen ohne Aufblasung kann man sogar auf kanonische Weise einen Homomorphismus $D(A) \longrightarrow D(B)$ definieren, der $H(A)$ in $H(B)$ abbildet. Flache und ganze Erweiterungen sind ohne Aufblasung (loc. cit.).

d) Zu Berechnungen von Divisorenklassengruppen, die o.a. funktorielle Eigenschaften ausnutzen, siehe [Samuel], [Fossum], auch [Bourbaki] chap. VII, hauptsächlich in den "Exercices".

e) Das vielleicht wichtigste Hilfsmittel bei der Berechnung von Divisorenklassengruppen ist folgender Satz von Nagata (den der Leser beweisen möge):
Sei S eine multiplikative Menge in einem Krull-Ring A. Dann ist $C(A) \longrightarrow C(S^{-1}A)$ surjektiv und der Kern von den Klassen derjenigen $\operatorname{div}(\mathfrak{p})$ erzeugt, für die $\mathfrak{p} \in P(A)$ und $\mathfrak{p} \cap S \neq \emptyset$ gilt.

Insbesondere zeigt man hiermit $C(A) = C(A[X])$. Siehe [Bourbaki] chap. VII §1 Prop. 18.

9) Sei A ein noetherscher oder krullscher Integritätsring, in dem jedes $\mathfrak{p} \in P(A)$ ein Hauptideal ist. Zeige: A ist faktoriell.

10) Bestimme die Primideale von $\mathbb{Z}[X]$. (Die Primideale der Höhe 1 sind Hauptideale, erzeugt von Primzahlen oder Polynomen vom Inhalt 1, die über $\mathbb{Q}[X]$ irreduzibel sind. Die Primideale der Höhe 2 sind von der

Form (p,f), wo p eine Primzahl und f modulo p irreduzibel ist.

§13 HOMOLOGISCHE DIMENSION

1. Injektive Moduln

Sei A ein Ring. Nach 3.14a) gibt es zu jedem A-Modul M eine exakte Folge $P_0 \longrightarrow M \longrightarrow 0$ mit einem projektiven (etwa freien) A-Modul P_0, also eine unendlich lange exakte Folge $\ldots P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ mit projektiven P_i. Wir wollen hier (13.6) zeigen, daß jeder A-Modul sich in einen injektiven einbetten läßt, es also eine unendlich lange exakte Folge $0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \ldots$ mit injektiven I^j gibt.

Satz 13.1 (Baer) *Ein A-Modul I ist genau dann injektiv, wenn folgendes gilt:*
Für jedes Ideal $\mathfrak{a}$ von A und jede A-lineare Abbildung $\varphi: \mathfrak{a} \longrightarrow I$ existiert eine Fortsetzung auf A (d.h. ein $\bar{\varphi}: A \longrightarrow I$ mit $\bar{\varphi}|\mathfrak{a} = \varphi$).

Beweis: Seien $N \subset M$ A-Moduln und $f: N \longrightarrow I$ ein A-Modulhomomorphismus. Definiere

$$\mathfrak{M} := \left\{(E,g) \mid E \text{ A-Modul mit } N \subset E \subset M,\ E \xrightarrow{g} I \text{ A-linear mit } g|_N = f\right\}.$$

Auf $\mathfrak{M}$ führt man eine Ordnung ein durch:

$$(E,g) \le (E',g') \iff E \subset E' \text{ und } g'|_E = g.$$

$\mathfrak{M}$ ist nichtleer, da $(N,f) \in \mathfrak{M}$, und, wie man leicht sieht, induktiv geordnet.
(E,g) sei nun ein maximales Element in $\mathfrak{M}$. Dann ist $E = M$ und g die gesuchte Fortsetzung von f auf M; denn:

Annahme: Es gibt $x \in M - E$.
Dann läßt sich g fortsetzen zu einem Homomorphismus $E + Ax \longrightarrow I$ im Widerspruch zur Maximalität von (E,g).
Beweis hierfür: Sei $\mathfrak{a}$ folgendes Ideal: $\mathfrak{a} := \{a \in A \mid ax \in E\}$.
Dann ist $\mathfrak{a} = \varphi^{-1}(E)$, wobei $\varphi: A \longrightarrow M$ durch $a \longmapsto ax$ definiert ist.
Nach Voraussetzung läßt sich $g \circ \varphi|_{\mathfrak{a}}$ fortsetzen zu einem Homomorphismus $\psi: A \longrightarrow I$, d.h. man ist in folgender Situation:

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[rrd, "\psi"] & M & \\
\mathfrak{a} \arrow[u, hook] \arrow[r, "\varphi|_{\mathfrak{a}}"] & E \arrow[u, hook] \arrow[r, "g"] & I
\end{tikzcd}$$

Man definiert $h: E + Ax \longrightarrow I$ durch $h(e+ax) = g(e) + \psi(a)$. Die Abbildung h ist wohldefiniert, denn seien $e,e' \in E$, $a,a' \in A$ mit $e+ax = e'+a'x$. Dann ist $(a-a')x = e'-e \in E$, also $a-a' \in \mathfrak{a}$, und daher $\psi(a) - \psi(a') = \psi(a-a') = g(\varphi(a-a')) = g((a-a')x) = g(e'-e) = g(e') - g(e)$. Es folgt $g(e) + \psi(a) = g(e') + \psi(a')$. Somit ist h eine Fortsetzung von g auf $E + Ax$. —

Definition 13.2 Sei A ein Integritätsring. Ein A-Modul Q heißt divisibel, wenn für jedes $a \in A - \{0\}$ die Homothetie $Q \xrightarrow{h_a} Q$ surjektiv ist, d.h. für jedes $x \in Q$ ein $y \in Q$ existiert mit $ay = x$.

Folgerung 13.3 *Sei A ein Hauptidealring. Ein A-Modul I ist injektiv genau dann, wenn I divisibel ist.* —

Feststellung 13.4 *Es sei A integer und Q ein divisibler A-Modul. Dann ist Q/U divisibel für jeden Untermodul U von Q.*

Beweis: Man hat für $a \in A - \{0\}$ folgendes kommutative Diagramm:

$$\begin{tikzcd}
Q \arrow[r, "h_a"] \arrow[d, "\pi"'] & Q \arrow[d, "\pi"] \\
Q/U \arrow[r, "h'_a"] & Q/U
\end{tikzcd} ,$$

wobei π die kanonische Projektion und h_a (bzw. h'_a) die Multiplikation mit a bezeichne. $\pi \circ h_a$ ist surjektiv, somit auch $h'_a \circ \pi$. Also ist h'_a surjektiv.

Feststellung 13.5 *Sei A ein Hauptidealring (etwa $A = \mathbb{Z}$). Dann läßt sich jeder A-Modul M in einen injektiven A-Modul einbetten.*

Beweis: Schreibe M als $M = A^{(I)}/K$. Die Einbettung $A^{(I)} \subset Q(A)^{(I)}$ induziert eine Einbettung $A^{(I)}/K \longrightarrow Q(A)^{(I)}/K$. $Q(A)^{(I)}$ ist divisibel, also auch $Q(A)^{(I)}/K$. Nach 13.3 ist $Q(A)^{(I)}/K$ injektiv. –

Satz 13.6 *Für einen (nicht notwendig kommutativen) Ring A gilt: Jeder A-Modul läßt sich in einen injektiven A-Modul einbetten.*

Beweis: Sei M ein A-Modul. Faßt man M als $\mathbb{Z}$-Modul auf, so existieren nach obiger Feststellung ein injektiver $\mathbb{Z}$-Modul Q sowie eine $\mathbb{Z}$-lineare injektive Abbildung $f: M \hookrightarrow Q$.

Man betrachte $\mathrm{Hom}_{\mathbb{Z}}(A,Q)$. Für $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A,Q)$ und $a \in A$ definiere man $a\varphi : A \longrightarrow Q$ durch $b \longmapsto \varphi(ba)$.

Behauptung: $\mathrm{Hom}_{\mathbb{Z}}(A,Q)$ ist auf diese Weise ein injektiver A-Modul.

Man rechnet leicht nach, daß $\mathrm{Hom}_{\mathbb{Z}}(A,Q)$ ein A-Modul ist.

Sei nun E ein A-Modul. Einer A-linearen Abbildung $E \xrightarrow{\varphi} \mathrm{Hom}_{\mathbb{Z}}(A,Q)$ entspricht eine $\mathbb{Z}$-lineare Abbildung $\psi: E \longrightarrow Q$, $x \longmapsto \varphi(x)(1_A)$.

Umgekehrt entspricht einer $\mathbb{Z}$-linearen Abbildung $\psi: E \longrightarrow Q$ eine A-lineare Abbildung $\varphi: E \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A,Q)$,

$$\begin{aligned} x \longmapsto \varphi(x):\ & A \longrightarrow Q \\ & a \longmapsto \psi(ax) . \end{aligned} \qquad (*)$$

Man hat also einen natürlichen Gruppenisomorphismus

$\mathrm{Hom}_A(E,\mathrm{Hom}_{\mathbb{Z}}(A,Q)) \simeq \mathrm{Hom}_{\mathbb{Z}}(E,Q)$.

Zum Beweis der Injektivität von $\mathrm{Hom}_{\mathbb{Z}}(A,Q)$:

Sei $g: E \hookrightarrow F$ injektiv und A-linear. Dann ist $\mathrm{Hom}_{\mathbb{Z}}(F,Q) \xrightarrow{g^*} \mathrm{Hom}_{\mathbb{Z}}(E,Q)$ surjektiv, da Q ein injektiver $\mathbb{Z}$-Modul ist, und daher ist

$$\mathrm{Hom}(F,\mathrm{Hom}_{\mathbb{Z}}(A,Q)) \xrightarrow{g^*} \mathrm{Hom}(E,\mathrm{Hom}_{\mathbb{Z}}(A,Q))$$

ebenfalls surjektiv.

Schließlich sieht man unmittelbar, daß der o.a. $\mathbb{Z}$-linearen Einbettung f vermöge der Zuordnung $(*)$ eine A-lineare Einbettung $M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A,Q)$ entspricht.

2. Ext und Tor

Definition 13.7 Sei A ein Ring. Man definiert für $i \in \mathbb{N}$ Funktoren in 2 Variablen Ext^i und Tor_i von $\mathcal{C} :=$ A-Mod nach $\mathcal{C}$ durch folgende Axiome:

Axiom 0): Ext^i_A und Tor^A_i sind in jeder Variablen A-linear.

Axiom 1): $\mathrm{Ext}^0_A = \mathrm{Hom}_A$ bzw. $\mathrm{Tor}^A_0 = \otimes_A$ $(\mathrm{Tor}^A_0(M,N) = M \otimes_A N)$.

Axiom 2): Zu jeder "kurzen" exakten Folge $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ von A-Moduln und jedes $N \in \operatorname{Ob} C$ gibt es (in N natürliche) Homomorphismen (sog. Verbindungshomomorphismen):

$$\operatorname{Ext}^i(M',N) \xrightarrow{d^*} \operatorname{Ext}^{i+1}(M'',N)$$
$$\operatorname{Ext}^i(N,M'') \xrightarrow{d_*} \operatorname{Ext}^{i+1}(N,M')$$

bzw.

$$\operatorname{Tor}_{i+1}(M'',N) \xrightarrow{d_*} \operatorname{Tor}_i(M',N)$$
$$\operatorname{Tor}_{i+1}(N,M'') \xrightarrow{d_*} \operatorname{Tor}_i(N,M'),$$

so daß die entstehenden langen Folgen

$$\ldots \longrightarrow \operatorname{Ext}^i(M'',N) \xrightarrow{g^*} \operatorname{Ext}^i(M,N) \xrightarrow{f^*} \operatorname{Ext}^i(M',N)$$
$$\xrightarrow{d^*} \operatorname{Ext}^{i+1}(M'',N) \xrightarrow{g^*} \operatorname{Ext}^{i+1}(M,N) \longrightarrow \ldots$$

bzw.

$$\ldots \longrightarrow \operatorname{Tor}_{i+1}(M',N) \xrightarrow{f_*} \operatorname{Tor}_{i+1}(M,N) \xrightarrow{g_*} \operatorname{Tor}_{i+1}(M'',N)$$
$$\xrightarrow{d_*} \operatorname{Tor}_i(M',N) \xrightarrow{f_*} \operatorname{Tor}_i(M,N)$$

sowie

$$\ldots \longrightarrow \operatorname{Ext}^i(N,M') \xrightarrow{f_*} \operatorname{Ext}^i(N,M) \xrightarrow{g_*} \operatorname{Ext}^i(N,M'')$$
$$\xrightarrow{d_*} \operatorname{Ext}^{i+1}(N,M') \xrightarrow{f_*} \operatorname{Ext}^{i+1}(N,M) \longrightarrow \ldots$$

bzw.

$$\ldots \longrightarrow \operatorname{Tor}_{i+1}(N,M') \xrightarrow{f_*} \operatorname{Tor}_{i+1}(N,M) \xrightarrow{g_*} \operatorname{Tor}_{i+1}(N,M'')$$
$$\xrightarrow{d_*} \operatorname{Tor}_i(N,M') \xrightarrow{f_*} \operatorname{Tor}_i(N,M) \longrightarrow \ldots$$

exakt sind.

Axiom 3): Für jeden projektiven A-Modul P, alle $i > 0$ und alle $N \in \operatorname{Ob} C$ gilt $\operatorname{Ext}^i(P,N) = 0$ bzw. $\operatorname{Tor}_i(P,N) = 0$.

Bemerkung 13.8 Die "Bifunktoren" Ext^i, Tor_i, $i \in \mathbb{N}$, sind bis auf natürliche Isomorphie durch die Axiome 0) bis 3) eindeutig bestimmt.
Zur Existenz und Eindeutigkeit dieser Funktoren sowie den grundlegenden Definitionen aus der homologischen Algebra vgl. die Aufgaben oder siehe z.B. §4 in [Hilton-Stammbach].

Für einen A-Modul N bezeichne $R^i(\operatorname{Hom}_A(-,N))$, $i \in \mathbb{N}$, die rechtsderivierten Funktoren von $\operatorname{Hom}_A(-,N)$ sowie $L_i(- \otimes_A N)$, $i \in \mathbb{N}$, die linksderivierten Funktoren von $- \otimes_A N$. Dann sind $R^i(\operatorname{Hom}_A(-,-))$ und $L_i(- \otimes_A -)$, $i \in \mathbb{N}$, Bifunktoren, die die Axiome 0) - 3) erfüllen.

Die Eindeutigkeit ergibt sich aus den folgenden Folgerungen 13.15 und 13.16. Außerdem sieht man hieran, daß es ausreicht, in Axiom 2) die langen exakten Sequenzen in der ersten Variablen zu fordern.

Folgerung 13.9 *Sei* P *ein* A*-Modul. Dann sind äquivalent:*

(i) P *ist projektiv.*

(ii) *Für alle* A*-Moduln* N *und alle* $i > 0$ *ist* $\mathrm{Ext}^i(P,N) = 0$.

(iii) *Für alle* A*-Moduln* N *ist* $\mathrm{Ext}^1(P,N) = 0$.

Beweis: (i) $\Rightarrow$ (ii) ist Axiom 3).
(ii) $\Rightarrow$ (iii) ist trivial.
(iii) $\Rightarrow$ (i): Sei $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ eine exakte Sequenz von A-Moduln. Nach Axiom 2) hat man eine lange exakte Sequenz
$0 \longrightarrow \mathrm{Hom}(P,N') \longrightarrow \mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(P,N'') \longrightarrow \mathrm{Ext}^1(P,N') \longrightarrow \ldots$.
Da $\mathrm{Ext}^1(P,N') = 0$, ist $\mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(P,N'')$ surjektiv, d.h. P ist projektiv. –

Folgerung 13.10 *Sei* I *ein injektiver* A*-Modul. Dann gilt:*
$\mathrm{Ext}^i(M,I) = 0$ *für alle* A*-Moduln* M *und alle* $i > 0$.

Beweis: Induktion nach i:
Sei $0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$ exakte Sequenz von A-Moduln, wobei P projektiv sei. Da I injektiv ist, ist
$0 \longrightarrow \mathrm{Hom}_A(M,I) \longrightarrow \mathrm{Hom}_A(P,I) \longrightarrow \mathrm{Hom}_A(K,I) \longrightarrow 0$ exakt.
Nach Axiom 2) hat man eine lange exakte Sequenz:
$0 \longrightarrow \mathrm{Hom}(M,I) \longrightarrow \mathrm{Hom}(P,I) \longrightarrow \mathrm{Hom}(K,I) \longrightarrow \mathrm{Ext}^1(M,I) \longrightarrow \mathrm{Ext}^1(P,I) \longrightarrow \ldots$
Nach Axiom 3) ist $\mathrm{Ext}^1(P,I) = 0$ und daher $\mathrm{Ext}^1(M,I) = 0$.

Sei nun $i > 1$: Der langen exakten Sequenz gemäß Axiom 2) entnimmt man den Teil $\mathrm{Ext}^{i-1}(K,I) \longrightarrow \mathrm{Ext}^i(M,I) \longrightarrow \mathrm{Ext}^i(P,I)$. Nach Induktionsvoraussetzung ist $\mathrm{Ext}^{i-1}(K,I) = 0$, und nach Axiom 3) ist $\mathrm{Ext}^i(P,I) = 0$. Daher ist auch $\mathrm{Ext}^i(M,I) = 0$. –

Folgerung 13.11 *Sei* I *ein* A*-Modul. Dann sind äquivalent:*

(i) I *ist injektiv.*

(ii) *Für alle* A*-Moduln* M *und alle* $i > 0$ *ist* $\mathrm{Ext}^i(M,I) = 0$.

(iii) *Für alle* A*-Moduln* M *ist* $\mathrm{Ext}^1(M,I) = 0$.

(iv) *Für alle Ideale* $\mathfrak{a}$ *von* A *ist* $\mathrm{Ext}^1(A/\mathfrak{a},I) = 0$.

Beweis: (i) $\Rightarrow$ (ii) ist Folgerung 13.10, die Implikationen (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) sind trivial.

(iv) ⇒ (i): Sei $\mathfrak{a}$ ein Ideal von A. Zur exakten Sequenz $0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$ hat man gemäß Axiom 2) die exakte Sequenz $0 \longrightarrow \mathrm{Hom}(A/\mathfrak{a},I) \longrightarrow \mathrm{Hom}(A,I) \longrightarrow \mathrm{Hom}(\mathfrak{a},I) \longrightarrow \mathrm{Ext}^1(A/\mathfrak{a},I)$.
Da $\mathrm{Ext}^1(A/\mathfrak{a},I) = 0$, folgt die Surjektivität von $\mathrm{Hom}(A,I) \longrightarrow \mathrm{Hom}(\mathfrak{a},I)$, d.h. jeder Morphismus von $\mathfrak{a}$ nach I setzt sich fort zu einem Morphismus von A nach I. Nach Satz 13.1 ist I injektiv. –

Folgerung 13.12 *Sei F ein flacher A-Modul. Dann ist* $\mathrm{Tor}_i(M,F) = 0$ *für alle A-Moduln M und alle $i > 0$.*

Das folgt analog zu 13.10 daraus, daß der Funktor $-\otimes F$ exakt ist und $\mathrm{Tor}_i(P,F) = 0$ für $i > 0$ und projektive P gilt. –

Da projektive A-Moduln flach sind, $F\otimes -$ ein exakter Funktor ist und $\mathrm{Tor}_i(F,P) = 0$ für $i > 0$ und projektive P nach 13.12 gilt, folgt weiter:

Folgerung 13.13 *Sei F ein flacher A-Modul. Dann ist* $\mathrm{Tor}_i(F,N) = 0$ *für alle $i > 0$ und alle A-Moduln N.* –

Folgerung 13.14 *Sei $0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$ eine exakte Sequenz von A-Moduln, P sei projektiv, N ein (beliebiger) A-Modul. Dann gilt:*
$\mathrm{Ext}^{i+1}(M,N) \simeq \mathrm{Ext}^i(K,N)$ *für* $i > 0$ *sowie*
$\mathrm{Ext}^1(M,N) \simeq \mathrm{Coker}(\mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(K,N))$.

Der Beweis folgt sofort aus der langen exakten Sequenz gemäß Axiom 2) und aus den Axiomen 3) und 1). –

Folgerung 13.15 *Sei* $0 \longrightarrow K \xrightarrow{d_r} P_{r-1} \xrightarrow{d_{r-1}} P_{r-2} \xrightarrow{d_{r-2}} \ldots \rightarrow P_0 \longrightarrow M \longrightarrow 0$ *eine exakte Sequenz von A-Moduln, die P_i seien projektiv und N ein (beliebiger) A-Modul. Dann gilt:* $\mathrm{Ext}^i(K,N) \simeq \mathrm{Ext}^{i+r}(M,N)$ *für* $i > 0$.

Beweis: Induktion nach r: Der Fall $r = 1$ ist Folgerung 13.14.
Sei nun $r > 1$: Sei $K' := \mathrm{Ker}\, d_{r-2} = \mathrm{Bild}\, d_{r-1}$. Dann sind
$0 \longrightarrow K \longrightarrow P_{r-1} \longrightarrow K' \longrightarrow 0$ sowie $0 \longrightarrow K' \longrightarrow P_{r-2} \rightarrow \ldots \rightarrow P_0 \rightarrow M \rightarrow 0$ exakt. Nach Folgerung 13.14 ist $\mathrm{Ext}^i(K,N) \simeq \mathrm{Ext}^{i+1}(K',N)$, und nach Induktionsvoraussetzung ist $\mathrm{Ext}^{i+1}(K',N) \simeq \mathrm{Ext}^{i+1+r-1}(M,N) = \mathrm{Ext}^{i+r}(M,N)$. –

Folgerung 13.16 *In der Situation von Folgerung 13.15 gilt ebenso*
$\forall\, i > 0$: $\mathrm{Tor}_{i+r}(M,N) \simeq \mathrm{Tor}_i(K,N)$ *und* $\mathrm{Tor}_{i+r}(N,M) \simeq \mathrm{Tor}_i(N,K)$.

Beweis: Die Behauptung folgt aus Axiom 3) bzw. Folgerung 13.12 und Axiom 2) analog zu den Beweisen von 13.14 und 13.15. –

Folgerung 13.17 *Sei* $0 \longrightarrow N \longrightarrow I_0 \longrightarrow \dots \longrightarrow I_{r-1} \longrightarrow E \longrightarrow 0$ *eine exakte Sequenz von* A-*Moduln, die* I_i *seien injektiv und* M *ein (beliebiger)* A-*Modul. Dann gilt:* $\mathrm{Ext}^i(M,E) \simeq \mathrm{Ext}^{i+r}(M,N)$ *für* $i > 0$.

Beweis: Aus Folgerung 13.10 folgt die Behauptung analog zu 13.14 und 13.15. –

Satz 13.18 *Sei* M *ein* A-*Modul und* $r \in \mathbb{N}$. *Dann sind äquivalent:*

(*i*) *Es existiert eine exakte Sequenz*
$0 \longrightarrow P_r \longrightarrow P_{r-1} \longrightarrow \dots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$,
wobei die P_i *projektiv sind.*

(*ii*) *Falls* $0 \longrightarrow K \longrightarrow P_{r-1} \longrightarrow \dots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ *eine exakte Sequenz mit projektiven* P_i *ist, ist* K *projektiv.*

(*iii*) *Für alle* A-*Moduln* N *und alle* $n > r$ *gilt* $\mathrm{Ext}^n(M,N) = 0$.

(*iv*) *Für alle* A-*Moduln* N *gilt* $\mathrm{Ext}^{r+1}(M,N) = 0$.

Beweis: (i) ⇒ (iii): Sei $n > r$. Mit Folgerung 13.15 und $P_r = K$ gilt: $\mathrm{Ext}^n(M,N) \simeq \mathrm{Ext}^{n-r}(P_r,N) = 0$, da P_r projektiv und $n - r > 0$ ist.
(iii) ⇒ (iv) ist trivial.
(iv) ⇒ (ii): Für alle A-Moduln N gilt nach Folgerung 13.15
$\mathrm{Ext}^1(K,N) \simeq \mathrm{Ext}^{r+1}(M,N) = 0$. Sei nun $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ exakt. Dann hat man eine lange exakte Sequenz
$0 \longrightarrow \mathrm{Hom}(K,N') \longrightarrow \mathrm{Hom}(K,N) \longrightarrow \mathrm{Hom}(K,N'') \longrightarrow \mathrm{Ext}^1(K,N') = 0$, also ist K projektiv.
(ii) ⇒ (i) ist trivial. –

Satz 13.19 *Es sei* N *ein* A-*Modul und* $r \in \mathbb{N}$. *Dann sind äquivalent:*

(*i*) *Es existiert eine exakte Sequenz* $0 \to N \to I_0 \to I_1 \to \dots \to I_r \to 0$, *wobei die* I_i *injektiv sind.*

(*ii*) *Falls* $0 \longrightarrow N \longrightarrow I_0 \longrightarrow I_1 \longrightarrow \dots \longrightarrow I_{r-1} \longrightarrow E \longrightarrow 0$ *exakte Sequenz mit injektiven* I_j *ist, dann ist* E *injektiv.*

(*iii*) *Für alle* A-*Moduln* M *und alle* $n > r$ *gilt* $\mathrm{Ext}^n(M,N) = 0$.

(*iv*) *Für alle* A-*Moduln* M *gilt* $\mathrm{Ext}^{r+1}(M,N) = 0$.

(v) *Für alle Ideale* $\mathfrak{a}$ *von* A *gilt* $\mathrm{Ext}^{r+1}(A/\mathfrak{a},N) = 0$.

Beweis: Die Implikationen (i) ⇒ (iii) ⇒ (iv), (ii) ⇒ (i) werden analog zum Beweis von Satz 13.18 gezeigt. (iv) ⇒ (v) ist trivial.

(v) ⇒ (ii): Nach Folgerung 13.17 gilt: $\mathrm{Ext}^1(E,A/\mathfrak{a}) \simeq \mathrm{Ext}^{r+1}(N,A/\mathfrak{a}) = 0$.

Nach Satz 13.11 ist E injektiv. —

Definition 13.20 Die projektive (injektive) Dimension eines A-Moduls M, abgekürzt $\mathrm{proj.dim}_A M$ ($\mathrm{inj.dim}_A M$), definiert man als die kleinste natürliche Zahl $r \in \mathbb{N}$, so daß Satz 13.18 (Satz 13.19) für M und r erfüllt ist - sofern es eine solche gibt. Andernfalls definiert man $\mathrm{proj.dim}\, M = \infty$ ($\mathrm{inj.dim}\, M = \infty$). Für den 0-Modul setzt man $\mathrm{proj.dim}\, 0 = \mathrm{inj.dim}\, 0 = -\infty$.

Satz 13.21 *Sei* A *ein Ring,* $r \in \mathbb{N}$. *Dann sind äquivalent:*

(i) *Für alle* A-*Moduln* M *gilt* $\mathrm{proj.dim}_A M \le r$.

(ii) *Für alle endlichen* A-*Moduln* M *gilt* $\mathrm{proj.dim}_A M \le r$.

(iii) *Für alle* A-*Moduln* N *gilt* $\mathrm{inj.dim}_A N \le r$.

(iv) *Für alle* A-*Moduln* M,N *und alle* $n > r$ *ist* $\mathrm{Ext}^n(M,N) = 0$.

(v) *Für alle* A-*Moduln* M,N *ist* $\mathrm{Ext}^{r+1}(M,N) = 0$.

(vi) *Für alle* A-*Moduln* N *und alle Ideale* $\mathfrak{a}$ *von* A *gilt* $\mathrm{Ext}^{r+1}(A/\mathfrak{a},N) = 0$.

(vii) *Für jedes Ideal* $\mathfrak{a}$ *von* A *ist* $\mathrm{proj.dim}_A A/\mathfrak{a} \le r$.

Beweis: Nach Satz 13.18 gilt (i) ⟺ (iv) ⟺ (v) und (vi) ⟺ (vii).
Nach Satz 13.19 gilt (iii) ⟺ (iv) ⟺ (v) ⟺ (vi).
(i) ⇒ (ii) ist trivial.
(ii) ⇒ (vii) ist trivial, da $A/\mathfrak{a}$ ein endlicher A-Modul ist. —

Definition 13.22 Sei A ein Ring. Die kohomologische Dimension von A, abgekürzt $\mathrm{coh.dim}\, A$, definiert man als

$$\sup\{\mathrm{proj.dim}_A M \mid M\ A\text{-Modul}\} = \sup\{\mathrm{inj.dim}_A M \mid M\ A\text{-Modul}\} .$$

N.B.: $\mathrm{coh.dim}\, A$ ist das kleinste $r \in \mathbb{N}$, das die Bedingungen (i) bis (vii) von Satz 13.21 erfüllt, falls es ein solches gibt.

Beispiele 13.23 a) Für einen Körper k ist $\mathrm{coh.dim}\, k = 0$.
b) Für einen Dedekindring A, der kein Körper ist, gilt $\mathrm{coh.dim}\, A = 1$.

Satz 13.24 *Seien A ein noetherscher Ring, $S \subset A$ eine multiplikative Menge. M,N seien A-Moduln und M endlich. Dann gilt für alle $r \in \mathbb{N}$:*
$$S^{-1}\mathrm{Ext}_A^r(M,N) \simeq \mathrm{Ext}^r_{S^{-1}A}(S^{-1}M, S^{-1}N)\,.$$

Beweis: Nach Satz 11.4 gilt dies für $r = 0$. Sei $r > 0$. Da A noethersch ist, sind endliche A-Moduln von endlicher Darstellung. Es gibt sogar eine exakte Sequenz endlich erzeugter A-Moduln
$$0 \longrightarrow K \longrightarrow F_{r-1} \xrightarrow{d_{r-1}} F_{r-2} \longrightarrow \ldots \longrightarrow F_0 \longrightarrow M \longrightarrow 0\,,$$
wobei die F_i frei sind. Dann ist die Sequenz
$$0 \longrightarrow S^{-1}K \longrightarrow S^{-1}F_{r-1} \xrightarrow{S^{-1}d_{r-1}} S^{-1}F_{r-2} \longrightarrow \ldots \longrightarrow S^{-1}F_0 \longrightarrow S^{-1}M \longrightarrow 0$$
ebenfalls exakt, und die $S^{-1}F_i$ sind frei über $S^{-1}A$.

Nach 13.14,15 ist $\mathrm{Ext}_A^r(M,N) \simeq \mathrm{Coker}(\mathrm{Hom}_A(F_{r-1},N) \longrightarrow \mathrm{Hom}_A(K,N))$ und entsprechend $\mathrm{Ext}^r_{S^{-1}A}(S^{-1}M,S^{-1}N) \simeq \mathrm{Coker}(\mathrm{Hom}_{S^{-1}A}(S^{-1}F_{r-1},S^{-1}N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}K,S^{-1}N))$.

Da F_{r-1} und K endlich darstellbar sind, hat man natürliche Isomorphismen $S^{-1}\mathrm{Hom}_A(F_{r-1},N) \xrightarrow{\sim} \mathrm{Hom}_{S^{-1}A}(S^{-1}F_{r-1},S^{-1}N)$ und
$S^{-1}\mathrm{Hom}_A(K,N) \xrightarrow{\sim} \mathrm{Hom}_{S^{-1}A}(S^{-1}K,S^{-1},N)$, also auch
$S^{-1}\mathrm{Ext}_A^r(M,N) \simeq \mathrm{Ext}^r_{S^{-1}A}(S^{-1}M,S^{-1}N)$. —

Folgerung 13.25 *Seien A ein noetherscher Ring, N ein A-Modul sowie M ein endlicher A-Modul. Dann gilt:* $\mathrm{proj.dim}_A M = \sup\limits_{\mathfrak{m}} \mathrm{proj.dim}_{A_\mathfrak{m}} M_\mathfrak{m}$, $\mathrm{inj.dim}_A N = \sup\limits_{\mathfrak{m}} \mathrm{inj.dim}_{A_\mathfrak{m}} N_\mathfrak{m}$ *und* $\mathrm{coh.dim}\, A = \sup\limits_{\mathfrak{m}} \mathrm{coh.dim}\, A_\mathfrak{m}$, *wobei* $\mathfrak{m}$ *alle maximalen Ideale von A durchläuft.* —

Satz 13.26 *Es sei* A *ein lokaler Ring mit Restklassenkörper* k, M *ein endlich darstellbarer* A*-Modul. Dann gilt:*

$$M \text{ ist frei} \iff \operatorname{Tor}_1(k,M) = 0 .$$

Beweis: "$\Rightarrow$" ist trivial nach 13.12.
"$\Leftarrow$": Man hat eine exakte Sequenz $0 \longrightarrow K \longrightarrow F \xrightarrow{\alpha} M \longrightarrow 0$ mit endlichem, freien F, derart daß $k \otimes \alpha$ ein Isomorphismus ist (vgl. 11.11). Nach 11.15 ist K endlich. Betrachtet man folgende exakte Sequenz
$0 \longrightarrow \operatorname{Tor}_1(k,M) \longrightarrow k \otimes K \longrightarrow k \otimes F \xrightarrow{\sim} k \otimes M \longrightarrow 0$, so liefert $\operatorname{Tor}_1(k,M) = 0$, daß $k \otimes K = 0$ gilt.
Mit dem Lemma von Nakayama folgt $K = 0$, also M frei. –

Folgerung 13.27 *Es sei* A *ein noetherscher, lokaler Ring mit Restklassenkörper* k, M *ein endlicher* A*-Modul und* $r \in \mathbb{N}$.
Dann sind äquivalent:
(*i*) $\operatorname{proj.dim}_A M = r$.
(*ii*) $\operatorname{Tor}_i(k,M) = 0$ *für* $i > r$ *und* $\operatorname{Tor}_i(k,M) \neq 0$ *für* $i \leq r$.
(*iii*) $\operatorname{Tor}_r(k,M) \neq 0$ *und* $\operatorname{Tor}_{r+1}(k,M) = 0$.

Beweis: (i) $\Rightarrow$ (ii): Da $\operatorname{proj.dim}_A M = r$ ist, erhält man aus der Folgerung 13.16, daß für alle A-Moduln N und alle $i > r$ gilt: $\operatorname{Tor}_i(N,M) = 0$. Sei nun $s \in \mathbb{N}$ mit $\operatorname{Tor}_{s+1}(k,M) = 0$ sowie $0 \longrightarrow K \longrightarrow F_{s-1} \longrightarrow \ldots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$ eine exakte Sequenz, wobei die F_i frei sind. Dann ist $\operatorname{Tor}_1(k,K) \simeq \operatorname{Tor}_{s+1}(k,M) = 0$ und deshalb K frei. Nach Satz 13.18 ist dann $\operatorname{proj.dim}_A M \leq s$. Falls also $s < r$ gilt, ist $\operatorname{Tor}_{s+1}(k,M) \neq 0$. Den Fall $r = 0$ möge der Leser behandeln!

(ii) $\Rightarrow$ (iii) ist trivial.
(iii) $\Rightarrow$ (i): Aus $\operatorname{proj.dim}_A M = s$ folgt $\operatorname{Tor}_i(N,M) = 0$ für alle $i > s$. Also ist $\operatorname{proj.dim} M \geq r$.
Sei nun $0 \longrightarrow K \longrightarrow F_{r-1} \longrightarrow \ldots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$ exakt mit endlichen freien F_i , so ist $\operatorname{Tor}_1(k,K) \simeq \operatorname{Tor}_{r+1}(k,M) = 0$, also K frei und deshalb $\operatorname{proj.dim} M \leq r$. –

Folgerung 13.28 *Es sei* A *noetherscher, lokaler Ring mit Restklassenkörper* k, M *ein endlicher* A*-Modul. Dann gilt:*
$\operatorname{proj.dim} M = \infty \iff$ *Für alle* $i \in \mathbb{N}$ *ist* $\operatorname{Tor}_i(k,M) \neq 0$.
$\iff$ *Für unendlich viele* $i \in \mathbb{N}$ *gilt:* $\operatorname{Tor}_i(k,M) \neq 0$. –

Folgerung 13.29 *Sei* A *ein lokaler, noetherscher Ring mit Restklassenkörper* k. *Dann gilt:* $\operatorname{coh.dim} A = \operatorname{proj.dim}_A k$.

Beweis: Sicher gilt $\operatorname{coh.dim} A \geq \operatorname{proj.dim}_A k$. Wenn aber $\operatorname{proj.dim}_A k = n < \infty$ ist, so folgt $\operatorname{Tor}_{n+1}(k,M) = 0$ für jeden A-Modul M aus 13.18, 13.16, Axiom 3). Deshalb gilt $\operatorname{proj.dim} M \leq n$ für jeden endlichen A-Modul M nach 13.27. Nach 13.21 hat man dann $\operatorname{coh.dim} A \leq n$. —

Aufgaben und Hinweise

Zunächst eine Serie von Aufgaben, welche die Konstruktion der Funktoren Ext^i und Tor_i beschreiben:

1) Ein Kettenkomplex $E_\bullet$ ist eine durch $i \in \mathbb{Z}$ indizierte ("beidseitig unendliche") Folge von A-Modulhomomorphismen
$\ldots \longrightarrow E_{i+1} \xrightarrow{d_{i+1}} E_i \xrightarrow{d_i} E_{i-1} \longrightarrow \ldots$, derart daß $d_i \circ d_{i+1} = 0$ gilt. Es ist also $\operatorname{Ker} d_i \supset \operatorname{Im} d_{i+1}$. Die i-te Homologie ist der A-Modul $H_i E_\bullet := \operatorname{Ker} d_i / \operatorname{Im} d_{i+1}$. Die i-te Homologie ist also ein Faktormodul eines Untermoduls von E_i, und sie verschwindet genau dann, wenn die Folge $E_{i+1} \xrightarrow{d_{i+1}} E_i \xrightarrow{d_i} E_{i-1}$ exakt ist. (Wo immer in der Mathematik eine Homologie auftritt, ist sie ein Kompliziertheitsmaß.)
N.B.: Je nach Zusammenhang schreibt man auch $E^\bullet$:
$\ldots \longrightarrow E^{i-1} \xrightarrow{d^i} E^i \xrightarrow{d^{i+1}} E^{i+1} \longrightarrow \ldots$ und $H^i E^\bullet = \operatorname{Ker} d^{i+1} / \operatorname{Im} d^i$ und spricht von Kokettenkomplex und Kohomologie.
Eine Kettenabbildung $f\colon E_\bullet \longrightarrow E'_\bullet$ zwischen Kettenkomplexen $E_\bullet$ und $E'_\bullet$ ist eine Familie $(f_i)_{i \in \mathbb{Z}}$ von A-linearen Abbildungen $f_i\colon E_i \longrightarrow E'_i$, derart daß das entsprechende unendliche Diagramm

$$\begin{tikzcd} \ldots \arrow[r] & E_i \arrow[r, "d_i"] \arrow[d, "f_i"'] & E_{i-1} \arrow[r] \arrow[d, "f_{i-1}"] & \ldots \\ \ldots \arrow[r] & E'_i \arrow[r, "d'_i"] & E_{i-1} \arrow[r] & \ldots \end{tikzcd}$$

kommutativ ist, d.h. $d'_i \circ f_i = f_{i-1} \circ d_i$ für alle $i \in \mathbb{Z}$ gilt.
Zeige: $f_i(\operatorname{Ker} d_i) \subset \operatorname{Ker} d'_i$ und $f_i(\operatorname{Im} d_{i+1}) \subset \operatorname{Im} d'_{i+1}$.

Mithin wird von f eine Familie von Homomorphismen

$$H_i(f): H_iE_\bullet \longrightarrow H_iE'_\bullet$$

induziert.

Die Kettenkomplexe (von A-Moduln) zusammen mit den Kettenabbildungen bilden eine Kategorie. Die Menge $\mathrm{Hom}_A(E_\bullet, E'_\bullet)$ aller Kettenabbildungen $E_\bullet \longrightarrow E'_\bullet$ ist ein A-Modul. H_i ist für jedes i ein A-linearer Funktor von der Kategorie der Kettenkomplexe in die Kategorie der A-Moduln.

2) a) Zwei Kettenabbildungen $f,g\colon E_\bullet \longrightarrow E'_\bullet$ heißen homotop, wenn es eine Familie von Homomorphismen $h_i\colon E_i \longrightarrow E'_{i+1}$ gibt, derart daß $f_i - g_i = h_{i-1} \circ d_i + d'_{i+1} \circ h_i$ für alle i gilt.
Zeige: Wenn f und g homotop sind, ist $H_i(f) = H_i(g)$ für alle i.

b) Eine Kettenabbildung $f\colon E_\bullet \longrightarrow E'_\bullet$ heißt eine Homotopieäquivalenz, wenn es eine Kettenabbildung $g\colon E'_\bullet \longrightarrow E_\bullet$ gibt, so daß $g \circ f$ homotop zu $\mathrm{id}_{E_\bullet}$ und $f \circ g$ homotop zu $\mathrm{id}_{E'_\bullet}$ ist. Zwei Kettenkomplexe heißen homotopieäquivalent, wenn es zwischen ihnen eine Homotopieäquivalenz gibt.
Zeige: Wenn f eine Homotopieäquivalenz ist, ist $H_i(f)$ ein Isomorphismus für jedes i. Homotopieäquivalente Kettenkomplexe haben somit isomorphe Homologien.

3) Sei $0 \longrightarrow E'_\bullet \xrightarrow{f} E_\bullet \xrightarrow{g} E''_\bullet \longrightarrow 0$ eine exakte Sequenz von Kettenabbildungen, d.h. $0 \longrightarrow E'_i \xrightarrow{f_i} E_i \xrightarrow{g_i} E''_i \longrightarrow 0$ sei exakt für jedes i.
Konstruiere für jedes i auf kanonische Weise einen Homomorphismus $d_{*i}\colon H_i(E''_\bullet) \longrightarrow H_{i-1}(E'_\bullet)$, derart daß die unendlich lange Folge

$$\ldots \longrightarrow H_{i+1}E''_\bullet \xrightarrow{d_{*i+1}} H_iE'_\bullet \xrightarrow{H_i(f)} H_iE_\bullet \xrightarrow{H_i(g)} H_iE''_\bullet$$
$$\xrightarrow{d_{*i}} H_{i-1}E'_\bullet \xrightarrow{H_{i-1}(f)} H_{i-1}E_\bullet \longrightarrow$$

exakt wird.
(Hinweis: Betrachte das kommutative Diagramm mit exakten Zeilen:

$$
\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & E'_i \arrow[r] \arrow[d, "d'_i"'] & E_i \arrow[r, shift left, "g_i"] \arrow[d, "d_i"'] \arrow[d, dashed, shift left=2] & E''_i \arrow[r] \arrow[d] \arrow[l, dashed, shift left] & 0 \\
0 \arrow[r] & E'_{i-1} \arrow[r, shift left, "f_{i-1}"] \arrow[d, "d'_{i-1}"'] & E_{i-1} \arrow[r] \arrow[d] \arrow[l, dashed, shift left] & E''_{i-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}
$$

Repräsentiere $c \in H_iE''$ durch ein $w \in E''_i$; wähle ein Urbild x von w unter g_i ; setze $y = d_i(x)$; zeige $y \in \operatorname{Im} f_{i-1}$; sei z das (eindeutige) Urbild von y unter f_{i-1} ; zeige $z \in \operatorname{Ker} d'_{i-1}$; sei c' die Restklasse von z modulo $\operatorname{Im} d'_i$, also $c' \in H_{i-1}E'$. Die Zuordnung $c \longmapsto c'$ ist wohldefiniert und eine A-lineare Abbildung $d_{*i}\colon H_iE'' \longrightarrow H_{i-1}E'$.)

4) Eine projektive Auflösung eines A-Moduls M ist eine (unendlich lange) exakte Folge: $\ldots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow M \longrightarrow 0$ mit projektiven P_i . Jeder Modul besitzt eine projektive (sogar freie) Auflösung. Genauer versteht man unter obiger projektiven Auflösung den Kettenkomplex $P_\bullet$ $\ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow 0$, zusammen mit dem naheliegenden Isomorphismus $\varepsilon\colon H_0P_\bullet \simeq M$. $(H_iP_\bullet = 0$ für $i \neq 0$.)
Sei $f\colon M \longrightarrow M'$ ein A-Modulhomomorphismus, und seien $P_\bullet$ bzw. $P'_\bullet$ projektive Auflösungen von M bzw. M' . Zeige:
a) Es gibt eine Kettenabbildung $f_\bullet\colon P_\bullet \longrightarrow P'_\bullet$ mit $H_0(f_\bullet) = f$.
b) Je zwei solche Kettenabildungen ($f_\bullet$ und $f'_\bullet$ mit $H_0(f_\bullet) = H_0(f'_\bullet) = f$) sind homotop.
(Konstruiere f_i und h_i sukzessive.)
Folgere:
c) Sind $P_\bullet$ und $P'_\bullet$ projektive Auflösungen desselben Moduls M , so sind sie homotopieäquivalent.

5) Sei $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ eine exakte Folge von A-Moduln. Zeige: Es gibt eine exakte Folge von projektiven Auflösungen:
$0 \longrightarrow P'_\bullet \xrightarrow{f_\bullet} P_\bullet \xrightarrow{g_\bullet} P''_\bullet \longrightarrow 0$ der Moduln M',M,M'' mit $H_0(f_\bullet) = f$ und $H_0(g_\bullet) = g$.

(Hinweis: Wähle projektive Auflösungen $P'_\bullet$ von M' und $P''_\bullet$ von M''. Setze $P_i := P'_i \oplus P''_i$. Konstruiere d_i sukzessive. I.a. ist $d_i \neq d'_i \oplus d''_i$.)

6) Seien M,N A-Moduln und $P_\bullet$ eine projektive Auflösung von M. Man erhält einen Kettenkomplex

$$E_\bullet = P_\bullet \otimes_A N$$

und einen Kokettenkomplex

$$E^\bullet = \mathrm{Hom}_A(P_\bullet, N) \qquad (E^i = \mathrm{Hom}(P_i, N)).$$

Definiere: $\mathrm{Tor}_i^A(M,N) := H_i(P_\bullet \otimes_A N)$ und $\mathrm{Ext}_A^i(M,N) = H^i\mathrm{Hom}(P_\bullet,N)$. Zeige: Tor_i^A und Ext_A^i sind - bis auf einen eindeutigen Isomorphismus - wohldefiniert. Zu jedem Homomorphismus $f: M \longrightarrow M'$ bzw. $g: N \longrightarrow N'$ gibt es eindeutig bestimmte Homomorphismen $\mathrm{Ext}_A^i(f,N): \mathrm{Ext}_A^i(M',N) \longrightarrow \mathrm{Ext}_A^i(M,N)$ bzw. $\mathrm{Ext}_A^i(M,g): \mathrm{Ext}_A^i(M,N) \longrightarrow \mathrm{Ext}_A^i(M,N')$; analog für Tor.

Zeige: Ext_A^i und Tor_i^A sind Funktoren in 2 Variablen, die die Axiome 0) bis 3) erfüllen.

7) Eine Subtilität haben wir unberücksichtigt gelassen, da sie in diesem Buch nicht gebraucht wird: Die zu einer kurzen exakten Sequenz $(*)\quad 0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ gehörigen Verbindungshomomorphismen $\mathrm{Ext}^i(M',N) \longrightarrow \mathrm{Ext}^{i+1}(M'',N)$ etc. sind unabhängig von den gewählten Auflösungen (allerdings wesentlich abhängig von $(*)$ selbst, nicht nur von M' und M''). Ferner erhält man aus einem kommutativen Diagramm mit exakten Zeilen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M'_1 & \longrightarrow & M_1 & \longrightarrow & M''_1 & \longrightarrow & 0 \\
 & & {\scriptstyle f'}\downarrow & & \downarrow & & {\scriptstyle f''}\downarrow & & \\
0 & \longrightarrow & M'_2 & \longrightarrow & M_2 & \longrightarrow & M''_2 & \longrightarrow & 0
\end{array}$$

kommutative Diagramme

$$\begin{array}{ccc}
\mathrm{Ext}^i(M'_1,N) & \xrightarrow{d_*} & \mathrm{Ext}^{i+1}(M''_1,N) \\
{\scriptstyle \mathrm{Ext}^i(f',N)}\downarrow & & \downarrow{\scriptstyle \mathrm{Ext}^i(f'',N)} \\
\mathrm{Ext}^i(M'_2,N) & \xrightarrow{d_*} & \mathrm{Ext}^{i+1}(M''_2,N)
\end{array}$$

etc. Vgl. [Hilton-Stammbach] Kap. V, §7.

8) Eine injektive Auflösung eines A-Moduls M ist eine (unendlich lange) exakte Sequenz $0 \longrightarrow M \longrightarrow I_0 \longrightarrow I_1 \longrightarrow \ldots$ mit injektiven A-Moduln I_j. Jeder A-Modul M besitzt eine solche. Man kann Ext auch durch injektive Auflösungen der 2. Variablen definieren und Tor durch projektive Auflösungen der 2. Variablen.
Auch kann man beide Variablen zugleich auflösen - beide projektiv für Tor, die 1. projektiv, die 2. injektiv für Ext. Die entstehenden Doppelkomplexe kann man zu einfachen Kettenkomplexen machen und deren (Ko-) Homologie berechnen. Alles führt zum gleichen Ergebnis.

9) Was Ext mit Extensionen, d.h. Erweiterungen, und Tor mit Torsion zu tun hat, kann man in [MacLane] und [Hilton-Stammbach] nachlesen.

10) Für nichtkommutative Ringe A sind Ext^i_A und Tor^A_i als Funktoren in die Kategorie der abelschen Gruppen definiert. Vgl. 10.12 und 10.A11.

