# Skript zur Algebra II
# Teil II

**Vorlesung im Wintersemester 2005**
**an der Technischen Universität Berlin**
**Prof. Dr. F. Heß**

II

# Inhaltsverzeichnis

# Vereinbarungen

Folgende allgemeine Festlegungen sollen gelten: Ein Ring $R$ ist (wenn nicht anders vermerkt) kommutativ und hat ein Einselement $1_R$ oder kurz 1. Jeder Homomorphismus $\phi : R \to S$ der Ringe $R$ und $S$ erfüllt $\phi(1_R) = 1_S$. Jeder Teilring eines Rings $R$ enthält $1_R$. Der Nullring ist $R = \{0\}$.

# Kapitel 1

# Ringe I

In diesem Kapitel wird die Ringtheorie behandelt. Für die grundlegenden Definitionen und Aussagen siehe Skript von Pohst.

## 1.1 Grundlagen

Noch einzugeben.

## 1.2 Einheiten, Nullteiler, nilpotente Elemente

**1.1 Definition.** Sei $R$ ein Ring.

1. Sind $a, b \in R$ mit $a \neq 0$, $b \neq 0$ und $ab = 0$, so heißen $a$ (linker) und $b$ (rechter) Nullteiler von $R$.

2. $R$ heißt nullteilerfrei, wenn es keine Nullteiler von $R$ gibt.

3. Ist $a \in R$ und $n \in \mathbb{Z}^{\geq 0}$ mit $a^n = 0$, so heißt $a$ nilpotent.

4. Sei $R$ Ring mit 1. Ein Element $a \in R$ heißt Einheit (invertierbar) in $R$, wenn es $b \in R$ mit $ab = ba = 1$ gibt, und $b$ heißt Inverses von $a$.

5. Die Menge der Einheiten von $R$ wird mit $U(R)$ oder $R^\times$ bezeichnet („$U$“ für „units“).

Das Element $b$ aus 4. ist nach den Überlegungen zu Inversen in Halbgruppen eindeutig bestimmt. Schreibweise: $a^{-1} = b$.

**1.2 Beispiel.** $R = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Es ist leichter, im direkten Produkt zu rechnen: $(2, 0)$ ist nilpotent, denn $(2, 0)^2 = (0, 0)$. $(1, 0)$ ist nicht nilpotent, aber

ein Nullteiler, denn $(1,0)(0,1) = (0,0)$. $(1,2)$ ist eine Einheit (sogar Idempotent), denn $(1,2)(1,2) = 1$. Ebenso ist $(3,2)$ eine Einheit.
Sei $\phi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ der Isomorphismus aus dem chinesischen Restsatz. Was sind die Urbilder der obigen Elemente in $\mathbb{Z}/12\mathbb{Z}$? Orthogonale Idempotente in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sind $(1,0)$ und $(0,1)$, und in $\mathbb{Z}/12\mathbb{Z}$ sind es $e_1 = -3$ und $e_2 = 4$. Damit $\phi(e_1) = (1,0)$ und $\phi(e_2) = (0,1)$. Weiter $\phi^{-1}((2,0)) = 2e_1 + 0e_2 = 6$, $6^2 = 36 = 0 \bmod 12$, $\phi^{-1}((1,2)) = e_1 + 2e_2 = 5$, $5^2 = 25 = 1 \bmod 12$.

**1.3 Beispiel.** $R = \mathbb{Z}$. Es gibt keine nilpotenten Elemente außer 0. Es gibt keine Nullteiler. Die Einheiten sind $1, -1$.

**1.4 Beispiel.** $R = K^{n\times n}$, $n \times n$ Matrizen über $K$ für $K = \mathbb{Q}$ oder $K = \mathbb{R}$ etc. Dies ist mit Matrizenaddition und Matrizenmultiplikation ein Ring. Einselement ist die Einheitsmatrix. Obere Dreiecksmatrizen $A \in K^{n\times n}$ mit 0 auf der Diagonalen sind nilpotent (das charakteristische Polynom einer solchen Matrix $A$ ist $x^n$, und nach dem Satz von Cayley-Hamilton gilt $A^n = 0$). Matrizen $A \in K^{n\times n}$ mit $\det(A) \neq 0$ sind Einheiten (invertierbar). Matrizen $A \in K^{n\times n}$ mit $\det(A) \neq 0$ sind Nullteiler (wähle $v \in K^n$, $v \neq 0$ mit $Av = 0$ und setze $B = (v, \ldots, v) \in K^{n\times n}$. Dann gilt $AB = 0$).

**1.5 Beispiel.** Orthogonale Idempotente ($n \geq 2$) sind Nullteiler.

Wenn $R$ ein Ring ist und wir von Einheiten oder $R^\times$ sprechen, so nehmen wir an, daß $R$ ein Einselement besitzt.

**1.6 Satz.** *Sei $R$ ein Ring.*

1. *$(R^\times, \cdot)$ ist Gruppe und wird Einheitengruppe von $R$ genannt.*
2. *Ist $I$ Ideal von $R$ und $I \cap R^\times \neq \emptyset$, so folgt $I = R$.*
3. *Sei $a \in R$. Die Abbildungen $R \to R$, $x \mapsto ax$ und $R \to R$, $x \mapsto xa$ sind genau dann injektiv, wenn $a$ kein Nullteiler ist.*
4. *Einheiten sind keine Nullteiler. Sind $a, b \in R$ keine Nullteiler, so ist auch $ab$ kein Nullteiler.*
5. *Nilpotente Elemente ungleich Null sind Nullteiler. Für $R$ kommutativ heißt $\mathrm{Rad}(R) = \{x \in R \mid x \text{ ist nilpotent}\}$ das (Nil-)Radikal von $R$ und ist ein Ideal von $R$.*
6. *Es sei $R$ isomorph zu einem direkten Produkt von Ringen $R_i$, also $R \cong \prod_{i\in I} R_i$. Dann gilt $R^\times \cong \prod_{i\in I} R_i^\times$. Für $I$ endlich gilt $\mathrm{Rad}(R) \cong \prod_{i\in I} \mathrm{Rad}(R_i)$.*

*Beweis.* Zu 1. Für $R = 0$ ist $R^\times = \{0\}$ einelementige Gruppe. Ansonsten gilt $0 \notin R^\times$, und für $a, b \in R^\times$ ist $ab \in R^\times$, denn $(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = 1$. Daher ist $R^\times$ eine Halbgruppe mit Einselemente und mit Inversen, also eine Gruppe.

Zu 2. Sei $a \in I \cap R^\times$. Dann gilt $a^{-1}a = 1 \in I$, also $r = r \cdot 1 \in I$ für alle $r \in R$, daher $I = R$.

Zu 3. Sind die Abbildungen injektiv, so gilt $ax = 0 \Rightarrow x = 0$ und $xa = 0 \Rightarrow x = 0$ für beliebiges $x \in R$, also ist $a$ kein Nullteiler. Ist umgekehrt $a \in R$ kein Nullteiler, so gilt $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$, für beliebige $x, y \in R$. Analog für $xa = ya$. Also sind die Abbildungen injektiv.

Zu 4. Sei $a \in R^\times$. Für $b \in R$ folgt aus $ab = 0$, daß $a^{-1}(ab) = (a^{-1}a)b = 0$ ist. Also ist $a$ kein linker Nullteiler. Analog für $ba = 0$ und $a$ ist auch kein rechter Nullteiler. Sind $a, b \in R$ beide keine Nullteiler, so sind die Abbildungen aus 1. und ihre Hintereinanderausführungen $x \mapsto (ab)x$, $x \mapsto x(ab)$ injektiv. Folglich ist $ab$ kein Nullteiler.

Zu 5. Sei $x \in \mathrm{Rad}(R)$, $x \neq 0$. Sei $n \in \mathbb{Z}^{\geq 0}$ minimal mit $x^n = 0$. Es gilt $n \geq 2$. Dann folgt $x^{n-1}x = xx^{n-1} = 0$, also ist $x$ linker und rechter Nullteiler. Für die Idealeigenschaft siehe Aufgabenblatt.

Zu 6. Sei $\phi : R \to \prod R_i$ der Isomorphismus. Elemente in $\prod R_i$ sind genau dann Einheiten, wenn in jeder Koordinate eine Einheit steht. Daher $\phi(R^\times) = (\prod R_i)^\times = \prod R_i^\times$. Weiter gilt $\mathrm{Rad}(\prod R_i) \subseteq \prod \mathrm{Rad}(R_i)$ durch koordinatenweise Betrachtung. Sei $x = (x_1, \ldots, x_n) \in \prod \mathrm{Rad}(R_i)$ mit $n = \#I$, und seien $n_i \in \mathbb{Z}^{\geq 0}$ mit $x_i^{n_i} = 0$ für alle $1 \leq i \leq n$. Setze $m = \prod n_i$. Dann gilt $x^m = 0$, also $x \in \mathrm{Rad}(\prod R_i)$ und damit $\mathrm{Rad}(\prod R_i) = \prod \mathrm{Rad}(R_i)$. Es folgt $\phi(\mathrm{Rad}(R)) = \mathrm{Rad}(\prod R_i) = \prod \mathrm{Rad}(R_i)$. □

**1.7 Beispiel.** Man kann sich die Aussagen des Satzes ganz gut an $\mathbb{Z}/12\mathbb{Z}$ bzw. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ klarmachen. Die Menge der Nullteiler ist im allgemeinen kein Ideal von $R$ (siehe Zerlegung der Eins in orthogonale Idempotente).

**1.8 Satz.** *Seien $R, S$ Ringe mit Eins und $\phi : R \to S$ ein Homomorphismus mit $\phi(1) = 1$. Für $x \in R^\times$ gilt dann $\phi(x) \in S^\times$ und $\phi(x^{-1}) = \phi(x)^{-1}$.*

*Beweis.* Es gilt $1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$ und analog $1 = \phi(x^{-1})\phi(x)$. Daher ist $\phi(x^{-1})$ Inverses von $\phi(x)$, also $\phi(x)^{-1} = \phi(x^{-1})$ per Definition. □

**1.9 Beispiel.** Die Aussage gilt nicht, wenn $\phi(1) \neq 1$ ist. Man betrachte zum Beispiel den Endomorphismus $R \times R \to R \times R$, $(x, y) \mapsto (x, 0)$.

## 1.3 Schiefkörper, Körper, einfache Ringe

**1.10 Definition.** Ein Ring mit $1 \neq 0$ heißt Schiefkörper, wenn $R^\times = R \backslash \{0\}$ gilt. Ist $R$ kommutativ, so heißt $R$ Körper.

Sei $R$ Körper, $S$ Ring. Ist $R$ Unterring von $S$, dann heißt $R$ Teilkörper von $S$. Ist dazu $S$ ein Körper, so heißt $S$ Ober- oder Erweiterungskörper von $R$. Es gelten analoge Bezeichnungen für Schiefkörper.

Homomorphismen von Schiefkörpern und Körpern sind Homomorphismen der zugrundeliegenden Ringe.

**1.11 Beispiel.** Sei

$$K = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\},$$

wobei $\bar{u}, \bar{v}$ die konjugiertkomplexen Zahlen von $u, v$ bezeichnen. Nachrechnen zeigt, daß $K$ unter Addition, Negierung und Multiplikation abgeschlossen ist. Außerdem enthält $K$ die Einheitsmatrix. Daher ist $K$ ein Ring mit Eins. Darüberhinaus gilt

$$\det \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} = |u|^2 + |v|^2,$$

damit ist jede von Null verschiedene Matrix invertierbar, und die Inversen haben die Form

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}^{-1} = \left(|u|^2 + |v|^2\right)^{-1} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix},$$

liegen also wieder in $K$. Damit ist $K$ also ein Schiefkörper. Da $K$ die Erzeuger der Gruppe $Q_8$ enthält, diese waren

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix},$$

ist $K$ nicht kommutativ und heißt Quaternionenschiefkörper.

**1.12 Beispiel.** Sei $p$ eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ Faktorring. Für $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$ gibt es $\lambda, \mu \in \mathbb{Z}$ mit $1 = \lambda a + \mu p$, also $1 \equiv \lambda a \bmod p$. Also ist $\lambda + p\mathbb{Z}$ das Inverse von $a + p\mathbb{Z}$ in $\mathbb{F}_p$ und $\mathbb{F}_p$ ist ein Körper mit $p$ Elementen.

**1.13 Beispiel.** Ist $n \in \mathbb{Z}^{\geq 0}$ keine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ auch kein Körper. Für $n = 0$ ist dies wegen $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$ klar. Für $n \neq 0$ enthält $\mathbb{Z}/n\mathbb{Z}$ Nullteiler. Sei $n = n_1 n_2$ mit $n_i \in \mathbb{Z}^{\geq 1}$. Dann folgt $(n_1 + n\mathbb{Z})(n_2 + n\mathbb{Z}) = n + n\mathbb{Z} = 0 + n\mathbb{Z}$, aber $n_i + n\mathbb{Z} \neq 0 + n\mathbb{Z}$, also sind die $n_i + n\mathbb{Z}$ Nullteiler in $\mathbb{Z}/n\mathbb{Z}$.

**1.14 Definition.** Sei $R$ ein Ring. Besitzt $R$ nur $\{0\}$ und $R$ als Ideale, so heißt $R$ einfach.

**1.15 Satz.** *Sei $R$ ein Ring.*

1. *Ist $R$ einfach und $\phi : R \to S$ ein Ringhomomorphismus, so ist $\phi$ entweder konstant gleich $0$ oder injektiv.*

2. *Schiefkörper sind einfache Ringe.*

3. *Sind $R, S$ Schiefkörper und $\phi : R \to S$ ein nicht konstanter Homomorphismus, so gilt $\phi(1) = 1$ und $\phi(x^{-1}) = \phi(x)^{-1}$ für alle $x \in R$.*

4. *Teilschiefkörper und Erweiterungsschiefkörper besitzen das gleiche Einselement.*

5. *Ist $R \neq 0$, kommutativ und einfach und besitzt $R$ ein Einselement, so ist $R$ ein Körper.*

6. *Ist $R \neq 0$, endlich und nullteilerfrei, so ist $R$ ein Körper.*

*Beweis.* Zu 1. Klar, da $\ker(\phi) = \{0\}$ oder $\ker(\phi) = R$ gelten muß.

Zu 2. Für jedes Ideal $I \neq 0$ gilt $I \cap R^\times \neq \emptyset$, also $I = R$.

Zu 3. Nach 1. ist $\phi$ injektiv und liefert daher einen Gruppenmonomorphismus $R^\times \to S^\times$. Daher $\phi(1) = 1$ und dann $\phi(x^{-1}) = \phi(x)^{-1}$ wie bei Ringen.

Zu 4. Folgt aus 3. für den Inklusionsmonomorphismus.

Zu 5. Sei $x \in R$, $x \neq 0$. Dann ist $Rx$ ein Ideal von $R$, da $R$ kommutativ ist, und es gilt $Rx \neq \{0\}$, da $R$ ein Einselement besitzt und somit $x \in Rx$ gilt. Es folgt $Rx = R$, da $R$ einfach ist. Daher gilt $1 \in Rx$, es gibt also $y \in R$ mit $1 = yx$, also $x \in R^\times$. Es folgt, daß $R\backslash\{0\} = R^\times$ gilt.

Zu 6. Die Menge $R\backslash\{0\}$ ist eine Halbgruppe, da $R$ nullteilerfrei ist. Sei $a \in R\backslash\{0\}$. Die Abbildung $x \mapsto ax$ ist injektiv. Da $R$ endlich ist, ist sie auch surjektiv. Für jedes $b \in R\backslash\{0\}$ gibt es also $x \in \mathbb{R}\backslash\{0\}$ mit $ax = b$. Eine Halbgruppe, in der diese Bedingung erfüllt ist, ist eine Gruppe (siehe Satz über Gruppen am Anfang des Semesters). Damit ist $R$ Schiefkörper. Der Rest des Beweises ist ziemlich schwer und lang (siehe Meyberg 2). □

**1.16 Bemerkung.** Aussage 5 kann ebenfalls dazu verwendet werden, zu zeigen, daß $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p$ ein Körper ist.

**1.17 Bemerkung.** Ist $R \neq 0$ und einfach, so folgt nicht, daß $R$ Schiefkörper ist. Als Beispiel betrachtet man $R = K^{n\times n}$ für einen Körper $K$. Ist $M \in R$ und $M \neq 0$, so ist es nicht schwer zu sehen, daß es $A_i, B_i \in R$ mit $\sum_i A_i M B_i = 1$ gibt. Folglich enthält jedes Ideal ungleich 0 eine Einheit und ist gleich $R$. Daher ist $R$ einfach. Für $n \geq 2$ enthält $R$ aber auch nicht invertierbare Matrizen und ist daher kein Schiefkörper (Details siehe Meyberg 1, Seite 120).

## 1.4 Charakteristik und Primkörper

Ist $R$ ein Ring mit 1, so gibt es genau einen Homomorphismus $\phi : \mathbb{Z} \to R$ mit $\phi(1) = 1_R$. Für $n \in \mathbb{Z}$ ist nämlich $\phi(n) = \phi(n \cdot 1) = n \cdot 1_R$, wobei $n \cdot 1 = 1 + \cdots + 1$

und $n \cdot 1_R = 1_R + \cdots + 1_R$ mit jeweils $n$ Einsen. Dann gibt es ein eindeutig bestimmtes $c \in \mathbb{Z}^{\geq 0}$, so daß $\ker(\phi) = c\mathbb{Z}$, und wir erhalten eine Einbettung von $\mathbb{Z}/c\mathbb{Z}$ in $R$.

**1.18 Definition.** Wir definieren die Charakteristik von $R$ als $\mathrm{char}(R) = c$.

**1.19 Satz.** *Sei $R$ ein Ring mit 1.*

1. $\mathrm{char}(R)$ *ist der kleinste Exponent von* $(R, +)$ *in* $\mathbb{Z}^{\geq 0}$.

2. *Für $R$ nullteilerfrei und $R \neq 0$ ist* $\mathrm{char}(R) = 0$ *oder* $\mathrm{char}(R)$ *eine Primzahl.*

*Beweis.* Zu 1. Mit $n = \mathrm{char}(R)$ gilt $n \cdot 1 = \sum_{i=1}^{n} 1 = 0$. Für $x \in R$ ergibt sich $n \cdot x = \sum_{i=1}^{n} x = (\sum_{i=1}^{n} 1)x = 0x = 0$. Also hat jedes $x$ eine Ordnung kleiner gleich $n$ und 1 hat Ordnung genau $n$.

Zu 2. Sei $n = \mathrm{char}(R)$. Für $n \neq 0$ gilt zunächst $n \geq 2$ wegen $R \neq 0$. Weiter wird $\mathbb{Z}/n\mathbb{Z}$ injektiv nach $R$ durch $\phi$ eingebettet. Da $R$ nullteilerfrei ist, gilt dies auch für $\mathbb{Z}/n\mathbb{Z}$. Also muß $n$ eine Primzahl sein. □

**1.20 Definition.** Sei $R$ ein Ring mit 1. Wir definieren den Primring von $R$ als $\cap\{U \mid U$ Unterring von $R$ mit $1 \in U\}$. Sei $R$ ein Schiefkörper. Wir definieren den Primkörper von $R$ als $\cap\{U \mid U$ Unterschiefkörper von $R\}$.

**1.21 Satz.** *Sei $R$ Ring mit Eins und $\phi : \mathbb{Z} \to R$ wie oben.*

1. $\phi(\mathbb{Z})$ *ist gleich dem Primring von $R$.*

2. *Ist $R$ nullteilerfrei und $R \neq 0$, so ist der Primring isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/p\mathbb{Z}$ für $p$ eine Primzahl.*

3. *Für einen Schiefkörper $R$ ist der Primkörper isomorph zu $\mathbb{Q}$ oder $\mathbb{Z}/p\mathbb{Z}$ für $p$ eine Primzahl.*

*Beweis.* Zu 1. Für einen Unterring $U$ von $R$ mit $1 \in U$ folgt $\phi(\mathbb{Z}) \subseteq U$. Da $\phi(\mathbb{Z})$ ein Unterring mit $1 \in \phi(\mathbb{Z})$ ist, folgt die Behauptung.

Zu 2. Folgt aus 1., $\phi(\mathbb{Z}) \cong \mathbb{Z}/\mathrm{char}(R)\mathbb{Z}$ und weil $\mathrm{char}(R) = 0$ oder eine Primzahl ist.

Zu 3. Der Primkörper enthält den Primring. Ist $\mathrm{char}(R)$ eine Primzahl, so ist der Primring bereits Körper und die Behauptung folgt. Ist $\mathrm{char}(R) = 0$ und ist $U$ ein Teilschiefkörper mit $\phi(\mathbb{Z}) \subseteq U$, so enthält $U$ einen zu $\mathbb{Q}$ isomorphen Teilkörper bestehend aus den Elementen $\{\phi(x)/\phi(y) \mid x, y \in \mathbb{Z}, y \neq 0\}$, woraus sich der Rest der Behauptung ergibt. □

**1.22 Satz.** *Sei $R$ ein kommutativer Ring der Charakteristik $p$, wobei $p$ eine Primzahl ist. Dann gilt $(x+y)^p = x^p + y^p$ für alle $x, y \in R$. Ferner definiert $x \mapsto x^p$ einen Endomorphismus von $R$, welcher Frobeniusendomorphismus (zur Potenz $p$) genannt wird.*

*Beweis.* Die erste Aussage folgt durch Anwendung des binomischen Satzes und weil die binomischen Koeffizienten außer dem ersten und dem letzten alle durch $p$ teilbar und daher hier Null sind. Die Teilbarkeit ergibt sich aus der Proposition zum ersten Satz von Sylow.

Wegen $(xy)^p = x^p y^p$ handelt es sich bei $x \mapsto x^p$ tatsächlich um einen Endomorphismus. □

Iterieren liefert Frobeniusendomorphismen $x \mapsto x^{p^k}$ zu Potenzen $p^k$. Wir sprechen auch von Frobeniusautomorphismen, wenn die Frobeniusendomorphismen injektiv und surjektiv sind.

## 1.5 Noethersche Ringe

**1.23 Definition.** Ein Ring $R$, in dem jedes Ideal durch endlich viele Elemente erzeugt werden kann, heißt noethersch.

**1.24 Satz.** *Sei $R$ ein Ring. Dann sind äquivalent:*

1. *$R$ ist noethersch.*
2. *Jede aufsteigende Kette von Idealen $I_1 \subseteq I_2 \subseteq \ldots$ von $R$ wird stationär, es gibt also $n \in \mathbb{Z}^{\geq 1}$ mit $I_m = I_n$ für alle $m \in \mathbb{Z}^{\geq n}$.*
3. *In jeder nichtleeren Menge $M$ von Idealen gibt es ein maximales Element, es gibt also $I \in M$, so daß für alle $J \in M$ mit $I \subseteq J$ bereits $I = J$ folgt.*

*Beweis.* Siehe Skript von Pohst. □

**1.25 Beispiel.** Der Ring $\mathbb{Z}$ ist noethersch, da jedes Ideal sogar von nur einem Element erzeugt werden kann. Einfache Ringe mit 1 sind noethersch.

**1.26 Beispiel.** Sei $I = \mathbb{Z}$ und $R = \prod_{i \in I} \mathbb{Z}$. Dann ist $R$ nicht noethersch. Die Mengen $I_i = \{f \in R \,|\, f(j) = 0 \text{ für } j \notin \{1, \ldots, i\}\}$ bilden eine echt aufsteigende Kette von Idealen von $R$, die nicht stationär wird.

**1.27 Satz.** *Faktorringe noetherscher Ringe sind noethersch. Epimorphe Bilder noetherscher Ringe sind noethersch.*

*Beweis.* Siehe Meyberg 1 oder Skript von Pohst. □

**1.28 Bemerkung.** Unterringe noetherscher Ringe sind nicht unbedingt noethersch. Als Beispiel (Begriffe werden später eingeführt) kann man einen Polynomring $R$ in unendlich vielen Variablen und dessen Quotientenkörper $K$ betrachten. Dann ist $K$ als Körper noethersch, aber $R$ ist nicht noethersch.

## 1.6 Maximale Ideale

**1.29 Definition.** Sei $R$ ein Ring. Ein Ideal $\mathfrak{m}$ von $R$ heißt maximales Ideal von $R$, wenn $\mathfrak{m} \neq R$ ist und für alle Ideale $I$ von $R$ mit $\mathfrak{m} \subseteq I \subseteq R$ bereits $I = \mathfrak{m}$ oder $I = R$ gilt.

**1.30 Satz.** *Sei $R$ ein Ring und $\mathfrak{m}$ ein Ideal von $R$.*

1. *Ist $\mathfrak{m}$ maximales Ideal und $I$ ein beliebiges Ideal von $R$ mit $I \not\subseteq \mathfrak{m}$, so gilt $I + \mathfrak{m} = R$.*

2. *$\mathfrak{m}$ ist genau dann maximales Ideal von $R$, wenn $R/\mathfrak{m}$ einfach ist.*

3. *Ist $R$ kommutativ mit Einselement, so ist $\mathfrak{m}$ genau dann maximal, wenn $R/\mathfrak{m}$ ein Körper ist.*

*Beweis.* Leicht. □

**1.31 Beispiel.** Die maximalen Ideale von $\mathbb{Z}$ sind genau die Ideale $p\mathbb{Z}$, wo $p$ eine Primzahl ist.

**1.32 Definition.** Sei $M$ eine Menge und $\leq$ eine Relation auf $M$. Dann heißt $\leq$ eine Halbordnung auf $M$, wenn die Eigenschaften

$$x \leq x, \quad (x \leq y \text{ und } y \leq x) \Rightarrow x = y, \quad (x \leq y \text{ und } y \leq z) \Rightarrow x \leq z$$

für alle $x, y, z \in M$ gelten. Gilt dazu $x \leq y$ oder $y \leq x$ für alle $x, y \in M$, so heißt $\leq$ eine Ordnung auf $M$.

Sei $\leq$ eine Halbordnung auf $M$. Für jede Teilmenge $X$ von $M$ schränkt sich $\leq$ zu einer Halbordnung auf $X$ ein. Eine Kette von $M$ ist eine Teilmenge $X$ von $M$, auf der $\leq$ eine Ordnung definiert.

Sei $\leq$ eine Halbordnung auf $M$ und $X \subseteq M$. Ein Element $m \in M$ mit $m \leq x \Rightarrow x = m$ für alle $x \in M$ heißt maximales Element von $M$. Ein Element $s \in M$ mit $x \leq s$ für alle $x \in X$ heißt obere Schranke von $X$ in $M$. Die Menge $M$ heißt induktiv geordnet, wenn jede nicht leere Kette $X$ von $M$ eine obere Schranke in $M$ besitzt.

**1.33 Axiom** (Lemma von Zorn)**.** *Sei $M$ eine bezüglich $\leq$ induktiv geordnete, nicht leere Menge. Dann gibt es ein maximales Element $m$ von $M$.*

*Beweis.* Das Lemma von Zorn ist äquivalent zum Auswahlaxiom, welches von den üblichen Axiomen der Mengenlehre unabhängig ist. Es handelt sich hierbei also eher um eine Annahme, die man treffen oder auch nicht treffen kann. Für gewöhnlich ist es praktisch, das Auswahlaxiom anzunehmen. □

**1.34 Satz.** *Sei $R$ ein Ring mit Einselement und $I$ ein Ideal von $R$ mit $I \neq R$. Dann gibt es ein maximales Ideal $\mathfrak{m}$ von $R$ mit $I \subseteq \mathfrak{m}$.*

*Beweis.* Wir definieren $M = \{J \mid J \text{ Ideal von } R \text{ mit } J \neq R \text{ und } I \subseteq J\}$. Die Inklusionsrelation $\subseteq$ liefert eine Halbordnung auf $M$, wie man unmittelbar sieht.

Wir behaupten, daß $M$ sogar induktiv geordnet ist. Sei dazu $X \subseteq M$ eine nicht leere Kette. Wir müssen zeigen, daß $X$ eine obere Schranke in $M$ besitzt, daß es also ein Ideal $\mathfrak{m}_X \in M$ mit $J \subseteq \mathfrak{m}_X$ für alle $J \in X$ gibt. Definiere $\mathfrak{m}_X := \cup_{J \in X} J$. Ähnlich wie bei aufsteigenden Vereinigungen von Gruppen oder Ringen sieht man leicht, daß es sich hierbei um ein Ideal von $R$ handelt. Es bleibt $\mathfrak{m}_X \neq R$ zu zeigen, um $\mathfrak{m}_X \in M$ zu erhalten. Nun gilt aber $1 \notin J$ für alle $J \in X$, folglich $1 \notin \mathfrak{m}_X$, also $\mathfrak{m}_X \neq R$.

Wegen $I \in M$ ist $M$ nicht leer. Nun wenden wir das Zornsche Lemma an und erhalten die Existenz eines Ideals $\mathfrak{m} \in M$, welches bezüglich $\subseteq$ in $M$ maximal ist. Es gilt also $\mathfrak{m} \neq R$ und $\mathfrak{m} \subsetneq J \Rightarrow J = R$ für jedes Ideal von $R$, und somit ist $\mathfrak{m}$ ein maximales Ideal von $R$. □

Die Aussage des Satzes gilt entsprechend für Links- und Rechtsideale. Für einen noetherschen Ring braucht man das Lemma von Zorn für die Existenz maximaler Ideale gar nicht anzuwenden. Ausgehend von $I = I_1 \subseteq I_2 \subseteq \ldots$ kommt man nach endlich vielen Schritten bei einem maximalen Ideal $\mathfrak{m}$ an.

**1.35 Satz.** *Seien $R, S$ Ringe und sei $\phi : R \to S$ Epimorphismus. Ist $\mathfrak{m}$ ein maximales Ideal von $S$, so ist $\phi^{-1}(\mathfrak{m})$ ein maximales Ideal von $R$.*

*Beweis.* Wir bekommen durch $\phi$ einen Isomorphismus $R/\phi^{-1}(\mathfrak{m}) \to S/\mathfrak{m}$. Da $R/\phi^{-1}(\mathfrak{m})$ mit $S/\mathfrak{m}$ einfach ist, muß $\phi^{-1}(\mathfrak{m})$ maximal sein. □

**1.36 Beispiel.** Die Aussage gilt im allgemeinen nicht, wenn $\phi$ nur Homomorphimus ist. Betrachte $R = \mathbb{Z}$, $S = \mathbb{Q}$ und $\phi$ der Inklusionshomomorphismus. Wähle $\mathfrak{m} = \{0\}$. Dann ist $\mathfrak{m}$ maximales Ideal von $\mathbb{Q}$, aber $\phi^{-1}(\mathfrak{m}) = \{0\}$ ist kein maximales Ideal von $\mathbb{Z}$.

## 1.7 Integritätsringe und Primideale

**1.37 Definition.** Sei $R$ ein kommutativer Ring.

Ein Ideal $\mathfrak{p}$ von $R$ heißt Primideal, wenn $\mathfrak{p} \neq R$ ist und für alle $a, b \in R$ aus $ab \in \mathfrak{p}$ bereits $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

Gilt $R \neq 0$ und ist $R$ nullteilerfrei, so heißt $R$ Integritätsring.

**1.38 Satz.** *Sei $R$ ein kommutativer Ring und $\mathfrak{p}$ ein Ideal von $R$ mit $\mathfrak{p} \neq R$. Dann sind äquivalent:*

1. *$\mathfrak{p}$ ist Primideal,*
2. *Sind $\mathfrak{a}, \mathfrak{b}$ Ideale von $R$, so folgt aus $\mathfrak{ab} \subseteq \mathfrak{p}$ bereits $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$.*
3. *$R \backslash \mathfrak{p}$ mit der Multiplikation aus $R$ ist eine Halbgruppe,*
4. *$R/\mathfrak{p}$ ist Integritätsring,*
5. *$\mathfrak{p}$ ist Kern eines Homomorphismus $\phi : R \to S$, wobei $S$ ein Integritätsring ist.*

*Beweis.* $1 \Rightarrow 2$. Ist Aussage 2 falsch, so gibt es Elemente $a \in \mathfrak{a} \backslash \mathfrak{p}$ und $b \in \mathfrak{b} \backslash \mathfrak{p}$ mit $ab \in \mathfrak{p}$, was im Widerspruch zur Vorausetzung 1 steht.

$2 \Rightarrow 1$. Seien $a, b \in R$ mit $ab \in \mathfrak{p}$. Für $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ gilt $\mathfrak{ab} \subseteq \mathfrak{p}$, wegen $\mathfrak{a} = Ra + \mathbb{Z}a$, $\mathfrak{b} = Ra + \mathbb{Z}b$ und folglich $\mathfrak{ab} = Rab + \mathbb{Z}ab = (ab)$. Also ergibt sich $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$, und daraus $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

$1 \Rightarrow 3$. Seien $a, b \in R \backslash \mathfrak{p}$. Da $\mathfrak{p}$ nach Annahme Primideal ist, muß $ab \notin \mathfrak{p}$ gelten, denn sonst wäre $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

$3 \Rightarrow 4$. $R/\mathfrak{p}$ ist genau dann nullteilerfrei, wenn Bedingung 3 gilt.

$4 \Rightarrow 5$. Wähle $S = R/\mathfrak{p}$ und den Restklassenepimorphismus. Nach Voraussetzung $\mathfrak{p} \neq R$ ist $S \neq 0$ und daher ein Integritätsring.

$5 \Rightarrow 1$. Seien $a, b \in R$ und $ab \in \mathfrak{p} = \ker(\phi)$. Dann gilt $\phi(ab) = \phi(a)\phi(b) = 0$. Da $S$ nullteilerfrei ist, folgt $\phi(a) = 0$ oder $\phi(b) = 0$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Wegen $\mathfrak{p} \neq R$ nach Voraussetzung ist $\mathfrak{p}$ Primideal. □

**1.39 Beispiel.** Die Primideale von $\mathbb{Z}$ sind genau die Ideale $p\mathbb{Z}$, wo $p$ eine Primzahl ist.

**1.40 Beispiel.** Sei $R$ kommutativ mit $R \neq 0$. Das Ideal $\{0\}$ ist genau dann Primideal, wenn $R$ nullteilerfrei ist. Der Nullring $R = 0$ besitzt kein Primideal.

**1.41 Satz.** *Sei $R$ kommutativ mit 1.*

1. *Jedes maximale Ideal von $R$ ist ein Primideal von $R$.*

*2. Zu jedem Ideal $I$ von $R$ mit $I \neq R$ gibt es ein Primideal $\mathfrak{p}$ von $R$ mit $I \subseteq \mathfrak{p}$.*

*Beweis.* Zu 1. Sei $\mathfrak{m}$ maximales Ideal von $R$. Dann gilt $1 \neq 0$ und $R/\mathfrak{m}$ ist ein Körper. Da Körper auch Integritätsringe sind, ist $\mathfrak{m}$ ein Primideal.

Zu 2. Wegen $I \neq R$ gilt $1 \neq 0$. Wähle $\mathfrak{p}$ als ein maximales Ideal $\mathfrak{m}$ mit $I \subseteq \mathfrak{m}$, welches nach Satz 1.34 existiert. □

**1.42 Satz.** *Seien $R, S$ kommutative Ringe und sei $\phi : R \to S$ ein Homomorphismus mit $(\phi(R)) = S$. Ist dann $\mathfrak{p}$ ein Primideal von $S$, so ist $\phi^{-1}(\mathfrak{p})$ ein Primideal von $R$.*

*Beweis.* Wir bekommen durch $\phi$ einen Monomorphismus $R/\phi^{-1}(\mathfrak{p}) \to S/\mathfrak{p}$. Der Ring $R/\phi^{-1}(\mathfrak{p})$ ist mit $S/\mathfrak{p}$ nullteilerfrei. Ferner gilt $(\phi(\phi^{-1}(\mathfrak{p}))) = \mathfrak{p}$ und daher nach Annahme $\phi^{-1}(\mathfrak{p}) \neq R$. □

Die Bedingung $(\phi(R)) = S$ ist beispielsweise erfüllt, wenn $R$ und $S$ kommutative Ringe mit Einselement sind und $\phi(1) = 1$ gilt.

**1.43 Beispiel.** Die Aussage gilt nicht, wenn die Voraussetzung $(\phi(R)) = S$ nicht gemacht wird. Zum Beispiel sei $R = \mathfrak{p}$ Primideal von $S$ und $\phi$ die Inklusionsabbildung. Dann ist $R = \phi^{-1}(\pi)$ kein Primideal. Speziell kann $\mathfrak{p}$ selbst auch ein Einselement besitzen: Man wähle zum Beispiel $R = \mathbb{Q}$, $S = \mathbb{Q} \times \mathbb{Q}$ und $\phi$ die Einbettung von $\mathbb{Q}$ in die erste Koordinate von $\mathbb{Q} \times \mathbb{Q}$. Das Ideal $\mathbb{Q} \times \{0\}$ ist ein Primideal (sogar maximales Ideal) von $\mathbb{Q} \times \mathbb{Q}$, aber $\phi^{-1}(\mathbb{Q} \times \{0\}) = \mathbb{Q}$ ist kein Primideal von $\mathbb{Q}$.

Homomorphe Bilder von Primidealen sind im allgemeinen keine Primideale mehr.

## 1.8 Teilbarkeit in Ringen

Die gewohnte Teilbarkeitslehre von $\mathbb{Z}$ kann verallgemeinert werden. Man setzt üblicherweise voraus, daß die zu betrachtenden Ringe kommutativ mit $1 \neq 0$ sind und keine Nullteiler besitzen.

**1.44 Definition.** Sei $R$ ein Integritätsring mit 1 und $a, b \in R$.

Das Element $a$ heißt Teiler von $b$, wenn es $c \in R$ mit $b = ca$ gibt. Entsprechend sagt man, daß $a$ das Element $b$ teilt, oder daß $b$ ein Vielfaches von $a$ ist, in Zeichen $a \mid b$.

Das Element $a$ heißt assoziiert zu $b$, wenn $c \in R$ mit $b = ca$ eine Einheit von $R$ ist, wenn also äquivalenterweise $a \mid b$ und $b \mid a$ gilt.

Ein Element $c \in R$ heißt größter gemeinsamer Teiler von $a$ und $b$, wenn für alle $d \in R$ aus $d \mid a$ und $d \mid b$ bereits $d \mid c$ folgt. Wir schreiben $c = \gcd(a, b)$, obwohl $c$ nur bis auf Multiplikation mit Einheiten eindeutig bestimmt ist. Die Elemente $a, b$ heißen teilerfremd, wenn $\gcd(a, b)$ eine Einheit von $R$ ist.

Ein Element $c \in R$ heißt kleinstes gemeinsames Vielfaches von $a$ und $b$, wenn für alle $d \in R$ aus $a \mid d$ und $b \mid d$ bereits $c \mid d$ folgt. Wir schreiben $d = \operatorname{lcm}(a, b)$, obwohl $c$ nur bis auf Multiplikation mit Einheiten eindeutig bestimmt ist.

Ein Element $p \in R \backslash R^\times$ mit $p \neq 0$ heißt Primelement von $R$, wenn aus $p \mid (ab)$ für alle $a, b \in R$ bereits $p \mid a$ oder $p \mid b$ folgt.

Ein Element $q \in R \backslash R^\times$ mit $q \neq 0$ heißt irreduzibel, wenn aus $q = ab$ für alle $a, b \in R$ bereits $a \in R^\times$ oder $b \in R^\times$ folgt.

**1.45 Beispiel.** Die Definition stimmt mit den bekannten Definitionen für $\mathbb{Z}$ überein. Primelemente und irreduzible Elemente in $\mathbb{Z}$ stimmen überein.

**1.46 Beispiel.** Sei $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ als Teilring von $\mathbb{R}$. Wegen $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$ ist $\varepsilon = 1 + \sqrt{2}$ eine Einheit in $R$. Da $\varepsilon^k$ für $k \in \mathbb{Z}^{\geq 0}$ eine streng monoton wachsende Folge in $\mathbb{R}$ definiert, gilt $\#R^\times = \infty$.

Man kann zeigen, daß in $\mathbb{Z}[\sqrt{2}]$ die Menge der Primelemente mit der Menge der irreduziblen Elemente übereinstimmt.

**1.47 Beispiel.** Sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ als Teilring von $\mathbb{C}$. Man kann zeigen, daß hier $R^\times = \{-1, 1\}$ gilt und beispielsweise $21 = 3 \cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5}) = (1+2\sqrt{-5})(1-2\sqrt{-5})$ eine Zerlegung von 21 in irreduzible, aber nicht prime Elemente ist.

**1.48 Lemma.** *Sei $R$ ein Integritätsring mit 1.*

1. *$1 \mid a$, $a \mid 0$ und $a \mid a$ für alle $a \in R$.*
2. *$a \mid 1$ genau dann, wenn $a \in R^\times$.*
3. *$a \mid b$ für alle $a \in R^\times$ und $b \in R$.*
4. *Für $a \mid b$ gilt auch $ax \mid bx$ für alle $x \in R$.*
5. *Für $a \mid x_i$ gilt $a \mid \sum_i r_i x_i$ für alle $r_i, x_i \in R$.*
6. *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$ für alle $a, b, c \in R$.*
7. *$a \mid b$ genau dann, wenn $Ra \supseteq Rb$ für alle $a, b \in R$.*

*Beweis.* Einfach und wird ausgelassen. □

**1.49 Satz.** *Sei $R$ Integritätsring mit 1 und $a \in R \backslash R^\times$, $a \neq 0$. Dann gilt:*

1. *Das Element $a$ ist genau dann Primelement von $R$, wenn $Ra$ Primideal von $R$ ist.*

2. *Das Element $a$ ist genau dann irreduzibel, wenn $Ra$ maximal in der Menge der von $R$ verschiedenen Hauptideale ist.*

3. *Jedes Primelement ist irreduzibel.*

4. *Je zwei irreduzible Elemente sind entweder assoziiert oder teilerfremd.*

*Beweis.* Zu 1. Ergibt sich aus $Ra \cdot Rb = Rab$ und Lemma 1.48, Punkt 7.

Zu 2. Die Äquivalenz der negierten Aussagen ergibt sich wie bei 1.

Zu 3. Sei $p \in R$ Primelement und $p = ab$ mit $a, b \in R$. Wegen $p \mid ab$ folgt $p \mid a$ oder $p \mid b$. Gilt beispielsweise $a = cp$ mit $c \in R$, so folgt $p = ab = cpb$, und daraus $1 = cb$ durch Kürzen von $p$ ($p \neq 0$ und $R$ nullteilerfrei), also $b \in R^\times$. Analog für $b = cp$, und $p$ ist also irreduzibel.

Zu 4. Seien $a, b \in R$ irreduzibel und sei $c = \gcd(a, b)$. Dann gibt es $e, d \in R$ mit $a = dc$ und $b = ec$. Da $a$ irreduzibel ist, folgt $c \in R^\times$ oder $d \in R^\times$. Im ersten Fall sind $a, b$ teilerfremd. Im zweiten Fall gilt $b = ed^{-1}a$ und wegen $a \notin R^\times$ ergibt sich $ed^{-1} \in R^\times$, da $b$ irreduzibel ist. Folglich sind $a$ und $b$ assoziiert. □

**1.50 Definition.** Ein Integritätsring $R$ mit 1 heißt Hauptidealring, wenn jedes Ideal von $R$ Hauptideal ist.

**1.51 Beispiel.** Der Ring $\mathbb{Z}$ ist Hauptidealring. Körper sind Hauptidealringe.

**1.52 Satz.** *Sei $R$ ein Hauptidealring. Dann gilt:*

1. *$R$ ist noethersch.*

2. *Sind $a_i \in R$ und $c \in R$ mit $Rc = \sum_i Ra_i$, so gilt $c = \gcd(a_1, \ldots, a_n)$.*

3. *Sind $a_i \in R$ und $c \in R$ mit $Rc = \cap_i Ra_i$, so gilt $c = \operatorname{lcm}(a_1, \ldots, a_n)$.*

4. *Sind $a_i \in R$, so gibt es $\lambda_i \in R$ mit $\gcd(a_1, \ldots, a_n) = \sum \lambda_i a_i$.*

5. *Ein Element $a \in R$ ist genau dann irreduzibel, wenn $a$ ein Primelemement von $R$ ist.*

6. *Jedes $a \in R$, $a \neq 0$ läßt sich als Produkt von Primelementen schreiben.*

*Beweis.* Zu 1. Klar, da jedes Ideal nur einen Erzeuger benötigt.

Zu 2. Wegen $a_i \in Rc$ gilt $c \mid a_i$ für alle $i$. Sei $d \in R$ mit $d \mid a_i$ für alle $i$. Dann folgt $Rd \supseteq \sum_i Ra_i = Rc$, also $d \mid c$.

Zu 3. Es gilt $c \in Ra_i$, also $a_i \mid c$ für alle $i$. Sei $d \in R$ mit $a_i \mid d$ für alle $i$. Dann gilt $Rd \subseteq \cap_i Ra_i = Rc$, also $c \mid d$.

Zu 4. Folgt aus 2, da $c \in \sum_i Ra_i$.

Zu 5. Sei $a \in R \backslash R^\times$, $a \neq 0$ irreduzibel. Dann ist $Ra \neq R$ und maximal in der Menge der Hauptideale. Da jedes Ideal Hauptideal ist, ist $Ra$ also maximales Ideal von $R$, und somit Primideal.

Zu 6. Sei $a \in R$, $a \neq 0$. Ist $a \in R^\times$, so wählen wir als Faktorisierung in Primelemente das leere Produkt. Ist andernfalls $a$ nicht irreduzibel, so gibt es $a_{1,1}, a_{1,2} \in R \backslash R^\times$ mit $a = a_{1,1}a_{1,2}$, also $Ra \subseteq Ra_{1,1}$ und $Ra \subseteq Ra_{1,2}$. Wiederholen wir eine solche Zerlegung induktiv mit $a_{1,1}$ und $a_{1,2}$, so bekommen wir aufsteigende Folgen von Hauptidealen $Ra \subseteq Ra_{1,i_1} \subseteq \cdots \subseteq Ra_{j,i_j} \subseteq \ldots$. Da $R$ noethersch ist, werden diese stationär und die zugehörigen Idealerzeuger somit irreduzibel. Da irreduzible Elemente auch Primelemente sind, folgt die Aussage. □

Aussage 4 des Satzes nennt man auch Satz von Bézout.

**1.53 Definition.** Ein Integritätsring $R$ mit 1 heißt faktorieller Ring (oder ZPE Ring), wenn sich jedes $a \in R$, $a \neq 0$ bis auf Einheiten eindeutig als Produkt von irreduziblen Elementen schreiben läßt.

**1.54 Beispiel.** Der Ring $\mathbb{Z}$ ist ein faktorieller Ring. Es gilt zum Beispiel $-6 = 2 \cdot (-3) = (-1) \cdot 2 \cdot 3$ mit den irreduziblen Elementen $2, -3, 3$ und der Einheit $-1$.

**1.55 Satz.** *Sei $R$ ein Integritätsring mit 1. Dann sind äquivalent:*

1. *$R$ ist faktorieller Ring.*
2. *Jedes $a \in R$, $a \neq 0$ ist Produkt irreduzibler Elemente, und jedes irreduzible Element ist Primelement.*
3. *Jedes $a \in R$, $a \neq 0$ ist Produkt von Primelementen.*

*Beweis.* $1 \Rightarrow 2$. Sei $q$ irreduzibel und $a, b \in R$ mit $q \mid (ab)$, also $ab = cq$ für ein $c \in R$. Das Element $q$ kommt daher wegen der Eindeutigkeit in der Faktorisierung von $ab$ in irreduzible Elemente vor. Diese setzt sich wegen der Eindeutigkeit aus der Faktorisierung von $a$ und von $b$ in irreduzible Elemente zusammen. Also kommt $q$ in einer dieser Faktorisierungen vor, daher $q \mid a$ oder $q \mid b$.

$2 \Rightarrow 3$. Klar.

$3 \Rightarrow 2$. Ist $q$ irreduzibel, so besteht die Faktorisierung von $q$ in Primelemente aus nur einem Element, nämlich $q$ selbst.

$2 \Rightarrow 1$. Seien $\varepsilon q_1 \cdots q_r = \varepsilon' q'_1 \cdots q'_s$ zwei Faktorisierungen in Primelemente $q_i, q'_j$ und Einheiten $\varepsilon, \varepsilon'$ mit $r \leq s$. Für $r = 0$ muß auch $s = 0$ gelten, da Primelemente keine Einheiten sind. Für $r \geq 1$ gilt $q'_s \mid q_i$ für ein $i$. Da $q_i$ irreduzibel ist, ist $q'_s$

assoziiert zu $q_i$. Vertauschen von $q_i$ und $q_r$ und Kürzen von $q'_s$ liefert $\varepsilon q_1 \dots q_{r-1} = \varepsilon'' q'_1 \cdots q'_{s-1}$ mit $\varepsilon'' \in R^\times$. Per Induktion folgt die Eindeutigkeitsaussage. □

Sei $P \subseteq R$ ein Vetretersystem der Äquivalenzklassen der Primelemente von $R$ unter Assoziation. Für $a \in R$, $a \neq 0$ und $p \in R$ bezeichnen wir mit $v_p(a)$ die Vielfachheit, mit der $p$ in der Faktorisierung von $a$ in Primelemente aus $P$ vorkommt. Es gilt also

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)},$$

wobei fast alle $v_p(a)$ gleich Null sind.

**1.56 Korollar.** *Sei $R$ ein Integritätsring mit 1 und $a_1, \dots, a_n \in R$.*

1. *Es gilt* $\gcd(a_1, \dots, a_n) = \prod_{p \in P} p^{\min\{v_p(a_i) \,|\, 1 \leq i \leq n\}}$.
2. *Es gilt* $\operatorname{lcm}(a_1, \dots, a_n) = \prod_{p \in P} p^{\max\{v_p(a_i) \,|\, 1 \leq i \leq n\}}$.
3. *Für $a, b \in R$, $a, b \neq 0$ ist $ab$ assoziiert zu* $\gcd(a, b)\operatorname{lcm}(a, b)$.

*Beweis.* Klar. □

**1.57 Definition.** Ein Integritätsring $R$ heißt euklidischer Ring, wenn es eine Abbildung $d : R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ mit der folgenden Eigenschaft gibt: Zu $a, b \in R$, $b \neq 0$ gibt es $h, r \in R$ mit $a = hb + r$ und $r = 0$ oder $d(r) < d(b)$.

Die in der Definition verlangte Abbildung $d$ heißt Gradfunktion. Die Zerlegung $a = hb + r$ mit $r = 0$ oder $d(r) < d(b)$ heißt Division mit Rest $r$.

**1.58 Satz.** *Jeder euklidische Ring ist ein Hauptidealring.*

*Beweis.* Sei $I$ ein Ideal von $R$ und $a \in I$, $a \neq 0$ ein Element mit $d(a) = \min\{d(b) \,|\, b \in I\backslash\{0\}\}$. Sei $b \in I$. Division mit Rest liefert $b = ha + r$, also $r = b - ha \in I$. Nach Wahl von $a$ ist $d(r) < d(a)$ nicht möglich, also gilt $r = 0$. Es folgt $I = Ra$.

Für $I = R$ folgt speziell $R = Rc$ mit einem $c \in R$. Es gibt $e \in R$ mit $c = ec$, und zu jedem $x \in R$ gibt es $y \in R$ mit $x = yc$. Nun ist $xe = (yc)e = y(ce) = yc = x$, also ist $e$ Einselement.

Damit ist $R$ ein Integritätsring mit 1, in dem jedes Ideal Haupideal ist. □

**1.59 Beispiel.** Der Ring $\mathbb{Z}$ wird mit $x \mapsto |x|$ als Gradfunktion zum euklidischen Ring.

In euklidischen Ringen können größte gemeinsame Teiler mit dem euklidischen Algorithmus berechnet werden. Genauer liefert der euklidische Algorithmus angewendet auf $a, b \in R$ Elemente $\lambda, \mu \in R$ mit $\gcd(a, b) = \lambda a + \mu b$.

## 1.9 Lokale Ringe und Lokalisierung

**1.60 Definition.** Sei $R$ ein kommutativer Ring mit Einselement. Wenn $R$ genau ein maximales Ideal besitzt, dann heißt $R$ lokaler Ring.

**1.61 Satz.** *Ein kommutativer Ring $R$ mit Einselement ist genau dann lokal, wenn $R\backslash R^\times$ ein Ideal von $R$ ist.*

*Für einen lokalen Ring $R$ ist $R\backslash R^\times$ das maximale Ideal von $R$.*

*Beweis.* „$\Rightarrow$“: Bezeichne $\mathfrak{m}$ das maximale Ideal von $R$ und sei $x \in R\backslash R^\times$. Dann gilt $R \neq Rx$, da $x$ keine Einheit ist. Da es ein maximales Ideal von $R$ gibt, welches $Rx$ enthält, folgt $Rx \subseteq \mathfrak{m}$, also $x \in \mathfrak{m}$ und $R\backslash R^\times \subseteq \mathfrak{m}$. Da $\mathfrak{m}$ keine Einheiten enthalten kann, gilt sogar $R\backslash R^\times = \mathfrak{m}$.

„$\Leftarrow$“: Ist $\mathfrak{m} = R\backslash R^\times$ ein Ideal, so ist es aus dem eben genannten Grund maximal und enthält auch jedes weitere Ideal $\neq R$ von $R$. Daher besitzt $R$ nur dieses eine maximale Ideal $\mathfrak{m}$. □

Sei $R \neq 0$ kommutativ und $U$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge von $R$. Wir wollen eine „Bruchrechnung“ mit Elementen aus $R$ im Zähler und Elementen aus $U$ im Nenner definieren. Dazu führen wir auf der Menge $R \times U$ eine Äquivalenzrelation $\sim$ ein. Für $(r_1, u_1), (r_2, u_2) \in R \times U$ gelte $(r_1, u_1) \sim (r_2, u_2)$ genau dann, wenn es ein $t \in U$ mit $t(r_1u_2 - r_2u_1) = 0$ gibt.

**1.62 Lemma.** *Die Relation $\sim$ ist eine Äquivalenzrelation.*

*Beweis.* Reflexivität und Symmetrie sind unmittelbar einsichtig. Für die Transitivität muß etwas gerechnet werden. Es gelte $(r_1, u_1) \sim (r_2, u_2)$ und $(r_2, u_2) \sim (r_3, u_3)$. Wir können also schreiben

$$\begin{aligned} t(r_1u_2 - r_2u_1) &= 0, \\ s(r_2u_3 - r_3u_2) &= 0 \end{aligned}$$

mit $t, s \in U$. Wir multiplizieren die erste Gleichung mit $su_3$ und die zweite mit $tu_1$ und erhalten

$$\begin{aligned} st(r_1u_2u_3 - r_2u_1u_3) &= 0 \\ st(r_2u_1u_3 - r_3u_1u_2) &= 0. \end{aligned}$$

Addition dieser Gleichungen und Ausklammern von $u_2$ liefert

$$stu_2(r_1u_3 - r_3u_1) = 0$$

mit $stu_2 \in U$. □

Die Verwendung von $t$ in der Definition von $\sim$ ist deswegen erforderlich, da wir aus $u_2(r_1u_3 - r_3u_1) = 0$ zum Schluß nicht ohne weiteres auf $r_1u_3 - r_3u_1 = 0$ schließen können. Enthält $U$ keine Nullteiler von $R$, so wäre dies möglich.

