Ringtheorie

Vorlesung von
Prof. Dr. B. Külshammer

WiSe1998/99

Ausarbeitung:
Jan Pluntke

Inhaltsverzeichnis

1 Ringe und Teilringe

1.1. Definition. Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+$, $\cdot$, die folgende Bedingungen erfüllen:

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

(ii) $\cdot$ ist assoziativ.

(iii) Es existiert ein neutrales Element bezüglich $\cdot$.

(iv) Für alle $a, b, c \in R$ gilt das **Distributivgesetz**

$$a(b+c) = ab + ac\ , \quad (a+b)c = ac + bc\ .$$

Bemerkungen. Das neutrale Element bezüglich $+$ bezeichnet man mit 0 (**Nullelement**), das neutrale Element bezüglich $\cdot$ mit 1 (**Einselement**). Bekanntlich sind beide eindeutig bestimmt. Man beachte, daß in manchen Büchern die Existenz eines Einselementes nicht verlangt wird. Statt $a + (-b)$ schreibt man oft $a - b$. Um Klammern zu sparen, rechnet man nach der Regel: Punktrechnung geht vor Strichrechnung. Für beliebige Elemente x, y eines Ringes R gilt stets:

$$0 \cdot x = 0\ , \quad (-x)y = -(xy) = x(-y)\ , \quad (-x)(-y) = xy\ .$$

Die Beweise führt man wie bei Körpern.

Beispiele.

(a) Bekannte Ringe sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) $\{0\}$ ist ein Ring mit $+$, $\cdot$; Einselement und Nullelement stimmen überein.

(c) Für jede Menge M ist die Potenzmenge $\mathfrak{P}(M)$ ein Ring, wenn man die Verknüpfungen folgendermaßen definiert:

$$A + B = (A \setminus B) \cup (B \setminus A)\ , \quad A \cdot B = A \cap B\ .$$

Nullelement ist $\emptyset$, Einselement ist M. Man nennt $\mathfrak{P}(M)$ den **Potenzmengenring** von M.

(d) Ist R ein Ring mit den Verknüpfungen $+$, $\cdot$, so auch mit den Verknüpfungen $+$, $\circ$, wobei man $a \circ b = ba$ setzt. Den so entstehenden Ring bezeichnet man mit R°, er heißt der R **entgegengesetzte Ring** (**opposite ring**).

(e) Für $n \in \mathbb{N}$ und jeden Ring R ist die Menge $\mathrm{Mat}(n, R)$ aller $n \times n$-Matrizen mit Koeffizienten in R ein Ring bezüglich der üblichen Addition und Multiplikation von Matrizen. Man nennt $\mathrm{Mat}(n, R)$ den **vollen Matrixring des Grades n über R.**

(f) Für jede Familie $(R_i)_{i \in I}$ von Ringen R_i ist auch das **direkte Produkt**

$$\bigtimes_{i \in I} R_i = \prod_{i \in I} R_i = \{(r_i)_{i \in I} : r_i \in R_i \text{ für } i \in I\}$$

ein Ring, wenn man komponentenweise rechnet:

$$(r_i)_{i \in I} \dotplus (s_i)_{i \in I} = (r_i \dotplus s_i)_{i \in I}\ .$$

Im Fall $R_i = R$ für alle $i \in I$ erhält man also den Ring

$$\bigtimes_{i\in I} R_i = \mathrm{Abb}(I, R)$$

aller Funktionen von I nach R, und im Fall $I = \{1, \dots, n\}$ für ein $n \in \mathbb{N}$ erhält man den Ring

$$\bigtimes_{i\in I} R_i = R_1 \times R_2 \times \cdots \times R_n = \{(r_1, \dots, r_n) : r_i \in R_i, i \in I\} \ .$$

(g) Ein **Monoid** ist eine Menge M mit einer assoziativen Verknüpfung $\cdot$ und einem neutralen Element 1_M. Für ein Monoid M und einen Ring R definiert man den **Monoidring** RM folgendermaßen:

Die Elemente von RM sind die Familien $(r_m)_{m\in M}$ von Elementen $r_m \in R$ mit

$$|\{m \in M : r_m \neq 0\}| < \infty \ .$$

Die Verknüpfungen in RM werden folgendermaßen definiert:

$$(r_m)_{m\in M} + (s_m)_{m\in M} := (r_m + s_m)_{m\in M} \ ,$$

$$(r_m)_{m\in M} \cdot (s_m)_{m\in M} := \Big(\sum_{\substack{p,q\in M\\ pq=m}} r_p s_q\Big)_{m\in M} \ .$$

Man beachte, daß die obige Summe jeweils endlich ist. Für $m \in M$ sei $\widehat{m} \in RM$ das Element, das 1 an der Stelle m und sonst lauter Nullen enthält. Dann ist $\widehat{1_M}$ das Einselement von RM. Für $r \in R$ und $(r_m)_{m\in M} \in RM$ setzt man

$$r \cdot (r_m)_{m\in M} := (r \cdot r_m)_{m\in M} \ .$$

Dann ist $(r_m)_{m\in M} = \sum_{m\in M} r_m \cdot \widehat{m}$, wobei die Summe auf der rechten Seite nur endlich viele von Null verschiedene Summanden enthält. Für $m, n \in M$ gilt: $\widehat{m}\widehat{n} = \widehat{mn}$. Man schreibt daher auch wieder m statt $\widehat{m}$. Die Elemente in RM haben also die Form $\sum_{m\in M} r_m m$, wobei nur endlich viele r_m von Null verschieden sind. Dabei gilt:

$$\sum_{m\in M} r_m m = \sum_{m\in M} s_m m \Longleftrightarrow r_m = s_m \text{ für alle } m \in M \ .$$

$$\sum_{m\in M} r_m m + \sum_{m\in M} s_m m = \sum_{m\in M} (r_m + s_m) m \ ,$$

$$\Big(\sum_{m\in M} r_m m\Big)\Big(\sum_{m\in M} s_m m\Big) = \sum_{m\in M} \Big(\sum_{\substack{p,q\in M\\ pq=m}} r_p s_q\Big) m \ .$$

Ist M eine Gruppe, so nennt man RM auch den **Gruppenring** von M über R.

1.2. Definition. Ein Ring R heißt **kommutativ**, falls $ab = ba$ für alle $a, b \in R$ ist.

Bemerkung. In dieser Vorlesung werden wir uns hauptsächlich mit nichtkommutativen Ringen beschäftigen.

1.3. Definition. Ein Element a eines Rings R heißt **rechtsinvertierbar** (**linksinvertierbar**), falls ein Element $b \in R$ mit $ab = 1$ ($ba = 1$) existiert. Gegebenenfalls nennt man b ein **rechtsinverses** (**linksinverses**) Element zu a. Ist a rechtsinvertierbar und linksinvertierbar, so heißt a **invertierbar** oder **Einheit** (**unit**).

Bemerkung. Es ist leicht zu sehen, daß die Einheiten in R eine Gruppe bezüglich $\cdot$ bilden. Man nennt diese Gruppe die **Einheitengruppe von** R und schreibt dafür $R^\times$ oder $U(R)$. Ist $U(R) = R \setminus \{0\}$, so nennt man R einen **Schiefkörper**. Kommutative Schiefkörper bezeichnet man auch als **Körper**.

Beispiel. Für $n \in \mathbb{N}$ bilden die invertierbaren $n \times n$-Matrizen die Einheitengruppe von $\mathrm{Mat}(n, R)$. Diese bezeichnet man als **allgemeine lineare Gruppe des Grades** n **über** R. Man schreibt dafür $\mathrm{GL}(n, R)$.

1.4. Definition. Ein Element a eines Rings R heißt **Linksnullteiler** (**Rechtsnullteiler**), falls ein Element $b \in R \setminus \{0\}$ existiert mit $ab = 0$ ($ba = 0$). Man nennt a einen **Nullteiler** in R, falls a Links- oder Rechtsnullteiler ist.

Beispiele.

(i) Wegen

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

sind $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ Nullteiler in $\mathrm{Mat}(2, \mathbb{R})$.

(ii) Außer im Fall $R = 0$ ist 0 stets Nullteiler in R.

Bemerkung. Man nennt einen Ring $R \neq 0$ **nullteilerfrei**, falls 0 der einzige Nullteiler in R ist. Offenbar sind Schiefkörper stets nullteilerfrei. (Die Umkehrung gilt nicht, siehe z.B. $\mathbb{Z}$.) Nullteilerfreie kommutative Ringe nennt man auch **Integritätsbereiche**. Jeder Körper ist Integritätsbereich, ebenso $\mathbb{Z}$.

1.5. Definition. Ein Element a eines Rings R nennt man **idempotent** (**nilpotent**), falls $a^2 = a$ ($a^n = 0$ für ein $n \in \mathbb{N}$) ist.

Bemerkungen.

(i) Ist $a \in R$ idempotent, so auch $1 - a$:

$$(1-a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - a\ .$$

(ii) Ist $a \in R$ nilpotent, so ist $1 - a$ invertierbar; denn aus $a^n = 0$ folgt:

$$(1-a)(1 + a + \ldots + a^{n-1}) = 1 - a^n = 1$$

und analog

$$(1 + a + \ldots + a^{n-1})(1-a) = 1 - a^n = 1\ .$$

1.6. Definition. Eine Teilmenge S eines Rings R nennt man **Teilring** von R, falls S mit den entsprechend eingeschränkten Verknüpfungen ein Ring ist.

Bemerkung. Wir verlangen nicht, daß die Einselemente von R und S übereinstimmen. Ist dies jedoch der Fall, so nennen wir S einen **unitären Teilring** von R. (Viele Bücher lassen nur unitäre Teilringe zu.) Eine Teilmenge S von R ist also genau dann ein unitärer Teilring von R, wenn gilt:

(i) $0, 1 \in S$,

(ii) $a, b \in S \Longrightarrow a - b, a \cdot b \in S$.

Beispiele.

(a) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ ist eine Folge unitärer Teilringe.

(b) Für jeden Ring R ist das **Zentrum** $Z(R) := \{z \in R : zr = rz$ für alle $r \in R\}$ immer ein unitärer Teilring von R. Offenbar ist $Z(R)$ stets kommutativ.

(c) $\{\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right) : a \in \mathbb{R}\}$ ist ein nichtunitärer Teilring von $\mathrm{Mat}(2, \mathbb{R})$.

(d) $\mathbb{R} \times 0$ ist ein nichtunitärer Teilring von $\mathbb{R} \times \mathbb{R}$.

(e) Man rechnet leicht nach, daß

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \quad , \quad a, b \in \mathbb{C} \right\}$$

ein unitärer Teilring von $Mat(2, \mathbb{C})$ ist. Wegen

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}^{-1} = \frac{1}{a\overline{a} + b\overline{b}} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \in \mathbb{H} \quad \text{im Fall } ab \neq 0$$

ist $\mathbb{H}$ ein Schiefkörper. Man nennt die Elemente von $\mathbb{H}$ **Quaternionen** (**Hamilton** 1843).

2 Homomorphismen, Ideale und Restklassen

2.1. Definition. Eine Abbildung $\varphi : R \to S$ zwischen Ringen R, S nennt man **Homomorphismus**, falls $\varphi(a \overset{\cdot}{+} b) = \varphi(a) \overset{\cdot}{+} \varphi(b)$ für alle $a, b \in R$ ist. Wie üblich definiert man **Monomorphismen**, **Epimorphismen**, **Isomorphismen**, **Endomorphismen**, **Automorphismen** und den Isomorphiebegriff $\cong$ für Ringe. Für jeden Homomorphismus $\varphi : R \to S$ nennt man $\mathrm{Ker}(\varphi) := \{a \in R : \varphi(a) = 0\}$ den **Kern** von φ.

Bemerkungen.

(i) Im Gegensatz zu manchen Büchern verlangen wir nicht $\varphi(1_R) = 1_S$. Ist dies jedoch der Fall, so nennt man φ **unitär**. Stets ist $\varphi(0) = 0$. Für einen unitären Homomorphismus $\varphi : R \to S$ und eine Einheit x in R ist $\varphi(x)$ eine Einheit in S und $\varphi(x)^{-1} = \varphi(x^{-1})$.

(ii) Die Komposition von zwei Homomorphismen ist wieder ein Homomorphismus, und die Umkehrabbildung φ^{-1} eines Isomorphismus ist wieder ein Isomorphismus. Stets ist die **Identitätsabbildung** $\mathrm{id}_R : R \to R$, $a \mapsto a$, ein Automorphismus. Daher bilden die Automorphismen von R eine Gruppe bezüglich der Komposition von Abbildungen, die **Automorphismengruppe** $\mathrm{Aut}(R)$ von R.

(iii) Für jeden Homomorphismus von Ringen $\varphi : R \to S$ und jeden Teilring T von R ist das Bild $\varphi(T) = \{\varphi(t) : t \in T\}$ ein Teilring von S, insbesondere ist das **Bild** von φ, $\mathrm{Bld}(\varphi) = \varphi(R)$, ein Teilring von S. Dagegen ist das **Urbild** $\varphi^{-1}(U)$ eines Teilrings U von S im allgemeinen kein Teilring von R (da $\varphi^{-1}(U)$ im allgemeinen kein Einselement enthält).

Beispiele.

(i) Die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$, ist ein Automorphismus von $\mathbb{C}$.

(ii) Für ein Element a eines Rings R und ein $n \in \mathbb{Z}$ definiert man

$$na := \begin{cases} a + \ldots + a \quad (n \text{ Summanden}) & \text{falls } n > 0 \\ 0 & \text{falls } n = 0 \\ -(|n|a) & \text{falls } n < 0\ . \end{cases}$$

Dann ist die Abbildung $\varphi : \mathbb{Z} \to R$, $n \mapsto n \cdot 1$, ein Homomorphismus. Sein Kern ist eine Untergruppe von $(\mathbb{Z}, +)$. Bekanntlich ist jede Untergruppe von $\mathbb{Z}$ von der Form $k\mathbb{Z} = \{k \cdot z : z \in \mathbb{Z}\}$ für ein eindeutig bestimmtes $k \in \mathbb{N}_0$. Man nennt k die **Charakteristik** von R und schreibt $k = \mathrm{char}(R)$. Zum Beispiel haben $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ alle die Charakteristik 0. Der Potenzmengenring aus Beispiel 1.1 (c) hat stets die Charakteristik 2.

2.2. Definition. Eine Teilmenge I eines Rings R nennt man **Ideal** in R, falls gilt:

(i) $(I, +)$ ist eine Untergruppe von $(R, +)$.

(ii) Für alle $r \in R$ und alle $x \in I$ ist $rx \in I$ und $xr \in I$.

Beispiele.

(a) Für jeden Ring R sind 0 und R Ideale in R. Ist $R \neq 0$ und sind 0 und R die einzigen Ideale in R, so nennt man den Ring R **einfach**. Wir werden später beweisen, daß jeder endliche einfache Ring zu einem vollen Matrixring über einem endlichen Körper isomorph ist (und umgekehrt auch).

(b) Enthält ein Ideal I eine Einheit u in R, so ist $r = ru^{-1}u \in I$ für alle $r \in R$, das heißt $R = I$. Insbesondere ist jeder Schiefkörper ein einfacher Ring.

(c) Für jede Familie $(I_j)_{j \in J}$ von Idealen des Rings R ist auch der Durchschnitt $\bigcap_{j \in J} I_j$ ein Ideal in R. Für jede Teilmenge A von R ist also

$$(A) := \bigcap_{\substack{I \text{ Ideal in } R \\ A \subseteq I}} I$$

ein Ideal in R, das von A **erzeugte Ideal**. Man zeigt leicht, daß (A) genau aus den Elementen der Form $\sum_{i=1}^{k} r_i a_i s_i$ mit $a_i \in A$, $r_i, s_i \in R$, $k \in \mathbb{N}_0$ besteht. Im Fall $A = \{a_1, \dots, a_n\}$ schreibt man auch $(a_1, \dots, a_n)$ statt $\big(\{a_1, \dots, a_n\}\big)$.

(d) Jedes Ideal in $\mathbb{Z}$ hat die Form $k\mathbb{Z} = (k)$ für ein eindeutig bestimmtes $k \in \mathbb{N}_0$.

(e) Für Ideale I und J eines Rings R sind auch die Summe

$$I + J := \{x + y : x \in I, y \in J\}$$

und das Produkt

$$IJ := \Big\{\sum_{i=1}^{k} x_i y_i : x_i \in I, y_i \in J, k \in \mathbb{N}_0\Big\}$$

Ideale in R. Dabei gilt:

(i) $I + J = (I \cup J) = J + I$,

(ii) $IJ = \big(\{xy : x \in I, y \in J\}\big) \subseteq I \cap J$,

(iii) $(IJ)K = I(JK)$,

(iv) $I(J + K) = IJ + IK, \quad (I + J)K = IK + JK$.

Bemerkung. Für jedes Ideal I eines Rings R und jedes Element $a \in R$ nennt man

$$a + I := \{a + x : x \in I\}$$

die **Restklasse** von a **modulo** I. Für $b \in R$ gilt dann:

$$a + I = b + I \iff a - b \in I\ .$$

Gegebenfalls schreibt man auch $a \equiv b \pmod{I}$. Die Menge aller Restklassen modulo I bezeichnet man mit $R/I = \{a + I : a \in R\}$. Auf R/I definiert man Verknüpfungen durch

$$(a + I) \dot{+} (b + I) := (a \dot{+} b) + I\ .$$

Man zeigt leicht, daß diese Verknüpfungen wohldefiniert sind und R/I zu einem Ring machen. Man nennt R/I den **Restklassenring** von R modulo I. Nullelement in R/I ist die Restklasse $0 + I = I$, Einselement ist die Restklasse $1 + I$. Die Abbildung $\nu : R \to R/I$,

$a \mapsto a+I$, ist offenbar ein Homomorphismus. Man nennt ν den **kanonischen Epimorphismus** von R nach R/I. Sein Kern ist das Ideal I. Jedes Ideal ist also Kern eines geeigneten Homomorphismus. Umgekehrt ist für jeden Homomorphismus von Ringen $\varphi : R \to S$ der Kern $\mathrm{Ker}(\varphi)$ ein Ideal in R; dies rechnet man schnell nach. Allgemeiner ist für jedes Ideal J in S das Urbild $\varphi^{-1}(J)$ ein Ideal in R. Dagegen ist das Bild $\varphi(I)$ eines Ideals I in R im allgemeinen kein Ideal in S.

Satz (Homomorphiesatz). *Für jeden Homomorphismus von Ringen $\varphi : R \to S$ ist die Abbildung*

$$\Phi : R/\mathrm{Ker}(\varphi) \to \mathrm{Bld}(\varphi)\ , \quad a + \mathrm{Ker}(\varphi) \mapsto \varphi(a)\ ,$$

ein Isomorphismus; insbesondere ist also $R/\mathrm{Ker}(\varphi) \cong \mathrm{Bld}(\varphi)$.

Beweis. Φ ist wohldefiniert und injektiv; denn für $a, b \in R$ gilt:

$$a + \mathrm{Ker}(\varphi) = b + \mathrm{Ker}(\varphi) \iff a - b \in \mathrm{Ker}(\varphi) \iff \varphi(a-b) = 0 \iff \varphi(a) = \varphi(b)\ .$$

Φ ist ein Homomorphismus; denn für alle $a, b \in R$ gilt:

$$\begin{aligned} \Phi\Big(\big(a + \mathrm{Ker}(\varphi)\big) \dotplus \big(b + \mathrm{Ker}(\varphi)\big)\Big) &= \varphi\big((a \dotplus b) + \mathrm{Ker}(\varphi)\big) = \varphi(a \dotplus b) \\ &= \varphi(a) \dotplus \varphi(b) = \Phi\big(a + \mathrm{Ker}(\varphi)\big) \dotplus \Phi\big(b + \mathrm{Ker}(\varphi)\big)\ . \end{aligned}$$

Offenbar ist Φ auch surjektiv.

2.3. Satz (Erster Isomorphiesatz). *Für jeden unitären Teilring S eines Rings R und jedes Ideal I in R ist*

$$S + I := \{s + x : s \in S, x \in I\}$$

ein unitärer Teilring von R, I ein Ideal in $S+I$ und $S \cap I$ ein Ideal in S mit

$$S/S\cap I \cong S+I/I\ .$$

Beweis. Offenbar ist $1 = 1 + 0 \in S + I$, und für $s, t \in S$, $x, y \in I$ gilt:

$$\begin{aligned} (s+x) - (t+y) &= \underbrace{(s-t)}_{\in S} + \underbrace{(x-y)}_{\in I} \in S + I\ , \\ (s+x)(t+y) &= \underbrace{st}_{\in S} + \underbrace{sy + xt + xy}_{\in I} \in S + I\ . \end{aligned}$$

Daher ist $S+I$ ein unitärer Teilring von R. Da I ein Ideal in R ist, ist I auch ein Ideal in $S+I$. Die Einschränkung des kanonischen Epimorphismus $\nu : R \to R/I$, $a \mapsto a+I$, auf S ist ein Homomorphismus $\varphi : S \to R/I$, $a \mapsto a + I$ mit

$$\mathrm{Ker}(\varphi) = S \cap \mathrm{Ker}(\nu) = S \cap I$$

und

$$\mathrm{Bld}(\varphi) = \{a + I : a \in S\} = \{a + x + I : a \in S, x \in I\} = S+I/I\ .$$

Daher ist $S \cap I$ ein Ideal in S, und $S+I/I$ ist ein Teilring von R/I. Aus dem Homomorphiesatz folgt:

$$S/S\cap I = S/\mathrm{Ker}(\varphi) \cong \mathrm{Bld}(\varphi) = S+I/I\ .$$

2.4. Satz (Zweiter Isomorphiesatz). *Für jedes Ideal I eines Rings R ist die Abbildung*

$$J \mapsto {}^{J}/_{I} := \{y + I : y \in J\}$$

eine Bijektion zwischen der Menge der Ideale in R, die I enthalten, und der Menge der Ideale in ${}^{R}/_{I}$. Dabei gilt:

$$\left({}^{R}/_{I}\right)/\left({}^{J}/_{I}\right) \cong {}^{R}/_{J} \, .$$

Beweis. Ist $\nu : R \to {}^{R}/_{I}$, $a \mapsto a + I$, der kanonische Epimorphismus und J ein Ideal in R mit $I \subseteq J$, so ist $\nu(J) = \{a + I : a \in J\} = {}^{J}/_{I}$ ein Ideal in ${}^{R}/_{I}$; denn für $r \in R$ und $y \in J$ ist

$$(r + I)(y + I) = \underbrace{ry}_{\in J} + I \in {}^{J}/_{I}$$

und analog $(y + I)(r + I) \in {}^{J}/_{I}$. Für jedes Ideal K in ${}^{R}/_{I}$ ist

$$J := \nu^{-1}(K) = \{a \in K : a + I \in K\}$$

ein Ideal in R mit $I = \mathrm{Ker}(\nu) = \nu^{-1}(0) \subseteq \nu^{-1}(K) = J$. Wegen der Surjektivität von ν ist $\nu(J) = \nu\big(\nu^{-1}(K)\big) = K$. Für jedes Ideal J von R mit $I \subseteq J$ ist umgekehrt

$$\nu^{-1}\left({}^{J}/_{I}\right) = \nu^{-1}\big(\nu(J)\big) = J + \mathrm{Ker}(\nu) = J + I = J \, ,$$

wie man leicht nachrechnet. Daher ist die angegebene Abbildung tatsächlich bijektiv.
Man betrachte die kanonischen Epimorphismen

$$\nu : R \to {}^{R}/_{I} \, , \quad r \mapsto r + I$$

und

$$\mu : {}^{R}/_{I} \to \left({}^{R}/_{I}\right)/\left({}^{J}/_{I}\right) .$$

Die Verknüpfung $\mu \circ \nu : R \to \left({}^{R}/_{I}\right)/\left({}^{J}/_{I}\right)$ ist ein Epimorphismus und

$$\begin{aligned} \mathrm{Ker}(\mu \circ \nu) &= \big\{a \in R : \mu\big(\nu(a)\big) = 0\big\} = \big\{a \in R : \nu(a) \in \mathrm{Ker}(\mu)\big\} \\ &= \nu^{-1}\big(\mathrm{Ker}(\mu)\big) = \nu^{-1}\left({}^{J}/_{I}\right) = J \, . \end{aligned}$$

Der Homomorphiesatz liefert also ${}^{R}/_{J} \cong \left({}^{R}/_{I}\right)/\left({}^{J}/_{I}\right)$.

2.5. Satz (Chinesischer Restsatz). *Für Ideale $I_1, \ldots, I_n$ in einem Ring R ist die Abbildung*

$$\varphi : R \to {}^{R}/_{I_1} \times \cdots \times {}^{R}/_{I_n} \, , \quad r \mapsto (r + I_1, \ldots r + I_n) \, ,$$

ein Homomorphismus mit $\mathrm{Ker}(\varphi) = I_1 \cap \cdots \cap I_n$; insbesondere ist ${}^{R}/_{I_1 \cap \cdots \cap I_n}$ zu einem Teilring von ${}^{R}/_{I_1} \times \cdots \times {}^{R}/_{I_n}$ isomorph. Ist jeweils $I_i + I_j = R$ für alle $i \neq j$, so ist φ surjektiv und

$$I_1 \cap \cdots \cap I_n = \sum_{g \in \mathrm{Sym}(n)} I_{g(1)} \cdots I_{g(n)}$$

$$(\mathrm{Sym}(n) = \text{ Gruppe der Permutationen von } \{1, \ldots, n\})$$

Insbesondere ist also ${}^{R}/_{I_1 \cap \cdots \cap I_n} \cong {}^{R}/_{I_1} \times \cdots \times {}^{R}/_{I_n}$.

Bemerkung. Ist also R kommutativ, so ist gegebenenfalls $I_1 \cap \dots \cap I_n = I_1 I_2 \cdots I_n$.

Beweis. Offenbar ist φ ein Homomorphismus und $\mathrm{Ker}(\varphi) = I_1 \cap \dots \cap I_n$. Nach dem Homomorphiesatz ist also

$$R/_{I_1 \cap \dots \cap I_n} \cong \mathrm{Bld}(\varphi) \subseteq R/_{I_1} \times \dots \times R/_{I_n} .$$

Sei also $I_i + I_j = R$ für alle $i \neq j$. Wir schreiben $1 = a_{ij} + b_{ij}$ mit $a_{ij} \in I_i$, $b_{ij} \in I_j$ für $i \neq j$. Dann ist $s_j = \prod_{k \neq j} a_{kj} \in I_i$ für $i \neq j$ und

$$s_j + I_j = \prod_{k \neq j} (1 - \underbrace{b_{kj}}_{\in I_j}) + I_j = 1 + I_j .$$

Für Elemente $r_1, \dots, r_n \in R$ und $r := r_1 s_1 + \dots + r_n s_n$ gilt also

$$r + I_i = \sum_{j=1}^{n} r_j s_j + I_i = r_i s_i + I_i = r_i + I_i \qquad (i = 1, \dots, n) ,$$

d.h. $\varphi(r) = (r_1 + I_1, \dots, r_n + I_n)$. Daher ist φ surjektiv und

$$R/_{I_1 \cap \dots \cap I_n} \cong R/_{I_1} \times \dots \times R/_{I_n} .$$

Für $g \in \mathrm{Sym}(n)$ ist außerdem $I_{g(1)} \cdots I_{g(n)} \subseteq I_1 \cap \dots \cap I_n$. Daher ist auch

$$\sum_{g \in \mathrm{Sym}(n)} I_{g(1)} \cdots I_{g(n)} \subseteq I_1 \cap \dots \cap I_n .$$

Zum Beweis der umgekehrten Inklusion sei zunächst $n = 2$. Für $x \in I_1 \cap I_2$ ist dann

$$x = 1 \cdot x = (a_{12} + b_{12})x = a_{12}x + b_{12}x \in I_1 I_2 + I_2 I_1 .$$

Folglich ist $I_1 \cap I_2 = I_1 I_2 + I_2 I_1$. Sei also $n \geq 3$ und bereits gezeigt, daß

$$I_1 \cap \dots \cap I_{n-1} = \sum_{h \in \mathrm{Sym}(n-1)} I_{h(1)} \cdots I_{h(n-1)}$$

ist. Wegen $1 = \prod_{i=1}^{n-1} (a_{in} + b_{in}) \in (I_1 \cap \dots \cap I_{n-1}) + I_n$ ist $R = (I_1 \cap \dots \cap I_{n-1}) + I_n$. Der Fall $n = 2$ ergibt also

$$\begin{aligned} I_1 \cap \dots \cap I_n &= (I_1 \cap \dots \cap I_{n-1}) \cap I_n = (I_1 \cap \dots \cap I_{n-1}) I_n + I_n (I_1 \cap \dots \cap I_{n-1}) \\ &= \sum_{h \in \mathrm{Sym}(n-1)} I_{h(1)} \cdots I_{h(n-1)} I_n + \sum_{h \in \mathrm{Sym}(n-1)} I_n I_{h(1)} \cdots I_{h(n-1)} \\ &\subseteq \sum_{g \in \mathrm{Sym}(n)} I_{g(1)} \cdots I_{g(n)} . \end{aligned}$$

2.6. Definition. Ein echtes Ideal M in einem Ring R nennt man **maximal**, falls kein Ideal I in R existiert mit $M \subsetneqq I \subsetneqq R$.

Bemerkung. Ein Ideal M in einem Ring R ist also nach dem zweiten Isomorphiesatz genau dann maximal in R, wenn $R/_M$ ein einfacher Ring ist.

Beispiel. Für $k \in \mathbb{N}_0$ gilt bekanntlich: $k\mathbb{Z}$ ist ein maximales Ideal in $\mathbb{Z} \iff k$ Primzahl.

2.7. Definition. Ein echtes Ideal P in einem Ring R nennt man **Primideal**, falls für je zwei Ideale I, J von R mit $IJ \subseteq P$ stets $I \subseteq P$ oder $J \subseteq P$ folgt.

Bemerkung. Man nennt einen Ring R **prim**, falls 0 in Primideal in R ist, d.h. falls für je zwei Ideale I, J in R mit $IJ = 0$ stets $I = 0$ oder $J = 0$ folgt.

Satz. *Gegeben sei eine nichtleere, multiplikativ abgeschlossene Teilmenge X eines Rings R (d.h. $x, y \in X \Longrightarrow xy \in X$). Dann ist jedes Ideal P in R, das maximal bezüglich der Eigenschaft $P \cap X = \emptyset$ ist, ein Primideal in R. Insbesondere ist jedes maximale Ideal M von R ein Primideal in R. Daher ist jeder einfache Ring prim.*

Beweis. Seien I, J Ideale in R mit $I \not\subseteq P$ und $J \not\subseteq P$. Wir müssen $IJ \not\subseteq P$ zeigen. Wegen $I' := I + P \supset P$ existiert ein Element $x \in I' \cap X$. Wegen $J' := J + P \supset P$ existiert analog ein Element $y \in J' \cap X$. Dann ist $xy \in I'J' \cap X$. Wegen $P \cap X = \emptyset$ folgt

$$P \not\supseteq I'J' = (I + P)(J + P) = IJ + IP + PJ + P^2 \subseteq IJ + P.$$

Daher ist $IJ \not\subseteq P$. Damit ist die erste Aussage bewiesen. Die zweite Aussage ist der Spezialfall $X = \{1\}$. Der Rest folgt.

2.8. Bemerkung. Gegeben sei eine nichtleere multiplikativ abgeschlossene Teilmenge X eines Rings R mit $0 \notin X$. Dann existiert stets ein Ideal P in R, das maximal bezüglich der Eigenschaft $P \cap X = \emptyset$ ist; dies ist eine Folgerung aus Zorns Lemma.

> **Zorns Lemma** besagt folgendes: Gegeben sei eine nichtleere Menge A mit einer (partiellen) Ordnung $\leq$. Jede vollständig geordnete Teilmenge V von A (d.h. für $v, w \in W$ gilt stets $v \leq w$ oder $w \leq v$) besitze eine obere Schranke $s \in A$ (d.h. für alle $v \in V$ ist stets $v \leq s$). Dann enthält A ein maximales Element m (d.h. aus $m \leq n \in A$ folgt $m = n$). Man kann zeigen, daß Zorns Lemma zum **Auswahlaxiom** der Mengenlehre äquivalent ist. Der Beweis gehört in die Mengenlehre. Wir wollen die Äquivalenz nicht beweisen, aber benutzen.

Die obige Aussage über Ringe folgt, indem man für A die Menge aller Ideale I von R mit $I \cap X = \emptyset$ nimmt. Wegen $\{0\} \in A$ ist $A \neq \emptyset$, und A ist durch die Inklusion $\subseteq$ geordnet. Ist V eine vollständig geordnete Teilmenge von A, so ist $S := \bigcup_{I \in V} I$ eine obere Schranke von V, denn S ist ein Ideal in R mit $S \cap X = \emptyset$. Nach Zorns Lemma enthält A ein maximales Element P, und P ist nach Satz 2.7 ein Primideal. Setzt man $X = \{1\}$, so erhält man, daß jeder Ring $R \neq 0$ mindestens ein maximales Ideal enthält. Diese Tatsache werden wir häufig benutzen.

Definition. Ein Ideal S in einem Ring R nennt man **Semiprimideal** in R, falls für jedes Ideal I in R mit $I^2 \subseteq S$ stets $I \subseteq S$ folgt.

Beispiel. Jedes Primideal R ist auch ein Semiprimideal. Außerdem ist stets R selbst ein Semiprimideal in R. Ferner ist der Durchschnitt von Semiprimidealen wieder ein Semiprimideal; insbesondere ist also jeder Durchschnitt von Primidealen ein Semiprimideal.

Satz. *Ein Ideal S in einem Ring R ist genau dann ein Semiprimideal in R, wenn S ein Durchschnitt von Primidealen ist.*

Beweis. Sei S ein Semiprimideal in R. Wir zeigen, daß S der Durchschnitt aller Primideale von R ist, die S enthalten. Dazu beweisen wir, daß zu jedem Element $x \in R \setminus S$ ein Primideal P von R mit $S \subseteq P$ und $x \notin P$ existiert. Sei $x \in R \setminus S$. Dann ist $RxR \not\subseteq S$, also auch $(RxR)(RxR) \not\subseteq S$, d.h. $xRx \not\subseteq S$. Wir setzen $x_0 := x$ und wählen ein Element $x_1 \in x_0Rx_0 \setminus S$. Analog wählen wir ein Element $x_2 \in x_1Rx_1 \setminus S$. Auf diese Weise erhalten wir Elemente $x_0, x_1, x_2, \ldots \in R \setminus S$ mit $x_{i+1} \in x_iRx_i$ für alle i. Nach Zorns Lemma existiert ein Ideal P in R mit $S \subseteq P$, das maximal bezüglich $x_0, x_1, x_2, \ldots \notin P$ ist. Es genügt zu zeigen, daß P ein Primideal ist. Falls nicht, so existieren Ideale I, J in R mit $I \not\subseteq P$, $J \not\subseteq P$, aber $IJ \subseteq P$. Dann sind $I' := I + P$ und $J' := J + P$ Ideale in R mit $I' \supset P$ und $J' \supset P$. Nach Wahl von P existieren also $i, j \in \mathbb{N}_0$ mit $x_i \in I'$, $x_j \in J'$. Für $m := \max\{i, j\}$ gilt also $x_m \in I' \cap J'$ und

$$x_{m+1} \in x_mRx_m \subseteq I'J' = (I+P)(J+P) = IJ + IP + PJ + P^2 \subseteq P,$$

Widerspruch!

2.9. Definition. Einen Ring R nennt man **semiprim**, falls 0 ein Semiprimideal ist (d.h. falls kein Ideal $I \neq 0$ mit $I^2 = 0$ existiert).

Bemerkungen. Ein Ideal I in einem Ring R heißt **nilpotent**, falls ein $n \in \mathbb{N}$ mit $I^n = 0$ existiert. Das bedeutet, daß $x_1x_2 \cdots x_n = 0$ ist für alle $x_1, \ldots, x_n \in I$. Insbesondere folgt $x^n = 0$ für alle $x \in I$, d.h. jedes Element in I ist nilpotent.
Ein Ideal I in R nennt man **Nilideal**, falls alle Elemente in I nilpotent sind. Jedes nilpotente Ideal ist also ein Nilideal; die Umkehrung gilt aber im allgemeinen nicht.
Man sieht leicht, daß R genau dann semiprim ist, wenn 0 das einzige nilpotente Ideal in R ist.
In einem beliebigen Ring R nennt man den Durchschnitt aller Primideale von R das **Primradikal** von R. Dieses ist also das kleinste Semiprimideal in R, und es enthält jedes nilpotente Ideal in R.

Satz. *In jedem Ring R ist das Primradikal S ein Nilideal.*

Beweis. Wir nehmen an, daß ein Element $x \in S$ existiert, das nicht nilpotent ist. Dann ist $X := \{x^n : n \in \mathbb{N}\}$ eine multiplikativ abgeschlossene Teilmenge von R mit $0 \notin X$. Nach Bemerkung 2.8 existiert ein Primideal P in R mit $P \cap X = \emptyset$, und man erhält den Widerspruch $x \in S \subseteq P$.

2.10. Satz. *In einem kommutativen Ring R ist das Primradikal genau die Menge der nilpotenten Elemente.*

Beweis. Nach Satz 2.9 ist jedes Element im Primradikal nilpotent. Umgekehrt ist für jedes nilpotente Element $x \in R$ das Ideal RxR nilpotent, da R kommutativ ist, also

$$(RxR)^n = RxRxRx \cdots xR = Rx^nR$$

gilt. Nach Bemerkung 2.9 ist also RxR und damit x im Primradikal von R enthalten.

3 Moduln

Sei R ein Ring.

3.1. Definition. Ein R-**Linksmodul** besteht aus einer Menge M und zwei Verknüpfungen $+ : M \times M \to M$, $(a, b) \mapsto a + b$, und $\cdot : R \times M \to M$, $(r, m) \mapsto rm$, mit folgenden Eigenschaften:

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

(ii) $(rs)m = r(sm)$ für $r, s \in R$, $m \in M$.

(iii) $(r + s)m = rm + sm$ für $r, s \in R$, $m \in M$.

(iv) $r(m + n) = rm + rn$ für $r \in R$, $m, n \in M$.

(v) $1m = m$ für $m \in M$.

Analog definiert man R-**Rechtsmoduln**.

Beispiele.

(a) Für jeden Körper K sind die K-Linksmoduln genau die K-Vektorräume.

(b) Für jeden Körper K und $m, n \in \mathbb{N}$ wird $\mathrm{Mat}(m, n, K)$ durch die Matrixmultiplikation zu einem $\mathrm{Mat}(m, K)$-Linksmodul und einem $\mathrm{Mat}(n, K)$-Rechtsmodul.

(c) Jede abelsche Gruppe $(A, +)$ wird zu einem $\mathbb{Z}$-Linksmodul, wenn man na für $n \in \mathbb{Z}$ und $a \in A$ wie in Beispiel 2.1 (ii) definiert. Umgekehrt ist in jedem $\mathbb{Z}$-Linksmodul M die Multiplikation mit einem Element $n \in \mathbb{Z}$ bereits durch die Addition festgelegt: $na = (1 + \cdots + 1)a = 1a + \cdots + 1a = a + \cdots + a$ für $a \in M$. Daher sind $\mathbb{Z}$-Linksmoduln nichts anderes als abelsche Gruppen.

(d) Jeder Ring R wird durch Ringaddition und Ringmultiplikation selbst zu einem R-Linksmodul und einem R-Rechtsmodul. Diesen nennt man jeweils **regulär**.

(e) Jeder R-Linksmodul wird zu einem R°-Rechtsmodul, wenn man definiert: $mr := rm$ ($m \in M$, $r \in R$). Auf diese Weise übertragen sich Eigenschaften von R-Linksmoduln auf R°-Rechtsmoduln. Ist R kommutativ, so ist $R^\circ = R$, d.h. jeder R-Linksmodul kann auch als R-Rechtsmodul aufgefaßt werden (und umgekehrt).

(f) Seien R, S Ringe, $\varphi : R \to S$ ein unitärer Ringhomomorphismus und M ein S-Linksmodul. Dann wird M zu einem R-Linksmodul, wenn man definiert: $rm = \varphi(r)m$, $r \in R$, $m \in M$. Ein wichtiger Spezialfall ist der, daß R ein unitärer Teilring von S und $\varphi : R \to S$, $r \mapsto r$, die Inklusionsabbildung ist. In diesem Fall nennt man den entstehenden R-Modul M die **Einschränkung** oder **Restriktion** des S-Moduls M. Man schreibt dafür $\mathrm{Res}_S^R(M)$.