11) Bestimme $\mathrm{proj.dim}_{\mathbb{Z}/4}\, \mathbb{Z}/2$.

12) (Schanuel) Für $i = 1,2$ seien $0 \longrightarrow K_i \longrightarrow P_i \longrightarrow M \longrightarrow 0$ (bzw. $0 \longrightarrow M \longrightarrow I_i \longrightarrow L_i \longrightarrow 0$) exakte Folgen von A-Moduln. Die P_i seien projektiv (bzw. die I_i injektiv). Zeige: $P_1 \oplus K_2 \simeq P_2 \oplus K_1$ (bzw. $I_1 \oplus L_2 \simeq I_2 \oplus L_1$) .

Die folgenden 4 Aufgaben dienen dazu, nichttriviale Beispiele flacher Moduln zu konstruieren.

13) Zeige: Ein A-Modul M ist genau dann flach, wenn $\mathrm{Tor}^A_1(M,A/\mathfrak{a}) = 0$ für jedes Ideal $\mathfrak{a}$ von A ist.

14) Für einen noetherschen Ring A und den Polynomring $B := A[X_1,\ldots,X_n]$ zeige man:

$$\mathrm{Ass}_B B = \{\mathfrak{p}[X_1,\ldots,X_n] \mid \mathfrak{p} \in \mathrm{Ass}\, A\} .$$

("$\supset$" ist einfach. Um "$\subset$" zu zeigen, darf man $n = 1$ annehmen.
Sei $\mathfrak{P} \in \mathrm{Ass}_B B$, $\mathfrak{p} = A \cap \mathfrak{P}$ und $S = A-\mathfrak{p}$. Dann ist $S^{-1}\mathfrak{P} \in \mathrm{Ass}_{S^{-1}B}\, S^{-1}B$ nach 4.11. Man darf also annehmen: $A = A_\mathfrak{p}$.
Es ist $\mathfrak{P} = \mathrm{Ann}(g)$ für ein $g \in B - \{0\}$. Wenn $\mathfrak{P} \supsetneqq \mathfrak{p}[X]$, gibt es ein $f \in \mathfrak{P}$, dessen höchster Koeffizient nicht in $\mathfrak{p}$ liegt, also eine Einheit ist. Es folgt $fg \neq 0$; Widerspruch.)
Eine weitgehende Verallgemeinerung ist [Bourbaki] chap. IV, §2, no. 6, Thm. 2.

15) Folgere aus A14: Sei A ein Ring, $f \in A[X_1,\dots,X_n]$ ein Polynom, dessen Koeffizienten das Ideal A von A erzeugen. Dann ist f kein Nullteiler von $A[X_1,\dots,X_n]$.
(Zunächst sieht man dies mittels A 14 leicht für noethersches A. Für beliebiges A sei nun g so gewählt, daß $fg = 0$ ist. Seien $a_1,\dots,a_r$ die Koeffizienten von f und $b_1,\dots,b_s$ die von g. Nach Voraussetzung gibt es $c_1,\dots,c_r \in A$ mit $a_1c_1 + \dots + a_rc_r = 1$. Betrachte nun den von $a_1,\dots,a_r,b_1,\dots,b_s,c_1,\dots,c_r$ erzeugten noetherschen Unterring von A.)

16) Sei $f \in A[X_1,\dots,X_n]$ und $B = A[X_1,\dots,X_n]/(f)$. Zeige:
a) Wenn die Koeffizienten von f das Ideal A erzeugen, ist B flach über A.
b) Wenn schon die Koeffizienten der Monome vom Grade >0 das Ideal A erzeugen, ist B sogar treuflach über A.
(Hinweis: Gib eine exakte Folge
$$0 \longrightarrow \mathrm{Tor}_1^A(B,A/\mathfrak{a}) \longrightarrow A[X_1,\dots,X_n] \otimes A/\mathfrak{a} \xrightarrow{h_f} A[X_1,\dots,X_n] \otimes A/\mathfrak{a}$$
an. Zeige mittels A 15, daß die Homothetie h_f injektiv ist.)

Eine weitgehende Verallgemeinerung von a) ist [Grothendieck] chap. 0_{IV}, 15.1.16.

17) Injektive Hülle: Nach 13.6 läßt sich jeder A-Modul M in einen injektiven A-Modul I einbetten. Nach Baer gibt es einen (bis auf i.a. nicht eindeutige Isomorphie) eindeutigen "minimalen" injektiven Modul $E(M)$, der M als Untermodul enthält. Zur präzisen Formulierung dieses Sachverhaltes und seinem Beweis siehe [MacLane] Chap.III, 11. (Vorsicht: Die Zuordnung $M \longrightarrow E(M)$ ist kein Funktor.)

18) Sei A ein noetherscher Ring, I ein injektiver A-Modul. Dann gibt es eine direkte Zerlegung $I \simeq \bigoplus_{j\in J} I_j$, wo $I_j \simeq E(A/\mathfrak{p}_j)$ mit $\mathfrak{p}_j \in \mathrm{Spec}\, A$ ist. Diese Darstellung ist im wesentlichen eindeutig. Siehe [Gabriel].

19) Während es nach A18 eine befriedigende Strukturtheorie injektiver Moduln über noetherschen Ringen gibt, ist die Sachlage für projektive Moduln wesentlich komplizierter. Es gibt hierüber eine reichhaltige Literatur. Der Leser möge in Büchern über Algebraische K-Theorie nachschauen ([Milnor], [Swan K], [Bass]).
Z.B. weiß man, daß projektive Moduln über $k[X_1,\dots,X_n]$ frei sind, wenn k ein Körper ist (oder gewissen anderen Ringklassen angehört).

Dieser Satz hat von seiner Vermutung bis zu seinem Beweis gut 20 Jahre gebraucht. Vgl. [Lam].

§14 REGULÄRE RINGE

Definition 14.1 Ein lokaler Ring A mit maximalem Ideal $\mathfrak{m}$ heißt regulär, wenn A noethersch und $\dim A = \mu(\mathfrak{m})$ ist.

Erinnerung: Für einen noetherschen lokalen Ring A mit maximalem Ideal $\mathfrak{m}$ und $k = A/\mathfrak{m}$ ist $\mu(\mathfrak{m}) = \mu_k(\mathfrak{m}/\mathfrak{m}^2)$. Ferner gilt $\dim A \leq \mu(\mathfrak{m})$. Vgl. 6.15 - 6.18.

Beispiele 14.2 Sei A lokal.

a) Für $\dim A = 0$ gilt: A ist regulär $\Longleftrightarrow$ A ist ein Körper.

b) Für $\dim A = 1$ gilt: A ist regulär $\Longleftrightarrow$ A ist ein DBR.

"$\Rightarrow$" ist 8.8 "(iv) $\Rightarrow$ (i)".

Im folgenden wollen wir den wichtigen Satz, daß ein regulärer lokaler Ring immer integer ist, zweimal beweisen (14.5 und 14.8).
Der erste Beweis benutzt von dem Hauptsatz der Dimensiontheorie (Theorem 6.9) nur die Gleichung $\dim_A(M) = s_A(M)$, genauer nur die Folgerung 6.10, kommt also - wie auf Seite 62 bemerkt - ohne das Hilbert-Samuel-Polynom aus.
Der zweite Beweis benötigt hingegen die Gleichung $\dim_A(M) = d_A(M)$ aus 6.9, wo $d_A(M)$ der Grad des zu M gehörigen Hilbert-Samuel-Polynoms ist. Er bringt mit Satz 14.6 zusätzlich eine interessante Charakterisierung regulärer Ringe, die jedoch im Rest des Buches nicht gebraucht wird.

Die jeweils benutzten Hilfsmittel 14.3 bzw. 14.7 sind für sich von Interesse.

Satz 14.3 (J. Tate)

Es sei A ein lokaler, noetherscher Ring mit maximalem Ideal $\mathfrak{m}$ und $x \in \mathfrak{m}$, so daß $Ax = (x)$ ein Primideal der Höhe ≥ 1 ist.
Dann ist A integer.

Beweis: a) Behauptung: Zu jedem $a \in A - \{0\}$ gibt es ein $a' \in A - (x)$ und ein $r \in \mathbb{N}$ mit $a = x^r a'$.
Beweis hierfür: Sei $a \in A - \{0\}$. Man konstruiert folgendermaßen eine Folge (a_i) von Elementen in A: $a_0 := a$, und für $i \geq 1$ wählt man, solange möglich, $a_i \in A$, so daß $a_{i-1} = a_i x$.
Dieses Verfahren bricht ab, d.h. es gibt ein $r \in \mathbb{N}$: $a_r \neq bx$ ist für alle $b \in A$.
Annahme: Es existiert eine unendliche Folge $(a_i)_{i \in \mathbb{N}}$ mit $a_0 = a$ und $a_i = a_{i+1}x$ für alle $i \in \mathbb{N}$. Dann hat man eine aufsteigende Kette von Hauptidealen $(a_0) \subset (a_1) \subset (a_2) \subset \ldots$. Da $x \in \mathfrak{m}$, gilt nach dem Lemma von Nakayama $(a_i) = (a_{i+1}x) = x \cdot (a_{i+1}) \subsetneqq (a_{i+1})$ für alle i.
Da A noethersch ist, bricht die Kette von Hauptidealen ab, d.h. es gibt ein $n \in \mathbb{N}$ mit $(a_m) = (a_n)$ für $m > n$. Widerspruch!
Somit gilt $a_r \notin (x)$ für ein $r \in \mathbb{N}$. Nach Konstruktion der Folge $a_0, \ldots, a_r$ ist $a = x^r a_r$.

b) Seien nun $a, b \in A - \{0\}$. Nach a) existieren $a', b' \in A - (x)$ und $r, s \in \mathbb{N}$ mit $a = x^r a'$ und $b = x^s b'$, also $ab = x^{r+s} a'b'$. Da (x) ein Primideal, ist $a'b' \notin (x)$, also auch nicht nilpotent. Daher existiert ein minimales Primideal $\mathfrak{p}$ mit $a'b' \notin \mathfrak{p}$.
Da $ht(x) \geq 1$, liegt x und daher auch x^{r+s} in keinem minimalen Primideal. Folglich gilt: $x^{r+s} \cdot a'b' \notin \mathfrak{p}$, also insbesondere $a \cdot b = x^{r+s} a'b' \neq 0$. —

Folgerung 14.4 *Es sei A ein lokaler, noetherscher Ring, der nicht integer ist, und $\mathfrak{P}$ ein Primideal, das ein Hauptideal ist.*
Dann ist $\mathfrak{P}$ minimal. —

Satz 14.5 *Ein regulärer lokaler Ring A ist integer.*

Beweis: Induktion nach $\dim A$: Falls $\dim A = 0$ ist, ist A ein Körper. Sei $\dim A = n > 0$.
Annahme: A ist nicht integer. Es sei $\mathfrak{m}$ das maximale Ideal von A, und $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ seien die minimalen Primideale von A sowie $k := A/\mathfrak{m}$.

<u>Behauptung:</u> Unter diesen Voraussetzungen gilt $\mathfrak{m} \subset \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$.

Beweis hierfür: Sei $x \in \mathfrak{m}-\mathfrak{m}^2$ (nach dem Lemma von Nakayama ist $\mathfrak{m}^2 \neq \mathfrak{m}$). Dann ist zu zeigen: $x \in \mathfrak{p}_i$ für ein i. Man ergänze $\overline{x} = x+\mathfrak{m}^2$ durch $(\overline{x}_i = x_i+\mathfrak{m}^2)_{i=2,\ldots,n}$ zu einer k-Basis von $\mathfrak{m}/\mathfrak{m}^2$. Folglich wird $\mathfrak{m}$ von $x,x_2,\ldots,x_n$ erzeugt (12.1). Betrachte $A/(x)$. Sei $\mathfrak{n} := \mathfrak{m}/(x)$ das maximale Ideal von $A/(x)$. Nach Folgerung 6.13 ist $\dim A/(x) \geq n-1$.
Aus $\dim A/(x) \leq \mu(\mathfrak{n})$ folgt: $\dim A/(x) = n-1 = \mu(\mathfrak{n})$. Also ist $A/(x)$ regulär und somit nach Induktionsvoraussetzung integer, d.h. (x) ist ein Primideal. Nach 14.4 ist (x) ein minimales Primideal, insbesondere also $x \in \bigcup_{i=1}^{r} \mathfrak{p}_i$.

Damit hat man $\mathfrak{m} \subset \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$. Aber wegen $\mathfrak{m} \not\subset \mathfrak{m}^2$ (Nakayama) ist $\mathfrak{m} \subset \mathfrak{p}_i$ für ein i, im Widerspruch zu $\dim A > 0$. —

Nun zum zweiten Beweis von 14.5.

<u>Satz 14.6</u> *Sei* A *ein lokaler noetherscher Ring mit dem maximalen Ideal* $\mathfrak{m}$ *und* $k = A/\mathfrak{m}$, *und sei* $x_1,\ldots,x_r$ *eine* k-*Basis von* $\mathfrak{m}/\mathfrak{m}^2$. *Dann sind äquivalent:*

(*i*) A *ist regulär.*

(*ii*) *Der durch* $X_i \longmapsto x_i$ *definierte Homomorphismus (von graduierten* k-*Algebren)* $\varphi: k[X_1,\ldots,X_r] \longrightarrow gr_{\mathfrak{m}}(A)$ *ist bijektiv.*

<u>Beweis:</u> (ii) $\Rightarrow$ (i): φ bildet den k-Vektorraum der homogenen Polynome vom Grad n bijektiv auf $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ ab. Also ist $l(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \binom{r+n-1}{r-1}$.
Folglich ist $l(A/\mathfrak{m}^n) = \sum_{i=0}^{n-1} l(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = \binom{r+n-1}{r}$, also ein Polynom in n vom Grade r. Mit Theorem 6.9 ist also $\dim A = r = \mu_k(\mathfrak{m}/\mathfrak{m}^2) = \mu(\mathfrak{m})$ und deshalb A regulär.

(i) $\Rightarrow$ (ii) Sei $I = \operatorname{Ker}\varphi$. Da φ sicherlich surjektiv ist, genügt es, $I = (0)$ zu beweisen. I ist ein graduiertes Ideal: $I = \bigoplus_{s\in\mathbb{N}} I_s$. Wenn man $I \neq (0)$ annimmt, gibt es ein homogenes Element $u \in I_h$. Sei H_s der Vektorraum der homogenen Polynome vom Grade s. Dann ist $u \cdot H_{s-h} \subset I_s$ für $s \geq h$. Deshalb gilt $l(\mathfrak{m}^s/\mathfrak{m}^{s+1}) = l(H_s/I_s) \leq \binom{r+s-1}{r-1} - \binom{r+s-h-1}{r-1}$ für $s \geq h$. Als Polynome in s haben $\binom{r+s-1}{r-1}$ und $\binom{r+s-h-1}{r-1}$ beide den Grad $r-1$ und den gleichen höchsten Koeffizienten. Deshalb ist $l(\mathfrak{m}^s/\mathfrak{m}^{s+1})$ für große s ein Polynom in s vom Grade $\leq r-2$, mithin

$l(A/\mathfrak{m}^s)$ für große s ein Polynom vom Grade $\leq r-1$. Nach 6.9 ist dann $\dim A \leq r-1 < \mu(\mathfrak{m})$ und deshalb A nicht regulär, im Gegensatz zur Voraussetzung. —

Satz 14.7 *Sei A ein Ring, der durch eine absteigende Folge von Idealen $I_0 = A \supset I_1 \supset I_2 \supset \dots$ filtriert ist, derart daß $\bigcap_{j\in\mathbb{N}} I_j = (0)$ gilt. Wenn der assoziierte graduierte Ring $\bigoplus_{j\in\mathbb{N}} I_j/I_{j+1}$ integer ist, so ist es auch A.*

Beweis: Seien $a,b \in A - (0)$ und $r,s \in \mathbb{N}$ so gewählt, daß $a \in I_r - I_{r+1}$ und $b \in I_s - I_{s+1}$ ist. Seien $\overline{a} = a + I_{r+1}$ und $\overline{b} = b + I_{s+1}$ die Restklassen. Dann ist $\overline{a}\,\overline{b} \in I_{r+s}/I_{r+s+1}$. Nach Voraussetzung ist $\overline{a}\,\overline{b} \neq 0$, d.h. $ab \notin I_{r+s+1}$, mithin $ab \neq 0$. —

Folgerung 14.8 (aus 14.6 und 14.7)

Ein regulärer lokaler Ring ist integer. —

Definition 14.9 Es sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und M ein A-Modul. Ein r-Tupel $(x_1,\dots,x_r) \in A^r$ heißt eine M-reguläre Folge, wenn

1) $x_i \in \mathfrak{m}$ für $1 \leq i \leq r$,
2) x_1 ein Nichtnullteiler von M ist, und
3) x_i für $i \geq 2$ ein Nichtnullteiler von $M/(x_1,\dots,x_{i-1})M$ ist.

Satz 14.10 *a) Wenn A ein regulärer, lokaler Ring mit maximalem Ideal $\mathfrak{m}$ ist, dann ist jedes minimale Erzeugendensystem von $\mathfrak{m}$ eine A-reguläre Folge.*
b) Wenn A ein noetherscher, lokaler Ring mit maximalem Ideal $\mathfrak{m}$ ist, das von einer A-regulären Folge $x_1,\dots,x_n$ erzeugt wird, dann ist A regulär, $x_1,\dots,x_n$ ein minimales Erzeugendensystem von $\mathfrak{m}$ sowie insbesondere $\dim A = n$.

Beweis: a) Sei A ein regulärer, lokaler Ring, $x_1,\dots,x_n$ ein minimales Erzeugendensystem von $\mathfrak{m}$.
Induktion nach n: Für $n = 0$ ist nichts zu zeigen. Sei $n > 0$.
Wie im Beweis von Satz 14.5 folgt, daß $A/(x_1)$ ein regulärer lokaler Ring der Dimension $n-1$ ist. $\overline{x}_2 = x_2 + (x_1),\dots,\overline{x}_n = x_n + (x_1)$ bilden daher ein minimales Erzeugendensystem für $\mathfrak{m}/(x_1)$. Nach Induktionsvoraussetzung sind $\overline{x_2},\dots,\overline{x_n}$ eine $A/(x_1)$-reguläre Folge in $A/(x_1)$ und

folglich $x_2,\dots,x_n$ eine $A/(x_1)$-reguläre Folge in A. Da A integer und $x_1 \neq 0$ ist, ist x_1 ein Nichtnullteiler in A, d.h. A-regulär. Insgesamt ist daher $x_1,\dots,x_n$ A-regulär.

b) Sei $x_1,\dots,x_n$ eine A-reguläre Folge mit $\mathfrak{m} = (x_1,\dots,x_n)$.

Behauptung: Für $i = 1,\dots,n$ ist $\dim A/(x_1,\dots,x_i) = \dim A - i$.

Dies zeigt man durch (einfache) Induktion nach i.
Sei $i = 1$: Es ist x_1 ein Nichtnullteiler und $x_1 \in \mathfrak{m}$. Mit 6.13 folgt $\dim A/(x_1) = \dim A-1$. (Die Primideale $\mathfrak{p}$ von A mit $\dim A/\mathfrak{p} = \dim A$ sind minimal, bestehen also aus Nullteilern.)

$i > 1$: x_i bzw. $\overline{x}_i$ ist Nichtnullteiler von $A/(x_1,\dots,x_{i-1})$ und $\overline{x}_i \in \mathfrak{m}/(x_1,\dots,x_{i-1})$. Wie oben folgt $\dim A/(x_1,\dots,x_i) = \dim A/(x_1,\dots,x_{i-1})-1 = \dim A - i$ (nach Induktionsvoraussetzung).

Insbesondere ist $0 = \dim A/(x_1,\dots,x_n) = \dim A - n$, also $\dim A = n$. Da aber $n = \dim A \leq \mu(\mathfrak{m}) \leq n$ gilt, ist A regulär und $x_1,\dots,x_n$ ein minimales Erzeugendensystem. —

Definition 14.11 Sei A ein (noetherscher) lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Eine A-reguläre Folge $x_1,\dots,x_n$ in $\mathfrak{m}$ heißt reguläres Parametersystem, falls $\mathfrak{m}$ von $x_1,\dots,x_n$ erzeugt wird.

Folgerung 14.12 *Sei* A *ein regulärer lokaler Ring mit maximalem Ideal* $\mathfrak{m}$. *Für* $x_1,\dots,x_r \in \mathfrak{m}$ *sind äquivalent:*

(*i*) $x_1,\dots,x_r$ *bilden einen Teil eines regulären Parametersystems von* A.

(*ii*) *Die Restklassen* $\overline{x}_1,\dots,\overline{x}_r$ *modulo* $(\mathfrak{m}^2)$ *sind linear unabhängig über* $k = A/\mathfrak{m}$.

(*iii*) $A/(x_1,\dots,x_r)$ *ist regulär, und es ist* $\dim A/(x_1,\dots,x_r) = \dim A - r$.

Beweis: (i) $\Longleftrightarrow$ (iii) folgt unmittelbar aus 14.10 und 12.1.
(ii) $\Longleftrightarrow$ (iii): Seien $\mathfrak{a} := (x_1,\dots,x_r)$ und $B := A/\mathfrak{a}$. B ist lokaler Ring mit maximalem Ideal $\mathfrak{n} = \mathfrak{m}/\mathfrak{a}$. Aus der exakten Folge
$0 \longrightarrow \mathfrak{a}/\mathfrak{a}\cap\mathfrak{m}^2 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{n}/\mathfrak{n}^2 \longrightarrow 0$ erhält man
$\mu_k(\mathfrak{n}/\mathfrak{n}^2) = \mu_k(\mathfrak{m}/\mathfrak{m}^2)-s$, wobei s die Dimension des von $\overline{x}_1,\dots,\overline{x}_r$ in $\mathfrak{m}/\mathfrak{m}^2$ erzeugten Untervektorraums ist. Wegen der Regularität von A folgt $\mu_k(\mathfrak{n}/\mathfrak{n}^2) = \dim A - s$. Ist nun (ii) erfüllt, so ist $s = r$. Außerdem gilt $\dim B = \dim A - r$ (vgl. Beweis von 14.10b).
Insgesamt folgt $\dim B = \dim A - r = \mu_k(\mathfrak{n}/\mathfrak{n}^2)$, d.h. B ist regulär von der

Dimension $\dim A - r$. Ist umgekehrt (iii) erfüllt, so gilt $\mu_k(\mathfrak{n}/\mathfrak{n}^2) = \dim B = \dim A - r$, also $r = s$. Es folgt (ii). –

Satz 14.13 *Es sei* A *ein regulärer lokaler Ring mit maximalen Ideal* $\mathfrak{m}$, $I \subset A$ *ein Ideal. Dann gilt:*

A/I *ist regulär*

$\Longleftrightarrow$ I *wird von einem Teil eines regulären Parametersystems erzeugt.*

Beweis: "$\Leftarrow$" ist 14.12 (i) $\Rightarrow$ (iii).

"$\Rightarrow$": $\mathfrak{n} := \mathfrak{m}/I$ sei das maximale Ideal von A/I. Seien $x_1,\ldots,x_r \in \mathfrak{m}$, so daß $x_1 + I,\ldots,x_r + I$ ein reguläres Parametersystem von A/I bilden. Dann sind $x_1,\ldots,x_r$ linear unabhängig modulo $\mathfrak{n}^2 = \mathfrak{m}^2 + I$, und $(x_1,\ldots,x_r) + I = \mathfrak{m}$. Seien $\overline{x}_i = x_i + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$ die Restklassen. Im k-Vektorraum $\mathfrak{m}/\mathfrak{m}^2$ gilt: $<\overline{x}_1,\ldots,\overline{x}_r> \oplus (\mathfrak{m}^2+I)/\mathfrak{m}^2 = \mathfrak{m}/\mathfrak{m}^2$. Man wähle eine Basis $\overline{y}_1,\ldots,\overline{y}_s$ von $(\mathfrak{m}^2+I)/\mathfrak{m}^2$, $y_i \in I$. Dann ist $(\overline{x}_1,\ldots,\overline{x}_r,\overline{y}_1,\ldots,\overline{y}_s)$ eine Basis von $\mathfrak{m}/\mathfrak{m}^2$. Nach 14.12 ist $x_1,\ldots,x_r,y_1,\ldots,y_s$ ein reguläres Parametersystem.

Behauptung: $I = (y_1,\ldots,y_s)$. Setze $I' = (y_1,\ldots,y_s)$. Dann ist $I' \subset I$ und A/I regulär von Dimension r sowie A/I' regulär von Dimension r nach 14.12. $I' \subset I$ sind daher Primideale von derselben Höhe, also $I' = I$. –

Satz 14.14 *Es sei* A *ein noetherscher, lokaler Ring mit maximalem Ideal* $\mathfrak{m}$ *und Restklassenkörper* k, M *ein endlicher* A*-Modul und* $x \in \mathfrak{m}$ *ein* M*-reguläres Element.*
Dann gilt: $\operatorname{proj.dim}_A M + 1 = \operatorname{proj.dim}_A(M/xM)$.

Beweis: Sei $\operatorname{proj.dim}_A M = r < \infty$ (bzw. $r = \infty$). Dann ist nach Voraussetzung $0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$ exakt. k wird als A-Modul von $\mathfrak{m}$ annulliert. Für alle i ist $\operatorname{Tor}_i(-,M)$ ein A-linearer Funktor, und daher wird $\operatorname{Tor}_i(k,M)$ ebenfalls von $\mathfrak{m}$ annulliert.
Wir haben folgende lange exakte Sequenz:

$$\mathrm{Tor}_{i+1}(k,M) \xrightarrow{\cdot x} \mathrm{Tor}_{i+1}(k,M) \longrightarrow \mathrm{Tor}_{i+1}(k,M/xM)$$
$$\longrightarrow \mathrm{Tor}_i(k,M) \xrightarrow{\cdot x} \mathrm{Tor}_i(k,M) \quad .$$

Aber x annulliert $\mathrm{Tor}_{i+1}(k,M)$ und $\mathrm{Tor}_i(k,M)$, also ist

$$0 \longrightarrow \mathrm{Tor}_{i+1}(k,M/xM) \longrightarrow \mathrm{Tor}_i(k,M) \longrightarrow 0 \quad \text{exakt.}$$

Nach 13.27f gilt für $i \le r$ (bzw. $i < \infty$), daß $\mathrm{Tor}_i(k,M) \neq 0$ und daher $\mathrm{Tor}_{i+1}(k,M/xM) \neq 0$ ist. Für $i > r$ ist $\mathrm{Tor}_i(k,M) = 0$, also auch $\mathrm{Tor}_{i+1}(k,M/xM) = 0$.
Insgesamt folgt daher: $\mathrm{proj.dim}_A\, M/xM = r+1$ (bzw. $\mathrm{proj.dim}_A\, M/xM = \infty$). –

Folgerung 14.15 *Es sei* A *ein noetherscher, lokaler Ring mit maximalem* $\mathfrak{m}$, M *ein endlicher* A*-Modul und* $x_1,\dots,x_s$ *in* $\mathfrak{m}$ *eine* M*-reguläre Folge. Dann gilt:* $\mathrm{proj.dim}\, M = \mathrm{proj.dim}(M/(x_1M+\dots+x_sM)) - s$. –

Folgerung 14.16 *Sei* A *ein regulärer lokaler Ring der Dimension* n. *Dann gilt:* $\mathrm{coh.dim}\, A = n < \infty$.

Beweis: Sei $k = A/\mathfrak{m}$ der Restklassenkörper von A. Für ein reguläres Parametersystem $x_1,\dots,x_n$ von A gilt:

$$\mathrm{coh.dim}\, A \overset{(13.29)}{=} \mathrm{proj.dim}_A\, k = \mathrm{proj.dim}_A(A/(x_1,\dots,x_n)) = n + \mathrm{proj.dim}_A A = n. \; –$$

Definition 14.17 Sei A ein lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{m}$ und M ein endlicher A-Modul.
$\mathrm{tf}_A M := \sup\{n \mid \exists\ M\text{-reguläre Folge der Länge } n \text{ in } \mathfrak{m}\}$ heißt die Tiefe von M. ($\mathrm{tf}\, M := \mathrm{tf}_A M$, wenn feststeht, was A ist.)
$\mathrm{tf}\, A$, die Tiefe von A, ist die Tiefe des A-Moduls A.

Feststellung 14.18 *Seien* $A,\mathfrak{m},M$ *wie oben. Dann gilt:*

a) *Ist* $M \neq 0$ *und* $x_1,\dots,x_r$ *eine* M*-reguläre Folge in* $\mathfrak{m}$, *so ist* $\dim(M/x_1M+\dots+x_rM) = \dim M - r$.
b) *Ist* $M \neq 0$, *so ist* $\mathrm{tf}\, M \le \dim M$ $(\mathrm{tf}(0) = \infty)$.
c) $\mathrm{tf}\, M = 0 \iff \mathfrak{m} \in \mathrm{Ass}\, M$.

Beweis: a) (Vgl. Beweis von 14.10b).) Wir wenden Induktion nach r an und sehen: Es genügt, den Fall $r = 1$ zu betrachten. x_1 ist ein Nichtnullteiler von M, also ist $x_1 \notin \mathfrak{p}$ für $\mathfrak{p} \in \mathrm{Ass}\, M$, deshalb $x_1 \notin \mathfrak{p}$ für alle $\mathfrak{p}$, die minimal in $\mathrm{Supp}\, M$ sind, mithin $x_1 \notin \mathfrak{p}$ für alle $\mathfrak{p} \in \mathrm{Supp}\, M$, für die $\dim M = \dim A/\mathfrak{p}$ gilt. Nach 6.13 ist $\dim(M/xM) = \dim M - 1$.

b) folgt sofort aus a).

c) $\operatorname{tf} M = 0 \Leftrightarrow$ jedes $x \in \mathfrak{m}$ ist Nullteiler für M

$$\overset{4.6}{\Longleftrightarrow} \mathfrak{m} \subset \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} \overset{1.21}{\Longleftrightarrow} \mathfrak{m} \in \operatorname{Ass} M .$$

Satz 14.19 *Es sei* A *ein noetherscher, lokaler Ring,* M *ein nichttrivialer, endlicher* A*-Modul mit* $\operatorname{proj.dim} M < \infty$.
Dann gilt: $\operatorname{tf} M + \operatorname{proj.dim} M = \operatorname{tf} A$. *(Insbesondere ist also* $\operatorname{tf} M \le \operatorname{tf} A$.)

Beweis: Sei $r = \operatorname{tf} A$ und $s = \operatorname{tf} M$ sowie $x_1,\dots,x_r$ eine A-reguläre Folge in $\mathfrak{m}$ und $y_1,\dots,y_s$ eine M-reguläre Folge in $\mathfrak{m}$.
Sei $B := A/(x_1,\dots,x_r)$ und $N := M/(y_1M + \dots + y_sM)$, dann ist $\mathfrak{m} \in \operatorname{Ass} B$ und $\mathfrak{m} \in \operatorname{Ass} N$. D.h. man hat exakte Folgen:

1) $0 \longrightarrow k \longrightarrow B \longrightarrow B' \longrightarrow 0$ und

2) $0 \longrightarrow k \longrightarrow N \longrightarrow N' \longrightarrow 0$.

"$\le$": Sei E ein endlicher A-Modul mit $\operatorname{proj.dim} E = n < \infty$.
Aus 1) erhält man eine exakte Folge:
$0 = \operatorname{Tor}_{n+1}(B',E) \longrightarrow \operatorname{Tor}_n(k,E) \longrightarrow \operatorname{Tor}_n(B,E)$. $\operatorname{Tor}_n(k,E)$ ist nichttrivial, also ist auch $\operatorname{Tor}_n(B,E) \neq 0$. Da nach 14.15 $\operatorname{proj.dim}_A B = r = \operatorname{tf} A$ gilt, ist $\operatorname{proj.dim} E = n \le r = \operatorname{tf} A$. Man wende dieses auf $E = N$ an: $\operatorname{proj.dim} M + \operatorname{tf} M = \operatorname{proj.dim} M + s \overset{14.15}{=\!=} \operatorname{proj.dim} N \le \operatorname{tf} A$.

"$\ge$": Da $\operatorname{proj.dim}_A B = r$, erhält man aus 2) die exakte Sequenz
$0 = \operatorname{Tor}_{r+1}(N',B) \longrightarrow \operatorname{Tor}_r(k,B) \longrightarrow \operatorname{Tor}_r(N,B)$. Da $\operatorname{Tor}_r(k,B) \neq 0$, ist auch $\operatorname{Tor}_r(N,B) \neq 0$. Daher ist $\operatorname{proj.dim}_A M + \operatorname{tf} M = \operatorname{proj.dim}_A N \ge r = \operatorname{tf}(A)$. —

Folgerung 14.20 *Es sei* A *ein noetherscher, lokaler Ring mit maximalem Ideal* $\mathfrak{m}$, M *ein endlicher* A*-Modul,* $\mathfrak{m} \in \operatorname{Ass}(A)$, *d.h.* $\operatorname{tf}(A) = 0$ *und* $\operatorname{proj.dim} M < \infty$. *Dann ist* M *ein freier* A*-Modul.* —

Satz 14.21 *Es sei* A *ein noetherscher, lokaler Ring mit maximalem Ideal* $\mathfrak{m}$, M *ein endlicher* A*-Modul,* $x \in \mathfrak{m}$ *sowohl* A*-regulär als auch* M*-regulär. Dann gilt:* $\operatorname{proj.dim}_{A/(x)} M/xM \le \operatorname{proj.dim}_A M$.

Beweis: Wenn $\operatorname{proj.dim} M = \infty$, ist nichts zu zeigen.
Induktion nach $n = \operatorname{proj.dim} M < \infty$.
Sei $n = 0$: Dann ist M ein projektiver, also freier A-Modul und M/xM ein freier $A/(x)$-Modul.

Sei $\underline{n > 0}$ und $0 \longrightarrow K \longrightarrow A^r \longrightarrow M \longrightarrow 0$ eine exakte Sequenz von A-Moduln. Dann ist $\operatorname{proj.dim} K = n-1$. Da x A-regulär ist, ist x A^r-regulär und daher K-regulär $(K \subset A^r)$.
Man hat dann folgendes kommutative Diagramm mit exakten Zeilen und Spalten:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \longrightarrow & A^r & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot x} & & \downarrow{\scriptstyle \cdot x} & & \downarrow{\scriptstyle \cdot x} & & \\
0 & \longrightarrow & K & \longrightarrow & A^r & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K/xK & \xrightarrow{\alpha} & (A/xA)^n & \longrightarrow & M/xM & \longrightarrow & 0
\end{array}$$

(Die letzte Zeile ist exakt, da für einen A-Modul N gilt: $N/xN \simeq N \otimes A/(x)$.) Nach dem Diagrammlemma 11.13 ist α injektiv. Die Induktionsvoraussetzung liefert $\operatorname{proj.dim}_{A/(x)} K/xK \leq \operatorname{proj.dim}_A K$. Daher: $\operatorname{proj.dim}_{A/(x)} M/xM \leq \operatorname{proj.dim}_{A/(x)} K/xK + 1 \leq \operatorname{proj.dim}_A K + 1 = \operatorname{proj.dim} M$. —

Theorem 14.22 *Sei* A *ein noetherscher, lokaler Ring. Dann gilt:*
A *ist regulär* $\Longleftrightarrow$ $\operatorname{coh.dim} A < \infty$.
In diesem Fall ist $\dim A = \operatorname{coh.dim} A$.

Beweis: "$\Rightarrow$" und "$\dim A = \operatorname{coh.dim} A$" ist Folgerung 14.16.
"$\Leftarrow$": Sei $\mathfrak{m}$ das maximale Ideal von A und $k = A/\mathfrak{m}$ der Restklassenkörper. Wir benutzen Induktion nach $n = \mu_k(\mathfrak{m}/\mathfrak{m}^2)$.

Sei $n = 0$: $\mu_k(\mathfrak{m}/\mathfrak{m}^2) = 0$ heißt $\mathfrak{m} = \mathfrak{m}^2$. Mit dem Lemma von Nakayama folgt $\mathfrak{m} = 0$, d.h. A ist ein Körper.

Sei nun $n > 0$.
Behauptung: Es existiert ein Nichtnullteiler x von A mit $x \in \mathfrak{m} - \mathfrak{m}^2$.
Beweis hierfür: Andernfalls wäre $\mathfrak{m} \subset \mathfrak{m}^2 \cup \bigcup_{\mathfrak{p} \in \operatorname{Ass} A} \mathfrak{p}$, also $\mathfrak{m} \subset \mathfrak{m}^2$ oder $\mathfrak{m} \subset \mathfrak{p}$ für ein $\mathfrak{p} \in \operatorname{Ass} A$. Da $\mu_k(\mathfrak{m}/\mathfrak{m}^2) > 0$, ist $\mathfrak{m} \not\subset \mathfrak{m}^2$, daher $\mathfrak{m} \in \operatorname{Ass} A$, d.h. $\operatorname{tf} A = 0$. Nach Voraussetzung ist $\operatorname{proj.dim} k < \infty$. Nach der Folgerung 14.20 ist k ein freier A-Modul: $k \simeq A^r$. Aber $\mathfrak{m} \neq 0$ und $\mathfrak{m} \cdot k = 0$, im Widerspruch zu $\mathfrak{m}A^r \neq 0$.

Man wähle nun einen Nichtnullteiler $x \in \mathfrak{m} - \mathfrak{m}^2$ und definiere $B := A/Ax$. B ist ein lokaler Ring mit maximalem Ideal $\mathfrak{n} = \mathfrak{m}/Ax$. Dann gilt:

$B/\mathfrak{n} = k$, $\mathfrak{n}^2 = \mathfrak{m}^2 + Ax$, $\mu_k(\mathfrak{n}/\mathfrak{m}^2) = \mu_k(\mathfrak{m}/\mathfrak{m}^2) - 1$, und $\dim B = \dim A-1$.
Es reicht nun, folgendes zu zeigen:

Behauptung: $\text{coh.dim } B < \infty$. Denn nach Induktionsvoraussetzung gilt dann: B ist regulär, also $\dim B = \mu_k(\mathfrak{n}/\mathfrak{n}^2)$. Mithin ist $\mu_k(\mathfrak{m}/\mathfrak{m}^2) = \mu_k(\mathfrak{n}/\mathfrak{n}^2) + 1 = \dim B+1 = \dim A$.

Beweis der Behauptung: Falls $\mathfrak{n} = (0)$, so ist B ein Körper.
Ist $\mathfrak{n} \neq (0)$, so gilt: $\text{coh.dim } B = \text{proj.dim}_B k = \text{proj.dim}_B \mathfrak{n} + 1$.
Also genügt es, $\text{proj.dim}_B \mathfrak{n} < \infty$ zu zeigen.
Nach Satz 14.21 ist $\text{proj.dim}_B \mathfrak{m}/\mathfrak{m}x \leq \text{proj.dim}_A \mathfrak{m}$, und nach Voraussetzung ist $\text{proj.dim}_A \mathfrak{m} < \infty$. Daher reicht es, folgende Behauptungen zu zeigen:

Behauptung 1): $\mathfrak{n} = \mathfrak{m}/Ax$ ist isomorph zu einem direkten Summanden von $\mathfrak{m}/\mathfrak{m}x$.

Behauptung 2): $\text{proj.dim}(M_1 \oplus M_2) = r < \infty \Rightarrow \text{proj.dim } M_1 \leq r$.

Zu 1): Sei $x, x_2, \ldots, x_n$ ein minimales Erzeugendensystem von $\mathfrak{m}$, d.h. $\bar{x}, \bar{x}_2, \ldots, \bar{x}_n$ eine Basis von $\mathfrak{m}/\mathfrak{m}^2$. Setze $\mathfrak{h} := Ax_2 + \ldots + Ax_n + \mathfrak{m}x$.
Dann ist $Ax + \mathfrak{h} = \mathfrak{m}$. Es gilt auch $Ax \cap \mathfrak{h} = \mathfrak{m}x$. Sei nämlich $a \in A$ mit $ax \in Ax \cap \mathfrak{h}$. Dann gibt es $a_i \in A$ und $m \in \mathfrak{m}$ mit
$ax = a_2x_2 + \ldots + a_nx_n + mx$. Aus der k-linearen Unabhängigkeit folgt $a \equiv 0$ $(\text{mod } \mathfrak{m})$, d.h. $a \in \mathfrak{m}$. Also ist $ax \in \mathfrak{m}x$.
Mithin ist $\mathfrak{m}/Ax \simeq \mathfrak{h}/\mathfrak{m}x$ und $\mathfrak{h}/\mathfrak{m}x \oplus Ax/\mathfrak{m}x = \mathfrak{m}/\mathfrak{m}x$.

Zu 2): Seien $0 \longrightarrow K_i \longrightarrow P_{i,r-1} \longrightarrow \ldots \longrightarrow P_{i,0} \longrightarrow M_i \longrightarrow$ exakte Folgen für $i = 1,2$ mit projektiven P_{ij}. Man erhält eine exakte Folge
$0 \longrightarrow K_1 \oplus K_2 \longrightarrow P_{i,r-1} \oplus P_{2,r-1} \longrightarrow \ldots \longrightarrow P_{1,0} \oplus P_{2,0} \longrightarrow M_1 \oplus M_2 \longrightarrow 0$.
Da $K_1 \oplus K_2$ n.V. projektiv ist, ist es auch K_1. —

Folgerung 14.23 *Sei A ein regulärer lokaler Ring. Dann ist auch $A_\mathfrak{p}$ regulär für jedes Primideal $\mathfrak{p}$ von A.*

Beweis: Sei M ein A-Modul. Da $n := \text{proj.dim}_A M \leq \text{coh.dim } A < \infty$, existiert eine exakte Sequenz von A-Moduln
$0 \longrightarrow P_n \longrightarrow \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$, wobei die P_i projektive A-Moduln sind. Gemäß Satz 3.38 ist die Sequenz
$0 \longrightarrow (P_n)_\mathfrak{p} \longrightarrow \ldots \longrightarrow (P_0)_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow 0$ exakt, wobei die $(P_i)_\mathfrak{p}$ projektive $A_\mathfrak{p}$-Moduln sind (10.54b)).

Also gilt: $\text{proj.dim}_{A_\mathfrak{p}} M_\mathfrak{p} \leq \text{coh.dim } A$, und somit
$\text{coh.dim } A_\mathfrak{p} \leq \text{coh.dim } A < \infty$. —

Bemerkung: Es gibt bis jetzt keinen homologiefreien Beweis für diese Aussage.

Definition 14.24 Für einen Ring A definiert man:
A ist regulär $\Longleftrightarrow$ A ist noethersch und $A_{\mathfrak{p}}$ ist regulär für alle $\mathfrak{p} \in \operatorname{Spec} A$.

Bemerkungen 14.25 a) Diese Definition stimmt nach 14.23 mit der bisherigen Definition überein, falls A lokal ist, und ist äquivalent zu: $A_{\mathfrak{m}}$ ist regulär für jedes $\mathfrak{m} \in \operatorname{Spmax} A$.

b) Jeder Dedekindring ist regulär.

Folgerung 14.26 *Sei* A *ein noetherscher Ring. Dann gilt:*
$\operatorname{coh.dim} A < \infty \Longleftrightarrow A$ *ist regulär und* $\dim A < \infty$.
In diesem Fall ist $\operatorname{coh.dim} A = \dim A$.

Beweis: Nach 13.25 ist $\operatorname{coh.dim} A = \sup\limits_{\mathfrak{m}} \operatorname{coh.dim} A_{\mathfrak{m}}$. —

Definition 14.27 a) Ein Ringhomomorphismus $\varphi\colon A \longrightarrow B$ heißt flach (bzw. treuflach), wenn B (vermöge φ) ein flacher (bzw. treuflacher) A-Modul ist.

b) Es seien A und B lokale Ringe mit maximalen Idealen $\mathfrak{m}$ bzw. $\mathfrak{n}$, $\varphi\colon A \longrightarrow B$ sei ein Ringhomomorphismus. φ heißt lokal, wenn $\varphi(\mathfrak{m}) \subset \mathfrak{n}$, d.h. $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$ ist.

Beispiele 14.28 Sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$.

a) $\mathfrak{p} \subsetneqq \mathfrak{m}$ sei ein Primideal. Dann ist der kanonische Homomorphismus $A \longrightarrow A_{\mathfrak{p}}$ flach, aber nicht lokal.

b) Sei $\mathfrak{a}$ ein Ideal in A mit $(0) \neq \mathfrak{a} \neq A$. Dann ist $A \longrightarrow A/\mathfrak{a}$ (selbstverständlich) lokal, aber nicht flach.
Es ist nämlich $\mathfrak{a} \otimes_A A/\mathfrak{a} \simeq \mathfrak{a}/\mathfrak{a}^2$ und $\mathfrak{a}\cdot(A/\mathfrak{a}) = 0$. Gemäß 12.23 wäre $\mathfrak{a} \otimes_A A/\mathfrak{a} \simeq \mathfrak{a}\cdot(A/\mathfrak{a})$, wenn $A/\mathfrak{a}$ flach über A wäre. Nach Nakayamas Lemma würde aus $\mathfrak{a}/\mathfrak{a}^2 = 0$ aber $\mathfrak{a} = (0)$ folgen.

Lemma 14.29 *a) Seien* $A \xrightarrow{f} B \xrightarrow{g} C$ *flache Ringhomomorphismen. Dann ist* $g \circ f$ *flach.*
b) Für einen Homomorphismus lokaler Ringe $f\colon A \longrightarrow B$ *gilt:*
f *ist treuflach* $\Longleftrightarrow$ f *ist flach und lokal.*
c) Ein treuflacher Ringhomomorphismus $f\colon A \longrightarrow B$ *ist injektiv.*

Beweis: a) Für einen A-Modul M hat man einen kanonischen Isomorphismus $(M \otimes_A B) \otimes_B C \simeq M \otimes_A C$.

b) "$\Leftarrow$": Wegen $\varphi(\mathfrak{m}) \subset \mathfrak{n}$ ist $B/\mathfrak{m}B \neq 0$. Mit 10.51 erhält man die Treuflachheit.

"$\Rightarrow$": Falls es ein $m \in \mathfrak{m}$ gibt mit $\varphi(m) \notin \mathfrak{n}$, so ist $\varphi(m) \in B^*$, also $\mathfrak{m}B = B$. Dann ist $B/\mathfrak{m}B = 0$ und φ nicht treuflach nach 10.51. –

c) Sei $\mathfrak{a} = \operatorname{Ker} f$. Da B flach über A ist, ist $\mathfrak{a} \otimes_A B \overset{(12.23)}{\simeq} \mathfrak{a}B = 0$. Da B treuflach ist, folgt $\mathfrak{a} = (0)$ gemäß 10.51.–

Satz 14.30 *Sei $A \longrightarrow B$ ein flacher, lokaler Homomorphismus noetherscher lokaler Ringe mit maximalen Idealen $\mathfrak{m}$ bzw. $\mathfrak{n}$. Dann gilt:*

a) Ist B ein regulärer Ring, so ist A regulär.

b) Sind A und $B/\mathfrak{m}B$ regulär, so ist B regulär, und
$\dim A + \dim B/\mathfrak{m}B = \dim B$.

Beweis: a) Sei $\dim B = n$ und
$0 \longrightarrow K \longrightarrow P_{n-1} \longrightarrow \dots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ eine exakte Folge von endlich erzeugten A-Moduln, wobei die P_i frei seien. Da B flach über A ist, ist $0 \longrightarrow K \otimes_A B \longrightarrow P_{n-1} \otimes_A B \longrightarrow \dots \longrightarrow P_0 \otimes B \longrightarrow M \otimes B \longrightarrow 0$ exakt, wobei die $P_i \otimes_A B$ frei über B sind. Da B regulär mit $\dim B = n$ ist, ist $K \otimes_A B$ frei über B, also flach über A.
D.h. der Funktor $\_ \otimes_A K \otimes_A B : A\text{-Mod} \longrightarrow B\text{-Mod}$ ist exakt.

Da B nach 14.29 treuflach ist, ist $\_ \otimes_A K$ ein exakter Funktor, d.h. K ist flach. Da A ein noetherscher, lokaler Ring und K endlicher A-Modul ist, ist K frei nach 11.16. Somit ist $\operatorname{proj.dim}_A M \leq n$. Es folgt $\operatorname{coh.dim} A \leq \operatorname{coh.dim} B < \infty$.

b) Da $A \subset B$ eine lokale Erweiterung ist, gilt $\mathfrak{n} \supset \mathfrak{m}$, also $\mathfrak{n} \supset \mathfrak{m}B$. Sei $x_1,\dots,x_m$ ein reguläres Parametersystem von A und $y_1,\dots,y_n \in \mathfrak{n}$, so daß $\overline{y}_1,\dots,\overline{y}_n \pmod{\mathfrak{m}B}$ ein reguläres Parametersystem von $B/\mathfrak{m}B$ ist.

Wegen Satz 14.10b) genügt es, folgendes zu zeigen:

1) $x_1,\dots,x_m,y_1,\dots,y_n$ ist eine B-reguläre Folge.

2) $x_1,\dots,x_m,y_1,\dots,y_n$ erzeugen $\mathfrak{n}$.

Beweis: 2) ist klar.
Zu 1): Zunächst ist $A / Ax_1 + \dots + Ax_{i-1} \xrightarrow{\cdot x_i} A / Ax_1 + \dots + Ax_{i-1}$ injektiv für $i = 1,\dots,m$. Da B flach über A ist, ist

$B \otimes_A (A / Ax_1 + \ldots + Ax_{i-1}) \xrightarrow{\cdot x_i} B \otimes_A (A / Ax_1 + \ldots + Ax_{i-1})$ injektiv.