Um die Äquivalenzklassen $R \times U/\sim = \{\, [(u,r)] \,|\, (u,r) \in R \times U \,\}$ zu einem Ring zu machen, definieren wir Addition und Multiplikation vertreterweise wie in der Bruchrechnung.

$$\begin{aligned} [(r_1,u_1)] + [(r_2,u_2)] &:= [(r_1u_2 + r_2u_1, u_1u_2)] \\ [(r_1,u_1)] \cdot [(r_2,u_2)] &:= [(r_1r_2, u_1u_2)], \end{aligned}$$

für alle $(r_1,u_1),(r_2,u_2) \in R \times U$.

**1.63 Definition.** Wir bezeichen $R[U^{-1}] := (R \times U/\sim, +, \cdot)$ als die Lokalisierung von $R$ bezüglich $U$.

**1.64 Satz.** *Sei $R$ ein kommutativer Ring und $U$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge von $R$. Dann ist $R[U^{-1}]$ ein kommutativer Ring mit Einselement.*

*Beweis.* Zur Wohldefiniertheit der oben definierten Operationen. Sei $(r_1', u_1') \in R \times U$ mit $[(r_1,u_1)] = [(r_1',u_1')]$, also $tr_1u_1' = tr_1'u_1$ für ein $t \in U$. Es genügt zu zeigen, daß $[(r_1'u_2 + r_2u_1', u_1'u_2)] = [(r_1u_2 + r_2u_1, u_1u_2)]$ und $[(r_1'r_2, u_1'u_2)] = [[(r_1r_2, u_1u_2)]$ gilt. Dann sind die Definitionen unabhängig von der Wahl der Vertreter auf der linken Seite, per Symmetrie dann auch auf der rechten Seite, und zusammen dann auf der linken und rechten Seite simultan. Für die Addition ergibt sich

$$\begin{aligned} t(r_1u_2 + r_2u_1)(u_1'u_2) &= tr_1u_2u_1'u_2 + tr_2u_1u_1'u_2 \\ &= tr_1'u_2u_1u_2 + tr_2u_1u_1'u_2 \\ &= t(r_1'u_2 + r_2u_1')(u_1u_2) \end{aligned}$$

und für die Multiplikation ergibt sich

$$tr_1'r_2u_1u_2 = tr_1r_2u_1'u_2.$$

Dies sind genau die Bedingungen für die Klassengleichheit und somit ist die Wohldefiniertheit bewiesen.

Die Assoziativität von $+$ und $\cdot$ läßt sich direkt für die Vertreter $(r,u)$ verifizieren. Die Distributivität von $+$ und $\cdot$ folgt ähnlich wie die Wohldefiniertheit.

Es gilt offenbar $[(r_1u, u_1u)] = [(r_1,u_1)]$ für alle $(r_1,u_1) \in R \times U$ und $u \in U$. Das Nullelement von $R[U^{-1}]$ ist $[(0,u)]$ für beliebiges $u \in U$, denn $[(0,u)] + [(r_1,u_1)] = [(r_1u, u_1u)] = [(r_1,u_1)]$. Das Einselement von $R[U^{-1}]$ ist $[(u,u)]$ für beliebiges $u \in U$, denn $[(u,u)] \cdot [(r_1,u_1)] = [(r_1u, u_1u)] = [(r_1,u_1)]$. □

**1.65 Definition.** Wir verwenden die Bruchschreibweise $r/u$ für $[(r,u)]$. Wir definieren eine äußere Verknüpfung $R \times R[U^{-1}] \to R[U^{-1}]$ durch $r \cdot (r_1/u_1) := (rr_1)/u_1$.

**1.66 Satz.** *Die Abbildung $\iota_U : R \to R[U^{-1}]$, $r \mapsto r \cdot 1_{R[U^{-1}]}$ ist ein Homomorphismus mit den folgenden Eigenschaften.*

1. $\ker(\iota_U) = \{r \in R \mid ur = 0 \text{ für ein } u \in U\}$.
2. $\iota_U(U) \subseteq R[U^{-1}]^\times$.
3. $\iota_U(R)R[U^{-1}] = R[U^{-1}]$.
4. *Besitzt $R$ das Einselement 1, so gilt $\iota_U(1) = 1_{R[U^{-1}]}$.*

*Beweis.* Zu 1. In $R[U^{-1}]$ gilt $(ru')/u' = 0$ für $u' \in U$ per Definition genau dann, wenn es $u \in U$ mit $ur = 0$ gibt.

Zu 2. Die Elemente $u_1/u_2$ für $u_1, u_2 \in U$ sind offenbar Einheiten in $R[U^{-1}]$.

Zu 3. Für jedes $u', u'' \in U$ gilt $r/u = ((ru')/u')/((uu'')/u'')$.

Zu 4. Es gilt $\iota_U(1) = (1u')/u' = u'/u' = 1_{R[U^{-1}]}$ für jedes $u' \in R$. □

Aus Aussage 1 oder 2 folgt, daß $R[U^{-1}] = \{0\}$ für $0 \in U$ gilt. In einem Integritätsring $R$ gilt $\ker(\iota_U) = 0$ falls $0 \notin U$, und $\iota_U : R \to R[U^{-1}]$ ist ein Monomorphismus.

**1.67 Satz** (Universelle Eigenschaft)**.** *Sei $R$ kommutativer Ring und $S$ kommutativer Ring mit 1. Sei $U$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge von $R$. Dann sind äquivalent.*

1. *Es gibt einen Homomorphismus $\iota : R \to S$ mit $\iota(U) \subseteq S^\times$, so daß es für jeden weiteren kommutativen Ring $T$ mit 1 und jeden Homomorphismus $\phi : R \to T$ mit $\phi(U) \subseteq T^\times$ genau einen Homomorphismus $\psi : S \to T$ mit $\psi \circ \iota = \phi$ gibt.*
2. $S \cong R[U^{-1}]$.

*Beweis.* „2 $\Rightarrow$ 1“: Es genügt, die Aussage 1 für $\iota_U : R \to R[U^{-1}]$ zu zeigen. Zunächst gilt wie erforderlich $\iota_U(U) \subseteq R[U^{-1}]^\times$. Sei $\phi : R \to T$ mit $\phi(U) \subseteq T^\times$. Wir definieren $\psi : R[U^{-1}] \to T$ durch $r/u \mapsto \phi(r)\phi(u)^{-1}$. Aufgrund der Homomorphieeigenschaft von $\phi$ ist $\psi$ zunächst wohldefiniert: Für $r/u = r'/u'$ gibt es $t \in U$ mit $tru' = tr'u$. Daraus folgt $\phi(t)\phi(r)\phi(u') = \phi(t)\phi(r')\phi(u)$ und wegen $\phi(t) \in S^\times$ bereits $\phi(r)\phi(u') = \phi(r')\phi(u)$. Da $\phi(u), \phi(u') \in S^\times$ ergibt sich $\phi(r)\phi(u)^{-1} = \phi(r')\phi(u')^{-1}$. Multiplikativität und Additivität folgen direkt aus

den Rechenregeln in $R[U^{-1}]$. Wegen $\psi(\iota_U(r)) = \psi((ru)/u) = \phi(ru)\phi(u)^{-1} = \phi(r)$ für $u \in U$ ist $\psi$ ein Homomorphismus mit $\psi \circ \iota_U = \phi$.

Sei $\psi'$ ein anderer Homomorphismus mit $\psi' \circ \iota_U = \phi$, und sei $r/u \in R[U^{-1}]$ beliebig. Dann gilt $r/u = \iota_U(r)\iota_U(u)^{-1}$, und damit $\psi'(r/u) = \psi'(\iota_U(r))\psi'(\iota_U(u))^{-1} = \phi(r)\phi(u)^{-1}$. Daher gilt $\psi' = \psi$ und $\psi$ ist eindeutig bestimmt.

„1 $\Rightarrow$ 2“: Nach „2 $\Rightarrow$ 1“ erfüllt $\iota_U : R \to R[U^{-1}]$ ebenfalls die Bedingung 1. Damit erhalten wir zu $\phi = \iota_U$ einen Homomorphismus $\psi_1 : S \to R[U^{-1}]$ mit $\psi_1 \circ \iota = \iota_U$. Analog erhalten wir zu $\phi = \iota$ einen Homomorphismus $\psi_2 : R[U^{-1}] \to S$ mit $\psi_2 \circ \iota_U = \iota$. Es ergibt sich $(\psi_1 \circ \psi_2) \circ \iota_U = \iota_U$ und $(\psi_2 \circ \psi_1) \circ \iota = \iota$. Die Eindeutigkeitsforderung in Bedingung 1 liefert nun $\psi_1 \circ \psi_2 = \mathrm{id}$ und $\psi_2 \circ \psi_1 = \mathrm{id}$. □

Wir bemerken, daß der Homomorphismus $\psi : S \to T$ die Gleichung $\psi(1_S) = 1_T$ erfüllt.

Man kann die Bedingung 1 also als alternative Definition der Lokalisierung nehmen. Dann heißt $S$ zusammen mit $R$, $U$ und $\iota$ Lokalisierung von $R$ bezüglich $U$. Aus der universellen Eigenschaft folgt wie im Beweis leicht, daß $S$ bis auf Isomorphie eindeutig bestimmt ist. Für die Existenz ist aber noch das Konstruktionsverfahren anzugeben.

**1.68 Satz.** *Sei $R$ kommutativer Ring.*

1. *Ist $U \subseteq R^\times$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge, so gilt $R[U^{-1}] \cong R$.*

2. *Sind $U \subseteq V \subseteq R$ nicht-leere, multiplikativ abgeschlossene Teilmengen, so gilt $R[V^{-1}] \cong R[U^{-1}][\iota_U(V)^{-1}]$.*

3. *Ist $U \subseteq R$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge, so gilt $R[U^{-1}] \cong \iota_U(R)[\iota_U(U)^{-1}]$.*

*Beweis.* Aufgabe. □

Ist $R$ ein kommutativer Ring mit Eins und ist $1 \notin U$, aber $1 \in V$, so gilt wegen $\iota_U(1) = 1$ nach Aussage 1 trotzdem $R[U^{-1}] = R[V^{-1}]$. Daher setzt man im Fall, daß $R$ ein Einselement hat, üblicherweise $1 \in U$ voraus.

Man wendet Lokalisierung an, wenn man einen Ring „vereinfachen“ möchte. Die guten Eigenschaften von $R$ übertragen sich auf $R[U^{-1}]$, und weitere können hinzukommen.

Wir vergleichen die Idealtheorie in $R$ und $R[U^{-1}]$ für einen kommutativen Ring $R$ und eine nicht-leere, multiplikativ abgeschlossene Teilmenge $U$ von $R$. Die Idealtheorie in $R[U^{-1}]$ stellt sich dabei als Vereinfachung der Idealtheorie in

$R$ heraus. Seien $\mathcal{I}(R)$ und $\mathcal{I}(R[U^{-1}])$ die Mengen der Ideale von $R$ beziehungsweise $R[U^{-1}]$. Wir betrachten die üblichen Abbildungen

$$i : \mathcal{I}(R) \to \mathcal{I}(R[U^{-1}]),\ I \mapsto \iota_U(I)R[U^{-1}],$$
$$j : \mathcal{I}(R[U^{-1}]) \to \mathcal{I}(R),\ J \mapsto \iota_U^{-1}(J).$$

Sei $I$ ein Ideal von $R$ und $\pi_I : R \to R/I$ der kanonische Epimorphismus. Sei $\bar{I} = \{r \in R \mid \exists\, u \in U \text{ mit } ur \in I\}$. Man prüft leicht nach, daß $\bar{I}$ ein Ideal von $R$ mit $\bar{I} \supseteq I$ ist und daß $\bar{\bar{I}} = \bar{I}$ gilt. Wir nennen $\bar{I}$ den Abschluß von $I$ bezüglich $U$. Gilt $\bar{I} = I$, so nennen wir $I$ bezüglich $U$ abgeschlossen. Sei $\mathcal{I}_U$ die Menge der abgeschlossenen Ideale von $R$.

**1.69 Satz.** *Mit den eingeführten Bezeichnungen gelten*

1. *$i(j(J)) = J$ und $j(i(I)) = \bar{I}$ für alle $J \in \mathcal{I}(R[U^{-1}])$ und alle $I \in \mathcal{I}(R)$.*
2. *Es gilt $\mathrm{im}(j) = \mathcal{I}_U$, so daß $i$ und $j$ zueinander inverse Bijektionen der Mengen $\mathcal{I}_U$ und $\mathcal{I}(R[U^{-1}])$ liefern.*
3. *Für $I \in \mathcal{I}(R)$ gilt $(R/I)[\pi_I(U)^{-1}] \cong R[U^{-1}]/i(I)$.*
4. *$j$ erhält Inklusionen, Summen, Schnitte, Produkte und Radikale etc. Dasselbe gilt für $i$ eingeschränkt auf $\mathcal{I}_U$.*
5. *Sei $I \in \mathcal{I}(R)$ ein Primideal (maximales Ideal). Dann ist $i(I)$ ein Primideal (maximales Ideal) für $I \cap U = \emptyset$ und $i(I) = R$ andernfalls. Sei $J \in \mathcal{I}(R[U^{-1}])$ ein Primideal. Dann ist $j(J)$ ein Primideal.*

*Beweis.* Zu 1. Für $J \in \mathcal{I}(R[U^{-1}])$ gilt allgemein $i(j(J)) = \iota_U(\iota_U^{-1}(J))R[U^{-1}] \subseteq J$. Für $r/u \in J$ ist aber auch $(ru')/u' \in J$ nach Muliplikation mit $(uu')/u' \in R[U^{-1}]^\times$ für beliebiges $u' \in U$, und damit $r \in \iota_U^{-1}((ru')/u')$. Daher $(ru')/u' \in \iota_U(\iota_U^{-1}(J))$ und $(ru')/(uu') = r/u \in \iota_U(\iota_U^{-1}(J))R[U^{-1}]$ nach Division mit $(uu')/u'$ wegen $(uu')/u' \in R[U^{-1}]^\times$. Wir haben damit $i(j(J)) = \iota_U(\iota_U^{-1}(J))R[U^{-1}] = J$ gezeigt.

Für $I \in \mathcal{I}(R)$ gilt $j(i(I)) = \iota_U^{-1}(\iota_U(I)R[U^{-1}]) = \{r \in R \mid \exists u \in U \text{ mit } ur \in I\} = \bar{I}$. Zum Beweis der zweiten Gleichung beachten wir zuerst $\iota_U(I)R[U^{-1}] = \{x/u'' \mid x \in I, u'' \in U\}$, wie man leicht sieht. Weiter gilt $r \in \iota_U^{-1}(\iota_U(I)R[U^{-1}])$ für $r \in R$ genau dann, wenn $\iota_U(r) = (ru')/u' \in \iota_U(I)R[U^{-1}] = \{x/u'' \mid x \in I, u'' \in U\}$ für ein beliebiges $u' \in U$ ist, wenn also $(ru')/u' = x/u''$ für ein $x \in I$ und $u', u'' \in U$ gilt. Dies ist aber äquivalent dazu, daß es $u \in U$ mit $ur \in I$ gibt.

Zu 2. Für $J \in \mathcal{I}(R[U^{-1}])$ gilt nach Aussage 1 nun $\overline{j(J)} = j(i(j(J))) = j(J)$, also $\mathrm{im}(j) = \mathcal{I}_U$. Daher sind $i$ und $j$ nach Aussage 1 zueinander inverse Bijektionen der Mengen $\mathcal{I}_U$ und $\mathcal{I}(R[U^{-1}])$.

Zu 3. Wir betrachten $S = (R/I)[\pi_I(U)^{-1}]$ und $\phi = \iota_{\pi_I(U)} \circ \pi_I : R \to S$. Wegen $\phi(U) \subseteq S^\times$ gibt es $\psi : R[U^{-1}] \to S$ nach Satz 1.67 mit $\psi(r/u) = (r+I)/(u+I)$. Dies zeigt, daß $\psi$ surjektiv ist. Sei nun $r/u \in R[U^{-1}]$ mit $\psi(r/u) = 0$. Dies ist genau dann der Fall, wenn es $u' \in U$ mit $(u'+I)(r+I) = 0+I$ beziehungsweise mit $u'r \in I$ gibt. Also gilt $r \in \bar{I}$ und $r/u \in i(\bar{I}) = i(I)$ nach Aussage 1. Dies zeigt $\ker(\psi) = i(I)$.

Zu 4. Die Aussagen für $j$ gelten allgemein, wenn $\iota_U$ nur irgendein Homomorphismus von Ringen ist. Wegen der Bijektivität von $i$ und $j$ auf $\mathcal{I}_U$ und $\mathcal{I}(R[U^{-1}])$ folgen die Aussagen hier auch analog für $i$. Zusatz zum Radikal: Es gilt zunächst $j(\mathrm{Rad}(J)) = \mathrm{Rad}(j(J))$ für alle $J \in \mathcal{I}(R[U^{-1}])$. Mit $I = j(J)$, $J = i(I)$ und durch Anwenden von $i$ ergibt sich $\mathrm{Rad}(i(I)) = i(\mathrm{Rad}(I))$ für alle $I \in \mathcal{I}(R)$.

Zu 5. Muß noch ein wenig angepasst werden (Wegen Satz 1.66, Aussage 3 und Satz 1.42 ist $I = j(i(I))$ ein Primideal von $R$, wenn $i(I)$ ein Primideal von $R[U^{-1}]$ ist. Für $I$ ein Primideal von $R$ gilt $0 \notin \pi_I(U)$, da es sonst $u \in U$ mit $u \in I$ geben und dann $I = \bar{I} = R$ folgen würde. Nun ist $(R/I)[\pi_I(U)^{-1}]$ mit $R/I$ wegen $0 \notin \pi_I(U)$ ein Integritätsring. Nach Aussage 3 ist also auch $R[U^{-1}]/i(I)$ ein Integritätsring und damit $i(I)$ ein Primideal.

Ist $I$ maximal, so sind $R/I$ und $(R/I)[\pi_I(U)^{-1}]$ nach Aussage 2 einfach. Wegen Aussage 3 ist $R[U^{-1}]/i(I)$ einfach und daher $i(I)$ maximal.) □

Für $U \cap I = \emptyset$ ist $I$ bezüglich $U$ genau dann abgeschlossen, wenn $\pi_I(U)$ eine Menge von Nichtnullteilern in $R/I$ ist. Bei der Berechnung von $\bar{I} = j(i(I))$ muß man also (zumindest im nullteilerfreien Fall) aus den Elementen von $I$ alle Elemente von $U$ herausdividieren, um das abgeschlossene Ideal zu erhalten.

Wenn die Definitionen etwas modifiziert werden, kann Aussage 3 auch in der hübschen Form $(R/I)[U^{-1}] \cong R[U^{-1}]/I[U^{-1}]$ geschrieben werden. Lokalisierung und Faktorisierung kommutieren also. Besitzt $R$ ein Einselement und ist $I$ maximal, so gilt $\pi_I(U) \subseteq (R/I)^\times$ und es ergibt sich $R/I \cong R[U^{-1}]/i(I)$.

Setzen wir $I = \overline{\{0\}} = \ker(\iota_U)$, so gilt $i(I) = \{0\}$. Dann ist $\iota_{\pi_I(U)} : R/I \to (R/I)[\pi_I(U)^{-1}]$ injektiv und es gilt $(R/I)[\pi_I(U)^{-1}] \cong R[U^{-1}]$. Wir können $\iota_U$ daher entsprechend in einen Epimorphimus und einen Monomorphismus faktorisieren.

**1.70 Satz.** *Sei $R$ kommutativer Ring und $U$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge von $R$ mit $0 \notin U$. Dann übertragen sich die Eigenschaften Ring mit Einselement, Integritätsring, einfach, noethersch, faktoriell, Hauptidealring und euklidisch auf $R[U^{-1}]$. Die Nullteiler von $R[U^{-1}]$ sind Bilder der Nullteiler von $R$.*

*Beweis.* Aufgabe, nachrechnen und die Abbildungen $i$ und $j$ verwenden. Die euklidische Gradfunktion $\delta_U$ auf $R[U^{-1}]$ wird $\delta_U(r/u) = \min\{\delta(x) \mid x \in \overline{(r)}\}$ (?). □

**1.71 Beispiel.** Sei $R = \mathbb{Z}$, $R[U^{-1}] = \mathbb{Z}[1/2]$ und $I = n\mathbb{Z}[1/2]$ mit $n \in \mathbb{Z}^{\geq 1}$. Wir zerlegen $n = 2^v n_1$ mit $n_1$ ungerade. Dann gilt $I = n_1\mathbb{Z}[1/2]$, da $1/2$ eine Einheit in $\mathbb{Z}[1/2]$ ist. Unter Verwendung von $j$ für die Ideale von $\mathbb{Z}[1/2]$ und $\mathbb{Z}$ wie oben sieht man ebenfalls $j(n\mathbb{Z}[1/2]) = n_1\mathbb{Z}$ nach Aussage 1. Nach Aussage 2 und Aussage 3 ergibt sich dann beispielsweise $\mathbb{Z}[1/2]/n\mathbb{Z}[1/2] \cong \mathbb{Z}/n_1\mathbb{Z}$.

Zusammenfassend schließlich ein paar typische Situationen.

**1.72 Definition.** Sei $R$ ein Integritätsring mit 1. Für ein Primideal $\mathfrak{p}$ ist $U = R\backslash\mathfrak{p}$ nicht-leer und multiplikativ abgeschlossen. Der Ring $R[U^{-1}]$ wird Lokalisierung von $R$ an $\mathfrak{p}$ genannt und mit $R_\mathfrak{p}$ bezeichnet.

**1.73 Satz.** *Sei $R$ ein Integritätsring mit* 1.

1. *Für das Primideal $\mathfrak{p}$ von $R$ ist $R_\mathfrak{p}$ lokaler Ring mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$.*
2. *Für das Nullprimideal $\mathfrak{p} = \{0\}$ von $R$ ist $R_\mathfrak{p}$ ein Körper.*

*Beweis.* Zu 1. Sei $x/y \in R_\mathfrak{p}\backslash\mathfrak{p}R_\mathfrak{p}$. Dann gilt $x \in R\backslash\mathfrak{p}$ und somit $y/x \in R_\mathfrak{p}$ nach Definition von $R_\mathfrak{p}$. Folglich $x/y \in R_\mathfrak{p}^\times$, so daß nach Satz 1.61 der Ring $R_\mathfrak{p}$ lokal mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$ ist.

Zu 2. Der Ring $R_\mathfrak{p}$ ist ein lokaler Ring mit maximalem Ideal $\{0\}$. Also gilt $R_\mathfrak{p}^\times = R_\mathfrak{p}\backslash\{0\}$ und $R_\mathfrak{p}$ ist damit nach Satz 1.61 ein Körper. □

Allgemein ist das Ideal $\mathfrak{p}R_\mathfrak{p}$ nur ein Primideal in $R_\mathfrak{p}$.

**1.74 Definition.** Sei $R$ ein Integritätsring mit 1. Der Körper $R_{\{0\}}$ wird Quotientenkörper von $R$ genannt und mit $\mathrm{Quot}(R)$ bezeichnet.

**1.75 Beispiel.** Sei $R = \mathbb{Z}$. Der Quotientenkörper von $\mathbb{Z}$ ist $\mathbb{Q}$. Für eine Primzahl $p$ und das Primideal $\mathfrak{p} = p\mathbb{Z}$ gilt $R_\mathfrak{p} = \{x/y \mid x, y \in \mathbb{Z} \text{ und } p \nmid y\}$. Das maximale Ideal ist $\mathfrak{p}R_\mathfrak{p} = \{x/y \mid x, y \in \mathbb{Z} \text{ und } p \nmid y, p \mid x\}$.

Ein weiteres Beispiel ist $\mathbb{Z}[1/3] = \{x/3^i \mid i \in \mathbb{Z}^{\geq 0}, x \in \mathbb{Z}\}$ oder $\mathbb{Z}[1/2, 1/3] = \{x/(2^i 3^j) \mid i, j \in \mathbb{Z}^{\geq 0}, x \in \mathbb{Z}\}$. In beiden Ringen ist 3 eine Einheit mit unendlicher Ordnung. In $\mathbb{Z}[1/2, 1/3]$ sind die Einheiten 2 und 3 sogar unabhängig, das heißt $2^i 3^j = 1$ geht nur für $i = 0$ und $j = 0$.

**1.76 Beispiel.** Sei $R = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und $U = \langle(1, 0)\rangle$. Um $R[U^{-1}]$ zu bestimmen, berechnen wir zuerst das Bild von $R$ in $R[U^{-1}]$ unter $\iota_U$. Es gilt $\ker(\iota_U) = \{r \in R \mid ur = 0 \text{ für ein } u \in U\} = \{0\} \times \mathbb{Z}/5\mathbb{Z}$. Also ist $\iota_U(R) \cong R/\ker(\iota_U) \cong \mathbb{Z}/3\mathbb{Z}$. Da $\iota_U(U) \subseteq \iota_U(R)^\times$ gilt hier bereits $R[U^{-1}] = \iota_U(R)$. Für $R = \mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und $U = \langle 3, 0\rangle$ ergäbe sich beispielsweise $R[U^{-1}] \cong \mathbb{Z}[1/3]$.

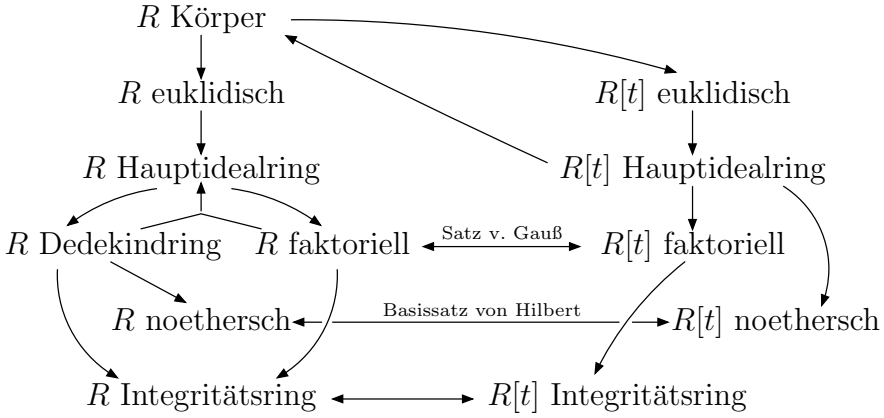
**1.77 Beispiel.** Enthält $U$ ein nilpotentes Element, so gilt $R[U^{-1}] = 0$.

**1.78 Bemerkung.** Die meisten Aussagen dieses Abschnitts können für nicht kommutative Ringe $R$ geeignet verallgemeinert werden, wenn man $U$ stets aus dem Zentrum von $R$ wählt, wenn also die Elemente aus $U$ mit allen Elementen von $R$ kommutieren.

# Kapitel 2

# Polynomringe

Wir betrachten in diesem Kapitel kommutative Ringe $R$ mit Einselement und die zugehörigen Polynomringe $R[t]$. Eine Übersicht über die (behandelten bzw. zu behandelnden) Ringeigenschaften und Beziehungen wird in der folgenden Abbildung gegeben.




Generalvoraussetzung für dieses Kapitel ist, daß Ringe Einselemente besitzen und daß Homomorphismen Einselemente auf Einselemente abbilden.

## 2.1 Univariate Polynomringe

**2.1 Definition.** Seien $R, S$ kommutative Ringe und $\phi : R \to S$ ein Homomorphismus. Wir definieren eine äußere Verknüpfung $\cdot : R \times S \to S$ durch $r \cdot x = \phi(r)x$ und nennen $S$ mit dieser äußeren Verknüpfung die durch $\phi$ definierte $R$-Algebra. Als Schreibweise verwenden wir wie üblich $rx = r \cdot x$.

Sind $S$ und $T$ $R$-Algebren, so verstehen wir unter einem $R$-Algebra Homomorphismus einen Ringhomomorphismus $f : S \to T$ mit $f(rx) = rf(x)$ für alle $r \in R$ und $x \in S$. Analog werden $R$-Algebra Mono-, Epi-, Iso-, Endo- und Automorphismen definiert.

Die Homomorphieeigenschaft von $\phi$ impliziert die üblichen bzw. erwarteten Assoziativitäts- und Distributivitätseigenschaften von $\cdot$, die zur Grundlage einer allgemeineren Definition von $R$-Algebra gemacht werden können. Enthält $S$ jedoch ein Einselement 1 (was wir hier in der Generalvoraussetzung annehmen), so wird jede $R$-Algebra durch einen solchen Homomorphismus $\phi : R \to S$ definiert, indem man nämlich $\phi(r) = r \cdot 1$ wählt.

Bei den lokalen Ringen haben wir $R[U^{-1}]$ in ähnlicher Weise als $R$-Algebra aufgefaßt.

Nun zur Definition des (univariaten) Polynomrings. Sei $R$ ein kommutativer Ring. Wir setzen

$$R[t] = \{f \mid f : \mathbb{Z}^{\geq 0} \to R \text{ mit } f(i) = 0 \text{ für fast alle } i \in \mathbb{Z}^{\geq 0}\}.$$

Für $f, g \in R[t]$ definieren wir $f + g \in R[t]$ durch

$$(f + g)(i) = f(i) + g(i)$$

und $f \cdot g \in R[t]$ durch

$$(f \cdot g)(i) = \sum_{\nu+\mu=i} f(\nu)g(\mu),$$

wobei $\nu, \mu$ über alle Zahlen in $\mathbb{Z}^{\geq 0}$ laufen. Man sieht leicht, daß $R[t]$ mit den inneren Verknüpfungen $+$ und $\cdot$ ein Ring ist. Das Nullelement von $R[t]$ wird durch die Funktion gegeben, welche jedes $i$ auf 0 abbildet. Das Einselement von $R[t]$ wird durch die Funktion gegeben, welche $i = 0$ auf das Einselement 1 von $R$ und $i \neq 0$ auf 0 abbildet. Mit $t$ bezeichnen wir die Funktion, die $i = 1$ auf 1 und $i \neq 1$ auf 0 abbildet.

Wir erhalten auch einen Monomorphismus $\phi : R \to R[t]$, $r \mapsto h_r$ mit $h_r(i) = r\,\delta_{0,i}$ (Kronecker-Delta). Damit kann $R$ als Teilring von $R[t]$ aufgefaßt werden und $R[t]$ wird zu einer $R$-Algebra. Es gilt $\phi(1) = 1$.

**2.2 Definition.** Sei $R$ kommutativer Ring. Die eben definierte $R$-Algebra $R[t]$ zusammen mit dem Element $t$ heißt Polynomring in der Variablen $t$ über $R$. Die Elemente von $R[t]$ heißen Polynome in der Variablen $t$ über $R$.

Zur Veranschaulichung ist es besser, die Elemente von $R[t]$ mittels $t$ auszudrücken. Man sieht aufgrund der Definitionen sofort, daß für $f \in R[t]$ folgendes

gilt: $f = \sum_{i=0}^{n} a_i t^i = \sum_{i=0}^{n} \phi(a_i) t^i$ mit $a_i = f(i) \in R$ und $n \in \mathbb{Z}^{\geq 0}$, so daß $f(j) = 0$ für alle $j > n$. Zwischen $a_i$ und $t^i$ steht hier die äußere Multiplikation. Die obigen Verknüpfungen sind gerade so gemacht, daß sich die erwarteten Rechenregeln für Polynome ergeben.

Zwei Polynome sind genau dann gleich, wenn alle vor den $t^i$ auftretenden Koeffzienten gleich sind. Speziell soll hier hervorgehoben werden, daß Polynome nicht als Funktionen aufgefaßt werden, wie vielleicht aus der Analysis gewohnt. Ist $k$ der endliche Körper mit zwei Elementen, so liefern $t \mapsto 1$ und $t \mapsto t^2 + t + 1$ die gleichen Funktionen $k \to k$, die Polynome 1 und $t^2 + t + 1$ sind aber verschiedene Elemente von $k[t]$.

Wir definieren noch ein paar grundlegene Begriffe im Zusammenhang mit Polynomringen und Polynomen. Die Polynome $t^i$ heißen Monome. Die Polynome $at^i$ heißen Terme. Sei $f \in R[t]$ mit $f = \sum_{i=0}^{n} a_i t^i$. Die $a_i$ heißen die Koeffizienten von $f$. Der Grad von $f$ ist $\deg(f) = \max\{i \mid 0 \leq i \leq n \text{ und } a_i \neq 0\}$. Es gilt insbesondere $\deg(0) = -\infty$ für $0 \in R[t]$. Für $\deg(f) \geq 0$ heißt $a_{\deg(f)}$ Leitkoeffizient von $f$. Der Term $a_{\deg(f)} t^{\deg(f)}$ heißt führender Term von $f$. Der Koeffizient $a_0$ heißt Absolutkoeffizient. Das Polynom $f$ heißt normiert, wenn der Leitkoeffizient gleich 1 ist. Gilt $\deg(f) \leq 0$, so heißt das Polynom konstant. Gilt $\deg(f) = 1$, so heißt das Polynom linear.

Sind $f, g \in R[t]$ so gilt $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ und $\deg(fg) \leq \deg(f) + \deg(g)$ unter Nachverfolgen der führenden Terme und unter Verwendung von „sinnvollen“ Rechenregeln für $-\infty$. Die zweite Ungleichung wird hier zur Gleichung, wenn $R$ nullteilerfrei ist.

**2.3 Satz.** *Sei $R$ ein kommutativer Ring. Der Polynomring $R[t]$ ist genau dann nullteilerfrei, wenn $R$ nullteilerfrei ist. In diesem Fall gilt $R[t]^\times = R^\times$.*

*Beweis.* Ist $R[t]$ nullteilerfrei, so ist auch $R$ als Teilring nullteilerfrei. Sind umgekehrt $f, g \in R[t] \backslash \{0\}$ mit $\deg(f) \geq 1$, so gilt $\deg(fg) = \deg(f) + \deg(g) \geq 1$, also $fg \neq 0$, also ist $R[t]$ mit $R$ nullteilerfrei.

Gilt $fg = 1$, so folgt $\deg(f) + \deg(g) = 0$. Wegen $\deg(f) \geq 0$ und $\deg(g) \geq 0$ gilt $\deg(f) = \deg(g) = 0$, also $f, g \in R$. □

Als Zusatz zur Aussage des Satzes bemerken wir, daß ein Polynom $f \neq 0$, dessen Leitkoeffizient kein Nullteiler ist, ebenfalls kein Nullteiler in $R[t]$ ist, denn es gilt $\deg(fg) = \deg(f) + \deg(g)$ für alle $g \in R[t]$.

In $(\mathbb{Z}/4\mathbb{Z})[t]$ gilt $(2t + 1)^2 = 1$, also $2t + 1 \in (\mathbb{Z}/4\mathbb{Z})[t]^\times$ als Gegenbeispiel zur Aussage 2, falls $R$ nicht nullteilerfrei ist.

Sei $\phi : R \to S$ ein Homomorphismus. Dies macht $S$ wie oben zu einer $R$-Algebra, indem wir die Multiplikation von $r \in R$ mit $x \in S$ durch $rx = \phi(r)x$ definieren. Wir erhalten dann einen $R$-Algebra Homomorphismus $\phi_x : R[t] \to$

$S$ durch die Zuordnung $\phi_x(f) = f(x) = \sum_i a_i x^i$, wo $f = \sum_i a_i t^i \in R[t]$ mit $a_i \in R$ ist. Dieser $R$-Algebra Homomorphismus wird als Einsetzhomomorphismus bezeichnet.

**2.4 Satz** (Universelle Eigenschaft)**.** *Sei $R$ ein kommutativer Ring und $S$ eine kommutative $R$-Algebra mit der folgenden universellen Eigenschaft:*

*$S$ besitze ein Element $x \in S$, so daß für jede kommutative $R$-Algebra $T$ und jedes Element $y \in T$ genau ein $R$-Algebra Homomorphismus $\psi : S \to T$ mit $\psi(x) = y$ existiert.*

*Dann gilt $S \cong R[t]$ als $R$-Algebren.*

*Beweis.* Seien $S_1, S_2$ zwei kommutative $R$-Algebren, die jeweils die universelle Eigenschaft mit $x_1 \in S_1$ und $x_2 \in S_2$ erfüllen. Dann gibt es $R$-Algebra Homomorphismen $\psi_1 : S_1 \to S_2$ mit $\psi_1(x_1) = x_2$ und $\psi_2 : S_2 \to S_1$ mit $f(x_2) = x_1$. Folglich gilt $\psi_2 \circ \psi_1 : S_1 \to S_2$ mit $\psi_2(\psi_1(x_1)) = x_1$ und $\psi_1 \circ \psi_2 : S_2 \to S_2$ mit $\psi_1(\psi_2(x_2)) = x_2$. Da auch die Identitäten auf $S_1$ und $S_2$ diese Eigenschaften haben, folgt aus der Eindeutigkeitsaussage der universellen Eigenschaft, daß $\psi_2 \circ \psi_1 = \mathrm{id}$ und $\psi_1 \circ \psi_2 = \mathrm{id}$, also $S_1 \cong S_2$ als $R$-Algebren gilt.

Die $R$-Algebra $R[t]$ zusammen mit $t \in R[t]$ erfüllt die universelle Eigenschaft: Der Einsetzhomomorphismus $\phi_y : R[t] \to T$, $f \mapsto f(y)$ liefert gerade den gesuchten $R$-Algebra Homomorphismus $\psi : R[t] \to T$. Aufgrund der $R$-Algebra Homomorphieeigenschaft ist auch klar, daß $\psi$ durch die Vorgabe von $t \mapsto y$ eindeutig bestimmt wird.

Erfüllt $S$ die universelle Bedingung, so folgt also $S \cong R[t]$ als $R$-Algebren. □

Man kann die universelle Eigenschaft also als alternative Definition des Polynomrings nehmen. Dann heißt die kommutative $R$-Algebra $S$ zusammen mit dem Element $x \in S$ Polynomring in der Variablen $x$ über $R$. Aus der universellen Eigenschaft folgt wie im Beweis, daß $S$ bis auf $R$-Algebra Isomorphie eindeutig bestimmt ist. Für die Existenz ist aber noch das Konstruktionsverfahren anzugeben.

**2.5 Satz** (Polynomdivision)**.** *Sei $R$ ein kommutativer Ring. Seien $f, g \in R[t]$ und $g$ habe invertierbaren Leitkoeffizienten. Dann gibt es eindeutig bestimmte $q, r \in R[t]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.*

*Beweis.* Beweis induktiv über $\deg(f)$. Für $\deg(f) < \deg(g)$ wähle $q = 0$ und $r = f$. Es gelte jetzt $\deg(f) \geq \deg(g)$. Wähle $c \in R$ mit $\deg(f - ct^{\deg(f)-\deg(g)}g) < \deg(f)$. Dies ist möglich, da der Leitkoeffizient von $g$ invertierbar ist. Induktiv gibt es $q', r \in R[t]$ mit $f - ct^{\deg(f)-\deg(g)}g = q'g + r$ und $\deg(r) < \deg(g)$. Setze $q = q' + ct^{\deg(f)-\deg(g)}$. Dann gilt $f = qg + r$, wie erforderlich.

Zur Eindeutigkeit bildet man die Differenz von $f = q_1 g + r_1$ und $f = q_2 g + r_2$ und erhält $(q_1 - q_2)g = r_1 - r_2$. Da $g$ einen invertierbaren Leitkoeffizienten hat, muß $q_1 - q_2 = 0$ gelten, weil die linke Seite sonst einen Grad $\geq \deg(g) > \deg(r_1 - r_2)$ hätte. Dann folgt aber $r_1 - r_2 = 0$ und die Eindeutigkeit ist bewiesen. □

Bei der Polynomdivision haben wir die Kommutativität von $R$ gar nicht ausgenutzt. Man kann in der Tat Polynomringe und Polynomdivision geeignet für nicht kommutative Ringe definieren. Man muß dann beispielsweise zwischen Links- und Rechtsdivision unterscheiden. In der Vorlesung gehen wir hier aber nicht näher darauf ein.

## 2.2 Polynomringe über Körpern

**2.6 Satz.** *Sei $R$ ein Ring. Dann sind äquivalent:*

(*i*) *$R$ ist ein Körper,*

(*ii*) *$R[t]$ ist ein euklidischer Ring,*

(*iii*) *$R[t]$ ist ein Hauptidealring.*

*Beweis.* $(i) \Rightarrow (ii)$: $R[t]$ ist offenbar ein Integritätsring. Darüberhinaus ist Proposition 2.5 für alle $g \neq 0$ anwendbar, und deg erfüllt die Bedingungen einer euklidischen Gradfunktion. $(ii) \Rightarrow (iii)$: Wurde bereits bewiesen. $(iii) \Rightarrow (i)$: Wir betrachten den Einsetzhomomorphismus $\phi_0 : R[t] \to R$, der durch $t \mapsto 0$ definiert wird. Als Teilring von $R[t]$ ist $R$ selbst Integritätsring. Daher ist $\ker(\phi)$ ein Primideal und als solches im Hauptidealring $R[t]$ maximal. Da $\phi$ surjektiv ist, ist folglich $R \cong R[t]/\ker(\phi)$ ein Körper. □

Aufgrund von Satz 2.6 sehen wir, daß $\mathbb{Z}[t]$ kein Hauptidealring ist. Ein (maximales) Ideal, welches kein Hauptideal ist, wird zum Beispiel durch $2\mathbb{Z}[t] + t\mathbb{Z}[t]$ gegeben. Die Ergebnisse des Abschnitts 2.5 zeigen, daß $\mathbb{Z}[t]$ immerhin ein faktorieller Ring ist, und daß $2, t$ Primelemente in $\mathbb{Z}[t]$ sind.

**2.7 Korollar.** *Sei $K$ ein Körper. Jedes $f \in K[t]\backslash\{0\}$ besitzt eine eindeutige Faktorisierung $f = c\prod p^{n_p}$ mit $c \in K^\times$, normierten irreduziblen $p \in K[t]$ und $n_p \geq 0$.*

**2.8 Korollar.** *Sei $K$ ein Körper und $f \in K[t]$ irreduzibel. Dann ist $K[t]/fK[t]$ ein Körper, welcher $K$ als Teilkörper enthält.*

*Beweis.* Für die letzte Aussage beachten wir $K \cap fK[t] = \{0\}$. Indem wir $K$ dann mit den Klassen $\{x + fK[t] \,|\, x \in K\}$ identifizieren, wird $K$ ein Teilkörper von $K[t]/fK[t]$. □

Mit dem letzten Korollar kann man sich aus gegebenen Körpern neue konstruieren. Diese Methode wird sehr oft verwendet.

## 2.3 Nullstellen von Polynomen

**2.9 Definition.** Sei $R$ kommutativer Ring und $S$ eine kommutative $R$-Algebra. Sei $f \in R[t]$. Ein Element $b \in S$ heißt Nullstelle (oder Wurzel) von $f$ in $S$ wenn $f(b) = 0$ gilt.

**2.10 Satz.** *Sei $R$ ein kommutativer Ring und $f \in R[t]$ vom Grad $n \geq 0$. Für jede Nullstelle $b \in R$ wird $f$ von $t - b$ geteilt.*

*Ist $R$ ein Integritätsring, so besitzt $f$ höchstens $n$ Nullstellen in $R$.*

*Beweis.* Division mit Rest durch $g = t - b$ liefert $q \in R[t]$ und $r \in R$ mit $f = q(t - b) + r$. Daraus folgt $f(b) = r = 0$, folglich ist $f$ durch $t - b$ teilbar. Ist nun $R$ Integritätsring und $a \neq b$ eine weitere Nullstelle von $f$ in $R$, so gilt $f(a) = q(a)(a-b)$ und folglich $q(a) = 0$, da $R$ Integritätsring ist. Wegen $\deg(q) = \deg(f) - 1$ erhält man induktiv, daß es höchstens $n$ Nullstellen von $f$ in $R$ geben kann. □

Die zweite Aussage in Satz 2.10 wird falsch, wenn $R$ kein Integritätsring ist. Als Gegenbeispiel betrachte man $R = \mathbb{Z} \times \mathbb{Z}$. Für das Polynom $f = (t-(1,1))(t-(2,2))$ gilt nämlich auch $f = (t - (1,2))(t - (2,1))$, so daß $f$ vier verschiedene Nullstellen in $R$ hat und darüberhinaus sich nicht eindeutig faktorisieren läßt.

**2.11 Satz.** *Jede endliche Untergruppe $U$ der multiplikativen Gruppe $K^\times$ eines Körpers $K$ ist zyklisch.*

*Beweis.* Sei $n = \#U$ und $m$ der Exponent von $U$. Dann gilt $m \leq n$ und jedes der $n$ Elemente von $U$ ist Nullstelle des Polynoms $t^m - 1$ in $K$. Da $t^m - 1$ nach Satz 2.10 maximal $m$ Nullstellen haben kann, folgt $n = m$. Eine abelsche Gruppe der Ordnung $n$ und des Exponenten $n$ ist jedoch zyklisch. □

Ist $R$ ein Integritätsring, $f \in R[t]$ mit $\deg(f) \geq 0$ und $b \in R$, so gibt es nach wiederholter Anwendung von Satz 2.10 ein eindeutig bestimmtes $m \in \mathbb{Z}^{\geq 1}$ und $g \in R[t]$ mit $f = (t - b)^m g$ und $g(b) \neq 0$.

**2.12 Definition.** Die Zahl $m$ heißt die Vielfachheit von $b$ in $f$. Für $m > 1$ nennen wir $b$ eine mehrfache Nullstelle.

Die Vielfachheit einer Nullstelle kann wie folgt bestimmt werden.

**2.13 Definition.** Die Ableitung des Polynoms $f \in R[t]$ mit $f = \sum_{i=0}^{n} a_i t^i$ ist definiert als $f' = \sum_{i=1}^{n} i a_i t^{i-1}$.

Die Ableitung erfüllt die (üblichen) Rechenregeln $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$, $(af)' = af'$ für $f, g \in R[t]$ und $a \in R$.

**2.14 Satz.** *Sei $R$ ein Integritätsring und $f \in R[t]$ mit $\deg(f) \geq 0$. Das Element $b \in R$ ist mehrfache Nullstelle von $f$ genau dann, wenn $f(b) = 0$ und $f'(b) = 0$.*

*Beweis.* Wir schreiben $f$ wie oben $f = (t-b)^m g$. Durch Ableiten erhalten wir $f' = (x-b)^m g' + m(x-b)^{m-1} g$. Ist $m > 1$ so gilt offenbar $f(b) = 0$ und $f'(b) = 0$. Ist umgekehrt $m = 1$ so gilt $f' = (x-b)g' + g$ und folglich $f'(b) = g(b) \neq 0$. Für $f'(b) = 0$ muß daher $m > 1$ gelten. □

**2.15 Korollar.** *Sei $F$ ein Körper, $K$ ein Teilkörper und $f \in K[t]$ irreduzibel.*

(*i*) *Gilt* $\mathrm{char}(K) = 0$*, so hat $f$ nur einfache Nullstellen in $F$.*

(*ii*) *Gilt* $\mathrm{char}(K) = p > 0$ *und hat $f$ mehrfache Nullstellen in $F$, so ist $f$ von der Form $f = g(t^p)$ mit $g \in K[t]$.*

*Beweis.* (*i*): Wegen $\mathrm{char}(K) = 0$ gilt $f' \neq 0$. Daher folgt aus $\deg(f') < \deg(f)$, daß $\gcd\{f, f'\} = 1$ und somit $1 = \lambda f + \mu f'$ mit geeigneten $\lambda, \mu \in K[t]$ ist. Dies gilt dann auch in $F[t]$, und $f$ und $f'$ haben folglich keine gemeinsamen Nullstellen in $F$. Wegen Satz 2.14 besitzt $f$ also keine mehrfachen Nullstellen in $F$. (*ii*): Es muß $f' = 0$ gelten, da sonst wie eben $\gcd\{f, f'\} = 1$ wäre und es keine mehrfachen Nullstellen in $F$ geben könnte. Wegen $f' = 0$ können die Monome in $f$ nur durch $p$ teilbare Exponenten haben. Also ist $f$ von der Gestalt $f = g(t^p)$. □

Ist $R$ ein Integritätsring mit $\mathrm{char}(R) = p$ und hat das Polynom $f = t^p - c$ eine Nullstelle $b \in R$, so gilt $f = t^p - b^p = (t-b)^p$. Also hat $f$ genau eine Nullstelle, und die mit Vielfachheit $p$.

## 2.4 Basissatz von Hilbert

**2.16 Satz.** *Sei $R$ ein kommutativer Ring. Der Polynomring $R[t]$ ist genau dann noethersch, wenn $R$ noethersch ist.*

*Beweis.* Sei $R[t]$ noethersch und $I$ ein Ideal von $R$. Das von $I$ in $R[t]$ erzeugte Ideal $J$ ist nach Voraussetzung endlich erzeugt, $J = \sum_{i=1}^{n} R[t] f_i$ mit geeigneten $f_i \in R[t]$. Dann gilt auch $I = \sum_{i=1}^{n} R f_i(0)$ und $I$ ist ebenfalls endlich erzeugt.

Sei nun $R$ noethersch und $J$ ein Ideal von $R[t]$. Wir weisen die Existenz einer endlichen Menge $M \subseteq J$ mit der folgenden Eigenschaft nach: Für jedes $f \in J$ mit $f \neq 0$ gibt es $e \in \mathbb{Z}^{\geq 0}$, $\lambda_1, \ldots, \lambda_n \in R$ und $f_1, \ldots, f_n \in M$ mit

$$\deg\Big(f - t^e \sum_{i=1}^{n} \lambda_i f_i\Big) < \deg(f). \tag{2.17}$$

Wenn wir dies iteriert $\deg(f) + 1$ mal anwenden, reduzieren wir $f$ modulo dem Ideal $R[t]M$ zu Null. Daraus folgt $f \in R[t]M$, also $J = R[t]M$ und $J$ ist endlich erzeugt.

Sei $J_i = \{f \in J \mid \deg(f) \leq i\}$ und $I_i = \{a_i \mid \sum_{j=0}^{i} a_j t^j \in J_i\}$ für $i \in \mathbb{Z}^{\geq 0}$. Da $J_i$ additiv und unter Multiplikation mit Elementen aus $R$ abgeschlossen ist, handelt es sich bei $I_i$ um ein Ideal von $R$. Wegen $tJ_i \subseteq J_{i+1}$ gilt $I_i \subseteq I_{i+1}$. Da $R$ noethersch ist, gibt es $m \in \mathbb{Z}^{\geq 0}$ mit $I_i = I_m$ für alle $i \geq m$ und die $I_0, \ldots, I_m$ sind jeweils endlich erzeugt. Für $0 \leq i \leq m$ gibt es daher endliche Mengen $M_i \subseteq J_i$ derart, daß die Leitkoeffizienten der Polynome eines jeden $M_i$ die zugehörigen Leitkoeffizientenideale $I_i$ erzeugen. Wir setzen $M = \cup_{i=0}^{m} M_i$. Aufgrund der Konstruktion von $M$ und wegen $I_i = I_m$ für $i \geq m$ sieht man direkt, daß jeder führende Term eines $f \in J$ als führender Term eines Polynoms der Form $t^e \sum_{i=0}^{n} \lambda_i f_i$ mit $e \in \mathbb{Z}^{\geq 0}$, $\lambda_i \in R$ und $f_i \in M$ auftritt, daß also (2.17) gilt. □

Der Basissatz von Hilbert liefert eine reine Existenzaussage für endliche Erzeugendensysteme von Idealen, jedoch kein sinnvolles Verfahren, wie diese zu konstruieren sind. Als Hilbert diesen Satz Ende des 19. Jahrhunderts bewies, sorgte dieser auch aufgrund seiner nicht konstruktiven Natur für erhebliches Aufsehen. Die Invariantentheorie war zu dieser Zeit ein großes und wichtiges Forschungsgebiet in der Mathematik und man schlug sich darin mit der expliziten Berechnung von Erzeugern gewisser Ideale herum. Von Gordan, einem Hauptvertreter der Invariantentheorie, stammt die Aussage, es handele sich beim Basissatz von Hilbert nicht um Mathematik, sondern um Theologie. In der Folge wurde die Axiomatisierung der Algebra vorangetrieben und man gewöhnte sich an formale, nicht konstruktive Beweise.

## 2.5 Satz von Gauß

Sei $R$ ein faktorieller Ring. Wir wollen im folgenden das Faktorisierungsverhalten von Polynomen aus $R[t]$ über dem Quotientenkörper $K = \mathrm{Quot}(R)$ von $R$ und über $R$ selbst untersuchen. Als Hilfsmittel verwenden wir dazu Bewertungen.

Wir beginnen zuerst mit einer allgemeinen Aussage.

**2.18 Proposition.** *Sei $\phi : R \to S$ ein Homomorphismus der kommutativen Ringe $R$ und $S$. Dann läßt sich $\phi$ zu einem Homomorphimus $\psi : R[t] \to S[t]$ fortsetzen, welcher durch koeffizientenweise Anwendung von $\phi$ definiert ist. Ist $\phi$ surjektiv, so ist auch $\psi$ surjektiv. Ferner gilt* $\ker(\psi) = \ker(\phi)R[t]$.

*Beweis.* Kann man direkt nachrechnen. Eine andere Argumentation ist die folgende. Wir verknüpfen $\phi$ mit dem Einbettungshomomorphismus $S \to S[t]$ und erhalten so $S[t]$ als $R$-Algebra. Der Einsetzhomomorphismus $\phi_t : R[t] \to S[t]$ wendet dann $\phi$ koeffizientenweise auf die Elemente von $R[t]$ an. Wir setzen also $\psi = \phi_t$. Die Aussagen über die Surjektivität und den Kern sind dann klar. □

**2.19 Proposition.** *Sei $R$ ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Durch koeffizientenweise Reduktion erhält man einen Epimorphismus $\phi : R[t] \to (R/\mathfrak{a})[t]$. Folglich gilt $R[t]/\mathfrak{a}R[t] \cong (R/\mathfrak{a})[t]$ und $\mathfrak{a}R[t]$ ist genau dann ein Primideal in $R[t]$, wenn $\mathfrak{a}$ ein Primideal in $R$ ist.*

*Beweis.* Folgt aus Proposition 2.18, angewendet auf den Reduktionshomomorphismus $R \to R/\mathfrak{a}$, und dem Homomorphiesatz. Ferner gilt, daß $\mathfrak{a}R[t]$ genau dann Primideal ist, wenn $R[t]/\mathfrak{a}R[t]$ ein Integritätsring ist, und daß $\mathfrak{a}$ genau dann Primideal ist, wenn $R/\mathfrak{a}$ und damit $(R/\mathfrak{a})[t]$ ein Integritätsring ist. Die bereits bewiesene Isomorphie liefert daher die zu beweisende Äquivalenz. □

Wir kommen nun zu den Bewertungen. Sei $P$ ein Repräsentantensystem der Primelemente von $R$. Jedes $x \in R\backslash\{0\}$ besitzt eine eindeutige Faktorisierung $x = \varepsilon \prod_{p \in P} p^{n_p}$, wobei $\varepsilon \in R^\times$ sowie $n_p \in \mathbb{Z}^{\geq 0}$ mit $n_p = 0$ für fast alle $p \in P$. Wir setzen $v_p(x) = n_P$ und $v_P(0) = \infty$ und erhalten damit für jedes $p \in P$ eine Abbildung $v_p : R \to \mathbb{Z} \cup \{\infty\}$. Für $x, y \in R$ gilt dann offenbar $v_p(xy) = v_p(x) + v_p(y)$ und $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ unter Beachtung „sinnvoller“ Rechenregeln mit $\infty$. Dies motiviert die folgende, allgemeine Definition.