(g) Für jede Familie $(M_i)_{i \in I}$ von R-Linksmoduln M_i ist auch das direkte Produkt

$$\bigtimes_{i \in I} M_i = \prod_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i \text{ für } i \in I\}$$

ein R-Linksmodul, wenn man komponentenweise rechnet. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man wie üblich auch

$$M_1 \times \cdots \times M_n = \bigtimes_{i=1}^{n} M_i = \prod_{i=1}^{n} M_i = \{(m_1, \ldots, m_n) : m_1 \in M_1, \ldots, m_n \in M_n\} .$$

(h) Für jede nichtleere Menge I und jeden R-Linksmodul M ist nach (g) auch $\mathrm{Abb}(I, M) = \prod_{i\in I} M$ ein R-Linksmodul. Für $r \in R$ und $f \in \mathrm{Abb}(I, M)$ ist dabei $(rf)(i) = rf(i)$ für $i \in I$. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man wie üblich auch M^n statt $\mathrm{Abb}\big(\{1, \ldots, n\}, M\big)$.

Bemerkungen.

(i) Wie in der Linearen Algebra beweist man, daß in jedem R-Linksmodul M gilt: $r0 = 0$ für $r \in R$, $0m = 0$ für $m \in M$, $(-1)m = -m$ für $m \in M$, usw. Aus $rm = 0$ folgt aber i.a. nicht, daß $r = 0$ oder $m = 0$ sein muß.

(ii) Wir werden im folgenden meist R-Linksmoduln behandeln. Statt „Linksmodul" werden wir kurz „Modul" sagen.

3.2. Definition. Ein **Untermodul** eines R-Moduls M ist eine Teilmenge N von M, die mit den entsprechend eingeschränkten Verknüpfungen ein R-Modul ist.

Bemerkung. Das bedeutet: $0 \in N$; $r, s \in R$, $x, y \in N \Longrightarrow rx + sy \in N$.

Beispiele.

(a) Für einen Vektorraum V über einem Körper K sind die Untermoduln von V genau die Untervektorräume von V.

(b) Für einen $\mathbb{Z}$-Modul A (d.h. eine abelsche Gruppe) sind die Untermoduln von A genau die Untergruppen von A.

(c) Für jeden R-Modul M und jede Familie $(N_i)_{i\in I}$ von Untermoduln N_i von M ist auch $\bigcap_{i\in I} N_i$ ein Untermodul von M. Insbesondere ist für jede Teilmenge X von M der Durchschnitt D aller Untermoduln von M, die X enthalten, ein Untermodul von M. Man zeigt leicht, daß D genau aus allen **R-Linearkombinationen** $r_1x_1 + \cdots + r_nx_n$ mit $r_1, \ldots, r_n \in R$, $x_1, \ldots, x_n \in X$, besteht. Man nennt D den von X **erzeugten Untermodul** von M und schreibt $D = RX$, im Fall $X = \{x\}$ für ein $x \in M$ auch $D = Rx$. Ein **Erzeugendensystem** von M ist eine Teilmenge Y von M mit $M = RY$. Besitzt der Modul M ein endliches Erzeugendensystem, so nennt man M **endlich erzeugt**. Ist $M = Ry$ für ein $y \in M$, so nennt man M **zyklisch**.

(d) Für jeden R-Modul M und jede Familie $(N_i)_{i\in I}$ von Untermoduln N_i von M bilden die Elemente der Form $\sum_{i\in I} x_i$ mit $x_i \in N_i$ für $i \in I$ und $|\{i \in I : x_i \neq 0\}| < \infty$ einen Untermodul von M. Diesen nennt man die **Summe** von $(N_i)_{i\in I}$. Man bezeichnet ihn mit $\sum_{i\in I} N_i$. Man zeigt leicht, daß $\sum_{i\in I} N_i$ der von $\bigcup_{i\in I} N_i$ erzeugte Untermodul von M ist. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreiben wir auch $\sum_{i=1}^n N_i$ oder $N_1 + \cdots + N_n$ statt $\sum_{i\in I} N_i$.

(e) Für jede Familie $(M_i)_{i\in I}$ von R-Moduln bilden die Elemente $(m_i)_{i\in I} \in \prod_{i\in I} M_i$ mit $|\{i \in I : m_i \neq 0\}| < \infty$ einen Untermodul von $\prod_{i\in I} M_i$. Diesen Untermodul nennt man das **Koprodukt** von $(M_i)_{i\in I}$. Man bezeichnet ihn mit $\coprod_{i\in I} M_i$.

(f) Die R-Untermoduln des regulären R-Linksmoduls R nennt man **Linksideale** von R. Ein Linksideal ist also eine Teilmenge L von R mit $0 \in L$ und $rx + sy \in L$ für alle $r, s \in R$, $x, y \in L$. Analog definiert man **Rechtsideale**. Eine Teilmenge I von R ist also genau dann ein Ideal in R, wenn I sowohl ein R-Linksideal als auch ein R-Rechtsideal in R ist.

(g) Für jeden R-Modul M sind $\{0\} =: 0$ und M Untermoduln von M. Man nennt 0 den **trivialen Untermodul** von M. Die Untermoduln N von M mit $N \neq M$ nennt man **echte Untermoduln** von M. Ist $M \neq 0$ und sind 0 und M die einzigen Untermoduln von M, so nennt man M **einfach** oder **irreduzibel**.

Satz (Dedekind-Identität). *Für Untermoduln U, V, W eines R-Moduls M mit $U \subseteq W$ gilt stets:*

$$(U + V) \cap W = U + (V \cap W)\ .$$

Beweis. Offenbar ist $U \subseteq (U + V) \cap W$ und $V \cap W \subseteq (U + V) \cap W$. Daher ist auch $U + (V \cap W) \subseteq (U + V) \cap W$.
Sind umgekehrt $u \in U$, $v \in V$ mit $u + v \in W$, so ist

$$v = \underbrace{u + v}_{\in W} - \underbrace{u}_{\in U \subseteq W} \in W\ ,$$

also $u + v \in U + (V \cap W)$.

3.3. Bemerkung. Für jeden R-Modul M, jeden Untermodul N von M und jedes Element $m \in M$ nennt man $m + N := \{m + n : n \in N\}$ die **Nebenklasse** von m **modulo** N. Für $m' \in M$ gilt dann

$$m + N = m' + N \Longleftrightarrow m - m' \in N\ .$$

Gegebenenfalls schreibt man auch $m \equiv m' \pmod{N}$. Die Menge ${}^{M}\!/_{N} = \{m + N : m \in M\}$ aller Nebenklassen modulo N wird zu einem R-Modul, wenn man definiert

$$(m + N) + (m' + N) := (m + m') + N, \quad r(m + N) := rm + N\ .$$

(Man rechnet leicht nach, daß dies wohldefiniert ist und die gewünschten Eigenschaften hat.) Man nennt ${}^{M}\!/_{N}$ den **Faktormodul** von M nach N.

3.4. Definition. Seien M, N R-Moduln. Eine Abbildung $f : M \to N$ mit

$$f(rx + sy) = rf(x) + sf(y) \quad \text{für alle } r, s \in R,\ x, y \in M\ ,$$

nennt man R-**linear** oder einen R-**Homomorphismus**. Wie üblich definiert man R-**Monomorphismen**, R-**Epimorphismen**, R-**Isomorphismen**, R-**Endomorphismen** und R-**Automorphismen**.

Bemerkungen.

(i) Für R-Homomorphismen $f, g : M \to N$ ist auch $f \pm g : M \to N$ ein R-Homomorphismus; dabei ist $f \pm g$ durch $(f \pm g)(x) := f(x) \pm g(x)$ für $x \in M$ definiert. Ferner ist die Nullabbildung $M \to N$, $m \mapsto 0$, ein R-Homomorphismus. Daraus folgt leicht, daß die R-Homomorphismen $f : M \to N$ eine abelsche Gruppe bezüglich $+$ bilden. Diese bezeichnet man mit $\mathrm{Hom}_R(M, N)$.

(ii) Für $r \in R$ und $f \in \mathrm{Hom}_R(M, N)$ definiert man $rf : M \to N$ durch

$$(rf)(x) := rf(x) \quad \text{für } x \in M\ .$$

Im allgemeinen ist rf *kein* R-Homomorphismus. Ist aber R kommutativ, so ist rf ein R-Homomorphismus, und $\mathrm{Hom}_R(M, N)$ wird auf diese Weise zu einem R-Modul.

(iii) Für R-Moduln L, M, N und R-Homomorphismen $f : L \to M$, $g : M \to N$ ist auch $g \circ f : L \to N$ ein R-Homomorphismus. Ferner ist $\mathrm{id}_M : M \to M$ ein R-Homomorphismus. Daraus folgt leicht, daß $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ ein Ring bezüglich $+$ und $\circ$ wird. Man nennt $\mathrm{End}_R(M)$ den **Endomorphismenring** von M. Außerdem zeigt man, daß M zu einem $\mathrm{End}_R(M)$-Modul wird, wenn man $fm := f(m)$ für $f \in \mathrm{End}_R(M)$ und $m \in M$ definiert. Sind f, g R-Isomorphismen, so auch $g \circ f$ und f^{-1}. Insbesondere bilden die R-Automorphismen von M eine Gruppe bezüglich $\circ$, die **Automorphismengruppe** von M. Bezeichnung: $\mathrm{Aut}_R(M)$.

(iv) Man nennt zwei R-Moduln M, N **isomorph** und schreibt $M \cong N$ oder genauer $M \cong_R N$, falls ein R-Isomorphismus $f : M \to N$ existiert. Der Isomorphiebegriff für Moduln hat die üblichen Eigenschaften.

(v) Seien M, N R-Moduln und $f \in \mathrm{Hom}_R(M, N)$. Man zeigt leicht, daß $f(U)$ für jeden Untermodul U von M ein Untermodul von N ist. Insbesondere ist $\mathrm{Bld}(f) := f(M)$ ein Untermodul von N. Analog ist $f^{-1}(V)$ für jeden Untermodul V von N ein Untermodul von M; insbesondere ist $\mathrm{Ker}(f) := f^{-1}(0) = \{x \in M : f(x) = 0\}$ ein Untermodul von M. Man nennt $\mathrm{Ker}(f)$ den **Kern** von f. Man zeigt leicht, daß die Abbildung

$$F : {}^{M}/_{\mathrm{Ker}(f)} \to \mathrm{Bld}(f)\ , \quad m + \mathrm{Ker}(f) \mapsto f(m)\ ,$$

wohldefiniert und ein R-Isomorphismus ist. Es ist also insbesondere

$${}^{M}/_{\mathrm{Ker}(f)} \cong \mathrm{Bld}(f) \quad (\textbf{Homomorphiesatz})\ .$$

Für jeden Untermodul U von M ist $f^{-1}\big(f(U)\big) = U + \mathrm{Ker}(f)$; daher erhält man durch $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$ zueinander inverse Bijektionen zwischen der Menge der Untermoduln von M, die $\mathrm{Ker}(f)$ enthalten, und der Menge aller Untermoduln von $\mathrm{Bld}(f)$. Außerdem zeigt man leicht, daß für Untermoduln K, L von M stets die Abbildung

$${}^{K}/_{K \cap L} \to {}^{K+L}/_{L}\ , \quad x + (K \cap L) \mapsto x + L\ ,$$

ein R-Isomorphismus ist (**erster Isomorphiesatz**). Schließlich gilt im Fall $K \subseteq L \subseteq M$:

$$\big({}^{M}/_{K}\big)/\big({}^{L}/_{K}\big) \cong {}^{M}/_{L} \quad (\textbf{zweiter Isomorphiesatz})\ .$$

Beispiele.

(a) Für jeden Untermodul N eines R-Moduls M sind die **Inklusionsabbildung** $N \to M$, $n \mapsto n$, und die **Restklassenabbildung** $f : M \to {}^{M}/_{N}$, $m \mapsto m + N$, R-Homomorphismen mit $\mathrm{Ker}(f) = N$.

(b) Für jede Familie $(M_i)_{i\in I}$ von R-Moduln M_i und jedes $j \in I$ ist der j-te **Projektor**

$$p_j : \prod_{i\in I} M_i \to M_j\ , \quad (m_i)_{i\in I} \mapsto m_j$$

ein R-Epimorphismus und der j-te **Injektor**

$$q_j : M_j \to \prod_{i\in I} M_i\ , \quad m_j \mapsto (m_i)_{i\in I}\ ,$$

wobei man $m_i := 0$ für $i \neq j$ setzt, ein R-Monomorphismus. Dabei ist stets $p_j \circ q_j = \mathrm{id}_{M_j}$ und $p_k \circ q_j = 0$ für $j \neq k$. Daher ist $e_j = q_j \circ p_j \in \mathrm{End}_R\big(\prod_{i\in I} M_i\big)$ mit $e_j^2 = e_j$ für alle j und $e_k \circ e_j = 0$ für $j \neq k$. Ist I endlich, so ist

$$\sum_{i\in I} e_i = \mathrm{id}_{\prod_{i\in I} M_i} \ .$$

Satz (Dritter Isomorphiesatz, Zassenhaus 1912-1991). *Für Untermoduln U_0, U, V_0, V eines R-Moduls M mit $U_0 \subseteq U$, $V_0 \subseteq V$, gilt stets*

$$\begin{aligned} U_0 + (U\cap V) \big/ U_0 + (U \cap V_0) &\cong V_0 + (V \cap U) \big/ V_0 + (V \cap U_0) \\ &\cong U \cap V \big/ (U_0 \cap V) + (V_0 \cap U) \ . \end{aligned}$$

Beweis. Aus Symmetriegründen reicht der Beweis von

$$U_0 + (U\cap V) \big/ U_0 + (U \cap V_0) \cong U \cap V \big/ (U_0 \cap V) + (V_0 \cap U) \ .$$

Dazu definieren wir eine Abbildung

$$f : U \cap V \to U_0 + (U\cap V) \big/ U_0 + (U \cap V_0)\ , \quad x \mapsto x + U_0 + (U \cap V_0) \ .$$

Offenbar ist f ein R-Epimorphismus mit Kern

$$(U\cap V) \cap \big(U_0 + (U\cap V_0)\big) \overset{Dedekind}{=} \underbrace{(U \cap V \cap U_0)}_{=(V\cap U_0)} + (U \cap V_0) \ .$$

Der Rest folgt aus dem Homomorphiesatz.

3.5. Definition. Sei M ein R-Modul. Eine **Reihe von Untermoduln** von M ist eine endliche Folge von Untermoduln der Form

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_l = 0 \ .$$

Die Faktormoduln M_{i-1}/M_i nennt man die **Faktoren** der Reihe, die Zahl l ihre **Länge**. Zwei Reihen von Untermoduln von M nennt man **isomorph** (oder **äquivalent**), falls sie die gleiche Länge haben und ihre Faktoren bis auf die Reihenfolge isomorph sind. Eine **Verfeinerung einer Reihe** entsteht durch Einschieben von neuen Untermoduln. Sind alle M_i verschieden, so spricht man von einer Reihe **ohne Wiederholungen**.

Satz (Verfeinerungssatz von Schreier, 1901-1929). *Je zwei Reihen von Untermoduln eines R-Moduls M besitzen isomorphe Verfeinerungen.*

Beweis. Seien $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_l = 0$ und $M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = 0$ Reihen von Untermoduln von M. Zwischen M_{i-1} und M_i schieben wir jeweils die Untermoduln

$$M_{ik} := M_i + (M_{i-1} \cap N_k) \qquad (k = 1, \ldots, m-1)$$

ein, und zwischen N_k und N_{k-1} die Untermoduln

$$N_{ik} := N_k + (N_{k-1} \cap M_i) \qquad (i = 1, \ldots, l-1) \ .$$

Die analog definierten Untermoduln $M_{i0} = M_{i-1}$, $M_{im} = M_i$, $N_{0k} = N_{k-1}$, $N_{lk} = N_k$ kommen bereits in den ursprünglichen Reihen vor. Nach 3.4 hat man jeweils

$$M_{i,k-1} \big/ M_{ik} \cong N_{i-1,k} \big/ N_{ik} \ .$$

Damit folgt die Behauptung.

3.6. Definition. Eine Reihe von Untermoduln $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_l = 0$ eines R-Moduls M nennt man eine **Kompositionsreihe**, falls sie selbst keine Wiederholungen enthält, aber jede echte Verfeinerung.

Satz (Jordan-Hölder, 1835-1922; 1859-1937). *Besitzt ein R-Modul M eine Kompositionsreihe, so sind je zwei Kompositionsreihen von M isomorph.*

Beweis. Nach Schreier besitzen je zwei Kompositionsreihen von M isomorphe Verfeinerungen. Indem man notfalls Wiederholungen streicht, kann man annehmen, daß die Verfeinerungen keine Wiederholungen haben. Andererseits besitzen Kompositionsreihen keine echten Verfeinerungen ohne Wiederholungen. Also müssen die ursprünglichen Kompositionsreihen isomorph sein.

Bemerkung. Nach dem zweiten Isomorphiesatz ist eine Reihe von Untermoduln von M genau dann eine Kompositionsreihe, wenn ihre Faktoren einfach R-Moduln sind. Gegebenenfalls sind diese durch M bis auf Reihenfolge und Isomorphie eindeutig bestimmt. Man nennt sie die **Kompositionsfaktoren** von M. Außerdem ist die Länge einer Kompositionsreihe durch M eindeutig festgelegt. Man nennt sie die **(Kompositions-)Länge** von M.

3.7. Satz. *Für einen R-Modul M sind äquivalent:*

*(1) (**Aufsteigende-Ketten-Bedingung**)*
Zu jeder Folge $(N_i)_{i=1}^{\infty}$ von Untermoduln N_i von M mit $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ existiert ein $k \in \mathbb{N}$ mit $N_k = N_{k+1} = N_{k+2} = \cdots$.

*(2) (**Maximalbedingung für Untermoduln**)*
Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element (bezüglich $\subseteq$).

(3) Jeder Untermodul von M ist endlich erzeugt.

Definition. Gegebenenfalls nennt man M **noethersch** (Emmy Noether, 1882-1935).

Beweis.

(1) $\Longrightarrow$ (2): Sei $\mathfrak{M}$ eine nichtleere Menge von Untermoduln von M. Wir wählen $N_1 \in \mathfrak{M}$. Ist N_1 maximal, so sind wir fertig. Andernfalls existiert ein $N_2 \in \mathfrak{M}$ mit $N_1 \subsetneqq N_2$. Ist N_2 maximal, so sind wir wieder fertig. Andernfalls existiert ein $N_3 \in \mathfrak{M}$ mit $N_1 \subsetneqq N_2 \subsetneqq N_3$. Auf diese Weise fährt man fort. Aus (1) folgt, daß dieses Verfahren bei einem N_k enden muß. Dann ist N_k maximal in $\mathfrak{M}$.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt, N ein Untermodul von M und $\mathfrak{N}$ die Menge der endlich erzeugten Untermoduln von N. Wegen $0 \in \mathfrak{N}$ ist $\mathfrak{N} \neq \emptyset$. Nach (2) enthält $\mathfrak{N}$ ein maximales Element L. Ferner existieren $x_1, \ldots, x_n \in L$ mit $L = Rx_1 + \cdots + Rx_n$. Wäre $L \neq N$, so existierte ein Element $y \in N \setminus L$, und es wäre $L \subsetneqq Rx_1 + \cdots + Rx_n + Ry \in \mathfrak{N}$, im Widerspruch zur Wahl von L. Daher ist $N = L$ und daher N endlich erzeugt.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt und $(N_i)_{i=1}^{\infty}$ eine Folge von Untermoduln von M mit $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$. Man zeigt leicht, daß $N := \bigcup_{i=1}^{\infty} N_i$ ein Untermodul von M ist. Wegen (3) existieren $x_1, \ldots, x_n \in N$ mit $N = Rx_1 + \cdots + Rx_n$. Für $i = 1, \ldots, n$ existiert ferner ein $k_i \in \mathbb{N}$ mit $x_i \in N_{k_i}$. Mit $k := \max\{k_1, \ldots, k_n\}$ ist $x_1, \ldots, x_n \in N_k$. Dann ist aber $N \subseteq N_k \subseteq N_{k+1} \subseteq \cdots \subseteq N$, d.h. $N = N_k = N_{k+1} = \cdots$.

3.8. Satz. *Für jeden Untermodul N eines R-Moduls M gilt: M noethersch $\iff$ N und M/N noethersch.*

Beweis.

„$\Longrightarrow$“: Mit M erfüllt auch N die Bedingung (2) aus 3.7. Analog erfüllt auch M/N diese Bedingung, da jeder Untermodul von M/N die Form U/N hat, wobei U ein Untermodul von M mit $N \subseteq U$ ist.

„$\Longleftarrow$“: Seien N und M/N noethersch. Sei außerdem $(M_i)_{i=1}^{\infty}$ eine Folge von Untermoduln von M mit $M_1 \subseteq M_2 \subseteq \cdots$. Dann ist

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \cdots .$$

Da N noethersch ist, existiert ein $k \in \mathbb{N}$ mit

$$M_k \cap N = M_{k+1} \cap N = M_{k+2} \cap N = \cdots .$$

Analog ist

$$M_1 + N/N \subseteq M_2 + N/N \subseteq M_3 + N/N \subseteq \cdots .$$

Da M/N noethersch ist, existiert ein $l \in \mathbb{N}$ mit

$$M_l + N/N = M_{l+1} + N/N = M_{l+2} + N/N = \cdots .$$

Für $n \geq \max\{k, l\}$ gilt dann:

$$\begin{aligned} M_n &= M_n + (N \cap M_n) = M_n + (N \cap M_{n+1}) \overset{Dedekind}{=} (M_n + N) \cap M_{n+1} \\ &= (M_{n+1} + N) \cap M_{n+1} = M_{n+1} . \end{aligned}$$

3.9. Satz. *Für einen R-Modul M sind äquivalent:*

*(1) (**Absteigende-Ketten-Bedingung**)*
Zu jeder Folge $(N_i)_{i=1}^{\infty}$ von Untermoduln von M mit $N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$ existiert ein $k \in \mathbb{N}$ mit $N_k = N_{k+1} = N_{k+2} = \cdots$.

*(2) (**Minimalbedingung für Untermoduln**)*
Jede nichtleere Menge von Untermoduln von M besitzt ein minimales Element (bezüglich $\subseteq$).

Definition. Gegebenenfalls nennt man M **artinsch** (Emil Artin, 1898-1962).

Beweis.

(1) $\Longrightarrow$ (2): analog zu 3.7.

(2) $\Longrightarrow$ (1): Sei $(N_i)_{i=1}^{\infty}$ eine Folge von Untermoduln von M mit $N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$. Ist (2) erfüllt, so existiert in der Menge $\mathfrak{N} = \{N_i : i = 1, 2, \ldots\}$ ein minimales Element N_k. Es ist also $N_k = N_{k+1} = N_{k+2} = \cdots$.

Bemerkungen.

(i) Analog zu 3.8 beweist man, daß für jeden Untermodul N eines R-Moduls M gilt: M artinsch $\Longleftrightarrow$ N und ${}^{M}\!/_{N}$ artinsch.

(ii) Sind N, N' artinsche (noethersche) Untermoduln eines R-Moduls M, so ist auch $N+N'$ artinsch (noethersch). Denn es ist ${}^{N+N'}\!/_{N'} \cong {}^{N}\!/_{N \cap N'}$.

3.10. Satz. *Ein R-Modul M besitzt genau dann eine Kompositionsreihe, wenn er artinsch und noethersch ist.*

Beweis.

„$\Longrightarrow$“: Sei $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_l = 0$ eine Kompositionsreihe. Die Kompositionsfaktoren ${}^{M_0}\!/_{M_1}, \ldots, {}^{M_{l-1}}\!/_{M_l}$ sind einfach, also noethersch und artinsch. Nach Satz 3.8 und Bemerkung 3.9 (i) sind also $M_l, M_{l-1}, \ldots, M_0 = M$ noethersch und artinsch.

„$\Longleftarrow$“: Sei M artinsch und noethersch, und $\mathfrak{N}$ die Menge aller Untermoduln von M, die eine Kompositionsreihe haben. Wegen $0 \in \mathfrak{N}$ ist $\mathfrak{N} \neq \emptyset$. Da M noethersch ist, enthält $\mathfrak{N}$ ein maximales Element N. Wir wählen eine Kompositionsreihe $N = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_l = 0$ und nehmen $M \neq N$ an. Dann ist die Menge $\mathfrak{M}$ aller von 0 verschiedenen Untermoduln von ${}^{M}\!/_{N}$ nichtleer. Da mit M auch ${}^{M}\!/_{N}$ artinsch ist, enthält $\mathfrak{M}$ ein minimales Element ${}^{L}\!/_{N}$. Offenbar ist ${}^{L}\!/_{N}$ einfach. Folglich ist $L \supseteq N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_l = 0$ eine Kompositionsreihe im Widerspruch zur Wahl von N.

3.11. Definition. Man nennt den Ring R **linksnoethersch** (**linksartinsch**), wenn der reguläre R-Linksmodul R noethersch (artinsch) ist. Analog definiert man **rechtsnoethersche** und **rechtsartinsche** Ringe. Ist R linksnoethersch und rechtsnoethersch (linksartinsch und rechtsartinsch), so nennt man R **noethersch** (**artinsch**).

Beispiel. Für $n \in \mathbb{N}$ und jeden Körper K ist $R := \mathrm{Mat}(n, K)$ artinsch und noethersch, denn jedes Linksideal (Rechtsideal) ist gleichzeitig ein K-Untervektorraum.

Satz. *Jeder endlich erzeugte Linksmodul M über einem linksnoetherschen (linksartinschen) Ring R ist noethersch (artinsch).*

Beweis. Wir schreiben $M = Rm_1 + \cdots + Rm_n$ mit $m_1, \ldots, m_n \in M$. Für $i = 1, \ldots, n$ ist dann $f_i : R \to Rm_i$, $r \mapsto rm_i$, ein R-Epimorphismus. Dabei ist $Rm_i = f_i(R) \cong {}^{R}\!/_{\mathrm{Ker}(f_i)}$ noethersch nach Satz 3.8 (artinsch nach Bemerkung 3.9 (i)). Folglich ist M noethersch (artinsch) nach Bemerkung 3.9 (ii).

4 Einfache und halbeinfache Moduln

Sei R ein Ring.

4.1. Bemerkung. Seien M, N R-Moduln und $f \in \mathrm{Hom}_R(M,N)$. Wie in der linearen Algebra zeigt man: f injektiv $\Longleftrightarrow \mathrm{Ker}(f) = 0$.

Satz (Schurs Lemma, 1875-1941). *Für R-Moduln M, N gilt stets:*

(i) Ist M einfach, so ist jedes $f \in \mathrm{Hom}_R(M,N) \setminus \{0\}$ injektiv.

(ii) Ist N einfach, so ist jedes $f \in \mathrm{Hom}_R(M,N) \setminus \{0\}$ surjektiv.

(iii) Sind M und N einfach und nicht isomorph, so ist $\mathrm{Hom}_R(M,N) = 0$.

(iv) Ist M einfach, so ist $\mathrm{End}_R(M)$ ein Schiefkörper.

Beweis.

(i): Sei M einfach und $f \in \mathrm{Hom}_R(M,N) \setminus \{0\}$, d.h. $M \neq \mathrm{Ker}(f)$. Da M einfach ist, folgt $\mathrm{Ker}(f) = 0$, d.h. f ist injektiv.

(ii): Analog.

(iii) und (iv): Folgen aus (i) und (ii).

4.2. Definition. Ein echtes Linksideal M in R nennt man **maximal**, falls kein Linksideal L in R mit $M \subsetneq L \subsetneq R$ existiert. Analog definiert man **minimale** Linksideale.

Bemerkungen.

(i) Ein Linksideal M in R ist genau dann maximal, wenn R/M ein einfacher R-Modul ist. Ein Linksideal M in R ist genau dann minimal, wenn M ein einfacher R-Modul ist.

(ii) Zu jedem echten Linksideal L in R existiert ein maximales Linksideal M in R mit $L \subseteq M$; dies beweist man mit Zorns Lemma analog zu Bemerkung 2.8. Insbesondere besitzt jeder Ring $R \neq 0$ ein maximales Linksideal M, also auch einen einfachen R-Modul (nämlich R/M). Es gibt Ringe, die keine minimalen Linksideale enthalten (z.B. $\mathbb{Z}$).

Satz. *Zu jedem einfachen R-Modul S existiert ein maximales Linksideal M in R mit*

$$S \cong R/M \,.$$

Beweis. Sei $s \in S \setminus \{0\}$. Dann ist die Abbildung $f : R \to S$, $r \mapsto rs$, ein von 0 verschiedener R-Homomorphismus. Nach Schur ist f surjektiv, also $S \cong R/\mathrm{Ker}(f)$ einfach, d.h. $\mathrm{Ker}(f)$ ist ein maximales Linksideal in R.

4.3. Satz. *Für jede Familie $(N_i)_{i \in I}$ von Untermoduln eines R-Moduls M sind die folgenden Aussagen äquivalent:*

(1) Die Abbildung

$$f : \coprod_{i\in I} N_i \to \sum_{i\in I} N_i\ , \quad (n_i)_{i\in I} \mapsto \sum_{i\in I} n_i\ ,$$

ist ein R-Isomorphismus.

(2) Ist $(n_i)_{i\in I} \in \coprod_{i\in I} N_i$ mit $\sum_{i\in I} n_i = 0$, so ist $n_i = 0$ für alle i.

(3) Für jedes $j \in I$ ist $N_j \cap \sum_{i\in I\setminus\{j\}} N_i = 0$.

Beweis.

(1) $\Longrightarrow$ (2): Klar.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt und $x \in N_j \cap \sum_{i\in I\setminus\{j\}} N_i$. Wir schreiben $x = \sum_{i\in I\setminus\{j\}} n_i$ mit $n_i \in N_i$ für alle i und $\big|\{i \in I \setminus \{j\} : n_i \neq 0\}\big| < \infty$. Setzt man $n_j := -x \in N_j$, so ist $(n_i)_{i\in I} \in \coprod_{i\in I} N_i$ mit $\sum_{i\in I} n_i = 0$. Aus (2) folgt also $n_j = 0$ für alle j; insbesondere ist $x = -n_j = 0$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt. Offenbar ist die Abbildung f in (1) ein R-Epimorphismus. Wir nehmen an, daß f nicht injektiv ist. Dann ist $\mathrm{Ker}(f) \neq 0$. Wir wählen ein Element $(n_i)_{i\in I} \in \mathrm{Ker}(f) \setminus \{0\}$. Dann existiert ein $j \in I$ mit $n_j \neq 0$. Wegen

$$0 = f((n_i)_{i\in I}) = \sum_{i\in I} n_i$$

ist

$$0 \neq n_j = -\sum_{i\in I\setminus\{j\}} n_i \in N_j \cap \sum_{i\in I\setminus\{j\}} N_i$$

im Widerspruch zu (3).

Definition. Gegebenenfalls nennt man die Summe der Familie $(N_i)_{i\in I}$ **direkt** und schreibt

$$\sum_{i\in I} N_i = \bigoplus_{i\in I} N_i\ .$$

Bemerkungen.

(i) Im Fall $I = \{1, \ldots, n\}$ zeigt man leicht, daß die Summe der Familie $(N_i)_{i=1}^n$ genau dann direkt ist, wenn $N_j \cap \sum_{i=1}^{j-1} N_i = 0$ für $j = 1, \ldots, n$ ist. Gegebenenfalls schreibt man auch $N_1 \oplus \cdots \oplus N_n$ oder $\bigoplus_{i=1}^n N_i$.

(ii) Ist I beliebig und $\sum_{i\in I} N_i = \bigoplus_{i\in I} N_i$, so ist für $j \in I$ der j-te **Projektor**

$$p_j : \bigoplus_{i\in I} N_i \to N_j\ , \quad \sum_{i\in I} n_i \mapsto n_j\ ,$$

ein R-Epimorphismus, und der j-te **Injektor**

$$q_j : N_j \to \bigoplus_{i\in I} N_i\ , \quad n_j \mapsto n_j\ ,$$

ist ein R-Monomorphismus. Dabei gilt wie früher: $p_j \circ q_j = \mathrm{id}_{N_j}$, $p_k \circ q_j = 0$ für $j \neq k$, $e_j := q_j \circ p_j \in \mathrm{End}_R\big(\bigoplus_{i\in I} N_i\big)$, $e_j^2 = e_j$ für alle j und $e_k \circ e_j = 0$ für $j \neq k$. Ist I endlich, so ist ferner $\sum_{i\in I} e_i = \mathrm{id}_{\oplus_{i\in I} N_i}$.

4.4. Satz. *Für einen R-Modul M sind äquivalent:*

(1) M läßt sich als Summe einfacher Untermoduln schreiben.

(2) M läßt sich als direkte Summe einfacher Untermoduln schreiben.

(3) Zu jedem Untermodul N von M existiert ein Untermodul N' von M mit $M = N \oplus N'$.

Definition. Gegebenenfalls nennt man M **halbeinfach** oder **vollständig reduzibel**. Einen Untermodul N' wie in (3) nennt man ein **Komplement** von N in M.

Beweis.

(1) $\Longrightarrow$ (2): Sei $M = \sum_{i\in I} M_i$ mit einer Familie $(M_i)_{i\in I}$ einfacher Untermoduln von M. Dann ist

$$\mathfrak{J} = \Big\{J \subseteq I : \sum_{j\in J} M_j \text{ direkt}\Big\}$$

nichtleer wegen $\emptyset \in \mathfrak{J}$ und geordnet durch $\subseteq$. Ist $\mathfrak{K}$ eine nichtleere totalgeordnete Teilmenge von $\mathfrak{J}$ und $S := \bigcup_{K\in\mathfrak{K}} K (\subseteq I)$, so ist $\sum_{s\in S} M_s$ direkt; denn sonst existiert eine endliche Teilmenge T von S mit der Eigenschaft, daß $\sum_{t\in T} M_t$ nicht direkt ist. Ferner existiert ein $K \in \mathfrak{K}$ mit $T \subseteq K$. Folglich ist $\sum_{k\in K} M_k$ nicht direkt, im Widerspruch zu $K \in \mathfrak{K} \subseteq \mathfrak{J}$. Dies zeigt, daß S eine obere Schranke von $\mathfrak{K}$ in $\mathfrak{J}$ ist. Nach Zorns Lemma enthält $\mathfrak{J}$ ein maximales Element Z. Wäre $\sum_{z\in Z} M_z \neq M$, so gäbe es ein $i \in I$ mit $M_i \not\subseteq \sum_{z\in Z} M_z$. Dann wäre $M_i \cap \sum_{z\in Z} M_z$ ein echter Untermodul von M_i. Da M_i einfach ist, folgt $M_i \cap \sum_{z\in Z} M_z = 0$. Daher ist

$$M_i + \sum_{z\in Z} M_z = M_i \oplus \sum_{z\in Z} M_z = M_i \oplus \bigoplus_{z\in Z} M_z\ ,$$

d.h. $Z \cup \{i\} \in \mathfrak{J}$ im Widerspruch zur Wahl von Z. Also ist $M = \sum_{z\in Z} M_z = \bigoplus_{z\in Z} M_z$.

(2) $\Longrightarrow$ (3): Sei $M = \bigoplus_{i\in I} M_i$ mit einer Familie $(M_i)_{i\in I}$ einfacher Untermoduln von M, und sei N ein Untermodul von M. Dann ist $\mathfrak{J} = \big\{J \subseteq I : N \cap \sum_{j\in J} M_j = 0\big\}$ wegen $\emptyset \in \mathfrak{J}$ nichtleer und durch $\subseteq$ geordnet. Wie oben zeigt man, daß jede total geordnete Teilmenge $\mathfrak{K}$ von $\mathfrak{J}$ eine obere Schranke in $\mathfrak{J}$ hat. Nach Zorn enthält $\mathfrak{J}$ ein maximales Element Z. Wäre $N + \sum_{z\in Z} M_z \neq M$, so wäre $M_i \not\subseteq N + \sum_{z\in Z} M_z$ für ein $i \in I$. Dann wäre aber $M_i \cap \big(N + \sum_{z\in Z} M_z\big) = 0$ wegen der Einfachheit von M_i, also wäre

$$M_i + \Big(N + \sum_{z\in Z} M_z\Big) = M_i \oplus \Big(N \oplus \bigoplus_{z\in Z} M_z\Big) = N \oplus \bigoplus_{z\in Z\cup\{i\}} M_z\ ,$$

d.h. $Z \cup \{i\} \in \mathfrak{J}$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt und S die Summe aller einfachen Untermoduln von M. Dann existiert ein Untermodul N von M mit $M = S \oplus N$. Wir nehmen $N \neq 0$ an und wählen $x \in N \setminus \{0\}$. Dann ist $f : R \to N$, $r \mapsto rx$, R-linear mit $\mathrm{Bld}(f) = Rx$. Nach Bemerkung 4.2 existiert ein maximales Linksideal L in R mit $\mathrm{Ker}(f) \subseteq L$. Dann ist $L/\mathrm{Ker}(f)$ ein Untermodul von $R/\mathrm{Ker}(f)$ und

$$\big(R/\mathrm{Ker}(f)\big)/\big(L/\mathrm{Ker}(f)\big) \cong R/L$$

ein einfacher R-Modul. Wegen $R/\mathrm{Ker}(f) \cong \mathrm{Bld}(f) = Rx$ enthält auch Rx einen Untermodul L' mit der Eigenschaft, daß Rx/L' einfach ist. Wegen (3) existiert ein Untermodul K von M mit $M = L' \oplus K$. Nach Dedekind ist

$$Rx = Rx \cap M = Rx \cap (L' + K) = L' + (Rx \cap K) = L' \oplus (Rx \cap K) ,$$

also $Rx \cap K \cong Rx/L'$ ein einfacher R-Modul, d.h. $Rx \cap K \subseteq S \cap N = 0$, Widerspruch.

4.5. Satz. *Ist N ein Untermodul eines halbeinfachen R-Moduls M, so sind N und M/N halbeinfach.*

Beweis. Zu jedem Untermodul U von N existiert nach Voraussetzung ein Untermodul V von M mit $M = U \oplus V$. Nach Dedekind ist also

$$N = N \cap M = N \cap (U + V) = U + (N \cap V) = U \oplus (N \cap V) .$$

Daher ist N halbeinfach. Ferner existiert ein Untermodul N' von M mit $M = N \oplus N'$. Dann ist $M/N \cong N'$. Außerdem ist N' halbeinfach, also auch M/N.

4.6. Definition. Man nennt R **halbeinfach**, falls der reguläre R-Linksmodul R halbeinfach ist.

Bemerkungen.

(i) Eigentlich müßte man „linkshalbeinfach" sagen. Es wird sich aber bald zeigen, daß jeder „linkshalbeinfache" Ring R auch „rechtshalbeinfach" ist und umgekehrt.

(ii) Sei R halbeinfach und $R = \bigoplus_{i\in I} M_i$ mit einfachen Untermoduln (minimalen Linksidealen) von R. Wir schreiben $1 = \sum_{i\in I} m_i$ mit $m_i \in M_i$ für alle i und $J := \{i \in I : M_i \neq 0\}$ endlich. Dann ist $1 = \sum_{i\in J} m_i$, also $r = r1 = \sum_{i\in J} rm_i \in \sum_{i\in J} M_i$. Folglich ist $R = \sum_{i\in J} M_i = \bigoplus_{i\in J} M_i$. Dies zeigt, daß R eine direkte Summe von *endlich vielen* einfachen Untermoduln ist. Insbesondere ist R linksnoethersch und linksartinsch. Schreibt man $R = M_1 \oplus \cdots \oplus M_n$ mit einfachen Untermoduln $M_1, \ldots, M_n$, so ist

$$R = M_1 \oplus \cdots \oplus M_n \supseteq M_2 \oplus \cdots \oplus M_n \supseteq \cdots \supseteq M_n \supseteq 0$$

eine Kompositionsreihe von R, deren Faktoren zu $M_1, \ldots, M_n$ isomorph sind. Nach Jordan-Hölder sind also $M_1, \ldots, M_n$ bis auf Isomorphie und Reihenfolge durch R eindeutig bestimmt. Ist S ein einfacher R-Modul, so existiert nach Satz 4.2 ein maximales Linksideal L in R mit $S \cong R/L$. Man kann die Reihe $R \supseteq L \supseteq 0$ zu einer Kompositionsreihe von R verfeinern. Nach Jordan-Hölder ist R/L zu einem M_i isomorph. Das zeigt, daß jeder einfache R-Modul zu einem der M_i isomorph ist. Insbesondere besitzt R bis auf Isomorphie nur endlich viele einfache Moduln.