Da $B \otimes_A (A / Ax_1 + \ldots + Ax_{i-1}) \simeq B /(Bx_1 + \ldots + Bx_{i-1})$, ist x_i ein Nicht-nullteiler von $B /(Bx_1 + \ldots + Bx_{i-1})$.

D.h. $x_1,\ldots,x_n$ ist eine B-reguläre Folge.

Für $i = 1,\ldots,n$ ist ferner $\overline{y}_i$, und daher auch y_i, ein Nichtnullteiler von $B /(Bx_1 + \ldots + Bx_n + By_1 + \ldots + By_{i-1})$. Insgesamt ist $x_1,\ldots,x_m,y_1,\ldots,y_n$ B-regulär. —

Satz 14.31 *Sei* A *ein (nicht notwendig lokaler) regulärer Ring. Dann ist der Polynomring* $A[X_1,\ldots,X_n]$ *ebenfalls regulär.*

Beweis: Es reicht, die Behauptung für den Fall $n = 1$ zu beweisen. Es sei also $\mathfrak{P}$ ein Primideal von $A[X]$ und $\mathfrak{p} = A \cap \mathfrak{P}$. Dann ist $T := A - \mathfrak{p} \subset S := A[X] - \mathfrak{P}$. $A[X]_{\mathfrak{P}} = S^{-1}(A[X])$ und $A_{\mathfrak{p}}[X] = A_{\mathfrak{p}} \otimes_A A[X] = T^{-1}(A[X])$ (10.44, 10.46). Daher ist $A[X]_{\mathfrak{P}} = S^{-1}(A_{\mathfrak{p}}[X])$ und somit flach über $A_{\mathfrak{p}}$. Ferner ist $A_{\mathfrak{p}} \subset A[X]_{\mathfrak{P}}$ eine lokale Erweiterung und $A_{\mathfrak{p}}$ nach Voraussetzung regulär.
Sei $k_{\mathfrak{p}} := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$.
$A[X]_{\mathfrak{P}} / \mathfrak{p}A[X]_{\mathfrak{P}} \simeq k_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A[X]_{\mathfrak{P}} \simeq k_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} S^{-1}A_{\mathfrak{p}}[X] \simeq S^{-1}(k_{\mathfrak{p}}[X]) \simeq k_{\mathfrak{p}}(X)$. $k_{\mathfrak{p}}(X)$ ist regulär, also ist $A[X]$ regulär nach Satz 14.30. —

Wir wollen zeigen, daß reguläre lokale Ringe faktoriell sind, und brauchen dazu das folgende

Lemma 14.32 *Sei* S *eine multiplikative Menge von Nichtnullteilern eines Ringes* A. *Ferner seien* $\mathfrak{a}_1,\ldots,\mathfrak{a}_m,\mathfrak{b}_1,\ldots,\mathfrak{b}_n$ *S-Ideale von* A, *und es gebe einen Isomorphismus* $\varphi: \mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{a}_m \xrightarrow{\sim} \mathfrak{b}_1 \oplus \ldots \oplus \mathfrak{b}_n$. *Dann ist* $m = n$ *und* $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_m \simeq \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n$.

Beweis: Der Isomorphismus φ ist durch eine $n \times m$-Matrix (f_{ij}) gegeben, wobei $f_{ij} \in \mathrm{Hom}_A(\mathfrak{a}_j,\mathfrak{b}_i)$ ist. Nach 12.18 ist $\mathrm{Hom}_A(\mathfrak{a}_j,\mathfrak{b}_i) \simeq \mathfrak{b}_i : \mathfrak{a}_j$, daher existieren $q_{ij} \in S^{-1}A$, so daß $f_{ij}(a) = q_{ij}a$ für $a \in \mathfrak{a}_j$ gilt. D.h. φ ist durch die Matrix $Q := (q_{ij})$ gegeben.
Ebenso ist der inverse Isomorphismus φ^{-1} durch eine Matrix $Q' \in M(m \times n, S^{-1}A)$ gegeben, so daß $QQ' = E_n$, $Q'Q = E_m$ (mit Einheitsmatrizen E_n,E_m) gilt. Da A kommutativ ist, gilt $n = m$ und $Q' = Q^{-1}$. (Man kann etwa zu Restklassen nach einem maximalen Ideal von $S^{-1}A$

übergehen und erhält Identitäten $\overline{Q}\,\overline{Q}' = E_n$, $\overline{Q}'\overline{Q} = E_m$ über einem Körper, woraus $n = m$ wegen der Invarianz der Vektorraumdimension folgt.)

Behauptung: $\det(Q) \cdot \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_m = \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_m$.

Beweis hierfür: "$\subset$": Für $i,j \in \{1,\ldots,m\}$ und $a_j \in \mathfrak{a}_j$ gilt $q_{ij}a_j \in \mathfrak{b}_i$. Die Elemente der i-ten Zeile des Matrizenprodukts

$$Q \cdot \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{pmatrix}$$

liegen somit in $\mathfrak{b}_i$. Folglich gilt nach der Leibnizregel:

$$\det(Q)a_1 \cdot \ldots \cdot a_m = \det\left(Q\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}\right) \in \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_m .$$

Da die Elemente der Form $a_1 \ldots a_m$ mit $a_j \in \mathfrak{a}_j$ ein Erzeugendensystem von $\mathfrak{a}_1 \ldots \mathfrak{a}_m$ bilden, ist die Inklusion bewiesen.

"$\supset$": Da Q^{-1} den inversen Isomorphismus φ^{-1} beschreibt, folgt wie oben $\det(Q)^{-1}\, \mathfrak{b}_1 \ldots \mathfrak{b}_m = \det(Q^{-1})\, \mathfrak{b}_1 \ldots \mathfrak{b}_m \subset \mathfrak{a}_1 \ldots \mathfrak{a}_m$ und daher die Behauptung. —

Satz 14.33 *Ein regulärer, lokaler Ring* A *ist faktoriell.*

Beweis: Induktion nach $\dim A$. Im Falle $\dim A = 0$ ist A ein Körper, also auch faktoriell. Sei $\dim A > 0$: Wähle $x \in \mathfrak{m}-\mathfrak{m}^2$: Betrachte $B := A_x = S^{-1}A$, wobei $S = \{1,x,x^2,\ldots\}$ ist.

Behauptung: B ist faktoriell.

Es gilt $\dim B < \dim A$, und B ist regulär, aber für $\dim A > 1$ nicht lokal. Sei nun $\mathfrak{a}$ ein divisorielles Ideal von B. Nach 12.51 genügt es zu zeigen, daß $\mathfrak{a}$ ein Hauptideal von B ist. Da B noethersch ist, gilt für jedes maximale Ideal $\mathfrak{n}$ von B, daß $\mathfrak{a}_\mathfrak{n}$ divisoriell in $B_\mathfrak{n}$ ist (11.4). $B_\mathfrak{n}$ ist regulär und lokal mit $\dim B_\mathfrak{n} < \dim A$ und daher nach Induktionsvoraussetzung faktoriell. Also ist $\mathfrak{a}_\mathfrak{n}$ ein Hauptideal und somit ein freier $B_\mathfrak{n}$-Modul. Mithin ist $\mathfrak{a}$ ein projektiver B-Modul.

Es existiert ein endlicher A-Modul M mit $M_x \simeq \mathfrak{a}$. (Man kann M als den A-Untermodul von $\mathfrak{a}$ wählen, der von einem B-Erzeugendensystem von $\mathfrak{a}$ erzeugt wird.) M besitzt eine endliche Auflösung durch endlich erzeugte freie A-Moduln

$$0 \longrightarrow A^{r_n} \longrightarrow A^{r_{n-1}} \longrightarrow \ldots \longrightarrow A^{r_0} \longrightarrow M \longrightarrow 0 .$$

Der bequemeren Schreibweise weiter unten wegen nehmen wir o.B.d.A. an, daß n gerade ist. Durch Tensorieren mit B erhält man folgende lange exakte Sequenz:

$$0 \longrightarrow B^{r_n} \longrightarrow B^{r_{n-1}} \longrightarrow \dots \longrightarrow B^{r_o} \longrightarrow \mathfrak{a} \longrightarrow 0 .$$

Diese spaltet man in kurze exakte Sequenzen auf:

$$\begin{array}{l}
0 \longrightarrow K_1 \longrightarrow B^{r_o} \longrightarrow \mathfrak{a} \longrightarrow 0 \\
0 \longrightarrow K_2 \longrightarrow B^{r_1} \longrightarrow K_1 \longrightarrow 0 \\
\qquad\vdots \\
0 \longrightarrow K_{n-1} \longrightarrow B^{r_{n-2}} \longrightarrow K_{n-2} \longrightarrow 0 \\
0 \longrightarrow B^{r_n} \longrightarrow B^{r_{n-1}} \longrightarrow K_{n-1} \longrightarrow 0 .
\end{array}$$

Da $\mathfrak{a}$ projektiv ist, zerfällt (siehe folgende Anmerkung) die erste kurze exakte Sequenz, folglich ist K_1 projektiv. Daher zerfällt die zweite kurze exakte Sequenz, also ist K_2 projektiv usw. Induktiv folgt somit, daß alle K_i projektiv sind und alle kurzen exakten Sequenzen zerfallen. Also hat man:

$$\begin{array}{l}
\mathfrak{a} \oplus K_1 \simeq B^{r_o} \\
K_1 \oplus K_2 \simeq B^{r_1} \\
K_2 \oplus K_3 \simeq B^{r_2} \\
\quad \ddots \\
K_{n-2} \oplus K_{n-1} \simeq B^{r_{n-2}} \\
K_{n-1} \oplus B^{r_n} \simeq B^{r_{n-1}} ,
\end{array}$$

und daher:

$$\underbrace{\mathfrak{a} \oplus K_1}_{B^{r_o}} \oplus \underbrace{K_2 \quad \dots}_{B^{r_2}} \quad \dots \quad \underbrace{\oplus K_{n-1}}_{B^{r_{n-2}}} \oplus B^{r_n} \simeq B^{r_o} \oplus B^{r_2} \dots B^{r_{n-2}} \oplus B^{r_n} \quad \text{sowie}$$

$$\mathfrak{a} \oplus \underbrace{K_1 \oplus K_2}_{B^{r_1}} \quad \dots \quad \oplus \underbrace{K_{n-1} \oplus B^{r_n}}_{B^{r_{n-1}}} \simeq \mathfrak{a} \oplus B^{r_1} \oplus \quad \dots \quad \oplus B^{r_{n-1}} .$$

Also: $\mathfrak{a} \oplus B^m \simeq B^{m'}$, wobei $m = \sum_{j=1}^{n/2} r_{2j-1}$ und $m' = \sum_{j=0}^{n/2} r_{2j}$ ist.

Nach obigem Lemma gilt:

$$\mathfrak{a} = \mathfrak{a}\underbrace{B \cdot \dots \cdot B}_{m\text{-mal}} \simeq \underbrace{B \cdot \dots \cdot B}_{m'\text{-mal}} = B .$$

Somit ist $\mathfrak{a}$ ein Hauptideal und die Behauptung bewiesen.
Da $x \in \mathfrak{m}-\mathfrak{m}^2$, ist $A/(x)$ regulär und deshalb integer (14.12 und 14.5), also x ein Primelement von A. Folglich hat jedes Element $b \in B = A_x (\supset A)$ eine eindeutige Darstellung

$$b = ax^r \quad \text{mit} \quad r \in \mathbb{Z},\ a \in A \quad \text{und} \quad x \nmid a .$$

Insbesondere sei p prim in B mit einer Darstellung $p = p'x^{-r}$, $p' \in A$, $r \in \mathbb{Z}$ und $x \nmid p'$.

<u>Behauptung:</u> p' ist prim in A.

(Im folgenden Beweis der Behauptung bezeichne "$|_A$" die Teilbarkeit in A, "$|_B$" die in B.)
Seien $a_1, a_2 \in A$ mit $p' |_A a_1a_2$. Dann gilt $p = p'x^r |_B a_1a_2$, und da p prim in B ist, gilt o.B.d.A.: $p|_B a_1$, also auch $p' |_B a_1$.
Sei $b \in B$ mit $p'b = a_1$ und einer Darstellung $b = b'x^s$, $b' \in A$, $x \nmid b'$.
Daher $p'b'x^s = a_1$. Wäre $s < 0$, so hätte man $p'b' = x^{-s}a_1$, also $p'b' \in Ax$, somit $p' \in Ax$ oder $b' \in Ax$, im Widerspruch zur Konstruktion. Also ist $s > 0$, und folglich $p' |_A a_1$.

Zum Schluß sei nun $a \in A \setminus \{0\}$. Man zerlegt a in B wie folgt:

<u>1. Fall:</u> $a \in B^*$.
Man hat Darstellungen $a = x^r a'$, $a^{-1} = x^s a''$ mit $r,s \in \mathbb{Z}$, $a', a'' \in A$, $a' \cdot a'' \notin Ax$. Aus $1 = x^{r+s}a'a''$ folgt $r+s = 0$, denn $a'a'' \notin Ax$.
Somit ist $a' \in A^*$, $x^r \in A$ und $a = a'x^r$ die gesuchte Primfaktorzerlegung von a.

<u>2. Fall:</u> $a \notin B^*$.
Dann hat a in B eine Primfaktorzerlegung $a = up_1 \dots p_m$ $(u \in B^*)$.
Für $i = 1,\dots,m$ ist dann $p_i = p_i' x^{r_i}$, wobei p_i' prim in A und $p_i' \notin Ax$ ist. Ferner ist $u = vx^s$ mit $v \in A^*$. Also ist $a = v \cdot x^r \cdot p_1' \cdot \dots \cdot p_m'$ mit $r = s + \Sigma r_i \geq 0$. —

<u>Anmerkung 14.34</u> Man sagt: "Eine kurze exakte Sequenz $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ zerfällt", wenn es ein $g': M'' \longrightarrow M$ mit $g \circ g' = \mathrm{id}_{M''}$ gibt (oder - äquivalent hierzu - wenn es ein $f': M \longrightarrow M'$ mit $f' \circ f = \mathrm{id}_{M'}$ gibt). In diesem Falle ist $M \simeq M' \oplus M''$ gemäß 3.17.

<u>Bemerkung 14.35</u> Im Beweis wurde allgemein für einen Integritätsring A gezeigt: Wenn $x \in A$ prim und A_x faktoriell ist, so ist A faktoriell.

Ebenso zeigt man für einen Integritätsring A: Ist S eine multiplikative Teilmenge von A, die als solche von Primelementen erzeugt wird, und ist $S^{-1}A$ faktoriell, so ist A faktoriell.

Beispiel: Sei B ein faktorieller Ring, $S = B - \{0\}$. Dann ist $S^{-1}B[X]$ euklidisch, also faktoriell. S ist von Primelementen in B erzeugt, welche nach dem Gaußschem Lemma prim in $B[X]$ sind. Also folgt: $B[X]$ ist faktoriell.

Folgerung 14.36 *Ein lokaler regulärer Ring ist ein ganz abgeschlossener Integritätsring.*

Dies folgt sofort mit 7.9. —

Man kann diese Folgerung zu Aussagen über nichtlokale reguläre Ringe ausnutzen.

Satz 14.37 *a) Ein Ring A ist reduziert.*
$\Longleftrightarrow$ $A_{\mathfrak{m}}$ ist reduziert für jedes maximale Ideal $\mathfrak{m}$.

b) Sei A ein noetherscher Ring. Dann gilt: A ist endliches direktes Produkt ganz abgeschlossener Integritätsringe. $\Longleftrightarrow$ $A_{\mathfrak{m}}$ ist ein ganz abgeschlossener Integritätsring für jedes maximale Ideal $\mathfrak{m}$

Beweis: a) "$\Rightarrow$": Sei $\frac{x}{s} \in A_{\mathfrak{m}}$ nilpotent, wobei $x \in A$, $s \in A-\mathfrak{m}$ ist. Dann gibt es ein $n \in \mathbb{N}$, so daß $\frac{x^n}{s^n} = 0$, d.h. es gibt ein $t \in A-\mathfrak{m}$ mit $tx^n = 0$. Dann ist $(tx)^n = 0$. Da A reduziert ist, ist $tx = 0$, und daher $\frac{x}{s} = 0$.

"$\Leftarrow$": Sei $x \in \operatorname{Nil} A$, $\mathfrak{a} := Ax$ und $n \in \mathbb{N}$ mit $x^n = 0$. Dann gilt für alle maximalen Ideale $\mathfrak{m}$ in A: In $A_{\mathfrak{m}}$ ist $(\frac{x}{1})^n = 0$, also nach Voraussetzung $\frac{x}{1} = 0$. Somit ist $\mathfrak{a}_{\mathfrak{m}} = 0$ für jedes maximale Ideal $\mathfrak{m}$, also $\mathfrak{a} = 0$.

b) "$\Rightarrow$": Es sei $A = B_1 \times \ldots \times B_n$, wobei die B_i integer und ganz abgeschlossen sind, und sei $\mathfrak{m}$ ein maximales Ideal in A. Dann gibt es ein j und ein maximales Ideal $\mathfrak{n}$ in B_j, so daß
$\mathfrak{m} = B_1 \times \ldots \times B_{j-1} \times \mathfrak{n} \times B_{j+1} \times \ldots \times B_n$.
Da $A-\mathfrak{m} \supset \{0\} \times \ldots \times \{0\} \times (B_j-\mathfrak{n}) \times \{0\} \ldots \times \{0\}$ gilt, ist $A_{\mathfrak{m}} \simeq (B_j)_{\mathfrak{n}}$, also integer und ganz abgeschlossen.

"$\Leftarrow$": Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ die minimalen Primideale von A. Da A nach a) reduziert ist, ist $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n = (0)$ und folglich die kanonische

Abbildung $A \xrightarrow{\varphi} A/\mathfrak{p}_1 \times \ldots \times A/\mathfrak{p}_n$ injektiv. Nach dem Chinesischen Restsatz ist φ surjektiv, falls man für $i \neq j$ gezeigt hat: $\mathfrak{p}_j + \mathfrak{p}_j = A$. Wäre dieses nicht der Fall, so gäbe es ein maximales Ideal $\mathfrak{m} \supset \mathfrak{p}_i + \mathfrak{p}_j$, und $A_\mathfrak{m}$ hätte mindestens 2 minimale Primideale, wäre also nicht integer, im Widerspruch zur Voraussetzung. Noch zu zeigen bleibt, daß $A/\mathfrak{p}_i$ ganz abgeschlossen ist. Wie unter "⇒" zeigt man für alle maximalen Ideale $\mathfrak{n}$ in $A/\mathfrak{p}_i$: Es ist $(A/\mathfrak{p}_i)_\mathfrak{n} = A_\mathfrak{m}$ für ein maximales Ideal $\mathfrak{m}$ in A, also ganz abgeschlossen in $Q(A/\mathfrak{p}_i)$. $A/\mathfrak{p}_i = \bigcap_\mathfrak{n} (A/\mathfrak{p}_i)_\mathfrak{n}$ ist daher ebenfalls ganz abgeschlossen. —

Folgerung 14.38 *Ein regulärer (nicht notwendig lokaler) Ring ist ein endliches direktes Produkt ganz abgeschlossener Integritätsringe.* —

Satz 14.39 *Sei* A *ein noetherscher Integritätsring. Dann sind äquivalent:*

(i) $A_\mathfrak{m}$ *ist faktoriell für jedes maximale Ideal* $\mathfrak{m}$ *von* A.

(ii) $C(A) = \operatorname{Pic} A$.

Beweis: (i) ⇒ (ii): Es ist $\operatorname{Pic} A \subset C(A)$. Sei $\mathfrak{a}$ ein divisorielles, gebrochenes Ideal von A. Dann ist auch $\mathfrak{a}_\mathfrak{m}$ divisoriell in $A_\mathfrak{m}$ für jedes maximale Ideal $\mathfrak{m}$ von A, da A noethersch ist (11.4).

Nach Voraussetzung ist $\mathfrak{a}_\mathfrak{m}$ ein Hauptideal in $A_\mathfrak{m}$ für jedes $\mathfrak{m}$ und deshalb $\mathfrak{a}$ invertierbar.

(ii) ⇒ (i): Sei $\mathfrak{b}$ ein divisorielles Ideal in $A_\mathfrak{m}$, $\mathfrak{b} = \mathfrak{b}'_\mathfrak{m}$ mit einem gebrochenen Ideal $\mathfrak{b}'$ von A. Dann ist $\mathfrak{a} = (\mathfrak{b}'^{-1})^{-1}$ ein divisorielles Ideal von A und $\mathfrak{a}_\mathfrak{m} = \mathfrak{b}$. Nach Voraussetzung liegt in $\operatorname{div}(\mathfrak{a})$ ein invertierbares Ideal. Da diese divisoriell sind, ist $\mathfrak{a}$ invertierbar. Also ist $\mathfrak{b} = \mathfrak{a}_\mathfrak{n}$ invertierbar für den lokalen Ring $A_\mathfrak{m}$ und deshalb nach 12.22 und 12.7 ein Hauptideal. —

Folgerung 14.40 *Für einen regulären Integritätsring* A *gilt* $C(A) = \operatorname{Pic} A$. —

Aufgaben und Hinweise

1) Das Theorem 14.22 läßt sich wie folgt verallgemeinern: Sei A lokal und noethersch, $\mathfrak{a}$ ein Ideal endlicher projektiver Dimension, derart daß $\mathfrak{a}/\mathfrak{a}^2$ frei über $A/\mathfrak{a}$ ist. Dann ist $\mathfrak{a}$ von einer A-regulären Folge erzeugt. Siehe [Kunz], Kapitel VII, Satz 2.1 und die dort angegebene Literatur.

2) Der Satz 14.33 läßt sich wie folgt verallgemeinern: Sei A ein noetherscher Ring, S die Menge seiner Nichtnullteiler und $\mathfrak{a}$ ein S-Ideal endlicher projektiver Dimension. Dann ist $(\mathfrak{a}^{-1})^{-1}$ (also auch $\mathfrak{a}^{-1} = ((\mathfrak{a}^{-1})^{-1})^{-1}$) invertierbar. Überlege, daß dies wirklich eine Verallgemeinerung von 14.33 ist. Wenn $\mathfrak{a}$ sogar eine endliche Auflösung durch freie A-Moduln besitzt, ist $(\mathfrak{a}^{-1})^{-1}$ ein Hauptideal. Zum Beweis siehe [MacRae], [Krämer], [Ischebeck]. Eine etwas schwächere Form findet sich in [Bourbaki], Chap. VII, §4, no. 7, Corollaire 2 de la Proposition 16. Dort wird zusätzlich vorausgesetzt, daß A integer und ganz abgeschlossen ist. Beachte dazu, daß man die Ganzabgeschlossenheit eines regulären Ringes aus der Ganzabgeschlossenheit des zugehörigen graduierten Ringes folgern kann [Bourbaki], Chap. V, §1, no. 4, Proposition 15. (Für noethersche Ringe stimmen die Begriffe "ganz abgeschlossen" und "vollständig ganz abgeschlossen" überein.)

3) In der Regel wird Satz 14.33 mit einem Satz aus der Theorie der äußeren Potenzen anstelle des Lemmas 14.32 - hinter dem implizit natürlich auch die Theorie der äußeren Potenzen steht - bewiesen. Dies soll hier entwickelt werden:

a) Sei M ein A-Modul. Seine n-te äußere Potenz ist $\Lambda^n M := M \otimes_A \dots \otimes_A M/U$, wobei das Tensorprodukt n Faktoren hat und U als A-Modul von denjenigen $x_1 \otimes \dots \otimes x_n$ erzeugt wird, wo $x_i = x_j$ für ein Paar i,j mit $i \neq j$ gilt. Insbesondere gilt $\Lambda^1 M = M$. Man definiert $\Lambda^0 M := A$. Das Bild von $y_1 \otimes \dots \otimes y_n$ bei der kanonischen Abbildung $M \otimes \dots \otimes M \longrightarrow \Lambda^n M$ wird mit $y_1 \wedge \dots \wedge y_n$ bezeichnet. Es ist $x \wedge y = -y \wedge x$, allgemeiner

$$y_1 \wedge \dots \wedge y_i \wedge \dots \wedge y_j \wedge \dots \wedge y_n = -y_1 \wedge \dots \wedge y_j \wedge \dots \wedge y_i \wedge \dots \wedge y_n .$$

b) Sei $\{x_i \mid i \in I\}$ ein Erzeugendensystem von M . Zeige, daß man auf folgende Weise ein Erzeugendensystem von $\Lambda^n M$ erhält: Man versehe I mit einer totalen (d.h. vollständigen, d.h. linearen) Ordnung "$\leq$" . Dann wird $\Lambda^n M$ von

$\left\{x_{i_1} \wedge \ldots \wedge x_{i_n} \mid i_j \in I;\ i_1 < i_2 < \ldots < i_n\right\}$ erzeugt. Wenn M von m Elementen $x_1,\ldots,x_m$ erzeugt wird, gilt also $\Lambda^n M = 0$ für $n > m$, und $\Lambda^m M$ ist monogen, mit dem Erzeuger $x_1 \wedge \ldots \wedge x_m$.

c) Eine multilineare (genauer n-lineare) Abbildung $\varphi\colon M \times \ldots \times M \longrightarrow N$ heißt (bekanntlich) alternierend, wenn $\varphi(x_1,\ldots,x_n) = 0$ für alle n-Tupel $(x_1,\ldots,x_n) \in M \times \ldots \times M$ mit zwei gleichen Komponenten gilt. Zeige für $\Lambda^n M$ die universelle Eigenschaft: Jede alternierende n-lineare Abbildung $\varphi\colon M \times \ldots \times M \longrightarrow N$ faktorisiert eindeutig über die "kanonische" Abbildung (welche?) $M \times \ldots \times M \longrightarrow \Lambda^n M$. Folgere: Λ^n "ist" ein Funktor von der Kategorie der A-Moduln in dieselbe. ($\Lambda^0(f) = \mathrm{id}_A$ für alle Homomorphismen $f\colon M \longrightarrow N$.)

d) Konstruiere einen kanonischen Isomorphismus $\Lambda^n(M \oplus N) \simeq \bigoplus_{r=0}^{n} (\Lambda^r M \otimes_A \Lambda^{n-r} N)$. Für $0 \le r \le n$ hat man den naheliegenden Homomorphismus $\varphi_r\colon \Lambda^r M \otimes \Lambda^{n-r} N \longrightarrow \Lambda^n(M \oplus N)$,

$$(x_1 \wedge \ldots \wedge x_r) \otimes (y_{r+1} \wedge \ldots \wedge y_n)$$
$$\longmapsto (x_1,0) \wedge \ldots \wedge (x_r,0) \wedge (0,y_{r+1}) \wedge \ldots \wedge (0,y_n).$$

Umgekehrt erhält man einen (vielleicht weniger naheliegenden) Homomorphismus $\psi_r\colon \Lambda^n(M \oplus N) \longrightarrow \Lambda^r M \otimes \Lambda^{n-r} N$,

$$(x_1,y_1) \wedge \ldots \wedge (x_n,y_n) \longmapsto \sum_{\sigma \in S(n,r)} \mathrm{sign}(\sigma) \cdot$$
$$(x_{\sigma(1)} \wedge \ldots \wedge x_{\sigma(r)}) \otimes (y_{\sigma(r+1)} \wedge \ldots \wedge y_{\sigma(n)}).$$

Dabei ist $S(n,r)$ eine gewisse Menge von Permutationen der Menge $\{1,\ldots,n\}$, nämlich $S(n,r) := \left\{\sigma \in S_n \mid \sigma(1) < \ldots < \sigma(r) \text{ und } \sigma(r+1) < \ldots < \sigma(n)\right\}$.

Die φ_r bzw. ψ_r setzen sich zu Homomorphismen φ bzw. ψ zusammen, die zueinander invers sind.

e) Zeige: $\Lambda^n(A^r) \simeq A^{\binom{n}{r}}$, wo $\binom{n}{r}$ der Binomialkoeffizient ist.

f) Folgere aus d) und e), daß $\Lambda^n P$ projektiv ist, wenn P es ist.

g) Für ein Ideal $\mathfrak{a} \neq (0)$ des Ringes A gelte $\mathfrak{a} \oplus A^m \simeq A^n$ mit gewissen $m,n \in \mathbb{N}$. Zeige: $\mathfrak{a} \simeq A$, d.h. $\mathfrak{a}$ ist ein von einem Nichtnullteiler erzeugtes Hauptideal. Dabei sollen die obigen Überlegungen anstelle von Lemma 14.32 benutzt werden. ($\mathfrak{a}$ ist projektiv und

endlich erzeugt. Durch Lokalisieren sieht man erst $m = n-1$ und dann, daß $\mathfrak{a}$ projektiv vom Rang 1 ist. Es folgt
$A \simeq \Lambda^n A^n \simeq \bigoplus_{r=0}^{n} (\Lambda^r \mathfrak{a}) \otimes (\Lambda^{n-r} A^m) \simeq \mathfrak{a} \oplus Q$ mit einem A-Modul Q. Da $\mathfrak{a}$ vom Rang 1 ist, ergibt sich $Q = 0$.)

4) Zeige: Man hat kanonische bilineare Abbildungen $\Lambda^n M \times \Lambda^m M \longrightarrow \Lambda^{n+m} M$, definiert durch $(x_1 \wedge \ldots \wedge x_n, y_1 \wedge \ldots \wedge y_m) \longrightarrow x_1 \wedge \ldots \wedge x_n \wedge y_1 \wedge \ldots \wedge y_m$. In dem A-Modul $\Lambda M := \bigoplus_{n \geq 0} \Lambda^n M$ wird auf diese Weise eine Multiplikation erklärt, die ΛM zu einer assoziativen, aber meist nicht kommutativen, graduierten A-Algebra macht. (Wenn man das Produkt in ihr mit $\wedge$ bezeichnet, gilt $x \wedge y = (-1)^{mn} y \wedge x$ für $x \in \Lambda^n M$, $y \in \Lambda^m M$.) Die Zuordnung $M \longrightarrow \Lambda M$ ist ein Funktor. ΛM heißt äußere Algebra von M.

b) Aus 3d) folgt $\Lambda(M \oplus N) \simeq (\Lambda M) \otimes_A (\Lambda N)$, wobei das Tensorprodukt ein solches von A-Algebren ist. Vgl. 10.54 c).

5) Sei $f: A^n \longrightarrow A^n$ ein Endomorphismus. Dann ist $\Lambda^n f: \Lambda^n A^n \longrightarrow \Lambda^n A^n$ die Homothetie von $\det(f)$.

§ 15 DIFFERENTIALMODULN

Definition 15.1 Es sei A ein Ring, M ein A-Modul. Eine Derivation von A in M ist eine Abbildung $d: A \longrightarrow M$ mit den Eigenschaften

(a) $d(a+b) = d(a) + d(b)$ und

(b) $d(ab) = bd(a) + ad(b)$ für $a,b \in A$.

Bemerkungen 15.2 Sei $d: A \longrightarrow M$ eine Derivation von A in M.

a) Es ist $d(1) = d(1.1) = d(1) + d(1)$, also $d(1) = 0$.

b) Für $s \in A^*$ folgt aus $0 = d(ss^{-1}) = s^{-1}d(s) + sd(s^{-1})$, daß $d(s^{-1}) = -s^{-2}d(s)$.

c) Ker d ist ein Unterring von A:
Ker d ist eine Untergruppe von A bezüglich der Addition. Nach Bemerkung a) ist $1 \in \operatorname{Ker} d$, und für alle $a,b \in \operatorname{Ker} d$ gilt:
$d(ab) = b \cdot d(a) + a \cdot d(b) = 0$.

Beispiele 15.3 a) Sei I ein offenes Intervall in $\mathbb{R}$, A der Ring der (stetig) differenzierbaren Funktionen $I \longrightarrow \mathbb{R}$, sowie M der A-Modul aller (stetigen) Funktionen $I \longrightarrow \mathbb{R}$. Die Abbildung $d: A \longrightarrow M$, die jeder Funktion ihre Ableitung zuordnet, ist eine Derivation von A in M.

b) Sei U offen in $\mathbb{R}^n$, A der Ring der (stetig) partiell differenzierbaren Funktion $U \longrightarrow \mathbb{R}$, M der A-Modul der (stetigen) Funktionen. Dann sind die partiellen Ableitungen Derivationen von A in M.

c) Sei U offen in $\mathbb{R}^n$, A der Ring der (stetig) differenzierbaren Funktionen $U \longrightarrow \mathbb{R}$, M die Menge aller (stetigen) Abbildungen $U \longrightarrow (\mathbb{R}^n)^\vee$. ($(\mathbb{R}^n)^\vee$ ist der Dualraum des $\mathbb{R}^n$.) M ist auf kanonische Weise ein A-Modul, und die totale Ableitung $D: A \longrightarrow (\mathbb{R}^n)^\vee$ ist eine Derivation.

d) Sei A wie unter c) und $x \in U$. $M = \mathbb{R}$ sei als A-Modul gegeben durch $A \times \mathbb{R} \longrightarrow \mathbb{R}$, $(f,r) \longmapsto f(x) \cdot r$. Dann sind die partiellen Ableitungen in x Derivationen von A in M. Sei $M = (\mathbb{R}^n)^\vee$ als A-Modul gegeben durch $A \times M \longrightarrow M$, $(f,v) \longmapsto f(x) \cdot v$. Dann ist die totale Ableitung eine Derivation von A in M.

e) Sei $A = R[X_i, i \in I]$ der Polynomring in einer beliebigen Menge von Unbestimmten über einem Ring R. Dann ist jede formale partielle Ableitung $\frac{\partial}{\partial X_i}: A \longrightarrow A$ eine Derivation.

Definition 15.4 Es sei A eine R-Algebra, M ein A-Modul. Eine R-Derivation $d: A \longrightarrow M$ ist eine Derivation, die R-linear ist.

Bemerkung 15.5 a) Sei die R-Algebra-Struktur von A durch einen Homomorphismus $\varphi: R \longrightarrow A$ gegeben. Für eine Derivation $d: A \longrightarrow M$ gilt dann:

$$d \text{ ist eine } R\text{-Derivation} \iff \varphi(R) \subset \operatorname{Ker} d .$$

b) Sei $d: A \longrightarrow M$ eine R-Derivation, $\varphi: B \longrightarrow A$ ein R-Algebrenhomomorphismus und $\psi: M \longrightarrow N$ ein A-Modulhomomorphismus. Dann ist $\delta := \psi \circ d \circ \varphi: B \longrightarrow N$ eine R-Derivation.

Definition 15.6 Eine R-Derivation $d: A \to M$ heißt universelle R-Derivation von A, falls sich für jede R-Derivation $\delta: A \longrightarrow N$ das folgende Diagramm eindeutig durch eine A-lineare Abbildung φ kommutativ ergänzen läßt:

$$\begin{tikzcd} A \arrow[r, "d"] \arrow[dr, "\delta"'] & M \arrow[d, dashed, "\varphi"] \\ & N \end{tikzcd} .$$

Bemerkungen und Definition 15.7 a) Falls eine universelle R-Derivation $d: A \longrightarrow M$ existiert, so ist diese aufgrund der universellen Eigenschaft von d eindeutig bis auf einen eindeutigen Isomorphismus bestimmt.
D.h. zu universellen R-Derivationen $d: A \longrightarrow M$, $d': A \longrightarrow M'$ gibt es genau einen A-Modulisomorphismus $f: M \longrightarrow M'$, derart daß das Dreieck

$$\begin{tikzcd} A \arrow[r, "d"] \arrow[dr, "d'"'] & M \arrow[d, "f"] \\ & M' \end{tikzcd}$$

kommutativ ist.
Falls $d: A \longrightarrow M$ eine universelle R-Derivation ist, nennt man M "den" Differentialmodul von A über R. Bezeichnung: $D_R(A) := M$.

(N.B.: Der Leser möge den Differentialmodul $D_R(A)$ trotz ähnlicher Symbolik nicht mit der Divisorenhalbgruppe $D(A)$ verwechseln.)

b) Falls der Differentialmodul $D_R(A)$ existiert mit universeller Derivation $d: A \longrightarrow D_R(A)$, so ist er als A-Modul von $d(A)$ erzeugt, da der von $d(A)$ erzeugte Untermodul $\langle d(A)\rangle$ von $D_R(A)$ (zusammen mit $d|_{\langle d(A)\rangle}$) die universelle Eigenschaft des Differentialmoduls erfüllt.

Die Existenz des Differentialmoduls wird sich aus folgenden beiden Sätzen ergeben:

Satz 15.8 *Sei* $A = R[X_i, i \in I]$. *Dann existiert der Differentialmodul* $D_R(A)$. *Sei* $d: A \longrightarrow D_R(A)$ *die universelle Derivation von* A, *dann ist* $D_R(A) = \bigoplus_{i \in I} AdX_i$.

Beweis: Definiere $M := A^{(I)}$ und $d: A \longrightarrow M$, $f \longmapsto (\frac{\partial f}{\partial X_i})_{i \in I}$.
Dann ist d wohldefiniert, da $\frac{\partial f}{\partial X_i} = 0$ für fast alle $i \in I$ gilt, und offenbar eine Derivation von A in M. Bezeichne $(e_i, i \in I)$ die kanonische Basis von M. Dann ist $dX_i = e_i$ für alle $i \in I$.

Nun ist d eine universelle Derivation von A:
Sei nämlich $\delta: A \longrightarrow N$ eine Derivation mit $\delta(X_i) = n_i$ für alle $i \in I$.
Man definiere $\varphi: A^{(I)} \longrightarrow N$ durch $\varphi(e_i) = n_i$ für alle i.
Aus Definition 15.1 gewinnt man leicht die Regel $\delta(f) = \sum_{i \in I} \frac{\partial f}{\partial X_i} \cdot \delta(X_i)$ für Polynome f. Somit ist $\delta(f) = \sum_{i \in I} \frac{\partial f}{\partial X_i} n_i$ und deshalb $\delta = \varphi \circ d$.

Sei nun $\psi: M \longrightarrow N$ eine A-lineare Abbildung mit $\delta = \psi \circ d$. Dann gilt $\psi(e_i) = \psi(dX_i) = \delta(X_i) = n_i = \varphi(e_i)$ für alle $i \in I$. Also ist $\varphi = \psi$. –

Lemma 15.9 *Sei* $d: A \longrightarrow D_R(A)$ *die universelle* R*-Derivation von* A, $\mathfrak{a}$ *ein Ideal von* A. *Dann ist*

$$\mathfrak{a}D_R(A) \subset Ad(\mathfrak{a}) = \mathfrak{a}D_R(A) + d(\mathfrak{a}) .$$

Beweis: a) "$\subset$": Für alle $a \in \mathfrak{a}$ und $b \in A$ gilt:
$ad(b) = d(ab) - bd(a) \in Ad(\mathfrak{a})$. Da $D_R(A)$ nach 15.7b) von $d(A)$ erzeugt wird, ist $\mathfrak{a}D_R(A) \subset Ad(\mathfrak{a})$.

b) "=": Wegen a) gilt $\mathfrak{a}D_R(A) + d(\mathfrak{a}) \subset A\,d(\mathfrak{a})$. Umgekehrt: Für alle $a \in \mathfrak{a}$ und $b \in A$ gilt $bd(a) = -ad(b) + d(ab)$, also ist $Ad(\mathfrak{a}) \subset \mathfrak{a}D_R(A) + d(\mathfrak{a})$. –

Satz 15.10 *Wenn der Differentialmodul* $D_R(A)$ *einer* R*-Algebra von* A *existiert, dann existiert auch* $D_R(A/\mathfrak{a})$ *für jede Restklassenalgebra* $A/\mathfrak{a}$. *Man hat einen kanonischen Isomorphismus:* $D_R(A/\mathfrak{a}) \simeq D_R(A) / Ad(\mathfrak{a})$.

Beweis: Wegen Lemma 15.9 wird $D_R(A) / Ad(\mathfrak{a})$ durch $\mathfrak{a}$ annulliert, ist also auf kanonische Weise ein $A/\mathfrak{a}$-Modul. Nach dem Homomorphiesatz hat man eine eindeutig bestimmte R-lineare Abbildung $d': A/\mathfrak{a} \longrightarrow D_R(A) / Ad(\mathfrak{a})$, so daß das folgende Diagramm (in dem κ und λ die kanonischen Abbildungen sind) kommutiert:

$$\begin{array}{ccc} A & \xrightarrow{\quad d \quad} & D_R(A) \\ {\scriptstyle\kappa}\downarrow & & \downarrow{\scriptstyle\lambda} \\ A/\mathfrak{a} & \xrightarrow{\quad d' \quad} & D_R(A)/Ad(\mathfrak{a}) \end{array} .$$

Offenbar ist d' eine R-Derivation.
Sei nun N ein $A/\mathfrak{a}$-Modul und $\delta: A/\mathfrak{a} \longrightarrow N$ eine R-Derivation.
Dann ist $\delta^* := \delta \circ \kappa: A \longrightarrow N$ eine R-Derivation von A in N mit $\delta^*(\mathfrak{a}) = 0$. Die universelle Eigenschaft von $D_R(A)$ liefert einen A-Modulhomomorphismus $\varphi: D_R(A) \longrightarrow N$, so daß $\delta^* = \varphi \circ d$ gilt. Da $\delta^*(\mathfrak{a}) = 0$ ist, faktorisiert φ über $D_R(A) / Ad(\mathfrak{a})$, d.h. es existiert ein Homomorphismus $\psi: D_R(A) / Ad(\mathfrak{a}) \longrightarrow N$ mit $\varphi = \psi \circ \lambda$.

Also ist $\delta \circ \kappa = \delta^* = \varphi \circ d = \psi \circ \lambda \circ d = \psi \circ d' \circ \kappa$. Da κ surjektiv ist, ist $\delta = \psi \circ d'$. Sei nun $\psi': D_R(A) / Ad(\mathfrak{a}) \longrightarrow N$ A-linear mit $\delta = \psi' \circ d'$. Dann gilt $\psi'(\alpha) = \psi(\alpha)$ für alle $\alpha \in d'(A/\mathfrak{a})$. Da $d'(A/\mathfrak{a}) = \lambda(d(A))$ ist, wird $D_R(A) / Ad(\mathfrak{a})$ von $d'(A/\mathfrak{a})$ erzeugt. Somit ist $\psi' = \psi$. –

Folgerung 15.11 *In der Situation von Satz 15.10 ist die Folge von* $A/\mathfrak{a}$-*Moduln*

$$\mathfrak{a}/\mathfrak{a}^2 \xrightarrow{\overline{d}} D_R(A) / \mathfrak{a}D_R(A) \xrightarrow{\kappa} D_R(A/\mathfrak{a}) \longrightarrow 0$$

exakt. Hierbei ist $\overline{d}$ *von* $d: A \longrightarrow D_R(A)$ *induziert und* κ *der kanonische Homomorphismus* $D_R(A) / \mathfrak{a}D_R(A) \longrightarrow D_R(A) / Ad(\mathfrak{a}) = D_R(A/\mathfrak{a})$.
(Vgl. Lemma 15.9.)

Beweis: $\overline{d}$ ist wohldefiniert, da für alle $x,y \in \mathfrak{a}$ gilt:
$d(xy) = xd(y) + yd(x) \in \mathfrak{a}D_R(A)$. Nach Lemma 15.9 ist $Ad(\mathfrak{a}) = d(\mathfrak{a}) + \mathfrak{a}D_R(A)$ und deshalb $\operatorname{Ker} \kappa = (d(\mathfrak{a}) + \mathfrak{a}D_R(A)) / \mathfrak{a}D_R(A) = \operatorname{im} \overline{d}$.
Somit ist die Sequenz exakt. –

Folgerung 15.12 *Für alle R-Algebren A existiert der Differentialmodul* $D_R(A)$. –

Satz 15.13 *Sei* S *eine multiplikative Teilmenge einer R-Algebra* A. *Dann hat man einen kanonischen Isomorphismus von* $S^{-1}A$-*Moduln*
$D_R(S^{-1}A) \simeq S^{-1}D_R(A)$.

Beweis: Man definiere $d': S^{-1}A \longrightarrow S^{-1}D_R(A)$ durch $d'(\frac{a}{s}) = \frac{sd(a)-ad(s)}{s^2}$.

a) d' ist wohldefiniert:
Seien $t,s,s' \in S$ und $a,a' \in A$ mit $t(sa'-s'a) = 0$. Dann ist $t^2s'^2(sd(a)-ad(s)) = t^2s^2(s'd(a')-a'd(s'))$, wie man sich leicht überzeugt, also ist $d'(\frac{a}{s}) = d'(\frac{a'}{s'})$ in $S^{-1}D_R(A)$.

b) d' ist eine R-Derivation:
Seien $a,b \in A$, $s,t \in S$.

i) $d'(\frac{a}{s} + \frac{b}{t}) = d'(\frac{ta+sb}{st}) = \frac{st^2d(a)-at^2d(s)+s^2td(b)-s^2bd(t)}{(st)^2} = d'(\frac{a}{s}) + d'(\frac{b}{t})$.

ii) $d'(\frac{a}{s}\cdot\frac{b}{t}) = d'(\frac{ab}{st}) = \frac{as(td(b)-bd(t))}{(st)^2} + \frac{bt(sd(a)-ad(s))}{(st)^2} =$
$= \frac{a}{s}d'(\frac{b}{t}) + \frac{b}{t}d'(\frac{a}{s})$.

iii) $d'(\frac{a}{1}) = d(a)$, insbesondere $d'(R) = 0$.

c) d' ist eine universelle R-Derivation:
Sei N ein $S^{-1}A$-Modul und $\delta\colon S^{-1}A \longrightarrow N$ eine R-Derivation.

$$\begin{tikzcd}
A \arrow[r, "d"] \arrow[d, "i_{A,S}"] & D_R(A) \arrow[d, "i_{D_R(A),S}"] \arrow[dd, bend left=70, "\varphi"] \\
S^{-1}A \arrow[r, "d'"] \arrow[dr, "\delta"'] & S^{-1}D_R(A) \arrow[d, dashed, "\varphi'"] \\
& N
\end{tikzcd}$$

Dann ist $\delta \circ i_{A,S}$ eine R-Derivation, wird also durch einen A-Modulhomomorphismus $\varphi\colon D_R(A) \longrightarrow N$ gegeben. Man definiert φ' durch $\varphi'(\frac{m}{s}) := \frac{1}{s}\,\varphi(m)$, d.h. $\varphi' := S^{-1}\varphi$, wenn man N mit $S^{-1}N$ identifiziert (vgl. 3.34). φ' ist insbesondere $S^{-1}A$-linear. Wenn $\varphi''\colon S^{-1}D_R(A) \longrightarrow N$ eine weitere $S^{-1}A$-lineare Abbildung mit $\varphi'' \circ d' = \delta$ ist, so erhält man $\varphi'' \circ i_{D_R(A),S} \circ d = \delta \circ i_{A,S}$ und deshalb $\varphi'' \circ i_{D_R(A),S} = \varphi' \circ i_{D_R(A),S}$ wegen der Universalität von d. Mit 3.34 folgt dann $\varphi'' = \varphi'$. –

Folgerung 15.14 *Sei A eine R-Algebra endlichen Typs, S eine multiplikative Teilmenge von A. Dann ist $D_R(S^{-1}A)$ ein endlicher $S^{-1}A$-Modul.*

Beweis: Da A als R-Algebra isomorph zu $R[X_1,\dots,X_n]/\mathfrak{a}$ für geeignete n und $\mathfrak{a}$ ist, folgt dies sofort aus 15.8, 15.10 und 15.13. –

Feststellung und Definition 15.15 *Seien $\varphi\colon A \longrightarrow B$ ein R-Algebrenhomomorphismus, $d\colon A \longrightarrow D_R(A)$ und $d'\colon B \longrightarrow D_R(B)$ die universellen Derivationen. Dann ist $d' \circ \varphi$ eine Derivation von A in $D_R(B)$. Also existiert genau ein Homomorphismus $\alpha\colon D_R(A) \longrightarrow D_R(B)$ von A-Moduln mit $d' \circ \varphi = \alpha \circ d$. Diesen Homomorphismus bezeichnet man mit $D_R(\varphi)$. Die Abbildung zwischen Kategorien $D_R\colon$ {R-Algebren} $\longrightarrow$ {R-Moduln}, definiert durch $A \mapsto D_R(A)$, $\varphi \longmapsto D_R(\varphi)$, ist ein Funktor.*

Beweis: i) Sei $\varphi = \mathrm{id}_A$. Dann ist $d \circ \varphi = \mathrm{id}_{D_R(A)} \circ d$, also ist $D_R(\mathrm{id}_A) = \mathrm{id}_{D_R(A)}$.
ii) Sei $\psi\colon B \longrightarrow C$ ein weiterer R-Algebrenhomomorphismus, und $d''\colon C \longrightarrow D_R(C)$ sei die universelle Derivation von C. Dann ist $d'' \circ \psi \circ \varphi = D_R(\psi) \circ d' \circ \varphi = D_R(\psi) \circ D_R(\varphi) \circ d$, also ist $D_R(\psi \circ \varphi) = D_R(\psi) \circ D_R(\varphi)$. –

Sei $\varphi\colon A \longrightarrow B$ ein R-Algebrenhomomorphismus. Dann ist $\mathrm{Im}(D_R(\varphi))$ ein A-Untermodul des B-Moduls $D_R(B)$. Mit $B \cdot \mathrm{Im}(D_R(\varphi))$ sei der von $\mathrm{Im}(D_R(\varphi))$ erzeugte B-Untermodul von $D_R(B)$ bezeichnet.