**2.20 Definition.** Sei $R$ ein Integritätsring. Unter einer (nicht-archimedischen, exponentiellen) Bewertung auf $R$ verstehen wir eine Abbildung $v : R \to \mathbb{R} \cup \{\infty\}$ mit den folgenden Eigenschaften für alle $x, y \in R$.

(*i*) $v(x) = \infty$ genau dann, wenn $x = 0$,

(*ii*) $v(xy) = v(x) + v(y)$,

(*iii*) $v(x + y) \geq \min\{v(x), v(y)\}$.

Ein weiteres Beispiel einer Bewertung wird durch die negierte Gradfunktion $-\deg$ auf $R[t]$ gegeben.

Normalerweise betrachtet man solche Bewertungen für den Fall, daß $R$ ein Körper ist. Daher ist das folgende Lemma nützlich.

**2.21 Lemma.** *Eine Bewertung auf dem Integritätsring $R$ läßt sich auf eindeutige Weise auf $K = \mathrm{Quot}(R)$ fortsetzen.*

*Beweis.* Man definiert $v(x/y) = v(x) - v(y)$. Die Bedingungen $(i)$-$(iii)$ ergeben sich durch direktes Nachrechnen. Die Eindeutigkeit ergibt sich auch Bedingung $(ii)$: Für $v(x/y)$ muß gelten: $v(x/y) + v(y) = v(x)$, wodurch $v(x/y)$ eindeutig festgelegt wird. □

Ist $R$ ein faktorieller Ring, so erhalten wir nun durch die Fortsetzung der $v_p$ auf $K$ für jedes $x \in K^\times$ eine eindeutige Faktorisierung $x = \varepsilon \prod_{p \in P} p^{v_p(x)}$ mit geeignetem $\varepsilon \in R^\times$. Für nicht faktorielle Ringe kann man sich die Bewertungen $v$ als Exponenten in verallgemeinerten Faktorisierungen vorstellen.

**2.22 Definition.** Sei $v$ eine Bewertung auf einem Körper $K$.

$(i)$ Die Menge $R_v = \{x \in K \mid v(x) \geq 0\}$ heißt Bewertungsring von $v$.

$(ii)$ Die Menge $\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}$ heißt Bewertungsideal von $v$.

**2.23 Lemma.** *Der Bewertungsring $R_v$ ist ein Ring und das Bewertungsideal $\mathfrak{p}_v$ ist ein Primideal in $R_v$.*

*Beweis.* Die Aussagen ergeben sich unmittelbar aus $(i)$-$(iii)$. □

Man kann darüberhinaus zeigen, daß $\mathfrak{p}_v$ das einzige Primideal von $R_v$ und somit maximal ist. Außerdem sind genau die Elemente in $R_v \backslash \mathfrak{p}_v$ Einheiten in $R_v$, kurz $R_v$ ist ein lokaler Ring. Wir benötigen diese Aussagen für das folgende aber nicht.

**2.24 Satz.** *Eine Bewertung $v$ des Integritätsrings $R$ läßt sich zu einer Bewertung $w$ auf $R[t]$ durch $w(f) = \min_i v(a_i)$ für $f = \sum_i a_i t^i \in R[t]$ fortsetzen.*

*Beweis.* Die Bedingungen $(i)$ und $(iii)$ aus Definition 2.20 ergeben sich direkt aus der Definition von $w$: Es gilt $w(f) = \infty$ genau dann, wenn alle $v(a_i) = \infty$, also $f = 0$. Für $g = \sum_i b_i t^i$ sehen wir weiterhin $w(f+g) = \min_i v(a_i + b_i) \geq \min_i \min\{v(a_i), v(b_i)\} = \min\{\min_i v(a_i), \min_i v(b_i)\} = \min\{w(f), w(g)\}$. Bedingung $(ii)$ ist der Inhalt des nachfolgenden Lemmas von Gauß. □

**2.25 Lemma** (Gauß)**.** *Für alle $f, g \in R[t]$ gilt $w(fg) = w(f) + w(g)$.*

*Beweis.* Die Aussage gilt im Falle $f = 0$ oder $g = 0$. Wir nehmen daher $f \neq 0$ und $g \neq 0$ an. Wir setzen $v$ auf $K = \mathrm{Quot}(R)$ fort und betrachten die Situation in $K[t]$. Allgemein gilt $w(ch) = v(c) + w(h)$ für $c \in K$ und $h \in K[t]$. Wir verwenden dies für die folgende Normierung. Seien $r, s$ diejenigen Indizes, für die $w(f) = v(a_r)$

und $w(g) = v(b_s)$ gilt, wobei $g = \sum_i b_i t^i$. Wir setzen $\tilde{f} = f/a_r$ und $\tilde{g} = g/b_s$. Die Ungleichung $v(a_i/a_r) = v(a_i) - v(a_r) \geq 0$ ist scharf. Daher gilt $w(\tilde{f}) = 0$ und analog $w(\tilde{g}) = 0$. Zum Beweis des Lemmas genügt nun also $w(\tilde{f}\tilde{g}) = 0$ zu zeigen, da hieraus $w(fg) = w(a_r\tilde{f}b_s\tilde{g}) = v(a_rb_s) + w(\tilde{f}\tilde{g}) = v(a_rb_s) + w(\tilde{f}) + w(\tilde{g}) = v(a_r) + v(b_s) + w(\tilde{f}) + w(\tilde{g}) = w(a_r\tilde{f}) + w(b_s\tilde{g}) = w(f) + w(g)$ folgt.

Offenbar gilt $\tilde{f}, \tilde{g} \in R_v[t]$. Sei $\phi : R_v[t] \to (R_v/\mathfrak{p}_v)[t]$ wie in Proposition 2.19 der Homomorphismus, der die Koeffizienten reduziert. Für $h \in R_v[t]$ gilt $w(h) = 0$ genau dann, wenn $\phi(h) \neq 0$. Wir haben also $\phi(\tilde{f}) \neq 0$ und $\phi(\tilde{g}) \neq 0$. Da $(R_v/\mathfrak{p}_v)[t]$ mit $R_v/\mathfrak{p}_v$ ein Integritätsring ist, ergibt sich $\phi(\tilde{f}\tilde{g}) = \phi(\tilde{f})\phi(\tilde{g}) \neq 0$ und daraus $w(\tilde{f}\tilde{g}) = 0$. □

**2.26 Satz.** *Sei $V$ eine Menge von Bewertungen des Körpers $K$ und $R = \cap_{v\in V} R_v$. Sei $f \in R[t]$ normiert. Sind $g, h \in K[t]$ normiert mit $f = gh$, so gilt $g, h \in R[t]$.*

*Beweis.* Wir setzen $v \in V$ wie in Satz 2.24 zur Bewertung $w$ auf $K[t]$ fort. Dann gilt $w(f) = 0$, $w(g), w(h) \leq 0$ und $w(f) = w(g) + w(h)$. Es folgt $w(g) = w(h) = 0$, also $g, h \in R_v[t]$. Da dies für jedes $v \in V$ gilt, ergibt sich $g, h \in R[t]$. □

Satz 2.26 ist ein Beispiel für das Lokal-Global Prinzip. Der Ring $R$ wird global durch alle $v \in V$ definiert. Wir beweisen die Aussage lokal, daß heißt bezüglich $R_v$ für jedes $v \in V$ einzeln, und können dann durch Kombination der lokalen Aussagen die globale Aussage für $R$ erhalten.

Nach diesen allgemeinen Überlegungen kehren wir nun zu dem Fall zurück, daß $R$ faktoriell ist.

**2.27 Korollar.** *Sei $R$ faktoriell, $K = \mathrm{Quot}(R)$ und $f \in R[t]$ normiert. Sind $g, h \in K[t]$ normiert mit $f = gh$, so gilt $g, h \in R[t]$.*

*Beweis.* Sei $V = \{v_p \,|\, p \in P\}$ die Menge der auf $K$ fortgesetzten Bewertungen $v_p$. Für $x \in K$ gilt dann $x \in R$ genau dann, wenn $v_p(x) \geq 0$ für alle $p \in P$. Dies heißt $R = \cap_{v\in V} R_v$. Die Aussage folgt nun mit Satz 2.26. □

Das Faktorisierungsverhalten normierter Polynome in $R[t]$ entspricht also dem in $K[t]$. Wir wenden uns jetzt auch nicht normierten Polynomen zu. Wir bezeichnen mit $w_p$ die Fortsetzungen von $v_p$ auf $K[t]$ wie oben.

**2.28 Definition.** Der Inhalt $I(f)$ eines Polynoms $f \in K[t]\backslash\{0\}$ ist definiert als $I(f) = \prod_{p\in P} p^{w_p(f)}$. Das Polynom $f$ heißt primitiv, wenn $I(f) = 1$ ist.

Der Inhalt von $f$ ist offenbar gleich dem größten gemeinsamen Teiler der Koeffizienten von $f$. Ferner gilt $f \in R[t]$ genau dann, wenn $I(f) \in R$. Aus Lemma 2.25 folgt $I(fg) = I(f)I(g)$. Ähnlich wie im Beweis von Satz 2.24 können wir jedes

Polynom $f \in R[t]\backslash\{0\}$ primitiv machen, indem wir seinen Inhalt $I(f)$ herausdividieren: Das Polynom $\tilde{f} = f/I(f)$ liegt in $R[t]$ und ist primitiv. Wir bemerken, daß $I(f)$ und $\tilde{f}$, aber nicht jedoch die Eigenschaft, primitiv zu sein, von der Wahl von $P$ abhängen.

**2.29 Satz** (Gauß)**.** *Sei $R$ kommutativ. Dann ist $R[t]$ genau dann faktoriell, wenn $R$ faktoriell ist. In diesem Fall bestehen die Primelemente von $R[t]$ genau aus den Primelementen von $R$ und den primitiven Polynomen in $R[t]$, welche in $K[t]$ für $K = \mathrm{Quot}(R)$ irreduzibel sind.*

*Beweis.* Ist $R[t]$ faktoriell, so muß auch $R$ faktoriell sein, denn da $R[t]$ nullteilerfrei ist, enthält jede Faktorisierung von Elementen aus $R$ in Primelemente aus $R[t]$ nur solche Faktoren, welche aus $R$ stammen. Diese Faktoren sind auch Primelemente von $R$.

Sei nun umgekehrt $R$ faktoriell. Die Primelemente von $R$ bleiben prim in $R[t]$. Ist nämlich $p$ ein solches, so ist $R/pR$ und damit auch $R[t]/pR[t] \cong (R/p)[t]$ unter Verwendung von Proposition 2.19 ein Integritätsring.

Sei nun $q \in R[t]$ primitiv und irreduzibel in $K[t]$. Wir wollen zeigen, daß $q$ Primelement ist. Seien $f, g \in R[t]$, so daß $q \mid fg$ gilt. Da $q$ Primelement in $K[t]$ ist, gibt es $h \in K[t]$, so daß etwa $f = qh$ gilt. Mit Lemma 2.25 sehen wir $I(q)I(h) = I(f) \in R$. Wegen $I(q) = 1$ folgt also $I(h) \in R$ und somit $h \in R[t]$. Daher gilt $q \mid f$ in $R[t]$.

Sei $f \in R[t]\backslash\{0\}$. Gilt $\deg(f) = 0$, so faktorisiert $f$ bereits in $R$ in Primelemente, und dies ist auch eine Faktorisierung in $R[t]$ in Primelemente. Gelte nun $\deg(f) \geq 1$. Wir wollen zeigen, daß $f$ in die bereits diskutierten Primelemente von $R[t]$ faktorisiert. Wir schreiben zunächst $f = a\tilde{f}$ mit $a = I(f)$ und $\tilde{f} \in R[t]$. Das Element $a$ faktorisiert in $R$, und dies liefert auch eine Faktorisierung in Primelemente in $R[t]$. Sei $\tilde{f} = c\prod_i \tilde{f}_i$ eine Faktorisierung in irreduzible Polynome in $K[t]$. Wir können durch geeignete Skalierung mit dem Inhalt annehmen, daß die $\tilde{f}_i$ primitiv sind und somit auch in $R[t]$ liegen. Da $\tilde{f}$ ebenfalls primitiv ist, folgt durch Anwendung von $I(\cdot)$ und aus der Multiplikativität von $I(\cdot)$, daß $c \in R^\times$ gilt. Daher faktorisiert $\tilde{f}$ in die Primelemente $c\tilde{f}_1$ und $\tilde{f}_i$ aus $R[t]$ für $i > 1$. □

Beispiele für Primelemente in $\mathbb{Z}[t]$ sind $t$, $-t$, $t+3$, $2t-1$, $t^2-3$, $5t^2-2$, ....

## 2.6 Irreduzibilität von Polynomen

Es ist im allgemeinen nicht einfach, die Irreduzibilität eines Polynoms festzustellen oder seine Faktorisierung anzugeben. Es gibt keine expliziten Formeln, mit denen diese Fragen direkt beantwortet werden könnten, und man greift daher

auf Algorithmen bzw. Rechenverfahren zurück. Die Entwicklung solcher Algorithmen ist ein Forschungsgebiet der Computeralgebra. Im folgenden geben wir zwei Irreduzibilitätskriterien an und beschreiben die Faktorisierungsmethode von Kronecker für Polynome über $\mathbb{Z}$.

**2.30 Satz** (Reduktionssatz)**.** *Sei $\phi : R \to S$ ein Homomorphismus der Integritätsringe $R$ und $S$ und $\psi : R[t] \to S[t]$ seine Fortsetzung wie in Proposition 2.18. Sei $f \in R[t]$ mit $\deg(\psi(f)) = \deg(f)$ und $\psi(f)$ irreduzibel in $S[t]$. Sind dann $g, h \in R[t]$ mit $f = gh$, so folgt $g \in R$ oder $h \in R$.*

*Beweis.* Es gilt $\deg(g) + \deg(h) = \deg(f) = \deg(\psi(f)) = \deg(\psi(g)) + \deg(\psi(h))$. Wegen $\deg(\psi(f)) \leq \deg(f)$ und $\deg(\psi(g)) \leq \deg(g)$ ergibt sich $\deg(\psi(f)) = \deg(f)$ und $\deg(\psi(g)) = \deg(g)$. Es ist daher nicht möglich, daß $\deg(g) \geq 1$ und $\deg(h) \geq 1$ gilt, weil sonst $\psi(f)$ das Produkt zweier nicht konstanter Polynome und somit nicht irreduzibel wäre. □

Als Beispiel betrachten wir das Polynom $f = t^3 + 6t^2 + 8t + 4 \in \mathbb{Z}[t]$ und den Reduktionshomomorphismus $\phi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. Es gilt $\psi(f) = t^3 - t + 1 \in (\mathbb{Z}/3\mathbb{Z})[t]$. Da $\psi(f)$ keine Nullstelle in $\mathbb{Z}/3\mathbb{Z}$ besitzt, ist es irreduzibel. Folglich ist auch $f$ irreduzibel.

Dieses Beispiel könnte den Gedanken nahelegen, daß es für jedes irreduzible Polynom $f \in \mathbb{Z}[t]$ eine Primzahl $p$ gäbe, so daß $\psi(f) \in (\mathbb{Z}/p\mathbb{Z})[t]$ irreduzibel wäre. Dies ist jedoch nicht richtig. Das Polynom $f = t^4 - 16t^2 + 4$ ist irreduzibel in $\mathbb{Z}[t]$ und faktorisiert beispielsweise modulo jeder Primzahl entweder in zwei irreduzible Polynome vom Grad zwei oder vier Linearfaktoren. Der Beweis dieses Faktorisierungsverhaltens kann unter Verwendung der Galoistheorie geführt werden.

Satz 2.30 kann jedoch auch nutzbringend eingesetzt werden, wenn $\psi(f)$ nicht unbedingt als irreduzibel vorausgesetzt wird, sondern wenn nur Geeignetes über die möglichen Zerlegungen von $\psi(f)$ bekannt ist. Dieser Ansatz wird in dem folgenden Satz benutzt.

**2.31 Satz** (Irreduzibilitätskriterium von Eisenstein)**.** *Sei $R$ ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ein primitives Polynom. Gibt es ein Primelement $p \in R$ mit $p \mid a_i$ für $0 \leq i \leq n-1$, $p \nmid a_n$ und $p^2 \nmid a_0$, so ist $f$ irreduzibel in $K[t]$ mit $K = \mathrm{Quot}(R)$.*

*Beweis.* Wir nehmen an, daß $f$ nicht irreduzibel ist. Wegen der Primitivität von $f$ gibt es dann nach Satz 2.29 Polynome $g, h \in R[t]$ mit $f = gh$, $\deg(g) \geq 1$ und $\deg(h) \geq 1$. Sei $S = R/pR$ und $\psi : R[t] \to S[t]$ der koeffizientenweise Reduktionshomomorphismus. Weil $p$ prim ist, ist $S$ ein Integritätsring. Wegen $p \nmid a_n$ gilt nun $\deg(\psi(g)) = \deg(g)$ und $\deg(\psi(h)) = \deg(h)$ wie im Beweis von

Satz 2.30. Wegen $p \mid a_i$ gilt weiterhin $\psi(f) = \psi(a_n)t^n = \psi(g)\psi(h)$. Sei $K = \mathrm{Quot}(S)$. Da $K[t]$ faktoriell ist, sind $\psi(g)$ und $\psi(h)$ von der Form $\psi(g) = bt^r$ und $\psi(h) = ct^s$ mit $b, c \in S$. Wegen $r, s \geq 1$ ist dann $\psi(g)(0) = \psi(h)(0) = 0$, also $p \mid g(0)$ und $p \mid h(0)$. Damit ist $p^2$ ein Teiler von $g(0)h(0) = f(0) = a_0$, im Widerspruch zur Voraussetzung. □

Satz 2.31 kann zum Beispiel auf die Polynome $f = t^n - p \in \mathbb{Z}[t]$ und $g = t^{p-1} + \cdots + t + 1 \in \mathbb{Z}[t]$ angewendet werden, wo $n \geq 1$ und $p$ eine Primzahl ist. Für $g$ benötigt man allerdings zuerst noch einen Trick. Als Hinweis betrachte man $g = (t^p - 1)/(t - 1)$ und die durch $t \mapsto t + 1$ definierte Abbildung.

Wir beschreiben nun das Verfahren von Kronecker zur Faktorisierung von Polynomen über $\mathbb{Z}$. Nach Satz 2.29 können wir uns dabei auf primitive Polynome beschränken.

**2.32 Proposition.** *Sei $K$ ein Körper. Sind $a_0, \ldots, a_n \in K$ paarweise verschieden und $b_0, \ldots, b_n \in K$, so gibt es ein eindeutig bestimmtes Polynom $f \in K[t]$ mit $\deg(f) \leq n$ und $f(a_i) = b_i$ für $0 \leq i \leq n$.*

*Beweis.* Zum Beweis der Eindeutigkeit sei $g \in K[t]$ ein weiteres Polynom mit $g(a_i) = b_i$. Wir setzen $h = f - g$. Dann gilt $\deg(h) \leq n$ und $h(a_i) = 0$ für $0 \leq i \leq n$. Nach Satz 2.10 muß dann $h = 0$ gelten. Für die Existenz verwenden wir den Chinesischen Restsatz. Die Polynome $t - a_i$ sind irreduzibel und paarweise koprim. Daher gibt es ein $g \in K[t]$ mit $g \equiv b_i \bmod (t - a_i)$ und folglich $g(a_i) = b_i$ für $0 \leq i \leq n$. Wir können das gesuchte $f$ mit $\deg(f) \leq n$ dann als den Rest der Division von $g$ durch $\prod_{i=0}^{n}(t - a_i)$ definieren. □

Die Berechnung des Polynoms $f \in K[t]$ kann mit dem Lagrangeschen Interpolationspolynom oder dem Newtonschen Interpolationsverfahren erfolgen.

Sei nun $f \in \mathbb{Z}[t]$ primitiv und $g, h \in \mathbb{Z}[t]$ mit $f = gh$. Dann ist $g = \pm 1$ oder $\deg(g) \geq 1$. Für paarweise verschiedene $a_i \in \mathbb{Z}$ mit $0 \leq i \leq \deg(g)$ gilt $f(a_i) = g(a_i)h(a_i)$, also $g(a_i) \mid f(a_i)$. Das Polynom $g$ ist durch die Werte $g(a_i)$ eindeutig bestimmt. Sind die $f(a_i) \neq 0$, so gibt es für $g(a_i)$ nur endlich viele Möglichkeiten. Hieraus ergibt sich folgende Strategie, um alle Teiler von $f$ vom Grad $r$ zu bestimmen:

1. Bestimme paarweise verschiedene $a_0, \ldots, a_r \in \mathbb{Z}$ mit $f(a_i) \neq 0$.
2. Berechne $B = \{(b_i) \in \mathbb{Z}^{r+1} : b_i \mid f(a_i) \text{ für } 0 \leq i \leq r\}$.
3. Konstruiere $g \in \mathbb{Q}[t]$ für jedes $(b_i) \in B$ unter Benutzung von Proposition 2.32.
4. Teste $\deg(g) = r$, $g \in \mathbb{Z}[t]$ und $g \mid f$.

Es ist klar, daß dies ein endliches Verfahren zur Faktorisierung von primitiven Polynomen über $\mathbb{Z}$ liefert:

1. Ist $f \neq \pm 1$, so gibt es nichts (mehr) zu tun.
2. Bestimme einen Teiler $g \neq \pm 1$ von $f$ kleinsten Grades.
3. Setze $f \leftarrow f/g$ und fahre mit 1. fort.

Der Teiler in Schritt 2 ist wegen der Minimalität irreduzibel. Gegebenenfalls verwendet man aus Normierungsgründen nur Teiler $g$ mit positiven Leitkoeffizienten.

Als einfaches Beispiel betrachten wir $f = t^3 - 15t^2 + 71t - 105$ und wollen alle Linearfaktoren in $f$ bestimmen. Da $f$ normiert ist, müssen die Linearfaktoren ebenfalls normiert sein. Durch Auswertung bei $t = 0$ ersehen wir, daß nur $t - b$ mit $b \mid 105$ in Frage kommen kann. Wir haben $105 = 3 \cdot 5 \cdot 7$. Nachrechnen ergibt, daß $f(3) = f(5) = f(7) = 0$ ist. Also gilt $f = (t-3)(t-5)(t-7)$.

Abschließend bemerken wir, daß sich das Verfahren von Kronecker rekursiv zur Faktorisierung von Polynomen über $\mathbb{Z}[t_1, \ldots, t_n]$ und den entsprechenden Quotientenkörpern verallgemeinern läßt.

Moderne Algorithmen zur Polynomfaktorisierung verwenden andere, effizientere Ansätze als das Verfahren von Kronecker.

## 2.7 Multivariate Polynomringe

Sei $R$ ein kommutativer Ring. Iterieren wir die Konstruktion eines univariaten Polynomrings, so erhalten wir multivariate Polynomringe.

**2.33 Definition.** Sei $R$ ein kommutativer Ring und $n \in \mathbb{Z}^{\geq 0}$. Die $R$-Algebra $R[t_1] \cdots [t_n]$ zusammen mit den Elementen $t_1, \ldots, t_n$ heißt Polynomring in den $n$ Variablen $t_1, \ldots, t_n$ über $R$. Wir verwenden die Schreibweise $R[t_1, \ldots, t_n]$.

Die Elemente von $R[t_1, \ldots, t_n]$ heißen Polynome in den Variablen $t_1, \ldots, t_n$ über $R$.

Jedes Element $f \in R[t_1, \ldots, t_n]$ läßt sich in der Form

$$f = \sum_{i_1, \ldots, i_n = 0}^{m} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

mit eindeutig bestimmten $a_{i_1, \ldots, i_n} \in R$ schreiben. Die Polynome $x_1^{i_1} \cdots x_n^{i_n}$ heißen Monome, die Polynome $a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$ heißen Terme und die $a_{i_1, \ldots, i_n}$ heißen die Koeffizienten von $f$. Man kann jetzt verschiedene Gradfunktionen definieren. Zu Gewichten $w_1, \ldots, w_n$ kann man beispielsweise $\deg(x_1^{e_1} \cdots x_n^{e_n}) = \sum_i w_i e_i$ setzen und diese Gradfunktion per Maximumsbildung auf $R[t_1, \ldots, t_n]$ fortsetzen. Man erhält den sogenannten Totalgrad für $w_i = 1$. Polynomdivision bezüglich dieser allgemeinerer Gradfunktionen ist im allgemeinen jedoch nicht mehr möglich, wenn

nicht alle $w_i$ bis auf ein $w_j$ gleich Null sind. Ein Polynom $f$ heißt homogen vom Grad $d$, wenn alle darin auftretenden Terme der gleichen Totalgrad $d$ haben.

Die Aussagen über univariate Polynomringe übertragen sich iterativ auf multivariate Polynomringe, soweit keine speziellen Annahmen über $R$ getroffen wurden, die sich nicht induktiv fortsetzen.

**2.34 Satz.** *Sei $R$ kommutativer Ring.*

1. *$R[t_1, \ldots, t_n]$ ist genau dann nullteilerfrei, wenn $R$ nullteilerfrei ist. In diesem Fall gilt $R[t_1, \ldots, t_n]^\times = R^\times$.*

2. *Sei $S$ eine kommutative $R$-Algebra mit der folgenden universellen Eigenschaft:*

   *$S$ besitze Elemente $x_1, \ldots, x_n \in S$, so daß für jede kommutative $R$-Algebra $T$ und Elemente $y_1, \ldots, y_n \in T$ genau ein $R$-Algebra Homomorphismus $\psi : S \to T$ mit $\psi(x_i) = y_i$ für alle $1 \leq i \leq n$ existiert.*

   *Dann gilt $S \cong R[t_1, \ldots, t_n]$ als $R$-Algebren.*

3. *$R[t_1, \ldots, t_n]$ ist genau dann noethersch, wenn $R$ noethersch ist.*

4. *$R[t_1, \ldots, t_n]$ ist genau dann faktoriell, wenn $R$ faktoriell ist.*

*Beweis.* Per Induktion unter Verwendung der entsprechenden Aussagen für den univariaten Fall. □

Die Homomorphismen $\psi$ aus Aussage 2 heißen wieder Einsetzhomomorphismen. Ist $S$ eine $R$-Algebra, $f \in R[t_1, \ldots, t_n]$ und sind $y_1, \ldots, y_n \in S$, so schreiben wir $f(y_1, \ldots, y_n)$ für das Bild von $f$ unter dem durch $t_i \mapsto y_i$ definierten Einsetzhomomorphismus $R[t_1, \ldots, t_n] \to S$. Gilt $f(y_1, \ldots, y_n) = 0$, so nennen wir $(y_1, \ldots, y_n)$ eine Nullstelle von $f$ in $S$. Für $n > 1$ entsprechen Nullstellen von $f$ in $R$ keinen besonderen Faktoren von $f$, wie das bei $n = 1$ und Linearfaktoren der Fall ist.

Lineare Abbildungen von $k$-Vektorräumen können durch Angabe der Werte auf einer Basis (über $k$ linear unabhängiges Erzeugendensystem) eindeutig definiert werden. Die Situation hier ist ganz analog: $R$-Algebra Homomorphismen mit Definitionsbereich $R[t_1, \ldots, t_n]$ und Bildbereich eine $R$-Algebra können durch die Angabe der Werte auf $t_1, \ldots, t_n$ eindeutig definiert werden. Der von $R$ und den $t_1, \ldots, t_n$ erzeugte Teilring von $R[t_1, \ldots, t_n]$ ist bereits ganz $R[t_1, \ldots, t_n]$. Die $t_1, \ldots, t_n$ bilden daher ein „Erzeugendensystem von $R[t_1, \ldots, t_n]$ über $R$“. Für ein Polynom $f = \sum_{i_1, \ldots, i_n = 0}^{m} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n} \in R[t_1, \ldots, t_n]$ mit $f = 0$ folgt, daß alle $a_{i_1, \ldots, i_n} = 0$ sind. In diesem Sinn sind die $t_1, \ldots, t_n$ also auch „über $R$ algebraisch unabhängig“. Dies motiviert folgende Definition.

**2.35 Definition.** Sei $R$ ein kommutativer Ring und $S$ eine kommutative $R$-Algebra. Die Elemente $y_1, \ldots, y_n \in S$ heißen algebraisch unabhängig über $R$, wenn der Einsetzhomomorphimus $\psi : R[t_1, \ldots, t_n] \to S$ mit $\psi(t_i) = y_i$ injektiv ist.

Für algebraisch unabhängige $y_1, \ldots, y_n \in S$ und den Einsetzhomomorphismus $\psi : R[t_1, \ldots, t_n] \to S$ mit $\psi(t_i) = y_i$ ist $\psi(R[t_1, \ldots, t_n])$ eine zu $R[t_1, \ldots, t_n]$ isomorphe $R$-Teilalgebra von $S$. Die $y_i$ verhalten sich also über $R$ wie Variablen. Zum Beispiel können wir $S = R[t_1, \ldots, t_n]$ und $y_i = t_i^2$ wählen.

Ferner sind die $t_1, \ldots, t_n$ aus $R[t_1, \ldots, t_n]$ stets algebraisch unabhängig über $R$.

**2.36 Definition.** Sei $R$ ein Integritätsring und $n \geq 1$. Der Quotientenkörper von $R[t_1, \ldots, t_n]$ heißt Körper der rationalen Funktionen in $t_1, \ldots, t_n$ über $R$ und wird mit $R(t_1, \ldots, t_n)$ bezeichnet.

Es gilt offenbar $R(t_1, \ldots, t_n) \cong \mathrm{Quot}(R[t_1, \ldots, t_i])(t_{i+1}, \ldots, t_n)$ für $0 \leq i < n$. Wir fassen $R(t_1, \ldots, t_n)$ wieder als $R$-Algebra mit den ausgezeichneten Elementen $t_1, \ldots, t_n$ auf.

## 2.8 Monoidringe, Potenzreihen- und Laurentreihenringe

Monoidringe, Potenzreihen- und Laurentreihenringe sollen hier nur ganz knapp behandelt werden.

Sei $R$ ein Ring und $G$ ein Monoid. Wir setzen

$$R[G] = \{f \mid f : G \to R \text{ und } f(g) = 0 \text{ für fast alle } g \in G\}.$$

Für $f, h \in R[G]$ definieren wir $f + h \in R[G]$ durch

$$(f + h)(g) = f(g) + h(g)$$

und $f \cdot h \in R[G]$ durch

$$(f \cdot h)(g) = \sum_{\nu\mu = g} f(\nu)h(\mu)$$

für alle $g \in G$, wobei die Summe über alle $\nu, \mu \in G$ mit $\nu\mu = g$ läuft. Die Summe erstreckt sich nur über endlich viele von Null verschiedene Summanden, so daß die Definition Sinn macht.

Man sieht leicht, daß $R[G]$ mit den inneren Verknüpfungen $+$ und $\cdot$ ein Ring ist. Das Nullelement von $R[G]$ wird durch die Funktion gegeben, welche jedes

$g$ auf 0 abbildet. Das Einselement von $R[G]$ wird durch die Funktion gegeben, welche $g = 1$ auf das Einselement 1 von $R$ und $g \neq 1$ auf 0 abbildet. Für $g \in G$ bezeichnen wir mit $g$ auch die Funktion aus $R[G]$, welche $h = g$ auf 1 und $h \neq g$ auf 0 für alle $h \in G$ abbildet.

Wir erhalten einen Monomorphismus $R \to R[G]$, $r \mapsto f_r$ mit $f_r(g) = r\,\delta_{g,1}$ (Kronecker-Delta). Damit fassen wir $R$ als Teilring von $R[G]$ auf und $R[G]$ wird zu einer $R$-Algebra. Wir erhalten darüberhinaus einen Monomorphismus $G \to R[G]^\times$ und fassen $G$ als Untergruppe von $R[G]^\times$ auf.

**2.37 Definition.** Sei $R$ ein Ring. Die eben definierte $R$-Algebra $R[G]$ zusammen mit dem Monomorphismus $G \to R[G]^\times$ heißt Monoidring von $G$ über $R$. Ist $G$ eine Gruppe, so heißt $R[G]$ auch Gruppenring von $G$ über $R$.

Zur Veranschaulichung ist es besser, die Elemente von $R[G]$ mittels der $g$ auszudrücken. Man sieht aufgrund der Definitionen sofort, daß für $f \in R[G]$ folgendes gilt: $f = \sum_{g\in G} a_g g$, mit $a_g = f(g)$ fast alle Null. Zwischen $a_g$ und $g$ steht hier die äußere Multiplikation. Die obigen Verknüpfungen sind gerade so gemacht, daß sich die „erwarteten“ Rechenregeln ergeben.

**2.38 Beispiel.** Für einen kommutativen Ring $R$ und den Monoid $G = (\mathbb{Z}^{\geq 0}, +)$ ergibt sich $R[G] \cong R[t]$ und $R[G^n] = R[t_1, \ldots, t_n]$. Für $G = (\mathbb{Z}/n\mathbb{Z}, +)$ ergibt sich $R[G] \cong R[t]/(t^n - 1)R[t]$.

Motiviert durch das Beispiel können Polynomringe in beliebig vielen Variablen wie folgt definiert werden.

**2.39 Definition.** Sei $R$ ein kommutativer Ring und $I$ eine Menge. Sei $G \leq \prod_{j\in I}(\mathbb{Z}^{\geq 0}, +)$ der Untermonoid des Produkt der Monoide $(\mathbb{Z}^{\geq 0}, +)$, welcher aus allen Elementen des Produkts besteht, deren Koordinaten fast alle Null sind. Seien $t_i \in G$ mit $t_i(j) = \delta_{i,j}$ und $T = \{t_i \mid i \in I\}$. Dann heißt $T$ die durch $I$ indizierte Variablenmenge.

Der Polynomring $R[T]$ mit der durch $I$ indizierten Variablenmenge $T$ über $R$ ist die $R$-Algebra $R[G]$ zusammen mit den $t_i \in T$ für $i \in I$.

**2.40 Bemerkung.** Für unendliches $I$ ist $R[T]$ nicht mehr noethersch, auch wenn $R$ noethersch ist. $R[T]$ ist aber immer noch faktoriell, wenn $R$ faktoriell ist.

Wir kommen nun zu den Potenzreihenringen. Sei $R$ ein kommutativer Ring. Die Definition des (univariaten) Potenzreihenring $R[[t]]$ in der Variablen $t$ über $R$ erfolgt ganz analog zu der von $R[t]$, nur daß für die Funktionen $f : \mathbb{Z}^{\geq 0} \to R$ die Bedingung $f(i) = 0$ für fast alle $i \in \mathbb{Z}^{\geq 0}$ fallen gelassen wird. Es handelt sich bei den Elementen von $R[[t]]$ also um „Polynome mit unendlich vielen Koeffizienten“.

Die Operationen + und · werden genauso definiert, wobei die Summe in der Definition von · stets endlich ist und daher Sinn macht.

Der (multivariate) Potenzreihenring $R[[t_1, \ldots, t_n]]$ wird dann als $R[[t_1]] \cdots [[t_n]]$ definiert. Wir fassen $R[[t_1, \ldots, t_n]]$ als $R$-Algebra mit den ausgezeichneten Elementen $t_1, \ldots, t_n$ auf. Wir können analog auch $R[[G]]$ für einen Monoid definieren, wenn es für jedes $g \in G$ nur endlich viele $\nu, \mu \in G$ mit $\nu\mu = g$ gibt, damit die Summe in der Definition von · wieder nur endlich ist.

Die Elemente von $R[[t_1, \ldots, t_n]]$ heißen Potenzreihen in $t_1, \ldots, t_n$ über $R$. Jedes $f \in R[[t_1, \ldots, t_n]]$ kann in der Form

$$f = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} t_1^{i_1} \cdots t_n^{i_n}$$

mit $a_{i_1, \ldots, i_n} \in R$ geschrieben werden.

**2.41 Lemma.** *Sei $R$ kommutativ.*

1. *Es gilt*

$$R[[t_1, \ldots, t_n]]^\times = \Big\{ \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} t_1^{i_1} \cdots t_n^{i_n} \;\Big|\; a_{i_1, \ldots, i_n} \in R \text{ und } a_{0, \ldots, 0} \in R^\times \Big\}.$$

2. *Ist $R$ ein Körper, so ist $R[[t_1, \ldots, t_n]]$ ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = \sum_{i=1}^n t_i R[[t_1, \ldots, t_n]]$.*

*Beweis.* Zu 1. Die Inklusion „$\subseteq$“ ist unmittelbar einsichtig. Für „$\supseteq$“ sei $f$ ein Element der rechten Seite. Ohne Einschränkung können wir nach Normierung $a_{0, \ldots, 0} = 1$ annehmen. Setze $g = 1 - f$. Dann können wir $h = \sum_{i=0}^\infty g^i \in R[[t_1, \ldots, t_n]]$ definieren und es gilt wie bei der geometrischen Reihe $h(1 - g) = hf = 1$.

Zu 2. Folgt direkt aus Aussage 1. □

Wir können in den Reihen auch endliche Hauptteile erlauben: Die Laurentreihenringe $R((t_1, \ldots, t_n))$ in den Variablen $t_1, \ldots, t_n$ über $R$ bestehen aus den Laurentreihen

$$f = \sum_{i_1, \ldots, i_n \geq m} a_{i_1, \ldots, i_n} t_1^{i_1} \cdots t_n^{i_n}$$

mit $a_{i_1, \ldots, i_n} \in R$ und $m \in \mathbb{Z}$. Addition und Multiplikation werden wie erwartet definiert und involvieren für jeden Koeffizienten des Ergebnis nur endlich viele Operationen in $R$. Der Laurentreihenring $R((t_1, \ldots, t_n))$ wird wieder als $R$-Algebra mit den ausgezeichneten Elementen $t_1, \ldots, t_n$ aufgefaßt.

Für einen Körper $k$ kann man mit dem Lemma leicht sehen, daß $k((t))$ ebenfalls ein Körper ist und das speziell $k((t)) \cong \mathrm{Quot}(k[[t]])$ gilt.

## 2.9 Symmetrische Polynome

Sei $R$ kommutativer Ring und $\mathrm{Aut}_R(R[t_1,\ldots,t_n])$ die Automorphismengruppe der $R$-Algebra $R[t_1,\ldots,t_n]$. Wir wollen einen Monomorphismus $\phi : S_n \to \mathrm{Aut}_R(R[t_1, \ldots, t_n])$ und somit eine Operation von $S_n$ auf $R[t_1,\ldots,t_n]$ durch $\sigma \cdot f = \phi(\sigma)(f)$ definieren.

Sei $\sigma \in S_n$. Wir erhalten den Einsetzhomomorphismus $\phi(\sigma) : R[t_1,\ldots,t_n] \to R[t_1,\ldots,t_n]$, $f \mapsto f(t_{\sigma(1)},\ldots t_{\sigma(t_n)})$. Offenbar gilt $\phi(\sigma) \in \mathrm{Aut}_R(R[t_1,\ldots,t_n])$, da $\phi(\sigma) \in \mathrm{End}_R(R[t_1,\ldots,t_n])$ und da $\phi(\sigma)$ bijektiv ist. Ferner ist leicht einsehbar, daß $\phi : S_n \to \mathrm{Aut}_R(R[t_1,\ldots,t_n])$ ein Monomorphismus ist. Damit gilt $\sigma(f+g) = \sigma f + \sigma g$, $\sigma(fg) = (\sigma f)(\sigma g)$ und $\sigma(rf) = r(\sigma f)$ für alle $f, g \in R[t_1,\ldots,t_n]$, $r \in R$ und $\sigma \in S_n$.

Sei $G \leq S_n$ und $R[t_1,\ldots,t_n]^G = \{f \mid f \in R[t_1,\ldots,t_n] \text{ und } \sigma f = f\}$. Dann ist $R[t_1,\ldots,t_n]^G$ ein Teilring von $R[t_1,\ldots,t_n]$, und die Elemente von $R[t_1,\ldots,t_n]^G$ heißen $G$-invariante Polynome. Wir sind speziell an $G = S_n$ interessiert, und in diesem Fall heißen die $G$-invarianten Polynome auch symmetrische Polynome und $R[t_1,\ldots,t_n]^G$ Ring der symmetrischen Polynome.

Sei $f \in R[t_1,\ldots,t_n][t]$ mit

$$f = \prod_{i=1}^{n}(t - t_i) = \sum_{i=0}^{n}(-1)^i s_i t^{n-i} \tag{2.42}$$

und $s_i \in R[t_1,\ldots,t_n]$. Es gilt beispielsweise $s_0 = 1$, $s_1 = \sum_{i=1}^n t_i$, $\ldots$, $s_n = \prod_{i=1}^n t_i$. Um sich die allgemeine Form der $s_i$ klarzumachen, multipliziere man $f$ „im Kopf“ aus! Die $s_i$ hängen im übrigen auch von $n$ ab.

Wir können die Operation von $S_n$ auf $R[t_1,\ldots,t_n]$ auf $R[t_1,\ldots,t_n][t]$ durch $\sigma t = t$ fortsetzen.

**2.43 Lemma.** *Die $s_i$ sind symmetrisch und homogen vom Grad $i$, für $0 \leq i \leq n$.*

*Beweis.* Es gilt $\sigma f = \prod_{i=1}^n (t - t_{\sigma(i)}) = \prod_{i=1}^n (t - t_i) = f$. Wegen $\sigma t = t$ folgt $\sigma(s_i) = s_i$ für $0 \leq i \leq n$ nach (2.42). Die Aussage über die Homogenität folgt, wenn man $f$ explizit ausmultipliziert und die $s_i$ hinschreibt. □

**2.44 Definition.** Das Polynom $s_i$ heißt das $i$-te elementar-symmetrische Polynom in $t_1,\ldots,t_n$, für $1 \leq i \leq n$.

**2.45 Satz.** *Jedes symmetrische Polynom in $t_1,\ldots,t_n$ läßt sich als Polynom in $s_1,\ldots,s_n$ schreiben. Die $s_1,\ldots,s_n$ sind algebraisch unabhängig über $R$.*

*Beweis.* Wir schicken eine Definition und eine Bemerkung über elementar-symmetrische Polynome voraus.

Zu Beweiszwecken definieren wir das Gewicht des Monoms $t_1^{e_1} \cdots t_n^{e_n}$ als $w(t_1^{e_1} \cdots t_n^{e_n}) = \sum_{i=1}^n ie_i$ und das Gewicht von $f \in R[t_1, \ldots, t_n]$ als das Maximum der Gewichte der in $f$ vorkommenden Monome. Dann folgt aus $w(f) \leq d$ für den Totalgrad $\deg(f(s_1, \ldots, s_n)) \leq d$.

Sei $(s_i)_0 = s_i(t_1, \ldots, t_{n-1}, 0)$. Ersetzen von $t_n$ durch 0 und Kürzen von $t$ in Gleichung (2.42) zeigt, daß $(s_i)_0$ für $1 \leq i \leq n-1$ die elementar-symmetrischen Polynome in den Variablen $t_1, \ldots, t_{n-1}$ sind.

Sei $f \in R[t_1, \ldots, t_n]^{S_n}$ mit $\deg(f) = d$. Wir zeigen, daß es $g \in R[t_1, \ldots, t_n]$ mit $w(g) \leq d$ und $f = g(s_1, \ldots, s_n)$ gibt. Der Beweis erfolgt per Induktion über $n$. Für $n = 1$ gilt $s_1 = t_1$ und die Aussage is korrekt. Wir nehmen nun an, die Aussage sei korrekt für $n-1$ Variablen für $n \geq 2$ und führen eine weitere Induktion über $d$ durch.

Für $d = 0$ ist $f$ konstant und die Aussage ist korrekt. Sei nun $d > 0$. Nach der Induktionsannahme gibt es $g_1 \in R[t_1, \ldots, t_{n-1}]$ mit $w(g_1) \leq d$ und $f(t_1, \ldots, t_{n-1}, 0) = g_1((s_1)_0, \ldots, (s_{n-1})_0)$. Wegen $\deg((s_i)_0) = \deg(s_i)$ und obiger Bemerkung gilt $\deg(g_1(s_1, \ldots, s_{n-1})) \leq d$. Setze $f_1 = f - g_1(s_1, \ldots, s_{n-1})$. Dann gilt $\deg(f_1) \leq d$ und $f_1$ ist symmetrisch. Weiter ist $f_1(t_1, \ldots, t_{n-1}, 0) = 0$, also gilt $t_n | f_1$ und wegen der Symmmetrie $s_n | f_1$ in $R[t_1, \ldots, t_n]$. Also gibt es $f_2 \in R[t_1, \ldots, t_n]$ mit $f_1 = s_n f_2$, $f_2$ symmetrisch und $\deg(f_2) \leq d - n < d$. Nach der Induktionsannahme gibt es $g_2 \in R[t_1, \ldots, t_n]$ mit $w(g_2) \leq d - n$ und $f_2 = g_2(s_1, \ldots, s_n)$. Mit $g = g_1 + t_n g_2 \in R[t_1, \ldots, t_n]$ folgt $f = g(s_1, \ldots, s_n)$ und $w(g) \leq d$, was zu beweisen war.

Der Beweis der algebraischen Unabhängigkeit erfolgt wieder mit Induktion über $n$. Für $n = 1$ ist die Aussage korrekt. Sei $f \in R[t_1, \ldots, t_n]$ ein Polynom kleinsten Totalgrads mit $f(s_1, \ldots, s_n) = 0$. Schreibe $f = \sum_{i=0}^m f_i t_n^i$ mit $f_i \in R[t_1, \ldots, t_{n-1}]$. Hier gilt $f_0 \neq 0$, da sonst $f = t_n g$, $s_n g(s_1, \ldots, s_n) = 0$ und damit $g(s_1, \ldots, s_n) = 0$ gälte, im Widerspruch zur Minimalität von $f$. Wir erhalten $f(s_1, \ldots, s_n) = \sum_{i=0}^m f_i(s_1, \ldots, s_{n-1}) s_n^i$ und nach $t_n \mapsto 0$ ergibt sich $f_0(s_1, \ldots, s_{n-1}) = 0$, im Widerspruch zur Induktionsannahme. □

Mit Galoistheorie und Aussagen über ganze Ringerweiterungen und über transzendente Körpererweiterungen läßt sich dieser Satz relativ gesehen leichter und kürzer, aber nicht konstruktiv beweisen. Die Relevanz des angegebenen Beweises liegt daher vornehmlich darin, daß er ein Verfahren zur Berechnung der $g$ liefert.

Das Polynom $g$ ist im übrigen eindeutig bestimmt, was aus der algebraischen Unabhängigkeit der $s_i$ folgt.

**2.46 Korollar.** *Sei $\psi : R[t_1, \ldots, t_n] \to R[t_1, \ldots, t_n]$ der durch $t_i \mapsto s_i$ definierte Einsetzhomomorphismus. Dann gilt $\mathrm{im}(\psi) = R[t_1, \ldots, t_n]^{S_n}$ und $\ker(\psi) = \{0\}$.*

*Beweis.* Die Inklusion $\mathrm{im}(\psi) \subseteq R[t_1, \ldots, t_n]^{S_n}$ ist klar. Der Rest ist genau die Aussage des Satzes, nur anders formuliert. □

Wir betrachten kurz zwei Anwendungen, in denen symmetrische Polynome vorkommen.

Sei $f = \prod_{i=1}^{n}(t - t_i)$. Die Diskriminante von $f$ ist definiert als

$$D(f) = \prod_{i<j}(t_i - t_j)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j}(t_i - t_j).$$

Es handelt sich hierbei um ein symmetrisches Polynom, welches folglich als Polynom $g_f$ in den Koeffizienten von $f$ geschrieben werden kann.

**2.47 Beispiel.** Für $f = t^2 + bt + c$ gilt $D(f) = b^2 - 4c$. Für $f = x^3 + at + b$ gilt $D(f) = -4a^3 - 27b^2$.

Diskriminanten kann man von jedem (normierten) Polynom über einem kommutativen Ring bilden, indem man die die Koeffizienten von $f$ für die $t_i$ in $g_f$ einsetzt.

Die Diskriminante eines Polynoms ist eine Invariante, mit Hilfe derer man feststellen kann, ob $f$ mehrfache Nullstellen über dem Grundring $R$ oder einem Erweiterungsring $S$ von $R$ besitzt. Ist das Polynom $f$ beispielsweise über $\mathbb{Z}$ gegeben, so gilt $D(f) \in \mathbb{Z}$ und die Primfaktoren $p$ von $D(f)$ liefern genau die Charakteristiken der endlichen Körper $\mathbb{F}_q$ mit $q = p^m$ (und $m \leq \deg(f)$), über denen das Polynom mehrfache Nullstellen hat. Dies findet Anwendung in der algebraischen Zahlentheorie.

Ein weiteres, einfaches Beispiel aus der algebraischen Geometrie: Wenn man die Nullstellenmenge eines Polynoms als geometrische Struktur betrachtet, dann faßt man mehrfache Nullstellen als irreguläre (singuläre) Punkte der geometrischen Struktur auf. Sei beispielsweise $f = (y - x)(y + x) = y^2 - x^2 \in R[x, y]$. Die Nullstellenmenge von $f$ in $\mathbb{R}^2$ ist gleich der Vereinigung der Geraden mit Steigung 1 und $-1$ durch den Ursprung. Für die Diskriminante von $f$ als Polynom in $y$ gilt nach obiger Formel $D(f) = 4x^2$. Daher hat $f$ dann und nur dann eine doppelte Nullstelle in $y$, wenn $x = 0$ ist. Dies ist offenbar richtig, da sich die beiden Geraden genau im Ursprung $x = 0$, $y = 0$ schneiden.

Die zweite Anwendung betrifft die Beziehung zwischen den Koeffizienten eines Polynoms und den Potenzsummen seiner Nullstellen, welche ebenfalls symmetrische Polynome sind. Die Potenzsummen von $f = \prod_{i=1}^{n}(t - t_i)$ sind definiert als

$$S_i = \sum_{j=1}^{n} t_j^i.$$

Sie können wie folgt in den elementar-symmetrischen Polynomen geschrieben werden.

Sei zunächst $R = \mathbb{Z}$. Wir verwenden die Einbettungen $\mathbb{Z}[t] \to \mathbb{Q}(t) \to \mathbb{Q}((t))$.

**2.48 Satz.** *Für $g = \prod_{i=1}^{n}(1 - t_i t)$ und $S_j = \sum_{i=1}^{n} t_i^j$ gilt:*

1. $g = \exp\bigl(-\sum_{j=1}^{\infty} S_j t^j/j\bigr)$.
2. $g'/g = -\sum_{j=1}^{\infty} S_j t^{j-1}$.
3. $(-1)^k k\sigma_k + \sum_{i=0}^{k-1}(-1)^i \sigma_i S_{k-i} = 0$ *für* $1 \le k \le n$ *und*
   $\sum_{i=0}^{n}(-1)^i \sigma_i S_{k-i} = 0$ *für* $k \ge n$.

*Beweis.* Zu 1. Wir rechnen mit $\log(1-t) = -\sum_{j=1}^{\infty} t^j/j$ und $\exp(t) = \sum_{j=0}^{\infty} t^j/j!$. Es gilt $\log((1-t_1)(1-t_2)) = \log(1-t_1) + \log(1-t_2)$ und $\exp(\log(1-t)) = 1 - t$. Wir erhalten $\log(g) = -\sum_{j=1}^{\infty} S_j t^j/j$ wegen der Regel für log und $g = \exp(-\sum_{j=1}^{\infty} S_j t^j/j)$ durch Anwenden von exp.

Zu 2. Ableiten beider Seiten von $\log(g) = -\sum_{j=1}^{\infty} S_j t^j/j$ liefert Aussage 2.

Zu 3. Wegen $g = \sum_{i=0}^{n}(-1)^i s_i t^i$ und $g' = \sum_{i=0}^{n} i(-1)^i s_i t^{i-1}$ folgt Aussage 3 durch Koeffizientenvergleich in der Gleichung $g' + g\sum_{j=1}^{\infty} S_j t^{j-1} = 0$, welche nach Aussage 2 gilt. □

Im Satz können wir nun $R$ und die $t_i$ speziell vorgeben: Aussage 1 gilt dann für jeden Integritätsring $R$ der Charakteristik Null, da $\mathbb{Q}$ Teilkörper von $\mathrm{Quot}(R)$ ist und die Gleichung darin Sinn macht. Aussage 2 und Aussage 3 sind über $\mathbb{Z}$ definiert und gelten daher für jeden Ring und beliebige Werte von $t_i$.

Die Zuordnung $k[t]\backslash\{0\} \to k((t))$, $f \mapsto f'/f$ für einen beliebigen Körper $k$ heißt im übrigen logarithmische Ableitung und erfüllt $(fg)'/(fg) = f'/f + g'/g$.

Mittels Aussage 3 kann man die Koeffizienten eines Polynoms und die Potenzsummen ineinander umrechnen, sofern die Charakteristik größer als $n$ ist. Diese Relationen heißen Newtonsche Relationen.

Der Satz kann für Endomorphismen endlichdimensionaler Vektorräume angewendet werden. Ist $f$ das charakteristische Polynom eines Endomorphismus $\phi$, so wird $f$ durch die Spuren der Potenzen von $\phi$ eindeutig bestimmt, vorausgesetzt, die Charakteristik ist groß genug. Das ist vorteilhaft, wenn die Spuren besser zugänglich sind als die Koeffizienten von $f$. Eine Anwendung in diese Richtung erfolgt bei den Zetafunktionen von algebraischen Kurven über endlichen Körpern bzw. den charakteristischen Polynomen der zugehörigen Frobeniusendomorphismen.

# Kapitel 3

# Moduln I

Ein Modul ist ein „Vektorraum“ über $K$, wobei $K$ nicht unbedingt ein Körper, sondern nur noch ein Ring zu sein braucht. Die Modultheorie kann als gemeinsame Verallgemeinerung der Ringtheorie und der linearen Algebra angesehen werden. Da die Theorie sehr umfangreich ist, können hier im wesentlichen nur grundlegende Definitionen und Sätze angeführt werden.

## 3.1 Grundlagen

Im folgenden bezeichnet $R$ immer einen (nicht notwendigerweise kommutativen) Ring mit Eins. Ringhomomorphismen bilden Einselemente auf Einselemente ab.

**3.1 Definition.** Sei $M$ eine abelsche Gruppe. Wir betrachten eine Multiplikation $\cdot : R \times M \to M$ mit

$$r \cdot (x + y) = r \cdot x + r \cdot y,\ (r + s) \cdot x = r \cdot x + s \cdot x \text{ (Distributivgesetze)}$$
$$(sr) \cdot x = s \cdot (r \cdot x) \text{ (Assoziativitätsgesetz)}$$

für alle $r, s \in R$ und $x, y \in M$. Außerdem gelte $1 \cdot x = x$ für alle $x \in M$. Dann heißt $M$ zusammen mit $\cdot$ ein $R$-Linksmodul.

Wie bei der Multiplikation in Ringen lassen wir $\cdot$ fort und schreiben nur $rx$ statt $r \cdot x$.

**3.2 Beispiel.** Jeder Vektorraum über einem Körper $K$ ist ein $K$-Linksmodul. Jeder Ring $R$ und jedes Linksideal von $R$ ist ein $R$-Linksmodul. Abelsche Gruppen $M$ sind $\mathbb{Z}$-Linksmoduln.

Ist $M$ ein $R$-Linksmodul und $r \in R$, so ist die Abbildung $x \mapsto rx$ ein Endomorphismus der abelschen Gruppe $M$, entsprechend erhalten wir einen Homomorphismus $\phi : R \to \mathrm{End}(M)$. Ist umgekehrt $M$ eine abelsche Gruppe und

$\phi : R \to \mathrm{End}(M)$ ein Homomorphismus, so definieren wir $rx = \phi(r)(x)$ für alle $r \in R$ und $x \in M$ und erhalten so einen $R$-Linksmodul $M$. Dies liefert also auch eine alternative Definition von $R$-Linksmodul.