Satz. *Ist R halbeinfach, so ist jeder R-Modul M halbeinfach.*

Beweis. Für $m \in M$ ist die Abbildung $f_m : R \to M$, $r \mapsto rm$, R-linear. Nach Satz 4.5 ist $Rm = \mathrm{Bld}(f_m) \cong R/\mathrm{Ker}(f_m)$ halbeinfach, d.h. Summe von einfachen Untermoduln. Wegen $M = \sum_{m\in M} Rm$ ist also auch M eine Summe von einfachen Untermoduln.

4.7. Satz (vergleiche Aufgabe 16). *Für jeden Ring R gilt:*

(i) Für $n \in \mathbb{N}$ und jeden R-Modul M ist $\mathrm{End}_R(M^n) \cong \mathrm{Mat}\big(n, \mathrm{End}_R(M)\big)$.

(ii) Sind $M_1, \ldots, M_n$ R-Moduln mit $\mathrm{Hom}_R(M_i, M_j) = 0$ *für $i \neq j$, so ist*

$$\mathrm{End}_R(M_1 \times \cdots \times M_n) \cong \mathrm{End}_R(M_1) \times \cdots \times \mathrm{End}_R(M_n) .$$

(iii) Für jedes Idempotent e in R ist $\mathrm{End}_R(Re) \cong (eRe)^\circ$*; insbesondere ist* $\mathrm{End}_R(R) \cong R^\circ$.

4.8. Satz (Wedderburn, 1882-1948). *Äquivalent sind:*

(1) R ist halbeinfach.

(2) Es existieren $l \in \mathbb{N}_0$, $d_1, \ldots, d_l \in \mathbb{N}$ und Schiefkörper $D_1, \ldots, D_l$ mit

$$R \cong_{\text{als Ring}} \operatorname{Mat}(d_1, D_1) \times \cdots \times \operatorname{Mat}(d_l, D_l) \; .$$

Gegebenenfalls sind $l, d_1, \ldots, d_l$ eindeutig (bis auf Reihenfolge), und $D_1, \ldots, D_l$ sind eindeutig bis auf Isomorphie.

Beweis.

(1) $\Longrightarrow$ (2): Sei R halbeinfach. Wir schreiben $R \cong_{\text{als } R\text{-Modul}} M_1^{d_1} \times \cdots \times M_l^{d_l}$ mit paarweise nichtisomorphen einfachen R-Moduln $M_1, \ldots M_l$ und $d_1, \ldots d_l \in \mathbb{N}$. Für verschiedene i, j ist dann $\operatorname{Hom}_R(M_i, M_j) = 0$ nach Schur. Daraus folgt leicht: $\operatorname{Hom}_R(M_i^{d_i}, M_j^{d_j}) = 0$. Daher gilt nach Satz 4.7

$$\begin{aligned} R^\circ &\cong \operatorname{End}_R(R) \\ &\cong \operatorname{End}_R(M_1^{d_1} \times \cdots \times M_l^{d_l}) \\ &\cong \operatorname{End}_R(M_1^{d_1}) \times \cdots \times \operatorname{End}_R(M_l^{d_l}) \\ &\cong \operatorname{Mat}\big(d_1, \operatorname{End}_R(M_1)\big) \times \cdots \times \operatorname{Mat}\big(d_l, \operatorname{End}_R(M_l)\big) \; . \end{aligned}$$

Für $i = 1, \ldots, l$ ist dabei $E_i := \operatorname{End}_R(M_i)$ ein Schiefkörper nach Schur. Daher ist

$$\begin{aligned} R &\cong \big(\operatorname{Mat}(d_1, E_1) \times \cdots \times \operatorname{Mat}(d_l, E_l)\big)^\circ \\ &= \operatorname{Mat}(d_1, E_1)^\circ \times \cdots \times \operatorname{Mat}(d_l, E_l)^\circ \\ &\cong \operatorname{Mat}(d_1, E_1^\circ) \times \cdots \times \operatorname{Mat}(d_l, E_l^\circ) \; , \end{aligned}$$

denn man hat jeweils einen Isomorphismus von Ringen $\operatorname{Mat}(d_i, E_i)^\circ \to \operatorname{Mat}(d_i, E_i^\circ)$, $A \mapsto A^T$. Jedes $D_i := E_i^\circ$ ist auch Schiefkörper.

(2) $\Longrightarrow$ (1): Sei $R = \operatorname{Mat}(d_1, D_1) \times \cdots \times \operatorname{Mat}(d_l, D_l)$ mit $d_1, \ldots, d_l \in \mathbb{N}$ und Schiefkörpern $D_1, \ldots, D_l$. Man rechnet leicht nach, daß

$$L_{ij} := 0 \times \cdots \times 0 \times \underbrace{\underset{j}{\begin{pmatrix} 0 & \ldots & 0 & * & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & * & 0 & \ldots & 0 \end{pmatrix}}}_{i} \times 0 \times \cdots \times 0$$

für $i = 1, \ldots, l$, $j = 1, \ldots, d_i$ ein einfacher R-Modul ist. Wegen $R = \oplus_{i=1}^{l} \oplus_{j=1}^{d_i} L_{ij}$ ist also R halbeinfach. Für alle i, j ist $\operatorname{Ann}_R(L_{ij}) = \operatorname{Mat}(d_1, D_1) \times \cdots \times \operatorname{Mat}(d_{i-1}, D_{i-1}) \times 0 \times \operatorname{Mat}(d_{i+1}, D_{i+1}) \times \cdots \times \operatorname{Mat}(d_l, D_l)$. Daher sind L_{ij} und $L_{i'j'}$ für verschiedene i, i' nicht isomorph. Andererseits sind stets L_{ij} und $L_{ij'}$ isomorph. Daher ist l die Anzahl der Isomorphieklassen einfacher R-Moduln. Ferner sind $d_1, \ldots, d_l$ nach Jordan-Hölder eindeutig bestimmt.
Für $i = 1, \ldots, l$ ist

$$e_i := \left(0, \ldots, 0, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 0, \ldots, 0\right)$$

ein Idempotent mit $Re_i = L_{i1}$. Daher gilt nach Satz 4.7:

$$\begin{aligned}\operatorname{End}_R(L_{i1}) &= \operatorname{End}_R(Re_i) = (e_i R e_i)^\circ \\ &= \left(0 \times \cdots \times 0 \times \begin{pmatrix} D_i & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix} \times 0 \times \cdots \times 0\right)^\circ \\ &\cong D_i^\circ \,.\end{aligned}$$

Folglich sind auch $D_1, \ldots, D_l$ eindeutig.

Bemerkung. Analog zeigt man, daß R genau dann „rechtshalbeinfach“ ist, wenn die Bedingung (2) erfüllt ist. Daher gilt:

$$R \text{ „linkshalbeinfach“} \iff R \text{ „rechtshalbeinfach“}$$

5 Das Jacobson-Radikal

Sei R ein Ring.

5.1. Definition. Sei M ein R-Modul.

(i) Ein echter Untermodul N von M heißt **maximal**, falls kein Untermodul L von M mit $N \subsetneqq L \subsetneqq M$ existiert. Entsprechend: **minimale** Untermoduln.

(ii) Den Durchschnitt D aller maximalen Untermoduln von M bezeichnet man als **(Jacobson-)Radikal** von M. Man schreibt $D = \operatorname{Rad}(M) = \operatorname{Rad}_R(M)$.
Die Summe aller minimalen Untermoduln von M bezeichnet man als **Sockel** von M. Man schreibt $S = \operatorname{Soc}(M) = \operatorname{Soc}_R(M)$.

Bemerkung. Ein Untermodul N von M ist genau dann maximal, wenn ${}^M/_N$ ein einfacher R-Modul ist. Ein R-Modul braucht keine maximalen Untermoduln zu besitzen. In diesem Fall setzt man $\operatorname{Rad}(M) := M$. Analog setzt man $\operatorname{Soc}(M) := 0$, falls M keine minimalen Untermoduln besitzt.

Satz.

(i) Für R-Moduln M, N und $f \in \operatorname{Hom}_R(M, N)$ ist stets $f(\operatorname{Rad}(M)) \subseteq \operatorname{Rad}(N)$.

(ii) Für jeden Untermodul N eines R-Moduls M ist stets $\operatorname{Rad}(N) \subseteq \operatorname{Rad}(M)$ und

$$\operatorname{Rad}(M) + {}^N/_N \subseteq \operatorname{Rad}\left({}^M/_N\right) .$$

(iii) Für jeden Untermodul N von M mit $N \subseteq \operatorname{Rad}(M)$ ist

$$\operatorname{Rad}\left({}^M/_N\right) = {}^{\operatorname{Rad}(M)}/_N ;$$

insbesondere ist $\operatorname{Rad}\left({}^M/\operatorname{Rad}(M)\right) = 0$.

(iv) Für jede Familie $(M_i)_{i\in I}$ von R-Moduln ist

$$\operatorname{Rad}\Big(\prod_{i\in I} M_i\Big) \subseteq \prod_{i\in I} \operatorname{Rad}(M_i) \quad \textit{und} \quad \operatorname{Rad}\Big(\coprod_{i\in I} M_i\Big) = \coprod_{i\in I} \operatorname{Rad}(M_i) .$$

Beweis.

(i) Sei L ein maximaler Untermodul von N. Dann ist ${}^N/_L$ ein einfacher R-Modul. Es sei $g : N \to {}^N/_L$ die Restklassenabbildung. Dann ist $g \circ f : M \to {}^N/_L$ R-linear. Im Fall $g \circ f = 0$ ist $\operatorname{Ker}(g \circ f) = M$, und im Fall $g \circ f \neq 0$ ist $g \circ f$ surjektiv nach Schur, also ${}^M/\operatorname{Ker}(g \circ f) \cong {}^N/_L$ nach dem Homomorphiesatz, d.h. $\operatorname{Ker}(g \circ f)$ ist ein maximaler Untermodul von M. In jedem Fall ist $\operatorname{Rad}(M) \subseteq \operatorname{Ker}(g \circ f)$, also $g\Big(f\big(\operatorname{Rad}(M)\big)\Big) = 0$, d.h. $f\big(\operatorname{Rad}(M)\big) \subseteq \operatorname{Ker}(g) = L$.

(ii) Wende (i) an auf die Inklusionsabbildung $N \to M$ und die Restklassenabbildung $M \to {}^M/_N$.

(iii) Im Fall $N \subseteq \operatorname{Rad}(M)$ entsprechen sich nach den Isomorphiesätzen die maximalen Untermoduln von M und von ${}^M/_N$.

(iv) Sei $j \in I$ und $p_j : \prod_{i \in I} M_i \to M_j$ der entsprechende Projektor. Nach (i) ist dann $p_j\Big(\operatorname{Rad}\big(\prod_{i\in I} M_i\big)\Big) \subseteq \operatorname{Rad}(M_j)$. Daher ist $\operatorname{Rad}\big(\prod_{i\in I} M_i\big) \subseteq \prod_{j\in I} \operatorname{Rad}(M_j)$. Nach (ii) ist also

$$\operatorname{Rad}\Big(\coprod_{i\in I} M_i\Big) \subseteq \operatorname{Rad}\Big(\prod_{i\in I} M_i\Big) \subseteq \prod_{j\in I} \operatorname{Rad}(M_j) .$$

Daher ist $\operatorname{Rad}\big(\coprod_{i\in I} M_i\big) \subseteq \coprod_{j\in I} \operatorname{Rad}(M_j)$. Sei $j \in I$ und $q_j : M_j \to \coprod_{i\in I} M_i$ der entsprechende Injektor. Dann gilt nach (i): $q_j\big(\operatorname{Rad}(M_j)\big) \subseteq \operatorname{Rad}\big(\coprod_{i\in I} M_i\big)$. Daher ist

$$\coprod_{j\in I} \operatorname{Rad}(M_j) = \sum_{j\in I} q_j\big(\operatorname{Rad}(M_j)\big) \subseteq \operatorname{Rad}\Big(\coprod_{i\in I} M_i\Big) .$$

5.2. Satz. *Für jeden R-Modul gilt:*

(i) $\operatorname{Rad}(M) = 0 \iff M$ *ist isomorph zu einem Untermodul eines direkten Produktes von einfachen R-Moduln.*

(ii) M *halbeinfach* $\Longrightarrow \operatorname{Rad}(M) = 0$.

(iii) M *endlich erzeugt und halbeinfach* $\iff M$ *artinsch und* $\operatorname{Rad}(M) = 0$.

(iv) M *endlich erzeugt und* $M \neq 0 \Longrightarrow \operatorname{Rad}(M) \neq M$.

Beweis.

(i)

„$\Longrightarrow$“: Sei $\operatorname{Rad}(M) = 0$ und $\mathfrak{M}$ die Menge der maximalen Untermoduln von M. Dann ist die Abbildung $f : M \to \prod_{N\in\mathfrak{M}} M/N$, $m \mapsto (m+N)_{N\in\mathfrak{M}}$, R-linear mit $\operatorname{Ker}(f) = \bigcap_{N\in\mathfrak{M}} N = \operatorname{Rad}(M) = 0$. Daher ist

$$M \cong \operatorname{Bld}(f) \subseteq \prod_{N\in\mathfrak{M}} \underbrace{M/N}_{\substack{\text{einfache}\\ R\text{-Moduln}}} .$$

„$\Longleftarrow$“: Sei $(S_i)_{i\in I}$ eine Familie einfacher R-Moduln und $f : M \to \prod_{i\in I} S_i$ ein R-Monomorphismus. Nach 5.1 gilt

$$f\big(\operatorname{Rad}(M)\big) = \operatorname{Rad}\big(f(M)\big) \subseteq \operatorname{Rad}\Big(\prod_{i\in I} S_i\Big) \subseteq \prod_{i\in I} \underbrace{\operatorname{Rad}(S_i)}_{=0} = 0 .$$

(ii) Folgt aus (i).

(iii)

„$\Longrightarrow$“: Sei M endlich erzeugt und halbeinfach. Dann ist $M = Rm_1 + \cdots + Rm_n$ mit endlich vielen $m_1, \ldots, m_n \in M$ und andererseits $M = \bigoplus_{i\in I} M_i$ mit einer Familie $(M_i)_{i\in I}$ einfacher Untermoduln. Es existiert eine *endliche* Teilmenge J von I mit $m_1, \ldots, m_n \in \bigoplus_{i\in J} M_i$. Dann ist aber $M \subseteq \bigoplus_{j\in J} M_j$. Jedes M_j ist artinsch, also auch M. Der Rest folgt aus (ii).

„$\Longleftarrow$“: Sei M artinsch und $\mathrm{Rad}(M) = 0$, o.B.d.A. $M \neq 0$. Dann ist $\mathfrak{M} := \{N : N$ Durchschnitt endlich vieler maximaler Untermoduln von $M\} \neq \emptyset$ (da $M \in \mathfrak{M}$). Folglich enthält $\mathfrak{M}$ ein minimales Element D. Für jeden maximalen Untermodul L von M ist $D \cap L \in \mathfrak{M}$. Also ist $D = D \cap L \subseteq L$ nach Wahl von D. Dies zeigt: $D \subseteq \mathrm{Rad}(M) = 0$. Es existieren also endlich viele maximale Untermoduln $M_1, \ldots, M_n$ von M mit $M_1 \cap \cdots \cap M_n = 0$. Daher ist die Abbildung

$$f : M \to {}^{M}\!/\!_{M_1} \times \cdots \times {}^{M}\!/\!_{M_n}\,, \quad m \mapsto (m + M_1, \ldots, m + M_n)$$

ein R-Monomorphismus. Da ${}^{M}\!/\!_{M_1}, \ldots, {}^{M}\!/\!_{M_n}$ einfach sind, ist ${}^{M}\!/\!_{M_1} \times \cdots \times {}^{M}\!/\!_{M_n}$ noethersch und halbeinfach, also auch M.

(iv) Sei $M \neq 0$ und endlich erzeugt, also $M = Rm_1 + \cdots + Rm_n$ mit $m_1, \ldots, m_n \in M$, n möglichst klein. Dann ist $N := Rm_2 + \cdots + Rm_n \neq M$, also

$$0 \neq {}^{M}\!/\!_{N} = R(m_1 + N)\ .$$

Die Abbildung $f : R \to {}^{M}\!/\!_{N}$, $r \mapsto r(m_1 + N)$, ist ein R-Epimorphismus mit $\mathrm{Ker}(f) \neq R$. Nach Bemerkung 4.2 (ii) existiert ein maximales Linksideal L in R mit $\mathrm{Ker}(f) \subseteq L$. Dann ist ${}^{L}\!/\!_{\mathrm{Ker}(f)}$ ein maximaler Untermodul von ${}^{R}\!/\!_{\mathrm{Ker}(f)}$, also

$$\mathrm{Rad}\left({}^{R}\!/\!_{\mathrm{Ker}(f)}\right) \neq {}^{R}\!/\!_{\mathrm{Ker}(f)}\ .$$

Wegen ${}^{M}\!/\!_{N} \cong {}^{R}\!/\!_{\mathrm{Ker}(f)}$ ist also

$${}^{M}\!/\!_{N} \neq \mathrm{Rad}\left({}^{M}\!/\!_{N}\right) \supseteq {}^{\mathrm{Rad}(M) + N}\!/\!_{N}\ ,$$

d.h. $\mathrm{Rad}(M) \neq M$.

5.3. Satz (Nakayamas Lemma). *Sei N ein Untermodul eines endlich erzeugten R-Moduls M mit $M = N + \mathrm{Rad}(M)$. Dann ist $M = N$.*

Beweis. Aus $M = N + \mathrm{Rad}(M)$ folgt $\mathrm{Rad}\left({}^{M}\!/\!_{N}\right) \supseteq {}^{\mathrm{Rad}(M)+N}\!/\!_{N} = {}^{M}\!/\!_{N}$. Da ${}^{M}\!/\!_{N}$ endlich erzeugt ist, folgt aus Satz 5.2: ${}^{M}\!/\!_{N} = 0$, d.h. $M = N$.

5.4. Satz. *Ein Element m eines endlich erzeugten R-Moduls M liegt genau dann im Radikal von M ($\mathrm{Rad}(M)$), wenn gilt: Für jeden Untermodul N von M mit $M = N + Rm$ ist $M = N$.*

Beweis.

„$\Longrightarrow$“: Sei $m \in \mathrm{Rad}(M)$ und N ein Untermodul mit $M = N + Rm$. Dann ist $M = N + \mathrm{Rad}(M)$, also $M = N$ nach Nakayama.

„$\Longleftarrow$“: Sei $m \in M \setminus \mathrm{Rad}(M)$, also $m \notin N$ für mindestens einen maximalen Untermodul N von M. Dann ist $M = N + Rm$, aber $M \neq N$.

5.5. Definition. Das Radikal des regulären R-Linksmoduls R nennt man auch das **(Jacobson-)Radikal** des Rings R. Man schreibt: $\mathrm{Rad}(R) = J(R)$.

Bemerkungen.

(i) $\mathrm{Rad}(R)$ ist also der Durchschnitt aller maximalen Linksideale von R. Wir werden bald sehen, daß $\mathrm{Rad}(R)$ auch der Durchschnitt aller maximalen Rechtsideale von R ist.

(ii) Nach Satz 5.2 ist $\mathrm{Rad}(R) \neq R$ außer im Fall $R = 0$.

(iii) Für jedes Element m eines R-Moduls M ist die Abbildung $f : R \to M$, $r \mapsto rm$, R-linear. Daher ist $\big(\mathrm{Rad}(R)\big)m = f\big(\mathrm{Rad}(R)\big) \subseteq \mathrm{Rad}(M)$. Dies zeigt $\big(\mathrm{Rad}(R)\big)M \subseteq \mathrm{Rad}(M)$. Insbesondere ist $\big(\mathrm{Rad}(R)\big)R \subseteq \mathrm{Rad}(R)$, d.h. $\mathrm{Rad}(R)$ ist ein (zweiseitiges) Ideal in R.

(iv) Für jedes Ideal I in R ist ${}^{\mathrm{Rad}(R)+I}/_{I} \subseteq \mathrm{Rad}\left({}^{R}/_{I}\right)$ nach Satz 5.1, und im Fall $I \subseteq \mathrm{Rad}(R)$ gilt sogar $\mathrm{Rad}\left({}^{R}/_{I}\right) = {}^{\mathrm{Rad}(R)}/_{I}$. Insbesondere ist $\mathrm{Rad}\left({}^{R}/_{\mathrm{Rad}(R)}\right) = 0$.

(v) Nach Satz 5.2 ist R genau dann halbeinfach, wenn R linksartinsch und $\mathrm{Rad}(R) = 0$ ist.

(vi) Ist R linksartinsch, so ist ${}^{R}/_{\mathrm{Rad}(R)}$ halbeinfach; denn mit R ist auch ${}^{R}/_{\mathrm{Rad}(R)}$ linksartinsch mit $\mathrm{Rad}\left({}^{R}/_{\mathrm{Rad}(R)}\right) = 0$. Also folgt die Behauptung aus (v).

(vii) Ist R linksartinsch, so ist jeder R-Modul M mit $\mathrm{Rad}(R)M = 0$ halbeinfach; man kann nämlich M als ${}^{R}/_{\mathrm{Rad}(R)}$-Modul auffassen. Nach (vi) ist ${}^{R}/_{\mathrm{Rad}(R)}$ halbeinfach, also auch jeder ${}^{R}/_{\mathrm{Rad}(R)}$-Modul. Dann ist M auch als R-Modul halbeinfach.

(viii) Ist R linksartinsch, so ist $\mathrm{Rad}(R)M = \mathrm{Rad}(M)$; denn wegen

$$\mathrm{Rad}(R)\left({}^{M}/_{\mathrm{Rad}(R)M}\right) = 0$$

ist der Modul ${}^{M}/_{\mathrm{Rad}(R)M}$ halbeinfach nach (vii). Aus 5.2 folgt also

$$0 = \mathrm{Rad}\left({}^{M}/_{\mathrm{Rad}(R)M}\right) = {}^{\mathrm{Rad}(M)}/_{\mathrm{Rad}(R)M}\,,$$

d.h. $\mathrm{Rad}(M) = \mathrm{Rad}(R)M$.

Satz.

$$\begin{aligned}\mathrm{Rad}(R) &= \{x \in R : 1 + axb \in U(R)\ \forall a, b \in R\}\\ &= \{x \in R : 1 + ax \in U(R)\ \forall a \in R\}\\ &= \{x \in R : 1 + ax \textit{ linksinvertierbar}\ \forall a \in R\}\\ &= \{x \in R : xS = 0\ \forall \textit{ einfachen } R\textit{-Moduln } S\}\,.\end{aligned}$$

Beweis.

(i) Seien $x \in \mathrm{Rad}(R)$ und $a, b \in R$, also $y := -axb \in \mathrm{Rad}(R)$. Wir zeigen: $1 - y \in U(R)$. Annahme: $R(1-y) \neq R$. Dann existiert ein maximales Linksideal L in R mit $R(1-y) \subseteq L$. Insbesondere ist $1 - y \in L$, und wegen $y \in \mathrm{Rad}(R) \subseteq L$ hat man den Widerspruch $1 \in L$. Also ist $R(1-y) = R$; insbesondere ist $1 = z(1-y)$ für ein $z \in R$, d.h. $1 - z = -zy \in \mathrm{Rad}(R)$. Mit den gleichen Argumenten wie für y existiert ein Element $u \in R$ mit $1 = u\big(1 - (1-z)\big) = uz$. Folglich ist $z \in U(R)$, also auch $1 - y \in U(R)$.

(ii) Sei $x \in R$ mit der Eigenschaft, daß $1+ax$ für alle $a \in R$ linksinvertierbar ist. Annahme: $xs \neq 0$ für einen einfachen R-Modul S. Dann ist $xS \neq 0$ für mindestens ein $s \in S$. Da S einfach ist, ist $Rxs = S$, also $s = rxs$ für ein $r \in R$. Dann ist $0 = (1-rx)s$. Da $1-rx$ linksinvertierbar ist, folgt $s = 0$, Widerspruch.

(iii) Sei $x \in R$ mit $xS = 0$ für alle einfachen R-Moduln S. Für jedes maximale Linksideal M von R ist R/M ein einfacher R-Modul. Also ist $0 = x\left(R/M\right) = xR+M/M$, d.h. $xR \subseteq M$; insbesondere ist $x \in M$. Dies zeigt: $x \in \mathrm{Rad}(R)$.

5.6. Bemerkung. Die erste Beschreibung von $\mathrm{Rad}(R)$ in 5.5 ist unabhängig davon, ob man Linksmoduln oder Rechtsmoduln betrachtet. Daher ist $\mathrm{Rad}(R)$ auch der Durchschnitt aller maximalen Rechtsideale von R und der Annulator aller einfachen R-Rechtsmoduln.

Satz. $\mathrm{Rad}(R)$ *enthält jedes Linksideal (Rechtsideal) N von R, das nur aus nilpotenten Elementen besteht. Insbesondere enthält das Jacobson-Radikal von R stets das Primradikal von R.*

Beweis. Sei $x \in N$ und $a \in R$. Dann ist $y := -ax \in N$, also $y^n = 0$ für ein $n \in \mathbb{N}$. Folglich ist $(1+y+y^2+\cdots+y^{n-1})(1-y) = 1-y^n = 1$, d.h. $1-y = 1+ax$ ist linksinvertierbar. Wende 5.5 an.

5.7. Satz. *Ist R linksartinsch (rechtsartinsch), so ist* $\mathrm{Rad}(R)$ *ein nilpotentes Ideal in R. Folglich stimmen in dieser Situation Jacobson-Radikal und Primradikal überein.*

Beweis. Sei R linksartinsch. Dann existiert $m \in \mathbb{N}$ mit $\mathrm{Rad}(R) =: J \supseteq J^2 \supseteq J^3 \supseteq \cdots \supseteq J^m = J^{m+1} = \cdots$. Wir nehmen $J^m \neq 0$ an. Dann existiert in der Menge aller Linksideale I von R mit $J^m I \neq 0$ ein minimales Element L. Wegen $J^m L \neq 0$ existiert ein $a \in L$ mit $J^m a \neq 0$. Daher ist $J^m a$ ein Linksideal in R mit $J^m a \subseteq L$ und $J^m J^m a = J^{2m} a = J^m a \neq 0$. Nach Wahl von L ist $J^m a = L$. Dann existiert $x \in J^m$ mit $xa = a$. Dann ist $(1-x)a = 0$. Wegen $1-x \in U(R)$ ist also $a = 0$. Widerspruch.

5.8. Satz (Hopkins). *Ist R linksartinsch, so auch linksnoethersch.*

Beweis. Sei $J := \mathrm{Rad}(R)$ und $n \in \mathbb{N}$ mit $J^n = 0$. Für $k = 1, \ldots, n-1$ ist J^{k-1}/J^k ein artinscher R-Modul mit $J\left(J^{k-1}/J^k\right) = J^k/J^k = 0$. Nach Bemerkung 5.5 (vii) ist also J^{k-1}/J^k halbeinfach. Der Beweis von Satz 5.2 (iii) zeigt, daß J^{k-1}/J^k noethersch ist. Daher ist auch R ein noetherscher R-Modul.

6 Lokale Ringe und unzerlegbare Moduln

Sei R ein Ring.

6.1. Satz. *Im Fall $R \neq 0$ sind äquivalent:*

(1) $\mathrm{Rad}(R)$ *ist ein maximales Linksideal in R.*

(2) ${}^{R}/_{\mathrm{Rad}(R)}$ *ist ein Schiefkörper.*

(3) $R = U(R) \cup J(R)$.

(4) Die nichtinvertierbaren Elemente in R bilden ein Ideal.

(5) Die Summe von je zwei nichtinvertierbaren Elementen in R ist nicht invertierbar.

Definition. Gegebenenfalls nennt man R **lokal**.

Beweis.

(1) $\Longrightarrow$ (2): Sei (1) erfüllt. Dann ist 0 maximales Linksideal in ${}^{R}/_{\mathrm{Rad}(R)} =: S$. Für $s \in S \setminus \{0\}$ ist also $Ss = S$; insbesondere existiert ein $t \in S$ mit $ts = 1$. Wegen $t \neq 0$ existiert analog ein $u \in S$ mit $ut = 1$. Daher ist $t \in U(S)$ und $s = t^{-1} \in U(S)$.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt und $x \in R \setminus J(R)$, d.h. $0 \neq x + J(R) \in {}^{R}/_{J(R)}$. Wegen (2) existiert ein $y \in R$ mit $1 + J(R) = \big(x + J(R)\big)\big(y + J(R)\big) = xy + J(R)$. Wir schreiben $xy = 1 + z$ mit $z \in J(R)$. Nach Satz 5.5 ist $1 + z \in U(R)$, also $xy(1+z)^{-1} = 1$. Daher ist x rechtinvertierbar. Analog ist x linksinvertierbar, d.h. $x \in U(R)$.

(3) $\Longrightarrow$ (4): Sei (3) erfüllt. Offenbar ist $U(R) \cap J(R) = \emptyset$. Daher ist $R \setminus U(R) = J(R)$ ein Ideal.

(4) $\Longrightarrow$ (5): Trivial.

(5) $\Longrightarrow$ (1): Sei (5) erfüllt. Wir nehmen an, daß R zwei verschiedene maximale Linksideale L, M besitzt. Dann ist $L + M = R$; insbesondere existieren $x \in L$, $y \in M$ mit $x + y = 1$. Offenbar sind x, y nicht invertierbar, im Widerspruch zu (5). Folglich enthält R genau ein maximales Linksideal L. Folglich ist $L = \mathrm{Rad}(R)$.

Beispiele.

(i) Jeder Schiefkörper ist lokal, $\mathbb{Z}$ dagegen nicht.

(ii) Für jede Primzahl p ist

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\}$$

ein lokaler Ring; denn für $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$ ist $\frac{a}{b} \cdot \frac{b}{a} = 1$, also $\frac{a}{b} \in U(\mathbb{Z}_{(p)})$. Daraus folgt leicht: $U(\mathbb{Z}_{(p)}) = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\}$. Jedes nichtinvertierbare Element in $\mathbb{Z}_{(p)}$ hat also die Form $\frac{x}{y}$ mit $x \in p\mathbb{Z}$, $y \in \mathbb{Z} \setminus p\mathbb{Z}$. Sind auch $x' \in p\mathbb{Z}$ und $y' \in \mathbb{Z} \setminus p\mathbb{Z}$, so ist

$$\frac{x}{y} + \frac{x'}{y'} = \frac{xy' + x'y}{yy'}$$

nicht invertierbar wegen $yy' \in \mathbb{Z} \setminus p\mathbb{Z}$, $xy' + x'y \in p\mathbb{Z}$.

Bemerkung. Sei R lokal und e ein Idempotent in R. Wegen $e + (1 - e) = 1$ ist $e \in U(R)$ oder $1 - e \in U(R)$. Wegen $e(1 - e) = e - e^2 = 0$ ist also $e = 0$ oder $\underbrace{1 - e = 0}_{\Longleftrightarrow e=1}$. In einem lokalen Ring sind also 0 und 1 die einzigen Idempotente.

6.2. Satz. *Für einen R-Modul $M \neq 0$ sind äquivalent:*

(1) Sind M_1, M_2 Untermoduln von M mit $M = M_1 \oplus M_2$, so ist $M_1 = 0$ oder $M_2 = 0$.

(2) 0 und 1 sind die einzigen Idempotente in $\mathrm{End}_R(M)$.

Definition. Gegebenenfalls nennt man M **unzerlegbar**.

Beweis.

(1) $\Longrightarrow$ (2): Sei (1) erfüllt und e ein Idempotent in $\mathrm{End}_R(M)$. Dann sind $\mathrm{Bld}(e)$ und $\mathrm{Ker}(e)$ Untermoduln von M mit $M = \mathrm{Ker}(e) \oplus \mathrm{Bld}(e)$; ist nämlich $x \in \mathrm{Bld}(e) \cap \mathrm{Ker}(e)$ und schreibt man $x = e(y)$ mit $y \in M$, so ist $0 = e(x) = e^2(y) = e(y) = x$. Daher ist $\mathrm{Bld}(e) \cap \mathrm{Ker}(e) = 0$. Ferner gilt für $m \in M$:

$$e\big(m - e(m)\big) = e(m) - e^2(m) = 0\ ,$$

d.h. $m - e(m) \in \mathrm{Ker}(e)$ und $m = m - e(m) + e(m) \in \mathrm{Ker}(e) + \mathrm{Bld}(e)$. Daher ist tatsächlich $M = \mathrm{Ker}(e) \oplus \mathrm{Bld}(e)$. Aus (1) folgt also $\mathrm{Bld}(e) = 0$ oder $\mathrm{Ker}(e) = 0$. Im ersten Fall ist $e = 0$, und im zweiten Fall ist $\mathrm{Bld}(e) = M$, d.h. e ist bijektiv. Wegen $e^2 = e$ ist also $e = \mathrm{id}_M$.

(2) $\Longrightarrow$ (1): Sei (2) erfüllt und $M = M_1 \oplus M_2$ mit Untermoduln M_1, M_2 von M. Wir bezeichnen die entsprechenden Projektoren und Injektoren mit p_1, p_2 bzw. q_1, q_2. Dann sind $e_1 := q_1 \circ p_1$ und $e_2 := q_2 \circ p_2$ Idempotente in $\mathrm{End}_R(M)$ mit $e_1 + e_2 = \mathrm{id}_M$. Wegen (2) folgt $e_1 = 0$ oder $e_2 = 0$, o.B.d.A. $e_1 = 0$. Dann ist $0 = e_1(M) = p_1(M) = M_1$.

Bemerkungen.

(i) Ist $\mathrm{End}_R(M)$ ein lokaler Ring, so ist M unzerlegbar. Gegebenenfalls nennt man M **streng unzerlegbar**. Nicht jeder unzerlegbare Modul ist streng unzerlegbar (z.B. $R = \mathbb{Z} = M$).

(ii) Nach (i) und Schurs Lemma ist jeder einfache R-Modul (streng) unzerlegbar. Die Umkehrung gilt im allgemeinen nicht.

(iii) Die folgenden Aussagen dienen als Vorbereitung auf einen Eindeutigkeitssatz für Zerlegungen in unzerlegbare Moduln.

6.3. Satz. *Sei $(M_i)_{i\in I}$ eine Familie streng unzerlegbarer Untermoduln eines R-Moduls M mit $M = \bigoplus_{i\in I} M_i$. Sind $f_1, f_2 \in \mathrm{End}_R(M)$ mit $\mathrm{id}_M = f_1 + f_2$, so existiert zu jedem $j \in I$ ein $k \in \{1, 2\}$ mit der Eigenschaft, daß $f_k|_{M_j}$ injektiv und $M = f_k(M_j) \oplus \bigoplus_{i\in I\setminus\{j\}} M_i$ ist.*

Beweis. Sei $j \in I$ fest, $p_j : M \to M_j$ Projektor, $q_j : M_j \to M$ Injektor. Dann ist

$$\mathrm{id}_{M_j} = p_j \circ q_j = p_j \circ \mathrm{id}_M \circ q_j = p_j \circ f_1 \circ q_j + p_j \circ f_2 \circ q_j$$

mit $p_j \circ f_1 \circ q_j, p_j \circ f_2 \circ q_j \in \mathrm{End}_R(M_j)$. Da $\mathrm{End}_R(M_j)$ lokal ist, ist $p_j \circ f_1 \circ q_j$ oder $p_j \circ f_2 \circ q_j$ invertierbar, d.h. bijektiv. O.B.d.A. sei $p_j \circ f_1 \circ q_j$ bijektiv. Dann ist $\underbrace{f_1 \circ q_j}_{=f_1|_{M_j}}$ injektiv. Sei $x \in f_1(M_j) \cap \bigoplus_{i\in I\setminus\{j\}} M_i$, also $x = f_1(y)$ mit $y \in M_j$. Dann ist

$$0 = p_j(x) = p_j\big(f_1(y)\big) = (p_j \circ f_1 \circ q_j)(y) \ ,$$

also $y = 0$ und $x = f_1(y) = 0$. Damit gilt $f_1(M_j) \cap \bigoplus_{i\in I\setminus\{j\}} M_i = 0$. Für $m \in M$ ist $p_j(m) \in M_j$, also $p_j(m) = (p_j \circ f_1 \circ q_j)(m_j)$ für ein $m_j \in M_j$. Dann ist

$$m - (f_1 \circ q_j)(m_j) \in \mathrm{Ker}(p_j) = \bigoplus_{i\in I\setminus\{j\}} M_i$$

und

$$m = f_1\big(q_j(m_j)\big) + \Big(m - f_1\big(q_j(m_j)\big)\Big) \in f_1(M_j) + \bigoplus_{i\in I\setminus\{j\}} M_i \ .$$

Damit ist die Behauptung bewiesen.

6.4. Satz. *Sei $(M_i)_{i\in I}$ eine Familie streng unzerlegbarer Untermoduln eines R-Moduls M mit $M = \bigoplus_{i\in I} M_i$. Außerdem seien $f_1, f_2 \in \mathrm{End}_R(M)$ mit $\mathrm{id}_M = f_1 + f_2$. Zu paarweise verschiedenen $j_1, \dots, j_t \in I$ existieren dann $k_1, \dots, k_t \in \{1, 2\}$ mit der Eigenschaft, daß $f_{k_1}|_{M_{j_1}}, \dots, f_{k_t}|_{M_{j_t}}$ injektiv sind und*

$$M = f_{k_1}(M_{j_1}) \oplus \cdots \oplus f_{k_t}(M_{j_t}) \oplus \bigoplus_{i\in I\setminus\{j_1,\dots,j_t\}} M_i$$

gilt.

Beweis. Nach Satz 6.3 existiert zunächst ein $k_1 \in \{1, 2\}$ mit der Eigenschaft, daß $f_{k_1}|_{M_{j_1}}$ injektiv und $M = f_{k_1}(M_{j_1}) \oplus \bigoplus_{i\in I\setminus\{j_1\}} M_i$ ist. Wegen $M_{j_1} \cong f_{k_1}(M_{j_1})$ ist auch $\mathrm{End}_R\big(f_{k_1}(M_{j_1})\big)$ lokal. Daher kann man auf diese Zerlegung Satz 6.3 wieder anwenden. Es existiert also ein $k_2 \in \{1, 2\}$ mit der Eigenschaft, daß $f_{k_2}|_{M_{j_2}}$ injektiv und $M = f_{k_1}(M_{j_1}) \oplus f_{k_2}(M_{j_2}) \oplus \bigoplus_{i\in I\setminus\{j_1,j_2\}} M_i$ ist. Auf diese Weise fährt man fort.

6.5. Satz. *Sei $(M_i)_{i\in I}$ eine Familie streng unzerlegbarer Untermoduln eines R-Moduls M mit $M = \bigoplus_{i\in I} M_i$. Außerdem sei $M = A \oplus B$ mit Untermoduln A, B von M, wobei A unzerlegbar und $p : M \to A$ der entsprechende Projektor ist. Dann existiert ein $j \in I$ mit der Eigenschaft, daß $p|_{M_j}$ ein R-Isomorphismus und $M = M_j \oplus B$ ist.*

Beweis. Sei $q : A \to M$ der entsprechende Injektor. Dann ist $e = q \circ p$ ein Idempotent in $\mathrm{End}_R(M)$ und $\mathrm{id}_M = e + (1 - e)$. Wir setzen $f_1 := e$ und $f_2 := 1 - e$. Wegen $A \neq 0$ existiert ein Element $a \in A \setminus \{0\}$. Wir schreiben $a = \sum_{i\in I} a_i$ mit $a_i \in M_i$ für alle i; dabei ist $\{i \in I : a_i \neq 0\}$ endlich, etwa $\{i \in I : a_i \neq 0\} = \{j_1, \dots, j_t\}$. Nach Satz 6.4 existieren $k_1, \dots, k_t \in \{1, 2\}$ mit der Eigenschaft, daß $f_{k_1}|_{M_{j_1}}, \dots, f_{k_t}|_{M_{j_t}}$ injektiv sind und

$$M = f_{k_1}(M_{j_1}) \oplus \cdots \oplus f_{k_t}(M_{j_t}) \oplus \bigoplus_{i\in I\setminus\{j_1,\dots,j_t\}} M_i$$

gilt. Wir nehmen an: $k_1 = \cdots = k_t = 2$. Dann ist

$$\begin{aligned} 0 = (\mathrm{id}_M - e)(a) &= (\mathrm{id}_M - e)\Big(\sum_{i \in I} a_i\Big) \\ &= \sum_{s=1}^{t} (\mathrm{id}_M - e)(a_{j_s}) = \sum_{s=1}^{t} f_{k_s}(a_{j_s}) \; . \end{aligned}$$

Die obige Zerlegung ergibt also $0 = f_{k_1}(a_{j_1}) = \cdots = f_{k_t}(a_{j_t})$ und $a_{j_1} = \cdots = a_{j_t} = 0$ im Widerspruch zu $a = a_{j_1} + \cdots + a_{j_t}$. Folglich existiert ein $s \in \{1, \ldots, t\}$ mit $k_s = 1$. Wir setzen $j := j_s$. Dann ist $e|_{M_j}$ injektiv und $M = e(M_j) \oplus L$ mit einem Untermodul L von M. Folglich ist $p|_{M_j}$ injektiv und $e(M_j) = p(M_j) \subseteq A$; also ist

$$A = M \cap A = \big(p(M_j) + L\big) \cap A \overset{Dedekind}{=} p(M_j) + (L \cap A) = p(M_j) \oplus (L \cap A) \; .$$

Da A unzerlegbar und $p(M_j) \neq 0$ ist, folgt $A = p(M_j)$. Daher ist $p|_{M_j}$ ein R-Isomorphismus. Zum Beweis von $M = M_j \oplus B$ sei $x \in M_j \cap B$. Dann ist $p(x) = 0$. Da $p|_{M_j}$ injektiv ist, folgt $x = 0$. Für $m \in M$ ist andererseits $p(m) \in A = p(M_j)$. Daher existiert ein $m_j \in M_j$ mit $p(m) = p(m_j)$. Folglich ist $m - m_j \in \mathrm{Ker}(p) = B$ und $m = m_j + m - m_j \in M_j + B$. Damit ist $M = M_j \oplus B$.