Satz 15.16 *In obiger Situation hat man einen kanonischen Isomorphismus*

$$D_A(B) \simeq D_R(B) \,/\, B\cdot \mathrm{Im}(D_R(\varphi))\ .$$

Sei $d\colon B \longrightarrow D_R(B)$ *die universelle Derivation von* B *über* R *und* $\kappa\colon D_R(B) \longrightarrow D_R(B) \,/\, B\cdot\mathrm{Im}(D_R(\varphi))$ *der kanonische Homomorphismus. Dann ist* $\kappa \circ d\colon B \longrightarrow D_R(B)\,/\,B\cdot\mathrm{Im}(D_R(\varphi))$ *die universelle A-Derivation von* B.

Beweis: Wegen $B\cdot\mathrm{Im}(D_R(\varphi)) = B\cdot d(\varphi(A))$ ist $\kappa \circ d(\varphi(A)) = 0$, also $\kappa \circ d$ eine A-Derivation.

Zur universellen Eigenschaft: Sei M ein B-Modul und $\delta\colon B \longrightarrow M$ eine A-Derivation, d.h. $\delta(\varphi(A)) = 0$. Da δ insbesondere eine R-Derivation ist, existiert genau ein B-Modulhomomorphismus $\alpha\colon D_R(B) \longrightarrow M$ mit $\delta = \alpha \circ d$. Betrachte das kommutative Diagramm (in dem $\bar\alpha$ noch konstruiert werden muß):

$$\begin{tikzcd} B \arrow[r, "d"] \arrow[dr, "\delta"'] & D_R(B) \arrow[r, "\kappa"] \arrow[d, "\alpha"] & D_R(B)\,/\,B\cdot\mathrm{Im}(D_R(\varphi)) \arrow[dl, dashed, "\bar\alpha"] \\ & M & \end{tikzcd}$$

Es ist $\alpha(d(\varphi(A))) = \delta(\varphi(A)) = 0$, also auch $\alpha(B\cdot\mathrm{Im}(D_R(\varphi))) = 0$. Nach dem Homomorphiesatz existiert ein eindeutiger Homomorphismus $\bar\alpha$, der obiges Diagramm kommutativ macht. —

Satz 15.17 *Sei* $K(\alpha) \supset K$ *eine einfache algebraische Körpererweiterung,* $f = \Sigma a_i X^i \in K[X]$ *das Minimalpolynom von* α *über* K. *Ferner seien* V *ein ein* $K(\alpha)$*-Vektorraum,* $\delta\colon K \longrightarrow V$ *eine Derivation und* $u \in V$. *Genau dann läßt sich* δ *zu einer Derivation* $\tilde\delta\colon K(\alpha) \longrightarrow V$ *mit* $\tilde\delta(\alpha) = u$ *fortsetzen, wenn* $\Sigma \alpha^i\,\delta(a_i) + f'(\alpha)u = 0$ *ist.*

Beweis: "$\Rightarrow$": Sei $\tilde\delta\colon K(\alpha) \longrightarrow V$ eine Derivation mit $\tilde\delta(\alpha) = u$ und $\tilde\delta|_K = \delta$. Dann ist

$$0 = \tilde\delta(0) = \tilde\delta(\Sigma a_i\alpha^i) = \Sigma\alpha^i\delta(a_i) + \Sigma a_i\cdot i\cdot\alpha^{i-1}\tilde\delta(\alpha) = \Sigma\alpha^i\delta(a_i) + f'(\alpha)u\ .$$

"$\Leftarrow$": Es gelte $(*)$ $\Sigma\alpha^i\delta(a_i) + f'(\alpha)u = 0$.

Vermöge des K-Algebrenhomomorphismus $\varphi\colon K[X] \longrightarrow K(\alpha)$, definiert durch $\varphi(X) = \alpha$, wird V zu einem $K[X]$-Modul.

Man sieht leicht, daß folgende Abbildungen Derivationen sind:

$\delta_1\colon K[X] \longrightarrow V,\ \Sigma b_iX^i \longmapsto \Sigma X^i\delta(b_i) = \Sigma\alpha^i\delta(b_i)$ und

$\delta_2\colon K[X] \longrightarrow V,\quad g(X) \longmapsto g'(X)\cdot u = g'(\alpha)u$.

Hierbei ist $\delta_1|_K = \delta$ und $\delta_2|_K = 0$.

Folglich ist $\delta_1+\delta_2$ eine Fortsetzung von δ auf $K[X]$. Wegen $(*)$ ist ferner $(\delta_1+\delta_2)(f) = 0$, und für alle $g \in K[X]$ gilt

$(\delta_1+\delta_2)(gf) = f\cdot(\delta_1+\delta_2)(g) + g\cdot(\delta_1+\delta_2)(f) = 0$, denn es ist $f \in \mathrm{Ann}\,V$.

Also faktorisiert $\delta_1+\delta_2$ über $K[X]/(f) \simeq K(\alpha)$ durch $\tilde\delta\colon K(\alpha) \longrightarrow V$.

Offensichtlich ist $\tilde\delta$ eine Derivation. —

Folgerung 15.18 *a) Sei $L \supset K$ eine separable algebraische Körpererweiterung. Dann läßt sich jede Derivation von K in einen L-Vektorraum auf genau eine Weise zu einer Derivation von L fortsetzen. Insbesondere ist $D_K(L) = 0$.*
b) Sei $L \supset K$ eine endliche Körpererweiterung und $D_K(L) = 0$. Dann ist L separabel über K.

Beweis: a) Sei zunächst L endlich über K. Nach dem Satz vom primitiven Element ist $L = K(\alpha)$ für ein geeignetes $\alpha \in L$. Sei $f = \Sigma\, a_i X^i :=$ $\mathrm{Mipo}(\alpha,K)$. Es ist $f'(\alpha) \neq 0$, da α separabel über K ist. Zu jeder Derivation $\delta\colon K \longrightarrow V$ mit einem L-Vektorraum V gibt es deshalb genau ein $u \in V$ mit $\Sigma\, \alpha^i \delta(a_i) + f'(\alpha)u = 0$, also nach 15.17 genau eine Fortsetzung nach L.

Sei nun L nicht notwendig endlich über K. Dann ist $L = \cup\, E$, wobei E diejenigen Körper zwischen K und L durchläuft, die endlich über K sind. Zu je zwei solchen Körpern E_1, E_2 gibt es einen dritten solchen E_3 mit $E_1 \cup E_2 \subset E_3$. Da es nach jedem solchen E genau eine Fortsetzung einer Derivation $\delta\colon K \longrightarrow V$ gibt, sieht man leicht die Eindeutigkeit und Existenz einer Fortsetzung nach L.

b) Angenommen, $L \supset K$ sei nicht separabel. Sei K_0 die separable Hülle von K in L. Dann ist die Erweiterung $L \supset K_0$ radiziell (i.e. rein inseparabel) und nichttrivial. Da $L \supset K$, also erst recht $L \supset K_0$ endlich ist, ist K_0 in einem maximalen echten Teilkörper K_1 von L enthalten. Dann ist $[L:K_1] = p = \mathrm{char}\, L > 1$ und $L = K_1(\alpha)$ mit einem $\alpha \in L$, für das $a := \alpha^p \in K_1$ ist. Es ist $f := \mathrm{Mipo}(\alpha,K_1) = X^p - a$, also $f' = 0$. Sei $V \neq 0$ ein L-Vektorraum und $u \in V - \{0\}$. Nach 15.17 gibt es eine Derivation $\tilde{\delta}\colon L \longrightarrow V$ mit $\tilde{\delta}(\alpha) = u$, welche die triviale Derivation $\delta\colon K_1 \longrightarrow V$ fortsetzt, d.h. eine K_1-Derivation ist. Dann ist $\tilde{\delta}$ erst recht eine K-Derivation von L, und zwar eine nichttriviale, da $\tilde{\delta}(\alpha) \neq 0$ ist. Dann muß aber $D_K(L) \neq 0$ sein. —

Bemerkungen 15.19 a) Sei L ein vollkommener Körper mit $\mathrm{char}\, L = p > 0$, d.h. $L = L^p$. Ferner seien $a, \alpha \in L$ mit $a = \alpha^p$ und d eine Derivation von L. Dann ist $d(a) = d(\alpha^p) = p\alpha^{p-1} d(\alpha) = 0$. Für jeden Teilkörper K von L ist deshalb $D_K(L) = 0$.
Trotzdem kann $L \supset K$ inseparabel (aber dann nicht endlich) sein.
Beispiel: $K = k(X)$, $L = \bigcup_{n \geq 0} K^{-p^n}$.

b) Sei $L = K(X_i,\ i \in I)$ eine rein transzendente Körpererweiterung von K.

Dann ist $D_K(L) = L^{(I)}$; denn es ist $L = S^{-1}K[X_i, i \in I]$ mit $S = K[X_i, i \in I] \setminus \{0\}$ (15.8 und 15.13).

Definition 15.20 Eine Körpererweiterung $L \supset K$ heißt endlich erzeugt, wenn es eine endliche Menge $M \subset L$ mit $L = K(M)$ gibt, d.h. wenn L der Quotientenkörper einer integren K-Algebra von endlichem Typ ist.

Satz 15.21 *Sei* $L \supset K$ *eine endlich erzeugte Körpererweiterung,* $d: L \longrightarrow D_K(L)$ *die universelle* K-*Derivation und* $M \subset L$ *minimal unter allen Mengen* $N \subset L$, *für die* $L \supset K(N)$ *separabel algebraisch ist. Dann ist* $d(M)$ *eine Basis des* L-*Vektorraumes* $D_K(L)$.

Beweis: Gemäß 15.16 gilt für eine beliebige Teilmenge M' von L die Isomorphie

(*) $$D_{K(M')}(L) \simeq D_K(L) / L \cdot d(K(M')) .$$

Ferner ist $d(K(M'))$ enthalten in $\langle d(M')\rangle$, dem von $d(M')$ erzeugten L-Vektorraum, d.h.

(**) $$L \cdot d(K(M')) = \langle d(M')\rangle .$$

(Man sieht dies wie folgt: Für Elemente $x \in M'$ und $a \in K$ ist $dx \in d(M')$ und $da = 0 \in \langle d(M')\rangle$. Wenn aber $f,g \in K(M')$ die Eigenschaft $df, dg \in \langle d(M')\rangle$ haben, sind auch $d(f+g) = df + dg$, $d(fg) = f \cdot dg + g \cdot df$ und $d(\frac{f}{g}) = \frac{1}{g} \cdot df - \frac{f}{g^2} dg$ Elemente von $\langle d(M')\rangle$.)

Sei jetzt $M' = M$. Dann ist $D_{K(M)}(L) = 0$ nach 15.18a). Wegen (*) und (**) ist $D_K(L)$ von $d(M)$ erzeugt.

Um die lineare Unabhängigkeit von $d(M)$ zu zeigen, sei $x \in M$ und $M' = M - \{x\}$. Nach Wahl von M ist x entweder transzendent oder inseparabel algebraisch über $K(M')$.

Im ersten Fall ist $D_{K(M')}(K(M)) \simeq K(M)$ nach 15.19b). (Es ist $K(M) = Q(K(M')[x])$.) Die universelle $K(M')$-Derivation $d: K(M) \longrightarrow D_{K(M')}(K(M))$ ist nicht trivial und läßt sich nach 15.18a) zu einer Derivation $\delta: L \longrightarrow D_{K(M')}(K(M)) \otimes_{K(M)} L \simeq L$ fortsetzen. Also ist $D_{K(M')}(L) \neq 0$.

Im zweiten Fall ist $D_{K(M')}(L) \neq 0$ nach 15.18b).

In beiden Fällen ist $D_K(L) \neq L \cdot d(K(M'))$ nach (*), also $D_K(L)$ nicht von $d(M')$ erzeugt nach (**). Da also keine echte Teilmenge von $d(M)$ den L-Vektorraum $D_K(L)$ erzeugt, ist $d(M)$ linear unabhängig. —

Definition 15.21 a) Eine Transzendenzbasis $(x_i)_{i\in I}$ einer Körpererweiterung $L \supset K$ heißt separierend, wenn L über $K(x_i;\ i \in I)$ separabel (algebraisch) ist.
b) Eine (nicht notwendig algebraische) Körpererweiterung heißt separabel, wenn sie eine separierende Transzendenzbasis besitzt.

Folgerung 15.22 *Sei $L \supset K$ eine endlich erzeugte Körpererweiterung. Dann ist $\mu_L(D_K(L)) \geq \operatorname{trgd}_K L$. Gleichheit gilt hier genau dann, wenn $L \supset K$ separabel ist.* –

Folgerung 15.23 *Sei $L \supset K$ eine endlich erzeugte, separable Körpererweiterung, $d: L \longrightarrow D_K(L))$ die universelle Derivation von L über K und $x_1,\ldots,x_n \in L$. Dann sind äquivalent:*
(i) $(x_1,\ldots,x_n)$ *ist eine separierende Transzendenzbasis von* $L \supset K$;
(ii) $(d(x_1),\ldots,d(x_n))$ *ist eine Basis von* $D_K(L)$ *über* L. –

Folgerung 15.24 (MacLane) *Sei $L \supset K$ endlich erzeugt und separabel. Dann enthält jedes Erzeugendensystem von L über K eine separierende Transzendenzbasis.* –

Satz 15.25 *Seien $k \hookrightarrow K$ und $K \overset{\varphi}{\hookrightarrow} L$ Körpererweiterungen, wobei $L \supset K$ separabel algebraisch ist. Ferner seien $d_L: L \longrightarrow D_k(L)$ die universelle k-Derivation von L und $d_K: K \longrightarrow D_k(K)$ die universelle k-Derivation von K. Dann induziert $D_k(\varphi): D_k(K) \longrightarrow D_k(L)$ einen Isomorphismus $f: D_k(K) \otimes_K L \longrightarrow D_k(L)$, definiert durch*
$f(\omega \otimes 1) := 1\cdot D_k(\varphi)(\omega)$.

Beweis: Da $L \supset K$ separabel algebraisch ist, ist $D_k(L)$ von $d_L(K)$ erzeugt, also ist f surjektiv.

Da $D_k(K)$ von $d_K(K)$ erzeugt wird, existieren $x_i \in K$ $(i \in I)$, so daß $(d_K(x_i) \mid i \in I)$ eine Basis von $D_k(K)$ ist. Sei $(h_i \mid i \in I)$ die duale Basis zu $(d_K(x_i) \mid i \in I)$, d.h. für jedes $i \in I$ sei $h_i: D_k(K) \longrightarrow K$ die durch $h_i(d_K(x_j)) = \delta_{ij}$ (Kroneckersymbol) definierte Linearform.

Da L über K separabel algebraisch ist, läßt sich für alle $i \in I$ die k-Derivation $\varphi \circ h_i \circ d_K: K \longrightarrow L$ eindeutig fortsetzen zu einer k-Derivation $\tilde{\delta}_i: L \longrightarrow L$.
Aufgrund der universellen Eigenschaft von $D_K(L)$ ist $\tilde{\delta}_i$ durch einen Homomorphismus $\tilde{h}_i: D_k(L) \longrightarrow L$ gegeben, d.h. $\tilde{h}_i \circ d_L = \tilde{\delta}_i$.

Nun ist $\delta_{ij} = (\varphi \circ h_i \circ d_K)(x_j) = \tilde{h}_i d_L(x_j) = h_i(D_k(\varphi)(d_K(x_j)))$. Daher ist $(D_k(\varphi)(d_K(x_i)) \mid i \in I)$ linear unabhängig und somit f injektiv. –

Satz 15.26 *Seien* $k \hookrightarrow K$ *und* $K \overset{\varphi}{\hookrightarrow} L$ *Körpererweiterungen, wobei* k *vollkommen und* $L \supset K$ *endlich sei. Dann gilt:*

$$\mu_K D_k(K) = \mu_L D_k(L) .$$

(Achtung: Im allgemeinen ist der von $D_k(\varphi)$ induzierte Homomorphismus $D_k(K) \otimes_K L \longrightarrow D_k(L)$ kein Isomorphismus.

Beweis: Wegen 15.25 kann man annehmen, daß $L \supset K$ radiziell (d.h. rein inseparabel) ist. Ferner kann man den Beweis auf den Fall reduzieren, daß $[L:K] = p = \text{char } K$ ist. Es gibt dann ein α mit $L = K(\alpha)$ und $\alpha^p =: a \in K$.

Im folgenden zeigen wir: Der Kern des K-Vektorraumhomomorphismus $D_k(\varphi)$ wird von $d_K(a) \neq 0$ erzeugt, während ein Komplement von $L \cdot \text{Im } D_k(\varphi)$ in $D_k(L)$ von $d_L(\alpha)$ erzeugt wird. Hieraus folgt die Behauptung.

Behauptung 1: $d_K(a) \neq 0$, d.h. es gibt eine k-Derivation $\delta: K \longrightarrow K$ mit $\delta(a) \neq 0$.

Da k vollkommen ist, ist $k^p = k$, also $k \subset K^p$. Wäre $a \in K^p$, so wäre $\alpha \in K$ im Widerspruch zur Wahl von α.

Nach dem Lemma von Zorn existiert ein maximaler Zwischenkörper F von $K \supset K^p$ mit $a \notin F$. Für alle $b \in K - F$ gilt $F(a) \subset F(b)$ nach Konstruktion von F. Wegen $b^p \in K^p \subset F$ ist aber $[F(b):F] = p = [F(a):F]$, also $F(a) = F(b)$. Somit ist $K = F(a)$.

Da $D_F(F(a)) \neq 0$ ist, existiert eine F-Derivation, also eine k-Derivation $\delta: F(a) \longrightarrow F(a)$ mit $\delta(a) \neq 0$.

Behauptung 2: $d_K(a)$ erzeugt $\text{Ker}(d_k(\varphi))$.

Da $D_k(K)$ von $d_k(K)$ erzeugt ist, existieren $b_i \in K$ $(i \in I)$, so daß $d_K(a)$ durch $(d_K(b_i) \mid i \in I)$ zu einer Basis von $D_k(K)$ fortgesetzt wird. Da $d_L(a) = d_L(\alpha^p) = p\alpha^{p-1} d_L(\alpha) = 0$ ist, genügt es, folgendes zu zeigen:

$$(D_k(\varphi)(d_K(b_i)) \mid i \in I) \text{ ist linear unabhängig über } L .$$

Für $i \in I$ sei $h_i: D_k(K) \longrightarrow K$ die Linearform mit $h_i(d_K(b_j)) = \delta_{ij}$ und $h_i(d_K(a)) = 0$, sowie $\delta_i := h_i \circ d_K$.

$$\begin{tikzcd}
K \arrow[r, "d_K"] \arrow[d, "\varphi"] \arrow[rr, bend left, "\delta_i"] & D_k(K) \arrow[r, "h_i"] \arrow[d, "D_k(\varphi)"] & K \arrow[d, "\varphi"] \\
L \arrow[r, "d_L"] \arrow[rr, bend right, "\tilde{\delta}_i"'] & D_k(L) \arrow[r, "\tilde{h}_i"] & L
\end{tikzcd}$$

Nach 15.17 läßt sich die k-Derivation $\varphi \circ \delta_i$ zu einer k-Derivation $\tilde{\delta}_i\colon L \longrightarrow L$ fortsetzen, da $\delta_i(1)\alpha^p - \delta_i(a) = -\delta_i(a) = 0$ sowie $(X^p-a)'(\alpha)u = p\alpha^{p-1}u = 0$ für alle $u \in L$ gilt. $\tilde{h}_i$ sei durch $\tilde{\delta}_i$ bestimmt. Nun ist $\delta_{ij} = \varphi(h_i(d_K(b_j))) = \tilde{h}_i d_L(\varphi(b_j)) = \tilde{h}_i(D_k(\varphi)(d_K(b_j)))$. Daher ist $(D_k(\varphi)(d_K(b_i)) \mid i \in I)$ linear unabhängig über L.

<u>Behauptung 3:</u> $L \cdot d_L(\alpha)$ ist komplementär zu $L \cdot \operatorname{Im} D_k(\varphi)$ in $D_k(L)$. $D_k(L)$ wird von $d_L(K) \cup \{d_L(\alpha)\}$ erzeugt. Aber $d_L(\alpha) \notin d_L(K)$, da $D_K(L) \neq 0$. –

<u>Folgerung 15.27</u> (F.K. Schmidt) *Sei* k *ein vollkommener Körper, und* $K \supset k$ *sei eine endlich erzeugte Körpererweiterung. Dann ist* $K \supset k$ *separabel, und es gilt*

$$\mu_K(D_k(K)) = \operatorname{trgd}_k K .$$

<u>Beweis:</u> Sei $x_1,\dots,x_n$ eine Transzendenzbasis von $K \supset k$, und $F := k(x_1,\dots,x_n)$. Dann ist $\mu_F(D_k(F)) = n$. Nach Satz 15.26 ist dann auch $\mu_K(D_k(K)) = n$.
Nach Satz 15.21 gibt es also $y_1,\dots,y_n \in K$, so daß $K \supset k(y_1,\dots,y_n)$ separabel algebraisch ist. Da $\{y_1,\dots,y_n\}$ eine Transzendenzbasis enthält und $\operatorname{trgd}_k K = n$ ist, ist $y_1,\dots,y_n$ eine Transzendenzbasis von K über k. –

<u>Aufgabe</u> (Grothendiecks Beschreibung des Differentialmoduls)
Sei R ein Ring, A eine R-Algebra. Man hat einen R-Algebrenhomomorphismus $\varphi\colon A \otimes_R A \longrightarrow A$, definert durch $a \otimes b \longrightarrow ab$. (Hier ist ein wenig zu zeigen.) Sei $I := \operatorname{Ker} \varphi$. Die Abbildung $d'\colon A \longrightarrow A \otimes_R A$, $a \longmapsto 1 \otimes a - a \otimes 1$ hat offenbar ihr Bild in I. Verknüpft mit der kanonischen Projektion $I \longrightarrow I/I^2$ erhält man eine Abbildung $d\colon A \longrightarrow I/I^2$.

Zeige: I/I^2 ist auf kanonische Weise ein A-Modul, und d ist "die" universelle R-Derivation von A, also $D_R(A) \simeq I/I^2$.
(Beachte, daß man auf $A \otimes_R A$, also auch auf I zwei naheliegende

A-Modulstrukturen hat, die i.a. nicht übereinstimmen. Diese beiden A-Modulstrukturen induzieren aber auf $(A \otimes_R A)/I \simeq A$ dieselbe Struktur, und zwar die kanonische A-Modulstruktur von A. Da I/I^2 von I annulliert wird, wird auch auf I/I^2 eine kanonische A-Modulstruktur induziert. Man rechnet dann leicht nach, daß d eine R-Derivation ist. Ferner kann man zeigen, daß I als A-Modul - bzgl. einer beliebigen der beiden A-Modulstrukturen - von $d'(A)$ erzeugt wird. $(\Sigma(a_i \otimes b_i) - \Sigma a_i d'(b_i) = \Sigma(a_i b_i \otimes 1) = 0$, wenn $\Sigma a_i \otimes b_i \in I$, d.h. $\Sigma a_i b_i = 0$ gilt.) Wenn $\delta: A \longrightarrow M$ eine R-Derivation ist, definiere $\varepsilon': I \longrightarrow M$ durch $a \otimes b \longmapsto a \cdot \delta(b)$. Man zeigt $\varepsilon'(I^2) = 0$ mit Hilfe der Tatsache, daß I^2 als A-Modul von Elementen der Form $(1 \otimes a - a \otimes 1)\cdot(1 \otimes b - b \otimes 1)$ erzeugt wird. Man erhält eine A-lineare Abbildung $\varepsilon: I/I^2 \longrightarrow M$. Ihre Eindeutigkeit ergibt sich daraus, daß I/I^2 von $d(A)$ erzeugt wird.)

§16 REGULARITÄTSKRITERIEN

Lemma 16.1 *Es sei* A *ein lokaler Ring mit maximalem Ideal* $\mathfrak{m}$, $f \in A[X]$ *und* $\alpha \in A$ *mit* $f(\alpha) \in \mathfrak{m}$ *und* $f'(\alpha) \notin \mathfrak{m}$.
Dann ist $f(\alpha - \frac{f(\alpha)}{f'(\alpha)}) \in \mathfrak{m}^2$.

Beweis: Sei $f = \sum_{i=0}^{n} a_i X^i$. Dann ist für $\alpha, \beta \in A$

$$f(\alpha+\beta) = \sum_{i=0}^{n} a_i(\alpha+\beta)^i = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} a_i \alpha^{i-j}\beta^j = \sum_{j=0}^{n} \beta^j \sum_{i=j}^{n} \binom{i}{j} a_i \alpha^{i-j} .$$

(Nebenbei bemerkt: Wenn $\mathbb{Q} \subset A$ ist, folgt hieraus

$$f(\alpha+\beta) = \sum_{j=0}^{n} \frac{\beta^j}{j!} f^{(j)}(\alpha) ,$$

die bekannte Taylorformel.)

Also ist

$$f(\alpha - \frac{f(\alpha)}{f'(\alpha)}) = f(\alpha) - \frac{f(\alpha)}{f'(\alpha)} f'(\alpha) + \sum_{j=2}^{n} (- \frac{f(\alpha)}{f'(\alpha)})^j \sum_{i=j}^{n} \binom{i}{j} a_i \alpha^{i-j}) \in \mathfrak{m}^2 . -$$

Definition 16.2 Sei k ein Körper. Eine k-Algebra A heißt im wesentlichen von endlichem Typ über k, wenn A von der Form $S^{-1}B$ ist, wo B eine k-Algebra von endlichem Typ und S multiplikativ in B ist.

Satz 16.3 *Sei* k *ein vollkommener Körper,* A *eine lokale* k*-Algebra, im wesentlichen von endlichem Typ mit maximalem Ideal* $\mathfrak{m}$. *Es gelte* $\mathfrak{m}^2 = (0)$.
Dann existiert ein Teilkörper $K \subset A$ *mit* $k \subset K$, *so daß*

$$A = K \oplus \mathfrak{m}$$

gilt.
(Eine weitgehende Verallgemeinerung dieses Satzes wird in §18 bewiesen.)

Beweis: Sei $\pi: A \longrightarrow A/\mathfrak{m}$ die kanonische Projektion. Zu finden ist ein Körper K mit $k \subset K \subset A$, so daß $\pi(K) = A/\mathfrak{m}$ gilt. Dann ist nämlich $\pi|_K: K \longrightarrow A/\mathfrak{m}$ ein Isomorphismus, so daß man 3.17 anwenden kann. Nach 15.24 existiert eine separierende Transzendenzbasis von $A/\mathfrak{m}$ über k. D.h. es gibt $x_1,\ldots,x_n, y_1,\ldots,y_m \in A/\mathfrak{m}$, so daß $A/\mathfrak{m} = k(x_1,\ldots,x_n,y_1,\ldots,y_m)$ gilt, jedes y_i separabel algebraisch über $k(x_1,\ldots,x_n,y_1,\ldots,y_{i-1})$ und jedes x_i transzendent über $k(x_1,\ldots,x_{i-1})$ ist. Mit Induktion nach $n+m$ genügt es, folgende Behauptung zu zeigen:

Sei k_1 ein Körper zwischen k und A und $x \in A/\mathfrak{m}$ transzendent oder separabel algebraisch über k_1. Dann existiert ein Repräsentant $y \in A$ von x, so daß $k_1[y]$ in einem Teilkörper von A enthalten ist.

a) Sei x transzendent über k. Man wähle einen beliebigen Repräsentanten $y \in A$ von x. Durch π wird $k_1[y]$ auf $k_1[x] \simeq k_1[X]$ abgebildet; daher ist $\pi|k_1[y]$ injektiv (und insbesondere $k_1[y]$ integer). Also ist $k_1[y] \cap \mathfrak{m} = \{0\}$, und somit sind alle Elemente von $k_1[y] - \{0\}$ invertierbar in A, d.h. $k_1(y) \subset A$.

b) Sei x separabel algebraisch über k_1. Mit f sei das Minimalpolynom von x über k_1 bezeichnet und mit $\tilde{y} \in A$ ein Repräsentant von x. Dann ist $\pi(f(\tilde{y})) = f(x) = 0$, also $f(\tilde{y}) \in \mathfrak{m}$. Da x separabel über k_1 ist, ist $\pi(f'(\tilde{y})) = f'(x) \neq 0$, also $f'(\tilde{y}) \in \mathfrak{m}$. Daher gilt nach Lemma 16.1 für $y := \tilde{y} - \frac{f(\tilde{y})}{f'(\tilde{y})}$, einem Repräsentanten von x, die Identität $f(y) = 0$. Deshalb ist $k_1[y] \simeq k_1[X]/(f)$, also ein Körper in A. —

N.B.: Für eine Primzahl p ist $\mathbb{Z}/(p^2) \not\simeq \mathbb{Z}/(p) \oplus (p)/(p^2)$.
Aber $\mathbb{Z}/(p^2)$ ist auch keine Algebra über einem Körper.

Satz 16.4 *Seien* $k,A,\mathfrak{m}$ *wie in Satz 16.3 (aber nicht notwendig* $\mathfrak{m}^2=(0)$). *Dann ist die Sequenz aus 15.11*

$$0 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\delta} D_k(A)/\mathfrak{m}D_k(A) \xrightarrow{\varphi} D_k(A/\mathfrak{m}) \longrightarrow 0$$

exakt.

Beweis: Zu zeigen ist noch die Injektivität von δ, das durch die universelle k-Derivation $d: A \longrightarrow D_k(A)$ induziert wird.

a) Reduktion auf den Fall $\mathfrak{m}^2=(0)$.

Das folgende kommutative Diagramm (mit den kanonischen Projektionen)

$$\begin{tikzcd} A \arrow[r, "\mu"] \arrow[dr, "\pi"'] & A/\mathfrak{m}^2 \arrow[d, "\lambda"] \\ & A/\mathfrak{m} \end{tikzcd}$$

liefert ein kommutatives Diagramm von k-Moduln

$$\begin{tikzcd} D_k(A) \arrow[r, "D_k(\mu)"] \arrow[dr, "D_k(\pi)"'] & D_k(A/\mathfrak{m}^2) \arrow[d, "D_k(\lambda)"] \\ & D_k(A/\mathfrak{m}) \end{tikzcd} .$$

Im folgenden Diagramm

$$\begin{tikzcd} \mathfrak{m}/\mathfrak{m}^2 \arrow[r, "\delta"] \arrow[d, "\mathrm{id}"] & D_k(A)/\mathfrak{m}D_k(A) \arrow[r, "\varphi"] \arrow[d, "\psi"] & D_k(A/\mathfrak{m}) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ \mathfrak{m}/\mathfrak{m}^2 \arrow[r, "\delta'"] & D_k(A/\mathfrak{m}^2)/\mathfrak{m}D_k(A/\mathfrak{m}^2) \arrow[r, "\varphi'"] & D_k(A/\mathfrak{m}) \arrow[r] & 0 \end{tikzcd}$$

seien die Zeilen gemäß 15.11 gegeben; insbesondere ist φ durch $D_k(\pi)$ und φ' durch $D_k(\lambda)$ induziert; ψ sei durch $D_k(\mu)$ induziert. Also ist das Diagramm kommutativ, und falls δ' injektiv ist, ist δ injektiv.

b) Sei jetzt $\mathfrak{m}^2=(0)$. Nach 16.3 existiert ein Teilkörper K von A mit $k \subset K$ und $A = K \oplus \mathfrak{m}$.

Die Abbildung $\varepsilon: K \oplus \mathfrak{m} \longrightarrow \mathfrak{m}$, $(x,m) \longmapsto m$, ist additiv, und man hat $\varepsilon(k) \subset \varepsilon(K) = 0$. Ferner gilt für $x_i \in K$, $m_i \in \mathfrak{m}$ $(i=1,2)$ offenbar $(x_1,m_1)\cdot(x_2,m_2) = (x_1x_2, x_1m_2 + x_2m_1)$, also $\varepsilon((x_1,m_1)\cdot(x_2,m_2)) =$
$= x_1m_2 + x_2m_1 = (x_1,m_1)m_2 + (x_2,m_2)m_1 = (x_1,m_1)\varepsilon(x_2,m_2)+(x_2,m_2)\varepsilon(x_1,m_1)$.
Somit ist ε eine k-Derivation von A und entspricht daher einem Homomorphismus $\alpha: D_k(A) \longrightarrow \mathfrak{m}$.

Da $\varepsilon|\mathfrak{m} = \mathrm{id}_{\mathfrak{m}}$, ist $\alpha \circ d|_{\mathfrak{m}} = \mathrm{id}_{\mathfrak{m}}$, wo $d: A \longrightarrow D_k(A)$ die universelle Derivation bezeichnet. Tensoriert man die Folge $\mathfrak{m} \xrightarrow{d|\mathfrak{m}} D_k(A) \xrightarrow{\alpha} \mathfrak{m}$ mit

$A/\mathfrak{m}$, so erhält man (wegen $\mathfrak{m}^2 = (0)$) eine Folge
$\mathfrak{m} \xrightarrow{d'} D_k(A)/\mathfrak{m}D_k(A) \xrightarrow{\alpha'} \mathfrak{m}$ mit $\alpha' \circ d' = id_{\mathfrak{m}}$. Deshalb ist d' injektiv. Nach Konstruktion ist aber $\delta = d'$ (im Falle $\mathfrak{m}^2 = (0)$). –

<u>Folgerung 16.5</u> *Sei* k *ein vollkommener Körper,* A *eine lokale* k*-Algebra, im wesentlichen von endlichem Typ, mit maximalem Ideal* $\mathfrak{m}$. *Dann gilt:*

$$\mu_A(\mathfrak{m}) + \operatorname{trgd}_k(A/\mathfrak{m}) = \mu_A(D_k(A)) .$$

<u>Beweis:</u> Aus Satz 16.4 folgt $\mu_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) + \mu_{A/\mathfrak{m}} D_k(A/\mathfrak{m}) = \mu_{A/\mathfrak{m}}\big(D_k(A)/\mathfrak{m}D_k(A)\big)$. Da k vollkommen ist, ist $A/\mathfrak{m}$ eine separabel erzeugte Körpererweiterung von k. Nach 15.26 gilt also $\mu_{A/\mathfrak{m}}(D_k(A/\mathfrak{m})) = \operatorname{trgd}_k A/\mathfrak{m}$.
Mit 12.10 folgt $\mu_A(\mathfrak{m}) + \operatorname{trgd}_k(A/\mathfrak{m}) = \mu_A(D_k(A))$. –

<u>Bemerkung 16.6</u> Sei k ein (nicht notwendig vollkommener) Körper.
Wir werden unter 17.25 zeigen:

Für eine integre k-Algebra B von endlichem Typ und ein Primideal $\mathfrak{p} \in B$ gilt:

$$\dim B_{\mathfrak{p}} + \dim B/\mathfrak{p} = \dim B .$$

Nach 9.2 gilt ferner $\dim B/\mathfrak{p} = \operatorname{trgd}_k Q(B/\mathfrak{p})$.
Folgerung 16.5 liefert für $A = B_{\mathfrak{p}}$ und vollkommenes k die Gleichung:

$$\mu_{B_{\mathfrak{p}}}(\mathfrak{p}B_{\mathfrak{p}}) + \operatorname{trgd}_k(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}) = \mu_{B_{\mathfrak{p}}}(D_k(B_{\mathfrak{p}})) .$$

Nun ist $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq Q(B/\mathfrak{p})$, und nach 15.13 gilt $D_k(B_{\mathfrak{p}}) \simeq D_k(B)_{\mathfrak{p}}$.
Also folgt $\mu_{B_{\mathfrak{p}}}(\mathfrak{p}B_{\mathfrak{p}}) + \dim B = \mu_{B_{\mathfrak{p}}}(D_k(B)_{\mathfrak{p}}) + \dim B_{\mathfrak{p}}$.
Da $B_{\mathfrak{p}}$ genau dann regulär ist, wenn $\mu_{B_{\mathfrak{p}}}(\mathfrak{p}B_{\mathfrak{p}}) = \dim B_{\mathfrak{p}}$ gilt, erhalten wir:

<u>Folgerung 16.7</u> *Sei* k *ein vollkommener Körper,* B *eine integre* k*-Algebra von endlichem Typ. Für* $\mathfrak{p} \in \operatorname{Spec} B$ *gilt dann:*

$$B_{\mathfrak{p}} \text{ ist regulär} \iff \dim B = \mu_{B_{\mathfrak{p}}}(D_k(B)_{\mathfrak{p}}) .$$

<u>Lemma 16.8</u> *Sei* A *ein lokaler Integritätsring und* M *ein endlich erzeugter* A*-Modul. Dann gilt:*

$$M \text{ ist frei} \iff \mu_A(M) = \mu_{Q(A)}(M \otimes_A Q(A)) .$$

<u>Beweis:</u> "$\Rightarrow$" ist klar.

"$\Leftarrow$": Sei $n = \mu_A(M)$. Dann gibt es eine exakte Folge

$$0 \longrightarrow K \longrightarrow A^n \xrightarrow{f} M \longrightarrow 0 ,$$

wo f die kanonische Basis von A^n auf ein minimales Erzeugendensystem von M abbildet.

Durch Tensorieren mit $Q(A)$ erhalten wir die exakte Folge von $Q(A)$-Vektorräumen

$$0 \longrightarrow K \otimes_A Q(A) \longrightarrow Q(A)^n \xrightarrow{f_*} M \otimes_A Q(A) \longrightarrow 0 .$$

Aus $\mu_{Q(A)}(M \otimes_A Q(A)) = n$ folgt, daß f_* bijektiv, also $K \otimes_A Q(A) = 0$ ist. Nun ist $K \otimes_A Q(A) \simeq S^{-1}K$ mit $S = A - \{0\}$. Die $s \in S$ sind keine Nullteiler für A, also auch nicht für $K \subset A^n$. Aus $S^{-1}K = 0$ folgt deshalb $K = 0$. —

<u>Satz 16.9</u> *Sei* k *ein vollkommener Körper,* A *eine lokale, integre* k*-Algebra im wesentlichen von endlichem Typ. Dann gilt:*

$$A \textit{ ist regulär} \iff D_k(A) \textit{ ist ein freier } A\textit{-Modul.}$$

<u>Beweis:</u> Es gibt eine k-Algebra B von endlichem Typ und ein $\mathfrak{p} \in \operatorname{Spec} B$ mit $A = B_{\mathfrak{p}}$. Wir haben

(*) $\qquad \dim B = \operatorname{trgd}_k(Q(B)) = \operatorname{trgd}_k(Q(A))$

wegen 9.2 und $Q(B) = Q(A)$. Da k vollkommen ist, gilt

(**) $\qquad \mu_{Q(A)}(D_k(Q(A))) = \operatorname{trgd}_k(Q(A)))$

nach 15.27. Somit haben wir:

$$\begin{aligned} A \text{ ist regulär} &\overset{16.7}{\iff} \dim B = \mu_A(D_k(A)) \\ &\overset{(*),(**)}{\iff} \mu_{Q(A)}(D_k(Q(A))) = \mu_A(D_k(A)) \\ &\overset{16.8}{\iff} D_k(A) \text{ ist frei über } A . \end{aligned}$$

(Beachte: $D_k(Q(A)) \simeq D_k(A) \otimes_A Q(A)$ nach 15.13.) —

<u>Satz 16.10</u> *Sei* A *ein noetherscher Integritätsring,* M *ein endlicher* A*-Modul. Dann gibt es ein* $s \in A - \{0\}$*, so daß* M_s *ein freier* A_s*-Modul ist.*

<u>Beweis:</u> Sei $S = A - \{0\}$ und $i_{S,M}$ der kanonische Homomorphismus $M \longrightarrow S^{-1}M$. Man hat eine exakte Sequenz von A-Moduln

$$0 \longrightarrow T \longrightarrow M \xrightarrow{i_{S,M}} S^{-1}M ,$$

wobei $T = \{x \in M \mid \exists\ s \in S \text{ mit } sx = 0\}$ ist. Da T endlich erzeugt ist, existiert ein $s_1 \in S$ mit $s_1T = 0$.
Sei $N := \mathrm{Im}(i_{S,M}) \simeq M/T$. Da $S^{-1}M$ als $Q(A)$-Vektorraum von N erzeugt wird, existiert eine Basis $y_1,\dots,y_n$ von $S^{-1}M$ mit $y_i \in N$. Dann ist $L := Ay_1 + \dots + Ay_n$ frei über A.
Wegen $S^{-1}L = S^{-1}M$ ist $S^{-1}N = S^{-1}L$. Aus $S^{-1}(N/L) \simeq S^{-1}N/S^{-1}L$ folgt somit $S^{-1}(N/L) = 0$. Also existiert ein $s_2 \in S$ so, daß $s_2(N/L) = 0$, d.h. $N_{s_2} = L_{s_2}$ ist.

Insgesamt gilt: $M_{s_1s_2} = N_{s_1s_2} = L_{s_1s_2}$ ist frei über $A_{s_1s_2}$. —

Folgerung 16.11 *Sei* k *ein vollkommener Körper,* B *eine integre* k-*Algebra von endlichem Typ. Dann existiert ein* $s \in B - \{0\}$, *so daß für* $\mathfrak{p} \in \operatorname{Spec} A$ *gilt:*

Falls $s \notin \mathfrak{p}$, *ist* $B_{\mathfrak{p}}$ *regulär.* —

Im Rest des Paragraphen wird eine weitergehende Aussage über die Menge der $\mathfrak{p}$, für die $B_{\mathfrak{p}}$ regulär ist, entwickelt.

Definitionen 16.12 Sei A ein Ring.
a) Für ein Ideal $\mathfrak{a}$ von A sei $V(\mathfrak{a}) :=$
$\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supset \mathfrak{a}\} = \operatorname{Supp}_A(A/\mathfrak{a})$.

b) Eine Teilmenge $T \subset \operatorname{Spec} A$ heißt (Zariski-) abgeschlossen, wenn es ein Ideal $\mathfrak{a}$ von A mit $T = V(\mathfrak{a})$ gibt. (Vgl. 1.A4, 9.A11.)

Bemerkung 16.13 Durch die (Zariski-) abgeschlossenen Teilmengen wird eine Topologie auf $\operatorname{Spec} A$ erklärt, die sogenannte Zariski-Topologie, denn es gilt:

1) Eine endliche Vereinigung abgeschlossener Teilmengen von $\operatorname{Spec} A$ ist abgeschlossen; $\emptyset$ ist abgeschlossen.

2) Ein beliebiger Durchschnitt abgeschlossener Teilmengen von $\operatorname{Spec} A$ ist abgeschlossen; $\operatorname{Spec} A$ ist abgeschlossen (in $\operatorname{Spec} A$).

Beweis: 0) $\operatorname{Spec} A = V((0))$ und $\emptyset = V((1))$.
1) $V(\mathfrak{a}_1) \cup \dots \cup V(\mathfrak{a}_n) = V(\mathfrak{a}_i \cdot \ldots \cdot \mathfrak{a}_m)$.
2) $\bigcap_{i\in I} V(\mathfrak{a}_i) = V(\sum_{i\in I} \mathfrak{a}_i)$.

Satz 16.14 *Sei* A *ein Ring*, M *ein endlicher* A-*Modul sowie* $m \in \mathbb{N}$. *Dann ist die Menge* $E_m := \{\mathfrak{p} \in \operatorname{Spec}(A) : \mu_{A_\mathfrak{p}}(M_\mathfrak{p}) \geq m\}$ *abgeschlossen.*

Beweis: Sei $x_1,\dots,x_r$ ein Erzeugendensystem von M über A. Dann ist $\{\frac{x_1}{1},\dots,\frac{x_r}{1}\}$ ein Erzeugendensystem von $M_\mathfrak{p}$ über dem lokalen Ring $A_\mathfrak{p}$, enthält also ein kürzestes Erzeugendensystem (12.1).

Seien $U_1,\dots,U_s$ diejenigen Untermoduln von M, die von jeweils m-1 Elementen der Menge $\{x_1,\dots,x_r\}$ erzeugt werden. Für jedes $\mathfrak{p} \in \operatorname{Spec} A$ gilt dann:

$$\mu_{A_\mathfrak{p}}(M_\mathfrak{p}) \leq m-1 \iff \exists\, j \in \{1,\dots,s\} \text{ mit } (M/U_j)_\mathfrak{p} = 0 .$$

Es folgt:

$$\mu_{A_\mathfrak{p}}(M_\mathfrak{p}) \geq m \iff \mathfrak{p} \in \operatorname{Supp}(M/U_j) \text{ für alle } j \in \{1,\dots,s\}$$
$$\iff \mathfrak{p} \in \bigcap_{j=1}^{s} \operatorname{Supp}(M/U_j) = \bigcap_{j=1}^{s} V(\operatorname{Ann}(M/U_j)) .$$

(Beachte 4.14.) Also ist E_m abgeschlossen nach 16.13,1). —

Folgerung 16.15 *Sei* A *ein noetherscher Integritätsring*, M *ein endlich erzeugter* A-*Modul. Dann ist* $\{\mathfrak{p} \in \operatorname{Spec} A \mid M_\mathfrak{p}$ *ist nicht frei über* $A_\mathfrak{p}\}$ *abgeschlossen in* Spec A.

Beweis: Für jedes $\mathfrak{p} \in \operatorname{Spec} A$ gilt:

$$\mu_{A_\mathfrak{p}}(M_\mathfrak{p}) \geq \mu_{Q(A)}(M \otimes_A Q(A))$$

sowie:

$$M_\mathfrak{p} \text{ ist frei } \overset{16.8}{\iff} \mu_{A_\mathfrak{p}}(M_\mathfrak{p}) = \mu_{Q(A)}(M \otimes_A Q(A)) . \text{ —}$$

Folgerung 16.16 *Sei* k *ein vollkommener Körper*, A *eine integre* k-*Algebra im wesentlichen von endlichem Typ. Dann ist*
$\operatorname{Sing}(A) := \{\mathfrak{p} \in \operatorname{Spec} A \mid A_\mathfrak{p}$ *ist nicht regulär*$\}$ *abgeschlossen in* Spec A. —

Bemerkung 16.17 Die Voraussetzungen von 16.16 seien erfüllt. Dann ist $\operatorname{Sing} A \neq \operatorname{Spec} A$, da A regulär in (0) ist. ($A_{(0)} = Q(A)$ ist ein Körper.) Daher ist $\operatorname{Sing}(A) = V(\mathfrak{a})$ mit einem Ideal $\mathfrak{a} \neq 0$. Höchstens endlich viele Primideale der Höhe 1 umfassen $\mathfrak{a}$: Sing A ist "dünn".

Spezieller sei V eine irreduzible algebraische Menge (über algebraisch abgeschlossenem k). Die maximalen Ideale $\mathfrak{m}$ von k[V], für die

$K[V]_{\mathfrak{m}}$ nicht regulär ist, entsprechen also Punkten $p \in V$, die eine Untervarietät niedrigerer Dimension bilden. Vom Standpunkt der (klassischen) algebraischen Geometrie aus gesehen sind also "die meisten" lokalen Ringe regulär.

Hinweis: Zu Regularitätskriterien über nichtvollkommenem Grundkörper siehe [Kunz 1].

§17 COHEN-MACAULAY-MODULN UND -RINGE

Im folgenden seien A *ein noetherscher lokaler Ring mit maximalem Ideal* $\mathfrak{m}$ *und* $k = A/\mathfrak{m}$, *ferner* M *ein endlicher* A*-Modul.*

Wir erinnern an die Definition der Tiefe $\operatorname{tf} M$ von M in 14.17, ferner an die Feststellungen $\operatorname{tf} M \le \dim M < \infty$ für $M \neq 0$ und "$\operatorname{tf} M = 0 \iff \mathfrak{m} \in \operatorname{Ass} M$" (14.18b) und c)).

Lemma 17.1 $\operatorname{tf} M = 0 \iff \operatorname{Hom}(k,M) \neq 0$.

Beweis: Da k ein einfacher A-Modul ist, ist "$\operatorname{Hom}(k,M) \neq 0$" äquivalent zu: "Es gibt einen injektiven Homomorphismus $k \longrightarrow M$". Letzteres bedeutet $\mathfrak{m} \in \operatorname{Ass} M$ nach 4.4a). –

Folgerung 17.2 *Eine* M*-reguläre Folge* $x_1,\dots,x_r$ *in* $\mathfrak{m}$ *ist genau dann (also solche) maximal, d.h. nicht verlängerbar, wenn* $\operatorname{Hom}(k,M/(x_1M+\dots+x_rM)) \neq 0$ *ist.* –

Satz 17.3 *Sei* $x_1,\dots,x_r$ *eine* M*-reguläre Folge in* $\mathfrak{m}$. *Dann ist* $\operatorname{Ext}^i(k,M) = 0$ *für* $i < r$ *und* $\operatorname{Hom}_A(k,M)/(x_1M+\dots+x_rM)) \simeq \operatorname{Ext}^r_A(k,M)$.

Beweis: Induktion nach r, wobei der Fall $r = 0$ trivial ist. (Für $r=0$ ist $x_1M+\dots+x_rM=0$.)
Sei jetzt $r > 0$. Aus der kurzen exakten Folge $0 \longrightarrow M \xrightarrow{x_1} M \longrightarrow M/x_1M \longrightarrow 0$ entsteht die lange exakte Folge

(*) $\operatorname{Ext}^i(k,M) \xrightarrow{x_1} \operatorname{Ext}^i(k,M) \longrightarrow \operatorname{Ext}^i(k,M/x_1M) \longrightarrow \operatorname{Ext}^{i+1}(k,M) \xrightarrow{x_1} \operatorname{Ext}^{i+1}(k,M)$.