Bei Linksmoduln wird $R$ von links an $M$ multipliziert. Analog zu Definition 3.1 definiert man $R$-Rechtsmoduln.

Für nicht kommutative Ringe ist es im allgemeinen nicht möglich, einen $R$-Linksmodul $M$ zu einem $R$-Rechtsmodul zu machen, indem man $xr = rx$ definiert. Wegen der Assoziativgesetze müßte sonst gelten $(r_1r_2)x = x(r_1r_2) = (xr_1)r_2 = r_2(xr_1) = r_2(r_1x) = (r_2r_1)x$ für $r_1, r_2 \in R$ und $x \in M$. Für kommutative Ringe ergibt sich jedoch kein Problem und man läßt die Unterscheidung in Links- und Rechtsmoduln üblicherweise fallen.

Ist $M$ ein $R$-Linksmodul, so kann man $M$ auf die offensichtliche Weise zu einem $R^{\mathrm{opp}}$-Rechtsmodul machen, wobei der Ring $R^{\mathrm{opp}}$ aus $R$ entsteht, indem man die Multiplikation in $R$ andersherum definiert bzw. ausführt. Entsprechend sind die Begriffe Linksmodul und Rechtsmodul symmetrisch und es genügt, sich nur auf Linksmoduln zu konzentrieren. Daher soll im folgenden ein $R$-Modul immer einen $R$-Linksmodul bezeichnen.

Bei Moduln $M$ ist es häufig praktisch, zuerst an die additive Struktur und dann an die $R$-lineare Struktur zu denken.

**3.3 Definition.** Ein Homomorphismus $f : M \to N$ der $R$-Moduln $M$ und $N$ ist ein Homomorphismus der abelschen Gruppen $M$ und $N$, welcher $R$-linear ist, für den also $f(rx) = rf(x)$ für alle $x \in M$ und $r \in R$ gilt.

Die Menge der Homomorphismen von $M$ nach $N$ wird mit $\mathrm{Hom}_R(M, N)$ bezeichnet. Für $f, g \in \mathrm{Hom}_R(M, N)$ definieren wir $f + g \in \mathrm{Hom}_R(M, N)$ durch $(f + g)(x) = f(x) + g(x)$. Damit wird $\mathrm{Hom}_R(M, N)$ zu einer abelschen Gruppe.

Wir benötigen weitere Definitionen, die auf der Hand liegen: Ist $U \subseteq M$ eine Untergruppe des $R$-Moduls $M$ und gilt $RU \subseteq U$, so heißt $U$ ein Untermodul von $M$. Für zwei Untermoduln $U, V$ von $M$ ist die Summe abelscher Gruppen $U + V$ wieder ein Untermodul von $M$ (also unter Multiplikation mit $R$ abgeschlossen), ebenso $U \cap V$. Wie bei Vektorräumen definieren wir Linearkombination, Erzeugendensystem, endlich erzeugt, linear unabhängig über $R$, Basis, innere und äußere direkte Summe, Mono-, Epi-, Iso-, Endo- und Automorphismen. Hintereinanderausführung von Abbildungen liefert einen Homomorphismus $\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(N, P) \to \mathrm{Hom}_R(M, P)$. Die zu einem Isomorphismus inverse Abbildung ist wieder ein Isomorphismus. Sei $f \in \mathrm{Hom}_R(M, N)$. Dann sind der Kern $\ker(f)$ und das Bild $\mathrm{im}(f)$ als abelsche Gruppen wegen der $R$-Linearität von $f$ Untermoduln von $M$ bzw. $N$. Für einen Untermodul $U$ von $M$ können wir $M/U$ als Faktorgruppe abelscher Gruppen betrachten. Wegen $RU \subseteq U$ können wir auf

den Klassen vertreterweise eine Multiplikation mit $R$ definieren, dies macht $M/U$ zu einem $R$-Modul, dem Faktormodul von $M$ nach $U$. Der kanonische Epimorphismus abelscher Gruppen $\pi : M \to M/U$ ist dann (per Definition) $R$-linear, also $\pi \in \mathrm{Hom}_R(M/U, N)$. Der Kokern eines $f \in \mathrm{Hom}_R(M, N)$ ist als $N/\mathrm{im}(f)$ definiert.

Es gelten wieder Homomorphie- und Isomorphiesätze:

**3.4 Satz.** *Seien $M$, $N$ $R$-Moduln.*

(*i*) *Für $f \in \mathrm{Hom}_R(M, N)$ und $U$ einen Untermodul von $M$ mit $U \subseteq \ker(f)$ gibt es genau ein $g \in \mathrm{Hom}_R(M/U, N)$ mit $f = g \circ \pi$, wobei $\pi \in \mathrm{Hom}_R(M, M/U)$ der kanonische Epimorphismus ist.*

(*ii*) *Für $f \in \mathrm{Hom}_R(M, N)$ gilt $M/\ker(f) \cong \mathrm{im}(f)$.*

(*iii*) *Für Untermoduln $U, V$ von $M$ gilt $(U + V)/V \cong U/(U \cap V)$.*

(*iv*) *Für Untermoduln $U, V$ von $M$ mit $U \subseteq V$ gilt $(M/U)/(V/U) \cong M/V$.*

*Beweis.* Für die unterliegenden abelschen Gruppen wurden diese Aussagen bereits in der Gruppentheorie gezeigt.

Zu (*i*) und (*ii*). Es gibt es zu jedem $x \in M/U$ ein $y \in \pi^{-1}(\{x\})$. Ist auch $r \in R$ beliebig, so gilt $g(rx) = g(r\pi(y)) = g(\pi(ry)) = f(ry) = rf(y) = rg(\pi(y)) = rg(x)$. Daher ist $g$ $R$-linear, also $g \in \mathrm{Hom}_R(M/U, N)$, und Aussage (*i*) ist bewiesen. Aussage (*ii*) ist dann eine direkte Folgerung aus (*i*).

Die Isomorphismen aus (*iii*) und (*iv*) werden jeweils durch einen kanonischen Epimorphismus abelscher Gruppen induziert. Da diese kanonischen Epimorphismen hier zusätzlich $R$-linear sind, sind auch die induzierten Isomorphismen $R$-linear. □

Wir kommen jetzt zu ein paar grundlegenden Begriffen, die bei Vektorräumen nur trivial auftreten oder zusammenfallen.

**3.5 Definition.** Sei $M$ ein $R$-Modul. Für einen Untermodul $U$ von $M$ heißt $\mathrm{Ann}(U) = \{r \in R \mid rx = 0 \text{ für alle } x \in U\}$ der Annulator von $U$. Ferner heißt $M$ treu, wenn $\mathrm{Ann}(M) = \{0\}$ gilt.

Die Menge der Torsionselemente (oder Nullteiler) von $M$ ist $\mathrm{Tor}(M) = \{x \in M \mid \mathrm{Ann}(Rx) \neq \{0\}\} = \{x \in M \mid \exists r \in R\backslash\{0\} \text{ mit } rx = 0\}$. Der Modul $M$ heißt ein Torsionsmodul, wenn $\mathrm{Tor}(M) = M$ ist, und torsionsfrei, wenn $\mathrm{Tor}(M) = \{0\}$ gilt.

Der Annulator ist ein Untermodul des $R$-Moduls $R$, also ein Linksideal von $R$. Für einen torsionsfreien $R$-Modul ist $R$ notwendigerweise nullteilerfrei (für

Nullteiler $a, b \in R$ und $x \in M$ ist entweder $bx = 0$ oder $a(bx) = (ab)x = 0$). Ein typisches Beispiel erhalten wir mit $M = R/I$, wobei $I$ ein Ideal in $R$ ist. Hier gilt $\mathrm{Ann}(M) = I$ und $\mathrm{Tor}(M) = M$.

**3.6 Satz.** *Sei $R$ ein Integritätsring und $M$ ein $R$-Modul. Dann ist $\mathrm{Tor}(M)$ ein Untermodul von $M$ und $M/\mathrm{Tor}(M)$ ist torsionsfrei.*

*Beweis.* Für $x, y \in \mathrm{Tor}(M)$ gibt es $r, s \in R\backslash\{0\}$ mit $rx = sy = 0$. Dann gilt $rs \neq 0$, da $R$ nullteilerfrei ist, und $rs(x-y) = 0$. Daher $x - y \in M$. Ferner gilt für $s \in R$ beliebig $r(sx) = 0$, also $sx \in \mathrm{Tor}(M)$. Daher ist $\mathrm{Tor}(M)$ ein Untermodul von $M$.

Sei $x \in M$ und $r \in R\backslash\{0\}$ mit $rx \in \mathrm{Tor}(M)$. Dann gibt es $s \in R\backslash\{0\}$ mit $s(rx) = 0$, folglich $(sr)x = 0$ und $sr \neq 0$. Es folgt $x \in \mathrm{Tor}(M)$ und $M/\mathrm{Tor}(M)$ ist daher torsionsfrei. □

**3.7 Definition.** Sei $M$ ein $R$-Modul. Der Rang von $M$ ist das Maximum der Kardinalitäten von über $R$ linear unabhängigen Teilmengen von $M$ und wird mit $\mathrm{rank}(M)$ bezeichnet.

Die Länge von $M$ ist die Länge, also das Maximum der Anzahl der Inklusionen, von echt absteigenden Ketten $\cdots \supsetneq M_i \supsetneq M_{i+1} \supsetneq \cdots$ von Untermoduln von $M$ mit $i \in \mathbb{Z}$ und wird mit $\mathrm{len}(M)$ bezeichnet.

Zum Beispiel hat $(\mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}$ den Rang eins und unendliche Länge. Der Nullmodul $\{0\}$ hat Länge Null. Für Vektorräume stimmen Rang und Länge überein und Rang und Länge sind unterschiedliche Verallgemeinerungen des Dimensionsbegriffs von Vektorräumen auf Moduln.

**3.8 Definition.** Der Modul $M$ heißt frei, wenn er eine Basis besitzt.

Der Begriff „frei“ soll heißen, daß es ein Erzeugendensystem von $M$ gibt, welches frei von nicht trivialen $R$-linearen Relationen ist. Die Moduln $R^n$ sind frei, die Einheitsvektoren liefern eine Basis. Besitzt ein Modul $M$ eine endliche Basis mit $n$ Elementen, so gilt $M \cong R^n$, wobei der Isomorphismus durch die Abbildung gegeben ist, die den Elementen von $M$ die Koordinaten in $R$ bezüglich der Basiselemente zuordnet.

Nicht jeder Modul ist frei: Als Beispiel betrachte man den $\mathbb{Z}$-Modul $\mathbb{Z}/3\mathbb{Z}$. Im allgemeinen können nur torsionsfreie Moduln frei sei.

Eine Basis eines $R$-Moduls $M$ ist eine maximale Menge von $R$-linear unabhängigen Elementen aus $M$, durch Hinzunahme eines Elements geht die lineare Unabhängigkeit verloren. Trotzdem brauchen Basen nicht die gleiche Kardinalität zu besitzen. Es gibt beispielsweise einen (nicht-kommutativen) Ring $R$ mit 1, für den $R^n \cong R^m$ für alle $n, m \in \mathbb{Z}^{\geq 1}$ gilt (siehe Abschnitt 4.5 oder Meyberg 1, Seite 178).

**3.9 Satz.** *Sei $M$ ein $R$-Modul.*

(*i*) *Seien $x_i \in M$ mit $i \in I$ und $I$ eine Indexmenge. Dann ist $M$ genau dann frei und die $x_i$ sind eine Basis, wenn es für jeden Modul $N$ und beliebige Elemente $y_i \in N$ genau einen Homomorphismus $f : M \to N$ mit $f(x_i) = y_i$ für alle $i \in I$ gibt.*

(*ii*) *Ist $R$ kommutativ, so hat jede Basis von $M$ die gleiche Kardinalität.*

*Beweis.* Zu (*i*). Beweis ist einfach und vom Prinzip ähnlich wie bei den Polynomringen.

Zu (*ii*). Sei $B$ eine Basis von $M$. Für $R = \{0\}$ ist der Satz korrekt, alle Basen sind leer. Ansonsten besitzt $R$ eine $1 \neq 0$ und somit ein ein maximales Ideal $\mathfrak{m}$. Dann ist $\mathfrak{m}M$ ein Untermodul von $M$ und $M/\mathfrak{m}M$ ein $R/\mathfrak{m}$-Modul. Weiter ist $B' = \{x + \mathfrak{m}M \,|\, x \in B\}$ eine Basis des $R/\mathfrak{m}$-Moduls $M/\mathfrak{m}M$, wie man leicht nachrechnet. Da $R/\mathfrak{m}$ ein Körper ist, handelt es sich bei $M/\mathfrak{m}M$ um einen $R/\mathfrak{m}$-Vektorraum. Es folgt $\#B' = \dim(M/\mathfrak{m}M)$ ist eindeutig bestimmt. □

Aus (*i*) folgt, daß jeder endlich erzeugte $R$-Modul $N$ epimorphes Bild eines freien Moduls $R^n$ ist.

Eine andere als die oben erwähnte Situation nicht freier Moduln tritt beispielsweise für Integritätsringe $R$ auf, die keine Hauptidealringe sind. Ist $I$ ein Ideal, welches nur von mindestens zwei Elementen erzeugt werden kann, so ist $I$ als $R$-Modul nicht frei. Man sieht dies wie folgt: Wäre $I$ frei, so müßte $I$ wegen $\operatorname{rank}(I) = 1$ eine einelementige Basis besitzen. Dies aber bedeutet gerade, daß $I$ ein Hauptideal ist.

Auch ist $I$ dann zwar ein Untermodul von $R$, aber kein direkter Summand von $R$ (wie das bei Untermoduln von Vektorräumen der Fall wäre). Dies gilt, weil aus $R \cong I \oplus N$ zunächst $N = \{0\}$ folgen würde, denn der Rang von $R$ ist eins und der von $I \oplus N$ für $N \neq \{0\}$ größer gleich zwei, da $N$ mit $R$ torsionsfrei sein muß. Gilt $R \cong I$ und bezeichnet $\phi : R \to I$ den Isomorphismus, so ist $I = \phi(R) = R\phi(1)$ und $I$ ist ein von $\phi(1)$ erzeugtes Hauptideal, im Widerspruch zur Annahme. Entsprechend ist auch nicht jeder (torsionsfreie) $R$-Modul von der Form $R^n$.

## 3.2 Matrizen über Ringen

Ähnlich wie in der linearen Algebra sind Matrizen auch in der Modultheorie nützliche Objekte. Wir wollen nun Matrizen über Ringen betrachten.

Wir befassen uns zunächst mit Determinanten von Matrizen über beliebigen, kommutativen Ringen. Sei $S = \mathbb{Z}[x_{1,1}, \ldots, x_{n,n}, y_{1,1}, \ldots, y_{n,n}]$, $M = (x_{i,j})_{i,j}$

und $N = (y_{i,j})_{i,j}$, so daß $M, N \in S^{n\times n}$ gilt. Dann können wir $M$ auch als Matrix über dem Quotientenkörper Quot($S$) von $S$ auffassen und es ist $\det(M) = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) x_{1,\sigma(1)} \cdots x_{n,\sigma(n)} \in S$, wie man es aus der linearen Algebra über Körpern gewöhnt ist. Analoges gilt für $N$. Für Determinanten gilt wie üblich $\det(MN) = \det(M)\det(N)$ und, daß det eine alternierende Multilinearform ist. Man beachte, daß dies Gleichungen im Polynomring $S = \mathbb{Z}[x_{1,1}, \ldots, x_{n,n}, y_{1,1}, \ldots, y_{n,n}]$ sind, da Determinanten hier nichts anderes als Polynome in den Koeffizienten von $M$ und $N$ sind. Ist $M_{i,j} \in S^{(n-1)\times(n-1)}$ die Matrix, die durch Streichen der $i$-ten Zeile und $j$-ten Spalte von $M$ entsteht, so gilt ferner $\det(M) = \sum_{i=1}^{n} (-1)^{i+j} x_{i,j} \det(M_{i,j})$.

Sei nun $R$ ein beliebiger, kommutativer Ring. Da die $x_{i,j}$ und $y_{i,j}$ nirgends im Nenner auftreten, können wir sie auch durch spezielle Werte aus $R$ ersetzen. Daher gelten die genannten Eigenschaften aufgrund der Homomorphieeigenschaft des Einsetzhomomorphismus auch für Matrizen über $R$.

Wir arbeiten auch häufig über Integritätsringen $R$. Hier kann man alles in $K = \text{Quot}(R)$ einbetten und so lineare Algebra über $K$ anwenden. Zum Beispiel sind die Spalten- und Zeilenvektoren von $M \in R^{n\times n}$ genau dann über $R$ linear unabhängig, wenn $\det(M) \neq 0$ gilt. Man beachte, daß linear unabhängig über $R$ und linear unabhängig über $K$ für $K = \text{Quot}(R)$ äquivalent sind (man kann Nenner rausmultiplizieren).

**3.10 Satz.** *Sei $R$ ein kommutativer Ring.*

(*i*) *Sei $A \in R^{n\times n}$, $x = (x_i)^t \in R^n$ und $b = (b_i)^t \in R^n$ mit $Ax = b$. Ist $B_i$ die Matrix, deren $i$-te Spalte gleich $b$ ist und die ansonsten mit $A$ übereinstimmt, so gilt $\det(B_i) = x_i \det(A)$.*

(*ii*) *Sei $M \in R^{n\times n}$ und $M' = ((-1)^{i+j} \det(M_{j,i}))_{i,j} \in R^{n\times n}$, wobei $M_{i,j}$ die Matrix ist, die durch Streichen der $i$-ten Zeile und $j$-ten Spalte von $M$ entsteht. Dann gilt $MM' = M'M = \det(M) I_n$.*

(*iii*) *Eine Matrix $M \in R^{n\times n}$ ist genau dann invertierbar, wenn $\det(M)$ in $R$ invertierbar ist.*

*Beweis.* (*i*): Die $i$-te Spalte $b$ in $B_i$ ist gleich der Linearkombination der Spalten von $A$ mit den Koeffizienten $x_i$. Sei $A_{i,j}$ die Matrix, die an der $i$-ten Spalte die $j$-Spalte von $A$ hat und ansonsten mit $A$ übereinstimmt. Dann gilt $\det(A_{i,j}) = \delta_{i,j} \det(A)$ (Kronecker-Delta) und aufgrund der Linearität der Determinante in der $i$-ten Spalte ergibt sich $\det(B_i) = \sum_{j=1}^{n} x_j \det(A_{i,j}) = x_i \det(A)$.

(*ii*): Für $S$ statt $R$ folgt die Behauptung als Polynomidentität, indem man die Einträge von $M'$ nach (*i*) unter Verwendung der obigen Entwicklung für Determinanten und durch Kürzen von $\det(M)$ berechnet. Für $M' = (x_{i,j})_{i,j}$ ergibt sich

genauer $x_{i,j}\det(M) = \det(\hat{M}_{i,j})$, wobei $\hat{M}_{i,j}$ die Matrix ist, die aus $M$ entsteht, wenn wir die $i$-te Spalte von $M$ durch den $j$-ten Einheitsvektor multipliziert mit $\det(M)$ ersetzen. Dann gilt $\det(\hat{M}_{i,j}) = (-1)^{i+j}\det(M)\det(M_{j,i})$ nach der Entwicklungsformel, da die $i$-te Spalte in $\hat{M}_{i,j}$ Null ist außer in der $j$-ten Zeile, wo $\det(M)$ steht. Folglich $x_{i,j}\det(M) = (-1)^{i+j}\det(M)\det(M_{j,i})$. Da $S$ nullteilerfrei ist und $\det(M) \neq 0$ gilt, folgt durch Kürzen $x_{i,j} = (-1)^{i+j}\det(M_{j,i})$ als Polynomidentität.

Durch Spezialisierung der Variablen folgt die Behauptung dann auch für $R$.

$(iii)$: Ist $M$ invertierbar, so gilt $1 = \det(MM^{-1}) = \det(M)\det(M^{-1})$. Wegen $M^{-1} \in R^{n\times n}$ folgt auch $\det(M^{-1}) \in R$ und $\det(M)$ ist invertierbar in $R$.

Umgekehrt sei $M \in R^{n\times n}$ und $M'$ wie in $(ii)$. Ist $\det(M)$ invertierbar, so ist $M'/\det(M)$ über $R$ definert und invers zu $M$. □

Satz 3.10, $(i)$ ist als Cramersche Regel bekannt. Die Matrix $M'$ in $(ii)$ nennt man häufig Pseudoinverse von $M$.

Invertierbare Matrizen über Ringen heißen auch unimodular. Ist $T \in R^{n\times n}$, $M$ ein $R$-Modul und $a_1, \ldots, a_n, b_1, \ldots, b_n \in M$ mit $(a_1, \ldots, a_n)T = (b_1, \ldots, b_n)$, so ist jedes $b_i$ eine Linearkombination der $a_i$ und der von den $b_i$ erzeugte Untermodul $U_2$ von $M$ ist also ein Untermodul des von den $a_i$ erzeugten Moduls $U_1$. Umgekehrt gilt für unimodulares $T$ aber auch $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)T^{-1}$, so daß sich jedes $b_i$ als Linearkombination der $a_i$ schreiben läßt und somit $U_1 = U_2$ gilt. Sind die $a_i$ und die $b_i$ Basen von $M$, so gibt es ein unimodulares $T \in R^{n\times n}$ mit $(a_1, \ldots, a_n)T = (b_1, \ldots, b_n)$.

**3.11 Satz.** *Für beliebiges $T$ gilt mit obiger Notation* $\det(T)U_1 \subseteq U_2$ *und* $\det(T) \in \mathrm{Ann}(U_1/U_2)$.

*Beweis.* Mit Satz 3.10, $(ii)$ und der Pseudoinversen $T'$ von $T$ gilt $TT' = \det(T)I_n$. Daraus folgt $\det(T)(a_1, \ldots, a_n) = (a_1, \ldots, a_n)TT' = (b_1, \ldots, b_n)T' \in U_2^n$, also $\det(T)U_1 \subseteq U_2$. Die Aussage über den Annulator folgt daraus direkt. □

Typische unimodulare, elementare Transformationen sind durch folgende Operationen gegeben: Mit Einheit multiplizieren, Vertauschen, Vielfaches eines Elements zu einem anderen addieren. Über euklidischen Ringen läßt sich jede unimodulare Transformation in diese elementaren Transformationen faktorisieren, wie in Abschnitt 3.4 gezeigt wird.

## 3.3 Noethersche und Artinsche Moduln

In diesem Abschnitt sind aufsteigende und absteigende Ketten von Untermoduln von Interesse.

**3.12 Definition.** Ein Modul heißt noethersch, wenn jede aufsteigende Kette von Untermoduln $\{0\} = M_0 \cdots \subseteq M_i \subseteq M_{i+1} \subseteq \cdots$ stationär wird.

Ein Modul heißt artinsch, wenn jede absteigende Kette von Untermoduln $M = M_0 \cdots \supseteq M_i \supseteq M_{i+1} \supseteq \cdots$ stationär wird.

Zum Beispiel ist jeder Hauptidealring $R$ als $R$-Modul noethersch, aber im allgemeinen nicht artinsch. Ist $I$ ein Ideal von $R$, so ist $R/I$ dann auch artinsch.

**3.13 Satz.** *Sei $R$ ein Ring und $M$ ein $R$-Modul. Dann sind äquivalent.*

(*i*) *$M$ ist noethersch.*

(*ii*) *Jede nichtleere Menge von Untermoduln von $M$ besitzt ein maximales Element.*

(*iii*) *Für jede Familie von Untermoduln $M_i$ mit $i \in I$ gibt es ein endliches $I_0 \subseteq I$ mit $\sum_{i\in I} M_i = \sum_{i\in I_0} M_i$.*

(*iv*) *Jeder Untermodul von $M$ ist endlich erzeugt.*

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Wenn (*ii*) nicht gilt, dann gibt es eine nicht-leere Menge $X$, die keinen maximalen Untermodul enthält. Zu jedem Modul aus $X$ gibt es dann stets einen umfassenderen Modul aus $X$. Man kann daher (mittels Auswahlaxiom) eine aufsteigende, nicht stationäre Kette definieren.

(*ii*) $\Rightarrow$ (*iii*): In der Menge aller Summen endlich vieler $M_i$ gibt es ein maximales Element $N = \sum_{i\in I_0} M_i$, wobei $I_0 \subseteq I$ endlich ist. Wegen der Maximalität folgt $N + M_i = N$ für alle $i \in I$, also $\sum_{i\in I} M_i = N$.

(*iii*) $\Rightarrow$ (*i*): Bilden die $M_i$ eine aufsteigende Kette, so gibt es ein $j$ für welches $\sum_i M_i = M_j$. Daher ist die Kette stationär.

(*iv*) $\Rightarrow$ (*iii*): Seien $a_j$ endlich viele Erzeuger von $\sum_{i\in I} M_i$. Für jedes $j$ gibt es ein endliches $I_j \subseteq I$ mit $a_j \in \sum_{i\in I_j} M_i$. Dann leistet $I_0 = \cup_j I_j$ das Gewünschte.

(*iii*) $\Rightarrow$ (*iv*): Sei $U$ ein Untermodul. Zu $I = U$ definiere $M_i = Ri$ für $i \in I$. Dann gilt $U = \sum_{i\in I} M_i = \sum_{i\in I_0} M_i$ für ein endliches $I_0 \subseteq I$. Also ist $I_0$ endliches Erzeugendensystem von $U$. □

Man beachte, daß in der Definition eines noetherschen Ring $R$ Ideale, also $R$-Links- und Rechtmoduln betrachten werden. Mit unserer Definition braucht daher ein noetherscher Ring nicht als $R$-Modul noethersch zu sein.

**3.14 Satz.** *Sei $M$ ein $R$-Modul.*

(*i*) *Ist $M$ noethersch, so auch $U$ und $M/U$ für alle Untermoduln $U$ von $M$.*

(*ii*) *Sind $U$ und $M/U$ noethersch für einen Untermodul $U$ von $M$, so ist auch $M$ noethersch.*

(*iii*) *Ist $M$ endlich erzeugt und $R$ als $R$-Modul noethersch, so ist $M$ noethersch.*

*Beweis.* (*i*): Aufsteigende Ketten von Untermoduln in $U$ sind auch aufsteigende Ketten von Untermoduln von $M$ und werden daher stationär. Analoges gilt für aufsteigendene Ketten von Untermoduln in $M/U$ und ihre Urbilder in $M$.

(*ii*): Sei $U_i$ eine aufsteigende Kette in $M$ und $U_i' = U \cap U_i$, $U_i'' = (U_i + U)/U$. Es gibt ein $n$, so daß $U_t' = U_n'$ und $U_t'' = U_n''$ für alle $t \geq n$ gilt. Wir zeigen nun $U_t = U_n$ für $t \geq n$. Sei $x \in U_t$. Wegen $U_t'' = U_n''$ gibt es $y \in U_n$ mit $x - y \in U$. Folglich $x - y \in U \cap U_t = U_t' = U_n' \subseteq U_n$. Es ergibt sich $x \in U_n$.

(*iii*): Zunächst ist $R^n$ nach (*ii*) noethersch, indem man $R^n/R \cong R^{n-1}$ betrachtet und Induktion anwendet. Als epimorphes Bild von $R^n$ ist dann auch $M$ wiederum nach (*ii*) noethersch. □

Es folgen die zu den beiden vorstehenden Satzen analogen Sätze für artinsche Moduln.

**3.15 Satz.** *Sei $R$ ein Ring und $M$ ein $R$-Modul. Dann sind äquivalent.*

(*i*) *$M$ ist artinsch.*

(*ii*) *Jede nichtleere Menge von Untermoduln vom $M$ besitzt ein minimales Element.*

(*iii*) *Für jede Familie von Untermoduln $M_i$ mit $i \in I$ gibt es ein endliches $I_0 \subseteq I$ mit $\cap_{i \in I} M_i = \cap_{i \in I_0} M_i$.*

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Wenn (*ii*) nicht gilt, dann gibt es eine nicht-leere Menge $X$, die keinen minimalen Untermodul enthält. Zu jedem Modul aus $X$ gibt es dann stets einen darin echt enthaltenen Modul aus $X$. Man kann daher (mittels Auswahlaxiom) eine absteigende, nicht stationäre Kette definieren.

(*ii*) $\Rightarrow$ (*iii*): In der Menge aller Durchschnitte endlich vieler $M_i$ gibt es ein minimales Element $N = \cap_{i \in I_0} M_i$. Wegen der Minimalität folgt $N \cap M_i = N$ für alle $i \in I$, also $\cap_{i \in I} M_i = N$.

(*iii*) $\Rightarrow$ (*i*): Bilden die $M_i$ eine absteigende Kette, so gibt es ein $j$ für welches $\cap_i M_i = M_j$. Daher ist die Kette stationär. □

**3.16 Satz.** *Sei $M$ ein $R$-Modul.*

(*i*) *Ist $M$ artinsch, so auch $U$ und $M/U$ für alle Untermoduln $U$ von $M$.*

(*ii*) *Sind $U$ und $M/U$ artinsch für einen Untermodul $U$ von $M$, so ist auch $M$ artinsch.*

(*iii*) *Ist $M$ endlich erzeugt und $R$ als $R$-Modul artinsch, so ist $M$ artinsch.*

*Beweis.* (*i*): Absteigende Ketten von Untermoduln in $U$ sind auch absteigende Ketten von Untermoduln von $M$ und werden daher stationär. Analoges gilt für absteigendene Ketten von Untermoduln in $M/U$ und ihre Urbilder in $M$.

(*ii*): Sei $U_i$ eine absteigende Kette in $M$ und $U_i' = U \cap U_i$, $U_i'' = (U_i + U)/U$. Es gibt ein $n$, so daß $U_t' = U_n'$ und $U_t'' = U_n''$ für alle $t \geq n$ gilt. Wir zeigen nun $U_t = U_n$ für $t \geq n$. Sei $x \in U_n$. Wegen $U_t'' = U_n''$ gibt es $y \in U_t$ mit $x - y \in U$. Folglich $x - y \in U \cap U_n = U_n' = U_t' \subseteq U_t$. Es ergibt sich $x \in U_t$.

(*iii*): Zunächst ist $R^n$ nach (*ii*) artinscher Modul, indem man $R^n/R \cong R^{n-1}$ betrachet und Induktion anwendet. Als epimorphes Bild von $R^n$ ist dann auch $M$ wiederum nach (*ii*) artinsch. □

Wir nennen eine echt absteigende Kette wie in Definition 3.7 maximal oder eine Kompositionsreihe, wenn sich die Kette durch Einfügen bzw. Voranstellen oder Anhängen von weiteren Untermoduln (lokal) nicht verlängern läßt. Eine notwendige Bedingung ist also, daß $M_{i+1}$ maximal in $M_i$ für alle $i$ ist. Eine endliche Kompositionsreihe (also eine Kompositionsreihe endlicher Länge) besitzt darüberhinaus notwendigerweise $M$ und $\{0\}$ als Anfangs- und Endpunkt. Eine beliebige, echt absteigende Kette mit Anfangs- und Endpunkt $M$ und $\{0\}$ und mit $M_{i+1}$ maximal in $M_i$ ist umgekehrt eine endliche Kompositionsreihe.

Der folgende Satz steht im Zusammenhang mit dem Satz von Jordan-Hölder-Schreier. Das wird in der Algebra 2 noch einmal genauer und allgemeiner aufgegriffen und bewiesen.

**3.17 Satz.** *Sei $M$ ein Modul. Die Kompositionsreihen von $M$ besitzen alle die gleichen, maximalen Längen* $\mathrm{len}(M)$.

*Beweis.* Lassen wir aus. □

Wir vergleichen nun die Eigenschaften noethersch und artinsch mit der Länge $\mathrm{len}(M)$.

**3.18 Satz.** *Sei $M$ ein $R$-Modul. Dann sind äquivalent:*

(*i*) *$M$ ist noethersch und artinsch.*

(*ii*) *$M$ besitzt eine endliche Kompositionsreihe.*

(*iii*) $\mathrm{len}(M) < \infty$.

*Beweis.* $(i) \Rightarrow (ii)$: Zu jedem Untermodul $U \neq \{0\}$ von $M$ sei $X_U$ die Menge aller von $U$ verschiedener Untermoduln von $U$. Da $M$ noethersch ist und $X_U \neq \emptyset$ gilt, gibt es darin ein bezüglich Inklusion maximales Element $V$, so daß $V$ also ein maximaler Untermodul von $U$ ist.

Wir definieren mit dieser Beobachtung induktiv eine echt absteigende Kette $M = M_0 \supsetneq M_1 \supsetneq \ldots$. Da $M$ artinsch ist, muß diese Kette nach endlich vielen Schritten abbrechen, es muß also $M_n = \{0\}$ für ein $n \in \mathbb{Z}^{\geq 0}$ gelten. Dies liefert eine endliche Kompositionsreihe.

$(ii) \Rightarrow (iii)$: Nach Satz 3.17 stimmen $\mathrm{len}(M)$ und die Länge der endlichen Kompositionsreihe überein, also gilt $\mathrm{len}(M) < \infty$.

$(iii) \Rightarrow (i)$: Ist $M$ nicht noethersch oder nicht artinsch, so gibt es eine unendliche echt auf- oder absteigende Kette von Untermoduln von $M$. Daher gilt $\mathrm{len}(M) = \infty$. □

Als Folgerung aus diesem Satz bemerken wir: Sind die Längen echt absteigender, endlicher Ketten von Untermoduln in $M$ unbeschränkt, so enthält $M$ auch eine echt absteigende Kette von Untermoduln unendlicher Länge.

**3.19 Satz.** *Sei $M$ ein $R$-Modul und $U$ ein Untermodul. Dann gilt* $\mathrm{len}(M) = \mathrm{len}(U) + \mathrm{len}(M/U)$.

*Beweis.* Ketten von Untermoduln von $U$ sind auch Ketten von Untermoduln von $M$. Urbilder von Ketten von Untermoduln von $M/U$ unter dem kanonischen Epimorphismus sind wieder Ketten von Untermoduln von $M$, welche $U$ enthalten. Gilt daher $\mathrm{len}(U) = \infty$ oder $\mathrm{len}(M/U) = \infty$, so folgt $\mathrm{len}(M) = \mathrm{len}(U) + \mathrm{len}(M/U) = \infty$.

Sei nun $\mathrm{len}(U) < \infty$ und $\mathrm{len}(M/U) < \infty$. Die von Kompositionsreihen in $U$ und $M/U$ herrührenden Ketten endlicher Länge in $M$ mit den Anfangs- und Endpunkten $\{0\}$, $U$ und $U$, $M$ können aneinandergehängt werden und liefern eine Kompositionsreihe von $M$ der Länge $\mathrm{len}(U) + \mathrm{len}(M/U)$. Nach Satz 3.17 folgt $\mathrm{len}(M) = \mathrm{len}(U) + \mathrm{len}(M/U)$. □

Aus dem Satz ergibt sich auch $\mathrm{len}(M_1 \oplus M_2) = \mathrm{len}(M_1) + \mathrm{len}(M_2)$.

## 3.4 Moduln und Matrizen über Hauptidealringen

In diesem Abschnitt bezeichnet $R$ einen Hauptidealring. Wir leiten zuerst Aussagen über Matrixnormalformen her und wenden diese dann an, um Aussagen über endlich erzeugte Moduln über Hauptidealringen zu erhalten.

**3.20 Lemma.** *(i) Seien $a_1, \ldots, a_n \in R$. Dann gibt es eine unimodulare Matrix $U$ in $R^{n \times n}$ mit $(a_1, \ldots, a_n)U = (d, 0, \ldots, 0)$, wobei $d = \gcd\{a_1, \ldots, a_n\}$ ist.*

(*ii*) *Seien* $a_1, \ldots, a_n \in R$. *Dann gibt es eine Matrix* $A$ *in* $R^{n\times n}$, *deren erste Zeile gleich* $(a_1, \ldots, a_n)$ *ist und für die* $\det(A) = \gcd\{a_1, \ldots, a_n\}$ *gilt.*

*Beweis.* (*i*): Für $i < j$ gibt es $\lambda, \mu \in R$ mit $\lambda a_i + \mu a_j = c$ und $c = \gcd\{a_i, a_j\}$. Die Matrix

$$T' = \begin{pmatrix} \lambda & -a_j/c \\ \mu & a_i/c \end{pmatrix}$$

ist in $R^{2\times 2}$, unimodular und erfüllt $(a_i, a_j)T' = (c, 0)$. Wir können $T'$ zu einer unimodularen Matrix $T \in R^{n\times n}$ machen, indem wir $T'$ als (erweiterten) Diagonalblock in $I_n$ einbetten, so daß gilt:

$$\begin{aligned}(a_1, \ldots, a_{i-1}, a_i, &a_{i+1}, \ldots, a_{j-1}, a_j, a_{j+1}, \ldots, a_n)T \\ &= (a_1, \ldots, a_{i-1}, c, a_{i+1}, \ldots, a_{j-1}, 0, a_{j+1}, \ldots, a_n).\end{aligned}$$

Indem wir diese Schritte wiederholen und die so erhaltenen, unimodularen Transformationsmatrizen $T$ aufmultiplizieren, erhalten wir schließlich ein unimodulares $U \in R^{n\times n}$ mit $(a_1, \ldots, a_n)U = (d, 0, \ldots, 0)$.

(*ii*): Sei $U$ unimodular mit $(a_1, \ldots, a_n)U = (d, 0, \ldots, 0)$, $d = \gcd\{a_1, \ldots, a_n\}$ und $\det(U) = 1$ (andernfalls eine Spalte von $U$ durch $\det(U)$ dividieren). Sei $B$ die Matrix, deren erste Zeile $(d, 0, \ldots, 0)$ ist und die ansonsten mit $I_n$ übereinstimmt. Dann gilt $\det(B) = d$ und die Matrix $A = BU^{-1}$ erfüllt die Bedingungen. □

**3.21 Definition.** Sei $M = (m_{i,j}) \in R^{n\times m}$ und $I_j = \{\, i \mid 1 \le i \le n \text{ und } m_{i,j} \neq 0\}$. Wir setzen $j_0 = \max\{\, j \mid 1 \le j \le m \text{ und } I_j \neq \emptyset\}$, $i_j = \min I_j$ und definieren: $M$ ist in unterer Spalten-Dreiecksform, wenn $i_1 < \cdots < i_{j_0}$.

Sei $P \subseteq R$ ein Vertretersystem nicht-assoziierter Elemente von $R$ und $R_b \subseteq R$ ein Vertretersystem für die Restklassen $R/Rb$ für jedes $b \in P$. Die Matrix $M$ in unterer Spalten-Dreiecksform heißt in unterer Spalten-Hermite-Normalform, wenn für jedes $j = 1, \ldots, j_0$ gilt: $m_{i_j,j} \in P$ und $m_{i_j,k} \in R_{m_{i_j,j}}$ für $1 \le k < j$.

Entsprechend können obere Spalten- und untere, obere Zeilen-Dreiecksformen für $M$ definiert werden.

**3.22 Satz.** *Zu einer Matrix* $M \in R^{n\times m}$ *gibt es eine unimodulare Matrix* $T \in R^{m\times m}$, *so daß* $MT$ *in unterer Spalten-Dreiecksform ist. Sind Vertretersysteme* $P$ *und* $R_b$ *gegeben, so kann* $T$ *so gewählt werden, daß* $MT$ *in unterer Spalten-Hermite-Normalform ist. In diesem Fall ist* $MT$ *eindeutig durch* $M$ *bestimmt.*

*Beweis.* Für $M = 0$ ist der Satz korrekt. Sei nun $M \neq 0$ und $(a_1, \ldots, a_m) \neq 0$ die $i$-te Zeile von $M$ für $1 \le i \le n$ minimal. Nach Lemma 3.20, (*i*) gibt es ein unimodulares $U_1 \in R^{m\times m}$, so daß die $i$-te Zeile von $MU_1$ von der Form $(d, 0, \ldots, 0)$ mit $d = \gcd\{a_1, \ldots a_m\}$ ist. Alle Zeilen über der $i$-ten Zeile von $MU_1$ sind Null.

Sei $M'$ die Matrix, die aus $M$ durch Streichen der ersten $i$ Zeilen von $M$ und durch Streichen der ersten Spalte von $M$ entsteht. Per Induktion gibt es eine unimodulare Matrix $U' \in R^{(m-1)\times(m-1)}$, so daß $M'U'$ in unterer Spalten-Dreiecksform ist. Wir definieren

$$U_2 = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix} \in R^{m\times m}$$

und $U = U_1U_2$. Die Matrix $U$ ist unimodular. Dann gilt

$$MU = \begin{pmatrix} 0 & 0 \\ d & 0 \\ * & M'U' \end{pmatrix} \in R^{n\times m}$$

(die ersten Nullzeilen können auch wegfallen) und $MU$ ist daher in unterer Spalten-Dreiecksform.

Durch Multiplikation der Spalten mit Einheiten erreichen wir die Bedingung $m_{i_j,j} \in P$, durch Addieren von Vielfachen der $j$-ten Spalte zu den $k$-ten Spalten mit $k < j$ für $j = 1, \ldots, j_0$ erreichen wir die Bedingung $m_{i_j,k} \in R_{m_{i_j,j}}$. Aufgrund der Dreieckecksform bleibt die Matrix oberhalb der $i_j$-ten Zeile unverändert. Diese Transformationen entsprechen ebenfalls der Multiplikation mit einer unimodularen Matrix und liefern die untere Spalten-Hermite-Normalform von $M$.

Die Eindeutigkeitsaussagen erhält man am leichtesten aus der Interpretation der Spalten von $MU$ als Modulbasis: Sei $V$ der von den Spalten von $M$ erzeugte $R$-Untermodul von $R^n$. Aufgrund der Dreiecksform sind die Spalten ungleich Null von $MU$ linear unabhängig und bilden daher eine Basis von $V$.

Wir betrachten zunächst die Eindeutigkeit der Zeilenindizes der Stufen und die Eindeutigkeit bis auf Assoziation der Elemente auf den Stufen. Sei $V_i$ der Untermodul von $V$, dessen Elemente an den ersten $i-1$ Koordinaten Nulleinträge haben. Für die Menge $I = \{i_j \,|\, 1 \le j \le j_0\}$ der Zeilenindizes der Stufen in $MU$ gilt dann $I = \{i \,|\, 1 \le i \le n \text{ und } V_i \neq V_{i+1}\}$. Also ist $I$ unabhängig von $U$ und eindeutig durch $M$ bestimmt. Ferner liefert die Menge der $i$-ten Koordinaten der Elemente aus $V_i$ ein Ideal von $R$, welches gerade durch das Element auf der Stufe in Zeile $i$ erzeugt wird. Daher sind diese Elemente unabhängig von $U$ und bis auf Assoziation eindeutig durch $M$ bestimmt. Die Spalten $b_j$ von $MU$ für $1 \le j \le j_0$ sind dann ebenfalls bis auf Multiplikation mit Einheiten aus $R$ und modulo $\sum_{\nu=j+1}^{j_0} Rb_\nu$ unabhängig von $U$ und eindeutig durch $M$ bestimmt. Hieraus folgt auch die Eindeutigkeit der Hermite-Normalform unter weiterer Reduktion für $j = 1, \ldots, j_0$ nach links. □

**3.23 Satz.** *Sei $M$ ein Untermodul von $R^n$. Dann ist $M$ frei vom Rang $\le n$.*

*Beweis.* Mit $R^n$ ist auch $M$ noethersch und daher endlich erzeugt. Durch Anwendung der Hermite-Normalform auf die durch die Erzeuger gebildete Matrix erhalten wir eine Basis von $M$ in unterer Dreiecksform mit $\leq n$ Elementen. □

Der Eindeutigkeitsbeweis in Satz 3.22 liefert ebenfalls die Existenz einer Basis bestehend aus $\leq n$ Elementen jedes Untermoduls von $R^n$. Wir brauchen dabei nicht zu verwenden, daß $M$ noethersch oder endlich erzeugt ist. Dies ergibt sich als Konsequenz der Überlegung.

Eine unimodulare Matrix $M \in R^{n\times n}$ kann nach dem Satz in eine untere Dreiecksmatrix mit Einheiten bzw. Einsen auf der Diagonalen transformiert werden. Indem noch noch links reduziert (Hermite-Normalform bilden), erhält man $I_n$. Dies zeigt, daß sich jede unimodulare Matrix über $R$ in ein Produkt der elementaren, unimodularen Matrizen $T'$ bzw. $T$ aus dem Beweis von Lemma 3.20 zerlegen läßt. Für einen euklidischen Ring $R$ sind diese Matrizen selbst wieder Produkte der am Ende von Abschnitt 3.1 erwähnten elementaren Matrizen, da im euklidischen Algorithmus wechselseitig Vielfache von Elementen bzw. Spalten voneinander abgezogen werden.

Will man Hermite-Normalformen über einem euklidischen Ring "von Hand" ausrechnen, kann man wie folgt vorgehen. Man führt den euklidischen Algorithmus bezüglich der Elemente der ersten Zeile aus, rechnet aber mit den ganzen Spalten. Hierbei addiert man also in jedem Schritt ein Vielfaches einer Spalte zu einer anderen Spalte. Bei Bedarf multipliziert man Spalten mit Einheiten. Zum Schluß sind in der ersten Zeile alle Elemente bis auf das erste Null. Das erste ist der größte gemeinsame Teiler der Ausgangszeilenelemente und kann auch Null sein. Dann fährt man induktiv mit der zweiten Spalte ab dem zweiten Element fort. Komplexitätstechnisch gibt es wesentlich effizientere Verfahren zur Hermite-Normalformberechnung.

Typische, praktische Verwendungszwecke der Hermite-Normalform sind in etwa die Berechnung einer Basis eines durch ein Erzeugendensystem gegebenen Moduls $M \subseteq R^n$, Test auf Gleichheit, Test auf Inklusion, Summen- und Schnittberechnung zweier solcher Moduln.

Eine $r$-Minore der Matrix $M \in R^{n\times m}$ für $r \leq \min\{n, m\}$ ist die Determinante einer $(r \times r)$-Matrix, die durch Streichen von $n - r$ Zeilen und $m - r$ Spalten aus $M$ entsteht. Wir definieren $d_r(M)$ als den größten gemeinsamen Teiler aller $r$-Minoren von $M$ (ist bis auf Einheiten eindeutig bestimmt).

Wir nennen $M \in R^{n\times m}$ diagonal, wenn $M$ außerhalb der Diagonalen nur Nulleinträge besitzt ($M$ muß also nicht unbedingt quadratisch sein).

**3.24 Lemma.** *(i) Sei $M \in R^{n\times m}$ eine Diagonalmatrix mit den Diagonaleinträgen $a_1, \ldots, a_d$ für $d = \min\{n, m\}$. Dann gibt es unimodulare Matrizen*

*$U \in R^{n\times n}$ und $V \in R^{m\times m}$, so daß $UMV$ diagonal mit den Diagonaleinträgen $b_1, \ldots, b_d$ ist und $b_1 \mid \cdots \mid b_d$ gilt.*

(*ii*) *Seien $M \in R^{n\times m}$ und $U \in R^{n\times n}$, $V \in R^{m\times m}$ unimodulare Matrizen. Dann gilt $d_{r-1}(M) \mid d_r(M)$ und $d_r(M) \sim d_r(UMV)$.*

*Beweis.* (*i*): Sei $M'$ die Diagonalmatrix mit $a_i, a_j$ auf der Diagonalen und gelte $i < j$. Die unimodularen Transformationen gehen wie folgt: Addiere die zweite Zeile von $M'$ zur ersten. Wende $T'$ aus Lemma 3.20, (*i*) von rechts auf $M'$ an. Dies liefert

$$\begin{pmatrix} c & 0 \\ \mu a_j & d \end{pmatrix}$$

mit $c = \gcd\{a_i, a_j\}$ und $d = a_i a_j / c = \operatorname{lcm}\{a_i, a_j\}$. Nun ziehen wir das $\mu a_j/c$-fache der ersten Zeile von der zweiten Zeile ab und erhalten die Diagonalmatrix mit $c = \gcd\{a_i, a_j\}$, $d = \operatorname{lcm}\{a_i, a_j\}$ auf der Diagonalen und es gilt $c \mid d$. Durch sukzessives Vorgehen für $(i, j) = (1, 2), (1, 3), \ldots, (2, 3), (2, 4), \ldots, (n-1, n)$ und Aufmultiplizieren der entsprechenden unimodularen Transformationsmatrizen folgt (*i*).

(*ii*): Eine $r$-Minore kann nach dem Laplaceschen Entwicklungssatz als Linearkombination von $(r-1)$-Minoren geschrieben werden. Daher ist das von den $r$-Minoren erzeugte Hauptideal $I$ in dem von den $(r-1)$-Minoren erzeugten Hauptideal $J$ enthalten. Wegen $I = Rd_r(M)$ und $J = Rd_{r-1}(M)$ folgt $d_{r-1}(M) \mid d_r(M)$.

Eine $r$-Minore von $MV$ kann als $R$-Linearkombination von $r$-Minoren von $M$ geschrieben werden, wegen der Linearität der Determinante in den Spalten und da jede Spalte von $MV$ eine Linearkombination der Spalten von $M$ ist. Daher folgt wie eben $d_r(M) \mid d_r(MV)$. Weil $V$ unimodular ist, gilt auch $d_r(MV) \mid d_r(M)$ für $MV$ und $M = (MV)V^{-1}$. Analog folgt die Aussage für $UM$ und $UMV$. □

**3.25 Satz.** *Sei $M \in R^{n\times m}$ und $d = \min\{n, m\}$. Dann gibt es unimodulare Matrizen $U \in R^{n\times n}$ und $V \in R^{m\times m}$, so daß $UMV$ diagonal ist und für die Diagonalelemente $b_1 \mid \cdots \mid b_d$ gilt. Die $b_i$ sind bis auf Einheiten eindeutig bestimmt.*

*Beweis.* Wir wenden Lemma 3.20, (*i*) abwechselnd auf die erste Zeile (unimodulare Transformation von rechts) und erste Spalte (unimodulare Transformation von links) an. Die auftretenden Elemente in Position $(1, 1)$ erzeugen eine aufsteigende Kette von Idealen, welche stationär wird. Dann gilt aber, daß in der ersten Zeile und Spalte außer dem Element an Position $(1, 1)$ alle Elemente Null sind (das Element an Position $(1, 1)$ darf auch Null sein). Induktiv diagonalisieren wir dann die Matrix, die aus $M$ durch Streichen der ersten Zeile und Spalte entsteht, durch unimodulare Transformationen von links und von rechts. Mit Lemma 3.24, (*i*) erreichen wir die aufsteigende Teilerbedingung.

Es gilt $d_r(UMV) \sim \prod_{i=1}^{r} b_i$ und somit nach Lemma 3.24, $(ii)$ wegen $d_r(UMV) \sim d_r(M)$ auch $b_r \sim d_r(UMV)/d_{r-1}(UMV) \sim d_r(M)/d_{r-1}(M)$ für $d_{r-1}(M) \neq 0$. Gilt $d_r(M) = 0$ für $r$ minimal, so folgt wegen der Teilerbedingung $b_i \neq 0$ für $1 \leq i \leq r-1$ und $b_i = 0$ für $r \leq i \leq d$. Folglich sind die $b_r$ unabhängig von $U, V$ und bis auf Assoziation eindeutig durch $M$ bestimmt. □

**3.26 Definition.** Matrizen $UMV$ in der Diagonalform von Satz 3.25 nennt man auch in Smith-Normalform oder Elementarteilerform. Die Einträge $b_i$ nennt man Elementarteiler von $M$. Man kann zusätzlich fordern, daß die $b_i$ in einem Vertretersystem $P$ liegen.

Will man die Smith-Normalform "von Hand" ausrechnen, kann man wie im Beweis vorgehen. Man tut so, als wollte man die Spalten-Hermite-Normalform ausrechnen und transformiert die erste Zeile in die Form $(*, 0, \ldots, 0)$. Dann fährt man fort, die Zeilen-Hermite-Normalform auszurechen und transformiert die erste Spalte in die Form $(*, 0, \ldots, 0)^{tr}$. Dadurch wird im allgemeinen die erste Zeile wieder durcheinandergebracht, aber $*$ wird "kleiner", bis $*$ alle Elemente der ersten Zeile und Spalte teilt, und diese dann ohne etwas wieder durcheinanderzubringen zu Null gemacht werden können. Komplexitätstechnisch gibt es wieder wesentlich effizientere Verfahren zur Smith-Normalformberechnung.

Wir verwenden jetzt den Satz über die Smith-Normalform, um Aussagen über endlich erzeugte Moduln über Hauptidealringen zu erhalten. Der Satz über die Smith-Normalform kann als Aussage über die Existenz und „diagonale" Lage von Erzeugendensystemen von Moduln und Untermoduln gesehen werden.

Der folgende Existenzsatz ist der erste Teil des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen.

**3.27 Satz.** *Sei $M$ ein endlich erzeugter Modul über dem Hauptidealring $R$. Dann gibt es $b_i \in R \backslash R^{\times}$ mit $b_1 \mid \cdots \mid b_r$ und*

$$M \cong R/b_1R \oplus \cdots \oplus R/b_rR.$$

*Beweis.* Da $M$ endlich erzeugt ist, gibt es $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $f : R^n \to M$. Der Untermodul $N = \ker(f)$ ist nach Satz 3.23 endlich erzeugt und besitzt eine Basis $w_i$ mit $m \leq n$ Elementen. Wir ergänzen diese Basis um $n - m$ Nullspalten $w_{m+1}, \ldots, w_n$ zu einem Erzeugendensystem und bezeichnen die resultierende Matrix mit $A \in R^{n \times n}$. Die Einheitsvektoren $e_i$ in $R^n$ bilden eine Basis von $M$, und es gilt $(e_1, \ldots, e_n)A = (w_1, \ldots, w_n)$. Nach Satz 3.25 angewendet auf $A$ erhalten wir eine andere Basis $e_i'$ von $R^n$ und ein anderes Erzeugendensystem $w_i'$ von $N$, so daß $w_i' = a_i e_i'$ mit $a_i \in R$ und $a_i \mid a_{i+1}$ gilt. Daraus ergibt sich $M \cong R^n/N \cong R/a_1 \oplus \cdots \oplus R/a_nR$. Durch Fortlassen von Einheiten unter den $a_i$ erhalten wir die gewünschten $b_1, \ldots, b_r \in R \backslash R^{\times}$. □

**3.28 Korollar.** *Sei $M$ ein endlich erzeugter Modul über dem Hauptidealring $R$.*

(*i*) *Es gibt einen freien Modul $F$, so daß $M \cong \mathrm{Tor}(M) \oplus F$.*

(*ii*) *Ist $M$ torsionsfrei, so ist $M$ frei.*

(*iii*) *Mit den Bezeichnungen von Satz 3.27 gilt* $\mathrm{Ann}(M) = Rb_r$.

*Beweis.* Mit Satz 3.27 gilt $\mathrm{Tor}(M) \cong \oplus_{b_i \neq 0} R/Rb_i$ und $F = \oplus_{b_i=0} R$. Daraus folgen (*i*) und (*ii*). Aussage (*iii*) ist aufgrund der aufsteigenden Teilerbedingung auch klar. □

Der folgende Eindeutigkeitssatz ist der zweite Teil des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen.