6.6. Satz (Azumaya-Krull-Remak-Schmidt). *Seien $(M_i)_{i \in I}$ und $(N_j)_{j \in J}$ Familien unzerlegbarer Untermoduln eines R-Moduls M mit $M = \bigoplus_{i \in I} M_i = \bigoplus_{j \in J} N_j$. Für $i \in I$ sei M_i streng unzerlegbar. Dann existiert eine Bijektion $\beta : I \to J$ mit $M_i \cong N_{\beta(i)}$ für alle i.*

Beweis. Nach Satz 6.5 ist jedes N_j zu einem M_i isomorph. Daher ist auch $\mathrm{End}_R(N_j)$ lokal, d.h. N_j ist auch streng unzerlegbar. Daher sind die Voraussetzungen symmetrisch in beiden Zerlegungen. Wir definieren eine Äquivalenzrelation $\sim$ auf I durch $i \sim i' \iff M_i \cong M_{i'}$. Für $i \in I$ sei $\bar{i}$ die entsprechende Äquivalenzklasse. Ferner sei $\bar{I}$ die Menge aller Äquivalenzklassen $\bar{i}$. Analoge Bezeichnungen führen wir auf J ein.
Nach Satz 6.5 existiert zu jedem $i \in I$ ein $j \in J$ mit $M_i \cong N_j$. Wir setzen $\Phi(\bar{i}) := \bar{j}$ und erhalten so eine wohldefinierte bijektive Abbildung $\Phi : \bar{I} \to \bar{J}$. Es genügt zu zeigen, daß für $i \in I$ eine Bijektion $\beta_i : \bar{i} \to \Phi(\bar{i})$ existiert. Wir zeigen nur, daß für $i \in I$ eine Injektion $\Phi(\bar{i}) \to \bar{i}$ existiert. (Aus Symmetriegründen existiert dann analog eine Injektion $\bar{i} \to \Phi(\bar{i})$, und aus dem Satz von Schröder-Bernstein (Mengenlehre) folgt dann die Existenz einer Bijektion $\bar{i} \to \Phi(\bar{i})$.) Wir unterscheiden zwei Fälle:

Fall 1: $\bar{i}$ endlich.

Seien $j_1, \ldots, j_t \in \Phi(\bar{i})$ paarweise verschieden. Nach Satz 6.5 existiert ein $i_1 \in I$ mit $N_{j_1} \cong M_{i_1}$ und $M \cong M_{i_1} \oplus \bigoplus_{j \in J \setminus \{j_1\}} N_j$. Nach Satz 6.5 existiert analog ein $i_2 \in I$ mit $N_{j_2} \cong M_{i_2}$ und $M = M_{i_1} \oplus M_{i_2} \oplus \bigoplus_{j \in J \setminus \{j_1, j_2\}} N_j$. Auf diese Weise fahren wir fort und erhalten $i_1, \ldots, i_t \in I$ mit $N_{j_1} \cong M_{i_1}, N_{j_2} \cong M_{i_2}, \ldots, N_{j_t} \cong M_{i_t}$ und

$$M = M_{i_1} \oplus \cdots \oplus M_{i_t} \oplus \bigoplus_{j \in J \setminus \{j_1, \ldots, j_t\}} N_j \; .$$

Da diese Summe direkt ist, sind $i_1, \ldots, i_t$ paarweise verschieden. Daher ist $|\bar{i}| \geq t$. Folglich ist $\Phi(\bar{i})$ endlich und $|\bar{i}| \geq |\Phi(\bar{i})|$.

Fall 2: $\bar{i}$ ist unendlich.

Für $j \in J$ sei $p'_j : M \to N_j$ der entsprechende Projektor, und für jedes $k \in I$ sei

$E(k) := \{j \in J : p'_j|_{M_k}$ ist ein R-Isomorphismus$\}$. Wir zeigen zunächst, daß $E(k)$ stets endlich ist. Dazu wählen wir ein festes Element $m \in M_k \setminus \{0\}$ und schreiben $m = \sum_{j \in J} n_j$ mit $n_j \in N_j$ für alle j. Dabei ist $J_0 := \{j \in J : n_j \neq 0\}$ endlich. Für $j \in E(k)$ ist $0 \neq p'_j(m) = n_j$, d.h. $j \in J_0$. Daher ist $E(k) \subseteq J_0$; insbesondere ist $E(k)$ endlich.
Als nächstes zeigen wir, daß $\Phi(\bar{i}) = \bigcup_{k \in \bar{i}} E(k)$ ist. Für $k \in \bar{i}$ und $j \in E(k)$ ist nämlich $M_i \cong M_k \cong N_j$, d.h. $j \in \Phi(\bar{i})$. Für $j \in \Phi(\bar{i})$ ist umgekehrt $M_i \cong N_j$. Nach Satz 6.5 existiert ferner ein $k \in I$ mit der Eigenschaft, daß $p'_j|_{M_k}$ ein R-Isomorphismus ist; insbesondere ist $M_k \cong N_j \cong M_i$, also $k \in \bar{i}$ und $j \in E(k)$. Daher existiert eine Injektion $\Phi(\bar{i}) \to \bar{i} \times \mathbb{N}$. In der Mengenlehre zeigt man aber, daß eine Bijektion zwischen $\bar{i}$ und $\bar{i} \times \mathbb{N}$ existiert. Daher existiert eine Injektion $\Phi(\bar{i}) \to \bar{i}$, und wir sind fertig.

Bemerkungen. Zur Mengenlehre:

(i) Zunächst zeigen wir, daß für jede unendliche Menge X eine Bijektion $X \times \mathbb{N} \to X$ existiert. Dies ist bekanntlich richtig, falls X abzählbar ist. Im allgemeinen Fall ist also

$$F := \{f : Y \times \mathbb{N} \to Y \mid Y \subseteq X, f \text{ bijektiv}\}$$

nicht leer, da X eine abzählbare Teilmenge enthält. Wir definieren eine Ordnung $\leq$ auf F durch: $f \leq g :\Longleftrightarrow g$ Fortsetzung von f. Es ist leicht zu sehen, daß jede total geordnete Teilmenge von F eine obere Schranke besitzt. Nach Zorn enthält F ein maximales Element $g : Z \times \mathbb{N} \to Z$. Im Fall $Z = X$ sind wir fertig. Sei also $Z \neq X$. Wir nehmen an, daß $X \setminus Z$ unendlich ist. Dann existiert eine abzählbare Teilmenge Z' von $X \setminus Z$. Ferner existiert eine Bijektion $g' : Z' \times \mathbb{N} \to Z'$. Daher kann man g zu einer Bijektion $(Z \cup Z') \times \mathbb{N} \to Z \cup Z'$ fortsetzen im Widerspruch zur Maximalität von g. Sei also $X \setminus Z$ endlich. Dann existiert eine Bijektion $h : Z \to X$. Diese induziert eine Bijektion $h' : Z \times \mathbb{N} \to X \times \mathbb{N}$. Wir erhalten also eine Bijektion $X \times \mathbb{N} \xrightarrow{h'^{-1}} Z \times \mathbb{N} \xrightarrow{g} Z \xrightarrow{h} X$.

(ii) **Satz von Schröder-Bernstein:** Hat man Injektionen $f : X \to Y$ und $g : Y \to X$, so existiert eine Bijektion $h : X \to Y$.
Zum Beweis: Für $x = x_0 \in X$ sei y_0 das Urbild von x unter g (falls es existiert), x_1 das Urbild von y_0 unter f (falls es existiert), y_1 das Urbild von x_1 unter g (falls es existiert), usw. Es gibt folgende Möglichkeiten: Die Folge $x_0, y_0, x_1, y_1, \ldots$ ist unendlich, oder sie bricht bei einem $x_k \in X$ ab, oder sie bricht bei einem $y_l \in Y$ ab. Mit X_∞, X_X und X_Y bezeichnen wir die entsprechenden Teilmengen von X. Analog definieren wir Teilmengen Y_∞, Y_X und Y_Y von Y. Man zeigt leicht, daß

$$\begin{aligned} X_\infty &\to Y_\infty\,, & x &\mapsto f(x)\,, \\ X_X &\to Y_X\,, & x &\mapsto f(x) \text{ und} \\ Y_Y &\to X_Y\,, & y &\mapsto g(y) \end{aligned}$$

Bijektionen sind. Zusammen erhält man also eine Bijektion $X \to Y$.

6.7. Satz (Fittings Lemma). *Sei M ein artinscher und noetherscher R-Modul und $f \in \mathrm{End}_R(M)$. Dann existiert ein $k \in \mathbb{N}$ mit folgenden Eigenschaften:*

(i) $M \supseteq \mathrm{Bld}(f) \supseteq \mathrm{Bld}(f^2) \supseteq \cdots \supseteq \mathrm{Bld}(f^k) = \mathrm{Bld}(f^{k+1}) = \cdots$.

(ii) $0 \subseteq \operatorname{Ker}(f) \subseteq \operatorname{Ker}(f^2) \subseteq \cdots \subseteq \operatorname{Ker}(f^k) = \operatorname{Ker}(f^{k+1}) = \cdots$.

(iii) $M = \operatorname{Ker}(f^k) \oplus \operatorname{Bld}(f^k)$.

Beweis. Da M artinsch ist, bricht die Folge der Untermoduln $M \supseteq \operatorname{Bld}(f) \supseteq \operatorname{Bld}(f^2) \supseteq \cdots$ ab. Da M noethersch ist, bricht analog die Folge $0 \subseteq \operatorname{Ker}(f) \subseteq \operatorname{Ker}(f^2) \subseteq \cdots$ ab. Daher existiert ein k mit (i) und (ii).
Sei $x \in \operatorname{Ker}(f^k) \cap \operatorname{Bld}(f^k)$. Wir schreiben $x = f^k(y)$ mit $y \in M$. Dann ist $0 = f^k(x) = f^{2k}(y)$, d.h. $y \in \operatorname{Ker}(f^{2k}) = \operatorname{Ker}(f^k)$. Daher ist $0 = f^k(y) = x$. Daher ist $\operatorname{Ker}(f^k) \cap \operatorname{Bld}(f^k) = 0$. Sei $m \in M$. Dann ist $f^k(m) \in \operatorname{Bld}(f^k) = \operatorname{Bld}(f^{2k})$, also $f^k(m) = f^{2k}(n)$ für ein $n \in M$. Folglich ist $0 = f^k\big(m - f^k(n)\big)$, d.h. $m - f^k(n) \in \operatorname{Ker}(f^k)$ und

$$m = \underbrace{m - f^k(n)}_{\in \operatorname{Ker}(f^k)} + \underbrace{f^k(n)}_{\in \operatorname{Bld}(f^k)} \in \operatorname{Ker}(f^k) + \operatorname{Bld}(f^k)\ .$$

6.8. Satz. *Sei M ein R-Modul, der artinsch, noethersch und unzerlegbar ist. Dann ist jeder R-Endomorphismus von M entweder invertierbar oder nilpotent, und* $\operatorname{End}_R(M)$ *ist lokal, d.h. M ist streng unzerlegbar.*

Beweis. Sei $f \in \operatorname{End}_R(M)$, also $M = \operatorname{Ker}(f^k) \oplus \operatorname{Bld}(f^k)$ für ein $k \in \mathbb{N}$ nach Satz 6.7. Da M unzerlegbar ist, folgt $\operatorname{Ker}(f^k) = 0$ oder $\operatorname{Bld}(f^k) = 0$. Im Fall $\operatorname{Ker}(f^k) = 0$ ist $M = \operatorname{Bld}(f^k)$, d.h. f^k ist bijektiv. Dann ist auch f bijektiv. Im Fall $\operatorname{Bld}(f^k) = 0$ ist $f^k = 0$, d.h. f ist nilpotent.
Seien $f, g \in \operatorname{End}_R(M)$ nichtinvertierbar. Wir zeigen, daß auch $f + g$ nichtinvertierbar ist. Andernfalls ist $\operatorname{id}_M = f' + g'$ mit $f' = (f+g)^{-1} \circ f$, $g' := (f+g)^{-1} \circ g$. Andererseits sind f', g' nichtinvertierbar, also nilpotent. Nach Bemerkung 1.5 (ii) sind $f' = \operatorname{id}_M - g'$, $g' = \operatorname{id}_M - f'$ invertierbar. Widerspruch!

6.9. Satz. *Jeder R-Modul M, der artinsch oder noethersch ist, besitzt eine Zerlegung $M = M_1 \oplus \cdots \oplus M_n$ in endlich viele unzerlegbare Untermoduln $M_1, \ldots, M_n$.*

Beweis. Sei M artinsch und $\mathfrak{M}$ die Menge aller Untermoduln von M, die sich nicht als direkte Summe endlich vieler unzerlegbarer Untermoduln schreiben lassen. Wir nehmen $\mathfrak{M} \neq \emptyset$ an. Dann enthält $\mathfrak{M}$ ein minimales Element N. Es ist $N \neq 0$, und N ist nicht unzerlegbar, etwa $N = N_1 \oplus N_2$ mit echten Untermoduln N_1, N_2 von N. Für $i = 1, 2$ ist $N_i \notin \mathfrak{M}$, d.h. N_i läßt sich als direkte Summe endlich vieler unzerlegbarer Untermoduln schreiben. Folglich läßt sich auch N als direkte Summe von endlich vielen unzerlegbaren Untermoduln schreiben. Widerspruch!
Sei M noethersch und $\mathfrak{M}$ die Menge aller Untermoduln N von M mit der Eigenschaft, daß sich M/N nicht als direkte Summe von endlich vielen unzerlegbaren Untermoduln schreiben läßt. Wir nehmen $\mathfrak{M} \neq \emptyset$ an. Dann enthält $\mathfrak{M}$ ein maximales Element N. Es ist $M/N \neq 0$ und M/N ist zerlegbar, d.h. $M/N = M_1/N \oplus M_2/N$ mit Untermoduln M_1, M_2 von M, die N echt enthalten. Für $i = 1, 2$ ist $M_i \notin \mathfrak{M}$, d.h. M/M_i läßt sich schreiben als direkte Summe endlich vieler unzerlegbarer Untermoduln. Wegen $M/M_1 \cong {}^{M/N}/_{M_1/N} \cong M_2/N$ und $M/M_2 \cong M_1/N$ sind auch M_1/N, M_2/N direkte Summen endlich vieler unzerlegbarer Untermoduln, also auch M/N. Widerspruch!

Bemerkung. Ist M artinsch und noethersch, so folgt aus 6.6 und 6.8, daß M eine im wesentlichen eindeutige Zerlegung $M = M_1 \oplus \cdots \oplus M_n$ in endlich viele unzerlegbare Untermoduln besitzt. Ist M lediglich artinsch, so braucht die Zerlegung nicht eindeutig zu sein; dies wurde erst kürzlich gezeigt.

7 Freie und projektive Moduln

Sei R ein Ring.

7.1. Definition. Eine Teilmenge X eines R-Moduls nennt man **linear unabhängig** (über R), falls gilt: Ist $(r_x)_{x\in X}$ eine Familie von Elementen $r_x \in R$ mit $|\{x : r_x \neq 0\}| < \infty$ und $\sum_{x\in X} r_x x = 0$, so ist $r_x = 0$ für alle $x \in X$. Andernfalls nennt man X **linear abhängig** (über R).

Bemerkungen.

(i) Ist X linear unabhängig, so auch jede Teilmenge von X.

(ii) Ist jede endliche Teilmenge von X linear unabhängig, so auch X.

(iii) $\emptyset$ ist stets linear unabhängig.

(iv) Für $a, n \in \mathbb{N}$ ist $n(a + n\mathbb{Z}) = 0$ in $\mathbb{Z}/n\mathbb{Z}$. Daher ist $\emptyset$ die einzige über $\mathbb{Z}$ linear unabhängige Teilmenge von $\mathbb{Z}/n\mathbb{Z}$.

7.2. Definition. Sei M ein R-Modul. Ein linear unabhängiges Erzeugendensystem von M nennt man auch **Basis** von M (über R). Besitzt M eine Basis, so nennt man M **frei**.

Beispiele.

(a) Der Nullmodul ist stets frei mit Basis $\emptyset$.

(b) Für $n \in \mathbb{N}$ bilden $e_1 := (1, 0, \dots, 0), e_2 := (0, 1, 0, \dots, 0), \dots, e_n := (0, \dots, 0, 1)$ eine Basis von R_n.
Allgemeiner ist für jede (nichtleere) Menge I die Menge $\{e_i : i \in I\}$ eine Basis von $\coprod_{i\in I} R$, dabei ist $e_i(j) = \delta_{ij} 1_R$ für $i, j \in I$. Man nennt $\{e_i : i \in I\}$ die **Standardbasis** (**kanonische Basis**) von $\coprod_{i\in I} R$.

(c) Ist R ein Schiefkörper, so besitzt jeder R-Modul eine Basis; denn R ist halbeinfach, d.h. jeder R-Modul ist eine direkte Summe von einfachen R-Moduln, und jeder einfache R-Modul ist zu R isomorph.

Bemerkungen.

(i) Nicht jeder Modul besitzt eine Basis!

(ii) Freie R-Moduln können durchaus Basen verschiedener Länge haben!

(iii) Ist M ein freier R-Modul mit Basis B, so ist die Abbildung

$$\coprod_{b\in B} R \to M\ , \quad (r_b)_{b\in B} \mapsto \sum_{b\in B} r_b b\ ,$$

ein R-Isomorphismus.

Satz. *Jede Basis eines endlich erzeugten freien R-Moduls M ist endlich.*

Beweis. Sei $M = Rm_1 + \cdots + Rm_n$ und B eine Basis von M. Dann existiert eine endliche Teilmenge C von B mit der Eigenschaft, daß $m_1, \dots, m_n$ Linear-Kombinationen von Elementen in C sind. Daher wird M auch von C erzeugt, d.h. $C = B$.

7.3. Satz. *Jeder R-Modul M ist zu einem Faktormodul eines freien R-Moduls isomorph.*

Beweis. Sei E ein Erzeugendensystem von M (notfalls $E = M$). Dann ist $F = \coprod_{e \in E} R$ ein freier R-Modul, und die Abbildung $f : F \to M$, $(r_e)_{e \in E} \mapsto \sum_{e \in E} r_e e$ ist ein R-Epimorphismus. Daher ist $M \cong F/\mathrm{Ker}(f)$.

Bemerkung. Der Beweis zeigt auch, daß ein endlich erzeugter R-Modul M zu einem Faktormodul eines endlich erzeugten freien R-Moduls isomorph ist.

7.4. Definition. Eine Folge $L \xrightarrow{f} M \xrightarrow{g} N$ von R-Homomorphismen f, g nennt man **exakt**, falls $\mathrm{Bld}(f) = \mathrm{Ker}(g)$ ist. Eine (endliche oder unendliche) Folge von R-Homomorphismen der Form $\ldots \longrightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \longrightarrow \ldots$ nennt man **exakt**, wenn jede Teilfolge der Form $M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1}$ exakt ist. Eine exakte Folge der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ nennt man eine **kurze exakte Folge** (**Sequenz**).

Bemerkungen.

(i) Eine Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M$ ist genau dann exakt, wenn $\mathrm{Ker}(f) = 0$, d.h. wenn f injektiv ist.

(ii) Eine Folge von R-Homomorphismen der Form $M \xrightarrow{g} N \longrightarrow 0$ ist genau dann exakt, wenn $\mathrm{Bld}(g) = N$, d.h. wenn g surjektiv ist.

(iii) Eine Folge von R-Homomorphismen der Form $0 \longrightarrow M \xrightarrow{g} N \longrightarrow 0$ ist also genau dann exakt, wenn g bijektiv ist.

(iv) Eine Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ ist genau dann exakt, wenn f injektiv, g surjektiv und $\mathrm{Bld}(f) = \mathrm{Ker}(g)$ ist. Gegebenenfalls gilt nach dem Homomorphiesatz

$$N \cong M/\mathrm{Ker}(g) = M/\mathrm{Bld}(f) \qquad \text{und} \qquad \mathrm{Bld}(f) \cong L\,.$$

7.5. Satz. *Für eine kurze exakte Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ sind äquivalent:*

(1) Es existiert ein R-Homomorphismus $g' : N \to M$ mit $g \circ g' = \mathrm{id}_N$.

(2) Es existiert ein R-Homomorphismus $f' : M \to L$ mit $f' \circ f = \mathrm{id}_L$.

(3) Es existiert ein Untermodul U von M mit $M = \underbrace{\mathrm{Bld}(f)}_{\mathrm{Ker}(g)} \oplus U$.

Bemerkung. Gegebenenfalls sagt man, daß die kurze exakte Folge $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ **zerfällt**. Der Beweis wird zeigen, daß dann gilt:

$$M = \mathrm{Bld}(f) \oplus \mathrm{Ker}(f') = \mathrm{Ker}(g) + \mathrm{Bld}(g')\,.$$

Beweis.

(1) $\Longrightarrow$ (3): Sei (1) erfüllt. Für $m \in M$ ist dann

$$g\Big(m - g'\big(g(m)\big)\Big) = g(m) - \underbrace{(g \circ g')}_{=\mathrm{id}_N}\big(g(m)\big) = g(m) - g(m) = 0 ,$$

d.h. $m - g'\big(g(m)\big) \in \mathrm{Ker}(g)$ und

$$m = \underbrace{m - g'\big(g(m)\big)}_{\in \mathrm{Ker}(g)} + \underbrace{g'\big(g(m)\big)}_{\in \mathrm{Bld}(g')} .$$

Daher ist $M = \mathrm{Ker}(g) + \mathrm{Bld}(g')$. Ist $x \in \mathrm{Ker}(g) \cap \mathrm{Bld}(g')$ und $x = g'(y)$ mit $y \in N$, so ist $0 = g(x) = g\big(g'(y)\big) = y$, also $x = g'(y) = 0$. Daher ist $\mathrm{Ker}(g) \cap \mathrm{Bld}(g') = 0$, d.h. $M = \mathrm{Ker}(g) \oplus \mathrm{Bld}(g')$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt und $h : U \to N$ die Einschränkung von g. Wegen $M = \mathrm{Ker}(g) \oplus U$ ist h bijektiv. Die Abbildung $g' : N \to M$, $n \mapsto h^{-1}(n)$, ist ein R-Homomorphismus mit $g\big(g'(n)\big) = h\big(h^{-1}(n)\big) = n$ für $n \in N$.

(2) $\Longleftrightarrow$ (3): analog.

Beispiel. Für beliebige R-Moduln M_1, M_2 zerfällt die exakte Folge $0 \longrightarrow M_1 \xrightarrow{q_1} M_1 \times M_2 \xrightarrow{p_2} M_2 \longrightarrow 0$. Dabei sind p_1, p_2 und q_1, q_2 die entsprechenden Projektoren bzw. Injektoren.

7.6. Satz. *Für einen R-Modul P sind äquivalent:*

(1) P ist zu einem direkten Summanden eines freien R-Moduls isomorph.

(2) Zu jedem R-Epimorphismus $f : M \to N$ und jedem R-Homomorphismus $g : P \to N$ existiert ein R-Homomorphismus $h : P \to M$ mit $g = f \circ h$.

$$\begin{tikzcd}
& P \arrow[d, "g"] \arrow[dl, dashed, "h"'] & \\
M \arrow[r, "f"] & N \arrow[r] & 0
\end{tikzcd}$$

(3) Jede kurze exakte Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ zerfällt.

Definition. Gegebenenfalls nennt man P **projektiv**.

Beweis.

(1) $\Longrightarrow$ (2): Sei (1) erfüllt und o.B.d.A. P selbst ein direkter Summand eines freien R-Moduls F, d.h. $F = P \oplus Q$ für einen Untermodul Q von F. Die entsprechenden Projektoren und Injektoren seien p_1, p_2 und q_1, q_2. Außerdem wählen wir eine Basis B von F. Für $b \in B$ existiert wegen der Surjektivität von f ein Element $m_b \in M$ mit $g\big(p_1(b)\big) = f(m_b)$. Wir definieren eine Abbildung $k : F \to M$ durch

$$k\Big(\sum_{b \in B} r_b b\Big) := \sum_{b \in B} r_b \cdot m_b .$$

$$\begin{tikzcd}
 & F \arrow[d, "p_1"] \arrow[ddl, dashed, "k"'] & \\
 & P \arrow[d, "g"] \arrow[dl, dashed, "h"'] & \\
M \arrow[r, "f"] & N \arrow[r] & 0
\end{tikzcd}$$

Offenbar ist k ein R-Homomorphismus mit $f \circ k = g \circ p_1$. Für die Einschränkung $h : P \to M$ von k und $x \in P$ gilt also:

$$f\big(h(x)\big) = f\big(k(x)\big) = g\big(p_1(x)\big) = g(x) \ .$$

(2) $\Longrightarrow$ (3): Sei (2) erfüllt und $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ eine exakte Folge von R-Homomorphismen. Dann existiert ein R-Homomorphismus $h : P \to M$ mit $g \circ h = \mathrm{id}_P$.

$$\begin{tikzcd}
 & P \arrow[d, "\mathrm{id}_P"] \arrow[dl, dashed, "h"'] & \\
M \arrow[r, "g"] & P \arrow[r] & 0
\end{tikzcd}$$

Also zerfällt die Folge.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt. Nach 7.3 existiert ein freier R-Modul F und ein R-Epimorphismus $g : F \to P$. Wegen (3) zerfällt die exakte Folge $0 \longrightarrow \mathrm{Ker}(g) \hookrightarrow F \xrightarrow{g} P \longrightarrow 0$. Es existiert also ein R-Homomorphismus $g' : P \to F$ mit $g \circ g' = \mathrm{id}_P$. Nach Satz 7.5 ist $F \cong \mathrm{Ker}(g) \oplus \mathrm{Bld}(g')$. Wegen $g \circ g' = \mathrm{id}_P$ ist g' injektiv, also $P \cong \mathrm{Bld}(g')$.

Bemerkungen.

(i) Der obige Beweis und Bemerkung 7.3 zeigen, daß jeder endlich erzeugte projektive R-Modul zu einem direkten Summanden eines endlich erzeugten freien R-Moduls isomorph ist.

(ii) Freie Moduln sind stets projektiv; insbesondere ist der reguläre Linksmodul R projektiv.

(iii) Direkte Summanden von projektiven R-Moduln sind wieder projektiv.

(iv) Da Koprodukte von freien R-Moduln wieder frei sind, sind Koprodukte von projektiven Moduln wieder projektiv.

7.7. Bemerkung. Für einen R-Modul P und einen R-Homomorphismus $f : M \to N$ ist offenbar die Abbildung $f_P : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$, $h \mapsto f \circ h$, ein Homomorphismus abelscher Gruppen, d.h. ein $\mathbb{Z}$-Homomorphismus. Analog ist die Abbildung $f^P : \mathrm{Hom}_R(N, P) \to \mathrm{Hom}_R(M, P)$, $h \mapsto h \circ f$ ein $\mathbb{Z}$-Homomorphismus.

Satz.

(i) Für jeden R-Modul P und jede exakte Folge von R-Homomorphismen der Form

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0 \qquad (*)$$

ist die folgende Sequenz von $\mathbb{Z}$*-Homomorphismen exakt:*

$$0 \longrightarrow \operatorname{Hom}_R(P,L) \xrightarrow{f_P} \operatorname{Hom}_R(P,M) \xrightarrow{g_P} \operatorname{Hom}_R(P,N)\ . \qquad (**)$$

(ii) Ein R-Modul P ist genau dann projektiv, wenn für jede exakte Folge (∗) die folgende Sequenz von R-Moduln exakt ist:

$$0 \longrightarrow \operatorname{Hom}_R(P,L) \xrightarrow{f_P} \operatorname{Hom}_R(P,M) \xrightarrow{g_P} \operatorname{Hom}_R(P,N) \longrightarrow 0\ . \qquad (***)$$

Beweis.

(i) Sei $h \in \operatorname{Ker}(f_P)$, d.h. $0 = f_P(h) = f \circ h$. Da f injektiv ist, folgt $h = 0$. Also ist $\operatorname{Ker}(f_P) = 0$, d.h. f_P ist injektiv. Für $h \in \operatorname{Hom}_R(P,L)$ ist

$$g_P\big(f_P(h)\big) = \underbrace{g \circ f}_{=0} \circ h = 0\ .$$

Folglich ist $\operatorname{Bld}(f_P) \subseteq \operatorname{Ker}(g_P)$. Sei umgekehrt $h \in \operatorname{Ker}(g_P)$, d.h. $0 = g_P(h) = g \circ h$. Dann ist $\operatorname{Bld}(h) \subseteq \operatorname{Ker}(g) = \operatorname{Bld}(f)$. Für $x \in P$ existiert also ein Element $x' \in L$ mit $h(x) = f(x')$. Da f injektiv ist, ist x' durch x eindeutig bestimmt. Wir erhalten so eine Abbildung $k : P \to L$, $x \mapsto x'$. Für $r \in R$ ist $h(rx) = rh(x) = rf(x') = f(rx')$, d.h. $(rx)' = rx'$. Analog ist $(x+y)' = x' + y'$ für $x, y \in P$. Folglich ist $k \in \operatorname{Hom}_R(P,L)$ und $f_P(k) = f \circ k = h$. Dies zeigt $\operatorname{Ker}(g_P) \subseteq \operatorname{Bld}(f_P)$.

(ii)

„⟹“: Sei P projektiv und (∗) exakt. Nach (i) genügt zu zeigen, daß g_P surjektiv ist. Sei also $h \in \operatorname{Hom}_R(P,N)$. Da P projektiv ist, existiert ein R-Homomorphismus $k : P \to M$ mit $h = g \circ k = g_P(k) \in \operatorname{Bld}(g_P)$.

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "k"'] \arrow[d, "h"] & \\
M \arrow[r, "g"] & N \arrow[r] & 0
\end{tikzcd}$$

„⟸“: Der R-Modul P besitze die angegebene Eigenschaft. Ist

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

eine exakte Folge von R-Homomorphismen, so existiert zu $\mathrm{id}_P \in \operatorname{Hom}_R(P,P)$ ein $h \in \operatorname{Hom}_R(P,M)$ mit $\mathrm{id}_P = g_P(h) = g \circ h$. Folglich zerfällt die Sequenz. Daher ist P projektiv.

7.8. Satz. *Ein R-Modul P ist genau dann projektiv, wenn eine Familie $(x_i)_{i\in I}$ von Elementen in P und eine Familie $(f_i)_{i\in I}$ von Elementen in $\mathrm{Hom}_R(P,R)$ mit der folgenden Eigenschaft existiert: Für $x \in P$ ist $|\{i \in I : f_i(x) \neq 0\}| < \infty$ und $x = \sum_{i\in I} f_i(x)x_i$.*

Beweis.

„$\Longrightarrow$“: Sei P projektiv und $(x_i)_{i\in I}$ ein beliebiges Erzeugendensystem von P. Dann ist $F := \coprod_{i\in I} R$ ein freier R-Modul, und die Abbildung $g : F \to P$, $(r_i)_{i\in I} \mapsto \sum_{i\in I} r_i x_i$, ist ein R-Epimorphismus.
Da P projektiv ist, existiert ein R-Homomorphismus $h : P \to F$ mit $g \circ h = \mathrm{id}_P$.

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "h"'] \arrow[d, "\mathrm{id}_P"] & \\
F \arrow[r, "g"] & P \arrow[r] & 0
\end{tikzcd}$$

Für $i \in I$ ist dann $f_i := p_i \circ h \in \mathrm{Hom}_R(P,R)$, wobei $p_i : F \to R$ der i-te Projektor ist. Für $x \in P$ ist $h(x) \in F = \coprod_{i\in I} R$, also $\underbrace{p_j\big(h(x)\big)}_{f_i(x)} \neq 0$ für höchstens endlich viele $i \in I$.

Ferner ist

$$\begin{aligned}
\sum_{i\in I} f_i(x)x_i = \sum_{i\in I} p_i\big(h(x)\big)x_i &= g\Bigg(\underbrace{\Big(p_i\big(h(x)\big)\Big)_{i\in I}}_{h(x)}\Bigg) \\
&= g\big(h(x)\big) = x\ .
\end{aligned}$$

„$\Longleftarrow$“: Seien $(x_i)_{i\in I}$ und $(f_i)_{i\in I}$ wie angegeben. Dann ist $(x_i)_{i\in I}$ ein Erzeugendensystem von P. Ferner ist $F := \coprod_{i\in I} R$ ein freier R-Modul, und die Abbildung $g : F \to P$, $(r_i)_{i\in I} \mapsto \sum_{i\in I} r_i x_i$, ist ein R-Epimorphismus. Ferner ist die Abbildung $h : P \to F$, $x \mapsto \big(f_i(x)\big)_{i\in I}$, ein R-Homomorphismus mit $g\big(h(x)\big) = \sum_{i\in I} f_i(x)x_i = x$ für $x \in P$. Daher ist $g \circ h = \mathrm{id}_P$, d.h. die exakte Folge $0 \longrightarrow \mathrm{Ker}(g) \hookrightarrow F \xrightarrow{g} P \longrightarrow 0$ zerfällt. Folglich ist P zu einem direkten Summanden von F isomorph, d.h. P ist projektiv.

Bemerkung. Ist P projektiv, so kann man für $(x_i)_{i\in I}$ in dem Satz ein beliebiges Erzeugendensystem von P wählen.

7.9. Satz. *Ist R lokal, so ist jeder endlich erzeugte projektive R-Modul P frei.*

Beweis. Nach Bemerkung 5.5 (iii) ist $J(R)P \subseteq \mathrm{Rad}(P)$. Daher wird $P/\mathrm{Rad}(P)$ zu einem endlich erzeugten Modul über dem Schiefkörper $R/J(R)$ mit $\big(r + J(R)\big)\big(x + \mathrm{Rad}(P)\big) := rx + \mathrm{Rad}(P)$ für $r \in R$, $x \in P$. Wir wählen eine endliche Basis $b_1 + \mathrm{Rad}(P), \ldots, b_n + \mathrm{Rad}(P)$. Dann ist $N := Rb_1 + \cdots + Rb_n$ ein Untermodul von P mit $P = N + \mathrm{Rad}(P)$. Nach Nakayama ist also $P = N$, d.h. $b_1, \ldots, b_n$ erzeugen P. Folglich ist die Abbildung $f : R^n \to P$, $(r_1, \ldots, r_n) \mapsto \sum_{i=1}^n r_i b_i$, ein R-Epimorphismus. Da P projektiv ist, zerfällt die exakte Folge $0 \longrightarrow \mathrm{Ker}(f) \hookrightarrow R^n \xrightarrow{f} P \longrightarrow 0$. Daher existiert ein Untermodul U von R^n mit

$R^n = U \oplus \operatorname{Ker}(f)$. Seien $r_1, \ldots, r_n \in R$ mit $r_1 b_1 + \cdots + r_n b_n = 0$, also auch

$$\begin{aligned} 0 &= \sum_{i=1}^{n} r_i b_i + \operatorname{Rad}(P) \\ &= \sum_{i=1}^{n} \big(r_i + J(R)\big)\big(b_i + \operatorname{Rad}(P)\big) \ . \end{aligned}$$

Für $i = 1, \ldots, n$ ist $r_i + J(R) = 0$, d.h. $r_i \in J(R)$. Dies zeigt:

$$\begin{aligned} \operatorname{Ker}(f) \subseteq J(R)^n &= \big(\operatorname{Rad}(R)\big)^n = \operatorname{Rad}(R^n) \\ &= \operatorname{Rad}(U) \oplus \operatorname{Rad}\big(\operatorname{Ker}(f)\big) \ . \end{aligned}$$

Folglich ist $\operatorname{Ker}(f) = \operatorname{Rad}\big(\operatorname{Ker}(f)\big)$. Andererseits ist mit R^n auch $\operatorname{Ker}(f)$ endlich erzeugt, Nach Satz 5.2 (iv) ist also $\operatorname{Ker}(f) = 0$; insbesondere ist $r_1 = \cdots = r_n = 0$. Folglich bilden $b_1, \ldots, b_n$ eine Basis von P.

Bemerkung. Der Satz gilt auch, wenn P nicht endlich erzeugt ist (Kaplansky).

8 Injektive Moduln

Sei R ein Ring.

8.1. Satz. *Für einen R-Modul Q sind äquivalent:*

(1) Zu jedem R-Monomorphismus $f : M \to N$ und jedem R-Homomorphismus $g : M \to Q$ existiert ein R-Homomorphismus $h : N \to Q$ mit $g = h \circ f$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, dashed, "h"] \\
& Q &
\end{tikzcd}$$

(2) Zu jedem Linksideal L in R und jedem R-Homomorphismus $g : L \to Q$ existiert ein R-Homomorphismus $h : R \to Q$ mit $h|_L = g$.

(3) Zu jedem Linksideal L in R und jedem R-Homomorphismus $g : L \to Q$ existiert ein $x \in Q$ mit $g(a) = ax$ für $a \in L$.

Definition. Gegebenenfalls nennt man Q **injektiv**.

Beweis.

(1) $\Longrightarrow$ (2): (2) ist ein Spezialfall von (1):

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, hook] \arrow[d, "g"'] & R \arrow[dl, dashed, "h"] \\
& Q &
\end{tikzcd}$$

(2) $\Longrightarrow$ (3): Sei (2) erfüllt, L ein Linksideal in R und $g : L \to Q$ ein R-Homomorphismus. Dann existiert ein R-Homomorphismus $h : R \to Q$ mit $h|_L = g$. Für $a \in L$ ist dann $g(a) = h(a) = h(a \cdot 1) = a \cdot \underbrace{h(1)}_{x \in Q}$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt, $f : M \to N$ ein R-Monomorphismus und $g : M \to Q$ in R-Homomorphismus. Mit $\mathfrak{M}$ bezeichnen wir die Menge aller Paare (L, l), wobei L ein Untermodul von N mit $f(M) \subseteq L$ und $l : L \to Q$ ein R-Homomorphismus mit $l \circ f = g$ ist. Offenbar ist $\mathfrak{M} \neq \emptyset$, da $\big(\mathrm{Bld}(f), g \circ f^{-1}|_{\mathrm{Bld}(f)}\big) \in \mathfrak{M}$. Wir definieren eine Ordnung $\leq$ auf $\mathfrak{M}$ durch

$$(L, l) \leq (L', l') \Longleftrightarrow L \subseteq L' \text{ und } l'|_L = l\ .$$

Man rechnet leicht nach, daß jede total geordnete Teilmenge von $\mathfrak{M}$ eine obere Schranke in $\mathfrak{M}$ besitzt. Nach Zorn enthält $\mathfrak{M}$ ein maximales Element (Z, z). Im Fall $Z = N$ sind wir fertig. Daher nehmen wir $Z \neq N$ an und wählen ein Element $y \in N \setminus Z$. Dann ist $I := \{a \in R : ay \in Z\}$ ein Linksideal in R, und die Abbildung $\gamma : I \to Q$, $a \mapsto z(ay)$

ist ein R-Homomorphismus. Wegen (3) existiert ein Element $x \in Q$ mit $\gamma(a) = ax$ für $a \in I$. Wir setzen $Z' := Z + Ry$ und definieren eine Abbildung $z' : Z' \to Q$ durch $z'(a+ry) := z(a)+rx$ für $a \in Z$, $r \in R$; dies ist wohldefiniert. Sind nämlich $a_1, a_2 \in Z$, $r_1, r_2 \in R$ mit $a_! + r_1y = a_2 + r_2y$, so ist $(r_1 - r_2)y = a_2 - a_1 \in Z$, also $r_1 - r_2 \in I$ und $z(a_2 - a_1) = z\big((r_1 - r_2)y\big) = \gamma(r_1 - r_2) = (r_1 - r_2)x$, d.h. $z(a_1) + r_1x = z(a_2) + r_2x$. Man rechnet sofort nach, daß z' ein R-Homomorphismus mit $z'|_Z = z$ ist. Daher ist $(Z, z) < (Z', z') \in \mathfrak{M}$ im Widerspruch zur Wahl von (Z, z).