(Die Homothetien von x_1 wurden mit x_1 bezeichnet. Beachte - auch im folgenden -: Die Ext^j sind A-linear in beiden Variablen.) Da k von $x_1 \in \mathfrak{m}$ annulliert wird, sind die Homothetien von x_1 in der Folge (*) gleich gleich 0. Nach Induktionsvoraussetzung, angewandt auf den Modul M/x_1M, ist $\operatorname{Ext}^i(k,M/x_1M) = 0$ für $i < r-1$ und
$\operatorname{Ext}^{r-1}(k,M/x_1M) \simeq \operatorname{Hom}(k,M/(x_1M+\dots+x_rM))$.

Aus (*) folgt dann $\mathrm{Ext}^{i+1}(k,M) = 0$ für $i < r-1$, d.h. $\mathrm{Ext}^i(k,M) = 0$ für $i < r$ und deshalb weiter: $\mathrm{Ext}^r(k,M) \simeq \mathrm{Ext}^{r-1}(k,M/x_1M) \simeq \mathrm{Hom}(k,M/(x_1M + \ldots + x_rM))$. —

Folgerung 17.4 *Sei* $M \neq 0$. *Maximale* M*-reguläre Folgen in* $\mathfrak{m}$ *haben alle die Länge* $\mathrm{tf}\, M < \infty$. *Und zwar ist* $\mathrm{tf}\, M$ *gleich dem Minimum der* r, *für die* $\mathrm{Ext}^r(k,M) \neq 0$ *ist.*

Beweis: Da $\mathrm{tf}\, M < \infty$ ist, sind alle maximalen M-regulären Folgen in $\mathfrak{m}$ von endlicher Länge. Sei $x_1,\ldots,x_s$ eine beliebige solche. Nach 17.3 ist dann $\mathrm{Ext}^i(k,M) = 0$ für $i < s$ und $\mathrm{Ext}^s(k,M) \simeq \mathrm{Hom}(k,M/(x_1M + \ldots + x_sM)) \neq 0$, letzteres gemäß 17.2. Somit ist $s = \mathrm{Min}\{r \mid \mathrm{Ext}^r(k,M) \neq 0\}$. Man sieht: s ist unabhängig von der speziellen Wahl der maximalen M-regulären Folge in $\mathfrak{m}$. Also ist auch $\mathrm{tf}\, M = s$. —

Folgerung 17.5 *Sei* $M \neq 0$ *und* $x \in \mathfrak{m}$ *ein Nichtnullteiler für* M. *Dann ist* $\mathrm{tf}(M/xM) = \mathrm{tf}\, M - 1$.

Zum Beweis setze x zu einer maximalen M-regulären Folge $x,x_2,\ldots,x_r$ in $\mathfrak{m}$ fort. Dann ist $x_2,\ldots,x_r$ eine maximale (M/xM)-reguläre Folge in $\mathfrak{m}$. —

Definition 17.6 M heißt ein Cohen-Macaulay-Modul, wenn $\mathrm{tf}\, M = \dim M$ oder $M = 0$ ist. (Für $M = 0$ ist $\dim M = -\infty$, $\mathrm{tf}\, M = \infty$.) A heißt ein Cohen-Macaulay-Ring, wenn A als A-Modul ein Cohen-Macaulay-Modul ist.

Bemerkungen 17.7 a) Wenn M ein Cohen-Macaulay-Modul und $x_1,\ldots,x_r$ eine M-reguläre Folge in $\mathfrak{m}$ ist, so ist $M/(x_1M + \ldots + x_rM)$ ein Cohen-Macaulay-Modul. Denn wenn $x \in \mathfrak{m}$ ein Nichtnullteiler für M ist, gilt sowohl $\dim(M/xM) = \dim M - 1$ als auch $\mathrm{tf}(M/xM) = \mathrm{tf}\, M - 1$ gemäß 14.18a) und 17.5.

b) Jeder reguläre lokale Ring ist ein Cohen-Macaulay-Ring.

c) Wenn $\dim M = 0$ ist, ist M ein Cohen-Macaulay-Modul.

d) Wenn A reduziert und $\dim A = 1$ ist, ist A ein Cohen-Macaulay-Ring. Denn dann ist $\mathfrak{m}$ nicht minimal, folglich wegen der Reduziertheit nicht zu A assoziiert. (2.17, 4.6, 4.17, 1.21.)

e) Wenn A ein ganz abgeschlossener Integritätsring der Dimension 2 ist, ist A ein Cohen-Macaulay-Ring. Sei nämlich $x \in A - (0)$, dann ist $\mathfrak{m}$ nach 8.14 nicht zu A/Ax assoziiert.

f) Es gibt Ringe beliebig großer Dimension der Tiefe 0. Sei nämlich $x \in A - (A^* \cup \{0\})$ und $B := A/x\mathfrak{m}$. So ist $(x) \neq x\mathfrak{m}$, also $k \simeq (x)/x\mathfrak{m}$ und somit $\mathfrak{m} \in \operatorname{Ass} B$, ferner $\dim B \geq \dim A - 1$.

Lemma 17.8 *Seien* B *ein Ring und* E,F *endliche* B*-Moduln. Dann ist* $\operatorname{Supp}_B(E \otimes_B F) = \operatorname{Supp}_B E \cap \operatorname{Supp}_B F$.

Beweis: Zu zeigen ist:

$$(E \otimes_B F)_{\mathfrak{p}} \neq 0 \iff E_{\mathfrak{p}} \neq 0 \wedge F_{\mathfrak{p}} \neq 0 .$$

Nun ist $(E \otimes_B F)_{\mathfrak{p}} \simeq E_{\mathfrak{p}} \otimes_{B_{\mathfrak{p}}} F_{\mathfrak{p}}$ (11.8). Deshalb genügt es, folgendes zu zeigen: Wenn $E \neq 0$ und $F \neq 0$ endliche Moduln über einem lokalen Ring B sind, ist $E \otimes_B F \neq 0$.
Sei aber $\mathfrak{p}$ das maximale Ideal von B. Dann sind $E/\mathfrak{p}E$ und $F/\mathfrak{p}F$ nach 6.16 Vektorräume über $B/\mathfrak{p}$ mit Dimensionen $r,s > 0$. Man hat aber eine surjektive Abbildung $E \otimes_B F \longrightarrow (E/\mathfrak{p}E) \otimes_B (F/\mathfrak{p}F) \simeq (B/\mathfrak{p})^{rs} \neq 0$. —

Folgerung 17.9 *Seien* B,E *wie oben und* $\mathfrak{a}$ *ein Ideal von* B. *Dann ist* $\operatorname{Supp}(E/\mathfrak{p}E) = \operatorname{Supp} E \cap V(\mathfrak{a})$ *(siehe 16.12). Insbesondere ist* $\dim(E/\mathfrak{p}E) = \dim(A/\mathfrak{p})$ *für* $\mathfrak{p} \in \operatorname{Supp} E$.

Beweis: $E/\mathfrak{a}E \simeq E \otimes_A A/\mathfrak{a}$. —

Lemma 17.10 *Sei* $\mathfrak{p} \in \operatorname{Ass} M$ *und* x *ein Nichtnullteiler für* M. *Dann ist jedes minimale Primoberideal* $\mathfrak{q}$ *von* $\mathfrak{p} + Ax$ *zu* M/xM *assoziiert.*

Beweis: Nach 4.25 gibt es einen Untermodul N von M mit $\operatorname{Ass} N = \{\mathfrak{p}\}$ und $\operatorname{Ass}(M/N) = \operatorname{Ass} M - \{\mathfrak{p}\}$.
Wegen $\operatorname{Ass}(M/N) \subset \operatorname{Ass} M$ ist x auch ein Nichtnullteiler für $M' := M/N$.

Betrachte das folgende kommutative Diagramm mit exakten Zeilen und Spalten (mit den kanonischen Homomorphismen):

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} & & \\
0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N/xN & \longrightarrow & M/xM & \longrightarrow & M'/xM' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Nach 11.13 ist die Abbildung $N/xN \longrightarrow M/xM$ injektiv und deshalb $\mathrm{Ass}(N/xN) \subset \mathrm{Ass}(M/xM)$.

Nun ist $\mathfrak{q}$ minimal in $V(\mathfrak{p}+Ax) \overset{16.13}{=} V(\mathfrak{p}) \cap V(Ax) = \mathrm{Supp}(N) \cap \mathrm{Supp}(A/Ax)$ $\overset{17.8}{=} \mathrm{Supp}(N \otimes_A A/Ax) = \mathrm{Supp}(N/xN)$, also zu N/xN assoziiert. –

<u>Satz 17.11</u> *Es gilt* $\mathrm{tf}\, M \leq \mathrm{Min}\{\dim(A/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Ass}\, M\}$ *für* $M \neq 0$.

<u>Beweis:</u> Induktion nach $\mathrm{tf}\, M$, wobei der Fall $\mathrm{tf}\, M = 0$ trivial ist.

Sei $\mathrm{tf}\, M > 0$ und $x \in \mathfrak{m}$ ein Nichtnullteiler für M .

Nach 17.10 gibt es zu jedem $\mathfrak{p} \in \mathrm{Ass}\, M$ ein $\mathfrak{q} \in \mathrm{Ass}(M/xM)$ mit $\mathfrak{q} \supset \mathfrak{p} + Ax$, also $\dim(A/\mathfrak{q}) \leq \dim(A/\mathfrak{p}) - 1$, da $x \notin \mathfrak{p}$. Wegen 17.5 kann man auf M/xM die Induktionsvoraussetzung anwenden und erhält:
$\mathrm{tf}\, M = \mathrm{tf}(M/xM) + 1 \leq \mathrm{Min}\{\dim(A/\mathfrak{q}) \mid \mathfrak{q} \in \mathrm{Ass}(M/xM)\} + 1$
$\leq \mathrm{Min}\{\dim(A/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Ass}\, M\} - 1 + 1$. –

<u>Folgerung 17.12</u> *Sei* M *ein Cohen-Macaulay-Modul,* $\mathfrak{p} \in \mathrm{Supp}\, M$.
Dann sind äquivalent:
(i) $\mathfrak{p} \in \mathrm{Ass}\, M$;
(ii) $\mathfrak{p}$ *ist minimal in* $\mathrm{Supp}\, M$;
(iii) $\dim(A/\mathfrak{p}) = \dim M$.

Insbesondere umfaßt kein $\mathfrak{p} \in \mathrm{Ass}\, M$ *ein anderes* $\mathfrak{q} \in \mathrm{Ass}\, M$.

<u>Beweis:</u> Allgemein gilt (iii) $\overset{4.14}{\Longrightarrow}$ (ii) $\overset{4.15}{\Longrightarrow}$ (i) .
Für $\mathfrak{p} \in \mathrm{Ass}\, M$ ist aber $\dim(A/\mathfrak{p}) \leq \dim M$, ferner $\mathrm{tf}\, M \leq \dim(A/\mathfrak{p})$ nach 17.11. Wegen $\mathrm{tf}\, M = \dim M$ folgt (iii) aus (i). –

Bemerkung 17.13 Wenn M ein Cohen-Macaulay-Modul und $x_1,\dots,x_r$ in $\mathfrak{m}$ eine M-reguläre Folge ist, ist $N := M/(x_1M + \dots + x_rM)$ nach 17.7a) ein Cohen-Macaulay-Modul. Für $\mathfrak{p} \in \operatorname{Ass} N$ gilt deshalb $\dim A/\mathfrak{p} = \dim N \underset{14.18a)}{=} \dim M-r$. Alle $\mathfrak{p} \in \operatorname{Ass} N$ sind minimal in $\operatorname{Supp} N$.

Satz 17.14 *Sei* $M \neq 0$ *ein Cohen-Macaulay-Modul. Für eine Folge* $\underline{x} = (x_1,\dots,x_r)$ *in* $\mathfrak{m}$ *sind äquivalent:*

(i) *Die Folge* $\underline{x}$ *ist* M-*regulär;*

(ii) $\dim(M/(x_1M + \dots + x_rM)) = \dim M - r$;

(iii) $\underline{x}$ *ist Teil eines Parametersystems für* M.

Beweis: (i) $\Rightarrow$ (ii) ist 14.18a).

(ii) $\Rightarrow$ (i): Induktion nach r, wobei der Fall $r = 0$ trivial ist. Sei $N = M/(x_1M + \dots + x_{r-1}M)$. Dann ist N ein Cohen-Macaulay-Modul (17.7). Sei $\mathfrak{p} \in \operatorname{Ass} N$. Nach 17.12 ist $\dim A/\mathfrak{p} = \dim N = \dim M - r+1$. Da nach Voraussetzung $\dim N/x_rN = \dim M-r = \dim N-1$ ist, kann x_r nicht in $\mathfrak{p}$ liegen. (Sonst wäre $\mathfrak{p} \in \operatorname{Supp} N/x_rN = \operatorname{Supp} N \cap V(x_r)$.) Demnach ist x_r ein Nichtnullteiler für N. Da nach Induktionsvoraussetzung $x_1,\dots,x_{r-1}$ eine M-reguläre Folge ist, ist auch $x_1,\dots,x_r$ eine solche.

(ii) $\Rightarrow$ (iii): Sei $N := M/(x_1M + \dots + x_rM)$ und $x_{r+1},\dots,x_n$ ein Parametersystem für N.
Wegen (ii) ist $n = \dim M$. Da ferner $M/(x_1M + \dots + x_nM) \simeq N/(x_{r+1}N + \dots + x_nN)$, also von endlicher Länge ist, ist $x_1,\dots,x_n$ ein Parametersystem für M, und es folgt (iii).

(iii) $\Rightarrow$ (ii): Sei N wie oben $\dim M = n$ und $x_1,\dots,x_r,\dots,x_n$ ein Parametersystem für M. Da $N/(x_{r+1}N + \dots + x_nN) \simeq M/(x_1M + \dots + x_nM)$, also von endlicher Länge ist, folgt $\dim N \le n-r$ nach 6.9. Andererseits ist $\dim N = \dim(M/(x_1M + \dots + x_rM)) \ge \dim M - r$ nach 6.13. —

Satz 17.15 *Sei* M *ein Cohen-Macaulay-Modul,* $\mathfrak{p} \in \operatorname{Supp} M$ *und* $r = \dim M - \dim(M/\mathfrak{p}M)$. *Dann gibt es in* $\mathfrak{p}$ *eine* M-*reguläre Folge* $x_1,\dots,x_r$.

Beweis: Induktion nach r, wobei es für $r = 0$ die Behauptung leer ist.
Sei $r > 0$. Dann ist $\dim(A/\mathfrak{p}) \overset{17.9}{=} \dim(M/\mathfrak{p}M) < \dim M$. Nach 17.12 ist $\mathfrak{p}$ in keinem $\mathfrak{q} \in \operatorname{Ass} M$ enthalten, also auch nicht in deren Vereinigung

(1.21). Folglich gibt es in $\mathfrak{p}$ einen Nichtnullteiler x_1 von M. Indem man die Induktionsvoraussetzung auf M/x_1M anwendet, erhält man die gesuchte Folge. —

Bevor wir wichtige Folgerungen ziehen können, beweisen wir:

Lemma 17.16 *Seien B ein Ring, N ein B-Modul und $x_1,\dots,x_r$ eine N-reguläre Folge. Dann gilt:*

a) Wenn F ein flacher B-Modul ist, ist $x_1,\dots,x_r$ auch eine $N \otimes_B F$-reguläre Folge.

b) Wenn $S \subset B$ multiplikativ ist, dann ist $\frac{x_1}{1},\dots,\frac{x_r}{1}$ eine $S^{-1}N$-reguläre Folge in $S^{-1}B$.

Beweis: a) Wenn U ein Untermodul von N ist, kann man $U \otimes_B F$ wegen der Flachheit mit einem Untermodul von $N \otimes_B F$ identifizieren. Für $y_1,\dots,y_s \in B$ stimmen die Untermoduln $y_1(N \otimes F) + \dots + y_s(N \otimes F)$ und $(y_1N + \dots + y_sN) \otimes F$ von $N \otimes F$ überein. (Dies sieht man zum Beispiel, indem man sich die Elemente der Untermoduln hinschreibt.) Nach Voraussetzung ist für $1 \le s \le r$ die Homothetie von x_s auf $N/(x_1N + \dots + x_{s-1}N)$ injektiv. Dann ist sie es auch auf $(N/(x_1N + \dots + x_{s-1}N)) \otimes F$ $\simeq (N \otimes F)/(x_1(N \otimes F) + \dots + x_{s-1}(N \otimes F))$, da F flach ist.

b) Nach a) ist $x_1,\dots,x_r$ eine $S^{-1}N$-reguläre Folge in B, da $S^{-1}N \simeq N \otimes S^{-1}B$ und $S^{-1}B$ flach ist. Da aber die Homothetie von $\frac{x_s}{1}$ auf $S^{-1}(N/(x_1N + \dots + x_{s-1}N)) \simeq S^{-1}N/(x_1S^{-1}N + \dots + x_{s-1}S^{-1}N)$ mit der von x_s übereinstimmt, ist auch $\frac{x_1}{1},\dots,\frac{x_r}{1}$ eine $S^{-1}N$-reguläre Folge in $S^{-1}B$. —

Folgerung 17.17 *Unter den Voraussetzungen von 17.15 gilt:*

a) $M_{\mathfrak{p}}$ ist ein Cohen-Macaulay-Modul über $A_{\mathfrak{p}}$.

b) $\dim_A M = \dim_A(M/\mathfrak{p}M) + \dim_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$.

Beweis: Nach 17.15 gibt es eine M-reguläre Folge $x_1,\dots,x_r$ in $\mathfrak{p}$, wobei $r = \dim M - \dim(M/\mathfrak{p}M)$ ist. Dann ist
$\dim(M/(x_1M + \dots + x_rM)) = \dim M - r \underset{\text{Vor.}}{=} \dim(M/\mathfrak{p}M) \underset{17.9}{=} \dim(A/\mathfrak{p})$. Also ist $\mathfrak{p}$ minimal in $\mathrm{Supp}(M/(x_1M + \dots + x_rM))$. Deshalb ist $M_{\mathfrak{p}}/(\frac{x_1}{1}M_{\mathfrak{p}} + \dots + \frac{x_r}{1}M_{\mathfrak{p}})$ ein $A_{\mathfrak{p}}$-Modul endlicher Länge. Da $\frac{x_1}{1},\dots,\frac{x_r}{1}$ eine $M_{\mathfrak{p}}$-reguläre Folge in $\mathfrak{p}A_{\mathfrak{p}}$ ist, ist $M_{\mathfrak{p}}$ ein Cohen-Macaulay-Modul über $A_{\mathfrak{p}}$, und zwar von der Dimension $r = \dim_A M - \dim_A(M/\mathfrak{p}M)$. —

Folgerung 17.18 *Wenn* M *ein Cohen-Macaulay-Modul mit* $\operatorname{Supp} M = \operatorname{Spec} A$ *ist (insbesondere also, wenn* A *ein Cohen-Macaulay-Ring ist), gilt* $\dim A = \dim(A/\mathfrak{p}) + \operatorname{ht} \mathfrak{p}$ *für jedes* $\mathfrak{p} \in \operatorname{Spec} A$.

Beweis: Da $\operatorname{Supp}(M/\mathfrak{p}M) = \operatorname{Supp} A/\mathfrak{p}$ und $\operatorname{Supp}_{A_\mathfrak{p}} M_\mathfrak{p} = \operatorname{Spec} A_\mathfrak{p}$ ist, folgt dies aus 17.17. –

Definition 17.19 Sei B ein noetherscher (nicht notwendig lokaler) Ring und N ein endlicher B-Modul.
N heißt ein Cohen-Macaulay-Modul, wenn $N_\mathfrak{p}$ ein Cohen-Macaulay-Modul über $B_\mathfrak{p}$ für jedes $\mathfrak{p} \in \operatorname{Spec} B$ ist.
B heißt ein Cohen-Macaulay-Ring, wenn B als B-Modul ein Cohen-Macaulay-Modul ist.

N.B.: Wegen 17.17 a) stimmt diese Definition mit der ursprünglichen überein, wenn B lokal ist. (In 17.17 a) ist $\mathfrak{p} \in \operatorname{Supp} M$ vorausgesetzt. Aber andernfalls ist $M_\mathfrak{p} = 0$.)

Satz 17.20 *(Macaulays Ungemischtheitssatz)*
Sei B *ein noetherscher Cohen-Macaulay-Ring,* $x_1,\dots,x_r$ *eine* B*-reguläre Folge (in* B*). Dann ist jedes* $\mathfrak{p} \in \operatorname{Ass}(B/(x_1B + \dots + x_rB))$ *minimal in* $\operatorname{Ass}(B/(x_1B + \dots + x_rB))$.

Beweis: $B_\mathfrak{p}$ ist ein Cohen-Macaulay-Ring, also nach 17.17 und 17.7 auch $C := B_\mathfrak{p}/(x_1B_\mathfrak{p} + \dots + x_rB_\mathfrak{p})$. Nach 17.12 ist $\mathfrak{p}B_\mathfrak{p}$ minimal in $\operatorname{Supp} C$. –

N.B.: Satz 17.20 gilt insbesondere für $B = k[X_1,\dots,X_n]$ mit einem Körper k .

Definition 17.21 Ein noetherscher Ring heißt katenär oder ein Kettenring, wenn für je zwei Primideale $\mathfrak{p} \subset \mathfrak{q}$ von B alle nichtverfeinerbaren Primidealketten, die mit $\mathfrak{p}$ anfangen und mit $\mathfrak{q}$ aufhören, gleiche Länge haben.

Bemerkungen 17.22 a) Wenn der noethersche Ring B katenär ist, dann ist es auch jeder Restklassenring und jeder Bruchring von B .

b) Ein noetherscher Ring B ist genau dann katenär, wenn $B_\mathfrak{n}$ für jedes maximale Ideal $\mathfrak{n}$ von B katenär ist.

c) Wenn der noethersche Ring B katenär und integer ist und alle maximalen Ideale dieselbe Höhe haben, dann hat auch jeder integre Restklassenring C von B diese Eigenschaft, und für jedes $\mathfrak{q} \in \operatorname{Spec} C$ gilt

$$(*) \qquad \operatorname{ht} \mathfrak{q} + \dim(C/\mathfrak{q}) = \dim C .$$

Sei nämlich $\mathfrak{p} \in \operatorname{Spec} B$ und $\mathfrak{n} \supset \mathfrak{p}$ ein maximales Ideal von B. Wir betrachten nichtverfeinerbare Primidealketten

$$(0) = \mathfrak{p}_0 \subsetneqq \dots \subsetneqq \mathfrak{p}_r = \mathfrak{p} \qquad \text{und}$$
$$\mathfrak{p} = \mathfrak{p}_r \subsetneqq \dots \subsetneqq \mathfrak{p}_{r+s} = \mathfrak{n} .$$

Da B katenär ist, folgt $r+s = \operatorname{ht} \mathfrak{n}$. Nach Voraussetzung ist $\operatorname{ht} \mathfrak{n} = \dim B$ für alle maximalen Ideale $\mathfrak{n}$ von B. Für alle maximalen Ideale $\mathfrak{n}/\mathfrak{p}$ von $C = B/\mathfrak{p}$ gilt also $\operatorname{ht}_C(\mathfrak{n}/\mathfrak{p}) = s = \dim B - r$.
In dem integren katenären Ring C haben also auch alle maximalen Ideale dieselbe Höhe.

Zum Beweis von $(*)$ dürfen wir also $B = C$ und $\mathfrak{p} = \mathfrak{q}$ annehmen.

Mit obigen Bezeichnungen ist $\operatorname{ht} \mathfrak{p} = r$, da B katenär ist, und $\dim(B/\mathfrak{p}) = s$, wie oben gezeigt. Also ist
$\operatorname{ht} \mathfrak{p} + \dim(B/\mathfrak{p}) = r+s = \operatorname{ht} \mathfrak{n} = \dim B$.

<u>Satz 17.23</u> *Sei* B *ein noetherscher Ring. Es gebe einen endlichen Cohen-Macaulay-Modul* N *über* B *mit* $\operatorname{Supp} N = \operatorname{Spec} B$. *Dann ist jeder Restklassenring von* B *katenär.*

<u>Beweis:</u> Da man jede Primidealkette zu einer solchen "nach unten" verlängern kann, die mit einem minimalen Primideal beginnt, folgt dies aus der

<u>Behauptung:</u> Sei $\mathfrak{p} \in \operatorname{Spec} B$ und $\mathfrak{p}_0 \subsetneqq \dots \subsetneqq \mathfrak{p}_n = \mathfrak{p}$ eine nicht verfeinerbare Primidealkette mit einem minimalen Primideal $\mathfrak{p}_0$. Dann ist $n = \operatorname{ht} \mathfrak{p}$.

(Beachte: Diese Behauptung braucht für Restklassenringe (mit mehr als einem minimalen Primideal) von B nicht zu gelten.)

Den Beweis der Behauptung führen wir mit Induktion nach $\operatorname{ht} \mathfrak{p}$, wobei der Fall $\operatorname{ht} \mathfrak{p} = 0$ trivial ist.

Sei also $\operatorname{ht} \mathfrak{p} \geq 1$; dann ist auch $n \geq 1$. Nach Induktionsvoraussetzung ist $\operatorname{ht} \mathfrak{p}_{n-1} = n-1$.
Nun ist $N_{\mathfrak{p}}$ ein endlicher Cohen-Macaulay-Modul über dem lokalen

noetherschen Ring $B_{\mathfrak{p}}$ mit $\operatorname{Supp} N_{\mathfrak{p}} = \operatorname{Spec} B_{\mathfrak{p}}$. Nach 17.18 folgt

$$\begin{aligned}\operatorname{ht}\mathfrak{p} &= \dim(B_{\mathfrak{p}}/\mathfrak{p}_{n-1}B_{\mathfrak{p}}) + \operatorname{ht}\mathfrak{p}_{n-1}\\ &= 1 + n-1 .\end{aligned}$$ —

Wir wollen noch die Behauptungen in 9.A6 und 16.6 beweisen und benötigen dazu (teilweise) folgenden

Satz 17.24 *Sei* k *ein Körper. Dann ist der Polynomring* $B = k[X_1,\ldots,X_n]$ *katenär. Ferner hat jedes maximale Ideal* $\mathfrak{n}$ *von* B *die Höhe* n *und wird von* n, *aber nicht von weniger als* n *Elementen erzeugt.*

Beweis: B ist regulär (14.31), also ein Cohen-Macaulay-Ring (17.7b)), also katenär (17.23).

Den Rest zeigen wir mit Induktion nach n, wobei der Fall $n \le 1$ klar ist.

Sei $n > 1$. Nach 9.5 ist $\mathfrak{n}' := \mathfrak{n} \cap k[X_1,\ldots,X_{n-1}]$ ein maximales Ideal in $k[X_1,\ldots,X_{n-1}]$, also nach Induktionsvoraussetzung von der Höhe $n-1$ und von $n-1$ Elementen erzeugt. Dann ist $\mathfrak{p} := \mathfrak{n}'B$ ein Primideal der Höhe $n-1$ in B (siehe 6.27) und wird von $n-1$ Elementen erzeugt.

Nun ist $B/\mathfrak{p} \simeq (k[X_1,\ldots,X_{n-1}]/\mathfrak{n}')[X_n]$ ein Hauptidealring und kein Körper. Also wird das Primideal $\mathfrak{n}/\mathfrak{p}$ in $B/\mathfrak{p}$ von einem Element erzeugt, und es hat die Höhe 1. Deshalb wird $\mathfrak{n}$ von n Elementen erzeugt und hat die Höhe n. Denn B ist katenär.

Würde $\mathfrak{n}$ auch von weniger als n Elementen erzeugt, so wäre nach 6.19 $\operatorname{ht}\mathfrak{n} < n$. Widerspruch. —

Folgerung 17.25 *Sei* k *ein Körper und* C *eine* k*-Algebra von endlichem Typ.*

Dann ist C *katenär.*

Wenn zusätzlich C *integer ist, so gilt für jedes* $\mathfrak{p} \in \operatorname{Spec} C$ *die Gleichung*

$$\operatorname{ht}\mathfrak{p} + \dim(C/\mathfrak{p}) = \dim C .$$

Beweis: C ist von der Form $k[X_1,\ldots,X_n]/\mathfrak{a}$. Wende 17.24 und 17.22 an. —

Satz 17.26 *Sei* B *ein noetherscher Cohen-Macaulay-Ring, so ist auch der Polynomring* $B[X_1,\dots,X_n]$ *ein solcher.*

Beweis: Wir dürfen $n = 1$ annehmen und schreiben X anstelle von X_1.

Für ein beliebiges maximales Ideal $\mathfrak{n}$ von $B[X]$ ist zu zeigen, daß $B[X]_{\mathfrak{n}}$ ein (lokaler) Cohen-Macaulay-Modul ist.

Sei $\mathfrak{p} = B \cap \mathfrak{n}$. (Es ist $\mathfrak{p}$ prim, aber nicht notwendig maximal in B.) Wegen $B - \mathfrak{p} \subset B[X] - \mathfrak{n}$ ist $B[X]_{\mathfrak{n}} = (B_{\mathfrak{p}}[X])_{\mathfrak{n}B_{\mathfrak{p}}[X]}$. Deshalb dürfen wir annehmen: B ist lokal mit dem maximalen Ideal $\mathfrak{p}$, und $\mathfrak{n}$ ist ein maximales Ideal von $B[X]$ mit $\mathfrak{n} \cap B = \mathfrak{p}$.

Sei $x_1,\dots,x_r$ ein Parametersystem von B und $\mathfrak{a} := x_1B + \dots + x_rB$. Dann ist $\overline{B} := B/\mathfrak{a}$ von endlicher Länge und lokal, besitzt also genau ein Primideal, nämlich $\overline{\mathfrak{p}} := \mathfrak{p}/\mathfrak{a}$.

Das maximale Ideal $\overline{\mathfrak{n}} := \mathfrak{n}/(\mathfrak{a}[X])$ des Ringes $\overline{B}[X]$ umfaßt echt das Ideal $\overline{\mathfrak{p}}[X]$. Sei $f \in \overline{\mathfrak{n}} - \overline{\mathfrak{p}}[X]$.
Durch Subtraktion eines Polynoms mit Koeffizienten aus $\overline{\mathfrak{p}}$ erhält man aus f ein Polynom $g \in \overline{\mathfrak{n}}$, dessen höchster Koeffizient nicht in $\overline{\mathfrak{p}}$ liegt, also eine Einheit in $\overline{B}$ ist. Dieses g ist offenbar ein Nichtnullteiler von $\overline{B}[X]$. (Vgl. 13.A14.) Wenn also $x_{r+1} \in B[X]$ ein Repräsentant von g ist, ist $x_1,\dots,x_r,x_{r+1}$ eine $B[X]$-reguläre Folge in $\mathfrak{n}$.
Da $\mathrm{ht}_{B[X]}\mathfrak{p}[X] \overset{6.27}{=} \mathrm{ht}_B\mathfrak{p} = r$ ist, ist $\mathrm{ht}_{B[X]}\mathfrak{n} = r+1$ nach 6.25.
Da in $\mathfrak{n}$ eine $B[X]$-reguläre Folge der Länge $r+1$ existiert, ist $B[X]_{\mathfrak{n}}$ ein Cohen-Macaulay-Ring. —

Aufgaben und Hinweise

1) Seien A ein regulärer, lokaler Ring der Dimension n und $M \neq 0$ ein endlicher A-Modul. Zeige: Genau dann ist M frei, wenn M ein Cohen-Macaulay-Modul und $\dim M = n$ ist. (14.19)

2) Seien A wie oben und $a,b \in A - (A^* \cup \{0\})$ mit $a|b$, aber $b\nmid a$. Betrachte den Ring $B := A/(b)$ und den B-Modul $M := A/(a)$. Zeige: B ist ein Cohen-Macaulay-Ring, aber nicht regulär. M ist ein Cohen-Macaulay-Modul mit $\dim M = \dim B$, aber nicht frei über B. (14.5,17.7a))

3) Sei A wie oben und $\mathfrak{a}$ ein von (0) und A verschiedenes Ideal von A. Zeige die Äquivalenz der folgenden Aussagen:
(i) $\mathfrak{a}$ ist ein Hauptideal;
(ii) $\mathfrak{a}$ ist divisoriell;
(iii) $\mathrm{Ass}(A/\mathfrak{a})$ besteht aus lauter Primidealen der Höhe 1;
(iv) $A/\mathfrak{a}$ ist ein Cohen-Macaulay-Ring mit $\dim(A/\mathfrak{a}) = n-1$.

(Hinweis: (i) $\Rightarrow$ (iv): (A2); (iv) $\Rightarrow$ (iii): (17.12); (iii) $\Rightarrow$ (ii): Mit $\tilde{\mathfrak{a}} = (\mathfrak{a}^{-1})^{-1}$ betrachte $\mathrm{Ass}(\tilde{\mathfrak{a}}/\mathfrak{a}) \subset \mathrm{Ass}(A/\mathfrak{a})$, wende 12.47f an. A ist faktoriell (14.33), also krullsch. (ii) $\Rightarrow$ (i): (12.51).)

4) Unter dem Sockel $\mathrm{Soc}\, M$ eines Moduls M versteht man die Summe seiner einfachen Untermoduln.
Sei A wie oben. Man kann zeigen: Für jedes Parametersystem $x_1,\dots,x_d$ von A ist $\mathrm{Soc}(A/(x_1,\dots,x_d))$ ein 1-dimensionaler Vektorraum über dem Restklassenkörper k von A (siehe [Kunz] Kap. VI, Satz 3.17).
Sei jetzt zusätzlich $\dim A = 2$. Betrachte den A-Modul $M := A/\mathfrak{m}^2$, wobei $\mathfrak{m}$ das maximale Ideal von A sei. Es ist $\mu_k(\mathrm{Soc}\, M) = 2$, also $\mathfrak{m}^2$ nicht von einem Parametersystem erzeugt. Zeige: M ist nicht von der Form N/xN, wo N ein endlicher A-Modul und $x \in \mathfrak{m}$ ein Nichtnullteiler von N ist. (Wegen $N/\mathfrak{m}N \simeq M/\mathfrak{m}M \simeq k$ ist $\mu(N) = 1$, also $N \simeq A/\mathfrak{a}$. Wende A3 an.)

5) Sei A ein beliebiger noetherscher Ring und M ein endlicher A-Modul. Eine Permutation einer M-regulären Folge ist nicht immer eine solche. Beispiel: Die Folge $1, 0$, wenn $M \neq 0$ ist.
(Etwas weniger trivial, aber im Grunde auf dasselbe hinauslaufend ist das Beispiel: $A := \mathbb{Z}$, $M = \mathbb{Z} \oplus \mathbb{Z}/(n)$ mit der Folge m,n, wo m und n teilerfremd sind.)

a) Zeige: Wenn $x_1,\dots,x_r$ eine M-reguläre Folge in $\mathrm{Jac}\, A$ ist, ist auch jede Permutation dieser Folge eine solche. (Reduziere den Beweis auf den Fall $r = 2$. Zeige dann zuerst mit Hilfe von 17.10, daß x_2 ein Nichtnullteiler von M ist. Hierzu wird $x_1 \in \mathrm{Jac}\, A$ gebraucht! Vgl. [Kunz] Kap. VI, Lemma 3.2. Einen anderen Beweis kann man mit Hilfe des Koszul-Komplexes führen; siehe [Serre] Chap. IV A.

b) Zeige: Wenn $n_1,\dots,n_r \in \mathbb{N}_1 = \mathbb{N} - \{0\}$ sind und $x_1,\dots,x_r$ eine M-reguläre Folge ist, so ist auch $x_1^{n_1},\dots,x_r^{n_r}$ eine solche. (Wenn x ein Nichtnullteiler für M ist, so besitzt M/x^nM eine Kompositionsreihe, deren Faktoren isomorph zu M/xM sind.

Die Nullteiler für M/x^nM sind also (wegen 4.9) dieselben wie die für M/xM. Falls $x_1,\dots,x_r \in \operatorname{Jac} A$ sind, kann man die Behauptung auch aus a) folgern.)

6) Seien A noethersch, N ein endlicher, M ein beliebiger A-Modul.

a) Zeige: $\operatorname{Ass}(\operatorname{Hom}_A(N,M)) = \operatorname{Supp}(N) \cap \operatorname{Ass}(M)$.
(Zeige $\operatorname{Supp}(\operatorname{Hom}_A(N,M)) \supset \operatorname{Supp} N$ mit 11.4. Ein surjektiver Homomorphismus $A^n \longrightarrow N$ induziert eine Einbettung $\operatorname{Hom}(N,M) \hookrightarrow M^n$, also $\operatorname{Ass}(\operatorname{Hom}(N,M)) \subset \operatorname{Ass} M$. Umgekehrt, wenn $\mathfrak{p} \in \operatorname{Supp}(N) \cap \operatorname{Ass}(M)$, gibt es Homomorphismen $N_{\mathfrak{p}} \xrightarrow{\alpha} A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \xrightarrow{\beta} M_{\mathfrak{p}}$ mit α surjektiv und β injektiv. Beachte 4.11.)

b) Sei zusätzlich M ebenfalls endlich. Zeige:
$\operatorname{Hom}_A(N,M) = 0 \iff \exists\, x \in \operatorname{Ann} N$, x NNT für M .
("$\Leftarrow$": Aus "$0 \longrightarrow M \xrightarrow{x} M$ exakt" folgt: x operiert injektiv auf $\operatorname{Hom}(N,M)$. Andererseits ist $x \cdot \operatorname{Hom}(N,M) = 0$. "$\Rightarrow$": Wegen a) und 4.14 ist $\operatorname{Ann} N \not\subset \mathfrak{p}$ für alle $\mathfrak{p} \in \operatorname{Ass} M$.)

c) Sei (unter den Voraussetzungen von b)) $r = \operatorname{Inf}\{i \mid \operatorname{Ext}^i_A(N,M) \neq 0\}$. (Wenn $\operatorname{Ext}^i_A(N,M) = 0$ für alle i gilt, ist $r = \infty$.)

Zeige: Jede maximale M-reguläre Folge in $\operatorname{Ann} N$ hat die Länge r . (Kopiere mit Hilfe von b) den Beweis von 17.3.)

7) Seien A ein noetherscher lokaler Ring und M, N endliche A-Moduln. Zeige: $\operatorname{Ext}^i_A(N,M) = 0$ für $i < \operatorname{tf} M - \dim N$.
(Induktion nach $\dim N$. Wenn $\dim N = 0$ ist, ist $1 \le l(N) < \infty$. Für $l(N) = 1$, d.h. $N = k$, siehe 17.3. Für $l(N) > 1$ betrachte die von einer Folge $0 \longrightarrow N' \longrightarrow N \longrightarrow k \longrightarrow 0$ induzierte exakte Folge der "Ext" . Für $\dim N > 0$ sei E der größte Untermodul endlicher Länge von N . Betrachte die von $0 \longrightarrow E \longrightarrow N \longrightarrow N/E \longrightarrow 0$ induzierte exakte Folge der "Ext" . Man sieht so, daß man N durch N/E ersetzen, d.h. $E = 0$, also $\mathfrak{m} \notin \operatorname{Ass} N$ annehmen darf. Sei $x \in \mathfrak{m}$ ein NNT für N . Dann ist $\dim N/xN < \dim N$. Betrachte die durch $0 \longrightarrow N \xrightarrow{x} N \longrightarrow N/xN \longrightarrow 0$ induzierte exakte Folge der Ext, wende die Induktionsvoraussetzung auf N/xN an und die Tatsache, daß nach Nakayama x auf keinem endlichen A-Modul $\neq 0$ surjektiv operiert.)

8) Mit Hilfe von A6 und A7 kann man 17.15 auch beweisen.
Folgere ferner aus A6 und A7 (mit $N := A/\mathfrak{p}$): Unter den Voraussetzungen

von A7 sei $\mathfrak{p} \in \operatorname{Supp} M$. Dann ist

$$\dim M_{\mathfrak{p}} - \operatorname{tf} M_{\mathfrak{p}} \le \dim M - \operatorname{tf} M .$$

($\dim M - \operatorname{tf} M$ heißt für $M \neq 0$ die Cotiefe von M; 0 hat die Cotiefe 0.)

9) Serresche Bedingungen. Sei A ein noetherscher Ring, $n \in \mathbb{N}$. Definiere: A erfüllt die Bedingung (R_n), wenn $A_{\mathfrak{p}}$ regulär ist für jedes $\mathfrak{p} \in \operatorname{Spec} A$ mit $\operatorname{ht} \mathfrak{p} \le n$.
A erfüllt die Bedingung (S_n), wenn $\operatorname{tf} A_{\mathfrak{p}} \ge \operatorname{Min}\{n, \operatorname{ht} \mathfrak{p}\}$ für alle $\mathfrak{p} \in \operatorname{Spec} A$ ist. Zeige:

a) A ist genau dann reduziert, wenn A die Bedingungen (R_0) und (S_1) erfüllt.

b) A ist reduziert und ganz abgeschlossen in $S^{-1}A$ für $S = \operatorname{NNT}(A)$ genau dann, wenn A die Bedingungen (R_1) und (S_2) erfüllt. (8.14, 8A1).

10) Lokale vollständige Durchschnitte und lokale Gorensteinringe.
Definitionen: 1) Ein lokaler Ring A heißt lokaler vollständiger Durchschnitt, wenn es einen regulären lokalen Ring B und eine B-reguläre Folge $x_1, \ldots, x_r$ in B gibt, so daß $A \simeq B/(x_1, \ldots, x_r)$ ist.
2) Ein lokaler Ring A heißt ein Gorensteinring, wenn A noethersch und $\operatorname{inj.dim} A < \infty$ ist.
Man hat für lokale Ringe folgende Implikationen:

Regulär $\xRightarrow{a)}$ lokaler vollständiger Durchschnit $\xRightarrow{b)}$ Gorenstein $\xRightarrow{c)}$ Cohen-Macaulay.

Dabei ist a) trivial, b) einfach, c) nicht ganz einfach. (Der Leser möge einen Beweis von b) versuchen.)
Keine der Komplikationen ist umkehrbar. Zu a) siehe A2. Zu b) und c) sind die Beispiele nicht trivial.
Literatur: [Bass:G], [Herzog-Kunz], [Kaplansky], [Kunz].
(In [Kunz] werden Gorensteinringe auf eine - äquivalente - Weise definiert, für die die Implikation c) trivial ist.)

11) Sei A ein Hauptidealring mit unendlich vielen maximalen Idealen (etwa $A = \mathbb{Z}$). Formuliere und beweise einen zu 17.24 analogen Satz für $A[X_1, \ldots, X_n]$. (Beachte 9.A5.)

12) Sei k ein Körper, $\mathfrak{n} \subset k[X_1,\dots,X_n]$ das von $X_1,\dots,X_n$ erzeugte maximale Ideal im Polynomring und A der Unterring, der aus allen Polynomen ohne lineare Glieder besteht, schließlich $\mathfrak{m} = A \cap \mathfrak{n}$. Zeige: A ist von endlichem Typ über k, also noethersch, $\dim A_{\mathfrak{m}} = n$, $\operatorname{tf} A_{\mathfrak{m}} = 1$.
(Es ist $X^3 \notin X^2A$, aber $\mathfrak{m}\cdot X^3 \subset X^2A$.)

N.B.: $A_{\mathfrak{m}}$ ist integer, anders als der Ring $A/x\mathfrak{m}$ in 17.7f).

§18 KOMPLETTIERUNG

In diesem Paragraphen verstehen wir unter einer Filtrierung eines Ringes A *einfach eine absteigende Folge* $\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \dots$ *von Idealen mit* $\mathfrak{a}_0 = A$. *D.h. wir verzichten auf die Forderung* "$\mathfrak{a}_n\mathfrak{a}_m \subset \mathfrak{a}_{n+m}$".
(Der einzige Grund hierfür ist, daß sonst der Beweis von 18.57 etwas schwerfälliger würde.)

1. Cauchy-Folgen

Definition 18.1 Sei E ein Ring oder ein Modul, versehen mit Filtrierungen $F: E = E_0 \supset E_1 \supset E_2 \supset \dots$ und $F': E = E'_0 \supset E'_1 \supset E'_2 \supset \dots$.

Die Filtrierungen F und F' heißen äquivalent, wenn es zu jedem n ein m und ein m' mit $E_n \supset E'_m$ und $E'_n \supset E_{m'}$ gibt (d.h. wenn es zu jedem n ein m mit $E_n \supset E'_m$ und $E'_n \supset E_m$ gibt).

Bemerkung 18.2 Auf der Menge der Filtrierungen von E ist die Äquivalenz natürlich eine Äquivalenzrelation.

Konstruktion 18.3 Sei E ein Ring oder ein Modul, der mit einer Filtrierung $F = (E_n)_{n\in\mathbb{N}}$ versehen ist.

Eine Cauchy-Folge in E (bzgl. F) ist eine Folge $(x_i)_{i\in\mathbb{N}}$ mit $x_i \in E$, derart daß zu jedem $n \in \mathbb{N}$ ein $N \in \mathbb{N}$ existiert mit $x_i - x_j \in E_n$ für alle $i,j \geq N$.
Die Cauchy-Folgen bilden bzgl. gliedweiser Verknüpfungen einen Unterring bzw. Untermodul $\mathfrak{C}(E)$ von $E^{\mathbb{N}}$.

Eine Nullfolge in E (bzgl. F) ist eine Folge $(x_i)_{i\in\mathbb{N}}$ mit $x_i \in E$, derart daß zu jedem n ein N existiert mit $x_i \in E_n$ für $i \geq N$.

Die Nullfolgen bilden ein Ideal bzw. einen Untermodul $\mathfrak{N}(E)$ von $\mathfrak{C}(E)$. Dies ist einfach zu verifizieren.

Definiere: $\hat{E} := \mathfrak{C}(E)/\mathfrak{N}(E)$, die Komplettierung von E bzgl. F.

Sei $x \in E$. Die konstante Folge $(x)_{i\in\mathbb{N}}$ ist die Folge $(x_i)_{i\in\mathbb{N}}$ mit $x_i = x$ für alle i. Konstante Folgen sind Cauchy-Folgen.

Die Zuordnung $x \longmapsto (x)_{i\in\mathbb{N}}$, verkettet mit der kanonischen Projektion $\mathfrak{C}(E) \longrightarrow \mathfrak{C}(E)/\mathfrak{N}(E) = \hat{E}$, gibt also eine Abbildung

$$\varphi: E \longrightarrow \hat{E},$$

welche offenbar ein Homomorphismus ist.

Bemerkungen 18.4 a) Eine konstante Folge $(x)_{i\in\mathbb{N}}$ ist eine Nullfolge genau dann, wenn $x \in E_n$ für alle n ist. D.h.

$$\operatorname{Ker}\varphi = \bigcap_{n\in\mathbb{N}} E_n .$$

b) Wenn $E_n = 0$ ist für ein n, ist φ ein Isomorphismus.

Denn dann gibt es zu jeder Cauchy-Folge $(x_i)_{i\in\mathbb{N}}$ ein N mit $x_i = x_j$ für $i,j \geq N$. Die Folge $(x_i)_{i\in\mathbb{N}}$ ist also modulo $\mathfrak{N}(E)$ zu einer konstanten Folge kongruent.

c) Sei E mit zwei äquivalenten Filtrierungen F und F' versehen und $(x_i)_{i\in\mathbb{N}}$ eine Folge in E. Dann gilt offenbar: Die Folge $(x_i)_{i\in\mathbb{N}}$ ist eine Cauchy-Folge (bzw. Nullfolge) bezüglich F genau dann, wenn sie eine Cauchy-Folge (bzw. Nullfolge) bezüglich F' ist. Die Komplettierungen von E bzgl. F und F' stimmen also überein.

d) Sei E durch $F = (E_n)_{n\in\mathbb{N}}$ filtriert. Durch

$$d(x,y) = \operatorname{Inf}\{2^{-n} \mid x-y \in E_n\}$$

für $x,y \in E$ wird auf E eine Prämetrik definiert. D.h. es gilt

(i) $d(x,y) \in \mathbb{R}$, $d(x,y) \geq 0$, $d(x,x) = 0$,

(ii) $d(x,y) = d(y,x)$,

(iii) $d(x,y) \leq d(x,z) + d(z,y)$

für alle $x,y,z \in E$. (Es gilt sogar die Ungleichung (iii') $d(x,y) \leq \operatorname{Max}\{d(x,z),d(z,y)\}$, die (iii) impliziert.)

Die Prämetrik d ist eine Metrik, d.h. es gilt zusätzlich:

(iv) $d(x,y) = 0 \iff x = y$

genau dann, wenn $\bigcap_{n\in\mathbb{N}} E_n = \{0\}$ ist.

Bezüglich dieser (Prä-) Metrik d stimmen die o.a. Begriffe Cauchy-Folge, Nullfolge, Komplettierung mit den üblichen überein.

Definition 18.5 Ein Ring oder Modul E heißt bezüglich einer Filtrierung $F = (E_n)_{n\in\mathbb{N}}$ komplett, wenn der oben definierte Homomorphismus $\varphi\colon E \longrightarrow \hat{E}$ ein Isomorphismus ist.

Beachte, daß dies insbesondere $\bigcap_{n\in\mathbb{N}} E_n = \{0\}$ nach sich zieht. (Bei uns bedeutet "komplett" also dasselbe wie "complet et séparé" bei [Bourbaki].)

Beachte ferner, daß E komplett ist, wenn $E_m = 0$ für ein m gilt (18.4b)).

Definition 18.6 Seien E,E' Ringe oder Moduln, versehen mit Filtrierungen $F\colon E = E_0 \supset E_1 \supset \dots$ und $F'\colon E' = E'_0 \supset E'_1 \supset \dots$. Ein Homomorphismus $f\colon E \longrightarrow E'$ heißt stetig (bzgl. der Filtrierungen F,F'), wenn zu jedem $n \in \mathbb{N}$ ein $m \in \mathbb{N}$ mit $f(E_m) \subset E'_n$ existiert.