**3.29 Satz.** *Seien $a_i, b_j \in R \backslash R^\times$ mit $a_1 \mid \cdots \mid a_n$, $b_1 \mid \cdots \mid b_m$ und*

$$R/a_1R \oplus \cdots \oplus R/a_nR \cong R/b_1R \oplus \cdots \oplus R/b_mR.$$

*Dann gilt $n = m$ und $a_i \sim b_i$ für $1 \leq i \leq n$.*

*Beweis.* Per Induktion über $n$. Für $n = 0$ muß wegen $b_j \notin R^\times$ auch $m = 0$ gelten und die Behauptung des Satzes ist korrekt.

Für $n \geq 1$ gilt $Ra_n = \mathrm{Ann}(\oplus_i R/a_iR) = \mathrm{Ann}(\oplus_j R/b_jR) = Rb_m$, folglich $a_n \sim b_m$. Wir setzen $I = Ra_n = Rb_m$. Damit können wir $\oplus_i R/a_iR$ und $\oplus_j R/b_jR$ auch als (treue) $R/I$-Moduln betrachten und es gilt $\#\{\nu \mid 1 \leq \nu \leq n \text{ und } a_\nu \sim a_n\} = \mathrm{rank}(\oplus_i R/a_iR) = \mathrm{rank}(\oplus_j R/b_jR) = \#\{\mu \mid 1 \leq \mu \leq m \text{ und } b_\mu \sim b_m\}$. Bezeichnet $d$ diesen Wert, so gilt nach Induktionsvoraussetzung für die $R/I$-Moduln $\oplus_{i=1}^{n-d} R/a_iR$ und $\oplus_{j=1}^{m-d} R/b_jR$, daß $n - d = m - d$ und $a_i + I \sim b_i + I$ in $R/I$ für alle $1 \leq i \leq n - d$ gilt. Wegen $Ra_i \supseteq I$ und $Rb_i \supseteq I$ folgt daraus bereits $Ra_i = Rb_i$ beziehungsweise $a_i \sim b_i$ in $R$. Wir haben also $n = m$ und $a_i \sim b_i$ für alle $1 \leq i \leq n$, was zu zeigen war. □

Wir merken an, daß die $b_i$ auch Null sein können. Die Anzahl der $b_i$ mit $b_i = 0$ entspricht dem Rang von $M$.

Ein typischer, praktischer Verwendungszweck der Smith-Normalform ist damit, die Struktur bzw. Isomorphieklasse eines durch Erzeuger und $R$-Relationen gegebenen Moduls $M$ (also eines Faktormoduls) explizit zu bestimmen. Die Elemente $b_1, \ldots b_r$ aus Satz 3.27 sind entsprechend Satz 3.29 eindeutig bestimmt und heißen Elementarteiler des Moduls $M$.

Der folgende Satz ist die Primelementpotenzvariante des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen.

**3.30 Satz.** *Sei $M$ ein endlich erzeugter Modul über dem Hauptidealring $R$. Dann gibt es Primelemente $\pi_i \in R$, Exponenten $e_i \in \mathbb{Z}^{\geq 1}$ und $n \in \mathbb{Z}^{\geq 0}$ mit*

$$M \cong R/\pi_1^{e_1}R \oplus \cdots \oplus R/\pi_r^{e_r}R \oplus R^n.$$

*Die Isomorphieklasse von $M$ ist durch die $(\pi_i, e_i)$ und durch $n$ bis auf die Reihenfolge oder Assoziation der $\pi_i$ eindeutig bestimmt.*

*Beweis.* Sind $a, b \in R$ teilerfremd, so gilt nach dem chinesischen Restsatz $R/Rab \cong R/Ra \oplus R/Rb$ als $R$-Moduln. Dies erlaubt es, die direkte Summe in Satz 3.27 weiter zu zerlegen, so daß die $b_i$ nur noch Potenzen von Primelementen sind. Dies liefert die Existenz der $\pi_i$, $e_i$ und von $n$.

Umgekehrt kann man mit dem chinesischen Restsatz $R/\pi_1^{e_1}R \oplus \cdots \oplus R/\pi_r^{e_r}R$ auch wieder zu $R/b_1R \oplus \cdots \oplus R/b_mR$ mit $b_i \in R\backslash R^\times$ und $b_i \mid b_{i+1}$ auf genau eine Weise zusammenfassen (für jedes Primelement die Potenzen aufsteigend in eine Zeile schreiben und rechtsbündig anordnen. Die $b_i$ sind dann die Produkte der Primelementpotenzen in den Spalten). Die Eindeutigkeit der $b_i$ nach Satz 3.29 impliziert dann die Eindeutigkeit der $\pi_i$ und $e_i$ wie behauptet. Die Zahl $n$ ist als Rang von $M$ eindeutig bestimmt. □

**3.31 Bemerkung.** Für $R = \mathbb{Z}$ liefert der Satz den Struktursatz über endlich erzeugte, abelsche Gruppen.

Sei $G$ eine endlich erzeugte abelsche Gruppe. Dann gibt es $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $\phi : \mathbb{Z}^n \to G$. Die Bilder der Einheitsvektoren $\phi(e_i)$ sind Erzeuger von $G$, und die Elemente in $\ker(\phi)$ die Relationen. Ist $M \in \mathbb{Z}^{n\times n}$ eine Matrix, deren Spalten Erzeuger von $\ker(\phi)$ bilden, so kann die Struktur von $G$ wie in Satz 3.27 mittels der Smith-Normalform $M' = (b_i\delta_{i,j})_{i,j}$ von $M$ ermittelt werden. Für $\det(M) \neq 0$ gilt $\#G = |\prod_i b_i| = |\det(M')| = |\det(M)|$. Für $\det(M) = 0$ gilt $\#G = \infty$. Der betragsmäßig größte Eintrag in $M'$ ist gleich dem kleinsten Exponenten von $G$. Der Annulator von $G$ ist gleich dem vom kleinsten Exponenten erzeugten Ideal von $\mathbb{Z}$.

Analoges gilt für einen endlich erzeugten Modul $V$ über einem Polynomring $R = k[t]$, wobei $k$ ein Körper ist. Die Anzahlaussagen werden hier am besten durch Dimensionsaussagen ersetzt. Jeder $R$-Modul ist auch ein $k$-Vektorraum. Speziell gilt $\dim_k(R) = \infty$ und $\dim_k(R/Rb) = \deg(b)$ für $b \in R\backslash\{0\}$ nach der Eindeutigkeit der Reste der Polynomdivision. Beschreibt $M \in R^{n\times n}$ den Kern eines Epimorphismus $R^n \to V$ wie eben, so folgt $\dim_k(V) = \sum_i \deg(b_i) = \deg(\prod_i b_i) = \deg(\det(M')) = \deg(\det(M))$ für $\det(M) \neq 0$ und $\dim_k(V) = \infty$ für $\det(M) = 0$ nach Satz 3.27 unter Verwendung der Smith-Normalform $M' = (b_i\delta_{i,j})_{i,j}$ von $M$. Der Annulator von $V$ ist das vom gradgrößten Eintrag von $M'$ erzeugte Hauptideal von $R$.

Wir führen diese Überlegungen weiter und betrachten damit eine Anwendung von Satz 3.27 und Satz 3.29 in der linearen Algebra. Sei $V$ ein endlich dimensionaler $k$-Vektorraum und $\phi \in \mathrm{End}_k(V)$. Wir machen $V$ zu einem endlich erzeugten Modul über dem Hauptidealring $R = k[t]$ durch die Festlegung $tx = \phi(x)$. Nach Satz 3.27 gilt $V \cong R/Rb_1 \oplus \cdots \oplus R/Rb_r$. Seien $v_1, \ldots, v_r \in V$ die Urbilder der Einheitsbasis auf der rechten Seite. Mit $V_i = Rv_i$ gilt $V = V_1 \oplus \cdots \oplus V_r$. Eine $k$-Basis von $V_i$ wird durch $v_i, tv_i, t^2v_i, \ldots, t^{n_i-1}v_i$ mit $n_i = \deg(b_i)$ gegeben. Ist $b_i = \sum_{j=0}^{n_i} b_{i,j}t^j$, so gilt $t^{n_i}v_i = -\sum_{j=0}^{n_i-1} b_{i,j}(t^jv_i)$. Die $k$-Basen der $V_i$ liefern zusammen also eine $k$-Basis von $V$, so daß die Darstellungsmatrix von $\phi$ bezüglich dieser Basis in rationaler kanonischer Form ist. Wir können $V$ entsprechend der obigen Bemerkung 3.31 auch noch in kleinere Bestandteile zerlegen, wenn wir die $b_i$ faktorisieren.

Wir betrachten den Fall $V \cong R/R(t-a)^n$ und $v$ Urbild der Eins auf der rechten Seite. Eine Basis von $V$ wird wie eben betrachtet durch $v, tv, \ldots, t^{n-1}v$ gegeben. Eine andere Basis von $V$ erhalten wir mit $v, (t-a)v, (t-a)^2v, \ldots, (t-a)^{n-1}v$, denn die $t$-Potenzen und die $(t-a)$-Potenzen bilden beide $k$-Basen von $R/R(t-a)^r$. Wegen $t(t-a)^i = (t-a)^{i+1} + a(t-a)^i$ und $t(t-a)^{r-1} = (t-a)^r + a(t-a)^{r-1} \equiv a(t-a)^{r-1} \bmod (t-a)^r$ erhalten wir für diese Basis die üblichen Jordankästchen. Eine solche Zerlegung in mehrere Jordankästchen ist somit immer möglich, wenn $k$ algebraisch abgeschlossen ist. Wir erhalten darüberhinaus eine Zerlegung der Darstellungsmatrix $M$ von $\phi$ in der Form $M = M_1 + M_2$, wobei $M_1$ eine Diagonalmatrix und $M_2$ eine strikt untere Dreiecksmatrix (also nilpotent) ist. Entsprechend zerlegt sich $\phi$ in $\phi = \phi_1 + \phi_2$.

Ist $M$ die Darstellungsmatrix von $\phi$ bezüglich der Basis $v_i$ von $V$, so bilden die Spalten von $tI_n - M$ eine Basis der Kerns $N$ des Epimorphismus $R^n \to V$, welcher $e_i$ nach $v_i$ abbildet. Die Spalten sind nämlich einerseits im Kern $N$ enthalten. Auf der anderen Seite gilt für den von den Spalten von $tI_n - M$ erzeugten Untermodul $N'$ von $N$ die Gleichung $\dim_k(R^n/N') = \deg(\deg(tI_n - M)) = n$ wie oben dargelegt. Aus Dimensionsgründen ist daher $N' \subsetneq N$ nicht möglich und es gilt $N' = N$. Mit Hilfe von $tI_n - M$ und der Smith-Normalform kann man also die rationale kanonische Form oder die Jordan-Normalform von $M$ berechnen. In der obigen Notation ist $b_r$ (der Erzeuger des Annulators) das Minimalpolynom und $\det(tI_n - M) = \prod_i b_i$ das charakteristische Polynom von $\phi$.

Darstellungsmatrizen $M_1, M_2$ von $\phi$ bezüglich verschiedener Basen von $V$ liefern verschiedene charakteristische Matrizen $tI_n - M_1, tI_n - M_2$ und Kerne $N_1, N_2$ von $R^n$. Es gilt aber, daß $R^n/N_1$ und $R^n/N_2$ isomorph sind. Wegen der Eindeutigkeit der Elementarteiler stimmen daher die Smith-Normalformen von $tI_n - M_1$ und $tI_n - M_2$ überein. Gleichsetzen zeigt, daß $tI_n - M_1$ und $tI_n - M_2$ als Matrizen äquivalent über $R$ sind. Daher sind $M_1$ und $M_2$ genau dann ähnlich über $k$, wenn

$tI_n - M_1$ und $tI_n - M_2$ über $R$ äquivalent sind (Satz von Frobenius).

Nach Satz 3.11 gilt $\det(tI_n - M)R^n \subseteq N$ und äquivalenterweise $\det(tI_n - M)V = \{0\}$. Das ist der Satz von Cayley-Hamilton: Wenn man $\phi$ bzw. $M$ in sein charakteristisches Polynom $\det(tI_n - M)$ einsetzt, kommt Null heraus.

# Kapitel 4

# Moduln II

In diesem Kapitel werden das Tensorprodukt und die Begriffe projektiv, flach und lokal frei behandelt.

## 4.1 Tensorprodukte

Wir wollen auch kurz etwas zum Tensorprodukt sagen. Tensorprodukte bildet man von $R$-Moduln oder $R$-Algebren, und sie sind wieder $R$-Moduln bzw. $R$-Algebren. Wir betrachten vornehmlich den ersten Fall. Zur Vereinfachung sei $R$ ein kommutativer Ring und $M$, $N$ Moduln über $R$ (links und rechts). Dies ist für das folgende keine wesentliche Einschränkung, spart aber ein paar Fälle und etwas Notation. Beim Tensorprodukt $M \otimes_R N$ handelt es sich um einen $R$-Modul, welcher von formalen Produkten $m \otimes n$ für $m \in M$ und $n \in N$ erzeugt wird. Die Elemente sind also von der Form $\sum_i m_i \otimes n_i$ für $m_i \in M$ und $n_i \in N$. Hierbei soll sich $\otimes$ wirklich wie eine Multiplikation verhalten, nur daß sie nicht „ausgeführt“ wird sondern nur generisch ausgeführt wird (also unter Eingabe von $m$ und $n$ eben den „abstrakten Wert“ $m \otimes n$ zurückliefert). Entsprechend wird gefordert $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ und analog für $n_1, n_2$. Die Angabe von $R$ soll bedeuten, daß $mr \otimes n = m \otimes rn$ ist. Außerdem gelte $r(m \otimes n) = rm \otimes n = m \otimes rn$. Hier muß man im Nichtkommutativen etwas aufpassen, ob man von links oder rechts oder innen oder außen multiplizieren will. Beim Tensorprodukt von $R$-Algebren $M$ und $N$ soll per Definition auch noch $(m_1 \otimes n_1) \cdot (m_2 \otimes n_2) = (m_1 m_2) \otimes (n_1 n_2)$ gelten, doch dazu später.

**4.1 Definition.** Der $R$-Modul $P$ zusammen mit einer $R$-bilinearen Abbildung $h : M \times N \to P$ heißt Tensorprodukt von $M$ und $N$ über $R$, wenn folgendes gilt. Ist $g$ eine $R$-bilineare Abbildung $M \times N \to Q$ für einen beliebigen, weiteren $R$-Modul $Q$, so gibt es genau eine $R$-lineare Abbildung $f : P \to Q$ mit $g = f \circ h$.

**4.2 Satz.** *Für alle $R$-Moduln $M$ und $N$ existiert ein Tensorprodukt von $M$ und $N$ über $R$. Je zwei Tensorprodukte von $M$ und $N$ über $R$ sind isomorph.*

*Beweis.* Zunächst zur Existenz. Sei $V$ der von den Paaren $(m,n) \in M \times N$ erzeugte, freie $R$-Modul und $I$ der Untermodul von $V$, welcher von den Elementen der Form $(m_1+m_2,n)-(m_1,n)-(m_2,n)$, $(m,n_1+n_2)-(m,n_1)-(m,n_2)$, $(rm,n)-(m,rn)$ und $r(m,n)-(rm,n)$ erzeugt wird. Wir definieren die Abbildung $h : M \times N \to V/I$ durch $h(m,n) = (m,n)+I$. Die $R$-Bilinearität von $h$ folgt unmittelbar aufgrund der Definition von $I$. Wir behaupten, daß $V/I$ zusammen mit $h$ ein Tensorprodukt von $M$ und $N$ über $R$ ist.

Da $V$ frei ist, können wir eine vorgegebene, bilineare Abbildung $g : M \times N \to Q$ zu einer linearen Abbildung $f' : V \to Q$ durch $f'((m,n)) = g(m,n)$ machen. Nun gilt $I \subseteq \ker(f')$ und durch Abspalten des Restklassenhomomorphismus $V \to V/I$ erhalten wir $f : V/I \to Q$. Damit gilt $f \circ h = g$, und die Existenz von $f$ ist nachgewiesen. Es gibt aber auch nur einen einzigen Homomorphismus $f : V/I \to Q$ mit $f \circ h = g$, denn das Bild von $h$ ist ein Erzeugendensystem von $V/I$. Damit ist $V/I$ zusammen mit $h$ tatsächlich ein Tensorprodukt von $M$ und $N$ über $R$.

Jetzt zur Eindeutigkeit bis auf Isomorphie. Sind $B$ und $B'$ zwei Tensorprodukte von $M$ und $N$ über $R$ mit den zugehörigen bilinearen Abbildungen $h$ und $h'$, so gibt es $f \in \mathrm{Hom}_R(B,B')$ und $f' \in \mathrm{Hom}_R(B',B)$ mit $h' = f \circ h$ und $h = f' \circ h'$, also $h = f' \circ f \circ h$. Aufgrund der Eindeutigkeitsaussage für $B$ folgt $f' \circ f = \mathrm{id}_B$, und durch Symmetrie $f \circ f' = \mathrm{id}_{B'}$. Also sind $B$ und $B'$ isomorph. □

**4.3 Definition.** Für je zwei $R$-Moduln $M$ und $N$ bezeichne $M \otimes_R N$ ein (festgewähltes) Tensorprodukt von $M$ und $N$ über $R$ mit der bilinaren Abbildung $\cdot \otimes \cdot : M \times N \to M \otimes_R N$, $(x,y) \mapsto x \otimes y$.

Die Menge der bilinearen Abbildungen $M \times N \to Q$ bildet einen $R$-Modul, welcher in natürlicher Weise isomorph zum $R$-Modul $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N,Q))$ ist. Aufgrund der Eindeutigkeit von $f$ in Definition 4.1 erhalten wir eine Abbildung $\phi : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,Q)) \to \mathrm{Hom}_R(M \otimes_R N, Q)$, $g \mapsto f$ mit $g(x,y) = f(x \otimes y)$. Diese ist bijektiv: Sind $g_1$ und $g_2$ bilineare Abbildungen und $f_1$, $f_2$ die zugehörigen linearen Abbildungen und gilt $f_1 = f_2$, so ergibt sich auch $g_1 = f_1 \circ (\cdot \otimes \cdot) = f_2 \circ (\cdot \otimes \cdot) = g_2$. Also ist $\phi$ injektiv. Da für jedes lineare $f$ die Abbildung $g = f \circ (\cdot \otimes \cdot)$ bilinear ist, ist $\phi$ auch surjektiv. Es gilt also $\mathrm{Hom}_R(M \otimes_R N, Q) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,Q))$ (in natürlicher Weise als $R$-Moduln). Die Abbildung $\cdot \otimes \cdot$ ist damit „die universelle“, auf $M \times N$ definierte bilineare Abbildung.

Die Elemente von $M \otimes_R N$ wie im Satz konstruiert sind also von der Form $\sum_i m_i \otimes n_i$, wobei $\otimes$ die Axiome einer Multiplikation erfüllt und mit der Multiplikation mit Elementen aus $R$ verträglich ist. Speziell handelt es sich bei der Menge $\{m \otimes n \mid m \in M, n \in N\}$ um ein Erzeugendensystem von $M \otimes_R N$.

Seien nun $M_1, M_2, N_1, N_2$ Moduln über $R$ und $f_i \in \mathrm{Hom}_R(M_i, N_i)$. Wir erhalten die Produktabbildung $f_1 \times f_2 : M_1 \times M_2 \to N_1 \times N_2$. Durch Komposition mit der bilinearen Abbildung $h_N : N_1 \times N_2 \to N_1 \otimes_R N_2$ ergibt dies eine bilineare Abbildung $M_1 \times M_2 \to N_1 \otimes N_2$, und wir können die bilineare Abbildung $h_M : M_1 \times M_2 \to M_1 \otimes M_2$ abspalten. Dies liefert eine lineare Abbildung $M_1 \otimes M_2 \to N_1 \otimes N_2$, welche mit $T(f_1, f_2)$ und als das Tensorprodukt von $f_1$ und $f_2$ bezeichnet wird. Sie ist durch $T(f_1, f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ eindeutig bestimmt.

Zusammen erhalten wir eine Abbildung $\mathrm{Hom}_R(M_1, N_1) \times \mathrm{Hom}_R(M_2, N_2) \to \mathrm{Hom}_R(M_1 \otimes_R M_2, N_1 \otimes_R N_2)$, $(f_1, f_2) \mapsto T(f_1, f_2)$. Wegen $T(f_1, f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ und $(f + g)(x) = f(x) + g(x)$ für $f, g \in \mathrm{Hom}_R(M_i, N_i)$ ist diese Abbildung bilinear, und somit erhalten wir eine lineare Abbildung

$$\mathrm{Hom}_R(M_1, N_1) \otimes_R \mathrm{Hom}_R(M_2, N_2) \to \mathrm{Hom}_R(M_1 \otimes_R M_2, N_1 \otimes_R N_2),$$

welche durch $f_1 \otimes f_2 \mapsto T(f_1, f_2)$ definiert ist. Mittels dieses Homomorphismus können wir $f_1 \otimes f_2$ also stets auch als Element von $\mathrm{Hom}_R(M_1 \otimes_R M_2, N_1 \otimes_R N_2)$ auffassen. Unter Verwendung von Satz 4.4, $(ii)$ ist es nicht schwer zu beweisen, daß dies ein Isomorphismus ist, wenn die $M_i$ und $N_i$ beispielsweise endlich erzeugt und frei sind.

Die universelle Eigenschaft der Tensorprodukte und etwas „Diagrammjagd“ oder die konkrete Formel $T(f_1, f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ zeigen die folgende, bifunktorielle Eigenschaft von $T(\cdot, \cdot)$: Sind $P_1, P_2$ weitere $R$-Moduln und $g_i \in \mathrm{Hom}_R(N_i, P_i)$, so gilt $T(g_1 \circ f_1, g_2 \circ f_2) = T(g_1, g_2) \circ T(f_1, f_2)$.

Ein wichtiger Spezialfall ist $M_2 = N_2 = P_2 = Q$ und $f_2 = g_2 = \mathrm{id}$. Tensorieren mit $Q$ liefert dann einen Funktor in der Kategorie der $R$-Moduln, ein Homomorphimus $f : M \to N$ wird auf $T(f, \mathrm{id}) : M \otimes_R Q \to N \otimes_R Q$ mit $T(f, \mathrm{id})(m \otimes q) = f(m) \otimes q$ abgebildet. Dieser wird in Satz 4.4, $(iii)$ angewendet.

**4.4 Satz.** *Seien $M, N, P, Q$ $R$-Moduln und $M_i$ eine Familie von $R$-Moduln.*

$(i)$ $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$ *unter* $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$.

$(ii)$ $M \otimes_R N \cong N \otimes_R M$ *unter* $x \otimes y \mapsto y \otimes x$.

$(iii)$ $(\coprod_i M_i) \otimes_R N \cong \coprod_i (M_i \otimes_R N)$ *unter* $(\sum_i x_i) \otimes y \mapsto \sum_i (x_i \otimes y)$. *Das Tensorprodukt und die direkte Summenbildung sind also vertauschbar.*

$(iv)$ *Ist* $M \to N \to P \to 0$ *eine exakte Sequenz, dann ist auch die zugehörige, mit $Q$ tensorierte Sequenz* $M \otimes_R Q \to N \otimes_R Q \to P \otimes_R Q \to 0$ *exakt.*

*Beweis.* $(i)$: Wir zeigen die Existenz eines Homomorphismus $f : (M \otimes_R N) \otimes_R P \to M \otimes_R (N \otimes_R P)$ mit $(x \otimes y) \otimes z \to x \otimes (y \otimes z)$. Wollen wir dies als Definition für $f$

nehmen, ergibt sich das Problem, daß wir die Wohldefiniertheit von $f$ nachweisen müssen. Denn implizit extrahieren wir aus $(x \otimes y) \otimes z$ das unter Umständen nicht eindeutig bestimmte Paar $(x, y, z)$ und definieren damit das Bild $x \otimes (y \otimes z)$. Um diesem Problem entgegenzutreten, verwendet man standardmäßig die universelle Eigenschaft des Tensorprodukts.

Für $z \in P$ starten wir zunächst mit $g_z : M \times N \to M \otimes_R (N \otimes_R P)$, $g_z(x, y) = x \otimes (y \otimes z)$. Dies ist eine wohldefinierte bilineare Abbildung, so daß es $f_x : M \otimes N \to M \otimes_R (N \otimes_R P)$ mit $f_z(x \otimes y) = x \otimes (y \otimes z)$ gibt. Nun sei $g : (M \otimes_R N) \times P \to M \otimes_R (N \otimes_R P)$, $g(x \otimes y, z) = f_z(x \otimes y) = x \otimes (y \otimes z)$. Dies ist ebenfalls eine wohldefinierte, bilineare Abbildung. Damit erhalten wir schließlich den Homomorphismus $f : (M \otimes_R N) \otimes_R P \to M \otimes_R (N \otimes_R P)$ mit $(x \otimes y) \otimes z \to x \otimes (y \otimes z)$.

Analoge Argumente zeigen die Existenz eines Homomorphismus $f' : M \otimes_R (N \otimes_R P) \to (M \otimes_R N) \otimes_R P$ mit $x \otimes (y \otimes z) \to (x \otimes y) \otimes z$. Da es bei den Elementen um Erzeugende der Tensorprodukte handelt, ergibt sich $f \circ f' = \mathrm{id}$ und $f' \circ f = \mathrm{id}$.

Ein im Prinzip gleicher, aber kompakterer Beweis kann mit Hilfe des Lemmas von Yoneda geführt werden (siehe S. 116). Das geht wie folgt:

$$\begin{aligned} \mathrm{Hom}_R((M \otimes_R N) \otimes_R P, \cdot) &\cong \mathrm{Hom}_R(M \otimes_R N, \mathrm{Hom}_R(P, \cdot)) \\ &\cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, \mathrm{Hom}_R(P, \cdot))) \\ &\cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N \otimes_R P, \cdot)) \\ &\cong \mathrm{Hom}_R(M \otimes_R (N \otimes_R P), \cdot). \end{aligned}$$

Also gilt auch $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$, und zwar unter $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$, was man durch Nachverfolgen der einzelnen Isomorphismen sehen kann.

$(ii)$: Geht analog zu $(i)$ (direkt und mit Lemma von Yoneda).

$(iii)$: Wir definieren die bilineare Abbildung $g : (\coprod_i M_i) \times N \to \coprod_i (M_i \otimes N)$ durch $((\sum_i x_i), y) \mapsto \sum_i (x_i \otimes y)$, wobei wir die direkte Summeneigenschaft von $\coprod_i M_i$ verwenden. Daraus erhalten wir den Homomorphismus $f : (\coprod_i M_i) \otimes N \to \coprod_i (M_i \otimes N)$ mit $(\sum_i x_i) \otimes y \mapsto \sum_i (x_i \otimes y)$. Umgekehrt definieren wir die bilineare Abbildung $g_i' : M_i \times N \to (\coprod_i M_i) \otimes N$ durch $(x_i, y) \mapsto x_i \otimes y$ und erhalten den Homomorphismus $f_i' : M_i \otimes N \to (\coprod_i M_i) \otimes N$ mit $x_i \otimes y \mapsto x_i \otimes y$. Die universelle Eigenschaft der direkten Summe angewendet auf die $f_i'$ liefert jetzt einen Homomorphismus $f' : \coprod_i (M_i \otimes N) \to (\coprod_i M_i) \otimes N$ mit $\sum_i (x_i \otimes y) \mapsto (\sum_i x_i) \otimes y$. Die Abbildungsvorschriften für $f$ und $f'$ schreiben die Bilder von Erzeugendensystemen vor. Es ergibt sich $f \circ f' = \mathrm{id}$ und $f' \circ f = \mathrm{id}$.

Die Aussage $(iii)$ wird in Satz 4.5 noch einmal in allgemeinerer Form bewiesen.

$(iv)$: Seien $f_1 : M \to N$ und $f_2 : N \to P$ die Homomorphismen aus der exakten Sequenz und $g_1 : M \otimes_R Q \to N \otimes_R Q$ und $g_2 : N \otimes_R Q \to P \otimes_R Q$

die zugehörigen, tensorierten Homomorphismen. Die Aussage $0 \otimes_R Q = 0$ wird in Lemma 4.6, $(i)$ bewiesen.

Wir zeigen zuerst, daß $g_2$ surjektiv ist. Jedes Element aus $P \otimes_R Q$ ist eine endliche Summe von Elementen der Form $p \otimes q$. Daher genügt es zu zeigen, daß jedes dieser Elemente im Bild von $g_2$ liegt. Zu $p \in P$ gibt es aber $n \in N$ mit $f_2(n) = p$ nach Voraussetzung. Dann gilt $g_2(n \otimes q) = f(n) \otimes q = p \otimes q$, was zu zeigen war. Dies ergibt die Exaktheit bei $P \otimes_R Q$.

Da das Tensorieren der Nullabbildung die Nullabbildung liefert, folgt wegen $f_2 \circ f_1 = 0$ auch $g_2 \circ g_1 = 0$, also $\mathrm{im}(g_1) \subseteq \ker(g_2)$. Sei nun $I = \mathrm{im}(g_1)$ und $g_2' : N \otimes_R Q/I \to P \otimes_R Q$ der nach dem Homomorphiesatz eindeutig bestimmte Homomorphismus mit $g_2'(n \otimes q + I) = g_2(n \otimes q)$. Zum Nachweis der Exaktheit bei $N \otimes_R Q$ müssen wir beweisen, daß $g_2'$ injektiv ist. Dazu konstruieren wir einen Homomorphismus $h : P \otimes_R Q \to N \otimes_R Q/I$ mit $h \circ g_2' = \mathrm{id}$: Für $p \in P$ und $q \in Q$ sei $n \in N$ mit $f_2(n) = p$. Wir definieren $h' : P \times Q \to N \otimes_R Q/I$ durch $h'(p, q) := n \otimes q + I$. Dies ist wohldefiniert: Für $n_1, n_2 \in N$ mit $f_2(n_1) = f_2(n_2) = p$ gilt $f_2(n_1 - n_2) = 0$, also gibt es $m \in M$ mit $n_1 - n_2 = f_1(m)$. Dann folgt $n_1 \otimes q - n_2 \otimes q = (n_1 - n_2) \otimes q = f_1(m) \otimes q \in I$. Außerdem ist $h'$ bilinear, wie leicht zu sehen ist. Es gibt also einen Homomorphismus $h : P \otimes_R Q \to N \otimes_R Q/I$ mit $h(p \otimes q) = n \otimes q + I$. Nach Konstruktion gilt $h \circ g_2' = \mathrm{id}$ auf der Menge der Elemente der Form $n \otimes q + I$ und damit auch auf ganz $N \otimes_R Q/I$.

Man kann $(iv)$ auch kürzer beweisen. Tensorieren mit $Q$ ist nämlich ein linksadjungierter Funktor des Funktors $\mathrm{Hom}_R(Q, \cdot)$, denn es besteht die natürliche Äquivalenz

$$\mathrm{Hom}_R(\cdot \otimes Q, \cdot) \cong \mathrm{Hom}_R(\cdot, \mathrm{Hom}_R(Q, \cdot)).$$

Aufgrund allgemeiner Überlegungen ist dann Tensorieren mit $Q$ rechtsexakt, es gilt also $(iv)$ (siehe Kapitel 6). □

Bei nicht-kommutativen Ringen macht $(ii)$ wenig Sinn, da man sonst die Multiplikationen von links oder rechts oder innen oder außen umordnen muß und leicht durcheinander kommen kann.

Die Aussage $(iii)$ ist ein Spezialfall der folgenden Aussage für Kolimites von Diagrammen von $R$-Moduln (siehe Seite 119ff.).

**4.5 Satz.** *Sei $N$ ein $R$-Modul und $\mathcal{D}$ ein Diagramm von $R$-Moduln. Sei $\mathcal{D} \otimes_R N$ das Diagramm, welches aus $\mathcal{D}$ durch Tensorieren der in $\mathcal{D}$ vorkommenden Moduln mit $N$ entsteht. Dann gilt*

$$(\varinjlim \mathcal{D}) \otimes_R N \cong \varinjlim (\mathcal{D} \otimes_R N).$$

*Das Tensorprodukt und die Kolimesbildung sind also vertauschbar.*

*Beweis.* Wir zeigen, daß $\varinjlim(\mathcal{D}\otimes_R N)$ ein Tensorprodukt von $\varinjlim\mathcal{D}$ und $N$ ist. Sei $g : (\varinjlim\mathcal{D}) \times N \to Q$ bilinear. Für jedes $D_i$ in $\mathcal{D}$ sei $\iota_i : D_i \to \varinjlim\mathcal{D}$ die Injektion. Zurückziehen entlang $\iota_i$ liefert bilineare Abbildungen $g_i : D_i \times N \to Q$, und lineare Abbildungen $f_i : D_i \otimes_R N \to Q$. Da Tensorieren ein Funktor ist, bilden die $D_i \otimes_R N$ das Diagramm $\mathcal{D} \otimes_R N$. Etwas Diagrammjagd und die universelle Eigenschaft von Tensorprodukten zeigt, daß die $f_i$ einen Morphismus $\mathcal{D} \otimes_R N \to Q$ bilden. Die universelle Eigenschaft vom Kolimes zeigt, daß es eine lineare Abbildung $f : \varinjlim(\mathcal{D} \otimes_R N) \to Q$ gibt. Die Konstruktionsschritte von $f$ sind jeder für sich genommen eindeutig umkehrbar, so daß insbesondere $f$ eindeutig durch $g$ bestimmt ist. Für $Q = \varinjlim(\mathcal{D} \otimes_R N)$ erhalten wir die Strukurabbildung $h : (\varinjlim\mathcal{D}) \times N \to \varinjlim(\mathcal{D} \otimes_R N)$ wie in $(i)$ aus der Identität auf $\varinjlim(\mathcal{D} \otimes_R N)$.

Alternativ kann man auch allgemein argumentieren, daß linksadjungierte Funktoren Kolimites in Kolimites überführen. Das geht unter Verwendung von Satz **??** im wesentlichen so:

$$\begin{aligned}
\mathrm{Hom}_R((\varinjlim\mathcal{D}) \otimes_R N, \cdot) &\cong \mathrm{Hom}_R(\varinjlim\mathcal{D}, \mathrm{Hom}_R(N, \cdot)) \\
&\cong \varinjlim \mathrm{Hom}_R(\mathcal{D}, \mathrm{Hom}_R(N, \cdot)) \\
&\cong \varinjlim \mathrm{Hom}_R(\mathcal{D} \otimes_R N, \cdot) \\
&\cong \mathrm{Hom}_R(\varinjlim(\mathcal{D} \otimes_R N), \cdot).
\end{aligned}$$

Mit dem Lemma von Yoneda schließt man jetzt $(\varinjlim\mathcal{D}) \otimes_R N \cong \varinjlim(\mathcal{D} \otimes_R N)$. □

Hier sind ein paar einfache Formeln, die bei der Berechnung von vorgelegten Tensorprodukten hilfreich sind.

**4.6 Lemma.** *Seien $M, N$ Moduln über $R$.*

(*i*) *Ist $N = Rn$ frei vom Rang eins, so gilt $M \otimes_R N \cong M$ unter $m \otimes rn \mapsto rm$. Ist $N = \{0\}$, so gilt $M \otimes_R N \cong \{0\}$.*

(*ii*) *Sind die $m_i$ und $n_j$ ein Erzeugendensystem (eine Basis) von $M$ bzw. $N$, so ist $m_i \otimes n_j$ ein Erzeugendensystem (eine Basis) von $M \otimes_R N$.*

*Sind die $n_j$ eine Basis von $N$, so schreibt sich jedes Element aus $M \otimes_R N$ als Summe $\sum_j x_j \otimes n_j$ mit eindeutig bestimmten $x_j \in M$.*

(*iii*) *Es gilt $(M/I) \otimes_R (N/J) \cong M \otimes_R N/(I \otimes N + M \otimes J)$ für Untermoduln $I \subseteq M$ und $J \subseteq N$ unter $(m + I) \otimes (n + J) \mapsto (m \otimes n) + (I \otimes N + M \otimes J)$.*

(*iv*) *Es gelte $\sum_i m_i \otimes n_i = 0$ für $m_i \in M$ und $n_i \in N$, wobei die $n_i$ ein Erzeugendensystem von $N$ bilden. Dann gibt es $a_{i,j} \in R$ und $m'_j \in M$ mit $m_i = \sum_j a_{i,j} m'_j$ und $\sum_i a_{i,j} n_i = 0$ für alle $j$.*

*Beweis.* $(i)$: Sei $N = Ry$ und $h : M \times N \to M$ die durch $(x, ry) \mapsto rx$ definierte, bilineare Abbildung. Jede bilineare Abbildung $f : M \times N \to P$ liefert mit $x \mapsto f(x, y)$ eine lineare Abbildung $g : M \to P$ mit $f = g \circ h$, wobei $g$ wegen der Surjektivität von $h$ eindeutig bestimmt ist. Die Eindeutigkeit des Tensorprodukts ergibt $M \cong M \otimes_R N$.

Bilineare Abbildungen auf $M \times \{0\}$ sind alles Nullabbildungen, entsprechen also den linearen Abbildungen auf $\{0\}$. Mit der bilinearen Abbildung $h : M \times \{0\} \to \{0\}$ liefert eine ähnliche Schlußweise wie eben $\{0\} \cong M \otimes_R \{0\}$.

$(ii)$: Für $v = \sum_i \lambda_i m_i$ und $w = \sum_j \mu_j n_j$ gilt $v \otimes w = \sum_{i,j} \lambda_i \mu_j (m_i \otimes n_j)$. Da jedes Element in $M \otimes_R N$ eine Summe von Elementen der Form $v \otimes w$ ist, folgt die Aussage über die Erzeugendensysteme.

Sei $N$ frei mit Basis $n_j$. Aus $N = \oplus_j Rn_j$ folgt $M \otimes_R N \cong \oplus_j (M \otimes_R Rn_j) \cong \oplus_j M$ nach Satz 4.4, $(ii)$ und nach $(i)$. Unter den Isomorphismen wird $\sum_j x_j \otimes n_j$ mit $x_j \in M$ auf das Element von $\oplus_j M$ abgebildet, welches $x_j$ an der $j$-ten Koordinate enthält. Die $x_j$ sind also durch das Element $\sum_j x_j \otimes n_j$ eindeutig bestimmt. Dies zeigt die zweite Aussage in $(ii)$.

Ferner bilden hier die $m_i \otimes n_j$ eine Basis des $j$-ten Komponentenmodul $M$, so daß $m_i \otimes n_j$ für $i, j$ eine Basis von $M \otimes_R N$ ist.

$(iii)$: Ergibt sich durch dreimalige Anwendung von Satz 4.4, $(iii)$: Im folgenden sind die angegebenen „Untermoduln“ geeignet einzubetten. Es gilt $M/I \otimes N/J \cong (M/I \otimes N)/(M/I \otimes J)$ (tensorieren mit $M/I \otimes -$) und $M/I \otimes N \cong (M \otimes N)/(I \otimes N)$ (tensorieren mit $- \otimes N$) und $M/I \otimes J \cong (M \otimes J)/(I \otimes J)$ (tensorieren mit $- \otimes J$). Wir erhalten $M/I \otimes N/J \cong ((M \otimes N)/(I \otimes N))/((M \otimes J)/(I \otimes J)) \cong (M \otimes N)/(I \otimes N + M \otimes J)$, was zu zeigen war.

Eine bilineare Abbildung auf $(M/I) \times (N/J)$ entspricht den bilinearen Abbildungen auf $M \times N$, welche auf $I \times N$ und $M \times J$ Null sind, und diese wiederum entsprechen den linearen Abbildungen auf $M \otimes N$, deren Kern $I \otimes N + M \otimes J$ enthält. Dies verdeutlicht ebenfalls $M/I \otimes N/J \cong M \otimes N/(I \otimes N + M \otimes J)$.

$(iv)$: Gibt es solche Elemente $a_{i,j}$ und $m'_i$, so folgt $\sum_i m_i \otimes n_i = \sum_i \big(\sum_j a_{i,j} m'_j\big) \otimes n_i = \sum_j m'_j \otimes \big(\sum_i a_{i,j} n_i\big) = 0$.

Für die Rückrichtung sei $V$ frei und $f : V \to N$ surjektiv, so daß $n_i = f(g_i)$ für eine Basis $g_i$ von $V$ gilt. Die Sequenz $U \to V \to N \to 0$ mit $U = \ker(f)$ ist exakt. Aufgrund von Theorem 4.4, $(iii)$ ist damit auch die Sequenz $M \otimes_R U \to M \otimes_R V \to M \otimes_R N \to 0$ exakt. Weil das Element $\sum_i m_i \otimes g_i$ auf Null abgebildet wird, gibt es aufgrund der Exaktheit bei $V$ Elemente $m'_j \in M$ und $y_j \in U$ mit $\sum_i m_i \otimes g_i = \sum_j m'_j \otimes y_j$. Seien $a_{i,j} \in R$ mit $y_j = \sum_i a_{i,j} g_i$. Nach dem Beweis von $(ii)$ folgt aus $\sum_i m_i \otimes g_i = \sum_j m'_j \otimes \big(\sum_i a_{i,j} g_i\big) = \sum_i \big(\sum_j a_{i,j} m'_j\big) \otimes g_i$ durch Koeffizientenvergleich, daß $\sum_j a_{i,j} m'_j = m_j$ ist. Schließlich gilt $0 = f(y_j) = \sum_i a_{i,j} n_i$ für alle $j$. □

Die Aussage $(iv)$ führt das Rechnen in Tensorprodukten auf lineare Algebra zurück. Die Definition des Tensorprodukts ist dafür nicht besonders geeignet. Die $a_{i,j}$ können nach dem Beweis als „Strukturkonstanten“ gewählt werden.

Ist $R$ ein Ring und $I$ ein Ideal, so gilt $I \otimes_R R \cong I$ nach $(i)$, denn wegen $1 \in R$ ist $R$ ein freier $R$-Modul vom Rang eins. Nach $(iii)$ ergibt sich damit speziell $(R/I) \otimes_R (R/J) \cong R/(I+J)$ für Ideale $I, J$ von $R$.

Ein paar Beispiele: $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$, $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^3 \cong \mathbb{Z}^6$. Weiter $\mathbb{Z}/6\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ nach der eben gemachten Bemerkung. Ähnlich $\mathbb{Z}/3\mathbb{Z} \otimes 7\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$. Es gilt auch $1 \otimes 3 = 3 \otimes 1 = 0 \otimes 1 = 0$. Mit diesen Beispielen und Satz 4.4, $(ii)$ kann man Tensorprodukte von endlich erzeugten Moduln über Hauptidealringen nach Satz 3.27 leicht berechnen.

**4.7 Satz.** *Sei $M$ ein $R$-Modul und $I \subseteq R$ ein Ideal. Dann gilt*

$$(R/I) \otimes_R M \cong M/IM$$

*unter der Abbildung $(r+I) \otimes m \mapsto rm + IM$.*

*Beweis.* Wir tensorieren die exakte Sequenz $0 \to I \to R \to R/I \to 0$ über $R$ mit $M$ und erhalten nach Lemma 4.4, $(iii)$ und Lemma 4.6, $(i)$ die exakte Sequenz $I \otimes_R M \to M \to (R/I) \otimes_R M \to 0$. Das Bild von $I \otimes M$ in $M$ ist hierbei $IM$. Die Aussage über die Abbildung ergibt sich durch Nachverfolgen der einzelnen Abbildungen in den exakten Sequenzen. □

## 4.2 Induzierte und koinduzierte Moduln

Ist $M$ ein $R$-Modul und $f : R \to S$ ein Ringhomomorphismus (also $S$ eine $R$-Algebra), dann ist $S$ auch ein $R$-Modul und wir können $S \otimes_R M$ als $R$-Modul definieren. Durch $s(x \otimes m) = (sx) \otimes m$ können wir $S \otimes_R M$ zu einem $S$-Modul machen. Dies erlaubt es, den Ring eines Moduls zu wechseln. Eine formalere Begründung dieser Konstruktion lautet wie folgt. Durch $(s_1, s_2, m) \mapsto (s_1 s_2) \otimes m$ wird eine 3-lineare Abbildung $S \times S \times M \to S \otimes_R M$ definiert. Dies liefert eine lineare Abbildung $S \otimes_R (S \otimes_R M) \to S \otimes_R M$ und damit eine bilineare Abbildung $S \times (S \otimes_R M) \to S \otimes_R M$, $(s_1, s_2 \otimes m) \mapsto (s_1 s_2) \otimes m$.

Eine alternative Konstruktion, welche aus $M$ einen $S$-Modul macht, geht wie folgt: Wir betrachten die abelsche Gruppe $\mathrm{Hom}_R(S, M)$ und machen diese für $f \in \mathrm{Hom}_R(S, M)$ durch $(s \cdot f)(x) := f(sx)$ in einen $S$-Modul.

Wir bezeichnen $S \otimes_R M$ als den entlang $f$ induzierten Modul von $M$ und $\mathrm{Hom}_R(S, M)$ als den entlang $f$ koinduzierten Modul von $M$. Die Zuordnungen $M \mapsto S \otimes_R M$ und $M \mapsto \mathrm{Hom}_R(S, M)$ liefern Funktoren der Kategorie der $R$-Moduln in die Kategorie der $S$-Moduln.

Wir können beide Prozesse in gewissem Sinne auch wieder rückgängig machen. Ist $N$ ein $S$-Modul, so können wir $N$ auch als $R$-Modul mittels $r \cdot x := f(r)x$ für $x \in N$ auffassen. Diesen Modul bezeichnen wir mit $N|_R$. Die Zuordnung $N \mapsto N|_R$ liefert einen Funktor der Kategorie der $S$-Moduln in die Kategorie der $R$-Moduln.

**4.8 Satz.** *Sei $f : R \to S$ ein Ringhomomorphismus, $M$ ein $R$-Modul und $N$ ein $S$-Modul. Dann gibt es in $M$ und $N$ funktorielle Isomorphieen abelscher Gruppen*

$$\mathrm{Hom}_S(S \otimes_R M, N) \cong \mathrm{Hom}_R(M, N|_R)$$

$$\mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) \cong \mathrm{Hom}_R(N|_R, M).$$

*Beweis.* (Skizze) Die Menge $\mathrm{Hom}_S(S \otimes_R M, N)$ kann als Menge von $R$-bilinearen Abbildungen $\phi : S \times M \to N$ angesehen werden, für die zusätzlich $\phi(s \times m) = s\phi(1 \times m)$ gilt. So ein $\phi$ wird allerdings durch die $R$-lineare Abbildung $\psi(m) = \phi(1 \times m)$ definiert, welche ein Element in $\mathrm{Hom}_R(M, N|_R)$ ist. Diese Zuordung ist auch umkehrbar. Daraus ergibt sich die erste Isomorphie.

Die zweite Isomorphie ist wie folgt gegeben. Sei $f \in \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M))$. Dann ist das isomorphe Bild $g \in \mathrm{Hom}_R(N|_R, M)$ von $f$ durch $g(x) = f(x, 1)$ gegeben. Ist $g \in \mathrm{Hom}_R(N|_R, M)$, so erhalten wir das isomorphe Urbild $f \in \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M))$ von $g$ durch $f(x, s) = g(sx)$. Man prüft leicht nach, daß hierdurch ein Isomorphismus gegeben wird. □

( Der Satz besagt, daß $M \mapsto S \otimes_R M$ linksadjungierter Funktor zum rechtsadjungierten Funktor $N \mapsto N|_R$ ist, und daß $M \mapsto \mathrm{Hom}_R(S, M)$ rechtsadjungierter Funktor zum linksadjungierten Funktor $N \mapsto N|_R$ ist. Speziell ist $M \mapsto S \otimes_R M$ damit rechtsexakt, $M \mapsto \mathrm{Hom}_R(S, M)$ linksexakt und $N \to N|_R$ exakt.)

Sei $S$ eine $R$-Algebra, $M$ ein $S$-Modul und $N$ ein $R$-Modul. Dann wird $M|_R \otimes_R N$ vermöge $s(m \otimes n) := (sm \otimes n)$ zu einem $S$-Modul, den wir mit $M \otimes_R N$ bezeichnen. Dies ist im allgemeinen ein von $S \otimes_R (M|_R \otimes_R N)$ verschiedener $S$-Modul.

**4.9 Satz.** *Sei $S$ eine $R$-Algebra, $M$ ein $S$-Modul und $N$ ein $R$-Modul. Dann gilt*

$$M \otimes_S (S \otimes_R N) \cong M \otimes_R N$$

*als $S$-Moduln unter $m \otimes (s \otimes n) \mapsto (sm) \otimes n$. Die Isomorphie ist zudem funktoriell in $M$ und $N$.*

*Beweis.* Ähnlich wie bei der Assoziativität des Tensorprodukts. Die Abbildung $(m, s, n) \mapsto (sm) \otimes n$ ist $R$-bilinear in $s$ und $n$ und $S$-bilinear in $m$ und $s$. Daher gibt es den $S$-Homomorphismus $m \otimes (s \otimes n) \mapsto (sm) \otimes n$. Umgekehrt ist $(m, n) \mapsto$

$m \otimes (1 \otimes n)$ in $m$ und $n$ $R$-bilinear und in $m$ $S$-linear. Daher gibt es den $S$-Homomorphismus $m \otimes n \mapsto m \otimes (1 \otimes n)$. Die beiden $S$-Homomorphismen sind invers zueinander, was die Isomorphie beweist.

Die Funktorialität in $M$ und $N$ ergibt sich aus der konkreten Form der Isomorphie zusammen mit den funktoriellen Eigenschaften des Tensorprodukt. □

Die Funktoren „Tensorieren“ und „Induzieren“ vertauschen also in dem im Satz angegebenen Sinn.

Hier ist noch ein Vergleich induzierter und koinduzierter Moduln für $R$-Algebren $S$, welche als $R$-Modul frei von endlichem Rang sind.

**4.10 Satz.** *Ist die $R$-Algebra $S$ als $R$-Modul frei von endlichem Rang und $M$ ein $R$-Modul, so gibt es eine Isomorphie von $S$-Moduln*

$$S \otimes_R M \cong \mathrm{Hom}_R(S, M).$$

*Beweis.* Übung. □

## 4.3 Lokalisierungen

Sei $M$ ein $R$-Modul und $U$ eine multiplikativ abgeschlossene Teilmenge mit $1 \in U$ von $R$. Wir definieren die Lokalisierung $M[U^{-1}]$ genau wie $R[U^{-1}]$ als die Menge der formalen Brüche $m/u$ für $m \in M$ und $u \in U$, wobei $m_1/u_1 = m_2/u_2$ genau dann gelten soll, wenn es ein $v \in U$ mit $vm_1u_2 = vm_2u_1$ gibt. Unter Verwendung der üblichen Bruchrechentechnik wird $M[U^{-1}]$ ein $R[U^{-1}]$-Modul. Die Elemente $u/1$ mit $u \in U$ sind Einheiten in $R[U^{-1}]$, da $(u/1)(1/u) = 1$ gilt. Wir erhalten auch eine $R$-lineare Abbildung $h : M \to M[U^{-1}]$, $m \mapsto m/1$. Der Kern von $h$ besteht genau aus allen denjenigen $m \in M$, für die es ein $u \in U$ mit $um = 0$ gibt.

**4.11 Satz.** *Sei $M$ ein $R$-Modul und $U \subseteq R$ multiplikativ abgeschlossen. Dann gilt*

$$R[U^{-1}] \otimes_R M \cong M[U^{-1}]$$

*unter der Abbildung $(r/u) \otimes m \mapsto (rm)/u$.*

*Beweis.* Sei $h : R[U^{-1}] \times M \to M[U^{-1}]$ die Multiplikationsabbildung $r/u \times m \mapsto (rm)/u$ und $f : R[U^{-1}] \otimes_R M \to M[U^{-1}]$ der zugehörige $R$-lineare Homomorphismus (ist auch $R[U^{-1}]$-linear). Es ist offensichtlich, daß $h$ und $f$ surjektiv sind. Zum Beweis der Injektivität von $f$ sei $f(\sum_i (r_i/u_i) \otimes m_i) = 0$ mit $r_i \in R$, $u_i \in U$ und $m_i \in M$ beliebig. Es gibt $u \in U$ und $m \in M$ mit $\sum_i (r_i/u_i) \otimes m_i = (1/u) \otimes m$ ($(r_i/u_i) \otimes m_i = (1/u_i)(1 \otimes r_i m_i)$ schreiben, ausklammern und auf „Hauptnenner“ bringen). Da $u$ in $R[U^{-1}]$ eine Einheit ist, folgt aus $f((1/u) \otimes m) = 0$

durch Multiplikation mit $u$ bereits $uf((1/u)(1 \otimes m)) = f(u(1/u)(1 \otimes m)) = f(1 \otimes m) = m/1 = 0$ in $M[U^{-1}]$. Es gibt also $v \in U$ mit $vm = 0$ und daher $v(1 \otimes m) = 1 \otimes (vm) = 1 \otimes 0 = 0$. Da $v$ in $R[U^{-1}]$ eine Einheit ist, gilt $1 \otimes m = 0$ und auch $(1/u) \otimes m = 0$ in $R[U^{-1}] \otimes_R M$. □

Lokalisieren entspricht also dem Tensorieren mit $R[U^{-1}]$ über $R$ und ist damit ein Funktor. Zu einem Homomorphismus $f : M \to N$ gibt es also einen Homomorphismus $g : M[U^{-1}] \to N[U^{-1}]$.

**4.12 Satz.** *Sei $0 \to I \to M \to N$ eine exakte Sequenz. Dann ist auch die zugehörige, lokalisierte Sequenz $0 \to I[U^{-1}] \to M[U^{-1}] \to N[U^{-1}]$ exakt.*

*Beweis.* Seien $f_1 : I \to M$ und $f_2 : M \to N$ die Homomorphismen aus der exakten Sequenz und seien $g_1 : I[U^{-1}] \to M[U^{-1}]$ und $g_2 : M[U^{-1}] \to N[U^{-1}]$ die zugehörigen lokalisierten Homomorphismen.

Wir zeigen zuerst, daß $g_1$ injektiv und die Sequenz somit bei $I[U^{-1}]$ exakt ist. Ist $m/u \in \ker(g_1)$, so gilt $g_1(m/u) = f_1(m)/u = 0$ und daher gibt es ein $v \in U$ mit $vf_1(m) = 0$. Es folgt $f_1(vm) = 0$ und wegen der Injektivität von $f_1$ auch $vm = 0$. Somit gilt $m/u = 0$ und die Sequenz ist bei $I[U^{-1}]$ exakt.

Für jeden Monomorphismus $\phi : I \to M$ ist die Sequenz $0 \to I \to M \to M/\phi(M)$ mit der Nullabbildung, $\phi$ und dem kanonischen Epimorphismus exakt. Nach dem vorhergehenden Absatz überführt Lokalisieren also Monomorphismen in Monomorphismen.

Die Exaktheit bei $M[U^{-1}]$ folgt jetzt allgemein aus der Rechtsexaktheit des Lokalisierens bzw. des Tensorprodukts. Wir können $f_2$ in der Form $i \circ f_2'$ mit $f_2' : M \to f_2(M)$ und $i : f_2(M) \to N$ schreiben. Seien $g_2' : M[U^{-1}] \to f_2(M)[U^{-1}]$ und $j : f_2(M)[U^{-1}] \to N[U^{-1}]$ die lokalisierten Homomorphismen. Dann gilt wegen der Funktoreigenschaft des Lokalisierens bzw. des Tensorprodukts $g_2 = j \circ g_2'$. Mit $i$ ist auch $j$ nach dem bereits Bewiesenen ein Monomorphismus. Also folgt $\ker(g_2') = \ker(g_2)$.