8.2. Satz. *Für jede (nichtleere) Familie $(Q_i)_{i\in I}$ von R-Moduln gilt:*

$$\prod_{i\in I} Q_i \text{ ist injektiv} \iff Q_i \text{ injektiv für } i \in I\ .$$

Beweis. Wir setzen $Q := \prod_{i\in I} Q_i$ und bezeichnen mit p_j, q_j den j-ten Projektor bzw, Injektor ($j \in I$). Es sei $f : M \to N$ ein R-Monomorphismus.

„$\Longrightarrow$“: Sei Q injektiv, $j \in I$ und $g : M \to Q_j$ ein R-Homomorphismus. Dann existiert zu dem R-Homomorphismus $q_j \circ g : M \to Q$ ein R-Homomorphismus $k : N \to Q$ mit $q_j \circ g = k \circ f$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, dashed, "h"] \arrow[ddl, dashed, "k"] \\
& Q_j \arrow[d, "q_j"'] & \\
& Q &
\end{tikzcd}$$

Daher ist $h := p_j \circ k : N \to Q_j$ ein R-Homomorphismus mit $h \circ f = p_j \circ k \circ f = p_j \circ q_j \circ g = g$.

„$\Longleftarrow$“: Sei Q_i injektiv für alle i und $g : M \to Q$ ein R-Homomorphismus. Dann existiert für $i \in I$ zu dem R-Homomorphismus $p_i \circ g : M \to Q_i$ ein R-Homomorphismus $h_i : N \to Q_i$ mit $h_i \circ f = p_i \circ g$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, dashed, "h"] \arrow[ddl, dashed, "h_i"] \\
& Q \arrow[d, "p_i"'] & \\
& Q_i &
\end{tikzcd}$$

Daher ist $h : N \to Q$, $x \mapsto (h_i(x))_{i\in I}$ ein R-Homomorphismus mit

$$h\big(f(x)\big) = \Big(h_i\big(f(x)\big)\Big)_{i\in I} = \Big(p_i\big(g(x)\big)\Big)_{i\in I} = g(x)$$

für $x \in M$.

8.3. Satz. *Ein $\mathbb{Z}$-Modul A ist genau dann injektiv, wenn für $n \in \mathbb{N}$ und $a \in A$ ein $b \in A$ existiert mit $a = nb$.*

Bemerkung. Injektive $\mathbb{Z}$-Moduln nennt man daher auch **dividierbare abelsche Gruppen**.

Beweis.

„$\Longrightarrow$“: Sei A injektiv, $a \in A$, $n \in \mathbb{N}$. Dann ist die Abbildung $g : \mathbb{Z}n \to A$, $zn \mapsto za$ ein $\mathbb{Z}$-Homomorphismus. Nach 8.2 existiert ein Element $b \in A$ mit $g(x) = xb$ für $x \in \mathbb{Z}n$. Insbesondere ist $a = g(n) = nb$.

„$\Longleftarrow$“: Sei A dividierbar, I ein Ideal in $\mathbb{Z}$ und $g : I \to A$ ein $\mathbb{Z}$-Homomorphismus. o.B.d.A. $I \neq 0$, also $I = \mathbb{Z}n$ für ein $n \in \mathbb{N}$. Wir setzen $a := g(n) \in A$. Dann existiert ein $b \in A$ mit $a = nb$. Folglich ist $g(zn) = zg(n) = za = znb$ für $z \in \mathbb{Z}$.

Beispiele.

(i) $\mathbb{Q}$ ist ein injektiver $\mathbb{Z}$-Modul, $\mathbb{Z}$ selbst nicht.

(ii) Jeder Faktormodul eines injektiven $\mathbb{Z}$-Moduls ist wieder injektiv.

(iii) Koprodukte eines injektiven $\mathbb{Z}$-Moduls sind wieder injektiv.

8.4. Satz. *Jeder $\mathbb{Z}$-Modul M ist zu einem Untermodul eines injektiven $\mathbb{Z}$-Moduls isomorph.*

Beweis. Nach Satz 7.3 ist M zu einem Faktormodul eines freien $\mathbb{Z}$-Moduls isomorph, d.h. es existieren eine Menge I und ein Untermodul U von $\coprod_{i\in I}\mathbb{Z} =: F$ mit

$$M \cong {}^{F}\!/_{U} = \coprod_{i\in I} {}^{\mathbb{Z}}\!/_{U} \qquad \subseteq \underbrace{\coprod_{i\in I} {}^{\mathbb{Q}}\!/_{U}}_{\text{injektiv nach obigem Beispiel}} .$$

8.5. Bemerkung. Für jeden $\mathbb{Z}$-Modul A wird $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ zu einem R-Modul, wenn man rf für $r \in R$ und $f \in \mathrm{Hom}_{\mathbb{Z}}(R, A)$ durch

$$(rf)(x) = f(xr) \qquad \text{für } x \in R$$

definiert; dies rechnet man leicht nach.

Satz. *Für jeden injektiven $\mathbb{Z}$-Modul A ist* $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ *ein injektiver R-Modul.*

Beweis. Sei $f : M \to N$ ein R-Monomorphismus und $g : M \to \mathrm{Hom}_{\mathbb{Z}}(R, A)$ ein R-Homomorphismus. Dann ist $\gamma : M \to A$, $m \mapsto \big(g(m)\big)(1)$, ein $\mathbb{Z}$-Homomorphismus. Da A injektiv ist, existiert ein $\mathbb{Z}$-Homomorphismus $\delta : N \to A$ mit $\delta \circ f = g$.

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "\gamma"'] & N \arrow[dl, dashed, "\delta"] \\ & A & \end{tikzcd}$$

Für $x \in N$ ist die Abbildung $h_x : R \to A$, $r \mapsto \delta(rx)$, ein $\mathbb{Z}$-Homomorphismus, d.h. $h_x \in \operatorname{Hom}_{\mathbb{Z}}(R, A)$. Für $a, r \in R$ ist dabei $(ah_x)(r) = h_x(ra) = \delta(rax) = h_{ax}(r)$, d.h. $ah_x = h_{ax}$. Daraus folgt leicht, daß die Abbildung $h : N \to \operatorname{Hom}_{\mathbb{Z}}(R, A)$, $x \mapsto h_x$, R-linear ist. Für $m \in M$ und $r \in R$ ist

$$\begin{aligned} h_{f(m)}(r) &= \delta\big(rf(m)\big) = \delta\big(f(rm)\big) = \gamma(rm) = \big(g(rm)\big)(1) \\ &= \big(rg(m)\big)(1) = \big(g(m)\big)(1r) = \big(g(m)\big)(r)\ , \end{aligned}$$

d.h. $g(m) = h_{f(m)} = h\big(f(m)\big)$, d.h. $g = h \circ f$.

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, dashed, "h"] \\ & \operatorname{Hom}_{\mathbb{Z}}(R, A) & \end{tikzcd}$$

8.6. Bemerkung. Für jeden R-Modul M ist $\operatorname{Hom}_R(R, M)$ ein Untermodul des R-Moduls $\operatorname{Hom}_{\mathbb{Z}}(R, M)$, für $r \in R$ und $f \in \operatorname{Hom}_R(R, M)$ ist nämlich auch $rf \in \operatorname{Hom}_R(R, M)$ wegen $(rf)(ab) = f(abr) = af(br) = a(rf)(b)$ für $a, b \in R$. Ferner ist $\operatorname{Hom}_R(R, M) \to M$, $f \mapsto f(1)$, ein R-Isomorphismus; dies beweist man analog zu Aufgabe 16.

Satz. *Jeder R-Modul M ist zu einem Untermodul eines injektiven R-Moduls isomorph.*

Beweis. Nach Satz 8.4 ist der $\mathbb{Z}$-Modul M Untermodul eines injektiven $\mathbb{Z}$-Moduls Q. Wir können $\operatorname{Hom}_{\mathbb{Z}}(R, M)$ als R-Untermodul von $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ auffassen. Es ist also

$$M \cong \operatorname{Hom}_R(R, M) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R, M) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R, Q)\ ,$$

und $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ ist nach 8.5 ein injektiver R-Modul.

8.7. Satz. *Ein R-Modul Q ist genau dann injektiv, wenn jede kurze exakte Folge der Form $0 \longrightarrow Q \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ zerfällt.*

Beweis.

„$\Longrightarrow$“: Analog zu 7.6.

„$\Longleftarrow$“: Nach Satz 8.6 existiert ein injektiver R-Modul D mit $Q \subseteq D$. Nach Voraussetzung zerfällt die exakte Folge $0 \longrightarrow Q \hookrightarrow D \longrightarrow D/Q \longrightarrow 0$. Daher ist $D \cong Q \times D/Q$. Nach Satz 8.2 ist mit D auch Q injektiv.

8.8. Bemerkung. Im folgenden verwenden wir die Bezeichnungen aus Bemerkung 7.7.

Satz.

(i) Für jeden R-Modul Q und jede kurze exakte Folge von R-Homomorphismen

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0 \tag{$*$}$$

ist die folgende Sequenz von $\mathbb{Z}$-Homomorphismen exakt:

$$0 \longrightarrow \mathrm{Hom}_R(N,Q) \xrightarrow{g^Q} \mathrm{Hom}_R(M,Q) \xrightarrow{f^Q} \mathrm{Hom}_R(L,Q)\ . \tag{$**$}$$

(ii) Ein R-Modul Q ist genau dann injektiv, wenn für jede kurze exakte Folge von R-Homomorphismen ($*$) die folgende Sequenz von $\mathbb{Z}$-Homomorphismen exakt ist:

$$0 \longrightarrow \mathrm{Hom}_R(N,Q) \xrightarrow{g^Q} \mathrm{Hom}_R(M,Q) \xrightarrow{f^Q} \mathrm{Hom}_R(L,Q) \longrightarrow 0\ . \tag{$***$}$$

Beweis. Analog zu 7.7.

8.9. Definition. Einen Untermodul L eines R-Moduls M nennt man **wesentlich** (**essential**), falls $L \cap U \neq 0$ für jeden Untermodul $U \neq 0$ von M gilt. Gegebenenfalls nennt man M eine **wesentliche Erweiterung** (**essential extension**) von L. Existiert kein R-Modul N mit der Eigenschaft, daß M ein echter Untermodul von N und N eine wesentliche Erweiterung von L ist, so nennt man M eine **maximale wesentliche Erweiterung** von L.

Satz. *Ein R-Modul Q ist genau dann injektiv, wenn er keine echte wesentliche Erweiterung besitzt.*

Beweis. Sei Q injektiv und M eine wesentliche Erweiterung von Q. Da die exakte Folge $0 \longrightarrow Q \hookrightarrow M \longrightarrow M/Q \longrightarrow 0$ zerfällt, existiert ein Untermodul N von M mit $M = Q \oplus N$. Da Q wesentlich in M ist, folgt $N = 0$, d.h. $M = Q$.
Umgekehrt besitze Q keine echten wesentlichen Erweiterungen. Nach Satz 8.6 existiert ein injektiver R-Modul D mit $Q \subseteq D$. Nach Zorns Lemma existiert ein Untermodul U von D, der maximal bezüglich der Eigenschaft $U \cap Q = 0$ ist. Ist V/U ein von 0 verschiedener Untermodul von D/U, so ist $V \supsetneq U$, also $V \cap Q \neq 0$. Daher ist $V \cap Q \not\subseteq U$ und damit $V(Q+U) = (V \cap Q) + U \supsetneq U$, d.h. $\left(V/U\right) \cap \left(Q + U/U\right) \neq 0$. Dies zeigt, daß $Q + U/U$ ein wesentlicher Untermodul von D/U ist. Da

$$Q + U/U \cong Q/\underbrace{Q \cap U}_{=0} \cong Q$$

keine echte wesentliche Erweiterung besitzt, folgt $Q + U/U = D/U$, d.h. $D = Q + U = Q \oplus U \cong Q \times U$. Nach Satz 8.2 ist Q auch injektiv.

8.10. Satz. *Zu jedem Untermodul M eines injektiven R-Moduls Q existiert ein Untermodul N von Q mit $M \subseteq N \subseteq Q$, der eine maximale wesentliche Erweiterung von M ist.*

Beweis. Sei $\mathfrak{M}$ die Menge aller Untermoduln L von Q mit $M \subseteq L$, die wesentliche Erweiterungen von M sind. Wegen $M \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$. Ferner ist $\mathfrak{M}$ durch $\subseteq$ geordnet. Es ist leicht zu sehen, daß jede totalgeordnete Teilmenge von $\mathfrak{M}$ eine obere Schranke in $\mathfrak{M}$ besitzt. Nach Zorn enthält $\mathfrak{M}$ ein maximales Element N. Wir nehmen an, daß N keine maximale wesentliche Erweiterung von M ist. Dann existiert ein R-Modul $W \supsetneq N$, der eine wesentliche Erweiterung von M ist.
Da Q injektiv ist, existiert ein R-Homomorphismus $f : W \to Q$ mit $f(n) = n$ für $n \in N$.

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, hook] \arrow[d, hook] & W \arrow[dl, dashed, "f"] \\
& Q &
\end{tikzcd}$$

Insbesondere ist $\mathrm{Ker}(f) \cap N = 0$, also auch $M \cap \mathrm{Ker}(f) = 0$. Da M wesentlich in W ist, folgt $\mathrm{Ker}(f) = 0$, d.h. f ist injektiv. Folglich ist $W \cong f(W) \supsetneq f(N) = N$. Außerdem ist $f(W)$ eine wesentliche Erweiterung von $f(M) = M$. Dies ist ein Widerspruch zur Wahl von N.

9 Injektive Hüllen und projektive Decken

Sei R ein Ring.

9.1. Definition. Gegeben sei ein Untermodul M eines injektiven R-Moduls Q. Man nennt Q eine **injektive Hülle** (**injective hull**, **injective envelope**) von M, wenn kein echter injektiver Untermodul N von Q mit $M \subseteq N \subset Q$ existiert.

Satz. *Für einen Untermodul M eines R-Moduls Q sind äquivalent:*

(1) Q ist eine maximale wesentliche Erweiterung von M.

(2) Q ist injektiv und eine wesentliche Erweiterung von M.

(3) Q ist eine injektive Hülle von M.

Beweis.

(1) $\Longrightarrow$ (2): Sei (1) erfüllt. Ist W eine wesentliche Erweiterung von Q, so auch von M; denn für jeden Untermodul $U \neq 0$ von W ist $U \cap Q \neq 0$, also auch $0 \neq M \cap U \cap Q = U \cap M$. Wegen (1) ist also $Q = W$. Nach Satz 8.9 ist Q injektiv.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt und N ein injektiver Untermodul von Q mit $M \subseteq N \subseteq Q$. Da die exakte Folge $0 \longrightarrow N \hookrightarrow Q \longrightarrow Q/N \longrightarrow 0$ zerfällt, existiert ein Untermodul N' von Q mit $Q = N \oplus N'$. Wegen $M \cap N' = 0$ folgt aus (2): $N' = 0$, d.h. $Q = N$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt. Nach Satz 8.10 existiert ein Untermodul N von Q mit $M \subseteq N \subseteq Q$, der eine maximale wesentliche Erweiterung von M ist. Nach der schon bewiesenen Implikation (1) $\Longrightarrow$ (2) ist N injektiv, also $N = Q$.

Bemerkung. Nach Satz 8.6 existiert zu jedem R-Modul M ein injektiver R-Modul Q mit $M \subseteq Q$. Nach Satz 8.10 existiert ein Untermodul N von Q mit $M \subseteq N \subseteq Q$, der eine maximale wesentliche Erweiterung von M ist. Nach Satz 9.1 ist N eine injektive Hülle von M. Daher besitzt jeder R-Modul M eine injektive Hülle. Wir werden zeigen, daß diese bis auf Isomorphie eindeutig ist. (Man spricht daher auch oft von *der* injektiven Hülle von M.)

9.2. Satz. *Sei Q eine injektive Hülle eines R-Moduls M.*

(i) Ist $f : M \to M'$ ein R-Monomorphismus und Q' eine injektive Hülle von M', dann existiert ein R-Monomorphismus $f' : Q \to Q'$ mit $f'(m) = f(m)$ für $m \in M$.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, hook] & M' \arrow[d, hook] \\ Q \arrow[r, dashed, "f'"] & Q' \end{tikzcd}$$

Ist f sogar ein R-Isomorphismus, so auch f'.

(ii) Zu jedem injektiven R-Modul Q' mit $M \subseteq Q'$ existiert ein R-Monomorphismus $g : Q \to Q'$ mit $g(m) = m$ für $m \in M$.

$$
\begin{tikzcd}
 & M \arrow[dl, hook'] \arrow[dr, hook] & \\
Q \arrow[rr, dashed, "g"] & & Q'
\end{tikzcd}
$$

Beweis.

(i) Sei zunächst $f : M \to M'$ ein R-Homomorphismus. Da Q' injektiv ist, existiert ein R-Homomorphismus $f' : Q \to Q'$ mit $f'(m) = f(m)$ für $m \in M$.

$$
\begin{tikzcd}
0 \arrow[r] & M \arrow[r, hook] \arrow[d, "f"'] & Q \arrow[ddl, dashed, "f'"] \\
 & M' \arrow[d, hook] & \\
 & Q &
\end{tikzcd}
$$

Offenbar ist $\mathrm{Ker}(f') \cap M = \mathrm{Ker}(f) = 0$. Da M wesentlich in Q ist, folgt $\mathrm{Ker}(f') = 0$, d.h. f' ist ein R-Monomorphismus. Sei jetzt f ein R-Isomorphismus. Dann ist $f'(Q) \cong Q$ ein injektiver Untermodul von Q' mit $f'(Q) \supseteq f'(M) = f(M) = M'$. Da Q' eine injektive Hülle von M' ist, folgt $f'(Q) = Q'$, d.h. f' ist ein R-Isomorphismus.

(ii) Offenbar ist Q' injektive Hülle von Q'. Nach (i) existiert also zu der Inklusionsabbildung $f : M \to Q'$ ein R-Monomorphismus $f' : Q \to Q'$ mit $f'(m) = f(m) = m$ für $m \in M$.

Bemerkung. Wendet man (i) mit $f = \mathrm{id}_M$ an, so sieht man, daß zu je zwei injektiven Hüllen Q, Q' von M ein R-Isomorphismus $g : Q \to Q'$ mit $g(m) = m$ für $m \in M$ existiert.

9.3. Satz. *Gegeben sei eine Familie $(M_i)_{i\in I}$ von R-Moduln M_i. Für $i \in I$ sei W_i eine wesentliche Erweiterung von M_i. Dann ist $\coprod_{i\in I} W_i$ eine wesentliche Erweiterung von $\coprod_{i\in I} M_i$.*

Beweis. Sei zunächst $I = \{1,2\}$ und $U \neq 0$ ein Untermodul von $W_1 \times W_2$. Wir wählen ein Element $u = (u_1, u_2) \neq 0$ in U. Dann ist $u_1 \neq 0$ oder $u_2 \neq 0$, o.B.d.A. $u_1 \neq 0$. Nach Voraussetzung ist $M_1 \cap Ru_1 \neq 0$. Folglich existiert ein $r_1 \in R$ mit $0 \neq r_1u_1 \in M_1$. Im Fall $r_1u_2 = 0$ ist $0 \neq r_1(u_1,u_2) \in U \cap (M_1 \times M_2)$. Im Fall $r_1u_2 \neq 0$ ist $M_2 \cap Rr_1u_2 \neq 0$ nach Voraussetzung. Folglich existiert ein Element $r_2 \in R$ mit $0 \neq r_2r_1u_2 \in M_2$. Daher ist $0 \neq r_2r_1(u_1,u_2) \in U \cap (M_1 \times M_2)$. Damit ist die Behauptung im Fall $I = \{1,2\}$ gezeigt. Durch Induktion erhält man das Resultat für jede endliche Menge I. Sei jetzt I beliebig und $U \neq 0$ ein Untermodul von $\coprod_{i\in I} W_i$. Wir wählen ein Element $0 \neq u = (u_i)_{i\in I}$ in U. Dann ist $J := \{i \in I : u_i \neq 0\}$ endlich. Wir wissen schon, daß $\coprod_{j\in J} M_j$ wesentlich in $\coprod_{j\in J} W_j$ ist. Daher ist $R(u_j)_{j\in J} \cap \coprod_{j\in J} M_j \neq 0$. Folglich existiert ein Element $r \in R$ mit $0 \neq r(u_j)_{j\in J} \in \coprod_{j\in J} M_j$. Dann ist $0 \neq r(u_i)_{i\in I} \in U \cap \coprod_{i\in I} M_i$, d.h. $U \cap \coprod_{i\in I} M_i \neq 0$.

9.4. Satz. *Für R-Moduln $M_1, \ldots, M_n$ mit injektiven Hüllen $Q_1, \ldots, Q_n$ ist $Q_1 \times \cdots \times Q_n$ eine injektive Hülle von $M_1 \times \cdots \times M_n$.*

Beweis. Nach Satz 8.2 ist $Q_1 \times \cdots \times Q_n$ injektiv. Nach Satz 9.3 ist $Q_1 \times \cdots \times Q_n$ eine wesentliche Erweiterung von $M_1 \times \cdots \times M_n$. Nach Satz 9.1 ist also $Q_1 \times \cdots \times Q_n$ eine injektive Hülle von $M_1 \times \cdots \times M_n$.

> **Bis jetzt:** Jeder R-Modul ist isomorph zu einem Untermodul eines „möglichst kleinen" injektiven R-Moduls.
> **Ziel:** Jeder R-Modul ist isomorph zu einem Faktormodul eines „möglichst kleinen" projektiven R-Moduls.

9.5. Definition. Ein Untermodul L eines R-Moduls M heißt **überflüssig**(**superfluous**), falls für jeden echten Untermodul N von M auch $L + N \neq M$ ist.

Bemerkung. Offenbar ist die Summe von endlich vielen überflüssigen Untermoduln wieder überflüssig.

Satz. *Für jeden R-Modul M ist* $\mathrm{Rad}(M)$ *die Summe aller überflüssigen Untermoduln von M. Ist M endlich erzeugt, so ist* $\mathrm{Rad}(M)$ *selbst überflüssig in M.*

Beweis. Es sei L ein überflüssiger Untermodul von M und N ein maximaler Untermodul von M. Im Fall $L \not\subseteq N$ wäre $L+N = M$, also $N = M$, Widerspruch. Also ist $L \subseteq N$. Daher ist jeder überflüssige Untermodul von M in $\mathrm{Rad}(M)$ enthalten, also auch deren Summe.
Sei umgekehrt $x \in \mathrm{Rad}(M)$. Wir zeigen, daß Rx überflüssig in M ist. Dazu sei N ein Untermodul von M mit $M = Rx + N$. Dann ist $x + N \in {\mathrm{Rad}(M) + N}/{N} \subseteq \mathrm{Rad}\left({M}/{N}\right)$ und ${M}/{N} = {Rx + N}/{N} = R(x+N) \subseteq \mathrm{Rad}\left({M}/{N}\right)$. Nach einem Satz aus § 5 ist ${M}/{N} = 0$, d.h. $M = N$. Sei jetzt M endlich erzeugt und N ein Untermodul mit $M = N + \mathrm{Rad}(M)$. Nakayama sagt: $M = N$.

9.6. Satz. *(i) Sind L, M Untermoduln eines R-Moduls N mit $L \subseteq M \subseteq N$ und ist L überflüssig in M, so auch in N.*

(ii) Ist L_i für $i = 1, \ldots, n$ ein überflüssiger Untermodul eines R-Moduls M_i, so ist $L_1 \times \cdots \times L_n$ überflüssig in $M_1 \times \cdots \times M_n$.

Beweis.

(i) Sei U ein Untermodul von N mit $N = L + U$. Dann ist $M = M \cap N = L + (U \cap M)$, also $M = U \cap M \subseteq U$ und $N = L + U \subseteq M + U \subseteq U$.

(ii) o.B.d.A. $n = 2$. Offenbar ist $L_1 \times 0$ überflüssig in $M_1 \times 0$, also nach (i) auch in $M_1 \times M_2$. Analog ist $0 \times L_2$ überflüssig in $M_1 \times M_2$, also auch $\underbrace{(L_1 \times 0) + (0 \times L_2)}_{=L_1 \times L_2}$.

9.7. Definition. Eine **projektive Decke** (**projective cover**) eines R-Moduls M ist ein R-Epimorphismus $f : P \to M$, wobei P ein projektiver Modul und $\mathrm{Ker}(f)$ überflüssig in P ist. Oft bezeichnet man auch P selbst (ungenau) als projektive Decke von M.

Satz. *Gegeben seien ein R-Epimorphismus $h : M \to N$ und projektive Decken $f : P \to M$, $g : Q \to N$. Dann existieren R-Homomorphismen $k : P \to Q$, $l : Q \to P$ mit $k \circ l = \mathrm{id}_Q$ und $g \circ k = h \circ f$;*

$$\begin{tikzcd} P \arrow[r, dashed, "k"] \arrow[d, "f"] & Q \arrow[d, "g"] \\ M \arrow[r, "h"] & N \end{tikzcd}$$

insbesondere ist k surjektiv, l injektiv, $P = \mathrm{Ker}(k) \oplus \mathrm{Bld}(l)$, und die Einschränkung von k auf $\mathrm{Bld}(l)$ ist ein R-Isomorphismus $\mathrm{Bld}(l) \to Q$ (d.h. P enthält als direkten Summanden eine projektive Decke von N).

Beweis. Da P projektiv ist, existiert ein R-Homomorphismus $k : P \to Q$ mit $g \circ k = h \circ f$.

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[ddl, dashed, "k"'] & \\ & M \arrow[d, "h"] & \\ Q \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

Insbesondere ist $g\big(k(P)\big) = h\big(f(P)\big) = N$, d.h. $Q = k(P) + \mathrm{Ker}(g)$. Da $\mathrm{Ker}(g)$ überflüssig ist, folgt $Q = k(P)$, d.h. k ist surjektiv. Die exakte Sequenz $0 \longrightarrow \mathrm{Ker}(k) \hookrightarrow P \xrightarrow{k} Q \longrightarrow 0$ zerfällt, da Q projektiv ist. Folglich existiert ein R-Homomorphismus $l : Q \to P$ mit $k \circ l = \mathrm{id}_Q$, und es ist $P = \mathrm{Ker}(k) \oplus \mathrm{Bld}(l)$. Wegen $k \circ l = \mathrm{id}_Q$ ist k surjektiv und l injektiv. Daher liefert l einen R-Isomorphismus $Q \to \mathrm{Bld}(l)$, dessen Umkehrabbildung die Einschränkung von k ist.

Bemerkung. Ist h bijektiv, so auch k; denn aus $P = \mathrm{Ker}(k) + \mathrm{Bld}(l)$ folgt

$$N = h\big(f(P)\big) = g\big(k(P)\big) = g\Big(k\big(\mathrm{Bld}(l)\big)\Big) = h\Big(f\big(\mathrm{Bld}(l)\big)\Big)\,,$$

d.h. $M = f\big(\mathrm{Bld}(l)\big)$. Folglich ist $P = \mathrm{Bld}(l) + \mathrm{Ker}(f)$. Da $\mathrm{Ker}(f)$ überflüssig ist, folgt $P = \mathrm{Bld}(l)$. Also ist $\mathrm{Ker}(k) = 0$, d.h. k ist bijektiv.
Projektive Decken sind also bis auf Isomorphie eindeutig bestimmt. Man spricht dann auch von *der* projektiven Decke eines R-Moduls. Im Gegensatz zu injektiven Hüllen existieren aber projektive Decken nicht immer.

9.8. Satz. *Ist $f_i : P_i \to M_i$ für $i = 1, \ldots, n$ eine projektive Decke, so ist die Abbildung $f : P_1 \times \cdots \times P_n \to M_1 \times \cdots \times M_n$, $(x_1, \ldots, x_n) \mapsto \big(f_1(x_1), \ldots, f_n(x_n)\big)$, auch eine projektive Decke.*

Beweis. Offenbar ist $P_1 \times \cdots \times P_n$ projektiv und f surjektiv mit $\mathrm{Ker}(f) = \mathrm{Ker}(f_1) \times \cdots \times \mathrm{Ker}(f_n)$. Nach Satz 9.6 ist $\mathrm{Ker}(f)$ überflüssig in $P_1 \times \cdots \times P_n$.

9.9. Bemerkung. Für jedes Idempotent e in R ist $R = Re \oplus R(1-e)$; denn für $r \in R$ ist $r = r1 = r\big(e + (1-e)\big) = re + r(1-e)$. Also ist $R = Re + R(1-e)$. Für $r \in Re \cap R(1-e)$ ist $r = re = re(1-e) = r0 = 0$. Also ist $Re \cap R(1-e) = 0$.

Satz. *Für jedes Idempotent e in R und jedes Linksideal I in R mit $I \subseteq J(R)$ ist die Restklassenabbildung $f : Re \to {}^{Re}/_{Ie}$ eine projektive Decke.*

Beweis. Nach der obigen Bemerkung ist Re projektiv. Nach Aufgabe 36 ist $\mathrm{Ker}(f) = Ie \subseteq J(R)e = J(R)Re = \mathrm{Rad}(Re)$. Nach Satz 9.5 ist $\mathrm{Ker}(f)$ überflüssig in Re.

9.10. Satz. *Besitzt ein zyklischer R-Modul M eine projektive Decke, so ist $M \cong {}^{Re}/_{Ie}$ für ein Idempotent e in R und für ein Linksideal I in R mit $I \subseteq J(R)$. Ist M sogar einfach, so ist $M \cong {}^{Re}/_{J(R)e}$ für ein Idempotent e in R mit der Eigenschaft, daß eRe ein lokaler Ring ist.*

Beweis. Sei $f : P \to M$ eine projektive Decke. Offenbar ist auch $\mathrm{id}_R : R \to R$ eine projektive Decke. Da M zyklisch ist, existiert ein R-Epimorphismus $g : R \to M$. Nach Satz 9.7 existieren R-Homomorphismen $h : R \to P$, $k : P \to R$ mit $h \circ k = \mathrm{id}_P$, $f \circ h = g$, $R = \mathrm{Ker}(h) \oplus \mathrm{Bld}(k)$, $\mathrm{Bld}(k) \cong P$.

$$\begin{tikzcd} R \arrow[r, dashed, "h"] \arrow[d, "\mathrm{id}_R"] & P \arrow[d, "f"] \\ R \arrow[r, "g"] & M \end{tikzcd}$$

Nach Aufgabe 37 ist $\mathrm{Bld}(k) = Re$ für ein Idempotent e in R. Daher können wir o.B.d.A. $P = Re$ annehmen. Da $I := \mathrm{Ker}(f)$ überflüssig in P ist, ist $I \subseteq \mathrm{Rad}(P)$. Nach Aufgabe 36 ist $\mathrm{Rad}(P) = J(R)P = J(R)Re \subseteq J(R)$. Daher ist $I = Ie$ ein Linksideal in R mit $I \subseteq J(R)$ und ${}^{Re}/_{Ie} = {}^{P}/_{\mathrm{Ker}(f)} \cong M$. Sei jetzt M einfach. Wegen $M \cong {}^{P}/_{I}$ ist I ein maximaler Untermodul von $P = Re$. Wegen $I \subseteq \mathrm{Rad}(Re) < Re$ folgt $I = \mathrm{Rad}(Re) = J(R)e$. Nach Aufgabe 16 ist $(eRe)^\circ \cong \mathrm{End}_R(Re) =: E$. Daher genügt zu zeigen, daß E ein lokaler Ring ist. Dazu sei $\varphi \in E$ nicht invertierbar. Wir zeigen: $\varphi \in J(E)$.
Annahme: φ ist surjektiv. Dann zerfällt die exakte Folge $0 \longrightarrow \mathrm{Ker}(\varphi) \hookrightarrow P \xrightarrow{\varphi} P \longrightarrow 0$, d.h. es existiert ein Untermodul N von P mit $P = N \oplus \mathrm{Ker}(\varphi)$ und $N \cong P$. Da P genau einen maximalen Untermodul enthält, nämlich $\mathrm{Ker}(f) = \mathrm{Rad}(P)$ folgt $\mathrm{Ker}(\varphi) = 0$. Also ist φ bijektiv, Widerspruch.
Daher ist φ nicht surjektiv, d.h. $\varphi(P) \subseteq \mathrm{Rad}(P)$. Sei $\psi \in E$ beliebig. Nach Satz 5.5 genügt zu zeigen, daß $\omega = 1 - \varphi\psi$ invertierbar ist. Offenbar ist

$$\begin{aligned} P &= \mathrm{id}_P(P) = (\omega + \varphi\psi)(P) = \omega(P) + \varphi\big(\psi(P)\big) \\ &= \omega(P) + \mathrm{Rad}(P)\ . \end{aligned}$$

Da $\mathrm{Rad}(P)$ überflüssig in P ist, folgt $P = \omega(P)$, d.h. ω ist surjektiv. Wie oben zeigt man, daß ω sogar bijektiv ist.

10 Idempotente Elemente und semiperfekte Ringe

Sei R ein Ring.

10.1. Definition. Gegeben seien ein Ideal I in R und ein Idempotent ε in R/I. Man sagt, daß sich ε zu R **heben** läßt, falls ein Idempotent e in R mit $\varepsilon = e + I$ existiert.

Beispiel. Offenbar ist $3 + 6\mathbb{Z}$ ein Idempotent in $\mathbb{Z}/6\mathbb{Z}$. Dieses läßt sich nicht zu $\mathbb{Z}$ heben, denn 0 und 1 sind die einzigen Idempotente in $\mathbb{Z}$.

Satz. *Ist I ein Nilideal in R, so läßt sich jedes Idempotent ε in R/I zu R heben.*

Beweis. Wir schreiben $\varepsilon = u + I$ mit einem beliebigen $u \in R$. Wegen $0 = \varepsilon(1-\varepsilon) = u(1-u) + I$ ist $u(1-u) \in I$ und daher $u^m(1-u)^m = 0$ für ein $m \in \mathbb{N}$. Folglich ist

$$\begin{aligned} 1 = \big(u + (1-u)\big)^{2m} &= \sum_{i=0}^{2m} \binom{2m}{i} u^{2m-i}(1-u)^i \\ &= \underbrace{\sum_{i=0}^{m} \binom{2m}{i} u^{2m-i}(1-u)^i}_{=:\, e} + \underbrace{\sum_{i=m+1}^{2m} \binom{2m}{i} u^{2m-i}(1-u)^i}_{=:\, f} . \end{aligned}$$

Wegen $u^m(1-u)^m = 0$ ist $ef = 0$, d.h. $e = e1 = e(e+f) = e^2$. Wegen $u(1-u) \in I$ ist $e + I = u^{2m} + I = \varepsilon^{2m} = \varepsilon$.

10.2. Definition. Idempotente e, f in R mit $ef = 0 = fe$ nennt man **orthogonal**.

Bemerkung. Für paarweise orthogonale Idempotente $e_1, \dots, e_n$ in R ist auch $e_1 + \dots + e_n$ ein Idempotent.

Satz. *Es sei I ein Ideal in R mit $I \subseteq J(R)$ und der Eigenschaft, daß sich jedes Idempotent in R/I zu R heben läßt. Sind $\varepsilon_1, \dots, \varepsilon_n$ paarweise orthogonale Idempotente in R/I mit $\varepsilon_1 + \dots + \varepsilon_n = 1$, so existieren paarweise orthogonale Idempotente $e_1, \dots, e_n$ in R mit $1 = e_1 + \dots + e_n$ und $e_i + I = \varepsilon_i$ für $i = 1, \dots, n$ (d.h. man kann $\varepsilon_1, \dots, \varepsilon_n$ **simultan heben**).*

Beweis. Nach Voraussetzung existiert für $i = 1, \dots, n$ ein Idempotent f_i in R mit $f_i + I = \varepsilon_i$. Dann ist $u = f_1 + \dots + f_n \in R$ mit $u + I = \varepsilon_1 + \dots + \varepsilon_n = 1$ und $f_i f_j + I = \varepsilon_i \varepsilon_j = 0$ für $i \neq j$. Wir wenden Aufgabe 29 an. Danach ist u eine Einheit in R mit $1 + I = uu^{-1} + I = (u + I)(u^{-1} + I) = u^{-1} + I$. Für $i = 1, \dots, n$ ist außerdem $e_i := u^{-1} f_i$ ein Idempotent in R mit $e_i + I = (u^{-1} + I)(f_i + I) = \varepsilon_i$. Schließlich ist $e_i e_j = 0$ für $i \neq j$ und $e_1 + \dots + e_n = 1$.

10.3. Satz. *Für ein Idempotent $e \neq 0$ in R sind äquivalent:*

(1) e läßt sich nicht in der Form $e = f + g$ mit orthogonalen Idempotenten $f \neq 0$, $g \neq 0$ in R schreiben.

(2) Der R-Linksmodul Re ist unzerlegbar.

(3) 0 und e sind die einzigen Idempotente in eRe.

(4) Der R-Rechtsmodul eR ist unzerlegbar.

Definition. Gegebenenfalls nennt man e ein **primitives** Idempotent in R.

Beweis.

(1) $\Longrightarrow$ (2): Sei (1) erfüllt und $Re = L \oplus M$ mit Untermoduln L, M. Wir schreiben $e = f + g$ mit $f \in L$, $g \in M$. Ist $x \in Re$ und $y \in R$ mit $x = ye$, so ist $xe = ye^2 = ye = x$. Insbesondere ist $f = fe = f^2 + fg$ mit $f^2 \in L$, $fg \in M$. Folglich ist $f^2 = f$ und $fg = 0$. Analog ist $g^2 = g$ und $gf = 0$. Wegen (1) folgt $f = 0$ oder $g = 0$, o.B.d.A. $g = 0$. Dann ist aber $e = f \in L$ und damit $Re \subseteq L$, d.h. $M = 0$.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt. Nach Satz 6.2 sind 0 und 1 die einzigen Idempotente in $\operatorname{End}_R(Re)$. Nach Aufgabe 16 ist aber $\operatorname{End}_R(Re) \cong (eRe)^\circ$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt und $e = f + g$ mit orthogonalen Idempotenten f, g in R. Dann ist $f = (f+g)f(f+g) \in eRe$, also $f \in \{0, e\}$. Folglich ist $f = 0$ oder $g = 0$.

(4) $\Longleftrightarrow$ (1): Analog.

Bemerkung. Ist e ein Idempotent in R mit der Eigenschaft, daß eRe ein lokaler Ring ist, so ist e primitiv in R nach Bemerkung 6.1. Gegebenenfalls nennt man e **streng primitives Idempotent** oder **lokal**.

10.4. Satz. *Sei P ein projektiver R-Modul und $E := \operatorname{End}_R(P)$. Dann ist $J(E) = \big\{f \in E : f(P)$ überflüssig in $P\big\}$.*

Beweis.

„$\subseteq$“: Sei $f \in J(E)$ und N ein Untermodul von P mit $P = f(P) + N$. Für die Restklassenabbildung $g : P \to P/N$ gilt also: $g\big(f(P)\big) = f(P) + N/N = P/N$. Da P projektiv ist, existiert ein $h \in E$ mit $g \circ f \circ h = g$, d.h. $g \circ (1 - f \circ h) = 0$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "h"'] \arrow[d, "g"] & \\ P \arrow[r, "g\circ f"] & P/N \arrow[r] & 0 \end{tikzcd}$$

Wegen $f \in J(E)$ ist $1 - f \circ h$ invertierbar in E, also $g = 0$. Folglich ist $P = N$.

„$\supseteq$“: Sei $f \in E$ und $f(P)$ überflüssig in P. Sei außerdem $g \in E$ und $h = \mathrm{id}_P - f \circ g$. Dann ist $P = \mathrm{id}_P(P) = (h + f \circ g)(P) = h(P) + f\big(g(P)\big)$, also $P = h(P)$. Da P projektiv ist, zerfällt die exakte Folge $0 \longrightarrow \operatorname{Ker}(h) \hookrightarrow P \xrightarrow{h} P \longrightarrow 0$. Folglich existiert ein $k \in E$ mit $h \circ k = \mathrm{id}_P$. Daher ist h rechtsinvertierbar in E. Nach Satz 5.5 ist also $f \in J(E)$.

10.5. Satz. *Äquivalent sind:*

(1) Jeder einfache R-Modul besitzt eine projektive Decke.

(2) Jeder endlich erzeugte R-Modul besitzt eine projektive Decke.