Feststellung 18.7 *Seien E,E',F,F' wie oben und $f\colon E \longrightarrow E'$ ein stetiger Homomorphismus. Wenn eine Folge $(x_i)_{i\in\mathbb{N}}$ in E eine Cauchy-Folge (bzw. Nullfolge) ist, so ist auch die Folge $(f(x_i))_{i\in\mathbb{N}}$ eine Cauchy-Folge (bzw. Nullfolge) in E'. Durch f wird also ein Homomorphismus $\hat{f}\colon \hat{E} \longrightarrow \hat{E}'$ induziert. Man hat einen Funktor "$\wedge$" auf der Kategorie der filtrierten Ringe (bzw. A-Moduln) mit stetigen Homomorphismen als Morphismen.* —

Bemerkung 18.8 Zwei Filtrierungen F,F' auf einem Ring (bzw. Modul) E sind äquivalent genau dann, wenn die Identität auf E sowohl bezüglich F,F' als auch bezüglich F',F stetig ist.

Feststellung 18.9 *Seien A ein Ring, $\mathfrak{a} \subset A$ ein Ideal, E und E' A-Moduln, die mit Filtrierungen F bzw. F' versehen sind. Ferner sei F i.w. $\mathfrak{a}$-adisch und F' $\mathfrak{a}$-zulässig.*

Dann ist jeder A-Modulhomomorphismus $f: E \longrightarrow E'$ stetig bzgl. F,F'.

Insbesondere sind je zwei i.w. $\mathfrak{a}$-adische Filtrierungen auf einem A-Modul E äquivalent.

Beweis: Sei F (bzw. F') gegeben durch Untermoduln E_n von E (bzw. E'_n von E'). Da F i.w. $\mathfrak{a}$-adisch ist, gibt es nach Definition (5.3 - 4) ein n_o mit $E_{n_o+n} = \mathfrak{a}^n E_{n_o}$ für $n \geq 0$. Da F' $\mathfrak{a}$-zulässig ist, gilt $\mathfrak{a}^n E' = \mathfrak{a}^n E'_o \subset E'_n$. Deshalb ist $f(E_{n_o+n}) = \mathfrak{a}^n f(E_{n_o}) \subset \mathfrak{a}^n E' \subset E'_n$.

Für den Zusatz beachte, daß nach Definition i.w. $\mathfrak{a}$-adische Filtrierungen insbesondere $\mathfrak{a}$-zulässig sind. —

2. Inverse Limiten

Hier wird eine andere Beschreibung der Komplettierung gegeben.

Definitionen 18.10 a) Ein inverses System $(M_n,f_n)_{n\in\mathbb{N}}$ ist eine Familie von Ringen bzw. Moduln M_n, $n\in\mathbb{N}$, und Homomorphismen $f_n: M_n \longrightarrow M_{n-1}$, $n\in\mathbb{N}_1$.

(Man mache sich folgendes Bild: $\ldots \xrightarrow{f_3} M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_o$.)

b) Der inverse Limes (auch projektiver Limes genannt) des inversen Systems $(M_n,f_n)_{n\in\mathbb{N}}$ ist

$$\varprojlim (M_n,f_n)_{n\in\mathbb{N}} := \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} M_n \mid x_n \in M_n,\ f_n(x_n) = x_{n-1} \right\} .$$

Man schreibt auch $\varprojlim M_n$ oder $\varprojlim\limits_{n} M_n$ für $\varprojlim (M_n,f_n)_{n\in\mathbb{N}}$.

Bemerkungen 18.11 a) $\varprojlim M_n$ ist also eine gewisse Teilmenge des direkten Produktes $\prod_{n\in\mathbb{N}} M_n$, und zwar die Menge derjenigen Folgen $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in M_n$, in denen jedes Glied Bild des nächsten (unter der entsprechenden Abbildung) ist. Solche Folgen nennt man auch kohärent.

b) Offenbar ist $\varprojlim M_n$ ein Unterring (bzw. Untermodul) des direkten Produktes $\prod_{n\in\mathbb{N}} M_n$.

c) Wir haben hier einen - für unsere Zwecke ausreichenden - speziellen Begriff von inversen Systemen definiert.

d) Der inverse Limes eines inversen Systems kann sehr groß sein. Wenn die f_n surjektiv sind, hat $\varprojlim M_n$ die Mächtigkeit des unendlichen Produktes $M_0 \times \prod_{n\geq 1} \operatorname{Ker}(f_n)$. Wenn also die f_n surjektiv sind und $\operatorname{Ker}(f_n)$ für unendlich viele n nicht trivial ist, ist $\varprojlim M_n$ überabzählbar.

e) Wenn in dem inversen System (M_n, f_n) die Homomorphismen f_n für $n > N$ Isomorphismen sind, ist $\varprojlim M_n \simeq M_N$ auf kanonische Weise.

f) Zum dualen Begriff "direkter Limes" siehe [Schubert].

Sei jetzt E ein Ring oder Modul, der mit einer Filtrierung $E = E_0 \supset E_1 \supset \ldots$ versehen ist.

Die E/E_n zusammen mit den kanonischen (surjektiven) Homomorphismen $E/E_n \longrightarrow E/E_{n-1}$ bilden dann ein inverses System, und man hat den zugehörigen inversen Limes $\varprojlim E/E_n$.

Ferner hat man einen kanonischen Homomorphismus $\kappa: E \longrightarrow \varprojlim E/E_n$.

Sei nämlich $\pi_n: E \longrightarrow E/E_n$ die kanonische Projektion, so ist $(\pi_n(x))_{n\in\mathbb{N}}$ offenbar für jedes $x \in E$ eine kohärente Folge.

Man definiert $\kappa(x) = (\pi_n(x))_{n\in\mathbb{N}} \in \varprojlim(E/E_n)$.

Satz 18.12 *Sei* E *ein Ring oder Modul, der mit einer Filtrierung* $E = E_0 \supset E_1 \supset \ldots$ *versehen ist.*

Dann sind $\hat{E}$ *und* $\varprojlim_n(E/E_n)$ *isomorph. Genauer gilt: Es gibt einen kanonischen Isomorphismus* $f: \hat{E} \longrightarrow \varprojlim_n(E/E_n)$, *der folgendes Dreieck kommutativ macht:*

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[dr, "\kappa"'] & \hat{E} \arrow[d, "f"] \\ & \varprojlim_n (E/E_n) \end{tikzcd} .$$

<u>Beweis:</u> Sei $x \in \hat{E}$ repräsentiert durch eine Cauchy-Folge $(x_i)_{i\in\mathbb{N}}$ in E. Zu $n \in \mathbb{N}$ gibt es dann ein $N \in \mathbb{N}$, so daß $x_i - x_j \in E_n$ für alle $i,j \geq N$ gilt. D.h. für $i,j \geq N$ ist $\pi_n(x_i) = \pi_n(x_j)$ in E/E_n. Setze $\xi_n := \pi_n(x_i)$ für $i \geq N$.

Die ξ_n bilden dann eine kohärente Folge für das inverse System der E/E_n. Definiere $f(x) := (\xi_n)_{n\in\mathbb{N}} \in \varprojlim_n (E/E_n)$.

Wenn $(x_i')_{i\in\mathbb{N}}$ dasselbe x repräsentiert, ist $(x_i - x_i')_{i\in\mathbb{N}}$ eine Nullfolge und deshalb $\pi_n(x_i) = \pi_n(x_i')$ für genügend große i (abhängig von n). Also ist f wohldefiniert.

Offenbar ist f ein Homomorphismus, der obiges Diagramm kommutativ macht.

Um zu zeigen, daß f auch ein Isomorphismus ist, beschreiben wir eine inverse Abbildung $g: \varprojlim_n (E/E_n) \longrightarrow \hat{E}$.

Sei $(\xi_n)_{n\in\mathbb{N}} \in \varprojlim_n (E/E_n)$ eine kohärente Folge, $\xi_n \in E/E_n$. Sei $x_n \in E$ ein beliebiger Repräsentant von ξ_n. Da $x_{n+1} - x_n \in E_n$ ist, ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge, definiert also ein Element $g((\xi_n)_{n\in\mathbb{N}}) \in \hat{E}$.
Wenn man andere Repräsentanten x_n' von ξ_n wählt, ist $x_n - x_n' \in E_n$, also $(x_n - x_n')_{n\in\mathbb{N}}$ eine Nullfolge. Somit ist g wohldefiniert.
Die Gleichung $f \circ g = \mathrm{id}_{\varprojlim (E/E_n)}$ sieht man unmittelbar.

Wenn aber $(x_i)_{i\in\mathbb{N}}$ eine $x \in \hat{E}$ repräsentierende Cauchy-Folge in E ist, gibt es zu $n \in \mathbb{N}$ ein N_n mit $\xi_n = \pi_n(x_i) \in E/E_n$ konstant für $i \geq N_n$. Wenn nun y_n ein Repräsentant von ξ_n ist, gilt $y_n - x_i \in E_n$ für $i \geq N_n$. Also ist auch $y_i - x_i \in E_n$ für $i \geq \mathrm{Max}\{n, N_n\}$. Es folgt, daß $(y_i - x_i)_{i\in\mathbb{N}}$ eine Nullfolge ist. Da die Folge $(y_i)_{i\in\mathbb{N}}$ das Element $g \circ f(x)$ repräsentiert, ist $g \circ f = \mathrm{id}_{\hat{E}}$. —

<u>Definition 18.13</u> Ein Homomorphismus zwischen inversen Systemen $\alpha: (M_n, f_n)_{n\in\mathbb{N}} \longrightarrow (N_n, g_n)_{n\in\mathbb{N}}$ ist eine Familie $(\alpha_n)_{n\in\mathbb{N}}$ von Homomorphismen

$$\alpha_n: M_n \longrightarrow N_n ,$$

derart daß alle Quadrate

$$\begin{array}{ccc} M_{n+1} & \xrightarrow{\alpha_{n+1}} & N_{n+1} \\ \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle g_{n+1}} \\ M_n & \xrightarrow{\alpha_n} & N_n \end{array}$$

kommutativ sind. Die inversen Systeme von Ringen bzw. A-Moduln zusammen mit den o.a. Homomorphismen bilden eine Kategorie.

Feststellung 18.14 *Sei* $\alpha\colon (M_n,f_n) \longrightarrow (N_n,g_n)$ *ein Homomorphismus inverser Systeme. Die durch die* $\alpha_n\colon M_n \longrightarrow N_n$ *induzierte Abbildung* $\prod_{n\in\mathbb{N}} \alpha_n\colon \prod_{n\in\mathbb{N}} M_n \longrightarrow \prod_{n\in\mathbb{N}} N_n$ *bildet offenbar* $\varprojlim_n M_n$ *in* $\varprojlim_n N_n$ *ab.*

Man erhält also einen Homomorphismus $\alpha_* = \varprojlim_n \alpha_n\colon \varprojlim_n M_n \longrightarrow \varprojlim_n N_n$.
Man sieht sofort, daß auf diese Weise $\varprojlim$ *ein Funktor auf der Kategorie der inversen Systeme von Ringen oder von A-Moduln ist. Dieser Funktor ist A-linear auf der Kategorie der inversen Systeme von A-Moduln.* –

Feststellung 18.15 *Seien* $E = E_0 \supset E_1 \supset \ldots$ *und* $E' = E'_0 \supset E'_1 \supset \ldots$ *filtrierte Ringe oder Moduln und* $\alpha\colon E \longrightarrow E'$ *ein Homomorphismus, der* $\alpha(E_n) \subset E'_n$ *erfüllt. Dann ist das Quadrat*

$$\begin{array}{ccc} \hat{E} & \xrightarrow{\hat{\alpha}} & \hat{E}' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ \varprojlim_n E/E_n & \xrightarrow{\alpha_*} & \varprojlim_n E'/E'_n \end{array} ,$$

in dem f *und* f' *die kanonischen Isomorphismen (18.12) sind und* α_* *durch die durch* α *gegebenen Homomorphismen* $E/E_n \longrightarrow E'/E'_n$ *induziert ist, kommutativ.*

Dies folgt unmittelbar aus der Konstruktion von f und f' im Beweis von Satz 18.12. –

Definitionen 18.16 a) Ein inverses System (M_n,f_n) heißt surjektiv, wenn f_n für jedes $n \in \mathbb{N}$ surjektiv ist.

b) Das inverse System 0 sei auf naheliegende Weise definiert.

c) Eine Folge von Homomorphismen inverser Systeme von Moduln $(M'_n,f'_n) \xrightarrow{\alpha} (M_n,f_n) \xrightarrow{\beta} (M''_n,f''_n)$ heißt exakt, wenn jede der Folgen $M'_n \xrightarrow{\alpha_n} M_n \xrightarrow{\beta_n} M''_n$ exakt ist.

Satz 18.17 *a) Sei* $0 \longrightarrow (M'_n, f'_n) \xrightarrow{\alpha} (M_n, f_n) \xrightarrow{\beta} (M''_n, f''_n)$ *eine exakte Folge von inversen Systemen von* A-*Moduln. Dann ist die induzierte Folge* $0 \longrightarrow \varprojlim_n M'_n \xrightarrow{\alpha_*} \varprojlim_n M_n \xrightarrow{\beta_*} \varprojlim_n M''_n$ *ebenfalls exakt.*

b) Wenn darüber hinaus (M', f'_n) *ein surjektives System und* $0 \longrightarrow (M', f'_n) \xrightarrow{\alpha} (M_n, f_n) \xrightarrow{\beta} (M''_n, f''_n) \longrightarrow 0$ *exakt ist, so ist auch die induzierte Folge* $0 \longrightarrow \varprojlim_n M'_n \xrightarrow{\alpha_*} \varprojlim_n M_n \xrightarrow{\beta_*} \varprojlim_n M''_n \longrightarrow 0$ *exakt.*

Beweis: a) Die Injektivität von α_* sieht man an dem kommutativen Quadrat

$$\begin{tikzcd}
\varprojlim_n M'_n \arrow[r, "\alpha_*"] \arrow[d, hook] & \varprojlim_n M_n \arrow[d, hook] \\
\prod_n M'_n \arrow[r, "\Pi\alpha_n"] & \prod_n M_n
\end{tikzcd} ,$$

da auch $\Pi\alpha_n$ injektiv ist.

Da $\varprojlim$ ein additiver Funktor ist, ist $\beta_* \circ \alpha_* = (\beta \circ \alpha)_* = 0$.
Es bleibt, $\operatorname{Ker} \beta_* \subset \operatorname{Im} \alpha_*$ zu zeigen. Sei also $\xi = (x_n)_{n\in\mathbb{N}} \in \varprojlim_n M_n$ eine kohärente Folge mit $\beta_*(\xi) = 0$, d.h. $\beta_n(x_n) = 0$ für alle n. Nach Voraussetzung gibt es $y_n \in M'_n$ mit $\alpha_n(y_n) = x_n$. Da alle α_n injektiv sind, sieht man sofort, daß auch $\eta := (y_n)_{n\in\mathbb{N}}$ eine kohärente Folge ist. Und es ist $\alpha_*(\eta) = \xi$.

b) Es ist noch die Surjektivität von β_* zu zeigen.
Sei $\zeta := (z_n)_{n\in\mathbb{N}} \in \varprojlim_n M''_n$ eine kohärente Folge. Wir konstruieren induktiv eine kohärente Folge $\xi := (x_n)_{n\in\mathbb{N}} \in \varprojlim_n M_n$ mit $\beta_*(\xi) = \zeta$.

Wähle x_0 so, daß $\beta_0(x_0) = z_0$ ist. Angenommen, wir haben $x_0,\ldots,x_{n-1}$ schon gefunden. Betrachte das kommutative Diagramm mit exakten Zeilen

$$\begin{tikzcd}
M'_n \arrow[r, "\alpha_n"] \arrow[d, "f'_n"'] & M_n \arrow[r, "\beta_n"] \arrow[d, "f_n"'] & M''_n \arrow[d, "f''_n"'] \\
M'_{n-1} \arrow[r, "\alpha_{n-1}"] & M_{n-1} \arrow[r, "\beta_{n-1}"] & M''_{n-1}
\end{tikzcd} .$$

Sei x'_n ein Urbild von z_n unter β_n. Dann ist
$\beta_{n-1}(f_n(x'_n)-x_{n-1}) = f''_n\, \beta_n(x'_n)-\beta_{n-1}(x_{n-1}) = f''_n(z_n)-z_{n-1} = z_{n-1}-z_{n-1} = 0$.

Wegen der Exaktheit der unteren Zeilen gibt es $y_{n-1} \in M'_{n-1}$ mit $\alpha_{n-1}(y_{n-1}) = f_n(x'_n)-x_{n-1}$. Da nach Voraussetzung f'_n surjektiv ist, gibt es ein $y_n \in M'_n$ mit $f'_n(y_n) = y_{n-1}$. Für $x_n = x'_n-\alpha_n(y_n)$ ist dann $\beta_n(x_n) = \beta_n(x'_n)-\beta_n \circ \alpha_n(y_n) = \beta_n(x'_n) = z_n$ und $f_n(x_n) = f_n(x'_n-\alpha_n(y_n)) =$ $= f_n(x'_n)-(\alpha_{n-1} \circ f'_n)(y_n) = f_n(x'_n)-(f_n(x'_n)-x_{n-1}) = x_{n-1}$. Ein solches x_n war zu finden. —

Folgerung 18.18 *Seien* A *ein noetherscher Ring,* $\mathfrak{a} \subset A$ *ein Ideal und*

$$(*) \qquad 0 \longrightarrow E' \xrightarrow{\alpha} E \xrightarrow{\beta} E'' \longrightarrow 0$$

eine exakte Folge von endlichen A*-Moduln, die mit der* $\mathfrak{a}$*-adischen Filtrierung (5.3-4) versehen sind.*

Die nach 18.7 und 18.9 induzierte Folge

$$(**) \qquad 0 \longrightarrow \hat{E}' \xrightarrow{\hat{\alpha}} \hat{E} \xrightarrow{\hat{\beta}} \hat{E}'' \longrightarrow 0$$

ist dann ebenfalls exakt.

Beweis: Wir fassen E' als Untermodul von E auf. Die durch $(E' \cap \mathfrak{a}^n E)_{n\in\mathbb{N}}$ definierte Filtrierung auf E' ist i.w. $\mathfrak{a}$-adisch nach Artin-Rees (5.5), also nach 18.9 zur $\mathfrak{a}$-adischen Filtrierung auf E' äquivalent. Sie liefert nach 18.4 c) dieselbe Komplettierung.

Behauptung: Die durch (*) induzierte Folge

$$0 \longrightarrow E'/(E' \cap \mathfrak{a}^n E) \xrightarrow{\alpha_n} E/\mathfrak{a}^n E \xrightarrow{\beta_n} E''/\mathfrak{a}^n E'' \longrightarrow 0$$

ist für jedes n exakt.

Denn aus (*) erhält man durch Tensorieren mit $A/\mathfrak{a}^n$ die exakte Folge

$$E'/\mathfrak{a}^n E' \longrightarrow E/\mathfrak{a}^n E \xrightarrow{\beta_n} E''/\mathfrak{a}^n E'' \longrightarrow 0 ,$$

also - durch Verkettung mit der kanonischen Projektion $E' \longrightarrow E'/\mathfrak{a}^n E'$ - die exakte Folge

$$E' \xrightarrow{\alpha'_n} E/\mathfrak{a}^n E \xrightarrow{\beta_n} E''/\mathfrak{a}^n E'' \longrightarrow 0 ,$$

und offensichtlich ist $\operatorname{Ker} \alpha'_n = E' \cap \mathfrak{a}^n E$.

Wegen 18.17b) ist die induzierte Folge der inversen Limites exakt. Und diese ist nach 18.12 und 18.15 isomorph zur Folge (**). —

Definition 18.19 Sei A ein Ring, $\mathfrak{a} \subset A$ ein Ideal, M ein A-Modul. Die Komplettierung von A bzw. M bezüglich der $\mathfrak{a}$-adischen Filtrierung heißt $\mathfrak{a}$-adische Komplettierung. Ferner heißt A bzw. M $\mathfrak{a}$-adisch komplett, wenn die kanonische Abbildung $\varphi: A \longrightarrow \hat{A}$ bzw. $\varphi: M \longrightarrow \hat{M}$ ein Isomorphismus ist (vgl. 18.5).

Bemerkungen 18.20 a) Seien $A,\mathfrak{a},M$ wie oben, A und M mit der $\mathfrak{a}$-adischen Filtrierung versehen.

Sei $(x_i)_{i\in\mathbb{N}}$ eine Cauchy-Folge (bzw. Nullfolge) in M und $(a_i)_{i\in\mathbb{N}}$ eine Folge (etwa eine Cauchy-Folge) in A. Dann ist $(a_i x_i)_{i\in\mathbb{N}}$ eine Cauchy-Folge (bzw. Nullfolge) in M. Auf diese Weise wird $\mathfrak{C}(M)$ ein $\mathfrak{C}(A)$-Modul und $\mathfrak{N}(M)$ ein $\mathfrak{C}(A)$-Untermodul von $\mathfrak{C}(M)$ (Bezeichnungen wie in 18.3).

Ebenso sieht man, daß $\mathfrak{N}(A)\cdot\mathfrak{C}(M) \subset \mathfrak{N}(M)$ gilt. Der $\mathfrak{C}(A)$-Modul $\hat{M} = \mathfrak{C}(M)/\mathfrak{N}(M)$ wird also von $\mathfrak{N}(A)$ annulliert, ist mithin ein Modul über $\mathfrak{C}(A)/\mathfrak{N}(A) = \hat{A}$.

b) Wenn $(a_i)_{i\in\mathbb{N}}$ eine Cauchy-Folge (bzw. eine Nullfolge) in A und $x \in M$ ist, ist $(a_i x)_{i\in\mathbb{N}}$ eine Cauchy-Folge (bzw. eine Nullfolge) in M. Man erhält eine Abbildung $\hat{A} \times M \longrightarrow \hat{M}$, die A-bilinear ist bzgl. der kanonischen Abbildung $\varphi: A \longrightarrow \hat{A}$, also einen in M natürlichen $\hat{A}$-Modulhomomorphismus $\psi: \hat{A} \otimes_A M \longrightarrow \hat{M}$.

Satz 18.21 *Wenn M endlich darstellbar (insbesondere wenn A noethersch und M endlich ist), ist ψ ein Isomorphismus.*

Beweis: Zunächst sieht man, daß $\hat{A}^n = \hat{A} \otimes_A A^n$ durch ψ isomorph auf $(A^n)^\wedge$ abgebildet wird. Dies kann man aus der kanonischen Isomorphie $A^n/\mathfrak{a}^r(A^n) \simeq (A/\mathfrak{a}^r)^n$ oder aus 18.18 folgern.

Sei jetzt $A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$ exakt. Betrachte das kommutative Diagramm mit exakten Zeilen

$$\begin{tikzcd}
\hat{A}^m \arrow[r] \arrow[d, "\psi_1"'] & \hat{A}^n \arrow[r] \arrow[d, "\psi_2"'] & \hat{A} \otimes_A M \arrow[r] \arrow[d, "\psi_3"'] & 0 \arrow[d] \\
(A^m)^\wedge \arrow[r] & (A^n)^\wedge \arrow[r] & \hat{M} \arrow[r] & 0
\end{tikzcd}$$

Aus der Bijektivität von ψ_1 und ψ_2 folgt die von ψ_3. —

Satz 18.22 *Seien A ein noetherscher Ring und $\mathfrak{a} \subset A$ ein Ideal. Dann ist die $\mathfrak{a}$-adische Komplettierung $\hat{A}$ flach über A.*

Beweis: Sei $\alpha : N \longrightarrow M$ injektiv. Falls M (und damit N) endlich ist, ist $\alpha^*: \hat{A} \otimes_A N \longrightarrow \hat{A} \otimes_A M$ injektiv nach 18.18 und 18.21.

Die Flachheit von $\hat{A}$ folgt also aus

Lemma 18.23. *Seien A ein (nicht notwendig noetherscher) Ring, E ein A-Modul, derart daß jeder injektive Homomorphismus endlicher Moduln $N \longrightarrow M$ einen injektiven Homomorphismus $E \otimes_A N \longrightarrow E \otimes_A M$ induziert. Dann ist E flach.*

Beweis: Sei $\alpha: N' \longrightarrow M'$ ein injektiver Homomorphismus beliebiger A-Moduln und $\Sigma\, x_i \otimes y_i \in \operatorname{Ker}(E \otimes_A \alpha) \subset E \otimes N'$. D.h. es ist $\Sigma\, x_i \otimes \alpha(y_i) = 0$ in $E \otimes M'$. Mit den Bezeichnungen von 10.31 bedeutet dies $\Sigma\, (x_i, \alpha(y_i)) \in U \subset A^{(E\times M')}$.
D.h. $\Sigma\, (x_i, \alpha(y_i))$ ist eine Linearkombination gewisser Elemente der Formen $(x+x', z) - (x,z) - (x',z)$, $(x, z+z') - (x,z) - (x,z')$, $(ax,z) - a(x,z)$, $(x,az) - a(x,z)$ mit $a \in A$, $x, x' \in E$, $z, z' \in M'$.

Insgesamt werden endlich viele Elemente $z_1,\dots,z_r \in M'$ gebraucht, um $\Sigma\, (x_i, \alpha(y_i))$ in U darzustellen.

Sei nun $N \subset N'$ von den endlich vielen y_i und $M \subset M'$ von den $\alpha(y_i)$ und den z_j erzeugt. Dann wird N durch α in M abgebildet, und man hat $\Sigma\, x_i \otimes \alpha(y_i) = 0$ in $E \otimes M$. Da aber $E \otimes N \longrightarrow E \otimes M$ nach Voraussetzung injektiv ist, folgt $\Sigma\, x_i \otimes y_i = 0$ in $E \otimes N$, also erst recht in $E \otimes N'$. —

Satz 18.24 *Sei A ein noetherscher Ring, $\mathfrak{a} \subset A$ ein Ideal. Mit "$\wedge$" sei die $\mathfrak{a}$-adische Komplettierung bezeichnet. $\mathfrak{b}, \mathfrak{c}$ seien weitere Ideale. Dann gilt:*
a) $\hat{\mathfrak{b}} = \hat{A}\mathfrak{b} \simeq \hat{A} \otimes_A \mathfrak{b}$;
b) $(\mathfrak{b}\mathfrak{c})^\wedge = \hat{\mathfrak{b}}\hat{\mathfrak{c}}$, *insbesondere:* $(\mathfrak{a}^n)^\wedge = (\hat{\mathfrak{a}})^n$.

Beweis: a) Betrachte die Abbildung $\psi: \hat{A} \otimes_A \mathfrak{b} \longrightarrow \hat{\mathfrak{b}}$ aus 18.20b). Sie ist nach 18.21 ein Isomorphismus, da A noethersch ist. Ihr Bild besteht andererseits aus den Klassen von Cauchy-Folgen der Form $(a_i b)_{i\in\mathbb{N}} = (a_i)_{i\in\mathbb{N}} \cdot b$ mit $a_i \in A$, $b \in \mathfrak{b}$, liegt also in $\hat{A}\mathfrak{b} \subset \hat{\mathfrak{b}}$.
b) Nach a) ist $(\mathfrak{b}\mathfrak{c})^\wedge = \hat{A}(\mathfrak{b}\mathfrak{c}) = \hat{A}\mathfrak{b}\hat{A}\mathfrak{c} = \hat{\mathfrak{b}}\hat{\mathfrak{c}}$. —

Unter den Voraussetzungen von 18.24 haben wir kanonische Homomorphismen

$$\mathfrak{a}^n \xrightarrow{\psi} \hat{\mathfrak{a}}^n ,$$

also $\mathfrak{a}^m/\mathfrak{a}^n \longrightarrow \hat{\mathfrak{a}}^m/\hat{\mathfrak{a}}^n$ für $n \geq m \geq 0$, also $gr_{\mathfrak{a}}(A) \longrightarrow gr_{\hat{\mathfrak{a}}}(\hat{A})$.

Satz 18.25 *Unter den Voraussetzungen von 18.24 gilt:*

a) *Die angegebenen Homomorphismen*

$$\mathfrak{a}^m/\mathfrak{a}^n \longrightarrow \hat{\mathfrak{a}}^m/\hat{\mathfrak{a}}^n \quad \textit{insbesondere}$$

$$A/\mathfrak{a}^n \longrightarrow \hat{A}/\hat{\mathfrak{a}}^n \quad \textit{und}$$

$$gr_{\mathfrak{a}}(A) \longrightarrow gr_{\hat{\mathfrak{a}}}(\hat{A})$$

sind Isomorphismen.

b) *Der kanonische Homomorphismus* $\hat{A} \longrightarrow \hat{\hat{A}}$ *ist ein Isomorphismus.*

c) $\hat{\mathfrak{a}} \subset \mathrm{Jac}(\hat{A})$.

Beweis: a) Man hat ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd}
 & 0 \arrow[rr] & & \mathfrak{a}^n \arrow[rr] \arrow[dl] \arrow[dd] & & \mathfrak{a}^m \arrow[rr] \arrow[dl] \arrow[dd] & & \mathfrak{a}^m/\mathfrak{a}^n \arrow[rr] \arrow[dl, "\varphi"'] \arrow[dd, "\alpha"] & & 0 \\
0 \arrow[rr] & & (\mathfrak{a}^n)^\wedge \arrow[rr] \arrow[dr, "\beta_1"', "\sim"] & & (\mathfrak{a}^m)^\wedge \arrow[rr] \arrow[dr, "\beta_2"', "\sim"] & & (\mathfrak{a}^m/\mathfrak{a}^n)^\wedge \arrow[rrr] \arrow[dr, "\beta_3"'] & & & 0 \\
 & 0 \arrow[rr] & & \hat{\mathfrak{a}}^n \arrow[rr] & & \hat{\mathfrak{a}}^m \arrow[rr] & & \hat{\mathfrak{a}}^m/\hat{\mathfrak{a}}^n \arrow[rr] & & 0
\end{tikzcd}$$

Da $\mathfrak{a}^{n-m}(\mathfrak{a}^m/\mathfrak{a}^n) = 0$ ist, ist φ ein Isomorphismus gemäß 18.4b).
Da β_1 und β_2 nach 18.24 Isomorphismen sind, ist auch β_3 ein solcher.
Es folgt selbiges für α .

b) Wegen 18.24 stimmen die $\mathfrak{a}$-adische und die $\hat{\mathfrak{a}}$-adische Filtrierung auf $\hat{A}$ überein. Mit a) erhält man $\hat{\hat{A}} = \varprojlim_n \hat{A}/\hat{\mathfrak{a}}^n \simeq \varprojlim_n A/\mathfrak{a}^n = \hat{A}$.

c) Da $\hat{A}$ nach b) mit seiner $\hat{\mathfrak{a}}$-adischen Komplettierung übereinstimmt, ist jede Cauchy-Folge in $\hat{A}$ zu einer konstanten Folge kongruent modulo dem Ideal $\mathfrak{N}(\hat{A})$ der Nullfolgen. D.h. jede Cauchy-Folge "konvergiert".

Seien $x \in \hat{\mathfrak{a}}$, $y \in \hat{A}$. Dann ist auch $z := xy \in \hat{\mathfrak{a}}$. Man sieht nun leicht, daß die geometrische Reihe $\sum_{n=0}^{\infty} z^n$ (aufgefaßt als Folge ihrer Teilsummen) eine Cauchy-Folge ist. Da $(1-z) \sum_{n=0}^{\infty} z^n = 1$ ist, ist $1-xy = 1-z \in \hat{A}^*$, also $x \in \mathrm{Jac}(\hat{A})$ nach 1.23. —

Folgerung 18.26 *Sei* $\mathfrak{m}$ *ein maximales Ideal eines noetherschen Ringes* A.

a) *Dann ist die* $\mathfrak{m}$*-adische Komplettierung* $\hat{A}$ *von* A *ein lokaler Ring* *mit dem maximalen Ideal* $\hat{\mathfrak{m}}$.

b) *Ferner induziert der Homomorphismus* $i_{A,\mathfrak{m}}: A \longrightarrow A_{\mathfrak{m}}$ *einen Isomorphismus* $\hat{A} \longrightarrow (A_{\mathfrak{m}})^{\wedge}$, *wobei* $(A_{\mathfrak{m}})^{\wedge}$ *die* $\mathfrak{m}A_{\mathfrak{m}}$*-adische Komplettierung von* $A_{\mathfrak{m}}$ *bezeichnet.*
(Beachte, daß $\mathfrak{m}$-adische und $\mathfrak{m}A_{\mathfrak{m}}$-adische Filtrierung auf $A_{\mathfrak{m}}$ übereinstimmen.)

Beweis: a) Es ist $\hat{A}/\hat{\mathfrak{m}} \simeq A/\mathfrak{m}$ ein Körper, also $\hat{\mathfrak{m}}$ ein maximales Ideal von $\hat{A}$. Andererseits gilt $\hat{\mathfrak{m}} \subset \operatorname{Jac} \hat{A}$.

b) $i_{A,\mathfrak{m}}$ induziert Isomorphismen $A/\mathfrak{m}^n \longrightarrow A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^n$. –

Bemerkung 18.27 Sei A noethersch und $\mathfrak{a} \subset \operatorname{Jac} A$ ein Ideal. Dann ist die $\mathfrak{a}$-adische Komplettierung $\hat{A}$ treuflach über A. Ferner ist die kanonische Abbildung $\varphi: A \longrightarrow \hat{A}$ injektiv.
Es ist $\operatorname{Ker} \varphi \overset{18.4}{=} \cap\, \mathfrak{a}^n \overset{5.8}{=} (0)$. Da $\mathfrak{a} \subset \operatorname{Jac}(A)$, $\hat{\mathfrak{a}} \subset \operatorname{Jac}(\hat{A})$ und $A/\mathfrak{a} \simeq \hat{A}/\hat{\mathfrak{a}}$ ist, entspricht jedes maximale Ideal von A einem solchen von $\hat{A}$ und wird mit φ in dieses abgebildet. Da $\hat{A}$ flach über A ist, folgt die Treuflachheit mit 10.51. –

3. Noetherzität von Komplettierungen

Lemma 18.28 *Seien* E, E' *Moduln, versehen mit Filtrierungen* $F: E = E_0 \supset E_1 \supset \dots$, $F': E' = E'_0 \supset E'_1 \supset \dots$ *und* $f: E \longrightarrow E'$ *ein Homomorphismus, der* $f(E_n) \subset E'_n$ *erfüllt. Sei* $\operatorname{gr}(f): \operatorname{gr}_F(E) \longrightarrow \operatorname{gr}_{F'}(E')$ *der induzierte Homomorphismus* (s.u.).

a) *Wenn* $\operatorname{gr}(f)$ *injektiv und* $\bigcap_{n\in\mathbb{N}} E_n = (0)$ *ist, ist* f *injektiv.*

b) *Wenn* $\operatorname{gr}(f)$ *surjektiv,* E *bezüglich* F *komplett und* $\bigcap_{n\in\mathbb{N}} E'_n = (0)$ *ist, ist* f *surjektiv und* E' *komplett.*

Es ist $\operatorname{gr}_F(E) = \bigoplus_{n\in\mathbb{N}} E_n/E_{n+1}$. Da f für jedes n einen Homomorphismus $\operatorname{gr}_n(f): E_n/E_{n+1} \longrightarrow E'_n/E'_{n+1}$ induziert, induziert f einen Homomorphismus $\operatorname{gr}(f): \operatorname{gr}_F(E) \longrightarrow \operatorname{gr}_{F'}(E')$.

Beweis: a) Sei $x \in \operatorname{Ker} f$, etwa $x \in E_n$, und $\overline{x}$ die Restklasse modulo E_{n+1}. Da $f(x) = 0$, ist auch $\operatorname{gr}_n(f)(\overline{x}) = 0$. Es folgt $\overline{x} = 0$, da $\operatorname{gr}(f)$ injektiv ist.

Also ist $x \in E_{n+1}$. Induktiv folgt: Für alle n ist $x \in E_n$, mithin $x \in \bigcap_{n \in \mathbb{N}} E_n = \{0\}$.

b) Wir zeigen zunächst mit Induktion nach n, daß die durch f induzierte Abbildung $E/E_n \longrightarrow E'/E'_n$ surjektiv ist.
Der Fall $n = 0$ ist trivial. Für $n \geq 0$ betrachte das kommutative Diagramm mit naheliegenden Abbildungen, dessen Zeilen exakt sind:

$$(*) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & E_n/E_{n+1} & \xrightarrow{\alpha} & E/E_{n+1} & \xrightarrow{\beta} & E/E_n & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle g_n} & & \Big\downarrow{\scriptstyle h_{n+1}} & & \Big\downarrow{\scriptstyle h_n} & & \\ 0 & \longrightarrow & E'_n/E'_{n+1} & \xrightarrow{\alpha'} & E'/E'_{n+1} & \xrightarrow{\beta'} & E'/E'_n & \longrightarrow & 0 \end{array}$$

Nach Voraussetzung ist $g_n = \operatorname{gr}_n(f)$ surjektiv, nach Induktionsvoraussetzung ist es auch h_n. Die Surjektivität von h_{n+1} zeigt man mit folgender "Diagrammjagd": Zu $x' \in E'/E'_{n+1}$ gibt es ein $y \in E/E_{n+1}$ mit $h_n \circ \beta(y) = \beta'(x')$, da h_n und β surjektiv sind. Dann ist $x' - h_{n+1}(y) \in \operatorname{Ker} \beta' = \operatorname{Im} \alpha'$. Da g_n surjektiv ist, gibt es ein $z \in E_n/E_{n+1}$ mit $\alpha' \circ g_n(z) = x' - h_{n+1}(y)$. Für $x = y + \alpha(z)$ gilt dann $h_{n+1}(x) = x'$.

Durch f wird also eine exakte Folge von inversen Systemen

$$0 \longrightarrow (\operatorname{Ker} h_n)_{n \in \mathbb{N}} \longrightarrow (E/E_n)_{n \in \mathbb{N}} \longrightarrow (E'/E'_n)_{n \in \mathbb{N}} \longrightarrow 0$$

induziert, wobei die h_n dieselben wie im Diagramm $(*)$ sind.

Behauptung: Das inverse System $(\operatorname{Ker} h_n)_{n \in \mathbb{N}}$ ist surjektiv.

Der Beweis hierfür geschieht wieder mittels einer Diagrammjagd in $(*)$.

Sei $x \in \operatorname{Ker} h_n \subset E/E_n$ und $y \in \beta^{-1}(x) \subset E/E_{n+1}$. Dann ist $\beta' \circ h_{n+1}(y) = h_n(x) = 0$, also $h_{n+1}(y) \in \operatorname{Ker} \beta' = \operatorname{Im} \alpha'$. Mithin gibt es ein $z \in E_n/E_{n+1}$ mit $\alpha' \circ g_n(z) = h_{n+1}(y)$. Somit ist $y - \alpha(z) \in \operatorname{Ker} h_{n+1}$ und $\beta(y - \alpha(z)) = \beta(y) = x$.

Aus der Behauptung folgt mit 18.17b) die Surjektivität von $\varprojlim_n E/E_n \longrightarrow \varprojlim_n E'/E'_n$. Wir haben also ein kommutatives Diagramm

$$\begin{tikzcd} E = \hat{E} \arrow[r, "f"] \arrow[dr, "\hat{f}"'] & E' \arrow[d, "\varphi'"] \\ & \hat{E}' \end{tikzcd},$$

in dem $\hat{f}$ surjektiv ist.

Da $\operatorname{Ker} \varphi' = \bigcap_{n\in\mathbb{N}} E'_n = \{0\}$ ist, folgt Teil b) des Lemmas. —

Satz 18.29 *Sei* A *ein* $\mathfrak{a}$*-adisch kompletter Ring,* E *ein* A*-Modul, der mit einer* $\mathfrak{a}$*-zulässigen Filtrierung* $F\colon E = E_0 \supset E_1 \supset \dots$ *mit* $\bigcap_{n\in\mathbb{N}} E_n = \{0\}$ *versehen ist.*

a) Wenn $gr_F(E)$ *ein endlicher* $gr_{\mathfrak{a}}(A)$*-Modul ist, so ist* E *ein endlicher* A*-Modul.*

b) Wenn $gr_F(E)$ *ein noetherscher* $gr_{\mathfrak{a}}(A)$*-Modul ist, so ist* E *ein noetherscher* A*-Modul.*

Beweis: a) Man kann annehmen, daß $gr_F(E)$ von endlich vielen homogenen Elementen $\overline{x}_1,\dots,\overline{x}_r$ erzeugt ist (Beweis von 5.4), also $\overline{x}_i \in E_{n(i)}/E_{n(i)+1}$. Sei $x_i \in E_{n(i)}$ ein Repräsentant von $\overline{x}_i$.
Für $1 \le i \le r$ definieren wir auf dem A-Modul A folgende Filtrierung
$\Phi^i\colon A = A_0 = \dots = A_{n(i)} \supset A_{n(i)+1} = \mathfrak{a} \supset A_{n(i)+2} = \mathfrak{a}^2 \supset \dots$.
(Anders ausgedrückt:

$$\Phi^i = (A_n)_{n\in\mathbb{N}} \text{ mit } A_n = \begin{cases} A & \text{für } 0 \le n \le n(i) \\ \mathfrak{a}^{n-n(i)} & \text{für } n \ge n(i) \end{cases} \quad .)$$

Indem wir den i-ten Faktor von A^r mit der Filtrierung Φ^i versehen, erhalten wir auf A^r eine i.w. $\mathfrak{a}$-adische Filtrierung
$\Phi\colon A^r = (A^r)_0 \supset (A^r)_1 \supset \dots$. Die A-lineare Abbildung $f\colon A^r \longrightarrow M$, definiert durch $e_i \longmapsto x_i$ (wo $e_1,\dots,e_r$ die kanonische Basis von A^r ist), hat die Eigenschaften:

1) $f((A^r)_n) \subset E_n$,

2) $gr(f)\colon gr_\Phi(A^r) \longrightarrow gr_F(E)$ ist surjektiv.

Da A^r bzgl. der $\mathfrak{a}$-adischen Filtrierung, also auch bzgl. der zu dieser äquivalenten Filtrierung Φ komplett ist, folgt a) mit 18.28b).

b) Sei E' ein Untermodul von E. Die Filtrierung F', definiert durch $E'_n := E' \cap E_n$, ist $\mathfrak{a}$-zulässig. Offenbar sind die von der Inklusion $E' \hookrightarrow E$ induzierten Abbildung $E'_n/E'_{n+1} \longrightarrow E_n/E_{n+1}$ injektiv. Also läßt sich $gr_{F'}(E')$ als Untermodul des noetherschen $gr_{\mathfrak{a}}(A)$-Moduls $gr_F(E)$ auffassen, ist mithin endlich. Deshalb ist E' nach a) ein endlicher A-Modul. —

Folgerung 18.30 *Sei A ein noetherscher Ring, $\mathfrak{a} \subset A$ ein Ideal. Dann ist die $\mathfrak{a}$-adische Komplettierung $\hat{A}$ ebenfalls noethersch.*

Beweis: Nach 18.25 ist $\hat{A}$ $\hat{\mathfrak{a}}$-adisch komplett, und $gr_{\hat{\mathfrak{a}}}(\hat{A}) \simeq gr_{\mathfrak{a}}(A)$. Da $gr_{\mathfrak{a}}(A)$ nach 5.3 noethersch ist, folgt die Behauptung aus 18.29 b). —

4. Formale Potenzreihenringe

Definition 18.31 Sei A ein Ring. Unter dem formalen Potenzreihenring $A[[X_1,\ldots,X_n]]$ in n Unbestimmten über A versteht man den Ring der formalen unendlichen Summen (Potenzreihen)

$$\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1 \ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$$

(wobei im Unterschied zum Polynomring nicht gefordert wird, daß nur endlich viele Koeffizienten von 0 verschieden sind, und auch keinerlei Konvergenz verlangt wird - deshalb "formal".) Formal gesehen ist obige formale Potenzreihe einfach die Abbildung $\mathbb{N}^n \longrightarrow A$, $(i_1,\ldots,i_n) \longmapsto a_{i_1 \ldots i_n}$. Jede Abbildung $\mathbb{N}^n \longrightarrow A$ entspricht einer formalen Potenzreihe. Die Summe zweier formaler Potenzreihen wird auf naheliegendste Weise gebildet, das Produkt wie bei Polynomen oder konvergenten Potenzreihen:

$$\Big(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1 \ldots i_n} X_1^{i_1}\cdot\ldots\cdot X_n^{i_n}\Big)$$

$$\cdot \Big(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} b_{i_1 \ldots i_n} X_1^{i_1}\cdot\ldots\cdot X_n^{i_n}\Big)$$

$$= \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \Big(\sum_{\substack{(i_1,\ldots,i_n)\in\mathbb{N}^n \\ (j_1,\ldots,j_n)\in\mathbb{N}^n \\ \forall r:\ i_r+j_r=k_r}} a_{i_1 \ldots i_n} b_{j_1 \ldots j_n}\Big) X_1^{k_1}\cdot\ldots\cdot X_n^{k_n} ,$$

wobei die innere Summe eine ("nicht formale") endliche Summe in A ist.

$A[\![X_1,\ldots,X_n]\!]$ ist eine A-Algebra.

Man hat einen kanonischen Isomorphismus $A[\![X_1,\ldots,X_{n-1}]\!][\![X_n]\!] \simeq A[\![X_1,\ldots,X_n]\!]$.

Satz 18.32 *$A[\![X_1,\ldots,X_n]\!]$ ist die $(X_1,\ldots,X_n)$-adische Komplettierung des Polynomringes $A[X_1,\ldots,X_n]$. Insbesondere ist $A[\![X_1,\ldots,X_n]\!]$ noethersch, wenn A es ist.*

Beweis: Sei $B := A[X_1,\ldots,X_n]$, $I := (X_1,\ldots,X_n) = BX_1 + \ldots + BX_n$. Die Polynome vom Grade $< r$ bilden ein vollständiges Repräsentantensystem für B/I^r.

Der kanonischen Projektion $\pi_{r+1}: B/I^{r+1} \longrightarrow B/I^r$ entspricht bei den obengenannten Repräsentanten das "Weglassen" der Monome vom Grade r. Mit anderen Worten: Sei $F \in B/I^{r+1}$ repräsentiert durch das Polynom $f_0 + \ldots + f_{r-1} + f_r$, wo f_i homogen vom Grade i ist; dann wird $\pi_{r+1}(F)$ von $f_0 + \ldots + f_{r-1}$ repräsentiert. Ein Element aus $\varprojlim_r B/I^r$ wird also repräsentiert durch eine Folge der Form $(f_0, f_0+f_1, f_0+f_1+f_2, \ldots)$, wo f_i homogen vom Grade i ist. Dieser Folge entspricht die formale Potenzreihe $\sum_{r=0}^{\infty} f_r$. Man bekommt so eine offenbar bijektive Abbildung $f: \varprojlim_r B/I^r \longrightarrow A[\![X_1,\ldots,X_n]\!]$. Man prüft leicht nach, daß f ein Ringhomomorphismus ist.

Wenn A noethersch ist, ist dies auch $A[X_1,\ldots,X_n]$, also nach 18.30 auch $A[\![X_1,\ldots,X_n]\!]$. –

Satz 18.33 *Seien $f: A \longrightarrow B$ ein Ringhomomorphismus, $\mathfrak{b} \subset B$ ein Ideal, derart daß B $\mathfrak{b}$-adisch komplett ist. Zu jedem n-Tupel $b_1,\ldots,b_n$ mit $b_i \in \mathfrak{b}$ gibt es dann genau einen Ringhomomorphismus $F: A[\![X_1,\ldots,X_n]\!] \longrightarrow B$, der f fortsetzt und $F(X_i) = b_i$ erfüllt.*

Beweis: Sei $P \in A[\![X_1,\ldots,X_n]\!]$, $P = \Sigma\, a_{i_1 \ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$. Man kann $F(P) := \Sigma\, f(a_{i_1 \ldots i_n}) b_1^{i_1} \cdot \ldots \cdot b_n^{i_n}$ definieren. Denn diese Reihe konvergiert offenbar wegen $b_i \in \mathfrak{b}$. –

(Eine andere Möglichkeit des Beweises ist: Setze zunächst f zu $\overline{f}: A[X_1,\ldots,X_n] \longrightarrow B$ mit $\overline{f}(X_i) = b_i$ wie üblich fort. Für das Ideal $I = (X_1,\ldots,X_n)$ gilt dann $\overline{f}(I) \subset \mathfrak{b}$. Wende 18.7 an.)

Satz 18.34 *a) Sei A ein lokaler noetherscher Ring mit maximalem Ideal* $\mathfrak{m}$. *Dann ist auch* $A[\![X_1,\dots,X_n]\!]$ *lokal und noethersch und hat die Dimension* $n + \dim A$. *Sein maximales Ideal besteht aus denjenigen Potenzreihen, deren konstantes Glied in* $\mathfrak{m}$ *liegt.*

b) Wenn ferner A regulär (bzw. ein Cohen-Macaulay-Ring) ist, so ist auch $A[\![X_1,\dots,X_n]\!]$ *regulär (bzw. ein Cohen-Macaulay-Ring).*

Beweis: a) Nach 18.32 ist $A[\![X_1,\dots,X_n]\!]$ noethersch.

Da $(X_1,\dots,X_n) \subset \operatorname{Jac}(A[\![X_1,\dots,X_n]\!])$ nach 18.25 gilt, ist $\operatorname{Jac}(A[\![X_1,\dots,X_n]\!])$ das Urbild von $\mathfrak{m} = \operatorname{Jac} A$ bei der kanonischen Projektion

$$A[\![X_1,\dots,X_n]\!] \longrightarrow A[\![X_1,\dots,X_n]\!] / (X_1,\dots,X_n) \simeq A .$$

Also ist $A[\![X_1,\dots,X_n]\!]$ lokal, und sein maximales Ideal hat die behauptete Gestalt.