Die exakte Sequenz $I \to M \to f_2(M) \to 0$ mit $f_1$, $f_2'$ und der Nullabbildung geht wegen der Rechtsexaktheit des Tensorprodukts in die exakte Sequenz $I[U^{-1}] \to M[U^{-1}] \to f_2(M)[U^{-1}] \to 0$ mit $g_1$, $g_2'$ und der Nullabbildung über. Also gilt $\ker(g_2) = \ker(g_2') = \mathrm{im}(g_1)$ und wir erhalten die Exaktheit unserer Ausgangssequenz bei $M$. □

Satz 4.12 und Satz 4.4, (*iii*) bedeuten, daß Lokalisieren ein exakter Funktor ist. Ein exakter Funktor erhält Kerne und Kokerne.

Hier ist eine Anwendung des Lokalisierens: Nach der obigen Aussage über den Kern der Lokalisierungsabbildung $h$ kann ein torsionsfreier Modul $M$ über einem Integritätsring $R$ in den Vektorraum $\mathrm{Quot}(R) \otimes_R M$ eingebettet werden.

Bei der Untersuchung von solchen Moduln $M$ können wir also bei Bedarf auf einen umgebenden Vektorraum zurückgreifen.

Sei $M$ ein $R$-Modul und $\mathfrak{p}$ ein Primideal von $R$. Sei $U = R\backslash\mathfrak{p}$. Wir definieren dann die Lokalisierung von $M$ bei $\mathfrak{p}$ als $M_\mathfrak{p} = M[U^{-1}]$. Dies ist ein $R_\mathfrak{p}$-Modul. Ist $N$ ein weiterer $R$-Modul und $\phi : M \to N$ ein Homomorphismus, so erhalten wir durch Lokalisieren den Homomorphismus $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$.

Für $f \in R$ sei $U = \{f^i \mid i \in \mathbb{Z}^{\geq 0}\}$. Wir definieren die Lokalisierung von $M$ an $f$ als $M_f = M[U^{-1}]$. Dies ist ein $R_f$-Modul, wobei $R_f = R[U^{-1}]$. Ist $N$ ein weiterer $R$-Modul und $\phi : M \to N$ ein Homomorphismus, so erhalten wir durch Lokalisieren den Homomorphismus $\phi_f : M_f \to N_f$.

**4.13 Satz.** *Sei $M$ ein $R$-Modul.*

(*i*) *Für $m \in M$ ist $m = 0$ genau dann, wenn $m/1 = 0$ in $M_\mathfrak{m}$ für jedes maximale Ideal $\mathfrak{m}$ von $R$ gilt.*

(*ii*) *Es ist $M = 0$ genau dann, wenn $M_\mathfrak{m} = 0$ für jedes maximale Ideal $\mathfrak{m}$ von $R$ gilt.*

*Sei $\phi : M \to N$ ein Homomorphismus der $R$-Moduln $M$ und $N$ und sei $E$ eine der Eigenschaften „Isomorphismus“, „Monomorphismus“, „Epimorphismus“. Seien $f_i, g_i \in R$ mit $1 = \sum_i f_i g_i$. Dann sind äquivalent:*

(*iii*) *Der Homomorphismus $\phi$ besitzt die Eigenschaft $E$.*

(*iv*) *Die Homomorphismen $\phi_{f_i}$ besitzen die Eigenschaft $E$.*

(*v*) *Die Homomorphismen $\phi_\mathfrak{m}$ besitzen die Eigenschaft $E$ für alle maximalen Ideale $\mathfrak{m}$ von $R$.*

*Beweis.* (*i*): Das Element $m/1$ ist genau dann Null in $M_\mathfrak{m}$, wenn es ein $u \in R\backslash\mathfrak{m}$ mit $um = 0$ gibt, und dies ist äquivalent zur Bedingung $\mathrm{Ann}_R(m) \not\subseteq \mathfrak{m}$. Nun gilt $m = 0$ genau dann, wenn $\mathrm{Ann}_R(m) = R$ ist, und dieses gilt genau dann, wenn $\mathrm{Ann}_R(m) \not\subseteq \mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$ gilt.

(*ii*): Folgt aus (*i*).

(*iii*) $\Rightarrow$ (*iv*): Klar, da Lokalisieren an $f_i$ ein exakter Funktor ist.

(*iv*) $\Rightarrow$ (*v*): Für jedes $\mathfrak{m}$ gibt es ein $f_i$ mit $f_i \in R\backslash\mathfrak{m}$, da das von den $f_i$ erzeugte Ideal ganz $R$ ist. Sei $\mathfrak{m}'$ das von $\mathfrak{m}$ in $R_{f_i}$ erzeugte, maximale Ideal. Dann gilt $\phi_\mathfrak{m} = (\phi_{f_i})_{\mathfrak{m}'}$ und die Aussage folgt, da Lokalisieren bei $\mathfrak{m}'$ ein exakter Funktor ist.

(*v*) $\Rightarrow$ (*iii*): Sei $E =$ „Monomorphismus“. Der Homomorphimus $\phi$ ist genau dann ein Monomorphismus, wenn $\ker(\phi) = 0$ gilt. Da Lokalisieren Kerne in Kerne

überführt, gilt $0 = \ker(\phi_{\mathfrak{m}}) = \ker(\phi)_{\mathfrak{m}}$ für alle maximalen Ideale $\mathfrak{m}$, also $\ker(\phi) = 0$ nach $(ii)$.

Sei $E =$ „Epimorphismus“. Der Homomorphimus $\phi$ ist genau dann ein Epimorphismus, wenn $\operatorname{coker}(\phi) = 0$ gilt. Da Lokalisieren Kokerne in Kokerne überführt, gilt $0 = \operatorname{coker}(\phi_{\mathfrak{m}}) = \operatorname{coker}(\phi)_{\mathfrak{m}}$ für alle maximalen Ideale $\mathfrak{m}$, also $\operatorname{coker}(\phi) = 0$ nach $(ii)$.

Die Aussage für $E =$ „Isomorphismus“ folgt aus der für „Monomorphismus“ und „Epimorphismus“. □

## 4.4 Flache Moduln

Ist $I \subseteq R$ ein Ideal, so motivieren Satz 4.7 und Satz 4.11 auch die Formel $I \otimes_R M \cong IM$, wobei der Isomorphismus durch die Multiplikationsabbildung $i \otimes m \mapsto im$ gegeben sein sollte. Dies ist jedoch im allgemeinen falsch, die Abbildung ist zwar immer surjektiv (wegen der Rechtsexaktheit des Tensorprodukts, oder auch direkt einsichtig), aber nicht unbedingt injektiv. Für $I = Ra$ gilt zum Beispiel $I \otimes_R (R/I) \cong R \otimes_R (R/I) \cong R/I$, aber $I(R/I) = \{0\}$. Insbesondere ist das Bild von $I \otimes_R (R/I)$ in $R \otimes_R (R/I)$ gleich Null, denn in $R \otimes_R (R/I)$ gilt $ra \otimes x = r \otimes ax = r \otimes 0 = 0$. Man mache sich klar, daß man in $I \otimes_R (R/I)$ so nicht rechnen kann und vergleiche mit dem Kriterium in Lemma 4.6, $(iv)$. Die injektive Abbildung $I \to R$ wurde also durch Tensorierung mit $R/I$ in eine nicht injektive Abbildung überführt (nach Satz 4.4, $(iii)$ kann dies mit surjektiven Abbildungen nicht passieren). Dieses Verhalten wird zum Anlaß der folgenden Definition genommen.

**4.14 Definition.** Sei $M$ ein $R$-Modul. Dann heißt $M$ flach, wenn injektive Abbildungen zwischen beliebigen $R$-Moduln durch Tensorieren mit $M$ wieder in injektive Abbildungen überführt werden.

Anders ausgedrückt: $M$ heißt flach, wenn Tensorieren mit $M$ ein exakter Funktor ist.

Die Äquivalenz der beiden Definitionsvarianten in Definition 4.14 folgt aus der Rechtsexaktheit des Tensorprodukts.

**4.15 Satz.** *Ein $R$-Modul $M$ ist genau dann flach, wenn die Multiplikationsabbildung $i \otimes m \mapsto im$ einen Isomorphismus $I \otimes_R M \cong IM$ für alle Ideale $I$ von $R$ ergibt.*

*Beweis.* Wird ausgelassen. □

Ein Ausdruck $\sum_i \lambda_i m_i$ in $IM$ mit $\lambda_i \in I$ und $m_i \in M$ soll also genau dann Null sein, wenn dies aufgrund $R$-bilinearer Relationen der Fall ist. Der Modul $IM$

soll in diesem Sinn also keine Relationen außer den Relationen der Bilinearität zwischen $I$ und $M$ enthalten. Wir verwenden diesen Satz aber nicht weiter.

Ist $U$ ein Untermodul und direkter Summand des $R$-Moduls $M$, so erhalten wir durch Tensorieren der Inklusion $U \to M$ mit einem $R$-Modul $N$ stets eine Inklusion $U \otimes_R N \to M \otimes_R N$. Denn nach Lemma 4.4, $(ii)$ erhalten wir für $V$ mit $M \cong U \oplus V$ einen Isomorphismus $(U \otimes_R N) \oplus (V \otimes_R N) \to M \otimes_R N$, dessen Einschränkung auf $U \otimes_R N$ gerade unsere Abbildung $U \otimes_R N \to M \otimes_R N$ ergibt.

Grob gesagt verlieren beliebige Monomorphismen $U \to M$ durch Tensorieren mit $N$ ihre Injektivität genau dann, wenn Elemente $x \in U$ durch Einbetten nach $M$ zu Vielfachen $x = ry$ mit $y \in M$ und $r \in R$ werden, wobei $y$ nicht im Bild von $U$ in $M$ und $r$ im Annulator von Elementen $n$ aus $N$ liegt. Genauer sind $x, y$ durch $x_i, y_i$ und $r$ durch eine Matrix $(r_{i,j})_{i,j}$ und $n$ durch $n_j$ zu ersetzen. Vergleiche mit dem Kriterium aus Lemma 4.6, $(iv)$.

**4.16 Definition.** Ist $S$ eine $R$-Algebra und ist $S$ als $R$-Modul flach, so nennen wir $S$ eine flache $R$-Algebra. Ist $f : R \to S$ ein Ringhomomorphismus, so nennen wir $f$ flach, wenn die zugehörige $R$-Algebra $S$ flach ist.

**4.17 Satz.** *Es gelten die folgenden Aussagen:*

- $(i)$ *Für die $R$-Moduln $M_i$ ist $M = \coprod_i M_i$ genau dann flach, wenn jedes $M_i$ flach ist.*
- $(ii)$ *Sind $M$ und $N$ flache $R$-Moduln, dann ist auch $M \otimes_R N$ ein flacher $R$-Modul.*
- $(iii)$ *Ist $S$ eine $R$-Algebra und $N$ ein flacher $R$-Modul, so ist $S \otimes_R N$ ein flacher $S$-Modul.*
- $(iv)$ *Ist $S$ eine flache $R$-Algebra und $N$ ein flacher $S$-Modul, so ist $N|_R$ ein flacher $R$-Modul.*

*Beweis.* $(i)$: Sei $h : N \to P$ ein Homomorphismus. Durch Tensorieren erhalten wir $f : N \otimes_R M \to P \otimes_R M$ und $f_i : N \otimes_R M_i \to P \otimes_R M_i$. Nach Lemma 4.4, $(ii)$ gilt $N \otimes_R M \cong \coprod_i (N \otimes_R M_i)$ und $P \otimes_R M \cong \coprod_i (P \otimes_R M_i)$. Fassen wir damit die $N \otimes_R M_i$ und $P \otimes_R M_i$ als Untermoduln von $N \otimes_R M$ und $P \otimes_R M$ auf, so stimmen $f$ eingeschränkt auf $N \otimes_R M_i$ und $f_i$ überein. Dann ist $f$ genau dann injektiv, wenn alle $f_i$ injektiv sind, und dies beweist die Aussage.

$(ii)$: Tensorieren mit $M \otimes_R N$ entspricht Tensorieren mit $M$ und anschließend Tensorieren mit $N$. Da $\cdot \otimes_R M$ und $\cdot \otimes_R N$ exakt sind, ist auch $\cdot \otimes_R (M \otimes_R N)$ exakt.

(*iii*): Tensorieren über $S$ mit $S \otimes_R N$ ist nach Satz 4.9 das gleiche wie Tensorieren über $R$ mit $N$. Da $N$ flach ist, ist Tensorieren über $R$ mit $N$ exakt. Also ist Tensorieren über $S$ mit $S \otimes_R N$ ebenfalls exakt.

(*iv*): Sei $M$ ein $R$-Modul. Nach Satz 4.9 gilt dann (mit $M$ und $N$ vertauscht) die in $M$ funktorielle Isomorphie $M \otimes_R N \cong (M \otimes_R S) \otimes_S N$ als $S$-Moduln und somit auch als $R$-Moduln. Nach Voraussetzung sind $\cdot \otimes_R S$ und $\cdot \otimes_S N$ exakt, also ist auch $\cdot \otimes_R N$ exakt. □

Als Beispiel zu (*i*) sind alle freien $R$-Moduln flach, da $R$ als $R$-Modul flach ist. Ein endlich erzeugter Modul über einem Hauptidealring ist damit nach Satz 3.28, (*ii*) genau dann flach, wenn er torsionsfrei ist. Nach Satz 4.12 ist eine Lokalisierung $R[U^{-1}]$ als $R$-Modul stets flach.

Ein $R$-Modul $M$ heißt endlich präsentiert, wenn es einen Epimorphismus $R^n \to M$ mit $n < \infty$ und endlich erzeugtem Kern gibt.

Sei $f : R \to S$ ein Ringhomomorphismus, so daß $S$ eine $R$-Algebra wird, und seien $M$, $N$ zwei $R$-Moduln. Tensorieren mit $S$ über $R$ liefert einen $R$-Homomorphismus $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$ mit $f \mapsto \mathrm{id} \otimes f$. Da der Wertebereich ein $S$-Modul ist, faktorisiert dieser Homomorphismus nach Satz 4.8 eindeutig durch den $S$-Homomorphismus $\phi : S \otimes_R \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$ mit $s \otimes f \mapsto s(\mathrm{id} \otimes f)$.

**4.18 Satz.** *Sei $S$ als $R$-Modul flach und $M$ endlich präsentiert. Dann liefert $\phi$ einen Isomorphismus*

$$S \otimes_R \mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N).$$

*Beweis.* Soll noch eingegeben werden. □

Eine spezielle Anwendung des Satzes ergibt sich für $S = R[U^{-1}]$, so daß wir mit $\phi$ einen Isomorphismus $\mathrm{Hom}_R(M, N)[U^{-1}] \cong \mathrm{Hom}_{R[U^{-1}]}(M[U^{-1}], N[U^{-1}])$ erhalten. Beispielsweise gibt es damit für jeden Homomorphismus $f : M[U^{-1}] \to N[U^{-1}]$ ein $u \in U$ und $g : M \to N$ mit $uf(m) = g(m)$ in $N[U^{-1}]$ für alle $m \in M$. Es kann also aus der Existenz von Homomorphismen lokalisierter Moduln in gewisser Weise auf die Existenz von Homomorphismen der Ausgangsmoduln geschlossen werden.

## 4.5 Freie Moduln

In diesem Abschnitt diskutieren wir ein paar weitere Aspekte und Eigenschaften freier Moduln.

Satz 3.9, $(ii)$ hatte zum Inhalt, daß die Kardinalitäten beliebiger Basen eines $R$-Moduls für einen kommutativen Ring $R$ übereinstimmen. Für nicht kommutative Ringe ist dies im allgemeinen nicht richtig. Sei zum Beispiel $V$ ein unendlich dimensionaler $K$-Vektorraum. Dann gibt es einen Isomorphismus $f : V \oplus V \to V$. Wir bezeichnen mit $\iota_1, \iota_2 : V \to V \oplus V$ die Einbettung in den ersten bzw. zweiten Summand. Wir erhalten Vektorraumisomomorphismen $\mathrm{End}_K(V) \cong \mathrm{Hom}_K(V \oplus V, V)$ durch $g \mapsto g \circ f$ und $\mathrm{Hom}_K(V \oplus V, V) \cong \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ durch $h \mapsto (h \circ \iota_1, h \circ \iota_2)$. Mit $R = \mathrm{End}_K(V)$ liefert dies zusammen einen Vektorraumisomorphismus $\psi : R \to R \times R$. Werden $R$ und $R \times R$ in der natürlichen Weise als $R$-Moduln aufgefaßt, so ist $\psi$ sogar $R$-linear: Für $r, g \in R$ gilt $r\psi(g) = (r \circ g \circ f \circ \iota_1, r \circ g \circ f \circ \iota_2) = \psi(rg)$. Somit besitzt $R$ als $R$-Modul eine einelementige und eine zweielementige Basis („Eilenberg Schwindel“).

Freie Moduln besitzen die folgende Eigenschaft, wie in Satz 3.9, $(i)$ gezeigt wurde: Sei $B$ eine Basis des $R$-Moduls $M$ und $N$ irgendein weiterer $R$-Modul. Für jede Abbildung von Mengen $f : B \to N$ gibt es genau ein Element in $\mathrm{Hom}_R(M, N)$, welches $f$ fortsetzt. Ähnlich verhält es sich übrigens auch bei Polynomringen (die „frei“ erzeugten Ringen entsprechen) und dem Einsetzhomomorphismus. Hier sind zwei weitere Eigenschaften, die darauf aufbauen.

**4.19 Satz.** *Sei $N$ ein $R$-Modul.*

- $(i)$ *Es gibt einen freien $R$-Modul $M$ und einen Epimorphimus $f : M \to N$, so daß $N \cong M/\ker(f)$.*
- $(ii)$ *Ist $M$ ein freier $R$-Modul und $f : N \to M$ ein Epimorphismus, so gibt es ein $g : M \to N$ mit $f \circ g = \mathrm{id}_M$.*

*Beweis.* $(i)$ : Sei $B$ ein Erzeugendensystem von $N$ und $M = \coprod_{b \in B} R$. Wir definieren $f$ durch $f((\lambda_b)_{b \in B}) = \sum_{b \in B} \lambda_b b$. Dies Isomorphie folgt aus dem ersten Isomorphiesatz.

$(ii)$: Für jedes Basiselement $b \in B$ wählen wir ein Urbild $c \in f^{-1}(b)$ und definieren $g_0(b) = c$. Dies liefert $g_0 : B \to N$ und dann $g : M \to N$. □

Hier sind die zu Satz 4.17 analogen Aussagen für „frei“ statt „flach“.

**4.20 Satz.** *Es gelten die folgenden Aussagen:*

- $(i)$ *Für die $R$-Moduln $M_i$ ist $M = \coprod_i M_i$ frei, wenn jedes $M_i$ frei ist.*
- $(ii)$ *Sind $M$ und $N$ freie $R$-Moduln, dann ist auch $M \otimes_R N$ ein freier $R$-Modul.*
- $(iii)$ *Ist $S$ eine $R$-Algebra und $N$ ein freier $R$-Modul, so ist $S \otimes_R N$ ein freier $S$-Modul.*

(*iv*) *Ist $S$ eine freie $R$-Algebra und $N$ ein freier $S$-Modul, so ist $N|_R$ ein freier $R$-Modul.*

*Beweis.* (*i*): Die Vereinigung der Basen der $M_i$ liefert eine Basis von $M$.
(*ii*) und (*iii*): Folgen aus Satz 4.4, (*iii*) und Lemma 4.6, (*ii*).
(*iv*): Analog wie im Gradsatz: Sind die $n_j$ eine $S$-Basis von $N$ und die $s_i$ eine $R$-Basis von $S$, so sind die $s_i n_j$ eine $R$-Basis von $N$. □

Die Umkehrung der Aussage (*i*) ist im allgemeinen falsch. Es gibt Ringe $R$ und Ideale $I, J$ von $R$, so daß $R \oplus R \cong I \oplus J$ gilt, aber $I$ und $J$ nicht frei sind. Speziell dürfen $I, J$ hier keine Hauptideale sein. Konkrete Beispiele kommen später.

## 4.6 Projektive Moduln

Die Definition von „frei“ benötigt explizit Elemente von $M$. Auf der anderen Seite wird in Satz 4.19, (*ii*) eine nützliche, „elementfreie“ Eigenschaft angegeben. Diese macht somit auch in allgemeinerem kategoriellen Rahmen Sinn und man macht sie zur Grundlage einer weiteren Definition. Wie sich herausstellt, ist diese Eigenschaft echt schwächer als „frei“.

**4.21 Definition.** Sei $M$ ein $R$-Modul. Dann heißt $M$ projektiv, wenn es für jeden $R$-Modul $N$ und Epimorphismus $f : N \to M$ einen Homomorphismus $g : M \to N$ mit $f \circ g = \mathrm{id}_M$ gibt.

Der Homomorphismus $g$ ist wegen $f \circ g = \mathrm{id}_M$ injektiv.

**4.22 Satz.** *Sei $M$ ein $R$-Modul. Dann sind äquivalent.*

(*i*) *$M$ ist projektiv.*

(*ii*) *Es gibt einen $R$-Modul $U$ und einen freien $R$-Modul $N$ mit $M \oplus U \cong N$.*

(*iii*) *Es gibt ein Erzeugendensystem $B$ von $M$ und „Koordinatenfunktionale“ $\lambda_b \in \mathrm{Hom}_R(M, R)$ mit $x = \sum_{b \in B} \lambda_b(x) b$.*

(*iv*) *Seien $N_1, N_2$ beliebige $R$-Moduln und $f \in \mathrm{Hom}_R(N_1, N_2)$ ein Epimorphismus. Für jedes $g \in \mathrm{Hom}_R(M, N_2)$ gibt es ein $h \in \mathrm{Hom}_R(M, N_1)$ mit $g = f \circ h$.*

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Nach Satz 4.19, (*ii*) gibt es einen freien $R$-Modul $N$ und einen Epimorphismus $f : N \to M$. Wegen (*i*) gibt es einen Monomorphismus $g : M \to N$ mit $f \circ g = \mathrm{id}_M$. Für den Untermodul $U = \{x - g(f(x)) \,|\, x \in N\} \subseteq$

$\ker(f)$ gilt dann $g(M) + U = N$ und $g(M) \cap U \subseteq g(M) \cap \ker(f) = \{0\}$, also $N = g(M) \oplus U \cong M \oplus U$.

$(ii) \Rightarrow (iii)$: Nach $(ii)$ gibt es einen freien $R$-Modul $N$, einen Epimorphismus $f : N \to M$ mit $\ker(f) = U$ und einen Monomorphismus $g : M \to N$ mit $f \circ g = \mathrm{id}_M$. Seien die $a_i$ eine Basis von $N$. Dann sind die $b_i = f(a_i)$ ein Erzeugendensystem von $M$, weil $f$ surjektiv ist. Da die $a_i$ eine Basis bilden, gibt es Koordinatenfunktionale $\mu_i \in \mathrm{Hom}_R(N, R)$ mit $y = \sum_i \mu_i(y)a_i$ für alle $y \in N$. Wir definieren $\lambda_i \in \mathrm{Hom}_R(M, R)$ durch $\lambda_i(x) = \mu_i(g(x))$. Wegen $g(b_i) - a_i \in \ker(f)$ gilt dann $g(x - \sum_i \lambda_i(x)b_i) \in g(x) - \sum_i \mu_i(g(x))a_i + \ker(f) = \ker(f)$. Wegen $g(M) \cap \ker(f) = \{0\}$ folgt $g(x - \sum_i \lambda_i(x)b_i) = 0$. Da $g$ injektiv ist, ergibt sich $x - \sum_i \lambda_i(x)b_i = 0$ und damit $(iii)$.

$(iii) \Rightarrow (iv)$: Sei $B$ ein Erzeugendensystem mit Koordinatenfunktionalen $\lambda_b$ für $b \in B$ wie in $(iii)$. Wir wählen für jedes $b \in B$ ein $y_b \in f^{-1}(g(b))$. Dies ist möglich, da $f$ surjektiv ist. Wir definieren dann $h \in \mathrm{Hom}_R(M, N_1)$ durch $h(x) = \sum_b \lambda_b(x)y_b$. Nach Definition sind die $\lambda_b$ $R$-linear und für fast alle $b \in B$ gilt $\lambda_b(x) = 0$. Daher ist $h$ wohldefiniert und ein Element von $\mathrm{Hom}_R(M, N_1)$. Weiter gilt $f(h(x)) = \sum_b \lambda_b(x)f(y_b) = \sum_b \lambda_b(x)g(b) = g(\sum_b \lambda_b(x)b) = g(x)$, also wie gewünscht $f \circ h = g$.

$(iv) \Rightarrow (i)$: Sei $f : N \to M$ der Epimorphismus aus $(i)$ bzw. der Definition 4.21. Wir wenden $(iv)$ mit $N_1 = N$, $N_2 = M$ und $g = \mathrm{id}_M$ an und erhalten direkt Aussage $(i)$. □

Satz 4.22, $(iii)$ ist eine Verallgemeinerung der Aussage für freie Moduln $M$, daß man einen Homomorphismus $f : M \to N$ durch seine Werte auf einer Basis von $M$ definieren kann.

Ist $M$ ein $R$-Modul, so ist der Funktor $\mathrm{Hom}_R(M, \cdot)$ linksexakt. Satz 4.22, $(iv)$ läßt sich damit folgendermaßen umformulieren:

**4.23 Korollar.** *Ein $R$-Modul $M$ ist genau dann projektiv, wenn der Funktor $\mathrm{Hom}_R(M, \cdot)$ exakt ist.*

*Beweis.* Da $\mathrm{Hom}_R(M, \cdot)$ linksexakt ist, muß für Exaktheit nur noch nachgewiesen werden, daß surjektive Abildungen in surjektive Abbildungen überführt werden. Das ist aber genau die Aussage von $(iv)$. □

Hier sind die zu Satz 4.17 analogen Aussagen für „projektiv“ statt „flach“.

**4.24 Satz.** *Es gelten die folgenden Aussagen:*

(i) *Für die $R$-Moduln $M_i$ ist $M = \coprod_i M_i$ genau dann projektiv, wenn jedes $M_i$ projektiv ist.*

(*ii*) *Sind $M$ und $N$ projektive $R$-Moduln, dann ist auch $M \otimes_R N$ ein projektiver $R$-Modul.*

(*iii*) *Ist $S$ eine $R$-Algebra und $N$ ein projektiver $R$-Modul, so ist $S \otimes_R N$ ein projektiver $S$-Modul.*

(*iv*) *Ist $S$ eine projektive $R$-Algebra und $N$ ein projektiver $S$-Modul, so ist $N|_R$ ein projektiver $R$-Modul.*

*Beweis.* (*i*): Folgt direkt aus Satz 4.22, (*ii*) und Satz 4.20, (*i*).

(*ii*) und (*iii*): Folgen aus Satz 4.22, (*ii*), Satz 4.4, (*iii*) und Satz 4.20, (*ii*) und (*iii*).

(*iv*): Ähnlich wie im Gradsatz: Seien die $n_j$ ein Erzeugendensystem von $N$ mit den Koordinatenfunktionalen $\lambda_j \in \mathrm{Hom}_S(N, S)$ und die $s_i$ ein Erzeugendensystem von $S$ mit den Koordinatenfunktionalen $\mu_i \in \mathrm{Hom}_R(S, R)$. Dann sind die $s_i m_j$ ein Erzeugendensystem mit den Koodinatenfunktionalen $\mu_i \circ \lambda_j \in \mathrm{Hom}_R(N, R)$. Nach Satz 4.22, (*iii*) ist $N$ als $R$-Modul also projektiv. □

## 4.7 Satz von Cayley-Hamilton und Lemma von Nakayama

Im folgenden bezeichnet $R$ wieder einen kommutativen Ring mit 1.

**4.25 Satz** (Cayley-Hamilton)**.** *Sei $M$ ein von $n$ Elementen erzeugter $R$-Modul und $I$ ein Ideal von $R$. Sei $\phi \in \mathrm{End}_R(M)$ ein Endomorphismus von $M$. Gilt $\phi(M) \subseteq IM$, so gibt es ein $f = \sum_{i=0}^{n} \lambda_{n-i} x^i \in R[x]$ mit $\lambda_0 = 1$, $\lambda_i \in I^i$ für $0 \leq i \leq n$ und $f(\phi) = 0$ in $\mathrm{End}_R(M)$.*

*Beweis.* Seien $m_1, \ldots, m_n$ Erzeuger von $M$. Nach Voraussetzung existiert ein $A = (a_{i,j})_{i,j} \in I^{n \times n}$ mit $\phi(m_i) = \sum_{j=1}^{n} a_{i,j} m_j$ für alle $1 \leq i \leq n$. Vermöge $g(x)m := g(\phi)(m)$ wird $M$ zu einem $R[x]$-Modul. Dann gilt $x(m_1, \ldots, m_n)^t = A(m_1, \ldots, m_n)^t$ und $(xI_n - A)(m_1, \ldots, m_n)^t = 0$. Durch Multiplikation dieser Gleichung von links mit der Pseudoinversen von $xI_n - A$ (siehe Satz 3.10, (*ii*)) erhalten wir $\det(xI_n - A)(m_1, \ldots, m_n)^t = 0$. Setze $f = \sum_{i=0}^{n} \lambda_{n-i} x^i = \det(xI_n - A) \in R[x]$. Die $m_i$ sind ein Erzeugendensystem von $M$, es folgt also $fM = 0$ und damit $f(\phi) = 0$ in $\mathrm{End}_R(M)$. Durch direktes Ausrechnen der Koeffizienten $\lambda_i$ von $f$ mittels der Leibnizregel ergibt sich, daß $f$ in der Tat normiert vom Grad $n$ ist und daß $\lambda_i \in I^i$ gilt. □

**4.26 Definition.** Das Jacobsonradikal $J$ von $R$ ist der Schnitt aller maximalen Ideale von $R$. Das Radikal $\mathrm{Rad}(R)$ von $R$ ist der Schnitt aller Primideale von $R$.

Das Radikal von $R$ wird manchmal auch Nilradikal genannt. Das Jacobsonradikal $J$ und das Radikal $\mathrm{Rad}(R)$ von $R$ sind Ideale von $R$. Es gilt $J = \{r \in R \,|\, 1 + rs \in R^\times \text{ für alle } s \in R\}$ und $\mathrm{Rad}(R) = \{r \in R \,|\, r^n = 0 \text{ für ein } n \in \mathbb{Z}^{\geq 1}\}$.

**4.27 Lemma** (Nakayama)**.** *Sei $M$ ein endlich erzeugter Modul und $I$ ein Ideal, welches im Jacobsonradikal von $R$ enthalten ist. Gilt $M = N + IM$ für einen Untermodul $N$ von $M$, dann folgt $M = N$.*

*Beweis.* Wir beweisen die Aussage zunächst für $N = 0$, es gelte also $IM = M$. Wir wenden Satz 4.25 auf $\phi = \mathrm{id}_M$ an und erhalten $f(x) = x^n - g(x) \in R[x]$ mit $g \in I[x]$ und $f(1)M = 0$. Für $r = g(1)$ gilt also $r \in I$ und $f(1)M = (1-r)M = 0$. Da $r$ nach Voraussetzung in jedem maximalen Ideal von $R$ enthalten ist, gilt $1 - r \in R^\times$. Es folgt $M = (1 - r)M = 0$.

Sei nun $M = N + IM$. Faktorisieren nach $N$ liefert $M/N = I(M/N)$, also $M/N = 0$ und daher $M = N$. □

Eine mögliche Anwendung von Lemma 4.27 ist die folgende: Sind die Klassen von $n_1, \ldots, n_m \in M$ ein Erzeugendensystem von $M/IM$, so sind die $n_1, \ldots, n_m$ ein Erzeugendensystem von $M$. Allerdings darf man bei dieser Schlußweise nicht vergessen, daß $M$ als endlich erzeugt vorauszusetzen ist.

## 4.8 Beziehungen zwischen den Moduleigenschaften und lokal-global Aussagen

Sei $M$ ein $R$-Modul. Für $a \in R$ sei $I_a = \{b \in R \,|\, ab = 0\}$. Dann ist $I_a$ ein Ideal von $R$ und $I_aM$ ist ein Untermodul von $M$, der durch $a$ annulliert wird. Wir nennen $M$ im wesentlichen torsionsfrei, wenn für jedes $a \in R\backslash\{0\}$ und jedes $x \in M$ aus $ax = 0$ bereits $x \in I_aM$ folgt. Für einen Integritätsring $R$ ist $M$ genau dann im wesentlichen torsionsfrei, wenn $M$ torsionsfrei ist.

**4.28 Satz.** *Sei $M$ ein $R$-Modul. Dann gilt*

$$M \text{ frei } \Rightarrow M \text{ projektiv } \Rightarrow M \text{ flach } \Rightarrow M \text{ im wesentlichen torsionsfrei.}$$

*Beweis.* Die erste Implikation folgt direkt aus Satz 4.22, $(ii)$ mit $U = \{0\}$.

Die zweite Implikation folgt aus Satz 4.22, $(ii)$ und Satz 4.17, $(i)$. Damit ist $M$ als direkter Summand eines freien und damit flachen Moduls selbst flach.

Für die dritte Implikation sei $a \in R$. Dann ist $I_a$ der Kern von $R \to Ra$, $x \mapsto ax$, und es gilt $Ra \cong R/I_a$ und $Ra \otimes_R M \cong R/I_a \otimes_R M \cong M/I_aM$. Tensorieren der exakten Inklusionssequenz $0 \to Ra \to R$ mit $M$ liefert damit die exakte Sequenz $0 \to M/I_aM \to M$ nach Lemma 4.6, $(i)$, wobei der rechte

Monomorphismus durch $x + I_a M \mapsto ax$ gegeben ist. Also folgt aus $ax = 0$ bereits $x \in I_a M$, so daß $M$ im wesentlichen torsionsfrei ist. □

Wir wollen die Eigenschaften „frei“, „projektiv“ und „flach“ global und lokal vergleichen.

**4.29 Definition.** Ein $R$-Modul $M$ heißt lokal frei, wenn $M_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul für alle Primideale $\mathfrak{p}$ von $R$ ist. Analog definieren wir lokal projektiv und lokal flach.

**4.30 Lemma.** *Sei $M$ ein $R$-Modul.*

(*i*) *Ein Modul $M$ ist genau dann lokal frei (projektiv, flach), wenn $M_\mathfrak{m}$ frei (projektiv, flach) für alle maximalen Ideale von $R$ ist.*

(*ii*) *Ein freier (projektiver, flacher) Modul $M$ ist lokal frei (projektiv, flach).*

*Beweis.* Wir machen eine Vorbemerkung: Die Aussage (*iii*) der Sätze 4.20, 4.24 und 4.17 impliziert, daß die Eigenschaften frei, projektiv und flach unter Lokalisieren erhalten bleiben.

(*i*): Für jedes Primideal gibt es ein maximales Ideal $\mathfrak{m}$, so daß $M_\mathfrak{p}$ nur eine weitere Lokalisierung von $M_\mathfrak{m}$ ist. Aus der Vorbemerkung folgt damit die Aussage.

(*ii*): Ergibt sich unmittelbar aus der Vorbemerkung. □

**4.31 Satz.** *Sei $R$ ein lokaler Ring und $M$ ein endlich erzeugter $R$-Modul. Dann gilt*

$$M \text{ ist frei} \Leftrightarrow M \text{ ist projektiv} \Leftrightarrow M \text{ ist flach.}$$

*Beweis.* Wegen Satz 4.28 ist nur zu zeigen, daß aus $M$ flach bereits $M$ frei folgt.

Sei $\mathfrak{m}$ das maximale Ideal von $R$ und seien $x_1, \ldots, x_n \in M$, so daß die Klassen $\bar{x_i} = x_i + \mathfrak{m}M$ eine Basis des mit $M$ endlich erzeugten $R/\mathfrak{m}$-Vektorraums $M/\mathfrak{m}M$ bilden. Wir zeigen, daß die $x_i$ eine Basis von $M$ sind.

Sei $N = \sum_i Rx_i$. Dann gilt $M = N + \mathfrak{m}M$, und nach dem Lemma 4.27 folgt $M = N$, also sind die $x_i$ ein Erzeugendensystem von $M$.

Zum Beweis der Basiseigenschaft zeigen wir jetzt, daß für in $M/\mathfrak{m}M$ linear unabhängige, nicht notwendig erzeugende $\bar{x}_i$ die $x_i$ linear unabhängig in $M$ sind.

Wir schicken wir eine Bemerkung voraus. Seien $\lambda_i \in R$ mit $\sum_{i=1}^n \lambda_i x_i = 0$. Sei $I = \sum_{i=1}^n R\lambda_i$. Dann ist das Bild von $\sum_{i=1}^n \lambda_i \otimes x_i$ unter dem Homomorphismus $I \otimes_R M \to R \otimes_R M = M$ gleich $\sum_{i=1}^n \lambda_i x_i = 0$. Da die Inklusion $I \to R$ injektiv und $M$ flach ist, ist dieser Homomorphismus ebenfalls injektiv und es muß bereits $\sum_{i=1}^n \lambda_i \otimes x_i = 0$ gelten. Nach Lemma 4.6, (*iv*) angewendet für $N = I$ gibt es $a_{i,j} \in R$ und $y_j \in R$ mit $x_i = \sum_{j=1}^m a_{i,j} y_j$ und $\sum_{i=1}^n a_{i,j}\lambda_i = 0$ für alle $j$.

Um aus dieser Vorbemerkung auf die lineare Unabhängigkeit der $x_i$ zu schließen, verwenden wir Induktion über ihre Anzahl $n$. Für $n = 1$ gelte $\lambda_1 x_1 = 0$. Nach der Vorbemerkung gilt dann $x_1 = \sum_{j=1}^{m} a_{1,j} y_j$ und $a_{1,j}\lambda_1 = 0$ für alle $j$. Wegen $x_1 \notin \mathfrak{m}M$ gibt es ein $j$ mit $a_{1,j} \notin \mathfrak{m}$. Dann gilt $a_{1,j} \in R^\times$ und aus $a_{1,j}\lambda_1 = 0$ folgt $\lambda_1 = 0$.

Sei nun $n > 1$. Nach der Vorbemerkung gilt $x_i = \sum_{j=1}^{m} a_{i,j} y_j$ und $\sum_{i=1}^{n} a_{i,j}\lambda_i = 0$ für alle $j$ und mit $y_i \in M$, $a_{i,j} \in R$. Da $x_n \notin \mathfrak{m}M$ ist, gibt es $j$ mit $a_{n,j} \notin \mathfrak{m}$. Also ist $a_{n,j} \in R^\times$ und es gilt $\lambda_n = \sum_{i=1}^{n-1}(-a_{i,j}/a_{n,j})\lambda_i = \sum_{i=1}^{n-1} b_i\lambda_i$ mit $b_i = -a_{i,j}/a_{n,j}$. Dann folgt $0 = \sum_{i=1}^{n} \lambda_i x_i = \sum_{i=1}^{n-1} \lambda_i(x_i + b_i x_n)$. Die $\bar{x}_1 + b_1\bar{x}_n, \ldots, \bar{x}_{n-1} + b_{n-1}\bar{x}_n$ sind linear unabhängig in $M/\mathfrak{m}M$. Nach Induktionsvoraussetzung sind $x_1, \ldots, x_{n-1}$ also linear unabhängig in $M$. Daraus folgt $\lambda_i = 0$ für $1 \leq i \leq n-1$ und $\lambda_n = \sum_{i=1}^{n-1} b_i\lambda_i = 0$. Damit sind die $x_1, \ldots, x_n$ linear unabhängig. □

Die Voraussetzung an die endliche Erzeugung ist notwendig: Für $R = \mathbb{Z}_{(p)}$ ist $R$ zwar lokal und $M = \mathbb{Q}$ als $R$-Modul flach, aber $M$ ist nicht frei.

Der folgende Satz enthält den lokal-global Vergleich für die Eigenschaft „flach“.

**4.32 Satz.** *Sei $M$ ein $R$-Modul.*

(*i*) *$M$ ist genau dann flach, wenn $M$ lokal flach ist.*

(*ii*) *Ist $M$ endlich erzeugt, so ist $M$ genau dann flach, wenn $M$ lokal frei ist.*

*Beweis.* (*i*): Die Implikation $\Rightarrow$ folgt aus Lemma 4.30. Für die Implikation $\Leftarrow$ sei $M$ lokal flach. Sei $\phi : N \to P$ ein Monomorphismus und $\mathfrak{p}$ ein Primideal. Sei $\phi_1 : N \otimes_R M \to P \otimes_R M$. Nach Voraussetzung ist $M_\mathfrak{p}$ flach über $R_\mathfrak{p}$. Da $R_\mathfrak{p}$ flach über $R$ ist, ist $M_\mathfrak{p}$ nach Satz 4.17, (*ii*) auch flach über $R$. Daher ist $\phi_2 : N \otimes_R M_\mathfrak{p} \to P \otimes_R M_\mathfrak{p}$ ein Monomorphismus. Mit Satz 4.4, (*i*) und (*ii*) erhalten wir daraus den Monomorphismus $\phi_3 : (N \otimes_R M) \otimes_R R_\mathfrak{p} \to (P \otimes_R M) \otimes_R R_\mathfrak{p}$, welcher durch Tensorieren von $\phi_1$ mit $R_\mathfrak{p}$ entsteht. Da $\mathfrak{p}$ beliebig war, ist $\phi_1$ nach Satz 4.13 ein Monomorphismus. Also ist $M$ flach.

(*ii*): Ergibt sich aus (*i*) und Satz 4.31. □

Wir wollen noch einen lokal-global Vergleich der Eigenschaft „projektiv“ angeben und eine Verbindung zwischen „projektiv“ und „lokal frei“ herstellen. Dazu müssen wir voraussetzen, daß $M$ nicht nur endlich erzeugt, sondern sogar endlich präsentiert ist.

Zur Erinnerung: Ein $R$-Modul $M$ heißt endlich präsentiert, wenn es ein $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $\phi : R^n \to M$ mit endlich erzeugtem Kern gibt.

**4.33 Lemma.** *Sei $M$ ein endlich präsentierter $R$-Modul. Für jedes $m \in \mathbb{Z}^{\geq 1}$ und jeden Epimorphismus $\psi : R^m \to M$ ist dann* $\ker(\psi)$ *endlich erzeugt.*

*Ist $R$ noethersch und $M$ endlich erzeugt, so ist $M$ endlich präsentiert.*

*Ist $M$ endlich präsentiert und $U$ eine multiplikativ abgeschlossene Teilmenge von $R$ mit $1 \in U$, so ist auch $M[U^{-1}]$ als $R[U^{-1}]$-Modul endlich präsentiert.*

*Beweis.* Sei $\phi : R^n \to M$ ein Epimorphismus mit $\ker(\phi)$ endlich erzeugt und sei $\psi : R^m \to M$ ein weiterer Epimorphismus. Seien $(\lambda_{i,j})_j \in R^m$ mit $\phi(e_i) = \psi((\lambda_{i,j})_j)$ und $(\mu_{j,i})_i \in R^n$ mit $\phi((\mu_{j,i})_i) = \psi(e_j)$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$. Seien $(u_{s,i})_i \in R^n$ für endlich viele $s$ ein Erzeugendensystem von $\ker(\phi)$. Dann bilden die $((u_{s,i})_i, 0) \in R^n \times R^m$ zusammen mit den $((\mu_{j,i})_i, e_j) \in R^n \times R^m$ ein endliches Erzeugendensystem $U$ von $K = \{(x, y) \in R^n \times R^m \,|\, \phi(x) = \psi(y)\}$. Für jeden Erzeuger $u \in U$ gibt es ein $v_u \in \ker(\psi)$, so daß sich $u$ als $R$-Linearkombination der $(e_i, (\lambda_{i,j})_j) \in K$ und von $(0, v_u) \in K$ schreiben läßt. Die $(e_i, (\lambda_{i,j})_j)$ zusammen mit den $(0, v_u)$ für jedes $u$ liefern damit ein anderes, endliches Erzeugendensystem $V$ von $K$. Für $y \in \ker(\psi)$ können keine $(e_i, (\lambda_{i,j})_j)$ in den Darstellungen von $(0, y) \in K$ in $V$ auftreten. Also bilden die $v_u$ ein endliches Erzeugendensystem von $\ker(\psi)$.

Sei $R$ noethersch und $M$ endlich erzeugt. Da $M$ endlich erzeugt ist, gibt es einen Epimorphismus $\psi : R^n \to M$. Da $R$ noethersch ist, muß $\ker(\psi)$ nach Satz 3.14, (*iii*) und Satz 3.13 endlich erzeugt sein. Also ist $M$ endlich präsentiert.

Ist $M$ endlich präsentiert, so haben wir eine exakte Sequenz $R^s \to R^n \to M \to 0$. Durch Lokalisieren geht diese in die exakte Sequenz $R[U^{-1}]^s \to R[U^{-1}]^n \to M[U^{-1}] \to 0$ über, also ist $M[U^{-1}]$ endlich präsentiert. □

**4.34 Lemma.** *Sei $M$ ein endlich präsentierter $R$-Modul. Dann ist $M$ ist genau dann lokal frei, wenn es für jedes Primideal $\mathfrak{p}$ von $R$ ein $f \in R\backslash\mathfrak{p}$ gibt, so daß $M[f^{-1}]$ bereits ein freier $R[f^{-1}]$-Modul ist.*

*Beweis.* Das Lemma ist für $M = \{0\}$ richtig, da $M$ frei ist und dies auch für alle Lokalisierungen gilt. Es gelte also $M \neq \{0\}$.

„$\Leftarrow$“: Ist klar, da nur weiter lokalisiert werden muß.

„$\Rightarrow$“: Mit $M$ ist $M_\mathfrak{p}$ endlich erzeugt, so daß $M_\mathfrak{p}$ eine endliche Basis besitzt. Sei $m_1, \ldots, m_k$ eine Basis von $M_\mathfrak{p}$ mit $m_i \in M$. Jeder Erzeuger $v_j$ von $M$ kann aufgrund der Annahme in der Form $u_j v_j = \sum_{i=1}^k \lambda_{i,j} m_i$ mit $u_j \in R\backslash\mathfrak{p}$ und $\lambda_{i,j} \in R$ geschrieben werden. Sei $f = \prod_j u_j$. Dann gilt $f \in R\backslash\mathfrak{p}$ und $v_j = \sum_{i=1}^k (\lambda'_{i,j}/f) m_i$ in $M[f^{-1}]$ mit geeigneten $\lambda'_{i,j} \in R$. Die $m_i$ bilden also ein Erzeugendensystem von $M[f^{-1}]$.

Aus $\sum_i (\mu_i/u_i) m_i = 0$ in $M_\mathfrak{p}$ für beliebige $\mu_i \in R$ und $u_i \in R\backslash\mathfrak{p}$ folgt $\mu_i/u_i = 0$ für alle $i$ nach Voraussetzung, also gibt es für jedes $i$ ein $v_i \in R\backslash\mathfrak{p}$ mit $v_i \mu_i = 0$ in $R$. Der $R_\mathfrak{p}$-Modul aller solcher Tupel $(\mu_i/u_i)_i \in R_\mathfrak{p}^k$ ist nach Lemma 4.33 endlich erzeugt, da $M_\mathfrak{p}$ mit $M$ endlich präsentiert ist. Wir multiplizieren an $f$ die endlich vielen, auftretenden $v_i$ (für jeden Erzeuger des Tupelraums sind das $k$ Elemente

$v_i$). Jedes Tupel wird dann also durch koordinatenweise Multiplikation mit $f$ annulliert, ist also Null in $R[f^{-1}]^k$. Die $m_i$ sind daher auch linear unabhängig in $M[f^{-1}]$. □

Der Satz ist falsch, wenn auf die Voraussetzung der endlichen Erzeugung verzichtet wird. Sei zum Beispiel $R = \mathbb{Z}$ und $M$ der von $\{a/p \,|\, a \in \mathbb{Z}, p \text{ Primzahl}\}$ erzeugte $\mathbb{Z}$-Untermodul von $\mathbb{Q}$. Dann sind die $M_\mathfrak{p}$ für $\mathfrak{p} = \mathbb{Z}p$ isomorph zu den von $1/p$ erzeugten $R$-Untermoduln von $\mathbb{Q}$, also frei. Wegen der unbeschränkten Nenner kann es aber kein einziges $f$ wie im Lemma geben.

Torsion bleibt lokal nicht unbedingt erhalten. Siehe $R = K \times K$ und $M = R$. Dann ist $M$ nicht torsionsfrei, aber alle Lokalisierungen an Primidealen sind isomorph zu $K$, also torsionsfrei.

Der folgende Satz enthält den angestrebten lokal-global Vergleich für „projektiv“.

**4.35 Satz.** *Sei $M$ ein endlich präsentierter $R$-Modul. Dann sind äquivalent:*

(*i*) *$M$ ist projektiv.*

(*ii*) *$M$ ist flach.*

(*iii*) *$M$ ist lokal frei.*

(*iv*) *Es gibt $f_1, \ldots, f_n \in R$ mit $R = \sum_{i=1}^n Rf_i$, so daß $M[f_i^{-1}]$ frei über $R[f_i^{-1}]$ für alle $1 \leq i \leq n$ ist.*

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Folgt aus Satz 4.28. (*ii*) $\Rightarrow$ (*iii*): Folgt aus Satz 4.32.

(*iii*) $\Rightarrow$ (*iv*): Nach Lemma 4.34 gibt es für jedes maximale Ideal $\mathfrak{m}$ ein $f_\mathfrak{m} \in R\backslash\mathfrak{m}$, so daß $M[f_\mathfrak{m}^{-1}]$ ein freier $R[f_\mathfrak{m}^{-1}]$-Modul ist. Sei $N$ der von den $f_\mathfrak{m}$ erzeugte $R$-Untermodul von $R$ und $i : N \to R$ der Inklusionsmonomorphismus. Da jedes $f_\mathfrak{m}$ in $R_\mathfrak{m}$ eine Einheit ist, ist der lokalisierte Monomorphismus $i' : N_\mathfrak{m} \to R_\mathfrak{m}$ ein Isomorphismus. Nach Satz 4.13 ist damit $i$ ein Isomorphismus, es gilt also $N = R$. Wegen $1 \in N$ gibt es endlich viele $f_i$ unter den $f_\mathfrak{m}$ und $g_i \in R$ mit $1 = \sum_i g_i f_i$. Es ergibt sich (*iv*).

(*iv*) $\Rightarrow$ (*i*): Mit $M$ ist jedes $M[f_i^{-1}]$ endlich erzeugt, besitzt also eine endliche Basis. Für jedes $i$ seien $m_{i,j} \in M$ für endlich viele $j$, so daß die Bilder der $m_{i,j}$ in $M[f_i^{-1}]$ eine Basis von $M[f_i^{-1}]$ bilden. Seien $\mu_{i,j} \in \mathrm{Hom}_{R[f_i^{-1}]}(M[f_i^{-1}], R[f_i^{-1}])$ die Koordinatenfunktionale bezüglich der $m_{i,j}$, so daß $m/f_i^r = \sum_j \mu_{i,j}(m/f_i^r) m_{i,j}$ in $M[f_i^{-1}]$ für alle $m \in M$, $r \in \mathbb{Z}^{\geq 0}$ und $i$ gilt.

Nach Satz 4.18 gibt es $\lambda_{i,j} \in \mathrm{Hom}_R(M, R)$ und $k_{i,j} \in \mathbb{Z}^{\geq 1}$ mit $f_i^{k_{i,j}} \mu_{i,j}(m/f_i^r) = \lambda_{i,j}(m)/f_i^r$ in $R[f_i^{-1}]$ für alle $m \in M$ und $r \in \mathbb{Z}^{\geq 0}$. Sei $k = \max_{i,j} k_{i,j}$. Wir ersetzen $\lambda_{i,j}$ durch $f_i^{k-k_{i,j}} \lambda_{i,j}$, so daß nun speziell $f_i^k \mu_{i,j}(m) = \lambda_{i,j}(m)$ in $R[f_i^{-1}]$

und $f_i^k m = \sum_j \lambda_{i,j}(m) m_{i,j}$ in $M[f_i^{-1}]$ für alle $m \in M$ gilt. Da $M$ endlich erzeugt ist, gilt $f_i^k m = \sum_j \lambda_{i,j}(m) m_{i,j}$ auch in $M$, wenn wir zuvor $k$ groß genug wählen.

Potenzieren wir beide Seiten der Gleichung $1 = \sum_i g_i f_i$ mit einer ausreichend großen ganzen Zahl, erhalten wir einen Ausdruck $1 = \sum_i h_i f_i^k$ mit $h_i \in R$.

Es ergibt sich $m = (\sum_i h_i f_i^k) m = \sum_{i,j} (h_i \lambda_{i,j}(m)) m_{i,j}$ in $M$ für alle $m \in M$. Wir erhalten also Erzeuger $m_{i,j}$ und Koordinatenfunktionale $m \mapsto h_i \lambda_{i,j}(m)$, so daß $M$ nach Satz 4.22 projektiv ist. □

# Kapitel 5

# Ringe II

In diesem Kapitel werden das Tensorprodukt von Algebren, ganze Ringerweiterungen, gebrochene und invertierbare Ideale, Dedekindringe und die Faktorisierung in Dimension 1 und Kodimension 1 behandelt.

## 5.1 Tensorprodukt von Algebren

Wir kommen nun auf das Tensorprodukt von (kommutativen) $R$-Algebren $S_1$, $S_2$ zu sprechen. Die Multiplikation in $S_1 \otimes_R S_2$ wird durch $(x_1 \otimes_R y_1) \cdot (x_2 \otimes_R y_2) = (x_1x_2) \otimes (y_1y_2)$ definiert. Formal bekommen wir durch $(x_1, y_1, x_2, y_2) \mapsto S_1 \otimes_R S_2$, $(x_1, y_1, x_2, y_2) \mapsto (x_1x_2) \otimes_R (y_1y_2)$ eine 4-lineare Abbildung. Diese faktorisiert durch $S_1 \otimes_R S_2 \otimes_R S_1 \otimes_R S_2$ und zieht sich zu einer bilinearen Abbildung auf $(S_1 \otimes_R S_2) \times (S_1 \otimes_R S_2)$ zurück, welche die Multiplikation definiert.

Sei $T$ eine $R$-Algebra und $g_i : S_i \to T$ zwei $R$-lineare Ringhomomorphismen. Dann definieren wir eine bilineare Abbildung $g : S_1 \times S_2 \to T$ durch $g(x, y) = xy$, und diese faktorisiert eindeutig durch eine $R$-lineare Abbildung $f : S_1 \otimes_R S_2 \to T$, welche aufgrund der Definitionen ebenfalls ein Ringhomomorphismus ist. Daher erfüllt $S_1 \otimes_R S_2$ die universelle Eigenschaft einer direkten Summe in der Kategorie der $R$-Algebren (deren Morphismen $R$-lineare Ringhomomorphismen sind).

Der vollständigkeit halber noch der folgende Satz.