(3) $R/J(R)$ *ist ein halbeinfacher Ring, und jedes Idempotent in* $R/J(R)$ *läßt sich zu* R *heben.*

(4) Es existieren paarweise orthogonale streng primitive Idempotente $e_1, \ldots, e_n$ *in* R *mit* $e_1 + \cdots + e_n = 1$.

Beweis. (1) $\Longrightarrow$ (2): Sei (1) erfüllt und M ein endlich erzeugter R-Modul. Wir wählen ein Repräsentantensystem $(M_i)_{i\in I}$ für die Isomorphieklassen einfacher R-Moduln und für $i \in I$ eine projektive Decke $f_i : P_i \to M_i$. Dann setzen wir $P := \coprod_{i\in I} P_i$ und bezeichnen mit p_i und q_i die entsprechenden Projektoren und Injektoren. Wir betrachten den Untermodul $N := \sum_{f\in \mathrm{Hom}_R(P,M)} f(P)$ von M.
Annahme: $N \neq M$. Da M endlich erzeugt ist, existiert nach Satz 5.2 (iv) ein maximaler Untermodul L von M mit $N \subseteq L \subseteq M$. Dann ist M/L ein einfacher R-Modul, also $M/L \cong M_j$ für ein $j \in I$. Folglich ist $g_j : P \xrightarrow{p_j} P_j \xrightarrow{f_j} M_j \cong M/L$ ein R-Epimorphismus. Da P projektiv ist, existiert zur Restklassenabbildung $\mu : M \to M/L$ ein R-Homomorphismus $f : P \to M$ mit $\mu \circ f = g_j$;

$$\begin{tikzcd}
 & P \arrow[ld, dashed, "f"'] \arrow[d, "g_j"] & \\
M \arrow[r, "\mu"] & M/L \arrow[r] & 0
\end{tikzcd}$$

insbesondere ist $M/L = g_j(P) = \mu\big(f(P)\big) = f(P) + L/L$, also $f(P) \not\subseteq L$. Widerspruch!
Folglich ist $M = \sum_{f\in \mathrm{Hom}_R(P,M)} f(P)$. Andererseits ist $M = Rm_1 + \cdots + Rm_r$ mit endlich vielen $m_1, \ldots, m_r \in M$. Daher existieren *endliche* Teilmengen P_0 von P und H_0 von $\mathrm{Hom}_R(P, M)$ mit $M = \sum_{x\in P_0} \sum_{f\in H_0} Rf(x)$. Jedes $x \in P_0 \subseteq P = \coprod_{i\in I} P_i$ läßt sich in der Form $x = q_{i_1}(y_1) + \cdots + q_{i_t}(y_t)$ mit endlich vielen $i_1, \ldots, i_t \in I$ und $y_j \in P_{i_j}$ für $j = 1, \ldots, t$ schreiben. Folglich existieren endlich viele projektive Decken $Q_1, \ldots, Q_m$ einfacher R-Moduln $M_1, \ldots, M_m$ und R-Homomorphismen $g_1 : Q_1 \to M, \ldots, g_m : Q_m \to M$ mit $M = \sum_{i=1}^m g_i(Q_i)$. Dann ist $Q := Q_1 \times \cdots \times Q_m$ projektiv und $g : Q \to M$, $(y_1, \ldots, y_m) \mapsto \sum_{i=1}^m g_i(y_i)$, ein R-Epimorphismus. Dieser induziert einen R-Epimorphismus $\overline{g} : Q/J(R)Q \to M/J(R)M$, $y + J(R)Q \mapsto g(y) + J(R)M$. Offenbar ist $J(R)Q = J(R)Q_1 \times \cdots \times J(R)Q_m$ und $Q/J(R)Q \cong Q_1/J(R)Q_1 \times \cdots \times Q_m/J(R)Q_m$. Für $i = 1, \ldots, m$ existiert nach Satz 9.10 ein streng primitives Idempotent e_i in R mit $M_i \cong Re_i/J(R)e_i$, und nach Satz 9.9 ist $Q_i \cong Re_i$; insbesondere ist $Q_i/J(R)Q_i \cong Re_i/J(R)Re_i \cong M_i$ einfach. Daher sind $Q/J(R)Q$ und $M/J(R)M$ halbeinfach. Da M endlich erzeugt ist, ist $M/J(R)M$ eine *endliche* direkte Summe einfacher R-Moduln. Nach Satz 9.8 existiert also eine projektive Decke $h : P' \to M/J(R)M$. Zu der Restklassenabbildung $\pi : M \to M/J(R)M$ existiert ein R-Homomorphismus $k : P' \to M$ mit $h = \pi \circ k$.

$$\begin{tikzcd}
 & P' \arrow[ld, dashed, "k"'] \arrow[d, "h"] & \\
M \arrow[r, "\pi"] & M/J(R)M \arrow[r] & 0
\end{tikzcd}$$

Folglich ist

$$ {}^{M}\!/_{J(R)M} = h(P') = \pi\big(k(P')\big) = {}^{k(P') + J(R)M}\!/_{J(R)M} \,, $$

d.h. $M = k(P') + J(R)M$. Nach Nakayama ist also $M = k(P')$, d.h. k ist surjektiv. Da $\mathrm{Ker}(k) \subseteq \mathrm{Ker}(\pi \circ k) = \mathrm{Ker}(h)$ überflüssig ist, ist $f : P' \to M$ eine projektive Decke.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt. Wir zeigen zunächst, daß $\overline{R} = {}^{R}\!/_{J(R)}$ ein halbeinfacher Ring ist. Dazu sei $\overline{L} = {}^{L}\!/_{J(R)}$ ein Linksideal in $\overline{R}$. Dann ist L ein Linksideal in R, und der zyklische R-Modul ${}^{R}\!/_{L}$ besitzt nach Voraussetzung eine projektive Decke. Nach Satz 9.10 ist ${}^{R}\!/_{L} \cong {}^{Re}\!/_{Ie}$ für ein Idempotent e in R und ein Linksideal I in R mit $I \subseteq J(R)$. Folglich ist $J(R)\left({}^{Re}\!/_{Ie}\right) \cong J(R)\left({}^{R}\!/_{L}\right) = {}^{J(R)+L}\!/_{L} = 0$. Daher ist $J(R)e \subseteq Ie \subseteq J(R)e$, d.h. $Ie = J(R)e$ und ${}^{R}\!/_{L} \cong {}^{Re}\!/_{J(R)e}$. Man rechnet leicht nach, daß die Abbildung ${}^{Re}\!/_{J(R)e} \to \overline{R}\big(e + J(R)\big)$, $x + J(R)e \mapsto x + J(R)$, ein R-Isomorphismus ist. Daher ist ${}^{R}\!/_{L} \cong \overline{R}\big(e + J(R)\big)$ als R-Modul und $\overline{R}$-Modul. Da der letzte $\overline{R}$-Modul offenbar projektiv ist, zerfällt die exakte Folge

$$ 0 \longrightarrow {}^{L}\!/_{J(R)} \hookrightarrow {}^{R}\!/_{J(R)} \longrightarrow {}^{R}\!/_{L} \longrightarrow 0 \,. $$
$$ r + J(R) \mapsto r + L $$

Daher besitzt ${}^{L}\!/_{J(R)}$ ein Komplement in ${}^{R}\!/_{J(R)}$. Damit ist gezeigt, daß $\overline{R}$ ein halbeinfacher Ring ist.
Sei jetzt ε_1 ein Idempotent in $\overline{R}$ und $\varepsilon_2 = 1 - \varepsilon_1$. Dann ist $\overline{R} = \overline{R}\varepsilon_1 \oplus \overline{R}\varepsilon_2$. Nach Voraussetzung besitzen die R-Moduln $\overline{R}\varepsilon_1$, $\overline{R}\varepsilon_2$ projektive Decken $f_1 : P_1 \to \overline{R}\varepsilon_1$, $f_2 : P_2 \to \overline{R}\varepsilon_2$. Nach Satz 9.8 ist also die Abbildung

$$ f' : P_1 \times P_2 \to \overline{R} \,, \quad (x_1, x_2) \mapsto f_1(x_1) + f_2(x_2) \,, $$

auch eine projektive Decke. Andererseits ist nach Satz 9.9 die Restklassenabbildung $f : R \to \overline{R}$ eine projektive Decke. Nach Bemerkung 9.7 existiert ein R-Isomorphismus $g : P_1 \times P_2 \to R$ mit $f \circ g = f'$.

$$
\begin{tikzcd}
P_1 \times P_2 \arrow[r, dashed, "g"] \arrow[d, "f'"] & R \arrow[d, "f"] \\
\overline{R} \arrow[r, "\mathrm{id}_{\overline{R}}"] & \overline{R}
\end{tikzcd}
$$

Wegen $P_1 \times P_2 = (P_1 \times 0) \oplus (0 \times P_2)$ ist $R = Q_1 \oplus Q_2$ mit $Q_1 = g(P_1 \times 0)$, $Q_2 = g(0 \times P_2)$. Nach Aufgabe 37 existieren orthogonale Idempotente e_1, e_2 in R mit $Q_1 = Re_1$, $Q_2 = Re_2$ und $e_1 + e_2 = 1$. Dann ist $f(e_1) \in f(Q_1) = f\big(g(P_1 \times 0)\big) = f'(P_1 \times 0) = \overline{R}\varepsilon_1$ und analog $f(e_2) \in \overline{R}\varepsilon_2$. Aus $\varepsilon_1 + \varepsilon_2 = 1_{\overline{R}} = f(1_R) = f(e_1) + f(e_2)$ folgt $\varepsilon_1 = f(e_1)$ und $\varepsilon_2 = f(e_2)$.

(3) $\Longrightarrow$ (4): Sei (3) erfüllt. Nach Wedderburn ist $\overline{R} := {}^{R}\!/_{J(R)}$ ein direktes Produkt von endlich vielen vollen Matrixringen über Schiefkörpern:

$$ \overline{R} \cong \mathrm{Mat}(d_1, D_1) \times \cdots \times \mathrm{Mat}(d_k, D_k) \,. $$

Daher existieren endlich viele paarweise orthogonale Idempotente $\varepsilon_1, \ldots, \varepsilon_n$ in $\overline{R}$ (die diagonalen Matrixeinheiten

$$e_i := \left(0, \ldots, 0, \begin{pmatrix} 0 & & & & & & \\ & \ddots & & & & 0 & \\ & & 0 & & & & \\ & & & 1 & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}, 0, \ldots, 0 \right) \qquad)$$

mit der Eigenschaft, daß $\varepsilon_1 + \cdots + \varepsilon_n = 1$ und $\varepsilon_i \overline{R} \varepsilon_i$ für $i = 1, \ldots, n$ ein Schiefkörper ist. Nach (3) und Satz 10.2 existieren paarweise orthogonale Idempotente $e_1, \ldots, e_n$ in R mit der Eigenschaft, daß $e_1 + \cdots + e_n = 1$ und $\varepsilon_i = e_i + J(R)$ für $i = 1, \ldots, n$ ist. Für $i = 1, \ldots, n$ ist die Abbildung $e_i R e_i \to \varepsilon_i \overline{R} \varepsilon_i$, $x \mapsto x + J(R)$, ein Epimorphismus von Ringen mit Kern $e_i R e_i \cap J(R) = e_i J(R) e_i = J(e_i R e_i)$. Daher ist $e_i R e_i / J(e_i R e_i)$ ein Schiefkörper, d.h. $e_i R e_i$ ist ein lokaler Ring, d.h. e_i ist streng primitiv.

(4) $\Longrightarrow$ (1): Sei (4) erfüllt und $i \in \{1, \ldots, n\}$. Nach Satz 5.2 (iv) enthält $P_i := Re_i$ einen maximalen Untermodul M_i. Wir zeigen zunächst, daß M_i überflüssig in P_i ist. Dazu sei K_i ein Untermodul von P_i mit $P_i = K_i + M_i$. Dann ist

$$P_i / M_i = K_i + M_i / M_i \cong K_i / K_i \cap M_i \, .$$

Es existiert also ein R-Epimorphismus $f_i : P_i \to K_i / K_i \cap M_i$. Da P_i projektiv ist, existiert zu der Restklassenabbildung $\pi_i : K_i \to K_i / K_i \cap M_i$ ein R-Homomorphismus $g_i : P_i \to K_i$ mit $\pi_i \circ g_i = f_i$.

$$\begin{tikzcd} & P_i \arrow[dl, dashed, "g_i"'] \arrow[d, "f_i"] & \\ K_i \arrow[r, "\pi_i"] & K_i / K_i \cap M_i \arrow[r] & 0 \end{tikzcd}$$

Dann ist

$$\begin{aligned} K_i / K_i \cap M_i &= f_i(P_i) = \pi_i\big(g_i(P_i)\big) \\ &= \big(g_i(P_i) + (K_i \cap M_i)\big) / (K_i \cap M_i) \end{aligned}$$

und $K_i = g_i(P_i) + (K_i \cap M_i)$ und $P_i = K_i + M_i = g_i(P_i) + M_i$. Wir können g_i auch als R-Homomorphismus $g_i' : P_i \to P_i$ auffassen. Im Fall $K_i \neq P_i$ wäre g_i' nicht invertierbar in $E_i = \mathrm{End}_R(P_i)$. Nach Aufgabe 16 ist $E_i \cong (e_i R e_i)^\circ$ ein lokaler Ring, also $g_i' \in J(E_i)$. Nach Satz 10.4 ist also $\underbrace{g_i'(P_i)}_{=g_i(P_i)}$ überflüssig in P_i, und wir erhalten den Widerspruch $P_i = M_i$. Damit ist gezeigt, daß M_i überflüssig in P_i ist. Folglich ist $M_i \subseteq \mathrm{Rad}(P_i) \subseteq M_i$, d.h. $\mathrm{Rad}(P_i) = M_i$. Genauer gilt: $M_i = \mathrm{Rad}(Re_i) = J(R)Re_i = J(R)e_i$; insbesondere ist $Re_i / J(R)e_i = P_i / M_i$ einfach als R-Modul. Man rechnet leicht nach, daß die Abbildung $Re_i / J(R)e_i \to \big(R / J(R)\big)\big(e_i + J(R)\big)$, $x + J(R)e_i \mapsto x + J(R)$, ein R-Isomorphismus ist. Wir setzen $\overline{R} := R / J(R)$ und $\overline{e_i} := e_i + J(R)$. Dann ist $\overline{R} = \overline{R}\overline{e_1} \oplus \cdots \oplus \overline{R}\overline{e_n}$ mit einfachen $\overline{R}$-Moduln $\overline{R}\overline{e_1}, \ldots \overline{R}\overline{e_n}$. Daher ist $\overline{R}$ ein halbeinfacher Ring. Jeder einfache R-Modul wird von $J(R)$ annuliert, kann also als einfacher $\overline{R}$-Modul aufgefaßt werden. Da $\overline{R}$ halbeinfach ist, ist M zu einem der Moduln $\overline{Re_i}$ isomorph, d.h. $M \cong {}^{Re_i}/_{J(R)e_i}$. Nach Satz 9.9 ist die Restklassenabbildung $Re_i \to {}^{Re_i}/_{J(R)e_i}$ eine projektive Decke.

Definition. Sind (1)–(4) erfüllt, so nennt man R **semiperfekt**.

Bemerkung. R semiperfekt $\Longleftrightarrow$ R° semiperfekt.

Beispiele. Jeder links- oder rechtsartinsche Ring R ist semiperfekt; denn nach Bemerkung 5.5 (iv) ist ${}^{R}/_{J(R)}$ halbeinfach, und nach Satz 5.7 ist $J(R)$ nilpotent. Nach Satz 10.1 läßt sich also jedes Idempotent in ${}^{R}/_{J(R)}$ zu R heben.

10.6. Bemerkung. Es sei R ein semiperfekter Ring und $1 = e_1 + \cdots + e_n$ mit paarweise orthogonalen streng primitiven Idempotenten $e_1, \ldots, e_n$ in R. Im Beweis von Satz 10.5 haben wir gezeigt, daß ${}^{Re_i}/_{J(R)e_i}$ für $i = 1, \ldots, n$ ein einfacher R-Modul mit projektiver Decke $Re_i \to {}^{Re_i}/_{J(R)e_i}$, $x \mapsto x + J(R)e_i$, ist. Wir haben auch gesehen, daß jeder einfache R-Modul zu einem der R-Moduln ${}^{Re_1}/_{J(R)e_1}, \ldots, {}^{Re_n}/_{J(R)e_n}$ isomorph ist. Ferner wissen wir, daß $Re_1, \ldots, Re_n$ streng unzerlegbare projektive R-Moduln sind.

Satz. *In der obigen Situation ist jeder unzerlegbare projektive R-Modul P zu einem der Moduln $Re_1, \ldots, Re_n$ isomorph. Dabei gilt:*

$$Re_i \cong Re_j \Longleftrightarrow {}^{Re_i}/_{J(R)e_i} \cong {}^{Re_j}/_{J(R)e_j}\ .$$

Beweis. Da P projektiv ist, existieren Untermoduln Q, Q' eines freien R-Moduls F mit $F = Q \oplus Q'$ und $P \cong Q$. Ferner ist $F \cong \bigoplus_{i \in I} F_i$ mit zu R isomorphen Untermoduln F_i $(i \in I)$. Daher ist F eine direkte Summe von Untermoduln, von denen jeder zu einem Re_j isomorph ist. Nach Satz 6.5 ist also $P \cong Re_j$ für ein $j \in \{1, \ldots, n\}$. Für $i, j = 1, \ldots, n$ induziert jeder R-Isomorphismus $f : Re_i \to Re_j$ einen R-Isomorphismus $\overline{f} : {}^{Re_i}/_{J(R)e_i} \to {}^{Re_j}/_{J(R)e_j}$. Umgekehrt existiert zu jedem R-Isomorphismus $g : {}^{Re_i}/_{J(R)e_i} \to {}^{Re_j}/_{J(R)e_j}$ nach Bemerkung 9.7 ein R-Isomorphismus $f : Re_i \to Re_j$ mit $\overline{f} = g$.

10.7. Bemerkung. Es seien R ein semiperfekter Ring und M ein endlich erzeugter R-Modul. Im Beweis von Satz 10.5 haben wir gesehen, daß ${}^{M}/_{J(R)M}$ halbeinfach (genauer: eine direkte Summe von endlich vielen einfachen R-Moduln) ist. Folglich ist $0 = \mathrm{Rad}\left({}^{M}/_{J(R)M}\right) \supseteq \mathrm{Rad}(M) + {}^{J(R)M}/_{J(R)M}$, d.h. $\mathrm{Rad}(M) \subseteq J(R)M$. Nach Bemerkung 5.5 (iii) ist also $\mathrm{Rad}(M) = J(R)M$. Im Beweis von Satz 10.5 haben wir auch gesehen, daß jede projektive Decke $f : P \to {}^{M}/_{J(R)M}$ eine projektive Decke $g : P \to M$ induziert.

Satz. *Es sei R ein semiperfekter Ring und $1 = e_1 + \cdots + e_n$ mit paarweise orthogonalen streng primitiven Idempotenten $e_1, \ldots, e_n$ in R. Dann gilt:*

(i) Sind $f_1, \ldots, f_m$ paarweise orthogonale von 0 verschiedene Idempotente in R, so ist $m \leq n$.

(ii) Jedes Idempotent e in R läßt sich als Summe von endlich vielen paarweise orthogonalen primitiven Idempotenten schreiben.

(iii) Jedes primitive Idempotent f in R ist streng primitiv.

(iv) Ist $1 = f_1 + \cdots + f_m$ mit paarweise orthogonalen primitiven Idempotenten $f_1, \ldots, f_m$ in R, so ist $m = n$, und es existieren eine Einheit u in R und eine Permutation π von $1, \ldots, n$ mit $u^{-1}e_iu = f_{\pi(i)}$ für $i = 1, \ldots, n$.

Beweis. Setze $\overline{R} := {}^{R}/_{J(R)}$ und $\overline{e_i} := e_i + J(R)$ für $i = 1, \ldots, n$. Im Beweis von Satz 10.5 haben wir gesehen, daß $\overline{R} = \overline{Re_1} \oplus \cdots \oplus \overline{Re_n}$ mit einfachen $\overline{R}$-Moduln $\overline{Re_1}, \ldots, \overline{Re_n}$ ist. Daher ist die Kompositionslänge des regulären $\overline{R}$-Moduls gleich n.

(i) Für $i = 1, \ldots, n$ ist $f_i \notin J(R)$ nach Aufgabe 31, also $\overline{f_i} := f_i + J(R) \neq 0$. Dabei ist $\overline{Rf_1} + \cdots + \overline{Rf_m} = \overline{Rf_1} \oplus \cdots \oplus \overline{Rf_m}$ mit $\overline{Rf_i} \neq 0$ für $i = 1, \ldots, m$. Nach Schreier ist also $m \leq n$.

(ii) Ist $e = 0$ oder e primitiv, so ist nichts zu zeigen. Ansonsten schreiben wir $e = e_1 + e_1'$ mit paarweise orthogonalen Idempotenten $e_1 \neq 0$, $e_1' \neq 0$. Sind e_1 und e_1' primitiv, so sind wir fertig. Andernfals können wir o.B.d.A. annehmen, daß e_1' nicht primitiv ist. Dann schreiben wir $e_1' = e_2 + e_2'$ mit paarweise orthogonalen Idempotenten $e_2 \neq 0$, $e_2' \neq 0$. Jetzt ist $e = e_1 + e_2 + e_2'$ mit paarweise orthogonalen Idempotenten $e_1 \neq 0$, $e_2 \neq 0$, $e_2' \neq 0$. Sind e_1, e_2, e_2' primitiv, so sind wir fertig. Andernfalls setzen wir das Verfahren fort. Wegen (i) muß das Verfahren abbrechen.

(iii) Nach Voraussetzung ist Rf unzerlegbar, nach Satz 10.6 also sogar streng unzerlegbar. Folglich ist f streng primitiv.

(iv) Nach Voraussetzung ist $R = Re_1 + \cdots + Re_n = Rf_1 + \cdots + Rf_m$ mit streng unzerlegbaren R-Moduln $Re_1, \ldots, Re_n$, $Rf_1, \ldots, Rf_m$. Nach Krull-Schmidt ist $m = n$, und es existieren ein R-Automorphismus $\varphi : R \to R$ und eine Permutation π von $1, \ldots, n$ mit $\varphi(Re_i) = Rf_{\pi(i)}$ für alle i. Wir setzen $u = \varphi(1)$ und $v = \varphi^{-1}(1)$. Dann ist $1 = \varphi\big(\varphi^{-1}(1)\big) = \varphi(v1) = v\varphi(1) = vu$ und analog $uv = 1$, d.h. $u \in U(R)$ und $v = u^{-1}$. Ferner ist

$$\begin{array}{l} u = u1 = uf_1 + \cdots + uf_m \\ \| \\ \varphi(1) = \varphi(e_1) + \cdots + \varphi(e_n) = e_1 \underbrace{\varphi(1)}_{=u} + \cdots + e_n \underbrace{\varphi(1)}_{=u} \end{array}$$

mit $uf_i \in Rf_i$ und $e_i u = \varphi(e_i) \in Rf_{\pi(i)}$ für alle i. Folglich ist $e_i u = uf_{\pi(i)}$ für alle i.

10.8. Satz. *Für jeden semiperfekten Ring R gilt:*

(i) Für jedes Ideal I in R ist auch ${}^{R}/_{I}$ semiperfekt.

(ii) Für jedes Idempotent e in R ist eRe semiperfekt.

Beweis.

(i) Wir schreiben $1 = e_1 + \cdots + e_n$ mit paarweise orthogonalen streng primitiven Idempotenten $e_1, \ldots, e_n$. Dabei numerieren wir so, daß $e_1, \ldots, e_m \notin I$, $e_{m+1}, \ldots, e_n \in I$ gilt. Dann ist $1 = \overline{e_1} + \cdots + \overline{e_m}$ mit paarweise orthogonalen Idempotenten $\overline{e_i} = e_i + I$ in ${}^{R}/_{I} = \overline{R}$. Daher genügt zu zeigen, daß $\overline{e_i}$ für $i = 1, \ldots, m$ streng primitiv in $\overline{R}$ ist. Offenbar ist die Abbildung $\varphi_i : e_i Re_i \to \overline{e_i}\overline{R}\overline{e_i}$, $x \mapsto x + I$ ein Ring-Epimorphismus. Wegen $\overline{e_i} \neq 0$ ist $\operatorname{Ker}(\varphi_i) \neq e_i Re_i$. Da $e_i Re_i$ ein lokaler Ring ist, folgt $\operatorname{Ker}(\varphi_i) \subseteq J(e_i Re_i)$. Daher ist $J\left({}^{e_i Re_i}/_{\operatorname{Ker}(\varphi_i)}\right) = {}^{J(e_i Re_i)}/_{\operatorname{Ker}(\varphi_i)}$. Folglich sind auch ${}^{e_i Re_i}/_{\operatorname{Ker}(\varphi_i)}$ und $\overline{e_i}\overline{R}\overline{e_i}$ lokale Ringe.

(ii) Nach Satz 10.7 ist $e = e_1 + \cdots + e_m$ mit paarweise orthogonalen streng primitiven Idempotenten $e_1, \ldots, e_m$ in R. Für $i = 1, \ldots, m$ ist $e_i(eRe)e_i = e_iRe_i$ lokal, d.h. $e_1 = ee_1e, \ldots, e_m = ee_me$ sind auch streng primitiv in eRe.

10.9. Bemerkung. Ein Ring R heißt **linksperfekt**, falls jeder R-Linksmodul eine projektive Decke besitzt. Analog definiert man **rechtsperfekte** Ringe. (I.a. sind diese Begriffe nicht äquivalent.) Ist R linksperfekt und rechtsperfekt, so nennt man R **perfekt**. Man kann zeigen, daß die folgenden Aussagen über einen Ring R äquivalent sind:

(1) R ist linksperfekt.

(2) $R/J(R)$ ist halbeinfach, und zu jeder Folge $a_1, a_2, a_3, \ldots$ von Elementen in $J(R)$ existiert ein $n \in \mathbb{N}$ mit $a_1 \ldots a_n = 0$.

(3) Jeder R-Rechtsmodul erfüllt die Minimalbedingung für zyklische Untermoduln.

Daraus folgt insbesondere, daß jeder links- oder rechtsartinsche Ring linksperfekt ist.

11 Das Tensorprodukt

Sei R ein Ring.

11.1. Definition. Gegeben seien ein R-Rechtsmodul M, ein R-Linksmodul N und ein $\mathbb{Z}$-Modul A. Eine Abbildung $f: M \times N \to A$ nennt man (R-)**ausgeglichen** (**balanced**), falls für alle $m, m' \in M$, $n, n' \in N$, $r \in R$ gilt:

(i) $f(m + m', n) = f(m, n) + f(m', n)$.

(ii) $f(m, n + n') = f(m, n) + f(m, n')$.

(iii) $f(mr, n) = f(m, rn)$.

Bemerkung. Daraus folgt leicht:

(iv) $f(m, 0) = 0 = f(0, n)$.

(v) $f(-m, n) = -f(m, n) = f(m, -n)$.

Beispiel. Die Multiplikationsabbildung $R \times R \to R$, $(a, b) \mapsto ab$, ist ausgeglichen.

11.2. Bemerkung. Gegeben seien ein R-Rechtsmodul M und ein R-Linksmodul N. Dann ist $A := \coprod_{(m,n)\in M\times N} \mathbb{Z}$ ein freier $\mathbb{Z}$-Modul mit kanonischer Basis $\{e_{(m,n)} : (m, n) \in M \times N\}$. Mit X bezeichnen wir die Teilmenge von A, die aus allen Elementen der folgenden Form besteht:

$$\left.\begin{array}{l} e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)} \\ e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')} \\ e_{(mr,n)} - e_{(m,rn)} \end{array}\right\} m, m' \in M,\ n, n' \in N,\ r \in R\,.$$

Mit B bezeichnen wir den von X erzeugten $\mathbb{Z}$-Untermodul von A. Den Faktormodul $M \otimes_R N := A/B$ nennt man das **Tensorprodukt** von M und N. (Dies ist ein $\mathbb{Z}$-Modul, kein R-Modul!) Für $m \in M$, $n \in N$ setzt man $m \otimes n := e_{(m,n)} + B \in M \otimes_R N$. Die Abbildung $t: M \times N \to M \otimes_R N$, $(m, n) \mapsto m \otimes n$, nennt man die kanonische Abbildung von $M \times N$ in $M \otimes_R N$.

Satz. *In der obigen Situation gilt:*

(i) Die kanonische Abbildung $t: M \times N \to M \otimes_R N$ ist ausgeglichen, d.h. es gilt

$$\left.\begin{array}{l} (m + m') \otimes n = m \otimes n + m' \otimes n \\ m \otimes (n + n') = m \otimes n + m \otimes n' \\ mr \otimes n = m \otimes rn \\ 0 \otimes n = 0 = m \otimes 0 \\ (-m) \otimes n = -(m \otimes n) = m \otimes (-n) \end{array}\right\} m, m' \in M,\ n, n' \in N,\ r \in R\,.$$

(ii) Jedes Element in $M \otimes_R N$ läßt sich in der Form $\sum_{i=1}^{k} m_i \otimes n_i$ mit endlich vielen Elementen $m_1, \ldots, m_k \in M$, $n_1, \ldots, n_k \in N$ schreiben.

Beweis.

(i) Für $m, m' \in M$, $n \in N$ ist $e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)} \in X \subseteq B$, also

$$\underbrace{t(m+m',n)}_{(m+m')\otimes n} - \underbrace{t(m,n)}_{m\otimes n} - \underbrace{t(m',n)}_{m'\otimes n} = \underbrace{e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)} + B}_{=0}$$

Die anderen Gleichungen beweist man analog.

(ii) Jedes Element in A läßt sich in der Form $\sum_{i=1}^{k} z_i e_{(m_i,n_i)}$ mit endlich vielen Elementen $m_1, \ldots, m_k \in M$, $n_1, \ldots, n_k \in N$, $z_1, \ldots, z_k \in \mathbb{Z}$ schreiben. Daher läßt sich jedes Element in $M \otimes_R N = {}^{A}/_{B}$ in der Form $\sum_{i=1}^{k} z_i \underbrace{e_{(m_i,n_i)} + B}_{m_i \otimes n_i}$ schreiben. Nach (i) ist aber $-(m \otimes n) = (-m) \otimes n$ $(m \in M,\, n \in N)$.

11.3. Bemerkung. Die Schreibweise $\sum_{i=1}^{k} m_i \otimes n_i$ für ein Element in $M \otimes_R N$ ist i.a. nicht eindeutig. Auch läßt sich in der Regel nicht jedes Element in $M \otimes_R N$ in der Form $m \otimes n$ mit $m \in M$, $n \in N$ schreiben.

Satz (Universelle Eigenschaft des Tensorprodukt). *Gegeben seien ein R-Rechtsmodul M und ein R-Linksmodul N. Mit $t : M \times N \to M \otimes_R N$, $(m,n) \mapsto m \otimes n$ bezeichnen wir die kanonische Abbildung. Dann existiert zu jedem $\mathbb{Z}$-Modul L und jeder ausgeglichenen Abbildung $f : M \times N \to L$ genau ein $\mathbb{Z}$-Homomorphismus $f' : M \otimes_R N \to L$ mit $f'(m \otimes n) = f(m,n)$ für $m \in M$, $n \in N$.*

$$\begin{tikzcd}
M \times N \arrow[rr, "t"] \arrow[dr, "f"'] & & M \otimes_R N \arrow[dl, dashed, "f'"] \\
& L &
\end{tikzcd}$$

Beweis. Wir verwenden die obigen Bezeichnungen. Offenbar ist die Abbildung

$$F : A \to L\,, \qquad (z_{(m,n)})_{(m,n)\in M\times N} \mapsto \sum_{(m,n)\in M\times N} z_{(m,n)} f(m,n)\,,$$

$\mathbb{Z}$-linear. Für alle $m, m' \in M$, $n, n' \in N$, $r \in R$ ist also

$$F(e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}) = f(m+m',n) - f(m,n) - f(m',n) = 0\,,$$

$$F(e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}) = 0\,,$$

$$F(e_{(mr,n)} - e_{(m,rn)}) = 0\,.$$

Folglich ist $F(B) = 0$. Man kann also eine Abbildung $f' : M \otimes_R N = {}^{A}/_{B} \to L$, $a + B \mapsto F(a)$, definieren, und f' ist $\mathbb{Z}$-linear. Ferner gilt für $m \in M$, $n \in N$: $f'(m \otimes n) = f'(e_{(m,n)} + B) = F(e_{(m,n)}) = f(m,n)$. Sei jetzt $f'' : M \otimes_R N \to L$ ein $\mathbb{Z}$-Homomorphismus mit $f''(m \otimes n) = f(m,n)$ für $m \in M$, $n \in N$. Dann ist $f''(m \otimes n) = f'(m \otimes n)$. Aus Satz 11.2 (ii) folgt also: $f'' = f'$.

11.4. Satz. *Gegeben seien R-Rechtsmoduln M, M', R-Linksmoduln N, N' und R-Homomorphismen $f : M \to M'$, $g : N \to N'$. Dann existiert genau ein $\mathbb{Z}$-Homomorphismus $h : M \otimes_R N \to M' \otimes_R N'$ mit $h(m \otimes n) = f(m) \otimes g(n)$ für $m \in M$, $n \in N$.*

Beweis. Die Abbildung $H : M \times N \to M' \otimes_R N'$, $(m, n) \mapsto f(m) \otimes g(n)$, ist ausgeglichen; für $m, m' \in M$, $n, n' \in N$, $r \in R$ gilt nämlich:

$$\begin{aligned} H(m+m', n) &= f(m+m') \otimes g(n) = \big(f(m) + f(m')\big) \otimes g(n) \\ &= f(m) \otimes g(n) + f(m') \otimes g(n) = H(m,n) + H(m',n) \ , \\ H(m, n+n') &= f(m) \otimes g(n+n') = f(m) \otimes \big(g(n) + g(n')\big) \\ &= f(m) \otimes g(n) + f(m) \otimes g(n') = H(m,n) + H(m,n') \ , \\ H(mr, n) &= f(mr) \otimes g(n) = f(m)r \otimes g(n) \\ &= f(m) \otimes rg(n) = f(m) \otimes g(rn) = H(m, rn) \ . \end{aligned}$$

$$\begin{tikzcd} M \times N \arrow[rr, "t"] \arrow[dr, "H"'] & & M \otimes_R N \arrow[dl, "h"] \\ & M' \otimes_R N' & \end{tikzcd}$$

Es existiert also genau ein $\mathbb{Z}$-Homomorphismus $h : M \otimes_R N \to M' \otimes_R N'$ mit $h(m \otimes n) = H(m,n) = f(m) \otimes g(n)$ für $m \in M$, $n \in N$.

Definition. Man nennt h das **Tensorprodukt** von f und g und schreibt $h = f \otimes g$.

Bemerkung. Es ist also $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ mit $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ für $m \in M$, $n \in N$.

11.5. Satz.

(i) *Für R-Rechtsmoduln M, M', M'', R-Linksmoduln N, N', N'' und R-Homomorphismen $M \xrightarrow{f} M' \xrightarrow{f'} M''$, $N \xrightarrow{g} N' \xrightarrow{g'} N''$ gilt stets: $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.*

(ii) *Stets ist $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}$.*

(iii) *Für R-Rechtsmoduln M, M', R-Linksmoduln N, N' und R-Homomorphismen $f, f' : M \to M'$, $g, g' : N \to N'$ gilt stets*

$$\begin{aligned} &(f + f') \otimes g = f \otimes g + f' \otimes g \ , \\ &f \otimes (g + g') = f \otimes g + f \otimes g' \ , \\ &f \otimes 0 = 0 = 0 \otimes g \ , \\ &(-f) \otimes g = -(f \otimes g) = f \otimes (-g) \ . \end{aligned}$$

Beweis.

(i) Für $m \in M$, $n \in N$ gilt:

$$\begin{aligned}\big[(f' \otimes g') \circ (f \otimes g)\big](m \otimes n) &= (f' \otimes g')\big(f(m) \otimes g(n)\big) \\ &= f'\big(f(m)\big) \otimes g'\big(g(n)\big) \\ &= (f' \circ f)(m) \otimes (g' \circ g)(n) \\ &= \big[(f' \circ f) \otimes (g' \circ g)\big](m \otimes n) \ .\end{aligned}$$

(ii) Trivial.

(iii) Analog.

11.6. Satz. *Für jeden R-Rechtsmodul M existiert genau ein $\mathbb{Z}$-Isomorphismus $\mu : M \otimes_R R \to M$ mit $\mu(m \otimes r) = mr$ für $m \in M$, $r \in R$.*

Definition. Man nennt μ den **kanonischen** Isomorphismus zwischen $M \otimes_R R$ und M.

Beweis. Man zeigt leicht, daß die Abbildung $f : M \times R \to M$, $(m, r) \mapsto mr$ ausgeglichen ist. Folglich existiert genau ein $\mathbb{Z}$-Homomorphismus $\mu : M \otimes_R R \to M$ mit $\mu(m \otimes r) = f(m, r) = mr$ für $m \in M$, $r \in R$. Andererseits ist die Abbildung $\nu : M \to M \otimes_R R$, $m \mapsto m \otimes 1$, offenbar $\mathbb{Z}$-linear. Für $m \in M$, $r \in R$ ist

$$\begin{aligned}&\nu\big(\mu(m \otimes r)\big) = \nu(mr) = mr \otimes 1 = m \otimes r1 = m \otimes r \ , \\ &\mu\big(\nu(m)\big) = \mu(m \otimes 1) = m1 = m \ .\end{aligned}$$

Bemerkung. Analog hat man für jeden R-Linksmodul N einen **kanonischen** $\mathbb{Z}$-Isomorphismus $\nu : R \otimes_R N \to N$ mit $\nu(r \otimes n) = rn$ für $r \in R$, $n \in N$.

11.7. Satz. *Für jede Familie $(M_i)_{i \in I}$ von R-Rechtsmoduln M_i und jeden R-Linksmodul N gilt:*

$$\Big(\coprod_{i \in I} M_i\Big) \otimes_R N \cong \coprod_{i \in I} (M_i \otimes_R N)$$

Beweis. Wir setzen $M := \coprod_{i \in I} M_i$. Für $j \in I$ seien $p_j : M \to M_j$ und $q_j : M_j \to M$ der entsprechende Projektor bzw. Injektor. Dann sind $p_j \otimes \mathrm{id}_N : M \otimes_R N \to M_j \otimes_R N$, $q_j \otimes \mathrm{id}_N : M_j \otimes_R N \to M \otimes_R N$, $\mathbb{Z}$-Homomorphismen. Wir erhalten also $\mathbb{Z}$-Homomorphismen

$$\begin{aligned}&f : \coprod_{j \in I} (M_j \otimes_R N) \to M \otimes_R N \ , && (x_j)_{j \in I} \mapsto \sum_{j \in I} (q_j \otimes \mathrm{id}_N)(x_j) \ , \\ &g : M \otimes_R N \to \coprod_{j \in I} (M_j \otimes_R N) \ , && x \mapsto \big((p_j \otimes \mathrm{id}_N)(x)\big)_{j \in I} \ .\end{aligned}$$

Dabei beachte man, daß für $x \in M \otimes_R N$ die Menge $\{j \in I : (p_j \otimes \mathrm{id}_N)(x) \neq 0\}$ endlich ist; denn dies ist der Fall für ein Element der Form $(m_i)_{i \in I} \otimes n$, und dies vererbt sich auf endliche Summen von solchen Elementen. Für $m = (m_i)_{i \in I} \in M$ und $n \in N$ ist

$$f\big(g(m \otimes n)\big) = f\big((m_j \otimes n)_{j \in I}\big) = \sum_{j \in I} q_j(m_j) \otimes n = m \otimes n \ .$$

Daher ist $f \circ g = \mathrm{id}$. Analog gilt für $x = (x_j)_{j\in I} \in \coprod_{j\in I} M_j \otimes_R N$:

$$g\big(f(x)\big) = \sum_{j\in I} g\big((q_j \otimes \mathrm{id}_N)(x_j)\big) = \sum_{j\in I} \Big(\underbrace{(p_i \otimes \mathrm{id}_N)\big[(q_j \otimes \mathrm{id}_N)}_{\underbrace{(p_i \circ q_j)}_{0 \text{ oder } \mathrm{id}_{M_j}} \otimes \mathrm{id}_N}(x_j)\big]\Big)_{i\in I}$$

$$= \sum_{j\in I} (\delta_{ij} x_j)_{i\in I} = (x_j)_{j\in I}\ .$$

Folglich ist auch $g \circ f = \mathrm{id}$.

Definition. Man nennt die im Beweis konstruierte Abbildung g den **kanonischen** Isomorphismus zwischen $\big(\coprod_{i\in I} M_i\big) \otimes_R N$ und $\coprod_{i\in I} (M_i \otimes_R N)$.