Da $X_1,\dots,X_n$ eine $A[\![X_1,\dots,X_n]\!]$-reguläre Folge ist, folgt die Behauptung über die Dimension aus 14.18a).

b) Sei $\dim A = r$ und $y_1,\dots,y_r$ ein reguläres Parametersystem von A (bzw. eine A-reguläre Folge in $\mathfrak{m}$). Dann ist $X_1,\dots,X_n,y_1,\dots,y_r$ ein reguläres Parametersystem von $A[\![X_1,\dots,X_n]\!]$ (bzw. eine $A[\![X_1,\dots,X_n]\!]$-reguläre Folge der Länge $\dim A[\![X_1,\dots,X_n]\!]$ in $\operatorname{Jac}(A[\![X_1,\dots,X_n]\!])$). —

5. Komplette lokale Ringe

Definition 18.35 Unter der Komplettierung eines (semi-) lokalen Ringes A verstehen wir die Jac(A)-adische Komplettierung von A. Sie wird mit $\hat{A}$ bezeichnet.

Ein (semi-) lokaler Ring A heißt komplett, wenn er Jac(A)-adisch komplett ist.

Satz 18.36 *Seien A ein Ring,* $\mathfrak{m}_1,\dots,\mathfrak{m}_r$ *endlich viele paarweise verschiedene maximale Ideale,* $\mathfrak{J} := \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$ *und* $\hat{A}$ *die* $\mathfrak{J}$*-adische Komplettierung von A. Dann hat man eine kanonische Isomorphie*

$$\hat{A} \xrightarrow{\sim} \prod_{i=1}^{r} (A_{\mathfrak{m}_i})^{\wedge} .$$

Insbesondere ist ein kompletter semilokaler Ring ein direktes Produkt kompletter lokaler Ringe.

Beweis: Für $i \neq j$ und alle $n \geq 0$ sind $\mathfrak{m}_i^n$ und $\mathfrak{m}_j^n$ coprim gemäß 1.4. Nach dem Chinesischen Restsatz (1.9) hat man Isomorphismen

$$\phi: A/\mathfrak{J}^n \xrightarrow{\sim} \prod_{i=1}^{r} A/\mathfrak{m}_i^n .$$

Ferner kommutieren folgende Diagramme:

$$\begin{array}{ccc} A/\mathfrak{J}^{n+1} & \xrightarrow[\phi]{\sim} & \prod_{i=1}^{r} A/\mathfrak{m}_i^{n+1} \\ \Big\downarrow \kappa & & \Big\downarrow \prod_{i=1}^{r} \kappa_i \\ A/\mathfrak{J}^n & \xrightarrow[\phi]{\sim} & \prod_{i=1}^{r} A/\mathfrak{m}_i^n \end{array} ,$$

wobei $\kappa: A/\mathfrak{J}^{n+1} \longrightarrow A/\mathfrak{J}^n$ und $\kappa_i: A/\mathfrak{m}_i^{n+1} \longrightarrow A/\mathfrak{m}_i^n$ die kanonischen Projektionen sind.

Man erkennt $\varprojlim_n (A/\mathfrak{J}^n) \simeq \prod_{i=1}^{r} \varprojlim_n (A/\mathfrak{m}_i^n)$. —

Folgerung 18.37 *Sei A ein kompletter lokaler Ring mit dem maximalen Ideal $\mathfrak{m}$ und B eine A-Algebra, die als A-Modul von endlicher Darstellung ist. Dann ist B das direkte Produkt der Lokalisierungen nach seinen endlich vielen maximalen Idealen.*

Beweis: Nach 18.21 ist B als A-Modul $\mathfrak{m}$-adisch komplett, also auch $\mathfrak{m}B$-adisch komplett. $(\mathfrak{m}^nB = (\mathfrak{m}B)^n\,!)$

Insbesondere ist $\mathfrak{m}B \subset \mathrm{Jac}(B)$ (was auch aus 7.20 folgt). Andererseits ist $B/\mathfrak{m}B$ endlich über dem Körper $A/\mathfrak{m}$, also von endlicher Länge als A-Modul, erst recht als B-Modul. Folglich ist B semilokal, und es gibt ein r mit $(\mathrm{Jac}\, B)^r \subset \mathfrak{m}B$. Zusammen mit $\mathfrak{m}B \subset \mathrm{Jac}\, B$ sieht man, daß die $\mathfrak{m}$-adische und die $\mathrm{Jac}(B)$-adische Filtrierung auf B äquivalent sind.

B ist also $\mathrm{Jac}(B)$-adisch komplett, nach 18.36 also Produkt endlich vieler lokaler Algebren. —

Wir wollen aus 18.37 das Henselsche Lemma ableiten und benötigen dazu einige Hilfssätze, die auch für sich interessant sind:

Lemma 18.38 *Seien* $A \neq 0$ *ein Ring,* M *ein* A*-Modul,* $n,m \in \mathbb{N}$.

a) Aus $M \oplus A^n \simeq A^n$ *folgt* $M = 0$.

b) Aus $A^n \simeq A^m$ *folgt* $n = m$.

Beweis: a) Die Verkettung der Homomorphismen $A^n \xrightarrow{\sim} M \oplus A^n \xrightarrow{pr_1} M$ ist surjektiv; also ist M endlich erzeugt.

Sei $\mathfrak{m}$ ein maximales Ideal. Es gilt $M/\mathfrak{m}M \oplus (A/\mathfrak{m})^n \simeq (A/\mathfrak{m})^n$ über dem Körper $A/\mathfrak{m}$, also $M/\mathfrak{m}M = 0$. Dann ist auch $M_\mathfrak{m}/\mathfrak{m}M_\mathfrak{m} = 0$, also $M_\mathfrak{m} = 0$ nach Nakayama.

Mit 3.44 folgt $M = 0$.

b) folgt unmittelbar aus a). (Vgl. 3.A2.) –

Man nennt n den Rang des freien Moduls A^n.

Lemma 18.39 *Sei* A $(\neq 0)$ *ein Ring,* $f \in A[X]$ *ein unitäres Polynom (d.h. ein solches, dessen höchster Koeffizient* 1 *ist) vom Grade* n.

Dann ist $A[X]/(f)$ *als* A*-Modul frei vom Rang* n.

Beweis: Sei $\alpha \in B := A[X]/(f)$ die Restklasse von X.
Wir zeigen, daß $1,\alpha,\ldots,\alpha^{n-1}$ eine Basis von B über A ist.

Für $a_0,\ldots,a_{n-1} \in A$ gelte $\sum_{i=0}^{n-1} a_i\alpha^i = 0$. Dann ist $g := \sum_{i=0}^{n-1} a_iX^i$ ein Vielfaches von f. Da f unitär vom Grade $n > n-1$ ist, folgt $a_i = 0$ für $i = 0,\ldots,n-1$. Somit ist das n-Tupel $1,\alpha,\ldots,\alpha^{n-1}$ linear unabhängig.

Andererseits zeigt man $B = A + A\alpha + \ldots + A\alpha^{n-1}$ wie im Beweis von 7.2 (ii) $\Rightarrow$ (i). –

Eine Umkehrung obigen Lemmas ist

Satz 18.40 *Seien* A *ein Ring,* B *eine von einem Element* $\alpha \in B$ *erzeugte* A*-Algebra, die als* A*-Modul frei vom Rang* $n < \infty$ *ist.*

Dann gibt es genau ein unitäres Polynom $f \in A[X]$, *welches den Kern des durch* $X \longrightarrow \alpha$ *definierten* A*-Algebrenhomomorphismus* $\varphi: A[X] \longrightarrow B$ *erzeugt. Es ist* $\operatorname{grad} f = n$. *Wenn* $\mathfrak{m}$ *ein maximales Ideal in* A, $\overline{\alpha}$ *die Restklasse von* α *in* $B/\mathfrak{m}B$ *und* $\overline{f}$ *die von* f *in* $(A/\mathfrak{m})[X]$ *ist, so ist* $\overline{f} = \mathrm{Mipo}(\overline{\alpha},A/\mathfrak{m})$.

Beweis: Wir zeigen, daß $1,\alpha,\ldots,\alpha^{n-1}$ eine Basis des A-Moduls B, d.h. daß die durch $e_i \longmapsto \alpha^{i-1}$ definierte A-lineare Abbildung $h: A^n \longrightarrow B$ ein Isomorphismus ist. Wegen 3.45 genügt es, dies "lokal" zu zeigen.

Sei $\mathfrak{m} \subset A$ ein maximales Ideal, $\overline{\alpha}$ die Restklasse von α in $B/\mathfrak{m}B$, $g := \mathrm{Mipo}(\overline{\alpha}, A/\mathfrak{m})$ und $r = \mathrm{grad}\ g$. Dann ist $B/\mathfrak{m}B \simeq (A/\mathfrak{m})[X]/(g)$, also $1,\overline{\alpha},\ldots,\overline{\alpha}^{r-1}$ eine Vektorraumbasis von $B/\mathfrak{m}B$ über $A/\mathfrak{m}$.

Andererseits ist $B/\mathfrak{m}B \simeq (A/\mathfrak{m})^n$ als A-Modul. Es folgt $r = n$, d.h. $1,\overline{\alpha},\ldots,\overline{\alpha}^{n-1}$ ist eine Basis von $B/\mathfrak{m}B$ über $A/\mathfrak{m}$. Dann ist aber $1,\frac{\alpha}{1},\ldots,\frac{\alpha^{n-1}}{1}$ nach 12.1 eine Basis von $B_\mathfrak{m}$ über $A_\mathfrak{m}$, also $h_\mathfrak{m}$ ein Isomorphismus.

Da dies für alle maximalen Ideale $\mathfrak{m}$ von A gilt, ist h ein Isomorphismus nach 3.45.

Wir haben also eine Darstellung $\alpha^n = \sum\limits_{i=0}^{n-1} a_i\alpha^i$ mit $a_i \in A$. Folglich ist $f := X^n - \sum\limits_{i=0}^{n-1} a_iX^i \in \mathrm{Ker}\ \varphi$.

f ist unitär und hat den Grad n.

Wir erhalten einen surjektiven A-Algebrenhomomorphismus $\varphi': A[X]/(f) \longrightarrow B$. Als A-Moduln sind aber sowohl B (nach Voraussetzung) als auch $A[X]/(f)$ isomorph zu A^n.

Da A^n projektiv ist, hat man die A-Modulisomorphie $\mathrm{Ker}\ \varphi' \oplus A^n \simeq A^n$. Nach 18.38 ist $\mathrm{Ker}\ \varphi' = 0$, d.h. $\mathrm{Ker}\ \varphi$ von f erzeugt.

Wir überlassen es dem Leser, zu beweisen, daß unitäre Polynome $g,h \in A[X]$ nur dann dasselbe Ideal erzeugen, wenn $g = h$ ist.
Für ein maximales Ideal $\mathfrak{m}$ von A gilt nun $\overline{f}(\overline{\alpha}) = 0$. Da $\overline{f}$ unitär vom Grade n ist und $1,\overline{\alpha},\ldots,\overline{\alpha}^{n-1}$ über $A/\mathfrak{m}$ linear unabhängig sind, ist $\overline{f}$ das Minimalpolynom von $\overline{\alpha}$ über $A/\mathfrak{m}$. –

Lemma 18.41 *Seien* k *ein Körper und* $f = g_1^{n_1}\cdot\ldots\cdot g_r^{n_r}$ *die Primfaktorzerlegung eines Polynoms* $f \in k[X]-k$ *mit (irreduziblen) paarweise nicht-assoziierten* g_i. *Dann ist*

$$k[X]/(f) \simeq \prod_{i=1}^{r} k[X]/(g_i^{n_i}) ,$$

und jeder Faktor $k[X]/(g_i^{n_i})$ *ist ein lokaler Ring von endlicher Länge.*

Beweis: Aus dem Chinesischen Restsatz (1.9) folgt die Zerlegung.

Der Ring $k[X]/(g_i^{n_i})$ ist von endlicher Länge, da er ein endlich-dimensionaler k-Vektorraum ist.

Da $g_i^{n_i}$ in nur einem maximalen Ideal von $k[X]$, nämlich in (g_i) liegt, ist $k[X]/(g_i^{n_i})$ lokal. –

Satz 18.42 (Lemma von Hensel) *Sei A ein kompletter lokaler Ring, $\mathfrak{m}$ sein maximales Ideal, $k = A/\mathfrak{m}$ und $\pi\colon A[X] \longrightarrow k[X]$ die kanonische Projektion des Polynomringes über A auf den über k. Ferner sei $f \in A[X]$ ein unitäres Polynom und*

$\pi(f) = g_1^{n_1}\cdot\ldots\cdot g_r^{n_r}$ die Primfaktorzerlegung von $\pi(f)$ über k mit paarweise verschiedenen unitären (irreduziblen) g_i.

Dann gibt es eindeutig bestimmte unitäre $G_1,\ldots,G_r \in A[X]$ mit $\pi(G_i) = g_i^{n_i}$ und $f = G_1\cdot\ldots\cdot G_r$.

Beweis: Sei $B = A[X]/(f)$. Nach 18.37 ist B ein endliches direktes Produkt lokaler A-Algebren.

Wegen $\mathfrak{m}B \subset \mathrm{Jac}(B)$ entsprechen die maximalen Ideale von B denen von $B/\mathfrak{m}B \simeq k[X]/(\pi(f)) \simeq \prod_{i=1}^{r} k[X]/(g_i^{n_i})$.

Sei B_i der zu $k[X]/(g_i^{n_i})$ gehörende direkte Faktor von B und $\kappa_i\colon B \longrightarrow B_i$ die kanonische Projektion.

Sei α die Restklasse von X in B. Dann ist B_i von $\kappa_i(\alpha)$ erzeugt. Ferner ist B_i als direkter Summand des freien A-Moduls B projektiv, also frei nach 11.12. Und zwar ist sein Rang gleich $\mu_k(B_i/\mathfrak{m}B_i)$ $= \mu_k(k[X]/(g_i^{n_i})) = \operatorname{grad} g_i^{n_i}$.

Der Kern des Homomorphismus $A[X] \longrightarrow B_i$, $X \longmapsto \kappa_i(\alpha)$ wird nach 18.40 von einem unitären Polynom G_i erzeugt, für welches $\pi(G_i) = g_i^{n_i}$ gilt. Das Produkt $G_1\cdot\ldots\cdot G_r$ ist deshalb im Kern von $A[X] \longrightarrow B = \prod_{i=1}^{r} B_i$ enthalten, d.h. $f \mid G_1\cdot\ldots\cdot G_r$. Da aber $\operatorname{grad} f = \operatorname{grad}(G_1\cdot\ldots\cdot G_r)$ und f, $G_1\cdot\ldots\cdot G_r$ unitär sind, folgt $f = G_1\cdot\ldots\cdot G_r$. –

Folgerung 18.43 *Seien $A,\mathfrak{m},f,\overline{f}$ wie oben. Wenn $\overline{f}$ in $A/\mathfrak{m}$ eine einfache Nullstelle $\overline{\xi}$ hat, so gibt es einen Repräsentanten $\xi \in A$ von $\overline{\xi}$ mit $f(\xi) = 0$.*

Beweis: $X - \overline{\xi}$ ist dann nämlich ein "einfacher" Primfaktor von $\overline{f}$; d.h. $X-\overline{\xi} \mid \overline{f}$, aber $(X-\overline{\xi})^2 \nmid \overline{f}$. —

Satz 18.44 *Für einen lokalen noetherschen Ring* A *gilt:*

a) $\dim A = \dim \hat{A}$.

b) A *ist regulär* $\Longleftrightarrow$ $\hat{A}$ *ist regulär.*

Beweis: a) Sei $\mathfrak{m} = \mathrm{Jac}(A)$. Nach 18.25 ist $A/\mathfrak{m}^n \simeq \hat{A}/\hat{\mathfrak{m}}^n$, insbesondere $l_A(A/\mathfrak{m}^n) = l_{A/\mathfrak{m}^n}(A/\mathfrak{m}^n) = l_{\hat{A}/\hat{\mathfrak{m}}^n}(\hat{A}/\hat{\mathfrak{m}}^n) = l_{\hat{A}}(\hat{A}/\hat{\mathfrak{m}}^n)$. Nun ist $l_A(A/\mathfrak{m}^n)$ bzw. $l_{\hat{A}}(\hat{A}/\hat{\mathfrak{m}}^n)$ für große n ein Polynom in n, dessen Grad die Dimension von A bzw. $\hat{A}$ ist (6.9).

b) A ist gemäß 14.6 regulär genau dann, wenn $gr_{\mathfrak{m}}(A)$ ein Polynomring in einer Basis von $\mathfrak{m}/\mathfrak{m}^2$ ist. Beachte nun: $gr_{\mathfrak{m}}(A) \simeq gr_{\hat{\mathfrak{m}}}(\hat{A})$. —

Folgerung 18.45 *Sei* A *ein Hauptidealring und* $p \in A$ *ein Primelement. Dann ist die* (p)*-adische Komplettierung von* A *ein diskreter Bewertungsring.*

Sie ist nämlich nach 18.26 isomorph zur $pA_{(p)}$-adischen Komplettierung von $A_{(p)}$ also regulär, lokal und von der Dimension 1. —

Beispiel 18.46 Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist die Komplettierung $\hat{\mathbb{Z}}_{(p)}$ von $\mathbb{Z}_{(p)}$ gleich der (p)-adischen Komplettierung von $\mathbb{Z}$ und ein diskreter Bewertungsring. $\hat{\mathbb{Z}}_{(p)}$ ist der Ring der sogenannten ganzen p-adischen Zahlen. Er wird auch mit $\hat{\mathbb{Z}}_p$ oder $\mathbb{Z}_p$ bezeichnet. (Vorsicht: Letzteres Symbol wird auch oft für den Körper $\mathbb{Z}/(p)$ benutzt. Ferner müßte es eigentlich im Einklang mit unserer Definition von A_S in 9.A2 als $\mathbb{Z}[\frac{1}{p}]$ verstanden werden.)

Aufgrund des Henselschen Lemmas existieren in $\hat{\mathbb{Z}}_p$ viele algebraische, nichtrationale Zahlen, z.B. die $(p-1)$-ten Einheitswurzeln. Da es für $m \geq 1$ nach Dirichlets Satz über Primzahlen in arithmetischen Progressionen ([Serre A] Chap. VI) unendlich viele Primzahlen $p \equiv 1 \pmod m$ gibt, existieren in unendlich vielen $\hat{\mathbb{Z}}_p$ die m-ten Einheitswurzeln.
(Der Leser möge sich überlegen, in welchem $\hat{\mathbb{Z}}_p$ die Zahl $\sqrt{2}$ existiert. Vgl. loc.cit. Chap. I, Thm. 5 iii): Ergänzungssatz zum quadratischen Reziprozitätsgesetz. In demselben Buch: Chap.II,III findet der Leser weiteres zum Nutzen der p-adischen Zahlen.)

Mit $\mathbb{Q}_p$ wird der Quotientenkörper von $\hat{\mathbb{Z}}_p$ bezeichnet. Es ist
$\mathbb{Q}_p = \hat{\mathbb{Z}}_p[\frac{1}{p}] \simeq \hat{\mathbb{Z}}_p \otimes_{\mathbb{Z}} \mathbb{Q}$.
$\mathbb{Q}_p$ ist für kein p algebraisch abgeschlossen: $\sqrt{p} \notin \mathbb{Q}_p$. Mit diesem Argument sieht man, daß kein algebraisch abgeschlossener Körper eine nichttriviale diskrete Bewertung besitzt.
Da $\mathbb{C}$ algebraisch abgeschlossen und von gleicher Mächtigkeit (und von gleicher Charakteristik) wie $\mathbb{Q}_p$ ist, kann man $\mathbb{Q}_p$ in $\mathbb{C}$ einbetten - auf allerdings nicht kanonische Weise (Beweis?).

6. Koeffizientenringe

Definition 18.47 Sei A ein Ring. Die Charakteristik char A von A ist diejenige natürliche Zahl, die den Kern des (eindeutig bestimmten) Ringhomomorphismus $\mathbb{Z} \longrightarrow A$ erzeugt.

(N.B.: Diese Definition ist verschieden von der Bourbakis!)

Bemerkung: Für $m \geq 0$ ist $\operatorname{char}(\mathbb{Z}/m\mathbb{Z}) = m$. Also kommt jede natürliche Zahl als Charakteristik vor. Falls A integer ist, ist
$\operatorname{char} A = \operatorname{char} Q(A)$, also 0 oder eine Primzahl.

Bemerkungen 18.48 Sei A ein lokaler Ring, $\mathfrak{m}$ sein maximales Ideal, $k = A/\mathfrak{m}$.

a) Sei $\operatorname{char} k = 0$.

Dann ist $\operatorname{char} A = 0$.

Da nämlich die Verkettung

$$\mathbb{Z} \longrightarrow A \xrightarrow{\text{kan.}} k$$

injektiv ist, gilt dies erst recht für den Homomorphismus $\mathbb{Z} \longrightarrow A$.

Ferner läßt sich die Einbettung $\mathbb{Z} \hookrightarrow A$ zu einer Einbettung $\mathbb{Q} \hookrightarrow A$ fortsetzen.
Denn für $n \in \mathbb{Z} - \{0\}$ gilt: $n \cdot 1_A \notin \mathfrak{m}$. (Hier bezeichne 1_A das Eins-Element von A .) Also ist $n \cdot 1_A \in A^*$.

b) Sei $\operatorname{char} k = p > 0$.
Dann ist $\operatorname{char} A = p^n$ mit einem $n \in \mathbb{N}_1$ oder $\operatorname{char} A = 0$.

Beweis: Sei $r = \operatorname{char} A$. Die Homomorphismen $\mathbb{Z} \longrightarrow A \longrightarrow k$ induzieren surjektive Homomorphismen $\mathbb{Z} \longrightarrow \mathbb{Z}/(r) \longrightarrow \mathbb{Z}/(p)$. Es folgt $p \mid r$.

Sei $r = p^n \cdot s$ mit $p \nmid s$. Dann ist $s \cdot 1_A \notin \mathfrak{m}$, also $s \cdot 1_A \in A^*$.
Sei $a = (s \cdot 1_A)^{-1} \in A$. Dann ist $0 = ((p^n \cdot s)1_A)a = p^n(s \cdot 1_A)a = p^n \cdot 1_A$, also $p^n = \operatorname{char} A$.

c) Wenn $\operatorname{char} k = \operatorname{char} A = p > 0$ ist, besitzt A einen zu $\mathbb{Z}/(p)$ isomorphen Teilkörper.

d) A besitzt genau dann einen Teilkörper, wenn $\operatorname{char} k = \operatorname{char} A$ ist. In diesem Falle gibt es auch maximale Teilkörper, da die Menge aller Teilkörper eines Ringes induktiv geordnet ist.

Beispiele: $\mathbb{Q}[X]_{(X)}$, $\mathbb{Q}[\![X]\!]$; $\mathbb{Z}/p^n$; $\mathbb{Z}_{(p)}$, $\hat{\mathbb{Z}}_p$; $(\mathbb{Z}/(p)[\![X]\!]$.

Wir wollen zur Vorbereitung auf die Cohenschen Struktursätze folgendes zeigen: Sei A lokal, komplett mit maximalem Ideal $\mathfrak{m}$ und $k := A/\mathfrak{m}$, dann gibt es in A einen Unterring R einfacher Bauart (der im Falle "$\operatorname{char} k = \operatorname{char} A$" ein Körper, im Falle $\operatorname{char} k = p > 0$ ein sogenannter p-Ring (18.55) ist), derart daß R bei der kanonischen Projektion $A \longrightarrow k$ surjektiv auf k abgebildet wird, d.h. $R + \mathfrak{m} = A$ gilt.

Wir unterscheiden dabei, ob $\operatorname{char} k = 0$ oder > 0 ist.

Theorem 18.49 *Sei A ein kompletter lokaler Ring mit maximalem Ideal $\mathfrak{m}$, $k = A/\mathfrak{m}$ und der kanonischen Projektion $\pi\colon A \longrightarrow k$. Ferner sei $\operatorname{char} k = 0$.*
Für jeden maximalen Teilkörper K von A gilt dann $A = K \oplus \mathfrak{m}$ und - äquivalent dazu - $\pi(K) = k$.

Beweis: Da $\pi|_K\colon K \longrightarrow k$ injektiv ist, ergibt sich die Äquivalenz der beiden Behauptungen aus 3.17.

Angenommen, $\pi(K) \neq k$. Sei $y \in k - \pi(K)$. Wir unterscheiden 2 Fälle:

Fall 1: y ist transzendent über $\pi(K)$.

Wähle ein beliebiges Urbild $t \in \pi^{-1}(y)$. Für jedes von 0 verschiedene Polynom $f \in K[X]$ gilt dann $\pi(f(t)) \neq 0$, da t transzendent über $\pi(K)$ ist. Also ist $f(t) \in A^*$ für $f \neq 0$. Man erhält also mit $K(t)$ einen echt größeren Teilkörper als K in A; Widerspruch!

Fall 2: y ist algebraisch über $\pi(K)$.
Da $\operatorname{char} k = 0$ ist, ist y separabel über $\pi(K)$. Sei $f \in K[X]$ das unitäre Polynom, welches bei dem durch π induzierten Isomorphismus $K[X] \longrightarrow \pi(K)[X]$ zum Minimalpolynom von y über $\pi(K)$ wird.

Da y aus Separabilitätsgründen eine einfache Nullstelle seines Minimalpolynoms ist, gibt es nach Folgerung 18.42 zum Henselschen Lemma ein $x \in \pi^{-1}(y)$ mit $f(x) = 0$.

Der Unterring $K[x]$ von A ist also isomorph einem Restklassenring des Körpers $K[X]/(f)$, also zu letzterem Körper isomorph. Somit ist $k[x]$ ein echt größerer Teilkörper von A als K. Widerspruch! —

Der Fall "$\operatorname{char} k = p > 0$" erfordert einige Vorbereitungen.

Es sei jedoch darauf verwiesen, daß die Dinge sich sehr vereinfachen, wenn man zusätzlich $\operatorname{char} A = p$ voraussetzt. In diesem Falle kann man auf 18.55 bis 18.60 verzichten. Auch der Beweis von 18.62 wird dann kürzer. Siehe Bemerkung 18.63.

Im folgenden (bis 18.63) sei p *eine Primzahl. Für einen Ring* A *sei mit* A^{p^n} *hier die Menge* $\{a^{p^n} \mid a \in A\}$ *- und nicht der Modul der* p^n*-Tupel von Elementen von* A *- bezeichnet. (Entsprechend sind die Bezeichnungen* A^p, K^{p^n} *- für Körper* K *- etc. zu verstehen.)*

<u>Definition 18.50</u> Sei K ein Körper der Charakteristik p.

a) Eine Teilmenge $B \subset K$ heißt p-frei, wenn die Familie
$\tilde{B} := \left(\prod_{\alpha \in B} \alpha^{n_\alpha} \mid 0 \le n_\alpha < p,\ n_\alpha = 0 \text{ für fast alle } \alpha\right)$ linear unabhängig über K^p ist. (Die Indexmenge der o.a. Familie ist die Teilmenge derjenigen $(n_\alpha)_{\alpha\in B}$ von $\mathbb{N}^B$, die o.a. Bedingungen erfüllen.)

b) B heißt eine p-Basis, wenn $\tilde{B}$ eine Basis des K^p-Vektorraumes K ist.

<u>Bemerkung 18.51</u> Wenn K wie oben und $B \subset K$ eine Teilmenge ist, dann ist der Körper $K^p(B)$ von B als K^p-Vektorraum erzeugt. Wenn also B p-frei ist, ist $\tilde{B}$ eine K^p-Vektorraumbasis von $K^p(B)$ über K^p.

Satz 18.52 *Jeder Körper* K *der Charakteristik* p *besitzt eine* p-*Basis*.

(N.B.: Wenn K vollkommen ist, ist $\emptyset$ die einzige p-Basis.)

Beweis: Sei $\mathfrak{M}$ die Menge der p-freien Teilmengen von K. Da $\emptyset \in \mathfrak{M}$, ist $\mathfrak{M} \neq \emptyset$. Durch die Inklusion ist $\mathfrak{M}$ induktiv geordnet. (Da eine Familie von Vektorraumelementen genau dann linear unabhängig ist, wenn dies für jede endliche Teilmenge gilt, sieht man sofort: Die Vereinigung der Elemente einer Kette in $\mathfrak{M}$ gehört zu $\mathfrak{M}$.)

Sei B maximal in $\mathfrak{M}$. Ist B keine p-Basis von K, so gibt es ein $\alpha \in K - K^p(B)$. Da $1, \alpha, \ldots, \alpha^{p-1}$ eine (Vektorraum-) Basis von $K^p(B \cup \{\alpha\})$ über $K^p(B)$ ist, folgt die p-Freiheit der Menge $B \cup \{\alpha\}$ sofort aus dem

Lemma 18.53 *Seien* $K \subset L \subset E$ *Körpererweiterungen,* $(\alpha_i)_{i\in I}$ *eine Vektorraumbasis von* L *über* K, $(\beta_j)_{j\in J}$ *eine solche von* E *über* L, *so ist die Familie* $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ *eine Vektorraumbasis von* E *über* K.

Dies beweist man wie in dem wohlbekannten Fall, daß I und J endliche Mengen sind. —

Satz 18.54 *Sei* B *eine* p-*Basis eines Körpers* K *der Charakteristik* p *und* $m \in \mathbb{N}$. *Dann ist die Familie*

$$\left(\prod_{\alpha\in B} \alpha^{n_\alpha} \mid 0 \le n_\alpha < p^m,\ n_\alpha = 0 \text{ für fast alle } \alpha \in B \right)$$

eine Vektorraumbasis von K *über* K^{p^m}

Beweis: Die Zuordnung $x \longmapsto x^{p^r}$ definiert einen Isomorphismus

$$K \longrightarrow K^{p^r} \quad ,$$

welche K^p auf $K^{p^{r+1}}$ abbildet. Deshalb ist $\left\{\alpha^{p^r} \mid \alpha \in B\right\}$ eine p-Basis von K^{p^r}. Der Satz folgt dann mit Hilfe (m-1)-facher Anwendung des Lemmas 18.53. —

Definition 18.55 Ein p-Ring ist ein Ring R, derart daß das Ideal pR maximal und R pR-adisch komplett ist.

Beispiele: Jeder Körper der Charakteristik p, $\mathbb{Z}/p^n$, $\hat{\mathbb{Z}}_p$.

Satz 18.56 *Sei* R *ein* p-*Ring.*

a) R *ist lokal und noethersch mit dem maximalen Ideal* pR.

b) Sei $p1_R$ *nilpotent, etwa* $p^n1_R = 0$, $p^{n-1}1_R \neq 0$. *Die Ideale von* R *sind dann von der Form* p^rR *mit* $0 \le r \le n$. *Sie sind paarweise verschieden. Insbesondere ist* $l_RR = n < \infty$ *und* char $R = p^n$.

c) Sei $p1_R$ *nicht nilpotent. Dann ist* R *ein diskreter Bewertungsring der Charakteristik* 0 *und* $p = p1_R$ *das (bis auf assoziierte) einzige Primelement von* R.

d) Jeder Restklassenring von R, *der nicht zum Nullring isomorph ist, ist ein* p-*Ring.*

Beweis: Wir können wie im Beweis von 18.25c) schließen, daß $1-(px)y$ für jedes $x \in R$ und jedes $y \in R$ invertierbar, d.h. $px \in \mathrm{Jac}\, R$ für alle $x \in R$ ist (1.23). Also ist pR das einzige maximale Ideal von R.

Sei $a \in R - (0)$. Da nach Voraussetzung $\bigcap_{i\in\mathbb{N}} p^iR = \bigcap_{i\in\mathbb{N}} (pR)^i = (0)$ ist, gibt es ein größtes $r \in \mathbb{N}$, so daß $a = p^rb$ mit einem $b \in R$ ist.

Wegen der Maximalität von r ist $b \notin pR$, also $b \in R^*$. Schreibe $v(a) = r$. Sei $\mathfrak{a} \neq (0)$ ein Ideal von R und $a \in \mathfrak{a} - (0)$ so gewählt, daß $r := v(a)$ minimal ist. Insbesondere gilt $p^rR \subset \mathfrak{a}$.

Für jedes $a' \in \mathfrak{a} - (0)$ gibt es dann ein $s \ge r$ und ein $u \in R^*$ mit $a' = p^s u \in p^rR$. Es folgt $\mathfrak{a} \subset p^rR$, also $\mathfrak{a} = p^rR$.

Insbesondere ist somit jedes Ideal von R ein Hauptideal.

a) ist bewiesen.
b) ist klar.

c) Seien $a,b \in R - (0)$, $a = p^ru$, $b = p^sv$ mit $u,v \in R^*$. Dann ist $ab = p^{r+s}uv \neq 0$, da $p\cdot 1_R$ nicht nilpotent ist.

Also ist R integer.

Nach Obigem ist R ein lokaler Hauptidealring, d.h. ein diskreter Bewertungsring.

Da $p^r1_R \neq 0$ ist für alle r, ist auch char $R \neq p^r$ für alle r. Mit 18.48b) folgt char $R = 0$.

d) Jeder Restklassenring $R' \neq 0$ ist lokal mit maximalem Ideal $(p1_{R'})$. Wenn $R' \neq R$ ist, muß $R' = R/p^mR$ für ein m sein. Also ist R' pR'-adisch komplett. —

Satz 18.57 *Sei* $f\colon R \longrightarrow R'$ *ein Homomorphismus von* p-*Ringen.*

a) *Es gilt* $f(p^m R) \subset p^m R'$ *für alle* m. *Insbesondere ist* $f(pR) \subset pR'$, *also* f *lokal.*

b) *Es gilt* $l_R R \geq l_{R'} R'$. *Und es ist* f *genau dann injektiv, wenn* $l_R R = l_{R'} R'$ *ist.*

c) *Genau dann ist* f *surjektiv, wenn* f *einen Isomorphismus der Restklassenkörper* $\overline{f}\colon R/pR \longrightarrow R'/pR'$ *induziert.*

d) *Für* $m \leq l_{R'} R'$ *ist* $f^{-1}(p^m R') = p^m R$.

Beweis: a) ist trivial.

b) Sei $l_R R = n < \infty$. Dann ist $p^n \cdot 1_R = 0$, also ist $p^n 1_{R'} = f(p^n 1_R) = 0$. Wenn f injektiv ist, folgt aus $p^n 1_{R'} = 0$, daß auch $p^n 1_R = 0$ ist. Dann ist also $l_R(R) \leq l_{R'}(R')$ nach 18.56b) und deshalb $l_R(R) = l_{R'}(R')$.

Sei umgekehrt $l_R(R) = l_{R'}(R')$. Von f wird ein injektiver Homomorphismus der Restklassenkörper $\overline{f}_0\colon R/pR \longrightarrow R'/pR'$ induziert.

Für $r \in \mathbb{N}$ hat man folgendes kommutative Diagramm:

$$\begin{tikzcd}
R/pR \arrow[r, "\overline{f}_0"] \arrow[d, "\alpha"'] & R'/pR' \arrow[d, "\alpha'"] \\
p^r R/p^{r+1} R \arrow[r, "\overline{f}_r"] & p^r R'/p^{r+1} R'
\end{tikzcd}$$

wo α und α' durch die Multiplikation mit p^r induziert werden.

Wenn $p^r R' \neq (0)$ ist, ist α' injektiv, also mit $\overline{f_0}$ auch $\overline{f_r}$ injektiv. Die Behauptung folgt also mit Hilfe von 18.28a).

c) Wenn f surjektiv ist, dann auch $\overline{f}$. Ein surjektiver Körperhomomorphismus ist aber bijektiv.
Umgekehrt, wenn $\overline{f}$ surjektiv ist, gilt dies auch für die induzierten R-Modulhomomorphismen

$$p^r R/p^{r+1} R \longrightarrow p^r R'/p^{r+1} R' \ .$$

Die Behauptung folgt aus 18.28b).

d) Wegen a) gilt $p^m R \subset f^{-1}(p^m R')$. Da $l_R(R/p^m R) = l_{R'}(R'/p^m R') = m$ ist, wird nach b) ein injektiver Homomorphismus $R/p^m R \hookrightarrow R'/p^m R'$ induziert, also kann $p^m R$ keine echte Teilmenge von $f^{-1}(p^m R')$ sein. —

Satz 18.58 *Sei* $(R_n,f_n)_{n\geq 1}$ *ein surjektives inverses System von* p-*Ringen. Dann ist* $\varprojlim_n R_n$ *ein* p-*Ring*.

Beweis: Sei $l_n = l_{R_n}(R_n)$. Es gilt $l_{n+1} \geq l_n$ nach 18.57b). Wenn es ein $N \in \mathbb{N}$ gibt mit $l_i = l_j$ für $i,j \geq N$, so sind die f_n für $n > N$ injektiv, also nach Voraussetzung Isomorphismen. Dann ist $\varprojlim_n R_n \simeq R_N$.

Es ist also nur noch der Fall $l_n < \infty$ und $\lim\limits_{n\to\infty} l_n = \infty$ zu betrachten.
$R := \varprojlim_n R_n$ ist ein Unterring des direkten Produktes $\prod\limits_n R_n$. Durch die Projektion auf den m-ten Faktor erhält man für jedes m einen Homomorphismus $\pi_m\colon R \longrightarrow R_m$.

Aus der Definition des inversen Limes sieht man, daß π_m surjektiv ist, wenn die f_n für $n > m$ es sind. Da nach Voraussetzung alle f_n surjektiv sind, gilt dies auch für alle π_m.

Setze $I_m := \operatorname{Ker} \pi_m$; $I_o := R$.

Nach 18.12 ist R komplett bezüglich der Filtrierung $(I_m)_{m\in\mathbb{N}}$. Vermittels π_m bzw. π_n ist $R/I_m \simeq R_m$ und
$I_m/I_n \simeq p^{l_m} R_n$ für $n \geq m$. Denn I_m/I_n wird durch π_n auf den Kern des Homomorphismus $R_n \longrightarrow R_m$ abgebildet, der durch Verkettung der f_i mit $m < i \leq n$ entsteht. Dieser ist $p^m R_n$ nach 18.57d). Es folgt:

$$(*)\qquad I_m/I_n = (I_n + p^{l_m}R)\,/\,I_n\,.$$

Behauptung: Für $m \in \mathbb{N}_1$ ist $I_m = p^{l_m}R$.

Da $p^{l_m}R_m = 0$, ist $p^{l_m}R \subset I_m$.

Sei $x \in I_m$. Nach (*) gibt es zu jedem $n \geq m$ ein $y_n \in I_n$ und ein $z_n \in R$ mit $x = y_n + p^{l_m}z_n$.

Die Folge $(z_n)_{n\geq m}$ ist eine Cauchy-Folge in R bzgl. der Filtrierung durch $(I_i)_{i\in\mathbb{N}}$. Sei nämlich $j \in \mathbb{N}$ gegeben und $N \in \mathbb{N}$ so groß, daß $l_N - l_m \geq j$ ist, so gilt für $r,s \geq N$:

$$p^{l_m}(z_r-z_s) = y_s - y_r \equiv 0 \pmod{I_N}.$$

Für die Restklassen $\bar{z}_r,\bar{z}_s$ modulo I_N ist also

$$\bar{z}_r-\bar{z}_s \in (p^{l_N-l_m}R)\,/\,I_N \subset I_j/I_N\,,\quad \text{d.h. } z_r-z_s \in I_j\,.$$

Da R komplett ist, konvergiert die Folge $(z_n)_{n\geq m}$ gegen ein $z \in R$ und es ist $p^{l_m}z = p^{l_m}\lim\limits_{n\to\infty} z_n = \lim\limits_{n\to\infty}(p^{l_m}z_n) = x$. Die Behauptung ist somit bewiesen.

Da die Folge der l_n monoton gegen ∞ geht, sind die beiden Filtrierungen $(p^nR)_{n\in\mathbb{N}}$ und $(p^{l_n}R)_{n\in\mathbb{N}}$ (mit $l_0 = 0$) von R äquivalent im Sinne von 18.1. Mithin ist R nach 18.4c) auch pR-adisch komplett.

Als letztes ist noch zu zeigen, daß pR ein maximales Ideal von R ist. Wegen $pR \supset p^{l_1}R = I_1$ gilt: $R/pR \simeq (R/I_1)\,/\,p(R/I_1) \simeq R_1/pR_1$. Letzteres ist nach Voraussetzung ein Körper. —

Definition 18.59 Sei A ein Ring. Definiere induktiv: $A(0) := A$,
$A(n) := A^{p^n} + p\cdot A(n-1) := \{a^{p^n} + pb \mid a \in A,\ b \in A(n-1)\}$.

Satz 18.60 *Für jedes* $n \in \mathbb{N}$ *ist* $A(n)$ *ein Unterring von* A*, und zwar der von allen Elementen der Form* $p^r\cdot a^{p^{n-r}}$ *mit* $a \in A$, $0 \leq r \leq n$ *erzeugte Unterring.*

Beweis: Induktion nach n, wobei der Fall $n = 0$ trivial ist.

Sei jetzt $n > 0$. Wegen $0 \in A(n-1)$ ist $0 \in A(n)$ und $1 \in A(n)$, ferner $-1 \in A(n)$ für $p \neq 2$. Für $p = 2$ gilt aber $-1 = 1^{2^n} + 2(-1)$, also $-1 \in A(n)$, da $-1 \in A(n-1)$.

Aus der Induktionsvoraussetzung folgt auch leicht die multiplikative Abgeschlossenheit von $A(n)$.
Zur additiven Abeschlossenheit: Sei $f \in \mathbb{Z}[X,Y]$ so definiert, daß $(X+Y)^p = X^p + p\cdot f(X,Y) + Y^p$ gilt.

Für $i = 1,2$ seien $a_i \in A$, $b_i \in A(n-1)$. Dann ist
$a_1^{p^n} + pb_1 + a_2^{p^n} + pb_2 = (a_1^{p^{n-1}} + a_2^{p^{n-1}})^p - p\cdot f(a_1^{p^{n-1}}, a_2^{p^{n-1}}) + p(b_1+b_2)$.

Da nach Induktionsvoraussetzung $b_1+b_2 - f(a_1^{p^{n-1}}, a_2^{p^{n-1}}) \in A(n-1)$ ist, muß nur noch $(a_1^{p^{n-1}} + a_2^{p^{n-1}})^p \in A^{p^n} + pA(n-1)$ gezeigt werden.

Nun ist $a_1^{p^{n-1}} + a_2^{p^{n-1}} \in A(n-1)$, also $a_1^{p^{n-1}} + a_2^{p^{n-1}} = c^{p^{n-1}} + pd$ mit gewissen $c \in A$, $d \in A(n-2)$ - wobei $A(-1) = \{0\}$ gesetzt werden darf.

Wir erhalten $(a_1^{p^{n-1}}+a_2^{p^{n-1}})^p = c^{p^n} + pf(c^{p^{n-1}},pd) + p^p d^p$.

Da $pA(n-2) \subset A(n-1)$ gilt, ist $pd \in A(n-1)$ und $p^{p-1}d^p \in A(n-1)$.

Weil auch noch $c^{p^{n-1}} \in A(n-1)$ ist, haben wir

$c^{p^n} + p(f(c^{p^{n-1}},pd) + p^{p-1}d^p) \in A^{p^n} + pA(n-1)$.

Die Behauptung über die Erzeugbarkeit folgt sofort aus der Induktionsvoraussetzung. —

Lemma 18.61 *Sei* $A = \mathfrak{j}_0 \supset \mathfrak{j}_1 \supset \ldots$ *ein filtrierter Ring mit* $p\,1_A \in \mathfrak{j}_1$ *und* $\mathfrak{j}_r\mathfrak{j}_s \subset \mathfrak{j}_{r+s}$. *Seien* $x,y \in A$ *und* $n,m \in \mathbb{N}$, *ferner* $x \equiv y \bmod \mathfrak{j}_m$. *Dann gilt:*

$$x^{p^n} \equiv y^{p^n} \bmod \mathfrak{j}_{m+n}.$$

Beweis: Es genügt, den Fall $n = 1$ zu behandeln.

Da $x^p - y^p = (x-y)\cdot\sum_{i=0}^{p-1} x^i y^{p-1-i}$ und $x-y \in \mathfrak{j}_m$ ist, muß nur noch $\sum_{i=0}^{p-1} x^i y^{p-1-i} \in \mathfrak{j}_1$ gezeigt werden. Modulo $\mathfrak{j}_m$ ist dieser Ausdruck aber kongruent zu $\sum_{i=0}^{p-1} x^i x^{p-1-i} = px^{p-1} \in pR \subset \mathfrak{j}_1$. —

Theorem 18.62 *Seien* A *ein kompletter lokaler Ring,* $\mathfrak{m}$ *sein maximales Ideal,* $k = A/\mathfrak{m}$ *von der Charakteristik* p *und* $\pi\colon A \longrightarrow k$ *die kanonische Projektion. Dann gibt es einen* p-*Unterring* R *von* A *mit* $R+\mathfrak{m} = A$, *d.h.* $\pi(R) = k$. *Für jedes solche* R *gilt* $R \cap \mathfrak{m} = pR$.

Beweis: Sei $\overline{S}$ eine p-Basis von k und $S \subset A$ ein Repräsentantensystem für $\overline{S}$.

a) Wir behandeln zunächst den Fall, daß $\mathfrak{m}^{n+1} = (0)$ für ein $n \in \mathbb{N}$ ist. Für $m \in \mathbb{N}$ sei $R_m := (A(m))[S]$.

Behauptung 1: Sei A' ein Unterring von A, der S umfaßt. Dann gilt

$$A' \supset R_n \iff A' + \mathfrak{m} = A.$$

Beweis hierfür: "$\Rightarrow$" Zu zeigen ist $\pi(R_n) = k$. Es ist $\pi(A(n)) = k^{p^n}$, also $\pi(R_n) = k^{p^n}[\overline{S}] = k$ nach 18.54.

"$\Leftarrow$": Nach 18.60 ist zu zeigen: $A' \supset \left\{p^r a^{p^{n-r}} \mid a \in A,\ r = 0,\dots,n\right\} \cup S$.
Nach Voraussetzung gilt bereits $S \subset A'$. Da $A' + \mathfrak{m} = A$ ist, gibt es zu jedem $a \in A$ ein $a' \in A'$ mit $a \equiv a' \bmod \mathfrak{m}$. Wegen $p\cdot 1_A \in \mathfrak{m}$ folgt
$p^r(a^{p^{n-r}} - a'^{p^{n-r}}) \in \mathfrak{m}^{n+1} = (0)$ nach 18.61, d.h. $p^r a^{p^{n-r}} = p^r a'^{p^{n-r}} \in A'$.

Für alle n mit $\mathfrak{m}^{n+1} = 0$ ist also R_n der kleinste Unterring R von A mit $R \supset S$ und $R + \mathfrak{m} = A$.

Behauptung 2: Es ist $R \cap \mathfrak{m} = pR$.

Beweis hierfür: "$\supset$" ist klar, da $p\cdot 1_A \in \mathfrak{m}$ gilt.
"$\subset$": Wähle m so groß, daß $\mathfrak{m}^m = (0)$ ist, also nach Obigem $R = R_m = R_{m-1}$ gilt. $A(m)$ enthält die Elemente s^{p^m} mit $s \in S$. Deshalb wird R_m als $A(m)$-Modul von allen Monomen der Form $\prod_{s\in S} s^{\alpha_s}$, wo $0 \le \alpha_s < p^m$ und $\alpha_s = 0$ für fast alle s gilt, erzeugt.
Zusammen mit der Beziehung

$$A(m) = A^{p^m} + p\cdot A(m-1)$$

erhält man für jedes $x \in R$ die Darstellung

$$x = \sum_\alpha a_\alpha^{p^m} Z_\alpha + py$$

mit $a_\alpha \in A$, $y \in R_{m-1} = R$, wo Z_α die oben angegebenen Monome $\prod_{s\in S} s^{\alpha_s}$ durchläuft.
Wenn $x \in R \cap \mathfrak{m}$ ist, gilt $0 = \pi(x) = \sum_\alpha \pi(a_\alpha)^{p^m}\pi(Z_\alpha)$. Da $\pi(a_\alpha)^{p^m} \in k^{p^m}$ ist und die $\pi(Z_\alpha)$ nach 18.54 eine Basis von k über k^{p^m} bilden, folgt $\pi(a_\alpha) = 0$.
Dann ist aber $a_\alpha \in \mathfrak{m}$, also $a_\alpha^{p^m} \in \mathfrak{m}^{p^m} \subset \mathfrak{m}^m = (0)$, und es folgt $x = py$ mit $y \in R$.

Nach Behauptung 2 haben wir: $R/pR = R/(R\cap\mathfrak{m}) \simeq \pi(R) = k$; also ist pR ein maximales Ideal von R. Da aber $p^{n+1} \in \mathfrak{m}^{n+1} = (0)$ gilt, ist R ein p-Ring.
Wir vermerken noch:

R ist der einzige p-Unterring von A mit $R \supset S$ und $R + \mathfrak{m} = A$.