**5.1 Satz.** *Für ein Diagramm $\mathcal{D}$ von $R$-Algebren existieren $\varprojlim \mathcal{D}$ und $\varinjlim \mathcal{D}$ als $R$-Algebren.*

*Beweis.* Die Aussage für $\varprojlim \mathcal{D}$ wird ganz analog zu der für Moduln wie in Satz 6.5 gezeigt. Für $\varinjlim \mathcal{D}$ verwendet man eine ring- statt modultheoretische Konstruktion wie in Satz 4.2. Insbesondere betrachtet man eingeschränkte Tensorprodukte, deren Elemente $\cdots \otimes 1 \otimes a_i \otimes \cdots \otimes a_j \otimes 1 \otimes \cdots$ an fast allen Stellen eine 1 haben. Die Prinzipien sind ähnlich wie in Satz 6.5 und wir lassen die Details aus. □

Sind $S_1$ und $S_2$ $R$-Algebren und $X$ ein Menge von Variablen, so gilt $S_1[X] \otimes_R \mathcal{S}_2 \cong (S_1 \otimes_R S_2)[X]$. Ist $S_1 = R[X]/J$ für eine Menge von Variablen $X$ und ein Ideal $J$, so gilt $S_1 \otimes_R S_2 = S_2[X]/J$. Speziell ergibt sich $R[X] \otimes_R R[Y] \cong R[X \cup Y]$ und $(R[X]/I) \otimes_R (R[Y]/J) \cong R[X \cup Y]/\langle I, J\rangle$ für $Y$ eine weitere Menge von Variablen mit $X \cap Y = \{\}$. Diese Aussagen sind analog zu denen für Moduln.

Die Charakterisierung linear disjunkter Körpererweiterungen $E_1/K$ und $E_2/K$ in einem Erweiterungskörper $C$ zeigt, daß $E_1 \otimes_K E_2 \cong E_1E_2$ unter Verwendung der Multiplikationsabbildung genau dann gilt, wenn $E_1$ und $E_2$ linear disjunkt über $K$ sind.

## 5.2 Gebrochene und invertierbare Ideale, Primidealfaktorisierung

Sei $R$ ein Integritätsring. Der Homomorphismus $R \to \mathrm{Quot}(R)$, $r \mapsto r/1$ ist injektiv. Daher fassen wir $R$ im folgenden als Teilring von $\mathrm{Quot}(R)$ auf.

**5.2 Definition.** Ein $R$-Untermodul $I$ von $\mathrm{Quot}(R)$ heißt gebrochenes Ideal von $R$, wenn es ein $a \in R\backslash\{0\}$ mit $aI = \{ax \mid x \in I\} \subseteq R$ gibt.

Die Ideale von $R$ sind dann auch gebrochene Ideale von $R$. Zur Unterscheidung nennen wir die Ideale von $R$ auch ganze Ideale von $R$.

**5.3 Lemma.** *Seien $I, J \neq 0$ gebrochene Ideale von $R$. Die Isomorphismen $\phi : I \to J$ sind genau von der Form $\phi(x) = ax$ für ein eindeutig bestimmtes $a \in \mathrm{Quot}(R)\backslash\{0\}$ mit $aI = J$.*

*Beweis.* Sei $I$ ein gebrochenes Ideal, $a \in \mathrm{Quot}(R)\backslash\{0\}$ und $J = aI$. Dann ist $J$ ein gebrochenes Ideal, denn mit $bI \subseteq R$ und $a = r/u$ für $b, r, u \in R\backslash\{0\}$ gilt $bu \in R\backslash\{0\}$ und $(bu)J = r(aI) \subseteq rR \subseteq R$. Durch $x \mapsto ax$ wird dann ein Isomorphismus $\phi : I \to J$ definiert.

Sei umgekehrt $\phi : I \to J$ ein Isomorphimus und $U = R\backslash\{0\}$. Wir zeigen zuerst, daß sich $\phi$ zu einem $\mathrm{Quot}(R)$-Isomorphismus $\psi : \mathrm{Quot}(R) \to \mathrm{Quot}(R)$ fortsetzen läßt. Es gilt $I[U^{-1}] \cong \mathrm{Quot}(R) \otimes_R I \cong \mathrm{Quot}(R)I = \mathrm{Quot}(R)$, da $\mathrm{Quot}(R)$ über $R$ flach und $I \neq 0$ ist. Zusammen erhalten wir den Isomorphismus $f : I[U^{-1}] \to \mathrm{Quot}(R)$ mit $f(x/u) = x/u$. Außerdem kommutieren die Einbettungen $I \to I[U^{-1}]$ und $I \to \mathrm{Quot}(R)$ mit $f$, wie man unmittelbar sieht. Für $J$ bekommen wir analog $g : J[U^{-1}] \to \mathrm{Quot}(R)$ mit $g(x/u) = x/u$. Ist $\phi' : I[U^{-1}] \to J[U^{-1}]$ der lokalisierte Isomorphismus, so erhalten wir schließlich $\psi = g^{-1} \circ \phi' \circ f$ mit den gewünschten Eigenschaften.

Da $\psi : \mathrm{Quot}(R) \to \mathrm{Quot}(R)$ ein $\mathrm{Quot}(R)$-linearer Isomorphismus und 1 eine Basis von $\mathrm{Quot}(R)$ ist, folgt $\psi(x/u) = (x/u)\psi(1) = ax/u$ mit $a := \psi(1) \in$

$\mathrm{Quot}(R)\backslash\{0\}$ für alle $x \in R$ und $u \in U$. Speziell folgt $\phi(x) = \psi(x) = ax$ für alle $x \in I$. Aus $ax = bx$ für alle $x \in I$ folgt $a = b$, da $I \neq 0$ und $R$ nullteilerfrei ist. □

Ein gebrochenes Ideal ist also per Definition immer isomorph zu einem ganzen Ideal von $R$.

**5.4 Definition.** Sind $I, J$ gebrochene Ideale von $R$, so definieren wir $IJ = \{xy \,|\, x \in I, y \in J\}$. Ist $I \neq 0$, so definieren wir $(I : J) = \{x \in \mathrm{Quot}(R) \,|\, xI \subseteq J\}$ und $I^{-1} = (I : R)$.

Ein gebrochenes Ideal $I$ von $R$ heißt invertierbar, wenn es ein gebrochenes Ideal $J$ von $R$ mit $IJ = R$ gibt. Dann heißt $J$ das inverse Ideal von $I$.

Hier sind $IJ$ und $(I : J)$ wieder gebrochene Ideale. Denn aus $aI \subseteq R$ und $bJ \subseteq R$ folgt $(ab)IJ \subseteq R$, und für jedes $x \in I\backslash\{0\}$ gilt $bx(I : J) \subseteq bJ \subseteq R$.

Nach Lemma 5.3 gilt $(I : J) \cong \mathrm{Hom}_R(I, J)$. als abelsche Gruppen und $(I : I) \cong \mathrm{Hom}_R(I, I)$ als Ringe.

Weiter gilt $(IJ)K = I(JK)$, $IJ = JI$ und $IR = RI = I$ für gebrochene Ideale $I, J, K$. Damit bilden die gebrochenen Ideale eine abelsche Halbgruppe mit Einselement $R$.

Für invertierbare Ideale gilt notwendigerweise $I \neq 0$. Aufgrund der Definition von $I^{-1}$ gilt $II^{-1} \subseteq R$. Ist $I$ invertierbar mit inversem Ideal $J$, so gilt desweiteren $J \subseteq I^{-1}$. Daraus ergibt sich $R = IJ \subseteq II^{-1} \subseteq R$, also $II^{-1} = R$. Da Inverse in Halbgruppen mit 1 eindeutig bestimmt sind, folgt $I^{-1} = J$.

Ist $I$ invertierbar, so gilt $(I : J) = I^{-1}J$. Die Inklusion $\supseteq$ ist klar und gilt auch für nicht-invertierbares $I$. Auf der andere Seite gilt $(I : J)I \subseteq J$, also folgt durch Multiplikation mit $I^{-1}$ wie gewünscht $(I : J) \subseteq I^{-1}J$.

Die einfachsten invertierbaren Ideale sind die Hauptideale $\neq 0$.

Multiplikation mit invertierbaren Idealen erhält Inklusionen: Ist $I$ invertierbar und sind $J$ und $K$ gebrochene Ideale, so gilt $J \subseteq K \Leftrightarrow JI \subseteq KI$ und $J = K \Leftrightarrow JI = KI$.

Sind $I, J$ gebrochene Ideale, so sind auch $I + J$ und $I \cap J$ gebrochene Ideale.

**5.5 Definition.** Seien $I, K$ gebrochene Ideale von $R$ und $J$ ein ganzes Ideal von $R$. Gilt $IJ = K$, so sagen wir, daß $K$ durch $I$ teilbar und daß $I$ ein Teiler von $K$ ist. Wir schreiben $I \,|\, K$.

Sind $I, J, K$ wie in der Definition, dann gilt $I \supseteq IJ = K$, also $I \supseteq K$. Hiervon gilt auch die Umkehrung, wenn $I$ invertierbar ist:

**5.6 Lemma.** *Seien $I$ und $K$ gebrochene Ideale und sei $I$ invertierbar. Dann gilt $I \,|\, K$ genau dann, wenn $I \supseteq K$ ist.*

*Seien $I, J, K$ gebrochene Ideal mit $IJ = K$ und sei $K$ invertierbar. Dann sind auch $I$ und $J$ invertierbar.*

*Seien $\mathfrak{p}$ und $\mathfrak{q}$ invertierbare Primideale mit $\mathfrak{q} \supseteq \mathfrak{p}$. Dann gilt $\mathfrak{q} = \mathfrak{p}$.*

*Beweis.* Aus $I \mid K$ folgt $I \supseteq K$, wie vor dem Lemma bemerkt. Sind umgekehrt $I$ und $K$ gebrochene Ideale mit $I \supseteq K$ und ist $I$ invertierbar, so folgt $R = II^{-1} \supseteq KI^{-1}$. Mit $J = KI^{-1}$ gilt also $IJ = IKI^{-1} = II^{-1}K = K$, und $K$ wird von $I$ geteilt.

Aus $IJ = K$ folgt $I(JK^{-1}) = J(IK^{-1}) = R$, also sind $I$ und $J$ invertierbar (allgemein sind in einer Halbgruppe mit 1 Teiler von Einheiten wieder Einheiten).

Wir nehmen $\mathfrak{p} \neq 0$ an. Dann gibt es ein ganzes Ideal $I$ mit $\mathfrak{q}I = \mathfrak{p}$. Gilt $\mathfrak{q} \supset \mathfrak{p}$, so folgt $I \subseteq \mathfrak{p}$, da $\mathfrak{p}$ Primideal ist. Dann folgt $\mathfrak{p} = \mathfrak{q}I \subseteq \mathfrak{q}\mathfrak{p} \subseteq \mathfrak{p}$, also $\mathfrak{p} = \mathfrak{q}\mathfrak{p}$. Da $\mathfrak{p}$ invertierbar ist, folgt $R = \mathfrak{q}$ im Widerspruch zur Annahme. Also gilt $\mathfrak{q} = \mathfrak{p}$. □

**5.7 Satz.** *Sei $I$ ein ganzes invertierbares Ideal von $R$ und seien $\mathfrak{p}_i$ Primideale von $R$ mit $I = \prod_{i=1}^{n} \mathfrak{p}_i$. Die $\mathfrak{p}_i$ sind dann bis auf die Reihenfolge eindeutig bestimmt.*

*Beweis.* Es gelte nun $I = \prod_{i=1}^{n} \mathfrak{p}_i = \prod_{j=1}^{m} \mathfrak{q}_j$ mit anderen Primidealen $\mathfrak{q}_j$ und $m \geq n$. Die $\mathfrak{p}_i$ und $\mathfrak{q}_j$ sind nach Lemma 5.6 invertierbar. Nach Umordnung erhalten wir $\mathfrak{p}_n \supseteq \mathfrak{q}_m$ aus der Primidealeigenschaft von $\mathfrak{p}_n$ und $\mathfrak{p}_n = \mathfrak{q}_m$ nach Lemma 5.6. Multiplikation mit $\mathfrak{p}_n^{-1}$ liefert $\prod_{i=1}^{n-1} \mathfrak{p}_i = \prod_{j=1}^{m-1} \mathfrak{q}_j$. Induktiv gelangen wir zu $R = \prod_{j=1}^{m'} \mathfrak{q}_j$. Wegen $R \supset \mathfrak{q}_1 \supseteq \prod_{j=1}^{m'} \mathfrak{q}_j$ für $m' \geq 1$ folgt schließlich $m' = 0$. □

**5.8 Satz.** *Sei $R$ ein noetherscher Integritätsring und $\mathcal{I}$ eine Menge von ganzen, invertierbaren Idealen von $R$, die bezüglich der Idealmultiplikation abgeschlossen ist und für die $R \in \mathcal{I}$ gilt. Dann sind äquivalent:*

(*i*) *Jedes Ideal aus $\mathcal{I}$ läßt sich in Primideale aus $\mathcal{I}$ faktorisieren.*

(*ii*) *Für jedes Ideal $I \in \mathcal{I}$ mit $I \neq R$ gibt es ein invertierbares Primideal $\mathfrak{p}$ von $R$ mit $\mathfrak{p} \supseteq I$ und $\mathfrak{p}^{-1}I \in \mathcal{I}$.*

*Sei $\mathcal{I}$ eine Menge von ganzen, invertierbaren Idealen von $R$, die diese Eigenschaften erfüllt. Dann sind die Faktorisierungen in (i) eindeutig und die Primideale aus $\mathcal{I}$ erzeugen bezüglich der Idealmultiplikation und Idealinversion eine freie abelsche Gruppe von invertierbaren Idealen von $R$.*

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Sei $I \in \mathcal{I}$. Für $I = R$ ist nichts zu zeigen. Sei also $I \neq R$. Es gilt $I = \prod_{i=1}^{n} \mathfrak{p}_i$ mit invertierbaren Primidealen $\mathfrak{p}_i \in \mathcal{I}$ und $n \geq 1$. Wegen $\mathfrak{p}_1 \supseteq \prod_{i=1}^{n} \mathfrak{p}_i = I$ und $\mathfrak{p}_1^{-1}I = \prod_{i=2}^{n} \mathfrak{p}_i \in \mathcal{I}$ aufgrund der multiplikativen Abgeschlossenheit erfüllt $\mathcal{I}$ die Eigenschaft (*ii*).

(*ii*) $\Rightarrow$ (*i*): Falls nicht alle Ideale aus $\mathcal{I}$ eine Faktorisierung in invertierbare Primideale aus $\mathcal{I}$ zulassen, gibt es ein bezüglich Inklusion maximales Ideal $I \in \mathcal{I}$

mit dieser Eigenschaft, da $R$ nach Voraussetzung noethersch ist. Es gilt $I \neq R$, weil $R$ das leere Produkt ist. Nach $(ii)$ existiert ein invertierbares Primideal $\mathfrak{p}$ von $R$ mit $\mathfrak{p} \supseteq I$ und $\mathfrak{p}^{-1}I \in \mathcal{I}$. Da $I$ invertierbar ist, gilt $I \supset \mathfrak{p}I$, denn sonst hätten wir $R = \mathfrak{p}$ nach Multiplikation mit $I^{-1}$. Multiplikation mit $\mathfrak{p}^{-1}$ liefert nun $R \supseteq \mathfrak{p}^{-1}I \supset I$. Nach Konstruktion gibt es invertierbare Primideale $\mathfrak{p}_i \in \mathcal{I}$ mit $\mathfrak{p}^{-1}I = \prod_i \mathfrak{p}_i$. Daraus folgt $I = \mathfrak{p}\prod_i \mathfrak{p}_i$. Außerdem ergibt sich $\mathfrak{p} = I(\prod_i \mathfrak{p}_i)^{-1} \in \mathcal{I}$.

Die Faktorisierungen sind nach Satz 5.7 eindeutig bestimmt. Daraus und aus der Invertierbarkeit ergibt sich auch die letzte Aussage. □

**5.9 Definition.** Ist $I$ eine Menge von ganzen, invertierbaren Idealen mit den Eigenschaften aus Satz 5.8, dann sagen wir, daß $I$ die Primidealfaktorisierungseigenschaft besitzt.

Ein noetherscher Integritätsring, für den jedes Ideal $\neq 0$ invertierbar ist, heißt Dedekindring.

**5.10 Korollar.** *In einem Dedekindring läßt sich jedes Ideal $\neq 0$ eindeutig in Primideale faktorisieren.*

*Beweis.* Die Menge aller Ideale $\neq 0$ besitzt die Primidealfaktorisierungseigenschaft, so daß die Behauptung aus Satz 5.8 folgt. □

Beim einem Dedekindring handelt es sich also um einen bestmöglichen Ring, was die Primidealfaktorisierung in invertierbare Primideale angeht. Es ist jetzt interessant, nach anderen Kriterien für Ringe und Ideale zu suchen, mit denen die Eigenschaft in Satz 5.8 und speziell die Dedekindringeigenschaft überprüft werden kann.

## 5.3 Lokale Charakterisierungen invertierbarer Ideale

Wir untersuchen zunächst das Verhalten unter Lokalisierung.

**5.11 Lemma.** *Sei $R$ ein Integritätsring und $U$ eine multiplikativ abgeschlossene Teilmenge von $R$ mit $1 \in U$.*

- $(i)$ *Für jedes gebrochene (ganze) Ideal $I$ von $R$ ist $I[U^{-1}]$ ein gebrochenes (ganzes) Ideal von $R[U^{-1}]$.*
- $(ii)$ *Für gebrochene Ideale $I, J$ von $R$ gelten die Gleichungen $(IJ)[U^{-1}] = I[U^{-1}] \cdot J[U^{-1}]$, $(I^{-1})[U^{-1}] = (I[U^{-1}])^{-1}$ und $(I : J)[U^{-1}] = (I[U^{-1}] : J[U^{-1}])$.*
- $(iii)$ *Für ein invertierbares Ideal $I$ von $R$ ist $I[U^{-1}]$ invertierbar.*

(*iv*) *Ist $\mathcal{I}$ eine Menge von Idealen mit Primfaktorisierungseigenschaft und ist $\mathcal{I}[U^{-1}] := \{I[U^{-1}] \mid I \in \mathcal{I}\}$, so besitzt $\mathcal{I}[U^{-1}]$ ebenfalls die Primidealfaktorisierungseigenschaft.*

(*v*) *Für einen Dedekindring $R$ ist $R[U^{-1}]$ ebenfalls ein Dedekindring.*

*Beweis.* (*i*): Sei $I$ ein gebrochenes Ideal von $R$ und $a \in R\backslash\{0\}$ mit $aI \subseteq R$. Dann gilt auch $a(I[U^{-1}]) = (aI)[U^{-1}] \subseteq R[U^{-1}]$, also ist $I[U^{-1}]$ ein gebrochenes Ideal von $R[U^{-1}]$. Die Aussage über das ganze Ideal ist auch klar.

(*ii*): Sei $(\sum_i x_i y_i)/u \in (IJ)[U^{-1}]$ mit $x_i \in I$, $y_i \in J$ und $u \in U$. Dann gilt $(\sum_i x_i y_i)/u = \sum_i (x_i/u)(y_i/u) \in I[U^{-1}]J[U^{-1}]$, also $(IJ)[U^{-1}] \subseteq I[U^{-1}]J[U^{-1}]$. Sei $\sum_i (x_i/u_{1,i})(y_i/u_{2,i}) \in I[U^{-1}]J[U^{-1}]$ mit $x_i \in I$, $y_i \in J$ und $u_{1,i}, u_{2,i} \in U$. Indem wir diesen Ausdruck auf Hauptnenner bringen, erhalten wir $x_i' \in I$, $y_i' \in J$ und $u \in U$ mit $\sum_i (x_i/u_{1,i})(y_i/u_{2,i}) = (\sum_i x_i' y_i')/u \in (IJ)[U^{-1}]$, also $I[U^{-1}]J[U^{-1}] \subseteq (IJ)[U^{-1}]$.

Die Aussage für $I^{-1}$ ist ein Spezialfall von der für $(I : J)$ wegen $I^{-1} = (I : R)$.

Für $x/u_1 \in (I : J)[U^{-1}]$ mit $x \in (I : J)$ und $u_1 \in U$ gilt $(x/u_1)(y/u_2) = (xy)/(u_1 u_2) \in J[U^{-1}]$ für alle $y \in I$ und $u_2 \in U$, also folgt $(I : J)[U^{-1}] \subseteq (I[U^{-1}] : J[U^{-1}])$. Ist umgekehrt $x/u \in (I[U^{-1}] : J[U^{-1}])$ mit $x \in R$ und $u \in U$, so gilt $xy = (x/u)(uy) \in J[U^{-1}]$ für alle $y \in I$, also $xy \in J$. Daraus folgt $(I[U^{-1}] : J[U^{-1}]) \subseteq (I : J)[U^{-1}]$.

(*iii*): Nach (*ii*) gilt $I[U^{-1}](I[U^{-1}])^{-1} = I[U^{-1}](I^{-1})[U^{-1}] = (II^{-1})[U^{-1}] = R[U^{-1}]$.

(*iv*): Folgt aus (*ii*), (*iii*) und Satz 1.69, da Lokalisieren einer Primidealfaktorisierung wie in Satz 5.8, (*i*) wieder eine solche liefert (unter Umständen mit weniger Primidealen, falls Primideale zu $R[U^{-1}]$ lokalisieren).

(*v*): Die Ideale von $R[U^{-1}]$ sind nach Satz 1.69 von der Form $I[U^{-1}]$ für ein Ideal $I$ von $R$. Für $I \neq 0$ ist nach Voraussetzung $II^{-1} = R$ und $I[U^{-1}]$ nach (*iii*) invertierbar. □

**5.12 Satz.** *Sei $R$ ein Integritätsring. Jedes invertierbare Ideal $I$ von $R$ ist endlich erzeugt. Für ein gebrochenes Ideal $I \neq 0$ von $R$ sind äquivalent:*

(*i*) *$I$ ist invertierbar.*

(*ii*) *$I$ ist projektiv.*

(*iii*) *$I$ ist lokal frei vom Rang 1.*

*Beweis.* Zur endlichen Erzeugung: Sei $J$ das inverse Ideal von $I$. Wegen $IJ = R$ gibt es $x_i \in I$ und $y_i \in J$ mit $1 = \sum_{i=1}^n x_i y_i$. Sei $x \in I$ beliebig. Dann gilt $x = x \sum_{i=1}^n x_i y_i = \sum_{i=1}^n (xy_i) x_i$, wobei $xy_i \in R$ für alle $1 \leq i \leq n$ ist. Also sind die $x_i$ ein Erzeugendensystem von $I$.

$(i) \Rightarrow (ii)$: Sei $I$ invertierbar und die $x_i, y_i$ wie eben. Wir definieren $\lambda_i \in \mathrm{Hom}_R(I, R)$ durch $x \mapsto xy_i$. Dann sind die $\lambda_i$ Koordinatenfunktionale bezüglich der Erzeuger $x_i$ und $I$ ist nach Satz 4.22 projektiv.

$(ii) \Rightarrow (i)$: Sei nun $I$ projektiv. Dann gibt es nach Satz 4.22 ein Erzeugendensystem $x_i$ (vielleicht unendlich) und Koordinatenfunktionale $\lambda_i \in \mathrm{Hom}_R(I, R)$. Nach den Betrachtungen hinter Definition 5.2 gibt es $y_i \in \mathrm{Quot}(R)$ mit $\lambda_i(x) = xy_i$ für alle $x \in I$. Sei $x \in I \backslash \{0\}$. Dann gilt $x = \sum_i \lambda_i(x)x_i = \sum_i (xy_i)x_i$, wobei die Summe endlich ist. Division durch $x$ ergibt $1 = \sum_i y_i x_i$. Wegen $xy_i \in R$ für alle $x \in I$ gilt $y_i \in I^{-1}$. Also folgt $1 \in II^{-1}$ und somit $II^{-1} = R$.

$(ii) \Rightarrow (iii)$: Ist $I$ projektiv, so ist es nach dem bereits Bewiesenen invertierbar und endlich erzeugt. Nach Satz 4.35 ist $I$ lokal frei. Nach Lemma 5.3 können wir annehmen, daß $I$ ein ganzes Ideal von $R$ ist. Sei $\mathfrak{m}$ ein maximales von $R$. Da $I_\mathfrak{m}$ ein Ideal und $R_\mathfrak{m}$-Untermodul von $R_\mathfrak{m}$ ist und daher keine zwei Elemente linear unabhängig sein können, folgt, daß $I_\mathfrak{m}$ frei vom Rang 1 ist.

Hier ist noch ein anderer, direkter Beweis für $(i) \Rightarrow (iii)$: Sei $I$ invertierbar. Wegen $II^{-1} = R$ gibt es $x_i \in I$ und $y_i \in I^{-1}$ mit $1 = \sum_i x_i y_i$. Sei $\mathfrak{m}$ ein maximales Ideal von $R$. Dann gibt es ein $i$ mit $x_i y_i \in R_\mathfrak{m} \backslash \mathfrak{m}R_\mathfrak{m}$, also $x_i y_i \in R_\mathfrak{m}^\times$. Es folgt $(x_i y_i)^{-1} x_i \in I_\mathfrak{m}$ und $y_i((x_i y_i)^{-1} x_i) = 1$, also $y_i I_\mathfrak{m} = R_\mathfrak{m}$. Daraus ergibt sich $I_\mathfrak{m} = R_\mathfrak{m} y_i^{-1}$, also ist $I_\mathfrak{m}$ frei vom Rang 1.

$(iii) \Rightarrow (i)$: Wir betrachten den Inklusionshomomorphismus $\phi : II^{-1} \to R$. Für jedes maximale Ideal $\mathfrak{m}$ von $R$ bekommen wir unter Verwendung von Lemma 5.11 den lokalisierten Monomorphismus $\phi_\mathfrak{m} : I_\mathfrak{m} I_\mathfrak{m}^{-1} \to R_\mathfrak{m}$. Da $I_\mathfrak{m}$ frei vom Rang 1 ist, gibt es $a \in \mathrm{Quot}(R_\mathfrak{m})$ mit $I_\mathfrak{m} = aR_\mathfrak{m}$. Aus der Definition von $I_\mathfrak{m}^{-1}$ folgt $I_\mathfrak{m}^{-1} = a^{-1} R_\mathfrak{m}$. Es ergibt sich $I_\mathfrak{m} I_\mathfrak{m}^{-1} = R_\mathfrak{m}$, also ist $\phi_\mathfrak{m}$ surjektiv und nach Satz 4.13 ist $\phi$ ein Isomorphismus und daher $II^{-1} = R$. □

Sei $R$ ein kommutativer Ring mit 1. Die Länge der echt aufsteigenden Kette $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ von Primidealen $\mathfrak{p}_i$ von $R$ ist $n$. Die Dimension $\dim(R)$ von $R$ ist das Supremum über die Länge aller echt aufsteigenden Ketten von Primidealen von $R$.

Ist $\mathfrak{p}$ ein Primideal, so nennen wir $\dim(R/\mathfrak{p})$ die Dimension und $\dim(R_\mathfrak{p})$ die Kodimension von $R$.

Ist $R$ ein Integritätsring mit $\dim(R) = 0$, so ist $R$ ein Körper. Denn $\{0\}$ ist ein Primideal, und wegen $\dim(R) = 0$ ist es das einzige Primideal von $R$. Daher ist es maximal und jedes Element $\neq 0$ eine Einheit.

Ist $R$ ein Integritätsring mit $\dim(R) = 1$, so ist $\{0\}$ ein Primideal und jedes weitere Primideal ist $\neq 0$ und maximal.

Für einen Integritätsring $R$ ist Bedingung $\dim(R) \leq 1$ also äquivalent dazu, daß jedes Primideal $\neq 0$ von $R$ maximal ist.

Zum Beispiel ist die Dimension des Polynomrings $k[x_1, \ldots, x_n]$ über dem Körper $k$ gleich $n$.

Jeder Körper $K$ ist ein Dedekindring, denn $K$ ist das einzige Ideal $\neq 0$ und $K$ ist invertierbar. Für einen Dedekindring $R$ gilt $\dim(R) \leq 1$. Denn entweder ist $\{0\}$ maximales Ideal und $R$ ein Körper, oder jedes Primideal $\mathfrak{p} \neq 0$ ist invertierbar und wegen Lemma 5.6 maximal.

**5.13 Definition.** Ein diskreter Bewertungsring ist ein lokaler Hauptidealring der Dimension 1.

Ist $R$ ein diskreter Bewertungsring, so gibt genau ein maximales Ideal $\mathfrak{m} = \pi R \neq 0$ von $R$. Dann ist $\mathfrak{m}$ das einzige Primideal $\neq 0$, und $\pi$ ist ein Primelement. Da $R$ auch faktoriell ist, gibt es zu jedem $a \in R\backslash\{0\}$ genau ein $u \in R^\times$ und $e \in \mathbb{Z}^{\geq 0}$ mit $a = u\pi^e$. Die Zuordnung $v : R \to \mathbb{Z} \cup \{\infty\}$ mit $v(a) = e$ und $v(0) = \infty$ liefert eine surjektive, diskrete Bewertung (siehe Algebra 1).

**5.14 Lemma.** *Ist $R$ ein Integritätsring mit $\dim(R) = 1$ und $\mathfrak{p} \neq 0$ ein Primideal von $R$, dann gilt $\dim(R_\mathfrak{p}) = 1$.*

*Beweis.* Zunächst ist $R_\mathfrak{p}$ lokal mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$. Die Abbildung $I \mapsto IR_\mathfrak{p} = I_\mathfrak{p}$ ist nach Satz 1.69 invers zur Abbildung $J \mapsto J \cap R$ für Ideale $I$ von $R$ und $J$ von $R_\mathfrak{p}$. Wegen $\mathfrak{p} \neq 0$ folgt daraus $\mathfrak{p}R_\mathfrak{p} \neq 0$. Für jedes Primideal $\mathfrak{q}'$ von $R_\mathfrak{p}$ gilt $\mathfrak{q}' \subseteq \mathfrak{p}R_\mathfrak{p}$ und $\mathfrak{q} = \mathfrak{q}' \cap R$ ist ein Primideal von $R$ mit $\mathfrak{q} \subseteq \mathfrak{p}$. Es folgt $\mathfrak{q} = \{0\}$ oder $\mathfrak{q} = \mathfrak{p}$ und daraus $\mathfrak{q}' = \mathfrak{q}R_\mathfrak{p} = \{0\}$ oder $\mathfrak{q}' = \mathfrak{p}R_\mathfrak{p}$. Also gilt $\dim(R_\mathfrak{p}) = 1$. □

**5.15 Satz.** *Ein noetherscher Integritätsring $R$ der Dimension 1 ist genau dann ein Dedekindring, wenn $R_\mathfrak{p}$ für jedes Primideal $\mathfrak{p} \neq 0$ ein diskreter Bewertungsring ist.*

*Beweis.* $\Rightarrow$: Sei $R$ ein Dedekindring. Dann ist $R_\mathfrak{p}$ lokal und es gilt $\dim(R_\mathfrak{p}) = 1$ nach Lemma 5.14. Sei $J \neq 0$ ein Ideal von $R_\mathfrak{p}$. Wir setzen $I = J \cap R$. Dann gilt $I \neq 0$ und $I_\mathfrak{p} = J$. Da $R$ ein Dedekindring ist, ist $I$ invertierbar. Nach Satz 5.12 ist dann $J = I_\mathfrak{p}$ ein Hauptideal.

$\Leftarrow$: Sei $I \neq 0$ ein Ideal von $R$. Für jedes Primideal $\mathfrak{p}$ von $R$ ist $I_\mathfrak{p}$ ein Hauptideal, da $R_\mathfrak{p}$ ein Hauptidealring ist. Nach Satz 5.12 ist $I$ damit invertierbar. □

Dedekindringe treten beispielsweise als Maximalordnungen von Zahlkörpern und als Koordinatenringe nicht-singulärer algebraischer Kurven auf. Wir wollen die Aussage von Satz 5.15 noch etwas detaillierter und allgemeiner untersuchen. Der folgende und nächste Satz kann zum Beispiel auf beliebige Ordnungen von Zahlkörpern und auf die Koordinatenringe algebraischer Varietäten angewendet werden.

**5.16 Lemma.** *Ein noetherscher Integritätsring $R$ ist genau dann ein diskreter Bewertungsring, wenn $R$ ein lokaler Ring mit* $\dim(R) = 1$ *und das maximale Ideal* $\mathfrak{m}$ *ein Hauptideal ist.*

*Ein Ring $R$ ist genau dann ein diskreter Bewertungsring, wenn $R$ ein lokaler faktorieller Ring mit* $\dim(R) = 1$ *ist.*

*Sei $R$ ein faktorieller Ring. Dann ist $\mathfrak{p}$ genau dann ein Primideal von $R$ mit* $\dim(R_\mathfrak{p}) = 1$*, wenn $\mathfrak{p} = R\pi$ für ein Primelement $\pi$ von $R$ gilt.*

*Beweis.* Zur ersten Aussage: $\Rightarrow$ ist klar. Für $\Leftarrow$ sei nun $\mathfrak{m} = \pi R$ mit $\pi \neq 0$ wegen $\dim(R) = 1$. Für $x \in R\backslash\{0\}$ gibt es ein maximales $e \in \mathbb{Z}^{\geq 0}$ und $u \in R$ mit $x = u\pi^e$, da $R$ noethersch und nullteilerfrei ist. Wegen der Maximalität von $e$ folgt $u \in R\backslash\pi R = R^\times$. Ist $I$ ein Ideal von $R$ und $a \in I$ mit minimalem Exponenten $e$, dann gilt $a \mid b$ für alle $b \in I$, also $I = aR$.

Zur zweiten Aussage: $\Rightarrow$ ist klar. Für $\Leftarrow$ sei $\pi$ ein Primelement von $R$, welches wegen $\dim(R) = 1$ exisiert. Dann ist $R\pi$ ein Primideal und wegen $\dim(R) = 1$ ist $R\pi$ das maximale Ideal von $R$. Aus der ersten Aussage folgt, daß $R$ ein diskreter Bewertungsring ist.

Zur dritten Aussage: Wir machen eine allgemeine Vorbemerkung. Ist $R$ ein faktorieller Ring und $U$ eine multiplikativ abgeschlossene Teilmenge, so ist $R[U^{-1}]$ ebenfalls faktoriell. Sind die $\pi_i$ ein vollständiges Vertretersystem von Primelementen modulo Assoziation, so liefern die $\pi_i$, die nicht zu Einheiten in $R[U^{-1}]$ werden, ein vollständiges Vertretersystem von Primelementen von $R[U^{-1}]$ modulo Assoziation. Hier ist die Begründung: Für $x \in R$ ist $x \in R[U^{-1}]^\times$ genau dann, wenn es $y \in R$ und $u \in U$ mit $x(y/u) = 1$ gibt, also wenn $xy = u$ und $x \mid u$ gilt. Ist $\pi_i$ ein Primelement, welches kein Element aus $U$ teilt, so ist $\pi_i$ ein Primelement in $R[U^{-1}]$. Denn aus $\pi_i(c/w) = (a/u)(b/v)$ mit $a, b, c \in R$ und $u, v, w \in U$ folgt $\pi_i cuv = abw$, und daraus folgt $\pi_i \mid a$ oder $\pi_i \mid b$ nach Voraussetzung. Also teilt $\pi_i$ auch $a/u$ oder $b/v$ und ist damit ein Primelement von $R[U^{-1}]$. Jedes Element aus $R[U^{-1}]$ kann als Potenzprodukt der $\pi_i$ geschrieben werden, da dies bereits in $R$ möglich ist. Sind $\pi_i$ und $\pi_j$ assoziiert in $R[U^{-1}]$, so gibt es $u, v \in U$ mit $u\pi_i = \pi_j v$. Da $\pi_i$ und $\pi_j$ weder $u$ noch $v$ teilen, folgt $\pi_i = \pi_j$ nach Voraussetzung.

„$\Rightarrow$“: Wegen $\dim(R_\mathfrak{p}) = 1$ ist $R_\mathfrak{p}$ ein lokaler faktorieller Ring der Dimension 1 mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p} \neq 0$ und nach der zweiten Aussage des Lemmas ein diskreter Bewertungsring. Nach der obigen Vorbemerkung gibt es ein Primelement $\pi$ von $R$, welches kein Element von $U = R\backslash\mathfrak{p}$ teilt und für welches $\mathfrak{p}R_\mathfrak{p} = \pi R_\mathfrak{p}$ gilt. Aus $x = (y/u)\pi \in R$ beziehunsgweise $ux = y\pi$ für $x, y \in R$ mit $x \neq 0$ und $u \in U$ folgt $\pi \mid x$. Daher ergibt sich $\mathfrak{p} = \mathfrak{p}R_\mathfrak{p} \cap R = \pi R$ mit Satz 1.69.

„$\Leftarrow$“: Da $\pi$ Primelement ist, ist $\mathfrak{p} \neq 0$ ein Primideal. Ferner ist $R_\mathfrak{p}$ ein lokaler faktorieller Ring mit $\mathfrak{p}R_\mathfrak{p} \neq 0$. Daraus folgt $\dim(R_\mathfrak{p}) = 1$. □

Die erste Aussage des Lemmas trifft für alle Primideale $\neq 0$ eines Dedekin-

drings zu. Unter Beachtung von Lemma 4.27 heißt das nichts anderes, als daß $\dim(R_\mathfrak{m}) \cong \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ für alle maximalen Primideale von $R$ gilt. Man sagt, daß die lokalen Ringe $R_\mathfrak{m}$ regulär seien.

**5.17 Satz.** *Sei $R$ ein noetherscher Integritätsring und $\mathfrak{p}$ ein Primideal von $R$.*

(*i*) *Ist $\mathfrak{p}$ invertierbar, so ist $R_\mathfrak{p}$ ein diskreter Bewertungsring.*

(*ii*) *Ist $R_\mathfrak{p}$ ein diskreter Bewertungsring und $R_\mathfrak{m}$ faktoriell für jedes maximale Ideal $\mathfrak{m}$ von $R$ mit $\mathfrak{m} \supseteq \mathfrak{p}$, so ist $\mathfrak{p}$ invertierbar.*

*Beweis.* (*i*): Ist $\mathfrak{p}$ invertierbar, so gilt $\mathfrak{p} \neq 0$ und $\mathfrak{p}R_\mathfrak{p} \neq 0$. Es folgt $\dim(R_\mathfrak{p}) = 1$. Weiter ist $\mathfrak{p}R_\mathfrak{p}$ nach Satz 5.12 ein Hauptideal. Nach der ersten Aussage von Lemma 5.16 ist $R_\mathfrak{p}$ dann auch ein diskreter Bewertungsring.

(*ii*): Nach Satz 5.12 genügt es zu beweisen, daß $\mathfrak{p}$ lokal ein Hauptideal ist. Dazu können wir uns auf Lokalisierungen für maximale Ideale beschränken. Ist $\mathfrak{m}$ ein maximales Ideal von $R$ mit $\mathfrak{m} \not\supseteq \mathfrak{p}$, so gilt $\mathfrak{p}R_\mathfrak{m} = R_\mathfrak{m}$, also ist $\mathfrak{p}$ hier frei. Sei $\mathfrak{m}$ also ein maximales Ideal mit $\mathfrak{m} \supseteq \mathfrak{p}$. Dann ist $R_\mathfrak{m}$ nach Voraussetzung faktoriell und wir wollen zeigen, daß $\mathfrak{p}R_\mathfrak{m}$ ein Hauptideal ist. Zur Vereinfachung der Notation und da $R_\mathfrak{p}$ nur eine weitere Lokalisierung von $R_\mathfrak{m}$ ist, können wir annehmen: $R$ ist faktoriell, $\mathfrak{p}$ ist ein Primideal von $R$ und $\mathfrak{p}R_\mathfrak{p}$ ist ein Hauptideal. Aus der dritten Aussage von Lemma 5.16 folgt, daß $\mathfrak{p}$ wie gewünscht ein Hauptideal ist. □

Die Voraussetzung in (*iii*), daß $R_\mathfrak{p}$ ein diskreter Bewertungsring sein soll, könnten wir also wegen der zweiten Aussage von Lemma 5.16 auch durch $\dim(R_\mathfrak{p}) = 1$ ersetzen.

Ist $I$ ein Ideal von $R$, welches lokal frei vom Rang 1 ist, so nennen wir $I$ auch ein lokales Hauptideal.

**5.18 Satz.** *Sei $R$ ein noetherscher Integritätsbereich. Sei $\mathcal{S}$ die Menge der maximalen Ideale von $R$, für die $R_\mathfrak{m}$ nicht faktoriell ist, und sei $\mathcal{I}$ die Menge der lokalen Hauptideale $I \neq 0$, für die $I_\mathfrak{m} = R_\mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m} \in \mathcal{S}$ gilt. Dann besitzt $\mathcal{I}$ die Primidealfaktorisierungseigenschaft.*

*Beweis.* Zunächst gilt $R \in \mathcal{I}$ und jedes Ideal aus $\mathcal{I}$ ist ganz und nach Satz 5.12 invertierbar. Außderdem ist $\mathcal{I}$ nach Lemma 5.11 multiplikativ abgeschlossen.

Wir wollen die Eigenschaft (*ii*) in Satz 5.8 nachrechnen. Sei $I$ ein lokales Hauptideal von $R$. Für $I = R$ ist nichts zu zeigen. Für $I \neq R$ gibt es ein maximales Ideal $\mathfrak{n} \notin \mathcal{S}$ mit $I_\mathfrak{n} \neq R_\mathfrak{n}$, wobei $R_\mathfrak{n}$ faktoriell ist.

Da $I_\mathfrak{n}$ ein Hauptideal ist, gibt es $x \in R$ mit $I_\mathfrak{n} = xR_\mathfrak{n}$. Wegen $I_\mathfrak{n} \neq R_\mathfrak{n}$ ist $x$ keine Einheit in $R_\mathfrak{n}$ und es gibt ein Element $\pi \in R$, welches in $R_\mathfrak{n}$ ein Primelement mit $\pi \mid x$ ist. Sei $\mathfrak{p} = \pi R_\mathfrak{n} \cap R$. Dann ist $\mathfrak{p}$ ein Primideal von $R$ mit $\mathfrak{p} \supseteq I$.

Nach Konstruktion gilt $\mathfrak{p}R_\mathfrak{n} = \pi R_\mathfrak{n}$ und $R_\mathfrak{p}$ ist ein diskreter Bewertungsring nach der ersten Aussage in Lemma 5.16. Für jedes maximale Ideal $\mathfrak{m} \supseteq \mathfrak{p}$ gilt $\mathfrak{m} \notin \mathcal{S}$ und $R_\mathfrak{m}$ ist ein faktorieller Ring nach Voraussetzung. Denn für $\mathfrak{m} \in \mathcal{S}$ gilt $I_\mathfrak{m} = R_\mathfrak{m}$, und daraus folgt $I_\mathfrak{p} = R_\mathfrak{p}$, was hier nicht der Fall ist. Nach Satz 5.17, $(ii)$ ist $\mathfrak{p}$ daher invertierbar. Schließlich sind $\mathfrak{p}^{-1}$ und $\mathfrak{p}^{-1}I$ nach Satz 5.12 und Lemma 5.11 invertierbar und lokale Hauptideale, deren Lokalisierung bei $\mathfrak{m} \in \mathcal{S}$ gleich $R_\mathfrak{m}$ ist. Also gilt $\mathfrak{p}^{-1}I \in \mathcal{I}$. Damit erfüllt $\mathcal{I}$ die Primidealfaktorisierungseigenschaft. □

Die Menge $\mathcal{S}$ kann als Menge singulärer Punkte von $R$ aufgefaßt werden. Ist $\mathfrak{m}$ ein maximales Ideal (oder ein Primideal) und gilt $I_\mathfrak{m} \neq R_\mathfrak{m}$, so sagen wir, $\mathfrak{m}$ sei im Träger von $I$. Im Satz 5.18 wird also gefordert, daß die Ideale aus $\mathcal{I}$ keine singulären Punkte in ihren Trägern haben sollen.

Wir wollen die beiden voranstehenden Sätze hauptsächlich für $\dim(R) = 1$ anwenden. Hier ist ein $\dim(R) = 2$ Beispiel: Der Polynomring $k[x, y]$ über einem Körper ist faktoriell. Das maximale Ideal $\mathfrak{m} = Rx + Ry$ ist wegen $\dim(R_\mathfrak{m}) = 0$ nicht invertierbar. Jedes Primideal $\mathfrak{p}$ von $R$ mit $\dim(R_\mathfrak{p}) = 1$ ist ein Hauptideal und invertierbar.

## 5.4 Ganze Ringerweiterungen

Seien $S$ ein Ring und $R$ ein Teilring von $S$. Dann nennen wir $S$ auch einen Erweiterungsring von $R$ und $R \subseteq S$ eine Ringerweiterung. Gemäß unseren Konventionen gilt $1_R = 1_S$.

Ist $R \subseteq S$ eine Ringerweiterung, können wir $S$ auch als $R$-Algebra und $R$-Modul auffassen. Dann heißt $S$ von endlichem Typ über $R$, wenn $S$ als $R$-Algebra endlich erzeugt ist, wenn es also $x_1, \ldots, x_n \in S$ mit $S = R[x_1, \ldots, x_n]$ gibt. Weiter heißt $S$ endlich über $R$, wenn $S$ als $R$-Modul endlich erzeugt ist, wenn es also $y_1, \ldots, y_m \in S$ mit $S = Ry_1 + \cdots + Ry_m$ gibt.

Ein Element $x \in S$ heißt ganz über $R$, wenn es ein normiertes Polynom $f \in R[t]$ mit $f(x) = 0$ gibt. Die Ringerweiterung $R \subseteq S$ heißt ganz, wenn jedes $x \in S$ ganz über $R$ ist. Der ganze Abschluß von $R$ in $S$ ist $\mathrm{Cl}(R, S) = \{x \in S \mid x \text{ ganz über } R\}$. Der Ring $R$ heißt ganz abgeschlossen (normal) in $S$, wenn $\mathrm{Cl}(R, S) = R$ gilt. Ist $R$ ein Integritätsring, dann heißt $R$ ganz abgeschlossen (normal), wenn $R$ ganz abgeschlossen in $S = \mathrm{Quot}(R)$ ist.

**5.19 Lemma.** *Sei $R \subseteq S$ eine Ringerweiterung und $x \in S$. Dann sind äquivalent:*

$(i)$ *$x$ ist ganz über $R$.*

$(ii)$ *$R[x]$ ist endlich über $R$.*

(*iii*) *Es gibt einen über $R$ endlich erzeugten $R[x]$-Modul $M$ mit* $\mathrm{Ann}_{R[x]}(M) = \{0\}$.

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Sei $f(x) = 0$ mit $f = \sum_{i=0}^{n} \lambda_i t^i$ und $\lambda_i \in R$, $\lambda_n = 1$. Dann gilt $0 = f(x) = x^n + \sum_{i=1}^{n-1} \lambda_i x^i$, also $x^n = \sum_{i=0}^{n-1}(-\lambda_i)x^i$. Daher bilden $1, x, \ldots, x^{n-1}$ ein endliches Erzeugendensystem von $R[x]$.

(*ii*) $\Rightarrow$ (*iii*): Sei $M = R[x]$. Nach Voraussetzung ist $M$ endlich erzeugt über $R$ und wegen $1 \in M$ folgt aus $zM = \{0\}$ für $z \in R[x]$ bereits $z \cdot 1 = z = 0$. Also gilt $\mathrm{Ann}_{R[x]}(M) = \{0\}$.

(*iii*) $\Rightarrow$ (*i*): Sei $x \in R$ und $\phi \in \mathrm{End}_{R[x]}(M)$ mit $\phi(m) = xm$. Nach Satz 4.25 angewendet auf $M$, $I = R$ und $\phi$ gibt es ein normiertes $f \in R[t]$ mit $f(\phi) = 0$, also $f(x)M = \{0\}$. Wegen $\mathrm{Ann}_{R[x]}(M) = \{0\}$ folgt $f(x) = 0$. □

**5.20 Satz.** *Seien $R \subseteq S$ und $S \subseteq T$ Ringerweiterungen.*

(*i*) *Ist $S$ endlich über $R$, so ist $S$ ganz über $R$.*

(*ii*) *Wenn $T$ endlich über $S$ und $S$ endlich über $R$ ist, so ist $T$ endlich über $R$. Ist $T$ endlich über $R$, so ist $T$ endlich über $S$.*

(*iii*) *Sind die $x_1, \ldots, x_n \in S$ ganz über $R$, so ist $R[x_1, \ldots, x_n]$ endlich über $R$.*

(*iv*) *$T$ ist genau dann ganz über $R$, wenn $T$ ganz über $S$ und $S$ ganz über $R$ ist.*

(*v*) $\mathrm{Cl}(R, S)$ *ist ein Erweiterungsring von $R$.*

(*vi*) $\mathrm{Cl}(R, S)$ *ist ganz abgeschlossen in $S$. abgeschlossen.*

*Beweis.* (*i*): Folgt aus Lemma 5.19, (*iii*) mit $M = S$.

(*ii*): Sind die $x_i$ ein Erzeugendensystem von $T$ über $S$ und die $y_j$ ein Erzeugendensystem von $S$ über $R$, so sind die $x_i y_j$ ein Erzeugendensystem von $T$ über $R$, was die erste Aussage beweist.

Sind die $x_i$ ein Erzeugendensystem von $T$ über $R$, so sind die $x_i$ auch ein Erzeugendensystem von $T$ über $S$, was die zweite Aussage beweist.

(*iii*): Aus Lemma 5.19, (*ii*) und der zweiten Aussage in (*ii*) folgt, daß $R[x_1, \ldots, x_i]$ endlich über $R[x_1, \ldots, x_{i-1}]$ ist. Aus der ersten Aussage in (*ii*) mehrfach angewendet ergibt sich damit, daß $R[x_1, \ldots, x_n]$ endlich über $R$ ist.

(*iv*): „$\Rightarrow$“ folgt direkt aus der Definition von „ganz“. Für „$\Leftarrow$“ sei $x \in T$ und $f = \sum_{i=0}^{n} \lambda_i t^i \in S[t]$ mit $\lambda_n = 1$ und $f(x) = 0$. Nach (*iii*) und (*ii*) ist $R[\lambda_1, \ldots, \lambda_n, x]$ endlich über $R$ und wegen (*i*) dann auch ganz über $R$. Also ist speziell $x$ ganz über $R$.

(*v*): Es gilt $R \subseteq \mathrm{Cl}(R, S)$, da $R$ ganz über $R$ ist. Für $x, y \in \mathrm{Cl}(R, S)$ ist $R[x, y]$ nach (*iii*) und (*i*) ganz über $R$. Wegen $x + y, xy \in R[x, y]$ sind dann auch $x + y$ und $xy$ ganz über $R$, also gilt $x + y, xy \in \mathrm{Cl}(R, S)$.

(*vi*) $\mathrm{Cl}(R, S)$ ist nach (*iv*) ganz abgeschlossen in $S$. □

**5.21 Satz.** *Jeder faktorielle Ring $R$ ist ganz abgeschlossen.*

*Beweis.* Seien $x/u \in \mathrm{Quot}(R)$ mit $x, u \in R$ teilerfremd und $\lambda_i \in R$ mit $(x/u)^n + \sum_{i=0}^{n-1} \lambda_i (x/u)^i = 0$. Multiplikation mit $u^n$ liefert $x^n + \sum_{i=0}^{n-1} \lambda_i u^{n-i} x^i = 0$. Wegen $i \leq n-1$ ist $x^n$ durch $u$ teilbar, im Widerspruch zur Annahme. □

Ist $R \subseteq S$ eine ganze Ringerweiterung und $f : S \to T$ ein Homomorphismus, so ist $S' = \phi(S)$ ganz über $R' = \phi(R)$: Für $y \in S'$ gibt es $x \in S$ mit $\phi(x) = y$. Ist $f \in R[t]$ normiert mit $f(x) = 0$, so ist $\phi(f) \in R'[t]$ normiert und es gilt $\phi(f)(y) = \phi(f)(\phi(x)) = \phi(f(x)) = 0$. Also ist $y$ ganz über $R'$.

**5.22 Satz.** *Sei $R \subseteq S$ eine Ringerweiterung und $U$ eine multiplikativ abgeschlossene Teilmenge von $R$ mit $1 \in U$.*

(*i*) *Ist $R \subseteq S$ ganz, so ist auch $R[U^{-1}] \subseteq S[U^{-1}]$ ganz.*

(*ii*) *Es gilt $\mathrm{Cl}(R, S)[U^{-1}] = \mathrm{Cl}(R[U^{-1}], S[U^{-1}])$.*

(*iii*) *$R$ ist genau dann ganz abgeschlossen in $S$, wenn $R_\mathfrak{m}$ für jedes maximale Ideal $\mathfrak{m}$ von $R$ ganz abgeschlossen in $S_\mathfrak{m} = S[(R \backslash \mathfrak{m})^{-1}]$ ist.*

*Beweis.* (*i*): Die Aussage folgt aus der Bemerkung vor dem Satz.

(*ii*): Nach (*i*) ist $\mathrm{Cl}(R, S)[U^{-1}]$ ganz über $R[U^{-1}]$, es folgt also $\mathrm{Cl}(R, S)[U^{-1}] \subseteq \mathrm{Cl}(R[U^{-1}], S[U^{-1}])$.

Sei $x/u \in \mathrm{Cl}(R[U^{-1}], S[U^{-1}])$ mit $x \in S$ und $u \in U$. Für $x/u \in \mathrm{Cl}(R, S)[U^{-1}]$ müssen wir zeigen, daß es ein $v \in U$ mit $xv$ ganz über $R$ gibt. Sei $(x/u)^n + \sum_{i=0}^{n-1} (\lambda_i/u_i)(x/u)^i = 0$ mit $\lambda_i \in R$ und $u_i \in U$. Sei $v = \prod_{i=0}^{n-1} u_i$. Multiplikation mit $(uv)^n$ liefert $(xv)^n + \sum_{i=0}^{n-1} (\lambda_i u^{n-i} v^{n-i}/u_i)(xv)^i = 0$, wobei $\lambda_i u^{n-i} v^{n-i}/u_i \in R$ wegen $i \leq n-1$ gilt. Also ist $xv$ ganz über $R$ und es folgt $\mathrm{Cl}(R[U^{-1}], S[U^{-1}]) \subseteq \mathrm{Cl}(R, S)[U^{-1}]$.

(*iii*): Wir betrachten den Inklusionshomomorphismus $\phi : R \to \mathrm{Cl}(R, S)$ und die Lokalisierungen $\phi_\mathfrak{m} : R_\mathfrak{m} \to \mathrm{Cl}(R, S)_\mathfrak{m}$. Wegen $\mathrm{Cl}(R, S)_\mathfrak{m} = \mathrm{Cl}(R_\mathfrak{m}, S_\mathfrak{m})$ nach (*ii*) sind die $\phi_\mathfrak{m}$ genau dann Isomorphismen, wenn $R_\mathfrak{m}$ für alle $\mathfrak{m}$ ganz abgeschlossen in $S_\mathfrak{m}$ ist. Ebenso ist $\phi$ genau dann ein Isomorphismus, wenn $R$ ganz abgeschlossen in $S$ ist. Die Äquivalenz dieser Aussagen folgt nun aus Satz 4.13. □

Die Aussage (*iii*) gilt dann natürlich auch wieder für alle Primideale $\mathfrak{p}$ von $R$ anstelle der maximalen Ideale $\mathfrak{m}$ von $R$.

## 5.5 Globale Charakterisierung von Dedekindringen

Sei $M$ ein $R$-Modul. Ist $\mathfrak{p}$ ein Primideal von $R$ mit $\mathfrak{p} = \mathrm{Ann}_R(m)$ für ein $m \in M$, so heißt $\mathfrak{p}$ ein assoziiertes Primideal von $M$. Wegen $\mathfrak{p} \neq R$ folgt hier $m \neq 0$. Es gilt $\mathfrak{p} \supseteq \mathrm{Ann}_R(M)$.