Bemerkung. Analog hat man für jeden R-Rechtsmodul M und jede Familie $(N_i)_{i\in I}$ von R-Linksmoduln N_i einen **kanonischen** $\mathbb{Z}$-Isomorphismus zwischen $M \otimes_R \big(\coprod_{i\in I} N_i\big)$ und $\coprod_{i\in I} (M \otimes_R N_i)$.

11.8. Satz. *Für jeden R-Rechtsmodul M und jede exakte Folge von R-Linksmoduln*

$$0 \longrightarrow N \xrightarrow{g} N' \xrightarrow{g'} N'' \longrightarrow 0 \tag{$*$}$$

ist die folgende Sequenz von $\mathbb{Z}$-Moduln exakt:

$$M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes g} M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes g'} M \otimes_R N'' \longrightarrow 0\ . \tag{$**$}$$

Zerfällt $(*)$, so ist die folgende Sequenz von $\mathbb{Z}$-Moduln exakt und zerfallend:

$$0 \longrightarrow M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes g} M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes g'} M \otimes_R N'' \longrightarrow 0\ . \tag{$***$}$$

Beweis. Jedes Element in $M \otimes_R N''$ läßt sich in der Form $x = \sum_{i=1}^k m_i \otimes n_i''$ mit endlich vielen $m_1, \dots, m_k \in M$ und $n_1'', \dots, n_k'' \in N''$ schreiben. Da g' surjektiv ist, existiert für $i = 1, \dots, k$ ein Element $n_i' \in N'$ mit $n_i'' = g'(n_i')$. Folglich ist

$$x = \sum_{i=1}^k m_i \otimes g'(n_i') = \sum_{i=1}^k (\mathrm{id}_M \otimes g')(m_i \otimes n_i') = (\mathrm{id}_M \otimes g')\Big(\sum_{i=1}^k m_i \otimes n_i'\Big)\ .$$

Dies zeigt, daß $\mathrm{id}_M \otimes g'$ surjektiv ist. Offenbar ist $(\mathrm{id}_M \otimes g') \circ (\mathrm{id}_M \otimes g) = \mathrm{id}_M \otimes \underbrace{(g' \circ g)}_{=0} = 0$.

Daher ist $B := \mathrm{Bld}(\mathrm{id}_M \otimes g) \subseteq \mathrm{Ker}(\mathrm{id}_M \otimes g') =: K$.
Zum Beweis der umgekehrten Inklusion definieren wir eine Abbildung

$$f : M \times N'' \to {}^{M \otimes_R N'}\!/_B\ , \quad \big(m, g'(n')\big) \mapsto m \otimes n' + B\ .$$

Dies ist wohldefiniert; sind nämlich $n_1', n_2' \in N'$ mit $g'(n_1') = g'(n_2')$, so ist $n_1' - n_2' \in \mathrm{Ker}(g') = \mathrm{Bld}(g)$, d.h. $n_1' - n_2' = g(n)$ für ein $n \in N$. Damit ist

$$m \otimes n_1' + B = m \otimes n_2' + B + \underbrace{m \otimes g(n)}_{(\mathrm{id}_M \otimes g)(m \otimes n) \in B} + B = m \otimes n_2' + B\ .$$

Man rechnet leicht nach, daß f ausgeglichen ist. Es existiert also ein $\mathbb{Z}$-Homomorphismus f' : $M \otimes_R N'' \to {(M \otimes_R N')}/{B}$ mit $f'(m \otimes n'') = f(m, n'')$ für $m \in M$, $n'' \in N''$. Insbesondere ist

$$\big[f' \circ (\mathrm{id}_M \otimes g')\big](m \otimes n') = f'\big(m \otimes g'(n')\big) = f\big(m, g'(n')\big) = m \otimes n' + B$$

für $m \in M$, $n' \in N'$. Daher ist $\big[f' \circ (\mathrm{id}_M \otimes g')\big](x) = x + B$ für beliebige $x \in M \otimes N'$. Insbesondere gilt für alle $x \in K = \mathrm{Ker}(\mathrm{id}_M \otimes g')$:

$$0 = \big[f' \circ (\mathrm{id}_M \otimes g')\big](x) = x + B ,$$

d.h. $x \in B$. Damit ist auch $K \subseteq B$.
Jetzt zerfalle $(*)$. Dann existiert ein R-Homomorphismus $h : N' \to N$ mit $h \circ g = \mathrm{id}_N$. Daher ist $\mathrm{id}_M \otimes h : M \otimes_R N' \to M \otimes_R N$ ein $\mathbb{Z}$-Homomorphismus mit

$$(\mathrm{id}_M \otimes h) \circ (\mathrm{id}_M \otimes g) = \mathrm{id}_M \otimes (h \circ g) = \mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_R N} \ .$$

Folglich ist $\mathrm{id}_M \otimes g$ injektiv, und die Folge $(***)$ zerfällt.

Bemerkung. Analog ist für jede exakte Folge

$$0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{f'} M'' \longrightarrow 0 \tag{$*$}$$

von R-Rechtsmoduln und jeden R-Linksmodul N ...

Beispiel. Für $k \in \mathbb{N}$ betrachten wir die exakte Folge von $\mathbb{Z}$-Moduln $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \longrightarrow {\mathbb{Z}}/{k\mathbb{Z}} \longrightarrow 0$; dabei sei $f(z) := kz$ für $z \in \mathbb{Z}$. Für $l \in \mathbb{Z}$ ist also die folgende Sequenz exakt:

$$\mathbb{Z} \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) \xrightarrow{f \otimes \mathrm{id}} \mathbb{Z} \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) \longrightarrow \left({\mathbb{Z}}/{k\mathbb{Z}}\right) \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) \longrightarrow 0 \ .$$

Nach dem Homomorphiesatz ist also

$$\left({\mathbb{Z}}/{k\mathbb{Z}}\right) \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) \cong {\mathbb{Z} \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right)}/{\mathrm{Bld}(f \otimes \mathrm{id})} \, .$$

Für $x \in \mathbb{Z}$, $y \in {\mathbb{Z}}/{l\mathbb{Z}}$ ist

$$(f \otimes \mathrm{id})(x \otimes y) = f(x) \otimes y = (kx) \otimes y = k(x \otimes y) \ .$$

Daher ist $f \otimes \mathrm{id}$ nichts anderes als Multiplikation mit k. Folglich ist

$$\left({\mathbb{Z}}/{k\mathbb{Z}}\right) \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) \cong {\mathbb{Z} \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right)}/{k\left(\mathbb{Z} \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right)\right)} \, .$$

Ferner ist $\mathbb{Z} \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) \cong {\mathbb{Z}}/{l\mathbb{Z}}$. Daher ist

$$\begin{aligned}\left({\mathbb{Z}}/{k\mathbb{Z}}\right) \otimes_{\mathbb{Z}} \left({\mathbb{Z}}/{l\mathbb{Z}}\right) &\cong {\left({\mathbb{Z}}/{l\mathbb{Z}}\right)}/{\underbrace{k\left({\mathbb{Z}}/{l\mathbb{Z}}\right)}_{{k\mathbb{Z}+l\mathbb{Z}}/{l\mathbb{Z}}}} \cong {\mathbb{Z}}/{\underbrace{(k\mathbb{Z} + l\mathbb{Z})}_{\mathrm{ggT}(k,l)\mathbb{Z}}} \\ &= {\mathbb{Z}}/{\mathrm{ggT}(k,l)\mathbb{Z}} \, .\end{aligned}$$

Fr alle $k, l \in \mathbb{Z}$ gilt also:

$$\left(\mathbb{Z}/_{k\mathbb{Z}}\right) \otimes_{\mathbb{Z}} \left(\mathbb{Z}/_{l\mathbb{Z}}\right) \cong \mathbb{Z}/_{\mathrm{ggT}(k,l)\mathbb{Z}} \,.$$

Im Fall $k = l$ ist $k(x \otimes y) = x \otimes \underbrace{(ky)}_{=0} = 0$ fr alle $x \in \mathbb{Z}$, $y \in \mathbb{Z}/_{l\mathbb{Z}}$, d.h. $f \otimes \mathrm{id} = 0$. Fr $k \geq 2$ ist also $f \otimes \mathrm{id}$ nicht injektiv, d.h. i.a. folgt aus der Exaktheit von $(*)$ nicht die von $(***)$. **Fr einen Untermodul M eines R-Moduls M' kann man also $M \otimes_R N$ i.a. nicht als Untermodul von $M' \otimes N$ auffassen!**

11.9. Definition. Man nennt einen R-Linksmodul N **flach** (**flat**), falls fr jede exakte Folge von R-Rechtsmoduln $0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{f'} M'' \longrightarrow 0$ die folgende Sequenz von $\mathbb{Z}$-Moduln exakt ist:

$$0 \longrightarrow M \otimes_R N \xrightarrow{f \otimes \mathrm{id}_N} M' \otimes_R N \xrightarrow{f' \otimes \mathrm{id}_N} M'' \otimes_R N \longrightarrow 0 \,.$$

Analog definiert man **flache** R-Rechtsmoduln.

Satz.

(i) Fr jede Familie $(N_i)_{i \in I}$ von R-Linksmoduln N_i gilt:

$$\coprod_{i \in I} N_i \text{ ist flach } \iff N_i \text{ ist flach fr jedes } i \in I \,.$$

(ii) Jeder projektive R-Linksmodul ist flach.

Beweis.

(i) Wir setzen $N := \coprod_{i \in I} N_i$ und bezeichnen mit p_i und q_i die entsprechenden Projektoren und Injektoren. Fr jede exakte Folge von R-Rechtsmoduln $0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{f'} M'' \longrightarrow 0$ betrachten wir das Diagramm

$$\begin{array}{ccc} M \otimes_R N & \xrightarrow{f \otimes \mathrm{id}_N} & M' \otimes_R N \\ {\scriptstyle h}\downarrow\wr & & {\scriptstyle h'}\downarrow\wr \\ \coprod_{i \in I} (M \otimes_R N_i) & \xrightarrow{g} & \coprod_{i \in I} (M' \otimes_R N_i) \end{array}$$

dabei sind h, h' die kanonischen Isomorphismen aus Satz 11.7, und g ist definiert durch $g\big((x_i)_{i \in I}\big) = \big((f \otimes \mathrm{id}_{N_i})(x_i)\big)_{i \in I}$. Ferner ist $h' \circ (f \otimes \mathrm{id}_N) = g \circ h$; denn fr $m \in M$, $n = (n_i)_{i \in I} \in N$ gilt:

$$\begin{aligned} \big[h' \circ (f \otimes \mathrm{id}_N)\big](m \otimes n) &= h'\big(f(m) \otimes n\big) = \Big((\mathrm{id}_{M'} \otimes p_i)\big(f(m) \otimes n\big)\Big)_{i \in I} \\ &= \big(f(m) \otimes n_i\big)_{i \in I} = \big((f \otimes \mathrm{id}_{N_i})(m \otimes n_i)\big)_{i \in I} \\ &= g\big((m \otimes n_i)_{i \in I}\big) = g\big(h(m \otimes n)\big) \,. \end{aligned}$$

Also gilt: $f \otimes \mathrm{id}_N$ ist injektiv $\iff g$ injektiv $\iff f \otimes \mathrm{id}_{N_i}$ injektiv fr alle i.

(ii) Wir zeigen zunchst, da der regulre R-Linksmodul R flach ist. Dazu sei wieder $0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{f'} M'' \longrightarrow 0$ eine exakte Folge von R-Rechtsmoduln. Wir betrachten das Diagramm

$$\begin{tikzcd}
M \otimes_R R \arrow[r, "f \otimes \mathrm{id}_R"] \arrow[d, "\mu"', "\wr"] & M' \otimes_R R \arrow[d, "\mu'"', "\wr"] \\
M \arrow[r, "f"] & M'
\end{tikzcd}$$

Dabei sind μ, μ' die kanonischen Isomorphismen aus Satz 11.6. Fr $m \in M$, $r \in R$ ist

$$\big(\mu' \circ (f \otimes \mathrm{id}_R)\big)(m \otimes r) = \mu'\big(f(m) \otimes r\big) = f(m)r = f(mr) = f\big(\mu(m \otimes r)\big) \ .$$

Daher ist mit f auch $f \otimes \mathrm{id}_R$ injektiv. Damit ist gezeigt, da der regulre R-Linksmodul flach ist. Nach (i) ist also jeder freie R-Linksmodul flach. Nach (i) sind also auch projektive R-Linksmoduln flach.

12 Bimoduln

Seien R, S, T Ringe.

12.1. Definition. Ein R-S-**Bimodul** ist eine Menge M mit Verknpfungen

$$\begin{array}{rlll} M \times M & \to M\ , & (x,y) & \mapsto x+y\ , \\ R \times M & \to M\ , & (r,x) & \mapsto rx\ , \\ M \times S & \to M\ , & (x,s) & \mapsto xs\ , \end{array}$$

die folgende Bedingungen erfllen:

(i) M ist R-Linksmodul und S-Rechtsmodul.

(ii) Fr $r \in R$, $s \in S$, $m \in M$ ist $(rm)s = r(ms)$.

Beispiele.

(a) R selbst ist in natrlicher Weise ein R-R-Bimodul.

(b) Jeder R-Rechtsmodul M kann in natrlicher Weise als $\mathrm{End}_R(M)$-R-Bimodul aufgefat werden:

$$f(mr) = f(m)r \qquad \big(f \in \mathrm{End}_R(M), m \in M, r \in R\big)\ .$$

Analog kann jeder R-Linksmodul N in natrlicher Weise als R-$\mathrm{End}_R(N)^\circ$-Bimodul aufgefat werden.

Bemerkung. Man kann weite Teile der Modultheorie fr Bimoduln entwickeln: Unterbimoduln, Faktorbimoduln, Homomorphismen von Bimoduln, Isomorphiestze, usw. Dies werden wir nicht im Detail tun, sondern stillschweigend benutzen.

12.2. Bemerkungen.

(i) Gegeben seien ein R-S-Bimodul M und ein R-T-Bimodul N. Dann wird $\mathrm{Hom}_R(M,N)$ zu einem S-T-Bimodul mit $(sf)(m) = f(ms)$ und $(ft)(m) = f(m)t$ fr $s \in S$, $t \in T$, $f \in \mathrm{Hom}_R(M,N)$, $m \in M$; dies rechnet man leicht nach.

(ii) Gegeben seien ein R-S-Bimodul M und ein T-S-Bimodul N. Dann wird $\mathrm{Hom}_S(M,N)$ analog zu einem T-R-Bimodul mit $(tf)m = tf(m)$ und $(fr)(m) = f(rm)$ fr $r \in R$, $t \in T$, $f \in \mathrm{Hom}_R(M,N)$, $m \in M$.

Satz. *Fr jeden R-S-Bimodul M und jeden S-T-Bimodul N wird $M \otimes_S N$ zu einem R-T-Bimodul mit $r(m \otimes n) = (rm) \otimes n$ und $(m \otimes n)t = m \otimes (nt)$ fr $r \in R$, $t \in T$, $m \in M$, $n \in N$.*

Beweis. Fr $r \in R$ ist die Abbildung $f_r : M \times N \to M \otimes_S N$, $(m,n) \mapsto (rm) \otimes n$, S-ausgeglichen. Daher existiert genau ein $\mathbb{Z}$-Homomorphismus $f'_r : M \otimes_S N \to M \otimes_S N$ mit $f'_r(m \otimes n) = f_r(m,n) = (rm) \otimes n$ fr $m \in M$, $n \in N$. Fr $r, r' \in R$, $m \in M$, $n \in N$ gilt dann:

$$\begin{aligned} (f'_r \circ f'_{r'})(m \otimes n) &= f'_r\big((r'm) \otimes n\big) = (r \cdot r'm) \otimes n \\ &= (rr' \cdot m) \otimes n = f'_{rr'}(m \otimes n)\ ; \\ (f'_r + f'_{r'})(m \otimes n) &= \cdots = f'_{r+r'}(m \otimes n)\ ; \\ f'_1(m \otimes n) &= m \otimes n\ . \end{aligned}$$

Folglich ist $f'_r \circ f'_{r'} = f'_{rr'}$; $f'_r + f'_{r'} = f'_{r+r'}$; $f'_1 = \mathrm{id}_{M\otimes_S N}$. Definiert man also $rx := f'_r(x)$ fr $r \in R$, $x \in M \otimes_S N$, so wird $M \otimes_S N$ zu einem R-Linksmodul; denn fr alle $x, y \in M \otimes_S N$ und $r, r' \in R$ gilt: $r(r'x) = f'_r\big(f'_{r'}(x)\big) = f'_{rr'}(x) = (rr')x$; $(r + r')x = \cdots = rx + r'x$; $r(x + y) = \cdots = rx + ry$; $1x = \cdots = x$. Fr $r \in R$, $m \in M$, $n \in N$ ist ferner $r(m \otimes n) = f'_r(m\otimes n) = (rm)\otimes n$. Analog wird $M\otimes_S N$ zu einem T-Rechtsmodul mit $(m\otimes n)t = m\otimes(nt)$ fr $m \in M$, $n \in N$, $t \in T$. Ferner gilt fr $r \in R$, $t \in T$, $m \in M$, $n \in N$:

$$\big[r(m \otimes n)\big]t = \big[(rm) \otimes n\big]t = (rm) \otimes (nt) = r\big[m \otimes (nt)\big] = r\big[(m \otimes n)t\big] \ .$$

12.3. Satz. *Fr jeden R-Rechtsmodul L, jeden R-S-Bimodul M und jeden S-Linksmodul N existiert genau ein $\mathbb{Z}$-Isomorphismus*

$$f : (L \otimes_R M) \otimes_S N \to L \otimes_R (M \otimes_S N) \ ,$$

mit $f\big((x \otimes y) \otimes z\big) = x \otimes (y \otimes z)$ fr $x \in L$, $y \in M$, $z \in N$.

Beweis. Fr $z \in N$ ist die Abbildung $\beta_z : L \times M \to L\otimes_R (M \otimes_S N)$, $(x, y) \mapsto x \otimes (y \otimes z)$, R-ausgeglichen. Daher existiert genau ein $\mathbb{Z}$-Homomorphismus $\beta'_z : L\otimes_R M \to L\otimes_R (M \otimes_S N)$ mit $\beta'_z(x \otimes y) = \beta_z(x, y) = x \otimes (y \otimes z)$ fr $x \in L$, $y \in M$. Man zeigt leicht, da $\beta'_{z+z'} = \beta'_z + \beta'_{z'}$ und $\beta'_{sz}(u) = \beta'_z(us)$ fr $z, z' \in N$, $s \in S$, $u \in L\otimes_R M$ gilt. Daraus folgt, da die Abbildung $\gamma : (L\otimes_R M) \times N \to L\otimes_R (M \otimes_S N)$, $(u, z) \mapsto \beta'_z(u)$, S-ausgeglichen ist. Es existiert also genau ein $\mathbb{Z}$-Homomorphismus $f : (L\otimes_R M)\otimes_S N \to L\otimes_R (M\otimes_S N)$ mit $f(u\otimes z) = \gamma(u, z) = \beta'_z(u)$ fr $u \in L \otimes_R M$ und $z \in N$. Insbesondere ist $f\big((x \otimes y) \otimes z\big) = \beta'_z(x \otimes y) = x \otimes (y \otimes z)$ fr $x \in L$, $y \in M$, $z \in N$.
Analog existiert ein $\mathbb{Z}$-Homomorphismus $g : L \otimes_R (M \otimes_S N) \to (L \otimes_R M) \otimes_S N$ mit $g\big(x \otimes (y \otimes z)\big) = (x \otimes y) \otimes z$ fr $x \in L$, $y \in M$, $z \in N$. Man zeigt leicht: $g \circ f = \mathrm{id}_{(L\otimes_R M)\otimes_S N}$, $f \circ g = \mathrm{id}_{L\otimes_R (M\otimes_S N)}$. Die Eindeutigkeit von f ist klar.

Bemerkungen.

(i) Man nennt f den **kanonischen** Isomorphismus zwischen $(L \otimes_R M) \otimes_S N$ und $L \otimes_R (M \otimes_S N)$. Oft identifiziert man diese beiden $\mathbb{Z}$-Moduln vermge f und schreibt dann auch $L \otimes_R \otimes_S N$. Entsprechend schreibt man $x \otimes y \otimes z$ fr $x \in L$, $y \in M$, $z \in N$.

(ii) Sind Q, T weitere Ringe, und ist L ein Q-R-Bimodul und N ein S-T-Bimodul, so ist f ein Isomorphismus von Q-T-Bimoduln.

(iii) Analog sind viele der kanonischen $\mathbb{Z}$-Isomorphismen in § 11 Isomorphismen von Bimoduln, wenn die beteiligten Moduln Bimoduln sind.

12.4. Satz (Frobenius-Nakayama-Relation). *Fr jeden R-Rechtsmodul L, jeden R-S-Bimodul M und jeden S-Rechtsmodul N hat man einen $\mathbb{Z}$-Isomorphismus* $\mathrm{Hom}_S(L \otimes_R M, N) \cong \mathrm{Hom}_R\big(L, \mathrm{Hom}_S(M, N)\big)$.

Beweis. (Nach Bemerkung 12.2 (ii) ist $\mathrm{Hom}_S(M, N)$ ein R-Rechtsmodul mit $(fr)(m) = f(rm)$ fr $f \in \mathrm{Hom}_S(M, N)$, $r \in R$, $m \in M$.) Fr $\alpha \in \mathrm{Hom}_S(L \otimes_R M, N)$ und $x \in L$ ist die Abbildung $\alpha_x : M \to N$, $y \mapsto \alpha(x \otimes y)$, S-linear, d.h. $\alpha_x \in \mathrm{Hom}_S(M, N)$. Ferner gilt $\alpha_{x+x'} = \alpha_x + \alpha_{x'}$, $\alpha_{xr} = \alpha_x r$ fr $x, x' \in L$, $r \in R$: $(\alpha_x r)(y) = \alpha_x(ry) = \alpha(x \otimes ry) = \alpha(xr \otimes y) = \alpha_{xr}(y)$. Daher ist die Abbildung $\beta_\alpha : L \to \mathrm{Hom}_S(M, N)$, $x \mapsto \alpha_x$, R-linear. Wir erhalten also eine Abbildung $\beta : \mathrm{Hom}_S(L \otimes_R M, N) \to \mathrm{Hom}_R\big(L, \mathrm{Hom}_S(M, N)\big)$, $\alpha \mapsto \beta_\alpha$. Man rechnet leicht nach, da β $\mathbb{Z}$-linear ist. Fr $\varphi \in \mathrm{Hom}_R\big(L, \mathrm{Hom}_S(M, N)\big)$ ist umgekehrt die Abbildung $\omega_\varphi : L \times M \to N$, $(x, y) \mapsto \bigl[\varphi(x)\bigr](y)$, R-ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\omega'_\varphi : L \otimes_R M \to N$ mit $\omega'_\varphi(x \otimes y) = \omega_\varphi(x, y) = \bigl[\varphi(x)\bigr](y)$ fr $x \in L$, $y \in M$. Man zeigt leicht: $\omega'_\varphi \in \mathrm{Hom}_S(L \otimes M, N)$. Wir erhalten also eine Abbildung $\omega : \mathrm{Hom}_R\bigl(L, \mathrm{Hom}_S(M, N)\bigr) \to \mathrm{Hom}_S(L \otimes_R M, N)$, $\varphi \mapsto \omega'_\varphi$. Man zeigt leicht, da ω $\mathbb{Z}$-linear ist. Auerdem rechnet man nach, da $\beta_{\omega'_\varphi} = \varphi$ und $\omega'_{\beta_\alpha} = \alpha$ fr $\varphi \in \mathrm{Hom}_R\bigl(L, \mathrm{Hom}_S(M, N)\bigr)$ und $\alpha \in \mathrm{Hom}_S(L \otimes_R M, N)$ ist. Daher ist β bijektiv und $\beta^{-1} = \omega$.

Bemerkungen.

(i) Man nennt den im Beweis konstruierten $\mathbb{Z}$-Isomorphismus β **kanonisch**.

(ii) Analog hat man fr jeden R-S-Bimodul L, jeden S-Linksmodul M und jeden R-Rechtsmodul N einen **kanonischen** $\mathbb{Z}$-Isomorphismus

$$\mathrm{Hom}_R(L \otimes_S M, N) \cong \mathrm{Hom}_S\bigl(M, \mathrm{Hom}_R(L, N)\bigr) \ .$$

(iii) Der Satz ist die ringtheoretische Version der Bijektion

$$\mathrm{Abb}(L \times M, N) \to \mathrm{Abb}\bigl(L, \mathrm{Abb}(M, N)\bigr) \ ,$$

die man vielleicht besser in der folgenden Form schreibt:

$$N^{L \times M} \to (N^M)^L \ .$$

13 Kategorien und Funktoren

13.1. Definition. Eine **Kategorie** besteht aus folgenden Dingen:

(1) einer **Klasse** $\mathcal{C}$; die Elemente in $\mathcal{C}$ nennt man **Objekte**;

(2) einer Menge $\mathcal{C}(A, B)$ zu jedem Paar (A, B) von Objekten in $\mathcal{C}$; die Elemente in $\mathcal{C}(A, B)$ nennt man **Morphismen** von A nach B. Man schreibt sie in der Form $f : A \to B$ oder $A \xrightarrow{f} B$;

(3) einer Abbildung $\mathcal{C}(B, C) \times \mathcal{C}(A, B) \to \mathcal{C}(A, C)$, $(g, f) \mapsto g \circ f$, zu jedem Tripel (A, B, C) von Objekten in $\mathcal{C}$; diese Abbildung nennt man **Komposition**.

Dabei verlangt man, daß folgende Axiome erfüllt sind:

(i) $\mathcal{C}(A, B) \cap \mathcal{C}(C, D) = \emptyset$ für alle $A, B, C, D \in \mathcal{C}$ mit $(A, B) \neq (C, D)$.

(ii) $h \circ (g \circ f) = (h \circ g) \circ f$ für alle $A, B, C, D \in \mathcal{C}$, $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$, $h \in \mathcal{C}(C, D)$.

(iii) Für $A \in \mathcal{C}$ existiert ein Element $\mathrm{id}_A \in \mathcal{C}(A, A)$ mit $f \circ \mathrm{id}_A = f$ und $\mathrm{id}_A \circ g = g$ für alle $B \in \mathcal{C}$, $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, A)$.

Bemerkungen.

(i) Sind Morphismen und Kompositionen aus dem Zusammenhang klar, so sagt man kurz: $\mathcal{C}$ ist eine Kategorie.

(ii) Bekanntlich ist die „Gesamtheit" aller Mengen keine Menge mehr. Um Widersprüche dieser Art zu vermeiden, hat man den Begriff der „Klasse" eingeführt. Was Klassen genau sind, werden wir nicht definieren. Beispielsweise ist die Gesamtheit aller Mengen eine Klasse.

(iii) Für $A \in \mathcal{C}$ ist id_A eindeutig bestimmt; man nennt id_A die **Identität** von A in $\mathcal{C}$

Beispiele.

(a) Die Gesamtheit aller Mengen und Abbildungen bildet eine Kategorie; diese bezeichnen wir mit **Set**. Für Mengen A, B ist also $\mathbf{Set}(A, B) = \mathrm{Abb}(A, B)$ die Menge aller Abbildungen von A nach B.

(b) Die Gesamtheit aller Ringe und Ringhomomorphismen bildet eine Kategorie; diese bezeichnen wir mit **Ri**.

(c) Für jeden Ring R bildet die Gesamtheit aller R-Linksmoduln und R-Homomorphismen eine Kategorie; diese bezeichnen wir mit ${}_R\mathbf{Mod}$. Analog hat man eine Kategorie $\mathbf{Mod}_R$ von R-Rechtsmoduln und auch eine Kategorie ${}_R\mathbf{Mod}_S$ von R-S-Bimoduln ($R, S \in \mathbf{Ri}$). Für $M, N \in {}_R\mathbf{Mod}$ ist dabei ${}_R\mathbf{Mod}(M, N) = \mathrm{Hom}_R(M, N)$.

13.2. Definition. Gegeben seien Kategorien $\mathcal{C}$, $\mathcal{D}$. Ein **Funktor** von $\mathcal{C}$ nach $\mathcal{D}$ besteht aus folgenden Dingen:

(1) einer Abbildung $\Phi : \mathcal{C} \to \mathcal{D}$, $A \mapsto \Phi(A)$;

(2) einer Abbildung $\mathcal{C}(A, B) \to \mathcal{D}\big(\Phi(A), \Phi(B)\big)$, $f \mapsto \Phi(f)$, zu jedem Paar (A, B) von Objekten in $\mathcal{C}$.

Dabei verlangt man, daß folgende Axiome erfüllt sind:

(i) $\Phi(g \circ f) = \Phi(g) \circ \Phi(f)$ für alle $A, B, C \in \mathcal{C}$, $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$.

(ii) $\Phi(\mathrm{id}_A) = \mathrm{id}_{\Phi(A)}$ für $A \in \mathcal{C}$.

Gegebenenfalls schreibt man $\Phi : \mathcal{C} \to \mathcal{D}$ oder $\mathcal{C} \xrightarrow{\Phi} \mathcal{D}$.

Beispiele.

(a) Der **Vergißfunktor Ri** $\to$ **Set**, der jedem Ring R die zugrundeliegende Menge R zuordnet. In ähnlicher Weise hat man Vergißfunktoren ${}_R\mathbf{Mod} \to \mathbf{Set}$, ${}_R\mathbf{Mod} \to {}_\mathbb{Z}\mathbf{Mod}$, ${}_R\mathbf{Mod}_S \to {}_R\mathbf{Mod}$, usw.

(b) Für jede Kategorie $\mathcal{C}$ hat man den **Identitätsfunktor** $\mathrm{Id}_\mathcal{C} : \mathcal{C} \to \mathcal{C}$; dieser wird durch $\mathrm{Id}_\mathcal{C}(A) := A$ und $\mathrm{Id}_\mathcal{C}(f) := f$ für $A, B \in \mathcal{C}$, $f \in \mathcal{C}(A, B)$ definiert.

(c) Für jedes Objekt X einer Kategorie $\mathcal{C}$ hat man einen Funktor $\mathcal{C}(X, ?) : \mathcal{C} \to \mathbf{Set}$; dieser ordnet einem Objekt A in $\mathcal{C}$ die Menge $\mathcal{C}(X, A)$ und einem Morphismus $f : A \to B$ in $\mathcal{C}$ die Abbildung $\mathcal{C}(X, f) : \mathcal{C}(X, A) \to \mathcal{C}(X, B)$, $g \mapsto f \circ g$ zu.

(d) Für $R \in \mathbf{Ri}$ und $X \in {}_R\mathbf{Mod}$ hat man analog einen Funktor $\mathrm{Hom}_R(X, ?) : {}_R\mathbf{Mod} \to {}_\mathbb{Z}\mathbf{Mod}$; dieser ordnet jedem R-Modul M den $\mathbb{Z}$-Modul $\mathrm{Hom}_R(X, M)$und jedem R-Homomorphismus $f : M \to N$ den $\mathbb{Z}$-Homomorphismus

$$\mathrm{Hom}_R(X, f) : \mathrm{Hom}_R(X, M) \to \mathrm{Hom}_R(X, N)\ , \qquad g \mapsto f \circ g\ ,$$

zu. Für $S \in Ri$ und $X \in {}_R\mathbf{Mod}_S$ kann man analog einen Funktor $\mathrm{Hom}_R(X, ?) : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ definieren.

(e) Für $R, S \in \mathbf{Ri}$ und $X \in {}_R\mathbf{Mod}_S$ hat man einen Funktor $X \otimes_S ? : {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$; dieser ordnet einem S-Modul M den R-Modul $X \otimes_S M$ und einem S-Homomorphismus $f : M \to N$ den R-Homomorphismus $\mathrm{id}_X \otimes f : X \otimes_S M \to X \otimes_S N$ zu.

Bemerkungen. Für Kategorien $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ und Funktoren $\Phi : \mathcal{C} \to \mathcal{D}$, $\Psi : \mathcal{D} \to \mathcal{E}$, definiert man in offensichtlicher Weise einen Funktor $\Psi \circ \Phi : \mathcal{C} \to \mathcal{E}$. Für die so definierte **Komposition** von Funktoren gilt:

(i) $(\Omega \circ \Psi) \circ \Phi = \Omega \circ (\Psi \circ \Phi)$ für Kategorien $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$ und Funktoren $\Phi : \mathcal{C} \to \mathcal{D}$, $\Psi : \mathcal{D} \to \mathcal{E}$, $\Omega : \mathcal{E} \to \mathcal{F}$.

(ii) $\Phi \circ \mathrm{Id}_\mathcal{C} = \Phi$ und $\mathrm{Id}_\mathcal{C} \circ \Psi = \Psi$ für Kategorien $\mathcal{C}$, $\mathcal{D}$ und Funktoren $\Phi : \mathcal{C} \to \mathcal{D}$, $\Psi : \mathcal{D} \to \mathcal{C}$.

13.3. Definition. Ein Morphismus $f : A \to B$ in einer Kategorie $\mathcal{C}$ heißt **Isomorphismus**, wenn ein Morphismus $g : B \to A$ in $\mathcal{C}$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$ existiert.

Bemerkung. Man zeigt leicht, daß g durch f eindeutig bestimmt ist. Man nennt g das **Inverse** von f in $\mathcal{C}$ und schreibt dafür $g = f^{-1}$. Offenbar ist f^{-1} ebenfalls ein Isomorphismus in $\mathcal{C}$ und $(f^{-1})^{-1} = f$.

Beispiele.

(i) Stets ist id_A ein Isomorphismus in $\mathcal{C}$ und $\mathrm{id}_A^{-1} = \mathrm{id}_A$.

(ii) Sind $f : A \to B$ und $g : B \to C$ Isomorphismen in $\mathcal{C}$, so ist auch $g \circ f : A \to C$ ein Isomorphismus in $\mathcal{C}$, und $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(iii) Die Isomorphismen in **Ri** sind genau die Ringisomorphismen, und die Isomorphismen in ${}_R\mathbf{Mod}$ sind genau die R-Homomorphismen.

Satz. *Gegeben seien Kategorien $\mathcal{C}$, $\mathcal{D}$, ein Funktor $\Phi : \mathcal{C} \to \mathcal{D}$ und ein Isomorphismus $f : A \to B$ in $\mathcal{C}$. Dann ist $\Phi(f)$ ein Isomorphismus in $\mathcal{D}$ und $\Phi(f)^{-1} = \Phi(f^{-1})$.*

Beweis.

$$\Phi(f^{-1}) \circ \Phi(f) = \Phi(f^{-1} \circ f) = \Phi(\mathrm{id}_A) = \mathrm{id}_{\Phi(A)} \ ,$$
$$\Phi(f) \circ \Phi(f^{-1}) = \Phi(f \circ f^{-1}) = \Phi(\mathrm{id}_B) = \mathrm{id}_{\Phi(B)} \ .$$

13.4. Definition. Man nennt Objekte A, B in einer Kategorie $\mathcal{C}$ **isomorph** und schreibt $A \cong B$ oder $A \cong_{\mathcal{C}} B$, falls ein Isomorphismus $f \in \mathcal{C}(A, B)$ existiert.

Bemerkungen.

(i) Man zeigt leicht, daß $\cong_{\mathcal{C}}$ eine Äquivalenzrelation ist.

(ii) Aus Satz 13.3 folgt, daß für Kategorien $\mathcal{C}$, $\mathcal{D}$, Funktoren $\Phi : \mathcal{C} \to \mathcal{D}$ und Objekte $A, B \in \mathcal{C}$ gilt: $A \cong_{\mathcal{C}} B \Longrightarrow \Phi(A) \cong_{\mathcal{D}} \Phi(B)$.

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

(i) **mono**, falls für alle $C \in \mathcal{C}$ und alle $g, h \in \mathcal{C}(C, A)$ mit $f \circ g = f \circ h$ stets $g = h$ folgt.

(ii) **epi**, falls für alle $C \in \mathcal{C}$ und alle $g, h \in \mathcal{C}(B, C)$ mit $g \circ f = h \circ f$ stets $g = h$ folgt.

Satz. *Für $R \in$ **Ri**, $M, N \in {}_R\mathbf{Mod}$ und $f \in \mathrm{Hom}_R(M, N)$ gilt: f mono (epi) in ${}_R\mathbf{Mod} \Longleftrightarrow$ f injektiv (surjektiv).*

Beweis.

„$\Longrightarrow$“: Sei f mono und $i : \mathrm{Ker}(f) \to M$ die Inklusionsabbildung. Dann ist $f \circ i = 0 = f \circ 0$, also $i = 0$. Folglich ist $\mathrm{Ker}(f) = 0$, d.h. f ist injektiv.

„$\Longleftarrow$“: Seien f injektiv, $L \in {}_R\mathbf{Mod}$ und $g, h \in \mathrm{Hom}_R(L, M)$ mit $f \circ g = f \circ h$. Für $x \in L$ ist dann $f\big(g(x)\big) = f\big(h(x)\big)$, d.h. $g(x) = h(x)$. Folglich ist $g = h$.

Die andere Aussage beweist man analog.

Bemerkung. In **Ri** ist die Inklusionsabbildung $i : \mathbb{Z} \to \mathbb{Q}$ nicht surjektiv, aber epi!

13.6. Definition. Seien $R, S \in$ **Ri**. Ein Funktor $\Phi : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ heißt **additiv**, falls $\Phi(f + g) = \Phi(f) + \Phi(g)$ für alle $M, N \in {}_R\mathbf{Mod}$, $f, g \in \mathrm{Hom}_R(M, N)$ gilt.

Bemerkung. Daraus folgt, daß $\Phi(0_{M,N}) = 0_{\Phi(M),\Phi(N)}$ für die Nullabbildung $0_{M,N} : M \to N$ gilt.

Satz. *Seien $R, S \in$ **Ri** und $\Phi : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ ein additiver Funktor. Für den Nullmodul 0 in ${}_R\mathbf{Mod}$ ist dann $\Phi(0)$ „der“ Nullmodul in ${}_S\mathbf{Mod}$.*

Beweis. Für die Nullabbildung $0_{0,0} \in \mathrm{Hom}_R(0,0)$ gilt offenbar $0_{0,0} = \mathrm{id}_0$. Nach der obigen Bemerkung ist $0_{\Phi(0),\Phi(0)} = \Phi(0_{0,0}) = \Phi(\mathrm{id}_0) = \mathrm{id}_{\Phi(0)}$. Daraus folgt: $\Phi(0) = 0$.

Beispiele.

(i) Für $R, S \in \mathbf{Ri}$ und $X \in {}_R\mathbf{Mod}_S$ sind $\mathrm{Hom}_R(X, ?) : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ und $X \otimes_R ? : {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$ additive Funktoren.

(ii) Für Ringe R, S, T und additive Funktoren $\Phi : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$, $\Psi : {}_S\mathbf{Mod} \to {}_T\mathbf{Mod}$ ist auch $\Psi \circ \Phi : {}_R\mathbf{Mod} \to {}_T\mathbf{Mod}$ additiv.

14 Natürliche Transformationen und Äquivalenzen

14.1. Definition. Gegeben seien Kategorien $\mathcal{C}$, $\mathcal{D}$ und Funktoren $\Phi, \Psi : \mathcal{C} \to \mathcal{D}$. Eine **natürliche Transformation** von Φ nach Ψ ist eine Familie $\varphi = (\varphi_A)_{A \in \mathcal{C}}$ von Morphismen $\varphi_A \in \mathcal{D}\big(\Phi(A), \Psi(A)\big)$ mit $\Psi(f) \circ \varphi_A = \varphi_B \circ \Phi(f)$ für $A, B \in \mathcal{C}$, $f \in \mathcal{C}(A, B)$:

$$\begin{tikzcd} \Phi(A) \arrow[r, "\Phi(f)"] \arrow[d, "\varphi_A"] & \Phi(B) \arrow[d, "\varphi_B"] \\ \Psi(A) \arrow[r, "\Psi(f)"] & \Psi(B) \end{tikzcd}$$

Gegebenenfalls schreibt man: $\varphi : \Phi \Rightarrow \Psi$.