Denn R ist der kleinste solche. Gäbe es noch einen größeren p-Unterring, R', so induzierte die Inklusion $R \hookrightarrow R'$ einen Isomorphismus der Restklassenkörper, wäre also surjektiv nach 18.57c); d.h. $R = R'$.

b) Allgemeiner Fall: Sei $A_n := A/\mathfrak{m}^{n+1}$ und $\pi_n\colon A \longrightarrow A_n$ die kanonische Projektion.
In A_n gibt es einen eindeutig bestimmten p-Unterring R_n, der $\pi_n(S)$ umfaßt und die Eigenschaften des Satzes erfüllt. Da das Bild eines p-Ringes nach 18.56d) wieder ein solcher ist, sieht man nun leicht, daß R_{n+1} bei der kanonischen Projektion $A_{n+1} \longrightarrow A_n$ auf R_n abgebildet wird.
Man erhält

$$R := \varprojlim_n R_n \subset \varprojlim_n A_n = A\,.$$

Nach 18.58 ist R ein p-Ring. Offenbar ist $\pi(R) = k$, d.h. $R + \mathfrak{m} = A$. Da R lokal mit maximalem Ideal pR ist, ist $\mathfrak{m} \cap R = \operatorname{Ker}(\pi|_R) = pR$. —

<u>Bemerkung 18.63</u> Wenn - mit obigen Bezeichnungen - neben $\operatorname{char} k = p$ auch $\operatorname{char} A = p$ gilt, so ist der oben gefundene p-Ring R ein Körper, da dann $pR = (0)$ gilt, und es ist $A = R \oplus \mathfrak{m}$. In diesem Falle ist 18.62 einfacher zu beweisen:

<u>Beweis</u> von 18.62 unter der Zusatzbedingung, daß $\operatorname{char} A = p$ ist:

Sei $\overline{S}$ eine p-Basis von k und $S \subset A$ ein Repräsentantensystem für $\overline{S}$.

a) Sei zunächst $\mathfrak{m}^{n+1} = (0)$ für ein $n \in \mathbb{N}$.

Für $m \in \mathbb{N}$ ist A^{p^m} ein Unterring von A.

Sei m so groß, daß $p^m \geq n+1$ ist.

<u>Behauptung 1:</u> A^{p^m} ist ein Teilkörper von A, der durch π bijektiv auf k^{p^m} abgebildet wird.

Wenn nämlich a^{p^n} mit $a \in A$ keine Einheit in A^{p^n} ist, ist a^{p^n} und damit auch a keine solche in A, d.h. $a \in \mathfrak{m}$. Es folgt $a^{p^m} \in \mathfrak{m}^{p^m} \subset \mathfrak{m}^{n+1} = (0)$. Der Rest ist klar.

<u>Behauptung 2:</u> $A^{p^m}[S]$ ist ein Teilkörper von A, der durch π bijektiv auf k abgebildet wird.

Da $s^{p^m} \in A^{p^m}$ für alle $s \in S$ gilt, wird $A^{p^m}[S]$ als A^{p^m}-Modul von der Familie

$$Z := \Bigl(\prod_{s\in S} s^{\alpha_s} \;\Big|\; 0 \leq \alpha_s < p^m,\ \alpha_s = 0 \text{ für fast alle } s\Bigr)$$

erzeugt. Nach 18.54 ist aber die Familie $\pi(Z)$ linear unabhängig über k^{p^n}.

Der durch π induzierte surjektive Ringhomomorphismus

$$A^{p^m}[S] \longrightarrow k^{p^m}[\overline{S}]$$

ist also auch injektiv. Da $k^{p^m}[\overline{S}] = k$ ist, folgt die Behauptung.

<u>Behauptung 3:</u> Sei K ein Teilkörper von A mit $K \supset S$. Dann gilt

$$\pi(K) = k \iff K = A^{p^m}[S].$$

"$\Rightarrow$": Es ist $K^{p^m}[S] \subset A^{p^m}[S]$. Da $\pi(K^{p^m}[S]) = k^{p^m}[\overline{S}] = k$ ist und $A^{p^m}[S]$ bijektiv durch π auf k abgebildet wird, gilt $K^{p^m}[S] = A^{p^m}[S]$. Wegen $K \supset K^{p^m}[S]$ folgt $K \supset A^{p^m}[S]$. Da K durch π bijektiv auf k abgebildet wird, ist $K = A^{p^m}[S]$.

"$\Leftarrow$" ist trivial.

b) Im allgemeinen Fall sei $\pi_n: A \longrightarrow A/\mathfrak{m}^{n+1}$ die kanonische Projektion. Nach a) gibt es in jedem $A/\mathfrak{m}^{n+1}$ einen eindeutig bestimmten Teilkörper R_n, der bijektiv auf $k = (A/\mathfrak{m}^{n+1})/(\mathfrak{m}/\mathfrak{m}^{n+1})$ abgebildet wird und $R_n \supset \pi_n(S)$ erfüllt.
Bei der kanonischen Projektion

$$A/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}^n$$

wird R_n bijektiv auf R_{n-1} abgebildet. Man erhält also einen Teilkörper $R := \varprojlim_n R_n \subset \varprojlim_n (A/\mathfrak{m}^{n+1}) = A$, mit der gewünschten Eigenschaft. —

<u>Bemerkung 18.64</u> Wir wollen die Theoreme 18.49 und 18.62 nochmals - anders gruppiert - zusammenfassen: Sei A ein kompletter lokaler Ring, $\mathfrak{m}$ sein maximales Ideal und $k := A/\mathfrak{m}$.

a) Wenn $\operatorname{char} k = \operatorname{char} A$ ist, gibt es in A einen Teilkörper K mit $K \oplus \mathfrak{m} = A$.

b) Wenn $\operatorname{char} k \neq \operatorname{char} A$ ist, gilt $\operatorname{char} k = p$ mit einer Primzahl p, und es gibt einen p-Unterring R mit $R + \mathfrak{m} = A$.

7. Cohens Struktursätze

Theorem 18.65 *Sei* A *ein noetherscher kompletter lokaler Ring mit dem maximalen Ideal* $\mathfrak{m}$ *und* $k := A/\mathfrak{m}$. *Dann gilt:*

a) Wenn $\operatorname{char} k = \operatorname{char} A$ *ist, gibt es ein* $n \in \mathbb{N}$, *derart daß* A *isomorph einem Restklassenring von* $k[\![X_1,\ldots,X_n]\!]$ *ist.*

b) Wenn $\operatorname{char} k = p \neq \operatorname{char} A$ *ist, gibt es einen p-Ring* R *mit* $R/pR \simeq k$ *und ein* $n \in \mathbb{N}$, *derart daß* A *isomorph zu einem Restklassenring von* $R[\![X_1,\ldots,X_n]\!]$ *ist.*

Beweis: Sei $\pi\colon A \longrightarrow k$ die kanonische Projektion.

a) Sei K ein Teilkörper von k, der durch π isomorph auf k abgebildet wird. Es gibt also einen Isomorphismus $k \xrightarrow{\sim} K$. Verkettet mit der Inklusion $K \longrightarrow A$ erhält man einen Homomorphismus $\varphi'\colon k \longrightarrow A$.

Sei $\mathfrak{m} = Ax_1 + \ldots + Ax_n$. (A ist noethersch!) Nach 18.33 kann man φ' zu einem Homomorphismus $\varphi\colon k[\![X_1,\ldots,X_n]\!] \longrightarrow A$ mit $\varphi(X_i) = x_i$ fortsetzen.

Zu zeigen bleibt die Surjektivität von φ. Sei $\mathfrak{n} = (X_1,\ldots,X_n)$ das maximale Ideal von $k[\![X_1,\ldots,X_n]\!]$. Es gilt $\varphi(\mathfrak{n}^r) \subset \mathfrak{m}^r$ für alle r. Da $\mathfrak{n}^r$ von den Monomen vom Grade r in den $X_1,\ldots,X_n$ und $\mathfrak{m}^r$ von den Monomen vom Grade r in den $x_1,\ldots,x_n$ erzeugt wird und φ einen Isomorphismus $k[\![X_1,\ldots,X_n]\!]/\mathfrak{n} \longrightarrow A/\mathfrak{m}$ induziert, sieht man, daß der durch φ induzierte Homomorphismus

$$\operatorname{gr}_{\mathfrak{n}}(k[\![X_1,\ldots,X_n]\!]) \longrightarrow \operatorname{gr}_{\mathfrak{m}} A$$

surjektiv ist. Mit 18.28b) folgt die Surjektivität von φ.

b) wird so wie a) bewiesen:

Sei R ein p-Unterring von A mit $\pi(R) = k$ und $\mathfrak{m} = Ax_1 + \ldots + Ax_n$. Es gibt $\varphi\colon R[\![X_1,\ldots,X_n]\!] \longrightarrow A$ mit $\varphi(X_i) = x_i$ wie oben. $R[\![X_1,\ldots,X_n]\!]$ ist $\mathfrak{n}$-adisch komplett, wenn $\mathfrak{n} := (p\cdot 1_R, X_1,\ldots,X_n)$ ist. Dann folgt die Surjektivität von φ wie oben. —

Bemerkung 18.66 Man kann zeigen, daß jeder p-Ring R isomorph einem Restklassenring eines diskreten Bewertungsringes R' ist. ([Bourbaki] chap. IX §2 no. 3 Cor. de la prop. 5.) Im Falle b) von Theorem 18.65 ist dann A auch isomorph einem Restklassenring von $R'[\![X_1,\ldots,X_n]\!]$.

Wegen 18.34 ist also jeder noethersche komplette lokale Ring A isomorph einem Restklassenring eines regulären lokalen Ringes.

Zusatz 18.67 *Zusätzlich zur Voraussetzung von 18.65 sei* A *regulär von der Dimension* d. *Dann gilt:*

a) Wenn $\operatorname{char} k = \operatorname{char} A$ *ist, ist* $A \simeq k[\![X_1,\dots,X_d]\!]$.

b) Wenn $\operatorname{char} k = p \neq \operatorname{char} A$ *und* $p\cdot 1_A \notin \mathfrak{m}^2$ *ist, gibt es einen diskreten Bewertungsring* R *mit* $A \simeq R[\![X_1,\dots,X_{d-1}]\!]$.

(Siehe A19f. für den Fall $p\cdot 1_A \in \mathfrak{m}^2$.)

Beweis: a) Sei $x_1,\dots,x_d$ ein reguläres Parametersystem von A. Wie im Beweis von 18.65 konstruiert man einen surjektiven Homomorphismus $\varphi\colon k[\![X_1,\dots,X_d]\!] \longrightarrow A$, wobei $\pi\circ\varphi(k) = \mathrm{id}_k$ und $\varphi(X_i) = x_i$ ist. Die Injektivität von φ folgt mit 14.6 und 18.28 oder mit Hilfe von Dimensionsbetrachtungen. (Es ist $A \simeq k[\![X_1,\dots,X_d]\!] / \operatorname{Ker}\varphi$. Wäre $\operatorname{Ker}\varphi \neq 0$, so wäre $\dim A < \dim k[\![X_1,\dots,X_d]\!] = d$, da $k[\![X_1,\dots,X_d]\!]$ integer ist.)

b) Da $p\cdot 1_A \notin \mathfrak{m}^2$ ist, gibt es nach 14.12 ein reguläres Parametersystem von A der Form $p\cdot 1_A, x_1,\dots,x_{d-1}$. Es gibt einen p-Unterring R von A mit $\pi(R) = k$. Da A als regulärer Ring integer und $p\cdot 1_R = p\cdot 1_A \neq 0$ ist, ist R ein diskreter Bewertungsring mit maximalem Ideal pR. Die Einbettung $R \subset A$ kann man vermöge $(X_i \to x_i)$ zu einem surjektiven Homomorphismus $\varphi\colon R[\![X_1,\dots,X_{d-1}]\!] \longrightarrow A$ fortsetzen. Sei $\mathfrak{n} := (p\cdot 1_R, X_1,\dots,X_{d-1})$ das maximale Ideal von $R[\![X_1,\dots,X_{d-1}]\!]$. Man betrachtet wieder $\operatorname{gr}(\varphi)\colon \operatorname{gr}_{\mathfrak{n}}(R[\![X_1,\dots,X_{d-1}]\!]) \longrightarrow \operatorname{gr}_{\mathfrak{m}} A$ und schließt wie oben. —

Folgerung 18.68 (zu 18.65) *Jeder noethersche komplette lokale Ring* A *ist katenär.*

Beweis: A ist isomorph einem Restklassenring eines Ringes der Form $B = R[\![X_1,\dots,X_n]\!]$, wo R ein Körper oder ein p-Ring ist. Ein p-Ring ist ein diskreter Bewertungsring, d.h. ein regulärer lokaler Ring der Dimension 1, oder ein Ring endlicher Länge (18.56), d.h. es ist $\dim R = \operatorname{tf} R = 0$. In jedem Fall ist R ein Cohen-Macaulay-Ring; also ist nach 18.34 auch B ein solcher. Wende nun 17.23 an. —

Theorem 18.69 *Sei* A *ein noetherscher kompletter lokaler Ring der Dimension* d *mit Restklassenkörper* k .

a) Wenn $\operatorname{char} k = \operatorname{char} A$ *ist, gibt es einen Unterring* $B \simeq k[\![X_1,\dots,X_d]\!]$ *von* A *derart, daß* A *endlich über* B *ist.*

b) Wenn $\operatorname{char} k = p \neq \operatorname{char} A$ *und* $p\cdot 1_A$ *ein Nichtnullteiler von* A *ist, dann gibt es einen* p*-Ring* R *unendlicher Länge (also einen diskreten Bewertungsring) und einen Unterring* $B \simeq R[\![X_1,\dots,X_{d-1}]\!]$ *von* A *derart, daß* A *endlich über* B *ist.*

Beweis: a) Wie im Beweis von 18.65 hat man einen Homomorphismus $k \hookrightarrow A$, der verkettet mit der kanonischen Projektion $\pi: A \longrightarrow k$ die Identität auf k ergibt.

Sei $x_1,\dots,x_d$ ein Parametersystem von A und $\varphi: k[\![X_1,\dots,X_d]\!] \longrightarrow A$ durch $\varphi(X_i) = x_i$ definiert.

Setze $B' := k[\![X_1,\dots,X_d]\!]$ und $\mathfrak{n} := (X_1,\dots,X_d)$.

Behauptung 1: A ist (vermittels φ) eine endliche B'-Algebra.

Beweis hierfür: Durch φ wird ein Homomorphismus

$$\operatorname{gr}(\varphi): \operatorname{gr}_{\mathfrak{n}}(B') \longrightarrow \operatorname{gr}_{\mathfrak{n}A}(A)$$

induziert. Da B' $\mathfrak{n}$-adisch komplett und $\bigcap\limits_{r\in\mathbb{N}} \mathfrak{n}^r B' \subset \bigcap\limits_{r\in\mathbb{N}} \mathfrak{m}^r = (0)$ ist, genügt es nach 18.29 zu zeigen, daß $\operatorname{gr}_{\mathfrak{n}A}(A)$ (vermittels $\operatorname{gr}(\varphi)$) eine endliche $\operatorname{gr}_{\mathfrak{n}}(B')$-Algebra ist.

Zunächst sieht man, daß $A/\mathfrak{n}A$ endlich über $B'/\mathfrak{n}$ ist. Denn nach Definition eines Parametersystems ist $A/\mathfrak{n}A = A/(x_1A + \dots + x_dA)$ ein Ring endlicher Länge. Ferner hat man ein kommutatives Diagramm kanonischer Ringhomomorphismen

$$\begin{tikzcd} & k \arrow[dl, "\sim"'] \arrow[d] \arrow[dr, "\mathrm{id}_k"] & \\ B'/\mathfrak{n} \arrow[r, hook] & A/\mathfrak{n}A \arrow[r] & A/\mathfrak{m} = k \end{tikzcd} .$$

Daß $A/\mathfrak{n}A$ von endlicher Länge ist, bedeutet, daß $A/\mathfrak{n}A$ als k-Vektorraum, also als $(B'/\mathfrak{n})$-Vektorraum endlich-dimensional ist.

Sei nun $\bar{a}_1,\dots,\bar{a}_r$ ein Erzeugendensystem von $A/\mathfrak{n}A$, und seien $a_1,\dots,a_r \in A$ Repräsentanten der $\bar{a}_i$.

Dann ist $Aa_1 + \dots + Aa_r + \mathfrak{n}A = A$, also
$\mathfrak{n}^m a_1 + \dots + \mathfrak{n}^m a_r + \mathfrak{n}^{m+1}A = \mathfrak{n}^m A$. Es folgt:

$(\mathfrak{n}^m/\mathfrak{n}^{m+1})\bar{a}_1 + \ldots + (\mathfrak{n}^m/\mathfrak{n}^{m+1})\bar{a}_r = \mathfrak{n}^m A/\mathfrak{n}^{m+1}A$.

Deshalb erzeugen $\bar{a}_1,\ldots,\bar{a}_r$ den $gr_{\mathfrak{n}}(B')$-Modul $gr_{\mathfrak{n}A}(A)$.

Behauptung 2: φ ist injektiv. Da $B := \varphi(B') \subset A$ eine endliche Ringerweiterung ist, gilt $\dim B = \dim A$ nach 7.23.

Außerdem ist $\dim B' \underset{18.34a)}{=} d = \dim A$, also $\dim B = \dim B'$.

Wäre $\operatorname{Ker}\varphi \neq (0)$, so wäre

$$\dim B = \dim \varphi(B') = \dim(B'/\operatorname{Ker}\varphi) < \dim B' ,$$

da B' integer ist.

Mit den Behauptungen 1 und 2 ist a) bewiesen.

b) Sei R ein p-Unterring von A , derart daß $\pi(R) = k$ ist.

Da $p\cdot 1_A$ kein Nullteiler in A ist, ist $p\cdot 1_R = p\cdot 1_A$ nicht nilpotent, also R von unendlicher Länge.

Da $p\cdot 1_A$ ein Nichtnullteiler von A ist, gilt $\dim(A/pA) = \dim A - 1$ nach 14.18a). Wenn also $x_1,\ldots,x_{d-1}$ ein Parametersystem des A-Moduls A/pA ist, so ist $p,x_1,\ldots,x_{d-1}$ ein Parametersystem von A .

Definiere nun $B' := R[\![X_1,\ldots,X_{d-1}]\!]$, $\varphi: B' \longrightarrow A$ durch $\varphi(X_i) = x_i$, $\mathfrak{n} := (p\cdot 1_R, X_1,\ldots,X_{d-1})$ und argumentiere wie im Beweis von a). —

Obiges Theorem ist ein Analogon zum Noetherschen Normalisierungslemma 9.2. Deshalb erhält man auch analog zu 9.40 die Folgerung:

Satz 18.70 *Sei* A *ein noetherscher kompletter lokaler Integritätsring und* $Q(A) \subset K$ *eine endliche Körpererweiterung.*
Dann ist der ganze Abschluß B *von* A *in* K *endlich über* A .

Beweis: A ist endlich über einem Unterring $C \simeq R[\![X_1,\ldots,X_d]\!]$, wobei R ein Körper oder ein diskreter Bewertungsring ist. (Beachte, daß A integer ist.) B ist auch der ganze Abschluß von C in K . Wir dürfen also $A = C = R[\![X_1,\ldots,X_d]\!]$ annehmen.

Insbesondere ist ohne Einschränkung A regulär, also ganz abgeschlossen.

Sei nun $\operatorname{char} A = 0$. Da dann L über $Q(A)$ separabel und A ganz abgeschlossen ist, folgt in diesem Falle die Behauptung aus 7.26.

Sei jetzt $\operatorname{char} A$ ($= \operatorname{char} Q(A)$) $=: p > 0$. Für den Restklassenkörper k von A gilt dann ebenfalls $\operatorname{char} k = p$. Ferner dürfen wir $R = k$, d.h. $A = k[\![X_1,\ldots,X_d]\!]$ annehmen.

Wie im Beweis von 9.40 können wir die Behauptung auf den Fall reduzieren, daß K über $Q(A)$ radiziell (d.i. rein inseparabel) ist.

Sei $[K:Q(A)] =: p^r =: q$. Dann ist $K \subset Q(A)^{1/q} = Q(A^{1/q})$.

Man erkennt nun leicht, daß $A^{1/q} = k^{1/q}[\![X_1^{1/q},\ldots,X_d^{1/q}]\!]$ ist.

(Am einfachsten beweist man die hierzu äquivalente Behauptung $A^q = k^q[\![X_1^q,\ldots,X_d^q]\!]$.)

Da $A^{1/q} \simeq A$, also ganz abgeschlossen ist, gilt $B \subset A^{1/q} \cap K$.
(Es gilt sogar die Gleichheit.)

Behauptung: Es gibt eine Indexmenge I und eine A-lineare Einbettung $A^{1/q} \hookrightarrow A^I$.

(Der Gebrauch der Exponentialschreibweise bei $A^{1/q}$ bzw. A^q oben ist ein anderer als bei A^I!)

Wenn nämlich S eine Basis von $k^{1/q}$ über k ist, so bekommt man eine A-lineare Einbettung $k^{1/q}[\![X_1,\ldots,X_d]\!] \hookrightarrow A^S$.

N.B.: Wenn S endlich ist, ist S auch eine Basis von $k^{1/q}[\![X_1,\ldots,X_d]\!]$ über A. Wenn S hingegen unendlich ist, kann man i.a. eine Potenzreihe über $k^{1/q}$ mit ihren unendlich vielen Koeffizienten nicht als endliche Summe von Potenzreihen schreiben, deren Koeffizienten jeweils in $k\cdot s$ mit einem $s \in S$ liegen. Trotzdem gibt es für jedes $s \in S$ eine A-lineare "Projektion" $k^{1/q}[\![X_1,\ldots,X_d]\!] \longrightarrow k[\![X_1,\ldots,X_d]\!] = A$, wo jeder Koeffizient einer Potenzreihe durch seine "s-Komponente" ersetzt wird. Die Gesamtheit dieser Projektionen definiert die gewünschte Einbettung

$$k^{1/q}[\![X_1,\ldots,X_d]\!] \hookrightarrow A^S .$$

Ferner besitzt $A^{1/q} = k^{1/q}[\![X_1^{1/q},\ldots,X_d^{1/q}]\!]$ die endliche Basis T, die aus den Monomen $\prod_{i=1}^{d} X_i^{\alpha_i/q}$ mit $0 \le \alpha_i < q$ besteht. Also erhält man eine A-lineare Einbettung $A^{1/q} \hookrightarrow A^{S\times T}$.

Der Satz folgt nun aus dem

Lemma 18.71 *Sei* A *ein ganz abgeschlossener noetherscher Integritätsring,* $Q(A) \subset K$ *eine endliche Körpererweiterung und* B *der ganze Abschluß von* A *in* K. *Ferner existiere eine Indexmenge* I *und eine* A*-lineare Einbettung* $B \hookrightarrow A^I$.

Dann ist B *endlich über* A.

Beweis hierfür: Es gibt eine Projektion $\sigma\colon A^I \longrightarrow A$ auf einen der Faktoren mit $\sigma(B) \neq \{0\}$. Die Einschränkung $\sigma|B\colon B \longrightarrow A$ ist A-linear und nicht trivial. Da $K = \{\frac{b}{a} \mid b \in B\,,\ a \in A - (0)\}$ ist, wird durch $S(\frac{b}{a}) := \frac{\sigma(b)}{a}$ eine K-lineare Abbildung $K \longrightarrow Q(A)$ mit $\{0\} \neq S(B) \subset A$ definiert. Die Endlichkeit von B über A folgt dann wir im Beweis von 7.26. —

Satz 18.70 ist der Ausgangspunkt eines genaueren Studiums der Frage nach der Endlichkeit des ganzen Abschlusses.

([Bourbaki] Chap. IX §4 einschließlich der "Exercices".)

Aufgaben und Hinweise

1) In stärkerem Maße als sonst haben wir im letzen Paragraphen darauf verzichtet, Begriffe und Sätze in möglichst großer Allgemeinheit und Schärfe darzustellen. Zum Beispiel gibt es den Begriff der Komplettierung für beliebige topologische Gruppen ([Bourbaki T]). Filtrierungen und Graduierungen werden häufig durch $\mathbb{Z}$ und nicht nur durch $\mathbb{N}$ indiziert ([Bourbaki] Chap. III). Projektive Systeme lassen sich wesentlich allgemeiner definieren. Gewisse Eindeutigkeitsaussagen über Koeffizientenringe in 18.49, 18.62 haben wir weggelassen ([Bourbaki] Chap. IX). Das Henselsche Lemma läßt sich allgemeiner formulieren ([Bourbaki] Chap. III).

2) Seien $\mathfrak{a} \subset \mathfrak{b}$ Ideale eines Ringes A. Zeige:
a) Wenn A $\mathfrak{b}$-adisch komplett ist, ist A auch $\mathfrak{a}$-adisch komplett.
b) Wenn A noethersch und $\mathfrak{b}$-adisch komplett ist, ist auch $A/\mathfrak{a}$ $(\mathfrak{b}/\mathfrak{a})$-adisch komplett. (Dies kann man direkt einsehen oder mit Hilfe von 18.18 und 18.21.)

3) a) Sei k ein Körper mit $\operatorname{char} k \neq 2$, $a_0 = b_0^2 \neq 0$ in k.
Wenn $f = \sum_{i\geq 0} a_i X^i \in k[\![X]\!]$ ist, gibt es nach dem Henselschen Lemma (18.42) ein $g = \sum_{i\geq 0} b_i X^i \in k[\![X]\!]$ mit $g^2 = f$. Der Leser möge konkret überlegen, wie man die b_i sukzessive aus den a_j berechnen kann.

N.B.: In $k[X]_{(X)}$ ist $1+X$ kein Quadrat!

b) Zeige, daß $1+X$ in $(\mathbb{Z}/2)[\![X]\!]$ kein Quadrat ist.

Welche Voraussetzung des Henselschen Lemmas ist hier verletzt?

4) Sei k ein Körper mit $\operatorname{char} k \neq 2$, $f = X^2(1+X) - Y^2 \in k[X,Y]$. Zeige:

a) In $k[X,Y]$ ist f irreduzibel, während f in $k[\![X,Y]\!]$ das Produkt zweier irreduzibler formaler Potenzreihen ist. (A3a))

b) Der Ring $A := k[X,Y]_{(X,Y)}/(f)$ ist ein lokaler Integritätsring, während $\hat{A}$ zwei verschiedene minimale Primideale hat. (A2b))

5) Sei A ein noetherscher lokaler Ring und $x \in A$ ein Nichtnullteiler. Zeige: x ist ein Nichtnullteiler für $\hat{A}$. (18.22)
(Beachte, daß aus der Nullteilerfreiheit von A nicht die von $\hat{A}$ folgen muß. (A4))

6) Sei k ein nicht algebraisch abgeschlossener Körper, $f \in k[X]$ irreduzibel mit $\operatorname{grad} f > 1$. Der Restklassenkörper von $A := k[X]_{(f)}$ ist $k[X]/(f)$, während k der größte Teilkörper von A ist (Beweis?). Die Aussage von 18.49 bzw. 18.62 ist also nicht erfüllt.

7) Sei p eine Primzahl, $f \in \mathbb{Z}[X]$ ein unitäres Polynom, welches modulo p irreduzibel ist. Sei $A = \mathbb{Z}[X]_{(p,f)}$ und $\mathfrak{m}$ das maximale Ideal von A. Zeige: $\mathbb{Z}_{(p)}$ ist der größte Unterring von A, der ein diskreter Bewertungsring ist. Aber es ist $\mathfrak{m} + \mathbb{Z}_{(p)} \neq A$.

8) Seien A ein lokaler Ring, $\mathfrak{m}$ sein maximales Ideal, $k = A/\mathfrak{m}$, $\operatorname{char} k = p > 0$, $\pi\colon A \longrightarrow k$ kanonisch. Ferner gelte $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = (0)$.
Setze $U := \bigcap_{n\in\mathbb{N}} A^{p^n} - \{0\}$. Zeige:

a) U ist eine Untergruppe von A^* und wird durch π injektiv in k^* abgebildet.
(Zeige zunächst $U \subset A^*$. Seien $u,v \in U$ mit $u \equiv v \bmod \mathfrak{m}$ und $a^{p^n} = u$, $b^{p^n} = v$. Dann ist auch $a \equiv b \bmod \mathfrak{m}$, also $u \equiv v \bmod \mathfrak{m}^{n+1}$ (18.61).)

b) Wenn A komplett und k vollkommen ist, wird U durch π bijektiv auf k^* abgebildet. (Sei $\alpha \in k^*$. Da k vollkommen ist, gibt es zu jedem n ein $a_n \in A$ mit $\pi(a_n^{p^n}) = \alpha$. Die Folge $(a_n^{p^n})_{n\in\mathbb{N}}$ ist eine Cauchy-Folge: Für $m \leq n$ ist nämlich $a_m^{p^m} \equiv (a_n^{p^{n-m}})^{p^m} \bmod \mathfrak{m}$. Schließe wie unter a).

Die Elemente von U heißen multiplikative Repräsentanten von k^*.

c) Wenn auch $\operatorname{char} A = p$ ist, ist $U \cup \{0\}$ der einzige Teilkörper K von A mit $K \oplus \mathfrak{m} = A$.

d) Für $A = \hat{\mathbb{Z}}_p$ ist U die Menge der $(p-1)$-ten Einheitswurzeln (die sämtlich in $\hat{\mathbb{Z}}_p$ liegen; vgl. 18.46).

e) Für $A = \mathbb{Z}_{(p)}$ und $p \neq 2$ ist $U = \{1,-1\}$.

9) a) Seien A ein Ring, $\mathfrak{a} \subset \operatorname{Jac} A$ ein Ideal, P,Q endliche projektive A-Moduln, derart daß die projektiven $(A/\mathfrak{a})$-Moduln $P/\mathfrak{a}P (\simeq P \otimes_A A/\mathfrak{a})$ und $Q/\mathfrak{a}Q$ zueinander isomorph sind. Zeige: $P \simeq Q$.

(Finde ein kommutatives Diagramm

$$\begin{tikzcd} P \arrow[r, "f"] \arrow[d, "\text{kan.}"'] & Q \arrow[d, "\text{kan.}"] \\ P/\mathfrak{a}P \arrow[r] & Q/\mathfrak{a}Q \end{tikzcd} .$$

Zeige mit Nakayamas Lemma zuerst, daß $\operatorname{Coker} f = 0$, dann, daß $\operatorname{Ker} f$ ein direkter Summand von P, also endlich, schließlich, daß $\operatorname{Ker} f = 0$ ist.)

b) Folgere: Für einen Ring A und ein Ideal $\mathfrak{a} \subset \operatorname{Jac} A$ ist die von der kanonischen Projektion induzierte Abbildung $\operatorname{Pic} A \longrightarrow \operatorname{Pic}(A/\mathfrak{a})$ injektiv.

c) Folgere: $\operatorname{Pic} A[\![X]\!] \simeq \operatorname{Pic} A$ für jeden Ring.
(Betrachte die kanonischen Homomorphismen $A \longrightarrow A[\![X]\!] \longrightarrow A$.)

d) Folgere: Wenn A ein Hauptidealring ist, ist $A[\![X_1,\ldots,X_n]\!]$ faktoriell. (Letzterer Ring ist regulär! Siehe A10a).)

e) Es gibt faktorielle Ringe A, derart daß $A[\![X]\!]$ nicht faktoriell ist. Siehe [Bourbaki] Chap. VII §3, exerc. 8.

10) Sei A ein Hauptidealring. Wir interessieren uns für die Primideale von $A[\![X]\!]$. Zeige:

a) Jedes maximale Ideal hat die Form (X,p) mit p irreduzibel in A.

b) Die übrigen Primideale sind (0) und die der Höhe 1. Jedes Primideal der Höhe 1 wird von einem irreduziblen Element in $A[\![X]\!]$ erzeugt. (A9d))

c) Wenn $\sum_{i\in\mathbb{N}} a_iX^i$ prim (d.h. irreduzibel) in $A[\![X]\!]$ und nicht zu X assoziiert ist, so ist a_0 zu einer Primelementpotenz in A assoziiert.
(Andernfalls konstruiert man sukzessive eine Zerlegung, indem man eine Darstellung der 1 als Linearkombination teilerfremder Elemente in A benutzt.)

d) $f := \sum_{i\in\mathbb{N}} a_iX^i$ ist prim z.B., wenn a_0 prim in A ist.
Ferner ist f prim, wenn $a_0 = p^n$, $p \nmid a_1$ mit p prim in A und $n > 0$ ist. (Gib weitere hinreichende Bedingungen für die Irreduzibilität an.)

e) Sei p eine Primzahl, $S := \{0,1,\dots,p-1\}$. Zeige:
Zu jedem $f = p + \sum_{i\geq 1} a_iX^i \in \mathbb{Z}[\![X]\!]$ gibt es genau ein assoziiertes Element der Form $p + \sum_{i\geq 1} a_i'X^i$ mit $a_i' \in S$. Es gibt also überabzählbar viele paarweise nicht assoziierte Primelemente der Form $p + \sum_{i\geq 1} a_iX^i$ in $\mathbb{Z}[\![X]\!]$.

f) Verallgemeinere f) auf beliebige Hauptidealringe anstelle von $\mathbb{Z}$.

g) Folgere aus a) und b), daß der Ring $A[\![X]\!][X^{-1}] := S^{-1}(A[\![X]\!])$ mit $S = \{1,X,X^2,\dots.\}$ ein Hauptidealring ist.

11) a) Sei $(A_i)_{i\in I}$ eine Familie von krullschen Unterringen eines Körpers K und $A := \bigcap_{i\in I} A_i$. Für jedes $a \in A - \{0\}$ gelte: $a \in A_i^*$ für fast alle i. Zeige: A ist krullsch.

(Wenn man Bourbakis Definition eines krullschen Ringes ([Bourbaki] Chap. VII §1 no. 3 Def. 3.) benutzt, wird der Beweis einfacher als mit unserer Definition 12.43. Vgl. loc.cit. Exemple 3).)

b) Zeige: Wenn B ein Krull-Ring ist, ist auch $B[\![X]\!]$ ein solcher.
($B[\![X]\!] = Q(B)[\![X]\!] \cap \bigcap_{\mathfrak{p}\in P(B)} B_{\mathfrak{p}}[\![X]\!][X^{-1}]$. Verwende A10g).)

c) Sei B ein Krull-Ring.
Zeige: Die kanonischen Homomorphismen $B \hookrightarrow B[\![X]\!]$ und $B[\![X]\!] \longrightarrow B$

erfüllen die Bedingung (*) aus 12.A8a). Es werden also Homomorphismen $C(B) \longrightarrow C(B[\![X]\!])$ und $C(B[\![X]\!]) \longrightarrow C(B)$ induziert, deren Verkettung $\mathrm{id}_{C(B)}$ ergibt. D.h. $C(B)$ wird mit einem direkten Summanden von $C(B[\![X]\!])$ identifiziert.

12) Eine Verallgemeinerung von 18.36.

Sei A $\mathfrak{a}$-adisch komplett.
Zeige: Jede direkte Zerlegung von $A/\mathfrak{a}$ induziert eine solche von A.

13) a) Sei A $\mathfrak{a}$-adisch komplett und $\overline{P}$ ein endlicher projektiver $(A/\mathfrak{a})$-Modul.
Zeige: Es gibt einen endlichen projektiven A-Modul P mit $P/\mathfrak{a}P \simeq \overline{P}$.
(Stelle $\overline{P}$ als direkten Summanden eines freien $(A/\mathfrak{a})$-Moduls $(A/\mathfrak{a})^n$ dar. Die Projektion $(A/\mathfrak{a})^n \longrightarrow \overline{P}$, verkettet mit der Inklusion $\overline{P} \hookrightarrow (A/\mathfrak{a})^n$, ist ein idempotenter Endomorphismus $\overline{e}$, den wir als Element des Matrizenringes $M_n(A/\mathfrak{a})$ auffassen. Sei $e' \in M_n(A)$ ein Repräsentant. In dem kommutativen Ring $A[e']$, der endlich über A, also $\mathfrak{a}$-adisch komplett ist, läßt sich $\overline{e}$ durch ein idempotentes e repräsentieren.)

b) Folgere: Wenn A $\mathfrak{a}$-adisch komplett ist, ist der kanonische Homomorphismus $\operatorname{Pic} A \longrightarrow \operatorname{Pic}(A/\mathfrak{a})$ bijektiv.

14) Sei k ein algebraisch abgeschlossener Körper, A der lokale Ring einer Varietät V in einem Punkt $p \in V$. Sei A regulär. Zeige:

a) p liegt auf genau einer irreduziblen Komponente von V.

b) $\hat{A} \simeq k[\![X_1,\ldots,X_n]\!]$, wobei n die Dimension der irreduziblen Komponente ist, auf der p liegt.

15) Sei k wie oben und V eine irreduzible Varietät über k, ferner A ein lokaler Ring eines Punktes von V. Dann ist $Q(A) = Q(k[V])$. Es gibt zu einer festen Dimension $n > 0$ sehr viele paarweise nicht-isomorphe Körper der Form $Q(k[V])$ mit einer irreduziblen k-Varietät V. (Dies lernt man in der algebraischen Geometrie.)

Somit gibt es auch sehr viele lokale reguläre Ringe A der Dimension n, die im wesentlichen von endlichem Typ über k sind. Für alle diese ist $\hat{A} \simeq k[\![X_1,\ldots,X_n]\!]$. Für Kurven gilt genauer:

Seien C_i für $i = 1,2$ projektive, singularitätenfreie, irreduzible Kurven. ("Singularitätenfrei" heißt: Die lokalen Ringe sind regulär, d.h. hier DBR'e; der Begriff "projektive Varietät" - der nichts mit dem Begriff "projektiver Modul" zu tun hat, wird in jedem Buch über algebraische Geometrie erklärt.) Ferner sei $p_i \in C_i$ und A_i der lokale Ring von C_i in p_i für $i = 1,2$. Wenn dann A_1 und A_2 als k-Algebren isomorph sind, so gibt es einen Isomorphismus $\varphi: C_1 \longrightarrow C_2$ mit $\varphi(p_1) = p_2$.
Beachte dazu, daß die "meisten" singularitätenfreien, projektiven, irreduziblen Kurven eine endliche Automorphismengruppe haben.

16) Sei $f: A \longrightarrow B$ ein lokaler Homomorphismus noetherscher lokaler Ringe und M ein B-Modul, der als A-Modul endlich ist.
Zeige: $\mathrm{tf}_A(M) = \mathrm{tf}_B(M)$.

(Sei $a_1,\dots,a_r$ eine maximale M-reguläre Folge im maximalen Ideal $\mathfrak{m}$ von A. Dann ist $f(a_1),\dots,f(a_r)$ eine M-reguläre Folge nach Definition der A-Modulstruktur auf M; die $f(a_i)$ liegen im maximalen Ideal von B, da f lokal ist.
Setze $N := M/x_1M + \dots + x_rM = M/f(x_1)M + \dots + f(x_r)M$. Es ist $P := \mathrm{Hom}_A(A/\mathfrak{m},N) \neq 0$ ein A-Untermodul endlicher Länge von $\mathrm{Hom}_A(A,N) = N$. Aber P ist auch ein B-Untermodul von N!)

17) Seien A ein lokaler noetherscher Ring, M,N endliche A-Moduln.
Zeige: a) $\mathrm{Ext}^i_A(M,N) \otimes_A \hat{A} \simeq \mathrm{Ext}^i_{\hat{A}}(\hat{M},\hat{N})$.
b) $\mathrm{tf}_A(M) = \mathrm{tf}_{\hat{A}}(\hat{M})$.

18) Sei A ein lokaler noetherscher Ring mit Restklassenkörper k.
Es gelte entweder: $\mathrm{char}\, A = \mathrm{char}\, k$ oder $\mathrm{char}\, k = p > 0$, wobei $p \cdot 1_A$ Nichtnullteiler für A sei.
Dann ist $\hat{A}$ endlich über einem Unterring B der Form $k[[X_1,\dots,X_d]]$, wobei k ein Körper oder ein diskreter Bewertungsring ist. (18.69)

Zeige die Äquivalenz der Aussagen:

(i) A ist ein Cohen-Macaulay-Ring.
(ii) $\hat{A}$ ist ein Cohen-Macaulay-Ring.
(iii) $\hat{A}$ ist ein freier B-Modul.

19) Eine Eisensteinerweiterung eines lokalen Ringes B mit $\mathfrak{n} := \mathrm{Jac}(B)$ ist eine Ringerweiterung der Form $B \subset B[X]/(f)$, wobei $f = \sum_{i=0}^{n} a_i X^i$, $a_n = 1$, $a_i \in \mathfrak{n}$ für $i < n$ und $a_0 \notin \mathfrak{n}^2$.

Zeige: Eine Eisensteinerweiterung eines regulären lokalen Ringes ist wieder ein solcher. (In dem regulären lokalen Ring $B[X]_{(\mathfrak{n}[X] + XB[X])}$ läßt sich f zu einem regulären Parametersystem ergänzen (14.12).)

20) Sei A ein regulärer kompletter lokaler Ring der Dimension n, $\mathfrak{m} := \mathrm{Jac}(A)$, $k := A/\mathfrak{m}$. Es gelte $\mathrm{char}\, k = p \neq \mathrm{char}\, A$ und $p \cdot 1_A \in \mathfrak{m}^2$.

Zeige: A ist eine Eisensteinerweiterung eines Unterringes der Form $R[\![X_1,\ldots,X_{n-1}]\!]$, wobei R ein p-Ring unendlicher Länge ist.

(Es gibt ein Parametersystem $p \cdot 1_A, x_1,\ldots,x_{n-1}$ von A mit $x_i \notin \mathfrak{m}^2$.)

21) Sei A ein reduzierter noetherscher kompletter lokaler Ring, $S = \mathrm{NNT}(A)$. Zeige: Der ganze Abschluß von A in $S^{-1}A$ ist endlich über A.

(Leichte Reduktion auf 18.70.)

Nachträgliche Bemerkungen, Hinweise und Aufgaben

1) Um historisch korrekte Zuweisungen von Sätzen haben wir uns nicht gekümmert.

2) Die Idee, den Hilbertschen Basissatz indirekt zu beweisen, verdanken wir Herrn H.-J. Fendrich (Mainz). Sie findet sich in der Ausarbeitung einer Algebra-Vorlesung Herrn H.-J. Nastolds von 1968/69.

3) An der Aufgabe 1.A3 war ebenfalls Herr Fendrich beteiligt (um 1971).

4) Die von uns verwandte Beweisidee für die Sätze 9.40 und 18.69, die wir im Lemma 18.70 ausgedrückt haben, findet sich in Vorlesungsausarbeitungen von Herrn Nastold um 1969 und stammt möglicherweise von Herrn R. Kiehl (Mannheim-Heidelberg) und/oder Herrn L. Gerritzen (Bochum).

5) Seien A ein Ring, M ein endlicher A-Modul und $\mathfrak{a} \subset A$ ein Ideal mit $\mathfrak{a}M = M$.
   a) Zeige: Es gibt ein $a \in \mathfrak{a}$ mit $(1+a)M = \{0\}$.
   b) Folgere: Wenn A zusätzlich noethersch ist, ist $\bigcap_{n=0}^{\infty}(\mathfrak{a}^n M) = \{x \in M \mid \exists\, a \in \mathfrak{a}: (1+a)x = 0\}$.
   c) Folgere: Wenn A noethersch und integer und $\mathfrak{a} \neq A$ ist, gilt $\bigcap_{n=0}^{\infty} \mathfrak{a}^n = (0)$.

6) Seien V,W affine algebraische Varietäten über algebraisch abgeschlossenem Körper k. Zeige:
   Es ist $k[V \times W] \simeq k[V] \otimes_k k[W]$ (auf kanonische und natürliche Weise).

7) Seien k wie oben, $C_i = V(f_i)$ mit $f_i \in k[X,Y]-k$ für $i = 1,2$ ebene Kurven. Wenn $g \in (f_1,f_2)-(0)$ ist, läuft $C = V(g)$ offenbar durch die Schnittpunkte von C_1 mit C_2.
   Nach Max Nöther (dem Vater Emmy Noethers) ist $g \in (f_1,f_2)$ äquivalent dazu, daß C die Kurven C_1 und C_2 in deren gemeinsamen Schnittpunkten mit gewissen "Vielfachheiten" schneidet. Vgl. [Fulton] 5 Sect. 5 und [Walker] IV. 7, wo allerdings projektive Kurven betrachtet werden.
   Überlege, daß die Theorie der Primärzerlegung (§4 Abschnitt 2) (von E. Lasker und E. Noether) eine weitgehende Verallgemeinerung des Satzes von M. Nöther bedeutet.

LITERATUR

ARTIN, E., Questions de base minimale dans la théorie des nombres algébriques. Colloque international du CNRS (Paris 1950), 19-20

BASS, H., *Algebraic K-Theory*. Benjamin (New York, Amsterdam 1968)

BASS, H. [1], Big projective modules are free. Ill.J.of Math. 7 (1963), 24-31

BOURBAKI, N., *Algèbre Commutative*. Chap. I-VII Hermann (Paris 1961-65), Chap. VIII, IX Masson (Paris etc. 1983)

BOURBAKI, N. [A], *Algèbre*. Hermann (Paris 1958)

BOURBAKI, N. [T], *Topologie Générale*. Hermann (Paris 1960)

COHEN, I.S., Rings with Restricted Minimum Condition. Duke Math. J. 17 (1950), 27-42

DELIGNE, P., La conjecture de Weil. I und II, IHES Publ. Math. 43 (1974), 273-307 und 52 (1980), 137-252

FALTINGS, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Inventiones Math. 73 (1983), 349-366

FULTON, W., *Algebraic Curves*. Benjamin (New York, Amsterdam 1969)

GABRIEL, P., Objects injectifs dans les catégories abéliennes. Sem. P. Dubreil 1958/59 Fasc. 2. Exp. 17

GROTHENDIECK, A., DIEUDONNE, J., *Eléments de Géométrie Algébrique*. Chap. 0_{IV}, IHES Publ. Math. 20 (Bures-sur-Yvette 1964)

HARTSHORNE, R., *Algebraic Geometry*. Springer (New York, Heidelberg, Berlin 1977)

HERZOG, J., KUNZ, E., *Der kanonische Modul eines Cohen-Macaulay-Rings*. Springer LNM 238 (Berlin, Heidelberg, New York 1971)

HILTON, P.J., STAMMBACH, U., *A Course in Homological Algebra*. Springer (New York, Heidelberg, Berlin 1971)

ISCHEBECK, F., Gewisse additive Funktionen auf Modulkategorien. Archiv d.Math. 22 (1978), 252-259

IVERSEN, B., *Generic Local Structure in Commutative Algebra*. Springer LNM 310 (Berlin, Heidelberg, New York 1973)

JAFFARD, P., Théorie de la dimension dans les anneaux des polynomes. Memorial Sci.Math. 146 (1960)

KAPLANSKY, I. [C], *Commutative Rings*. Allyn and Bacon (Boston 1970)

KAPLANSKY, I., Projective Modules. Ann. of Math.(2) 68 (1958), 372-377

KRÄMER, H., Einige Anwendungen der G-Funktion von MacRae. Arch.Math. 22 (1971), 479-490

KUNZ, E., *Einführung in die kommutative Algebra und algebraische Geometrie*. Vieweg (Braunschweig, Wiesbaden 1980)

KUNZ, E. [1], Differentialformen inseparabler algebraischer Funktionenkörper. Math. Zeitschrift 76 (1961), 56-74

LAFON, J.-P., *Algèbre commutative: Langages géométrique et algébrique*. Hermann (Paris 1977)

LAM, T.Y., *Serre's Conjecture*. Springer LNM 635 (Berlin, Heidelberg, New York 1978)

LANG, S., *Algebra*. Addison-Wesley (Reading, Mass. 1965)

LANGMANN, K., Zum Satz von Frisch. Math. Ann. 229 (1977), 141f

LORENZ, F., *Einführung in die Algebra, Teil 1*. B.I. Wissenschaftsverlag (Mannheim, Wien, Zürich 1987)

MACLANE, S., *Homology*. Springer (Berlin, Göttingen, Heidelberg 1963)

MACRAE, R.E., On an Application of the Fitting Invariants. J.Algebra 2 (1965), 153-169

MILNOR, J., *Introduction to Algebraic K-Theory*. Ann. of Math. Studies (Princeton 1971)

MATSUMURA, H., *Commutative Algebra*. Benjamin (New York 1970)

MATSUMURA, H. [R] , *Commutative Ring Theory*. Cambridge University Press (Cambridge, New York 1986)

NAGATA, M., *Local Rings*. Interscience Publ. (New York, London 1962)

NAGATA, M. [2], On the derived normal rings of Noetherian integral domains. Mem. Coll. Sci., Univ. Kyoto 29 (1955), 293-303

NORTHCOTT, D.G., *Lessons on rings modules and multiplicities*. Cambridge University Press (Cambridge 1968)

SCHEJA, G., *Differentialmoduln lokaler analytischer Algebren*. Schriftenreihe des Math. Inst. d. Univ. Fribourg, Fribourg (1969/70)

SCHUBERT, H., *Kategorien I* . Springer (Berlin, Heidelberg, New York 1970)

SERRE, J.-P., *Algèbre Locale. Multiplicités*. Springer LNM 11 (Berlin, Heidelberg, New York 1965)

SERRE, J.P. [A], *Cours d'Arithmétique*. Presses Universitaires de France (Paris 1970)

SWAN, R.G., On Seminormality. J. Algebra 67 (1980), 210-229

SWAN, R.G. [K], *Algebraic K-Theory*. Springer LNM 76 (Berlin, Heidelberg, New York 1968)

SWAN, R.G., EVANS, E.G., *K-Theory of Finite Groups and Orders*. Springer LNM 149 (Berlin, Heidelberg, New York 1970)

WALKER, R.J., *Algebraic Curves*. Dover (New York 1962)

INDEX