**5.23 Satz.** *Sei $M \neq 0$ ein $R$-Modul.*

(*i*) *Sei $J$ ein maximales Ideal in der Menge*

$$\mathcal{I} = \{I \mid I \text{ Ideal von } R \text{ mit } I = \mathrm{Ann}_R(m) \text{ für ein } m \in M\backslash\{0\}\}.$$

*Dann ist $I$ ein Primideal.*

(*ii*) *Jeder noethersche $R$-Modul $M \neq 0$ besitzt ein assoziiertes Primideal.*

*Beweis.* (*i*): Sei $m \in M\backslash\{0\}$ mit $J = \mathrm{Ann}_R(m)$. Zunächst gilt $J \neq R$, da $m \neq 0$. Seien $x, y \in R$ mit $xy \in J$ und $x \notin J$. Dann ist $xm \neq 0$ und $(Ry + J)(xm) = \{0\}$. Wegen der Maximalität von $J$ folgt $J = Ry + J$, also $y \in J$. Daher ist $J$ ein Primideal.

(*ii*): Wegen $M \neq 0$ gilt $\mathcal{I} \neq \emptyset$. Es gilt zum Beispiel $\{0\} \in \mathcal{I}$. Da $M$ noethersch ist, gibt es in $\mathcal{I}$ ein maximales Ideal $J$, welches nach (*i*) ein Primideal ist. □

**5.24 Lemma.** *Sei $R$ ein lokaler noetherscher Integritätsring $R$ der Dimension* 1. *Dann sind äquivalent:*

(*i*) *$R$ ist ganz abgeschlossen.*

(*ii*) *$(I : I) = R$ für jedes Ideal $I \neq 0$ von $R$.*

(*iii*) *$R$ ist ein diskreter Bewertungsring.*

*Beweis.* (*i*) $\Rightarrow$ (*ii*): Wegen $RI = I$ gilt $(I : I) \supseteq R$. Da $R$ noethersch ist, ist $I$ ein endlich erzeugter $R$-Modul. Da $R$ ein Integritätsring und $I \neq 0$ ist, folgt $\mathrm{Ann}_R(I) = \{0\}$. Nach Satz 5.19, (*iii*) sind die Elemente aus $(I : I)$ ganz über $R$. Da $R$ ganz abgeschlossen ist, folgt $(I : I) \subseteq R$, also $(I : I) = R$.

(*ii*) $\Rightarrow$ (*iii*): Sei $\mathfrak{p}$ das maximale Ideal von $R$. Es gilt $R \subseteq \mathfrak{p}^{-1}$ und daher ist $\mathfrak{p}^{-1}\mathfrak{p}$ ein Ideal von $R$ mit $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. Da $\mathfrak{p}$ maximal ist, gilt $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ oder $\mathfrak{p}^{-1}\mathfrak{p} = R$.

Wir nehmen $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ an. Da $R$ Dimension 1 hat, ist $\mathfrak{p} \neq 0$. Nach (*ii*) gilt dann $\mathfrak{p}^{-1} \subseteq R$. Nach Satz 5.23 gibt es zu $x \in \mathfrak{p}\backslash\{0\}$ ein assoziiertes Primideal $\mathfrak{q} \subseteq R$ von $R/Rx$. Wegen $\mathfrak{q} \supseteq \mathrm{Ann}_R(R/Rx) = Rx \neq 0$ und da $R$ Dimension 1 hat,

folgt $\mathfrak{p} = \mathfrak{q}$. Nach der Definition von assoziiertem Primideal gibt es also $y \in R \backslash Rx$ mit $y\mathfrak{p} \subseteq Rx$. Es gilt also $(y/x)\mathfrak{p} \subseteq R$ und $y/x \notin R$. Daraus folgt $\mathfrak{p}^{-1} \not\subseteq R$. Also ist $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ nicht möglich, es gilt $\mathfrak{p}^{-1}\mathfrak{p} = R$. Damit ist $\mathfrak{p}$ invertierbar, und nach Satz 5.17, $(i)$ ist $R$ ein diskreter Bewertungsring.

$(iii) \Rightarrow (i)$: Jeder diskrete Bewertungsring ist auch ein faktorieller Ring. Nach Satz 5.21 ist $R$ ganz abgeschlossen. □

**5.25 Satz.** *Sei $R$ ein noetherscher Integritätsring $R$ der Dimension 1. Dann sind äquivalent:*

$(i)$ *$R$ ist ganz abgeschlossen.*

$(ii)$ *$(I : I) = R$ für jedes Ideal $I \neq 0$ von $R$.*

$(iii)$ *$R$ ist ein Dedekindring.*

*Beweis.* $(i) \Rightarrow (ii)$: Nach Satz 5.22, $(iii)$ ist $R_\mathfrak{p}$ ganz abgeschlossen für jedes Primideal $\mathfrak{p}$ von $R$. Nach Lemma 5.24 gilt damit $(I_\mathfrak{p} : I_\mathfrak{p}) = R_\mathfrak{p}$ für alle $\mathfrak{p}$. Nach Satz 4.13 und Lemma 5.11, $(ii)$ folgt $(I : I) = R$.

$(ii) \Rightarrow (iii)$: Für jedes Primideal $\mathfrak{p}$ von $R$ und jedes Ideal $J$ von $R_\mathfrak{p}$ ist $I = J \cap R$ ein Ideal von $R$ mit $I_\mathfrak{p} = J$. Wegen $(I : I) = R$ gilt $(J : J) = (I_\mathfrak{p} : I_\mathfrak{p}) = R_\mathfrak{p}$ nach Lemma 5.11, $(ii)$. Nach Lemma 5.24 ist $R_\mathfrak{p}$ ein diskreter Bewertungsring für alle $\mathfrak{p}$. Nach Satz 5.15 ist $R$ dann ein Dedekindring.

$(iii) \Rightarrow (i)$: Nach Satz 5.15 ist $R_\mathfrak{p}$ ein diskreter Bewertungsring für alle Primideale $\mathfrak{p}$ von $R$. Nach Lemma 5.24 ist $R_\mathfrak{p}$ ganz abgeschlossen für alle $\mathfrak{p}$. Nach Satz 5.22, $(iii)$ ist damit $R$ ganz abgeschlossen. □

Der Satz 5.25 enthält Lemma 5.24 als Spezialfall, wenn man $R$ lokalisiert. Die Äquivalenz von $(i)$ und $(ii)$ gilt auch ohne die Voraussetzung $\dim(R) = 1$, und $(iii)$ wird durch die Aussage ersetzt, daß für jedes zu $R/Rx$ mit $x \neq 0$ assoziierte Primideal $\mathfrak{p}$ der lokale Ring $R_\mathfrak{p}$ ein diskreter Bewertungsring ist. Dazu beweist man eine Version von Satz 4.13 unter der Voraussetzung $R$ noethersch, in der nur für solche assoziierte Primideale lokalisiert werden muß. Dann tauchen im Beweis von Satz 5.25 nur noch zu $R/Rx$ mit $x \neq 0$ assoziierte Primideale $\mathfrak{p}$ auf. Speziell wird Lemma 5.24 im Beweis von Satz 5.25 nur für $R_\mathfrak{p}$ mit zu $R_\mathfrak{p}/xR_\mathfrak{p}$ assoziierten Primidealen $\mathfrak{p}R_\mathfrak{p}$ angewendet. Der Beweis von Lemma 5.24 basiert dann direkt auf dieser Eigenschaft und benötigt die Voraussetzung $\dim(R) = 1$ nicht mehr.

Für einen ganz abgeschlossenen, noetherschen Integritätsring $R$ und ein Primideal $\mathfrak{p}$ von $R$ mit $\dim(R_\mathfrak{p}) = 1$ ist $R_\mathfrak{p}$ nach Satz 5.22, $(iii)$ ganz abgeschlossen und daher nach Lemma 5.24 ein diskreter Bewertungsring. Ist dann noch $R_\mathfrak{m}$ faktoriell für alle maximalen Ideale $\mathfrak{m} \supseteq \mathfrak{p}$, so ist $\mathfrak{p}$ nach Satz 5.17 invertierbar. Damit $R$ nicht singulär im Sinn der Bemerkung nach Satz 5.18 ist ($R_\mathfrak{m}$ faktoriell für jedes

maximale Ideal $\mathfrak{m}$ von $R$), muß $R$ also notwendigerweise ganz abgeschlossen sein. Für $\dim(R) = 1$ ist dies nach Satz 5.25 auch hinreichend, weil jedes Primideal $\mathfrak{p}$ mit $\dim(R_\mathfrak{p}) = 1$ maximal ist. Für $\dim(R) \geq 2$ gibt es Beispiele, in denen $R$ ganz abgeschlossen ist und es dennoch singuläre maximale Ideale $\mathfrak{m}$ von $R$ gibt (also $R_\mathfrak{m}$ nicht faktoriell).

Die Aussage $(ii)$ von Satz 5.25 kann für die Berechnung von $\mathrm{Cl}(R, \mathrm{Quot}(R))$ genutzt werden. Für invertierbare Ideale $I$ gilt stets $(I : I) = I^{-1}I = R$. Durch das Aufspüren geeigneter, nicht invertierbarer Ideale $I$ und die Bestimmung der Erweiterungsringe $(I : I)$ von $R$ können wir $R$ sukzessive zu $\mathrm{Cl}(R, \mathrm{Quot}(R))$ erweitern. Ist zum Beispiel $\mathfrak{p}$ ein Primideal $\neq 0$ mit $R_\mathfrak{p}$ nicht ganz abgeschlossen, so gilt $\mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p}$ und $\mathfrak{p}^{-1} \not\subseteq R$ nach dem Beweis von Lemma 5.24. Daraus folgt, daß $(\mathfrak{p} : \mathfrak{p})$ ein über $R$ ganzer Erweiterungsring von $R$ mit $(\mathfrak{p} : \mathfrak{p}) \neq R$ ist.

Im folgenden Satz wird das leere Produkt für $I = R$ mit eingerechnet.

**5.26 Satz.** *Sei $R$ ein Integritätsring mit der Eigenschaft, daß jedes Ideal ein Produkt von Primidealen ist. Dann ist $R$ ein Dedekindring.*

*Beweis.* Ist zwar nicht so schwer und lang, lassen wir aber aus. □

Die klassische Zusammenfassung der äquivalenten Eigenschaften eines Dedekindrings liefert nun der folgende Satz.

**5.27 Satz.** *Für einen Integritätsring $R$ sind äquivalent:*

- $(i)$ *$R$ ist ein Dedekindring.*
- $(ii)$ *Jedes Ideal läßt sich bis auf die Reihenfolge auf genau eine Weise als Produkt von Primidealen von $R$ schreiben.*
- $(iii)$ *$R$ ist noethersch und $R_\mathfrak{p}$ ist ein diskreter Bewertungsring für jedes maximale Ideal $\mathfrak{m} \neq 0$ von $R$.*
- $(iv)$ *$R$ ist ganz abgeschlossen und noethersch, und jedes Primideal von $R$ ist maximal.*

*Beweis.* $(i) \Rightarrow (ii)$: Satz 5.8.
$(ii) \Rightarrow (i)$: Satz 5.26.
$(i) \Leftrightarrow (iii)$: Satz 5.15.
$(i) \Leftrightarrow (iv)$: Satz 5.25. □

Hier ist eine weitere Eigenschaft von Dedekindringen (vgl. das Diagramm auf Seite 25).

**5.28 Satz.** *Ein noetherscher Integritätsbereich $R$ ist genau dann ein Hauptidealring, wenn $R$ ein Dedekindring und faktoriell ist.*

*Beweis.* „$\Rightarrow$“: Da Hauptideale $\neq 0$ invertierbar sind, ist diese Aussage klar.

„$\Leftarrow$“: Sei $\mathfrak{p} \neq 0$ ein Primideal von $R$ und $x \in \mathfrak{p}\backslash\{0\}$. Sei $Rx = \prod_i \mathfrak{p}_i$ die Faktorisierung in Primideale mit $\mathfrak{p}_1 = \mathfrak{p}$. Sei $x = \prod_j \pi_j$ eine Faktorisierung in Primelemente. Die Ideale $R\pi_j$ sind dann Primideale und es gilt $Rx = \prod_j R\pi_j$. Wegen der Eindeutigkeit der Faktorisierung folgt $\mathfrak{p} = R\pi_j$ für ein $j$. Also ist $\mathfrak{p}$ ein Hauptideal. Da $\mathfrak{p}$ beliebig war, sind alle Primideale und damit alle Ideale von $R$ Hauptideale. □

## 5.6 Beispiele

Beispiele für freie Moduln sind die $R$-Moduln $R^n$.

Ein Beispiel für einen projektiven, aber nicht freien Modul ist $R = \mathbb{Z}[\sqrt{-5}]$ und das Ideal $M = 2R + (1 + \sqrt{-5})R$. Der Beweis dieser Tatsache fällt in die algebraische Zahlentheorie ($R$ ist ganzalgebraisch abgeschlossen, also ein Dedekindring, und $M$ ist kein Hauptideal. Die Klassenzahl von $R$ ist 2).

Hier sind weitere Details zu diesem Beispiel. Sei $\rho = \sqrt{-5}$. Dann gilt $6 = 2{\cdot}3 = (1 + \rho)(1 - \rho)$. Man kann zeigen, daß 2, 3, $1 + \rho$ und $1 - \rho$ irreduzible Elemente in $R$ sind. Also ist $R$ ein Ring, in dem es keine eindeutige Faktorisierung in Primelemente mehr gibt. Zur Abhilfe wurden von Kummer in der zweiten Hälfte des 19. Jahrhunderts „ideale Zahlen“ eingeführt, mit denen dann eine eindeutige Faktorisierung möglich sein sollte (vergleichbar mit dem Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$, so daß jede Zahl in $\mathbb{Z}$ invertierbar wird). Bei diesen handelt es sich schlicht um (invertierbare) Ideale von $R$. Das geht dann wie folgt: Sei $\mathfrak{p} = 2R + (1 + \rho)R$, $\mathfrak{q}_1 = 3R + (1 + \rho)R$ und $\mathfrak{q}_2 = 3R + (1 - \rho)R$. Dann sind $\mathfrak{p}$, $\mathfrak{q}_1$ und $\mathfrak{q}_1$ Primideale. ( Ein Beweis dieser Tatsache kann im Prinzip wie folgt gehen: Sei $p$ eine Primzahl und $f = t^2 + 5 \in \mathbb{Z}[t]$ Dann gilt $R \cong \mathbb{Z}[t]/(f)$. Wir betrachten die natürlichen Homomorphismen $\phi : R \mapsto R \otimes_{\mathbb{Z}} \mathbb{F}_p$ und $\psi : R \otimes_{\mathbb{Z}} \mathbb{F}_p \to \mathbb{F}_p[t]/(g)$, wobei $g \in \mathbb{F}_p[t]$ die Reduktion von $f \in \mathbb{Z}[t]$ ist. Nach einer Übungsaufgabe wissen wir, daß $\psi$ ein Isomorphismus ist. Der Homomorphismus $\phi$ ist surjektiv und hat den Kern $pR$. Die Verknüpfung $\psi \circ \phi$ ist gerade der kanonische Epimorphismus. Damit entsprechen sich die Primideale $\mathfrak{p}$ von $R$ mit $p \in \mathfrak{p}$ und die Primideale von $R \otimes_{\mathbb{Z}} \mathbb{F}_p$ eineindeutig. Mit Hilfe des chinesischen Restsatzes können wir die Primideale von $\mathbb{F}_p[t]/(g)$ bestimmen, dann ihre Urbilder unter $\psi$ und ihre Urbilder unter $\phi$. Die Primideale von $\mathbb{F}_p[t]/(g)$ werden von den irreduziblen Faktoren von $g$ erzeugt. )

Weiter gilt

$$\begin{aligned} \mathfrak{p}^2 = 2R, \quad \mathfrak{q}_1\mathfrak{q}_2 = 3R \\ \mathfrak{p}\mathfrak{q}_1 = (1+\rho)R, \quad \mathfrak{p}\mathfrak{q}_2 = (1-\rho)R. \end{aligned}$$

Daraus folgt für die Faktorisierung von 6:

$$\begin{aligned} 6R &= 2R \cdot 3R = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2 \\ 6R &= (1+\rho)R \cdot (1-\rho)R = \mathfrak{p}\mathfrak{q}_1\mathfrak{p}\mathfrak{q}_2 = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2. \end{aligned}$$

Man sieht hier schön, wie durch die Hinzunahme der Primideale die Elementsituation ergänzt wird. Speziell sind $\mathfrak{p}$, $\mathfrak{q}_1$ und $\mathfrak{q}_2$ keine Hauptideale, denn sonst gäbe es ja Primelemente, welche 2, 3, $1+\rho$ und $1-\rho$ teilen würden und 2, 3, $1+\rho$ und $1-\rho$ könnten nicht irreduzibel sein.

Wegen $\mathfrak{p}^2 = 2R$ und $\mathfrak{q}_1\mathfrak{q}_2 = 3R$ sind diese Ideale invertierbare Ideale, da $2R$ und $3R$ invertierbar sind. Damit sind sie auch projektiv. Sie sind aber nicht frei, denn sonst müßten sie ja Hauptideale sein.

Typische Beispiele für flache, aber nicht projektive $R$-Moduln kann man aus den Moduln $M[U^{-1}]$, aufgefaßt als $R$-Moduln, erhalten. Sei $R = M = \mathbb{Z}$, $U = \langle 3 \rangle$ und $M[U^{-1}] = \mathbb{Z}[1/3]$. Der $\mathbb{Z}$-Modul $\mathbb{Z}[1/3]$ ist einerseits nicht endlich erzeugt, denn sonst wären die auftretenden Nenner in $\mathbb{Z}[1/3]$ beschränkt, andererseits sind aber je zwei Elemente aus $\mathbb{Z}[1/3]$ über $\mathbb{Z}$ linear abhängig. Insbesondere kann es keine Einbettung von $\mathbb{Z}[1/3]$ in einen freien $\mathbb{Z}$-Model geben, da in einem freien $\mathbb{Z}$-Modul Elemente nicht beliebig durch Potenzen von 3 teilbar sind, was aber in $\mathbb{Z}[1/3]$ der Fall ist. Nach Satz 4.22, (*ii*) ist $\mathbb{Z}[1/3]$ daher nicht projektiv. Ein weiteres Beispiel für diesen Effekt ist $\mathbb{Q}$ als $\mathbb{Z}$-Modul.

Torsionsfreie, aber nicht flache Moduln sind zum Beispiel das maximale Ideal $M$ von $R = k[[x_1, x_2]]$ als $R$-Modul, oder $M = \mathbb{Z}[(1+\sqrt{5})/2]$ als $R = \mathbb{Z}[\sqrt{5}]$-Modul.

# Kapitel 6

# Kategorien

Wir wollen in diesem Kapitel ein paar Worte über Kategorien und die Begriffe direkte Summe und direktes Produkt sagen, ohne allzusehr auf die Details einzugehen. Mit Hilfe von Kategorien kann man gängige mathematische Konstrukte und Situationen gebietsübergreifend und allgemein behandeln. Das ist für sich genommen interessant und manchmal in konkreten Anwendungen auch nützlich.

## 6.1 Allgemeine Bemerkungen

Unter eine Kategorie versteht man eine Ansammlung von mathematischen Objekten gleichen Typs und ihre strukturerhaltenden Abbildungen, welche Morphismen genannt werden. Beispiele sind Gruppen und Homomorphismen, Ringe und Ringhomomorphismen, topologische Räume und stetige Abbildungen, Mannigfaltigkeiten und differenzierbare Funktionen, Mengen und Abbildungen und eben auch Moduln über einem Ring $R$ und $R$-lineare Abbildungen, an denen wir hauptsächlich interessiert sind. Für solche Objekte gibt es immer wiederkehrende Konstruktionen wie direkte Summen und Produkte. In der Kategorientheorie werden unter anderem solche Gemeinsamkeiten und Prinzipien herausgearbeitet und abstrakt, häufig losgelöst von speziellen Typen mathematischer Objekte, untersucht.

In vielen Fällen handelt es sich bei den Objekten einer Kategorie nicht einmal um Mengen mit Elementen, sondern beispielsweise wieder um Abbildungen (zum Beispiel Funktoren, siehe unten). Entsprechend müssen die Morphismen keine Abbildungen sein. Trotzem sollen Morphismen einen „Definitionsbereich“ und einen „Bildbereich“ haben und es soll möglich sein, Morphismen zu „verknüpfen“ und auf Gleichheit zu testen, was man eben von echten Abbildungen erwarten würde.

Eine Abbildung zwischen zwei Kategorien, welche Objekte auf Objekte und

Morphismen auf Morphismen abbildet, mit Homomorphieeigenschaft bezüglich der Verknüpfung von Morphismen, heißt ein Funktor. Ein Beispiel ist der Vergißfunktor von der Kategorie der $R$-Moduln in die Kategorie der Mengen, der jedem Modul seine unterliegende Menge und jedem Homomorphismus die entsprechende Abbildung von Mengen zuordnet. Ein anderes Beispiel ist die Fixgruppenabbildung $\mathcal{G}_{E/K}$ aus der Galoistheorie, welche Körper und Inklusionsabbildungen nach Gruppen und umgekehrte Inklusionsabbildungen abbildet.

Ein Funktor stellt also eine Beziehung zwischen zwei Kategorien dar. Man kann einen Funktor zum Beispiel dazu benutzen, die Kategorie des Definitionsbereichs mit Hilfe der Kategorie des Bildbereichs zu untersuchen. Ein wichtiges Beispiel hierfür ist die Galoistheorie, wo Körper mit Hilfe von Gruppen untersucht werden. Ähnlich kann man auch gewissen topologischen Räumen ihre Fundamentalgruppen zuordnen und anhand dieser Gruppen Rückschlüsse auf die topologischen Räume ziehen.

Im folgenden wird eine Kurzzusammenfassung bzw. ein Glossar gängiger kategorientheoretischer Begriffe gegeben. Im allgemeinen müßten wir noch etwas auf mengentheoretische Probleme achten (siehe „Menge aller Mengen“), aber das soll uns hier nicht weiter stören.

## 6.2 Definitionen

Eine Kategorie $\mathcal{C}$ besteht aus einer Klasse $\mathrm{Obj}(\mathcal{C})$ von Objekten und einer Klasse $\mathrm{Mor}(\mathcal{C})$ von Morphismen mit den folgenden Eigenschaften. Jeder Morphismus $f \in \mathrm{Mor}(\mathcal{C})$ besitzt genau ein Objekt $A \in \mathrm{Obj}(\mathcal{C})$ als „Definitionsbereich“ und genau ein Objekt $B \in \mathrm{Obj}(\mathcal{C})$ als „Wertebereich“. Die Morphismen $f \in \mathrm{Mor}(\mathcal{C})$ mit Definitionsbereich $A$ und Wertebereich $B$ bilden eine Menge, die mit $\mathrm{Mor}_{\mathcal{C}}(A, B)$ bezeichnet wird. Wir schreiben auch $f : A \to B$. Es gibt Verknüpfungen $\circ : \mathrm{Mor}_{\mathcal{C}}(A, B) \times \mathrm{Mor}_{\mathcal{C}}(B, C) \to \mathrm{Mor}_{\mathcal{C}}(A, C)$ und ausgezeichnete Elemente $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$ mit $f \circ \mathrm{id}_A = f$, $\mathrm{id}_A \circ f = f$ und $(f \circ g) \circ h = f \circ (g \circ h)$ für beliebige $f, g, h \in \mathrm{Mor}(\mathcal{C})$, deren Definitions- und Wertebereiche entsprechend zusammenpassen.

Unser Standardbeispiel ist $\mathcal{C} = (R\text{-Moduln})$, die Kategorie der $R$-Moduln, für einen Ring $R$ mit 1. Hier schreiben wir $\mathrm{Hom}_R(A, B)$ statt $\mathrm{Mor}_{\mathcal{C}}(A, B)$. Man kann als weitere, abstrakte Beispiele aber auch geeignete, gerichtete Graphen heranziehen, wo die Ecken die Objekte und die Pfeile die Morphismen darstellen.

Eine Teilkategorie $\mathcal{D}$ einer Kategorie $\mathcal{C}$ erfüllt definitionsgemäß $\mathrm{Obj}(\mathcal{D}) \subseteq \mathrm{Obj}(\mathcal{C})$ und $\mathrm{Mor}_{\mathcal{D}}(A, B) \subseteq \mathrm{Mor}_{\mathcal{C}}(A, B)$ für alle $A, B \in \mathrm{Obj}(\mathcal{D})$ und heißt voll, wenn hier speziell $\mathrm{Mor}_{\mathcal{D}}(A, B) = \mathrm{Mor}_{\mathcal{C}}(A, B)$ gilt.

Ein Morphismus $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ heißt Isomorphismus, wenn es $g \in \mathrm{Mor}_{\mathcal{C}}(B, A)$

mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$ gibt. Zwei Objekte $A$ und $B$ heißen isomorph, wenn es einen Isomorphismus $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ gibt. Ein Morphismus $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ heißt Monomorphismus, wenn für alle Objekte $C$ und $g_1, g_2 \in \mathrm{Mor}_{\mathcal{C}}(C, A)$ aus $f \circ g_1 = f \circ g_2$ bereits $g_1 = g_2$ folgt. Ein Morphismus $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ heißt Epimorphismus, wenn für alle Objekte $C$ und $g_1, g_2 \in \mathrm{Mor}_{\mathcal{C}}(B, C)$ aus $g_1 \circ f = g_2 \circ f$ bereits $g_1 = g_2$ folgt.

Seien $\mathcal{C}, \mathcal{D}$ Kategorien. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ ordnet jedem Objekt $A \in \mathrm{Obj}(\mathcal{C})$ genau ein Objekt $F(A) \in \mathrm{Obj}(\mathcal{D})$ und jedem Morphismus $f \in \mathrm{Mor}(\mathcal{C})$ genau einen Morphismus $F(f) \in \mathrm{Mor}(\mathcal{C})$ zu, so daß folgendes gilt: Für $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ gilt $F(f) \in \mathrm{Mor}_{\mathcal{D}}(F(A), F(B))$, außerdem $F(g \circ f) = F(g) \circ F(f)$ für beliebige Morphismen $f, g \in \mathrm{Mor}(\mathcal{C})$ mit passendem Definitions- und Wertebereichen und $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ für alle Objekte $A \in \mathrm{Obj}(\mathcal{C})$. Speziell nennt man $F$ auch einen kovarianten Funktor. Einen kontravarianten Funktor erhalten wir, wenn $F(f) \in \mathrm{Mor}_{\mathcal{D}}(F(B), F(A))$ statt $F(f) \in \mathrm{Mor}_{\mathcal{D}}(F(A), F(B))$ und die entsprechenden Anpassungen gelten (wenn $F$ also die „Pfeilrichtung“ umkehrt). Den identischen Funktor auf $\mathcal{C}$ bezeichen wir mit $\mathrm{id}_{\mathcal{C}}$. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heißt voll bzw. treu, wenn $F : \mathrm{Mor}_{\mathcal{C}}(A, B) \to \mathrm{Mor}_{\mathcal{C}}(F(A), F(B))$ surjektiv bzw. injektiv ist.

Ist $\mathcal{C}$ eine Kategorie, so erhalten wir eine neue Kategorie $\mathcal{C}^{\mathrm{op}}$, die zu $\mathcal{C}$ duale Kategorie, indem wir „alle Pfeile“ umdrehen. Wir notieren einen Morphismus $f : A \to B$ dann einfach formal als $f^{\mathrm{op}} : B \to A$, ansonsten bleibt alles beim alten. Ein Funktor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ ist dann im wesentlichen nichts anderes als ein kontravarianter Funktor von $\mathcal{C}$ nach $\mathcal{D}$. Es gilt $(\mathcal{C}^{\mathrm{op}})^{\mathrm{op}} = \mathcal{C}$. Ein Beispiel für einen kontravarianten Funktor ist die Fixgruppenabbildung aus der Galoistheorie.

Eine natürliche Transformation $\phi : F \to G$ zweier Funktoren $F, G : \mathcal{C} \to \mathcal{D}$ besteht aus den folgenden Daten: Für jedes $A \in \mathrm{Obj}(\mathcal{C})$ ist $\phi_A : F(A) \to G(A)$ ein Morphismus in $\mathcal{D}$ mit der Eigenschaft, daß für jeden Morphismus $f : A \to B$ in $\mathcal{C}$ die Gleichung $G(f) \circ \phi_A = \phi_B \circ F(f)$ gilt (man zeichne das zugehörige, kommutative Diagramm). Speziell ist beispielsweise die identische natürliche Transformation $\phi = \mathrm{id}_F$ durch $\phi_A = \mathrm{id}_{F(A)}$ gegeben.

Eine natürliche Äquivalenz besteht aus zwei natürlichen Transformationen $\phi : F \to G$ und $\psi : G \to F$ mit $\phi \circ \psi = \mathrm{id}_G$ und $\psi \circ \phi = \mathrm{id}_F$. Wir schreiben dann $F \cong G$. Zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$ heißen äquivalent, wenn es Funktoren $F : \mathcal{C} \to \mathcal{D}$ und $G : \mathcal{D} \to \mathcal{C}$ mit $F \circ G \cong \mathrm{id}_{\mathcal{D}}$ und $G \circ F \cong \mathrm{id}_{\mathcal{C}}$ gibt.

Als Beispiel betrachten wir die Kategorie $\mathcal{C}$ der endlich dimensionalen $k$-Vektorräume ($k$ ein Körper). Die Zuordnung $V \mapsto V^*$ eines Vektorraums $V$ zu seinem Dualraum liefert einen Funktor $F : \mathcal{C}^{\mathrm{op}} \to \mathcal{C}$. In der linearen Algebra wird gezeigt, daß es eine „kanonische“ oder „natürliche“ Isomorphie $V^{**} \cong V$ gibt. Mit der eingeführten Terminologie heißt das genauer, daß es einen Isomorphismus

$\mathrm{id}_{\mathcal{C}} \to F^2$ in $\mathrm{Fun}(\mathcal{C},\mathcal{C})$ gibt. Also liefert $F$ auch eine Äquivalenz von Kategorien.

Das kartesische Produkt $\mathcal{C}\times\mathcal{D}$ zweier Kategorien $\mathcal{C}$ und $\mathcal{D}$ besitzt als Objekte und Morphismen Paare $(A,B)\in \mathrm{Obj}(\mathcal{C})\times\mathrm{Obj}(\mathcal{D})$ und $(f,g)\in \mathrm{Mor}(\mathcal{C})\times\mathrm{Mor}(\mathcal{D})$. Ein Bifunktor der Kategorien $\mathcal{C}$ und $\mathcal{D}$ in eine Kategorie $\mathcal{E}$ ist ein Funktor $\mathcal{C}\times\mathcal{D}\to\mathcal{E}$. Ein Bifunktor verhält sich also in beiden Argumenten funktoriell.

## 6.3 Funktorkategorien und Lemma von Yoneda

Funktoren $F,\, G:\mathcal{C}\to\mathcal{D}$ zweier Kategorien $\mathcal{C}$ und $\mathcal{D}$ und ihre natürlichen Transformationen $\phi : F\to G$ bilden die Objekte und Morphismen einer Kategorie $\mathrm{Fun}(\mathcal{C},\mathcal{D})$, welche die Funktorkategorie von $\mathcal{C}$ und $\mathcal{D}$ genannt wird. Die Eigenschaften einer Kategorie sind hierbei mit den naheliegenden Operationen leicht verifiziert. Eine natürliche Äquivalenz zweier Funktoren $F,G\in\mathrm{Obj}(\mathrm{Fun}(\mathcal{C},\mathcal{D}))$ entspricht also einem Isomorphismus in $\mathrm{Fun}(\mathcal{C},\mathcal{D})$, was mit der Schreibweise $F\cong G$ zusammenpaßt.

Sei $\mathcal{C}$ eine Kategorie und $X\in\mathrm{Obj}(\mathcal{C})$. Mit (Mengen) sei die Kategorie der Mengen und Abbildungen bezeichnet. Zwei besonders interessante Funktoren, genannt Hom-Funktoren, ergeben sich wie folgt. Für $A,B\in\mathrm{Obj}(\mathcal{C})$ sei $h_X(B)=\mathrm{Mor}_{\mathcal{C}}(X,B)$ und $h'_X(A)=\mathrm{Mor}_{\mathcal{C}}(A,X)$. Für $f:A\to B$ sei $h_X(f):h_X(A)\to h_X(B)$ gegeben durch $g\mapsto f\circ g$ und $h'_X(f):h'_X(B)\to h'_X(A)$ gegeben durch $g\mapsto g\circ f$. Man beachte, daß $h'_X$ die Pfeilrichtung umkehrt. Es ist leicht einsichtig, daß $h_X$ ein Funktor von $\mathcal{C}$ nach (Mengen) und $h'_X$ ein Funktor von $\mathcal{C}^{\mathrm{op}}$ nach (Mengen) ist. Wir schreiben manchmal $h_X=\mathrm{Mor}_{\mathcal{C}}(X,\cdot)$ und $h'_X=\mathrm{Mor}_{\mathcal{C}}(\cdot,X)$.

Die injektive Zuordnung $X\mapsto h_X$ liefert einen Funktor $h:\mathcal{C}^{\mathrm{op}}\to\mathrm{Fun}(\mathcal{C},$ (Mengen)). Die Beziehung von $\mathrm{Mor}_{\mathcal{C}}(Y,X)$ und $\mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathrm{Mengen}))}(h_X,h_Y)$ ist Inhalt des folgenden Lemmas, Aussage $(ii)$.

**6.1 Lemma** (Yoneda)**.** *Sei $\mathcal{C}$ eine Kategorie.*

$(i)$ *Für $X\in\mathrm{Obj}(\mathcal{C})$ und $F\in\mathrm{Fun}(\mathcal{C},(\mathit{Mengen}))$ gilt*

$$\mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathit{Mengen}))}(h_X,F)\cong F(X)$$

*unter der Abbildung $i:\mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathit{Mengen}))}(h_X,F)\to F(X)$, $\phi\mapsto\phi_X(\mathrm{id}_X)$ und ihrer Inversen $j:F(X)\to\mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathit{Mengen}))}(h_X,F)$, $x\mapsto\phi$ mit $\phi_Y(f)=F(f)(x)$.*

$(ii)$ *Der Funktor $h:\mathcal{C}^{\mathrm{op}}\to\mathrm{Fun}(\mathcal{C},\,(\mathit{Mengen}))$ liefert eine Äquivalenz von $\mathcal{C}^{\mathrm{op}}$ mit einer vollen Unterkategorie von $\mathrm{Fun}(\mathcal{C},(\mathit{Mengen}))$.*

*Beweis.* $(i)$: Für $\phi \in \mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathrm{Mengen}))}(h_X, F)$ ist $\phi_X : h_X(X) \to F(X)$. Da $\mathrm{id}_X \in h_X(X) = \mathrm{Mor}_{\mathcal{C}}(X, X)$, gilt $\phi_X(\mathrm{id}_X) \in F(X)$ und die Abbildung $i$ ist wohldefiniert.

Für $x \in F(X)$, $Y \in \mathrm{Obj}(\mathcal{C})$ und $f \in h_X(Y) = \mathrm{Mor}_{\mathcal{C}}(X, Y)$ ist $\phi_Y : h_X(Y) \to F(Y)$ mit $\phi_Y(f) = F(f)(x) \in F(Y)$ eine wohldefinierte Abbildung. Haben wir $g : Y \to Z$, so gilt

$$\begin{aligned}(F(g) \circ \phi_Y)(f) &= F(g)(\phi_Y(f)) = F(g)(F(f)(x)) = (F(g) \circ F(f))(x) \\ &= F(g \circ f)(x) = \phi_Z(g \circ f) = \phi_Z(h_X(g)(f)) = (\phi_Z \circ h_X(g))(f).\end{aligned}$$

Daraus folgt $F(g) \circ \phi_Y = \phi_Z \circ h_X(g)$ und $\phi \in \mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathrm{Mengen}))}(h_X, F)$. Also ist $j$ wohldefiniert.

Sei $\phi \in \mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\mathrm{Mengen}))}(h_X, F)$ und $x = \phi_X(\mathrm{id}_X)$. Mit $f \in h_X(Y)$ ergibt sich

$$\begin{aligned}j(i(\phi))_Y(f) &= F(f)(x) = F(f)(\phi_X(\mathrm{id}_X)) = (F(f) \circ \phi_X)(\mathrm{id}_X) \\ &= (\phi_Y \circ h_X(f))(\mathrm{id}_X) = \phi_Y(h_X(f)(\mathrm{id}_X)) = \phi_Y(f \circ \mathrm{id}_X) = \phi_Y(f),\end{aligned}$$

also $j \circ i = \mathrm{id}$, da $Y$ und $f$ beliebig waren. Sei $x \in F(X)$ und $\phi = j(x)$. Dann ergibt sich

$$i(j(x)) = i(\phi) = \phi_X(\mathrm{id}_X) = F(\mathrm{id}_X)(x) = x,$$

also $i \circ j = \mathrm{id}$, da $x$ beliebig war. Damit sind $i$ und $j$ zueinander inverse, bijektive Abbildungen, was zu zeigen war.

$(ii)$: $h$ ist ein Funktor mit injektiver Zuordnung $X \mapsto h_X$. Die Aussage folgt damit aus $(i)$ angewendet für den Fall $F = h_Y$ für $Y \in \mathrm{Obj}(\mathcal{C})$. □

Nach $(ii)$ können wir Objekte $X$ aus $\mathcal{C}$ also auch durch Funktorobjekte $h_X$ und Morphismen $f$ aus $\mathcal{C}$ durch natürliche Transformationen $h_X(f)$ in der unter Umständen größeren Kategorie $\mathrm{Fun}(\mathcal{C}, (\mathrm{Mengen}))$ ohne Informationsverlust darstellen. Dies bringt manchmal Vorteile mit sich (siehe Beispiel unten).

Ein Funktor $F \in \mathrm{Obj}(\mathrm{Fun}(\mathcal{C}, (\mathrm{Mengen})))$ heißt darstellbar, wenn es ein $X \in \mathrm{Obj}(\mathcal{C})$ und eine Isomorphie $F \cong h_X$ gibt. Das Objekt $X$ ist dann bis auf Isomorphie eindeutig bestimmt. Denn ist $f : h_X \to h_Y$ ein Isomorphismus, so ist auch $h^{-1}(f) : X \to Y$ aufgrund der Funktoreigenschaft von $h$ und der Bijektion in Lemma 6.1, $(i)$ ein Isomorphismus.

**6.2 Beispiel.** Um ein Beispiel zu geben sei $\mathcal{C}$ eine additive Kategorie (Morphismen können addiert werden, siehe Abschnitt unten) mit genau einem Objekt $X$. Die Axiome einer additiven Kategorie machen $\mathrm{Mor}_{\mathcal{C}}(X, X)$ mit $+$ und $\circ$ zu einem Ring $R$ mit 1. Ist umgekehrt $R$ ein Ring mit 1, so ist die Kategorie $\mathcal{C}$, welche als einziges Objekt die Menge $X = R$ und als Morphismen die Multiplikationen

$m_a : R \to R$, $x \mapsto ax$ mit $a \in R$ besitzt, aufgrund der Ringaxiome eine additive Kategorie. Ferner sind diese beiden Konstruktionen invers zueinander.

Für eine additive Kategorie sind $h_X$ und $F$ additive Funktoren ($F$ wird so gewählt, also sind die Funktoren verträglich mit der Addition von Morphismen), so daß das Lemma 6.1 mit der Kategorie (Abelsche Gruppen) statt (Mengen) richtig bleibt. Wir können $X$ bzw. $R = \mathrm{Mor}_{\mathcal{C}}(X, X)$ dann auch als $h_X$ bzw. $\mathrm{Mor}_{\mathrm{Fun}(\mathcal{C},(\text{Abelsche Gruppen}))}(h_X, h_X) \cong R$ in $\mathrm{Fun}(\mathcal{C}, (\text{Abelsche Gruppen}))$ darstellen. Aber worum handelt es sich bei $\mathrm{Fun}(\mathcal{C}, (\text{Abelsche Gruppen}))$? Jedes $F \in \mathrm{Fun}(\mathcal{C}, (\text{Abelsche Gruppen}))$ ist bereits durch die abelsche Gruppe $F(X)$ eindeutig bestimmt, da $\mathcal{C}$ nur das Objekt $X$ besitzt. Wegen der Additivität und Funktoreigenschaft von $F$ bekommen wir einen Ringhomomorphismus $F : R = \mathrm{Mor}_{\mathcal{C}}(X, X) \to \mathrm{Mor}_{(\text{Abelsche Gruppen})}(F(X), F(X))$, so daß $F(X)$ zu einem $R$-Modul wird. Jedes $F$ definiert also einen $R$-Modul $F(X)$, und damit ist die Kategorie $\mathrm{Fun}(\mathcal{C}, (\text{Abelsche Gruppen}))$ die Kategorie der $R$-Moduln.

Das Lemma von Yoneda reduziert sich in dieser Situation zu der Aussage $M \cong \mathrm{Hom}_R(R, M)$ über koinduzierte Moduln (vgl. Satz 4.8).

Wenn wir in $\mathcal{C}$ mehrere Objekte betrachten, erhalten wir eine Verallgemeinerung des Ringbegriffs, und $\mathrm{Fun}(\mathcal{C}, (\text{Abelsche Gruppen}))$ liefert dann eine Verallgemeinerung des Modulbegriffs. Mit der Methode des Beispiels kann man allgemein eine additive Kategorie in eine abelsche Kategorie einbetten.

Die obigen (kovarianten) Aussagen über $h_X$ besitzen analoge (kontravariante) Aussagen für $h'_X$ (die wir hier der Klarheit halber angeben, obwohl das eigentlich aus Symmetriegründen überflüssig ist).

**6.3 Lemma** (Yoneda'). *Sei $\mathcal{C}$ eine Kategorie.*

(*i*) *Für $X \in \mathrm{Obj}(\mathcal{C})$ und $F \in \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, (\textit{Mengen}))$ gilt*

$$\mathrm{Mor}_{\mathrm{Fun}(\mathcal{C}^{\mathrm{op}},(\textit{Mengen}))}(h'_X, F) \cong F(X)$$

*unter der Abbildung $i : \mathrm{Mor}_{\mathrm{Fun}(\mathcal{C}^{\mathrm{op}},(\textit{Mengen}))}(h'_X, F) \to F(X)$, $\phi \mapsto \phi_X(\mathrm{id}_X)$ und ihrer Inversen $j : F(X) \to \mathrm{Mor}_{\mathrm{Fun}(\mathcal{C}^{\mathrm{op}},(\textit{Mengen}))}(h'_X, F)$, $x \mapsto \phi$ mit $\phi_Y(f) = F(f)(x)$.*

(*ii*) *Der Funktor $h : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, (\textit{Mengen}))$ liefert eine Äquivalenz von $\mathcal{C}$ mit einer vollen Unterkategorie von $\mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, (\textit{Mengen}))$ .*

*Beweis.* Folgt direkt aus Lemma 6.1, wenn wir Lemma 6.1 mit $\mathcal{D} = \mathcal{C}^{\mathrm{op}}$ anwenden und beachten, daß $h'_X$ in $\mathcal{C}$ der gleiche Funktor wie $h_X$ in $\mathcal{D}$ ist (wir identifizieren $X$ in $\mathrm{Obj}(\mathcal{C})$ und in $\mathrm{Obj}(\mathcal{D})$). □

Ein kontravarianter Funktor $F : \mathcal{C} \to$ (Mengen) heißt darstellbar, wenn es ein $X \in \mathrm{Obj}(\mathcal{C})$ mit $F \cong h'_X$ gibt (das haben wir genau genommen noch nicht definiert). Das Objekt $X$ ist dann wieder bis auf Isomorphie eindeutig bestimmt.

Die Zuordnung $\mathrm{op} : \mathcal{C} \to \mathcal{C}^{\mathrm{op}}$ liefert im übrigen einen kontravarianten Funktor, welcher die Objekte und Morphismen bijektiv abbildet. Daher entsprechen die kontravarianten Funktoren von $\mathcal{C}$ nach $\mathcal{D}$ eineindeutig den (kovarianten) Funktoren $\mathcal{C}^{\mathrm{op}}$ nach $\mathcal{D}$. Man kann so in jeder Situation bzw. Aussage „die Pfeile umdrehen“ und eine entsprechende, duale Situation bzw. Aussage erhalten.

## 6.4 Limites und Kolimites

In diesem Abschnitt betrachten wir Limites und Kolimites am Beispiel der Kategorie der $R$-Moduln. Es handelt sich hierbei um allgemeine Formen der Begriffe direktes Produkt und direkte Summe, aber auch Kern und Kokern.

Die kategorielle Definition des direkten Produkts lautet wie folgt: Seien $A_1$,$A_2$, $B$ Moduln und $\pi_i \in \mathrm{Hom}_R(B, A_i)$ (Projektionen). Dann heißt $B$ ein direktes Produkt von $A_1$ und $A_2$, wenn für jeden Modul $C$ und $g_i \in \mathrm{Hom}_R(C, A_i)$ genau ein $f \in \mathrm{Hom}_R(C, B)$ existiert mit $\pi_i \circ f = g_i$. Es ist wieder günstig, sich ein graphisches Bild der Situation zu malen. Ein direktes Produkt ist bis auf Isomorphie eindeutig bestimmt: Ist $B'$ mit $\pi'_i$ ein weiteres direktes Produkt, so gibt es $f \in \mathrm{Hom}_R(B', B)$ und $f' \in \mathrm{Hom}_R(B, B')$ mit $\pi'_i = \pi_i \circ f$ und $\pi_i = \pi'_i \circ f'$, also $\pi'_i = \pi'_i \circ f' \circ f$. Aufgrund der Eindeutigkeitsbedingung für $B$ folgt $f' \circ f = \mathrm{id}_B$. Analog ergibt sich $f \circ f' = \mathrm{id}_{B'}$. Man zeigt nun, daß direkte Produkte existieren (dies muß nicht in jeder Kategorie der Fall sein), und zwar in Form der bekannten Konstruktion $B = A_1 \times A_2$. In der Kategorie der Mengen stimmt das direkte Produkt mit dem Schnitt überein.

Bei der direkten Summe geht man genau andersherum vor. Seien $A_1, A_2, B$ Moduln und $\iota_i \in \mathrm{Hom}_R(A_i, B)$ (Injektionen). Dann heißt $B$ eine direkte Summe von $A_1$ und $A_2$, wenn für jeden Modul $C$ und $g_i \in \mathrm{Hom}_R(A_i, C)$ genau ein $f \in \mathrm{Hom}_R(B, C)$ existiert mit $f \circ \iota_i = g_i$. Es ist günstig, sich ein graphisches Bild der Situation zu malen. Eine direkte Summe ist bis auf Isomorphie eindeutig bestimmt: Ist $B'$ mit $\pi'_i$ eine weitere direkte Summe, so gibt es $f \in \mathrm{Hom}_R(B, B')$ und $f' \in \mathrm{Hom}_R(B', B)$ mit $\iota'_i = f \circ \iota_i$ und $\iota_i = f' \circ \iota'_i$, also $f' \circ f \circ \iota_i = \iota_i$. Aufgrund der Eindeutigkeitsbedingung für $B$ folgt $f' \circ f = \mathrm{id}_B$. Analog ergibt sich $f \circ f' = \mathrm{id}_{B'}$. Man zeigt nun, daß direkte Summen existieren (dies muß nicht in jeder Kategorie der Fall sein), und zwar in Form der bekannten Konstruktion $B = A_1 \oplus A_2$. In der Kategorie der Mengen stimmt die direkte Summe mit der disjunkten Vereinigung überein.

Die Definition wird üblicherweise auf beliebige Familien von Moduln $A_i$ ver-

allgemeinert. Notationsweise schreibt man $\prod_i A_i$ für das direkte Produkt und $\coprod_i A_i$ für die direkte Summe, weil die direkte Summe das „umgekehrte“ direkte Produkt ist. Direkte Summen werden daher auch Koprodukte genannt. Dahinter steckt ein allgemeines Prinzip der Kategorientheorie, daß man durch Umkehrung der Morphismen (Pfeile) zu dualen Definitionen und Sätzen gelangt. Solche dualen Konstruktionen werden mit dem Präfix „Ko“ versehen.

Produkte und Koprodukte sind noch nicht die allgemeinste Definition, die man treffen kann. Zum Beispiel kann man beim Produkt zu $A_1, A_2$ noch einen Modul $A_3$ und Morphismen $h_i \in \mathrm{Hom}_R(A_i, A_3)$ für $i \in \{1, 2\}$ betrachten. Man definiert das Faserprodukt als Modul $B$ zusammen mit $\pi_j \in \mathrm{Hom}_R(B, A_j)$, so daß für jeden Modul $C$ und Abbildungen $g_j \in \mathrm{Hom}_R(C, A_j)$ für $j \in \{1, 2, 3\}$ mit $g_3 = h_i \circ g_i$ für $i \in \{1, 2\}$ ein eindeutig bestimmter Morphismus $f \in \mathrm{Hom}_R(C, B)$ mit $g_j = \pi_j \circ f$ für $j \in \{1, 2, 3\}$ existiert. Entsprechend wird Fasersumme bzw. Faserkoprodukt definiert.

Allgemein betrachtet man ganze Diagramme von $A_i$ und Morphismen zwischen den $A_i$. Unter einem Diagramm $\mathcal{A}$ von $R$-Moduln versteht man einfach eine Teilkategorie der Kategorie der $R$-Moduln. Unter einem Morphismus $g$ von $B$ nach $\mathcal{A}$ verstehen wir eine Sammlung von Morphismen $g_i \in \mathrm{Hom}_R(B, A_i)$ von $B$ zu den $A_i$ in $\mathcal{A}$, so daß folgendes gilt. Für alle Objekte $A_i$, $A_j$ und Morphismen $h \in \mathrm{Hom}_R(A_i, A_j)$ in $\mathcal{A}$ gelte $g_j = h \circ g_i$. Analog wird ein Morphismus von $\mathcal{A}$ nach $B$ definiert. Für einen Funktor $F$ ist $F(\mathcal{A})$ wieder ein Diagramm.

**6.4 Definition.** Der Limes des Diagramms $\mathcal{A}$ ist ein $R$-Modul $B$ zusammen mit einem Morphismus $\pi$ von $B$ nach $\mathcal{A}$ derart, daß es für jeden $R$-Modul $C$ und Morphismus $g$ von $C$ nach $\mathcal{A}$ genau ein $f \in \mathrm{Hom}_R(C, B)$ mit $g = \pi \circ f$ gibt. Man schreibt $B = \varprojlim \mathcal{A}$.

Der Kolimes des Diagramms $\mathcal{A}$ ist ein $R$-Modul $B$ zusammen mit einem Morphismus $\iota$ von $\mathcal{A}$ nach $B$ derart, daß es für jeden $R$-Modul $C$ und Morphismus $g$ von $\mathcal{A}$ nach $C$ genau ein $f \in \mathrm{Hom}_R(B, C)$ mit $g = f \circ \iota$ gibt. Man schreibt $B = \varinjlim \mathcal{A}$.

Andere Namen für Limes und Kolimes sind projektiver Limes und induktiver Limes, oder inverser und direkter Limes. Wir nennen die $\pi$ Projektionen und die $\iota_i$ Injektionen (die Projektionen müssen aber nicht unbedingt surjektiv und die Injektionen injektiv sein).

**6.5 Satz.** *Limes und Kolimes von Diagrammen existieren in der Kategorie der $R$-Moduln und sind bis auf Isomorphie eindeutig bestimmt.*

*Beweis.* Die Eindeutigkeit folgt wie bei direkten Produkten und Koprodukten. Für die Existenz des Limes gehen wir wie folgt vor. Wir bilden das direkte Produkt

$\prod_i A_i$ der Objekte im Diagramm $\mathcal{A}$ mit der Projektion $\pi' : \prod_i A_i \to \mathcal{A}'$, wobei $\mathcal{A}'$ das Diagramm ist, welches nur aus den $A_i$ und keinen Morphismen besteht. Ist $g : C \to \mathcal{A}$, so gibt es ein $f' \in \mathrm{Hom}_R(C, \prod_i A_i)$ mit $g = \pi' \circ f'$. Für $h \in \mathrm{Hom}_R(A_i, A_j)$ gilt $g_j(x) = h(g_i(x))$ für alle $x \in C$. Sei $B = \{(z_i)_i \in \prod_i A_i \,|\, h(z_i) = z_j \text{ für alle } h \in \mathrm{Hom}_R(A_i, A_j) \text{ in } \mathcal{A} \text{ und alle } i, j\}$. Das Bild von $C$ in $\prod_i A_i$ ist also in $B$ enthalten. Die Projektion $\pi$ wird durch Einschränkung von $\pi'$ auf $B$ definiert. Wegen der Bedingungen für $B$ gilt $\pi : B \to \mathcal{A}$. Dies zeigt, daß $B = \varprojlim \mathcal{A}$ ist.

Für die Existenz des Kolimes gehen wir wie folgt vor. Wir bilden die direkte Summe $\coprod_i A_i$ der Objekte im Diagramm $\mathcal{A}$ mit der Injektion $\iota' : \mathcal{A}' \to \coprod_i A_i$, wobei $\mathcal{A}'$ wieder das Diagramm ist, welches nur aus den $A_i$ und keinen Morphismen besteht. Ist $g : \mathcal{A} \to C$, so gibt es ein $f' \in \mathrm{Hom}_R(\coprod_i A_i, C)$ mit $g = f' \circ \iota'$. Für $h \in \mathrm{Hom}_R(A_i, A_j)$ gilt $g_j(h(x)) = g_i(x)$ für alle $x \in C$. Was die Werte von $g$ und $f'$ angeht, braucht man also nicht zwischen $x$ und $h(x)$ zu unterscheiden. In $\coprod_i A_i$ definieren wir $U$ als den durch $\{\iota'_j(h(x)) - \iota'_i(x) \,|\, x \in A_i, h \in \mathrm{Hom}_R(A_i, A_j) \text{ in } \mathcal{A} \text{ und alle } i, j\}$ erzeugten Untermodul. Dann ist $U$ im Kern von $f'$ enthalten. Sei $B = \coprod_i A_i / U$. Die Injektion $\iota$ wird durch $\iota'$ gefolgt vom Restklassenhomomorphismus $\coprod_i A_i \to B$ definiert. Wegen der Bedingungen für $B$ gilt $\iota : \mathcal{A} \to B$. Dies zeigt, daß $B = \varinjlim \mathcal{A}$ ist. □

Sei $p$ eine Primzahl. Als Beispiel betrachten wir das Diagramm $\mathcal{A}$ mit $A_i = \mathbb{Z}/p^i\mathbb{Z}$ und den Abbildungen $h_{i,j} : A_i \to A_j$, $x \bmod p^i \mapsto x \bmod p^j$ für $i \geq j$. Die Elemente von $\mathbb{Z}_p = \varprojlim \mathcal{A}$ sind „Zahlen“, die modulo beliebig hoher Primpotenzen bestimmt sind (zu vergleichen mit $\mathbb{R}$, dessen Zahlen in Dezimalentwicklung modulo beliebig hoher Potenzen von $10^{-1}$ definiert sind). Man kann den Limes statt für Moduln auch für Ringe bilden. Mengenmäßig bleibt $\mathbb{Z}_p$ gleich, wird aber zum Ring und heißt Ring der $p$-adischen ganzen Zahlen.

## 6.5 Universelle Konstruktionen und adjungierte Funktoren

Noch einzugeben.

## 6.6 Exaktheit

Noch einzugeben.