Beispiel. Sei $R \in \mathbf{Ri}$ und $\Phi : {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$, $M \mapsto M^{**}$, der Funktor, der jedem R-Modul M seinen **Bidual** $M^{**} = \mathrm{Hom}_R(\mathrm{Hom}_R(M, R), R)$ zuordnet (vergleiche Aufgabe 46). Mit $\varepsilon_M : M \to M^{**}$ bezeichnen wir die kanonische Abbildung; für $m \in M$ ist also $\varepsilon_M(m) : \mathrm{Hom}_R(M, R) \to R$, $\mu \mapsto \mu(m)$. Dann ist $\varepsilon := (\varepsilon_M)_{M \in {}_R\mathbf{Mod}} : \mathrm{Id}_{{}_R\mathbf{Mod}} \Rightarrow \Phi$ eine natürliche Transformation; denn man rechnet schnell nach, daß für $M, N \in {}_R\mathbf{Mod}$ und $f \in \mathrm{Hom}_R(M, N)$ gilt: $\varepsilon_N \circ f = f^{**} \circ \varepsilon_M$.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\varepsilon_M"] & N \arrow[d, "\varepsilon_N"] \\ M^{**} \arrow[r, "f^{**}"] & N^{**} \end{tikzcd}$$

Bemerkungen.

(i) Gegeben seien Kategorien $\mathcal{C}$, $\mathcal{D}$, Funktoren $\Phi, \Psi, \Omega : \mathcal{C} \to \mathcal{D}$ und natürliche Transformationen $\varphi : \Phi \Rightarrow \Psi$, $\psi : \Psi \Rightarrow \Omega$. Dann ist auch $\psi \circ \varphi := (\psi_A \circ \varphi_A)_{A \in \mathcal{C}} : \Phi \Rightarrow \Omega$ eine natürliche Transformation.

$$\begin{tikzcd} \Phi(A) \arrow[r, "\Phi(f)"] \arrow[d, "\varphi_A"] & \Phi(B) \arrow[d, "\varphi_B"] \\ \Psi(A) \arrow[r, "\Psi(f)"] \arrow[d, "\psi_A"] & \Psi(B) \arrow[d, "\psi_B"] \\ \Omega(A) \arrow[r, "\Omega(f)"] & \Omega(B) \end{tikzcd} \qquad \begin{tikzcd} \mathcal{C} \arrow[r, bend left=60, "\Phi"] \arrow[r, "\Psi"] \arrow[r, bend right=60, "\Omega"'] \arrow[r, phantom, shift left=3ex, "\Downarrow\varphi"] \arrow[r, phantom, shift right=3ex, "\Downarrow\psi"] & \mathcal{D} \end{tikzcd}$$

Man nennt $\psi \circ \varphi$ die **Komposition** von ψ und φ. Offenbar ist die Komposition von natürlichen Transformationen assoziativ.

(ii) Gegeben seien Kategorien $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, Funktoren $\Gamma : \mathcal{B} \to \mathcal{C}$, $\Phi, \Psi : \mathcal{C} \to \mathcal{D}$ und $\Delta : \mathcal{D} \to \mathcal{E}$ und eine natürliche Transformation $\varphi : \Phi \Rightarrow \Psi$:

$$
\begin{tikzcd}
\mathcal{B} \arrow[r, "\Gamma"] & \mathcal{C} \arrow[r, bend left, "\Phi"] \arrow[r, bend right, "\Psi"'] \arrow[r, phantom, "\Downarrow\varphi"] & \mathcal{D} \arrow[r, "\Delta"] & \mathcal{E}
\end{tikzcd}
$$

Dann sind auch

$$
\begin{aligned}
&\varphi \circ \Gamma = (\varphi_{\Gamma(B)})_{B\in\mathcal{B}} : \Phi\circ\Gamma \Rightarrow \Psi\circ\Gamma \quad \text{und}\\
&\Delta\circ\varphi = \big(\Delta(\varphi_C)\big)_{C\in\mathcal{C}} : \Delta\circ\Phi \Rightarrow \Delta\circ\Psi
\end{aligned}
$$

natürliche Transformationen:

$$
\begin{tikzcd}
\Phi\big(\Gamma(A)\big) \arrow[r, "\Phi\left(\Gamma(f)\right)"] \arrow[d, "\varphi_{\Gamma(A)}"] & \Phi\big(\Gamma(B)\big) \arrow[d, "\varphi_{\Gamma(B)}"] \\
\Psi\big(\Gamma(A)\big) \arrow[r, "\Psi\left(\Gamma(f)\right)"] & \Psi\big(\Gamma(B)\big)
\end{tikzcd}
\qquad
\begin{tikzcd}
\Delta\big(\Phi(C)\big) \arrow[r, "\Delta\left(\Phi(f)\right)"] \arrow[d, "\Delta(\varphi_C)"] & \Delta\big(\Phi(D)\big) \arrow[d, "\Delta(\varphi_D)"] \\
\Delta\big(\Psi(C)\big) \arrow[r, "\Delta\left(\Psi(f)\right)"] & \Delta\big(\Psi(D)\big)
\end{tikzcd}
$$

14.2. Definition. Gegeben seien Kategorien $\mathcal{C}$, $\mathcal{D}$ und Funktoren $\Phi, \Psi : \mathcal{C} \to \mathcal{D}$. Eine natürliche Transformation $\varphi : \Phi \Rightarrow \Psi$ nennt man eine **natürliche Äquivalenz**, falls φ_A für $A \in \mathcal{C}$ ein Isomorphismus in $\mathcal{D}$ ist.

Bemerkung. Gegebenenfalls ist $\varphi^{-1} := (\varphi_A^{-1})_{A\in\mathcal{C}} : \Psi \Rightarrow \Phi$ auch eine natürliche Äquivalenz, und es ist $(\varphi^{-1})^{-1} = \varphi$. Ist $\Omega : \mathcal{C} \to \mathcal{D}$ ein weiterer Funktor und $\psi = (\psi_A)_{A\in\mathcal{C}} : \Psi \Rightarrow \Omega$ eine weitere natürliche Äquivalenz, so ist auch $\psi\circ\varphi : \Phi \Rightarrow \Omega$ eine natürliche Äquivalenz, und es ist $(\psi\circ\varphi)^{-1} = \varphi^{-1}\circ\psi^{-1}$.

Beispiele.

(i) Stets ist $\mathrm{id}_\Phi := (\mathrm{id}_{\Phi(A)}) : \Phi \Rightarrow \Phi$ eine natürliche Äquivalenz.

(ii) Für $R \in \mathbf{Ri}$ und $M \in {}_R\mathbf{Mod}$ sei $\mu_M : R\otimes_R M \to M$, $r\otimes m \mapsto rm$, der kanonische Isomorphismus aus Bemerkung 11.7. Dann ist $\mu = (\mu_M)_{M\in {}_R\mathbf{Mod}}$ eine natürliche Äquivalenz:

$$
\begin{tikzcd}
{}_R\mathbf{Mod} \arrow[r, bend left, "R\otimes_R ?"] \arrow[r, bend right, "\mathrm{Id}_{{}_R\mathbf{Mod}}"'] \arrow[r, phantom, "\Downarrow\mu_M"] & {}_R\mathbf{Mod}
\end{tikzcd}
$$

Dies rechnet man leicht nach.

14.3. Definition. Gegeben seien Kategorien $\mathcal{C}$, $\mathcal{D}$. Wir nennen Funktoren $\Phi, \Phi' : \mathcal{C} \to \mathcal{D}$ **natürlich äquivalent** und schreiben $\Phi \sim \Phi'$, falls eine natürliche Äquivalenz $\varphi : \Phi \Rightarrow \Phi'$ existiert.

Bemerkung. Man zeigt leicht, daß $\sim$ eine Äquivalenzrelation ist.

Satz. *Gegeben seien Kategorien* $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ *und Funktoren* $\Phi, \Phi' : \mathcal{C} \to \mathcal{D}$ *und* $\Psi, \Psi' : \mathcal{D} \to \mathcal{E}$ *mit* $\Phi \sim \Phi'$ *und* $\Psi \sim \Psi'$. *Dann ist* $\Psi \circ \Phi \sim \Psi' \circ \Phi'$.

Beweis. Sei $\varphi : \Phi \Rightarrow \Phi'$ eine natürliche Äquivalenz. Dann ist auch

$$\Psi \circ \varphi = \big(\Psi(\varphi_A)\big)_{A \in \mathcal{C}} : \Psi \circ \Phi \Rightarrow \Psi \circ \Phi'$$

eine natürliche Äquivalenz. Daher gilt $\Psi \circ \Phi \sim \Psi \circ \Phi'$. Analog zeigt man: $\Psi \circ \Phi' \sim \Psi' \circ \Phi'$. Daraus folgt die Behauptung.

14.4. Satz. *Gegeben seien Kategorien* $\mathcal{C}$, $\mathcal{D}$ *und Funktoren* $\mathcal{C} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathcal{D}$ *mit* $\Psi \circ \Phi \sim \mathrm{Id}_{\mathcal{C}}$ *und* $\Phi \circ \Psi \sim \mathrm{Id}_{\mathcal{D}}$. *Für* $A, B \in \mathcal{C}$ *ist dann die Abbildung* $\Phi_{A,B} : \mathcal{C}(A,B) \to \mathcal{D}\big(\Phi(A), \Phi(B)\big)$, $f \mapsto \Phi(f)$, *bijektiv. Für* $f \in \mathcal{C}(A,B)$ *gilt dabei:* f *mono (epi)* $\Longleftrightarrow$ $\Phi(f)$ *mono (epi).*

Beweis. Seien $f, g \in \mathcal{C}(A,B)$ mit $\Phi(f) = \Phi(g)$. Dann ist $\Psi\big(\Phi(f)\big) = \Psi\big(\Phi(g)\big)$. Wir wählen eine natürliche Äquivalenz $\varphi : \Psi \circ \Phi \Rightarrow \mathrm{Id}_{\mathcal{C}}$:

$$\begin{tikzcd}
\Psi\big(\Phi(A)\big) \arrow[r, "\Psi(\Phi(f))", "\Psi(\Phi(g))"'] \arrow[d, "\varphi_A"] & \Psi\big(\Phi(B)\big) \arrow[d, "\varphi_B"] \\
A \arrow[r, "f", "g"'] & B
\end{tikzcd}$$

Dann ist $f = \varphi_B \circ \Psi\big(\Phi(f)\big) \circ \varphi_A^{-1} = \varphi_B \circ \Psi\big(\Phi(g)\big) \circ \varphi_A^{-1} = g$. Dies zeigt, daß $\Phi_{A,B}$ injektiv ist. Analog ist $\Psi_{C,D}$ für alle $C, D \in \mathcal{D}$ injektiv.
Zum Beweis der Surjektivität von $\Phi_{A,B}$ sei $h \in \mathcal{D}\big(\Phi(A), \Phi(B)\big)$. Wir setzen $f := \varphi_B \circ \Psi(h) \circ \varphi_A^{-1} \in \mathcal{C}(A,B)$ und vergleichen die folgenden Diagramme:

$$\begin{tikzcd}
\Psi\big(\Phi(A)\big) \arrow[r, "\Psi(h)"] \arrow[d, "\varphi_A"] & \Psi\big(\Phi(B)\big) \arrow[d, "\varphi_B"] \\
A \arrow[r, "f"] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
\Psi\big(\Phi(A)\big) \arrow[r, "\Psi(\Phi(f))"] \arrow[d, "\varphi_A"] & \Psi\big(\Phi(B)\big) \arrow[d, "\varphi_B"] \\
A \arrow[r, "f"] & B
\end{tikzcd}$$

Wir erhalten: $\Psi(h) = \varphi_B^{-1} \circ f \circ \varphi_A = \Psi\big(\Phi(f)\big)$. Da $\Psi_{\Phi(A),\Phi(B)}$ injektiv ist, folgt $h = \Phi(f)$.
Seien jetzt $f \in \mathcal{C}(A,B)$ mono, $D \in \mathcal{D}$ und $g, h \in \mathcal{D}\big(D, \Phi(A)\big)$ mit $\Phi(f) \circ g = \Phi(f) \circ h$. Anwendung von Ψ ergibt:

$$\underbrace{\Psi\big(\Phi(f)\big)}_{\varphi_B^{-1} \circ f \circ \varphi_A} \circ \Psi(g) = \underbrace{\Psi\big(\Phi(f)\big)}_{\varphi_B^{-1} \circ f \circ \varphi_A} \circ \Psi(h)\ .$$

Daraus folgt $f \circ \varphi_A \circ \Psi(g) = f \circ \varphi_A \circ \Psi(h)$, also $\varphi_A \circ \Psi(g) = \varphi_A \circ \Psi(h)$ (da f mono) und $\Psi(g) = \Psi(h)$. Da $\Psi_{D,\Phi(A)}$ injektiv ist, folgt $g = h$.
Sei jetzt umgekehrt $\Phi(f)$ mono. Dann ist analog $\Psi\big(\Phi(f)\big)$ mono. Daraus folgt leicht, daß auch $f = \varphi_B \circ \Psi\big(\Phi(f)\big) \circ \varphi_A^{-1}$ mono ist. Der Rest des Beweises geht analog.

14.5. Definition. Man nennt Ringe R, S **Morita-äquivalent** und schreibt $R \approx S$, falls additive Funktoren ${}_R\mathbf{Mod} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} {}_S\mathbf{Mod}$ mit $\Psi \circ \Phi \sim \mathrm{Id}_{{}_R\mathbf{Mod}}$ und $\Phi \circ \Psi \sim \mathrm{Id}_{{}_S\mathbf{Mod}}$ existieren.

Satz. $\approx$ *ist eine Äquivalenzrelation.*

Beweis.

- *Reflexivität:* Setze $\Phi := \Psi := \mathrm{Id}_{{}_R\mathbf{Mod}}$.
- *Symmetrie:* Vertausche Φ und Ψ.
- *Transitivität:* Seien R, S, T Ringe mit $R \approx S \approx T$. Dann existieren additive Funktoren ${}_R\mathbf{Mod} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} {}_S\mathbf{Mod}$, ${}_S\mathbf{Mod} \underset{\Delta}{\overset{\Gamma}{\rightleftarrows}} {}_T\mathbf{Mod}$ mit $\Psi \circ \Phi \sim \mathrm{Id}_{{}_R\mathbf{Mod}}$, $\Phi \circ \Psi \sim \mathrm{Id}_{{}_S\mathbf{Mod}}$, $\Gamma \circ \Delta \sim \mathrm{Id}_{{}_T\mathbf{Mod}}$, $\Delta \circ \Gamma \sim \mathrm{Id}_{{}_S\mathbf{Mod}}$. Folglich sind ${}_R\mathbf{Mod} \underset{\Psi\circ\Delta}{\overset{\Gamma\circ\Phi}{\rightleftarrows}} {}_T\mathbf{Mod}$ additive Funktoren mit

$$(\Psi \circ \Delta) \circ (\Gamma \circ \Phi) \sim \Psi \circ \mathrm{Id}_{{}_S\mathbf{Mod}} \circ \Phi = \Psi \circ \Phi \sim \mathrm{Id}_{{}_R\mathbf{Mod}} \text{ und}$$
$$(\Gamma \circ \Phi) \circ (\Psi \circ \Delta) \sim \Gamma \circ \mathrm{Id}_{{}_S\mathbf{Mod}} \circ \Delta = \Gamma \circ \Delta \sim \mathrm{Id}_{{}_T\mathbf{Mod}} \ .$$

Beispiel. Isomorphe Ringe sind Morita-äquivalent (Übungsaufgabe).

Bemerkung. Wir werden später sehen, daß gilt: $R \approx S \Longrightarrow R^\circ \approx S^\circ$.

15 Morita-Theorie

15.1. Satz. *Sei $R \approx S$ vermöge additiver Funktoren ${}_R\mathbf{Mod} \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} {}_S\mathbf{Mod}$. Für jede Familie $(M_i)_{i\in I}$ von R-Moduln M_i ist dann $\Phi\big(\prod_{i\in I} M_i\big) \cong \prod_{i\in I} \Phi(M_i)$ und $\Phi\big(\coprod_{i\in I} M_i\big) \cong \coprod_{i\in I} \Phi(M_i)$.*

Beweis. Wir setzen $M := \prod_{i\in I} M_i$. Für $j \in I$ sei $f_j \in \mathrm{Hom}_R(M, M_j)$ der entsprechende Projektor. Dann ist $\Phi(f_j) \in \mathrm{Hom}_S\big(\Phi(M), \Phi(M_j)\big)$. Folglich ist die Abbildung

$$f : \Phi(M) \to \prod_{j\in I} \Phi(M_j) =: N\,, \qquad x \mapsto \Big(\big[\Phi(f_j)\big](x)\Big)_{j\in I}$$

S-linear. Für $i \in I$ sei $g_i \in \mathrm{Hom}_S\big(N, \Phi(M_i)\big)$ der i-te Projektor. Wir wählen eine natürliche Äquivalenz $\varphi : \Psi \circ \Phi \Rightarrow \mathrm{Id}_{{}_R\mathbf{Mod}}$. Dann ist $\Psi(N) \xrightarrow{\Psi(g_i)} \Psi\big(\Phi(M_i)\big) \xrightarrow{\varphi_{M_i}} M_i$ R-linear. Folglich ist die Abbildung $g : \Psi(N) \to M$, $y \mapsto \Big(\big[\varphi_{M_i} \circ \Psi(g_i)\big](y)\Big)_{i\in I}$ R-linear. Daher ist $\Psi(N) \xrightarrow{g} M \xrightarrow{\varphi_M^{-1}} \Psi\big(\Phi(M)\big)$ R-linear. Wir setzen $h := \Psi^{-1}_{N,\Phi(M)}(\varphi_M^{-1} \circ g) \in \mathrm{Hom}_S\big(N, \Phi(M)\big)$. Für $j \in I$ ist dann

$$\begin{aligned}\Psi(\underbrace{g_j \circ f}_{\Phi(f_j)} \circ h) &= \Psi\big(\Phi(f_j)\big) \circ \Psi(h) = \Psi\big(\Phi(f_j)\big) \circ \varphi_M^{-1} \circ g \\ &= \varphi_{M_j}^{-1} \circ f_j \circ g = \varphi_{M_j}^{-1} \circ \varphi_{M_j} \circ \Psi(g_j) = \Psi(g_j)\,,\end{aligned}$$

also $g_j \circ f \circ h = g_j$. Folglich ist $f \circ h = \mathrm{id}_N$. Analog gilt für $i \in I$:

$$\underbrace{f_i \circ g}_{\varphi_{M_i}\circ\Psi(g_i)} \circ \Psi(f) = \varphi_{M_i} \circ \Psi(\underbrace{g_i \circ f}_{\Phi(f_i)}) = \varphi_{M_i} \circ \Psi\big(\Phi(f_i)\big) = f_i \circ \varphi_M\,.$$

Folglich ist $g \circ \Psi(f) = \varphi_M$ und daher

$$\Psi(h \circ f) = \Psi(h) \circ \Psi(f) = \varphi_M^{-1} \circ \underbrace{g \circ \Psi(f)}_{\varphi_M} = \mathrm{id}_{\Psi(\Phi(M))} = \Psi(\mathrm{id}_{\Phi(M)})\,,$$

also ist $h \circ f = \mathrm{id}_{\Phi(M)}$. Analog für das Koprodukt.

Bemerkung. Ein R-Modul M ist genau dann endlich erzeugt, wenn zu jeder Familie $(M_i)_{i\in I}$ von R-Moduln M_i und jedem R-Epimorphismus $f : \coprod_{i\in I} M_i \to M$ eine endliche Teilmenge J von I und ein R-Epimorphismus $g : \coprod_{j\in J} M_j \to M$ existieren (Übungsaufgabe).

15.2. Definition. Einen R-Modul M nennt man (R-)**Generator**, falls zu jedem R-Modul N eine Menge I existiert, so daß N zu einem Faktormodul von $\coprod_{i\in I} M$ isomorph ist. Einen R-Modul, der endlich erzeugt, projektiv und ein Generator ist, nennt man R-**Progenerator**.

Beispiele.

(i) Stets ist der reguläre R-Linksmodul ein R-Progenerator.

(ii) Ist R semiperfekt und sind $P_1, \ldots, P_n$ Repräsentanten für die Isomorphieklassen unzerlegbarer projektiver R-Moduln, so ist $P_1^{a_1} \times \cdots \times P_n^{a_n}$ für $a_1, \ldots, a_n \in \mathbb{N}$ ($a_i \neq 0$ für alle i!) ein R-Progenerator.

Satz. *Sei $R \approx S$ vermöge additiver Funktoren ${}_R\mathbf{Mod} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} {}_S\mathbf{Mod}$. Für $M \in {}_R\mathbf{Mod}$ gilt dann:*

(i) M endlich erzeugt $\iff \Phi(M)$ endlich erzeugt.

(ii) M projektiv (injektiv) $\iff \Phi(M)$ projektiv (injektiv).

(iii) M R-Generator $\iff \Phi(M)$ S-Generator.

(iv) M R-Progenerator $\iff \Phi(M)$ S-Progenerator.

Beweis.

„$\Longrightarrow$“:

(i) Sei M endlich erzeugt, $(N_i)_{i\in I}$ eine Familie von S-Moduln und $f : \coprod_{i\in I} N_i \to \Phi(M)$ ein S-Epimorphismus. Dann ist

$$\Psi(f) : \underbrace{\Psi\Big(\coprod_{i\in I} N_i\Big)}_{\cong \coprod_{i\in I} \Psi(N_i)} \to \underbrace{\Psi\big(\Phi(M)\big)}_{\cong M}$$

ein R-Epimorphismus. Nach Bemerkung 15.1 existiert eine endliche Teilmenge J von I und ein R-Epimorphismus $g : \coprod_{j\in J} \Psi(N_j) \to M$. Dann ist

$$\Phi(g) : \underbrace{\Phi\Big(\coprod_{j\in J} \Psi(N_j)\Big)}_{\cong \coprod_{j\in J} \Phi\big(\Psi(N_j)\big) \cong \coprod_{j\in J} N_j} \to \Phi(M)$$

ein S-Epimorphismus. Aus Bemerkung 15.1 folgt also, daß $\Phi(M)$ auch endlich erzeugt ist.

(ii) Sei M projektiv, $L, N \in {}_S\mathbf{Mod}$, $f \in \mathrm{Hom}_S(\Phi(M), N)$ und $g \in \mathrm{Hom}_S(L, N)$ surjektiv.

$$\begin{tikzcd}
 & \Phi(M) \arrow[dl, dashed, "k"'] \arrow[d, "f"] & \\
L \arrow[r, "g"] & N \arrow[r] & 0
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \Psi\big(\Phi(M)\big) \cong M \arrow[dl, dashed, "h"'] \arrow[d, "\Psi(f)"] & \\
\Psi(L) \arrow[r, "\Psi(g)"] & \Psi(N) \arrow[r] & 0
\end{tikzcd}$$

Dann ist $\Psi(g) \in \mathrm{Hom}_R\big(\Psi(L), \Psi(N)\big)$ surjektiv und

$$\Psi(f) \in \mathrm{Hom}_R\Big(\Psi\big(\Phi(M)\big), \Psi(N)\Big) .$$

Da $\Psi\big(\Phi(M)\big) \cong M$ projektiv ist, existiert ein R-Homomorphismus

$$h : \Psi\big(\Phi(M)\big) \to \Psi(L)$$

mit $\Psi(g) \circ h = \Psi(f)$. Dann ist $k := \Psi^{-1}_{\Phi(M),L}(h) \in \mathrm{Hom}_S\big(\Phi(M), L\big)$ mit $\Psi(f) = \Psi(g) \circ \Psi(k) = \Psi(g \circ k)$, d.h. $f = g \circ k$.
Die Aussage über die Injektivität gilt analog.

(iii) Sei M ein R-Generator und $N \in {}_S\mathbf{Mod}$. Dann ist $\Psi(N) \in {}_R\mathbf{Mod}$. Daher existieren eine Menge I und ein R-Epimorphismus $f : \coprod_{i\in I} M \to \Psi(N)$. Dann ist

$$\Phi(f) : \underbrace{\Phi\Big(\coprod_{i\in I} M\Big)}_{\cong \coprod_{i\in I} \Phi(M)} \to \underbrace{\Phi\big(\Psi(N)\big)}_{\cong N}$$

ein S-Epimorphismus.

(iv) Folgt aus (i) – (iii).

„$\Longleftarrow$“:

(i) Sei $\Phi(M)$ endlich erzeugt. Nach dem ersten Teil des Beweises ist dann $\Psi\big(\Phi(M)\big)$ endlich erzeugt, also auch M.

(ii) – (iv) Analog.

15.3. Satz. *Sei $R \approx S$ vermöge additiver Funktoren ${}_R\mathbf{Mod} \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} {}_S\mathbf{Mod}$. Dann ist $P := \Phi(R)$ ein S-Progenerator mit $\operatorname{End}_S(P) \cong R^\circ$.*

Beweis. Da der reguläre R-Linksmodul ein R-Progenerator ist, ist $P = \Phi(R)$ ein S-Progenerator. Nach Satz 14.4 ist die Abbildung

$$\operatorname{End}_R(R) \to \operatorname{End}_S\big(\Phi(R)\big)\ , \qquad f \mapsto \Phi(f)$$

ein Ringisomorphismus. Bekanntlich ist außerdem die Abbildung $\operatorname{End}_R(R) \to R^\circ$, $f \mapsto f(1)$ ein Ringisomorphismus.

Bemerkung. Wir werden zeigen, daß umgekehrt $R \approx S$ gilt, falls ein S-Progenerator P mit $R^\circ \cong \operatorname{End}_S(P)$ existiert.

15.4. Definition. Ein **Morita-Kontext** ist ein Sextupel, das aus Ringen R ,S, einem S-R-Bimodul P, einem R-S-Bimodul Q, einem S-S-Homomorphismus $\sigma : P \otimes_R Q \to S$ und einem R-R-Homomorphismus $\tau : Q \otimes_S P \to R$ mit $\sigma(x \otimes y)x' = x\tau(y \otimes x')$ und $y\sigma(x \otimes y') = \tau(y \otimes x)y'$ für alle $x, x' \in P$, $y, y' \in Q$.

Beispiel. Gegeben sei ein Ring S und ein S-Linksmodul P. Wir setzen $R := \operatorname{End}_S(P)^\circ$ und $Q := \operatorname{Hom}_S(P, S)$. Dann ist P ein S-R-Bimodul und Q ein R-S-Bimodul. Offenbar ist die Abbildung $P \times Q \to S$, $(x, y) \mapsto y(x)$, R-ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\sigma : P \otimes_R Q \to S$ mit $\sigma(x \otimes y) = y(x)$ für $x \in P$, $y \in Q$. Man rechnet leicht nach, daß σ ein S-S-Homomorphismus ist. Andererseits ist für $y \in Q$, $x \in P$ die Abbildung $\tau_{y,x} : P \to P$, $p \mapsto y(p)x$, S-linear. Wir erhalten also eine Abbildung $Q \times P \to R$, $(y, x) \mapsto \tau_{y,x}$, die, wie man leicht nachrechnet, S-ausgeglichen ist. Daher existiert ein $\mathbb{Z}$-Homomorphismus $\tau : Q \otimes_S P \to R$ mit $\tau(y \otimes x) = \tau_{y,x}$ für $y \in Q$, $x \in P$. Man rechnet leicht nach, daß dieser R-R-linear ist und daß so ein Morita-Kontext entsteht.

Bemerkung. Wir sind hauptsächlich an der Situation aus dem Beispiel interessiert, aber die Einführung eines Morita-Kontexts macht die Sache symmetrisch in R und S, P und Q.

Satz. *Im obigen Beispiel gilt:*

(i) Ist P endlich erzeugt und projektiv, so ist τ surjektiv.

(ii) Ist P ein S-Generator, so ist σ surjektiv.

Beweis.

(i) Sei $P = Sp_1 + \cdots + Sp_n$ projektiv. Nach 7.8 existiert dann $f_1, \ldots, f_n \in \mathrm{Hom}_S(P, S) = Q$ mit $p = \sum_{i=1}^n f_i(p)p_i = \sum_{i=1}^n \tau_{f_i,p_i}(p)$ für $p \in P$. Folglich ist $1_R = \mathrm{id}_P = \sum_{i=1}^n \tau_{f_i,p_i} = \sum_{i=1}^n \tau(f_i \otimes p_i) \in \mathrm{Bld}(\tau)$. Daher ist τ surjektiv.

(ii) Sei P ein S-Generator. Dann existieren eine Menge I und ein S-Epimorphismus $f : \coprod_{i \in I} P \to S$. Wir wählen ein Element $p = (p_i)_{i \in I} \in \coprod_{i \in I} P$ mit $f(p) = 1$. Wir setzen $j := \{i \in I : p_i \neq 0\}$ und bezeichnen mit g_i die entsprechenden Injektoren. Dann ist $p = \sum_{i \in J} g_i(p_i)$ und $1_S = f(p) = \sum_{i \in J} f\big(g_i(p_i)\big) = \sigma\big(\sum_{i \in J} p_i \otimes (f \circ g_i)\big) \in \mathrm{Bld}(\sigma)$. Folglich ist σ surjektiv.

15.5. Satz. *Sei $(R, S, P, Q, \sigma, \tau)$ ein Morita-Kontext. Ist σ surjektiv, so gilt:*

(i) σ ist bijektiv.

(ii) P und Q sind endlich erzeugt und projektiv als R-Moduln.

(iii) P und Q sind S-Generatoren.

(iv) Die Abbildung $Q \to \mathrm{Hom}_R(P, R)$, die jedem $q \in Q$ die Abbildung $P \to R$, $p \mapsto \tau(q \otimes p)$, zuordnet, ist ein R-S-Isomorphismus. Die Abbildung $P \to \mathrm{Hom}_R(Q, R)$, die jedem $p \in P$ die Abbildung $Q \to R$, $q \mapsto \tau(q \otimes p)$, zuordnet, ist ein S-R-Isomorphismus.

(v) Die Abbildung $S \to \mathrm{End}_R(P)$, die jedem $s \in S$ die Abbildung $P \to P$, $p \mapsto sp$, zuordnet, ist ein Ringisomorphismus. Die Abbildung $S^\circ \to \mathrm{End}_R(Q)$, die jedem $s \in S$ die Abbildung $Q \to Q$, $q \mapsto qs$ zuordnet, ist ein Ringisomorphismus.

Beweis. Wir wählen Elemente $p_1, \ldots, p_k \in P$, $q_1, \ldots, q_k \in Q$ mit $\sigma\big(\sum_{i=1}^k p_i \otimes q_i\big) = 1_S$.

(i) Sind $x_1, \ldots, x_l \in P$, $y_1, \ldots, y_l \in Q$ mit $\sigma\big(\sum_{j=1}^l x_j \otimes y_j\big) = 0$, so ist

$$\begin{aligned}\sum_{j=1}^{l} x_j \otimes y_j &= \sum_{i,j} x_j \otimes y_j \sigma(p_i \otimes q_i) = \sum_{i,j} x_j \otimes \underbrace{\tau(y_j \otimes p_i)}_{\in R} q_i \\ &= \sum_{i,j} x_j \tau(y_j \otimes p_i) \otimes q_i = \sum_{i,j} \sigma(x_j \otimes y_j) p_i \otimes q_i = 0\ .\end{aligned}$$

Daher ist σ injektiv.

(ii) Die Abbildungen $f : R^k \to P$, $(r_1, \ldots, r_k) \mapsto \sum_{i=1}^k p_i r_i$, und $g : P \to R^k$, $p \mapsto \big(\tau(q_1 \otimes p), \ldots, \tau(q_k \otimes p)\big)$, sind R-linear mit $f\big(g(p)\big) = \sum_{i=1}^k p_i \tau(q_i \otimes p) = \sum_{i=1}^k \sigma(p_i \otimes q_i) p = p$ für $p \in P$. Daher ist $0 \longrightarrow \mathrm{Ker}(f) \hookrightarrow R^k \xrightarrow{f} P \longrightarrow 0$ eine zerfallende exakte Folge. Folglich ist P ein endlich erzeugter projektiver R-Rechtsmodul.
Analog ist Q ein endlich erzeugter projektiver R-Linksmodul.

(iii) Die Abbildung $h : P^k \to S$, $(x_1, \ldots, x_k) \mapsto \sigma\big(\sum_{i=1}^k x_i \otimes q_i\big)$, ist S-linear. Wegen $h(p_1, \ldots, p_k) = \sigma\big(\sum_{i=1}^k p_i \otimes q_i\big) = 1_S$ ist h surjektiv. Daher ist P ein S-Generator.
Analog ist Q ein S-Generator.

(iv) Man rechnet leicht nach, daß die angegebene Abbildung $Q \to \mathrm{Hom}_R(P, R)$ wohldefiniert und R-S-linear ist. Ist $q \in Q$ mit $\tau(q \otimes p) = 0$ für alle $p \in P$, so ist

$$q = \sum_{i=1}^{k} q\sigma(p_i \otimes q_i) = \sum_{i=1}^{k} \underbrace{\tau(q \otimes p_i)}_{=0} q_i = 0 \ .$$

Andererseits gilt für $\lambda \in \mathrm{Hom}_R(P, R)$ und $p \in P$:

$$\begin{aligned}\lambda(p) = \lambda\Big(\sum_{i=1}^{k} \sigma(p_i \otimes q_i)p\Big) &= \lambda\Big(\sum_{i=1}^{k} p_i \underbrace{\tau(q_i \otimes p)}_{\in R}\Big) \\ = \sum_{i=1}^{k} \lambda(p_i)\tau(q_i \otimes p) &= \sum_{i=1}^{k} \tau\big(\lambda(p_i)q_i \otimes p\big) \ .\end{aligned}$$

Daher ist λ das Bild von $\sum_{i=1}^{k} \lambda(p_i)q_i$ unter der angegebenen Abbildung. Analog erhält man die zweite Aussage.

(v) Man rechnet leicht nach, daß die angegebene Abbildung $S \to \mathrm{End}_R(P)$ wohldefiniert und ein Ringhomomorphismus ist. Ist $s \in S$ mit $sP = 0$, so ist

$$s = s\sigma\Big(\sum_{i=1}^{k} p_i \otimes q_i\Big) = \sum_{i=1}^{k} \sigma(\underbrace{sp_i}_{=0} \otimes q_i) = 0 \ .$$

Für $\varphi \in \mathrm{End}_R(P)$ und $p \in P$ ist andererseits

$$\begin{aligned}\varphi(p) = \sum_{i=1}^{k} \varphi\big(\sigma(p_i \otimes q_i)p\big) &= \sum_{i=1}^{k} \varphi\big(p_i \underbrace{\tau(q_i \otimes p)}_{\in R}\big) \\ = \sum_{i=1}^{k} \varphi(p_i)\tau(q_i \otimes p) &= \sum_{i=1}^{k} \sigma\big(\varphi(p_i) \otimes q_i\big)p \ .\end{aligned}$$

Folglich ist φ das Bild von $\sum_{i=1}^{k} \sigma\big(\varphi(p_i) \otimes q_i\big)$ unter der angegebenen Abbildung. Die andere Aussage geht analog.

15.6. Satz (Morita). *Für Ringe R, S sind äquivalent:*

(1) $R \approx S$.

(2) Es existieren additive Funktoren ${}_R\mathbf{Mod} \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} {}_S\mathbf{Mod}$ *mit* $\Psi \circ \Phi \sim \mathrm{Id}_{{}_R\mathbf{Mod}}$ *und* $\Phi \circ \Psi \sim \mathrm{Id}_{{}_S\mathbf{Mod}}$.

(3) Es existiert ein S-Progenerator P mit $R^\circ \cong \mathrm{End}_S(P)$.

(4) Es existiert ein Morita-Kontext $(R, S, P, Q, \sigma, \tau)$, wobei σ, τ surjektiv sind.

(5) Es existiert ein S-R-Bimodul P und ein R-S-Bimodul Q mit $P \otimes_R Q \cong S$ (als S-S-Bimodul) und $Q \otimes_{S'} P \cong R$ (als R-R-Bimodul).

Beweis.

(1) $\iff$ (2): Definition 14.5.

(2) $\implies$ (3): Satz 15.3.

(3) $\implies$ (4): Satz 15.4.

(4) $\implies$ (5): Satz 15.5.

(5) $\implies$ (2): Seien P, Q wie in (5). Wir wählen entsprechende Isomorphismen von Bimoduln $\alpha : P \otimes_R Q \to S$, $\beta : Q \otimes_S P \to R$. Wir definieren $\Phi : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ durch $\Phi(M) := P \otimes_R M$ und $\Phi(f) := \mathrm{id}_P \otimes f : P \otimes_R M \to P \otimes_R M'$ für $M, M' \in {}_R\mathbf{Mod}$ und $f \in \mathrm{Hom}_R(M, M')$. Analog definieren wir $\Psi : {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$ durch $\Psi(N) := Q \otimes_S N$ und $\Psi(g) := \mathrm{id}_Q \otimes g : Q \otimes_S N \to Q \otimes_S N'$ für $N, N' \in {}_S\mathbf{Mod}$ und $g \in \mathrm{Hom}_S(N, N')$. Für $M \in {}_R\mathbf{Mod}$ haben wir einen R-Isomorphismus $\varphi_M : \Psi\big(\Phi(M)\big) = Q \otimes_S P \otimes_R M \xrightarrow{\beta \otimes \mathrm{id}_M} R \otimes_R M \xrightarrow{\mu_M} M$, $q \otimes p \otimes m \mapsto \beta(q \otimes p)m$. Die Familie $\varphi = (\varphi_M)_{M \in {}_R\mathbf{Mod}}$ ist dann eine natürliche Äquivalenz $\Psi \circ \Phi \Rightarrow \mathrm{Id}_{{}_R\mathbf{Mod}}$, denn für $M, M' \in {}_R\mathbf{Mod}$, $f \in \mathrm{Hom}_P(M, M')$, $q \in Q$, $p \in P$, $m \in M$ gilt:

$$\begin{array}{ccc} Q \otimes_S P \otimes_R M & \xrightarrow{\mathrm{id}_Q \otimes \mathrm{id}_P \otimes f} & Q \otimes_S P \otimes_R M' \\ \Big\downarrow{\scriptstyle \varphi_M} & & \Big\downarrow{\scriptstyle \varphi_{M'}} \\ M & \xrightarrow{\quad f \quad} & M' \end{array}$$

$$\big[\varphi_{M'} \circ (\mathrm{id}_Q \otimes \mathrm{id}_P \otimes f)\big](q \otimes p \otimes m) = \cdots = (f \circ \varphi_M)(q \otimes p \otimes m) \ .$$

Bemerkungen.

(i) Aus $R \approx S$ folgt $R^\circ \approx S^\circ$.

(ii) Man kann zeigen, daß in der obigen Situation $\Phi \sim (P \otimes_R \bullet)$.

Beispiele.

(a) Für $R \in \mathbf{Ri}$ und $n \in \mathbb{N}$ ist R^n ein R-Progenerator und

$$\mathrm{End}_R(R^n) \cong \mathrm{Mat}\big(n, \mathrm{End}_R(R)\big) \cong \mathrm{Mat}(n, R^\circ) \cong \mathrm{Mat}(n, R)^\circ \ .$$

Daher gilt stets: $\boxed{R \approx \mathrm{Mat}(n, R)}$.

(b) Für jedes Idempotent e in einem Ring R mit $ReR = R$ gilt $\boxed{R \approx eRe}$; wir haben nämlich einen Morita-Kontext $(R, eRe, eR, Re, \sigma, \tau)$, in dem $\sigma : eR \otimes_R Re \to eRe$, $x \otimes y \mapsto xy$, und $\tau : Re \otimes_{eRe} eR \to ReR = R$, $x \otimes y \mapsto xy$, surjektiv sind.

15.7. Bemerkung. Im folgenden bezeichnen wir mit $\mathrm{in}_Y^X : Y \to X$, $y \mapsto y$, die Inklusionsabbildung einer Teilmenge Y einer Menge X.

Satz. *Gegeben seien Ringe R, S, die vermöge additiver Funktoren ${}_R\mathbf{Mod} \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} {}_S\mathbf{Mod}$ Morita-äquivalent sind. Für $M \in {}_R\mathbf{Mod}$ ist dann*

$$L \mapsto \Lambda(L) := \mathrm{Bld}\big(\Phi(\mathrm{in}_L^M)\big)$$

eine Bijektion zwischen der Menge der Untermoduln von M und der Menge der Untermoduln von $\Phi(M)$. Für Untermoduln L, L' von M gilt dabei:

(i) $L \subseteq L' \iff \Lambda(L) \subseteq \Lambda(L')$.

(ii) $\Lambda(L \overset{+}{\cap} L') = \Lambda(L) \overset{+}{\cap} \Lambda(L')$

Beweis. Wir wählen eine natürliche Äquivalenz $\varphi : \Psi \circ \Phi \Rightarrow \mathrm{Id}_{{}_R\mathbf{Mod}}$ und betrachten die Abbildungen

$$\begin{array}{cl}
\big\{\text{Untermoduln von } M\big\} & \\
\downarrow \Lambda & L \mapsto \mathrm{Bld}\Big(\Phi\big(\mathrm{in}_L^M\big)\Big) \\
\big\{\text{Untermoduln von } \Phi(M)\big\} & \\
\downarrow \Delta & N \mapsto \mathrm{Bld}\Big(\Psi\big(\mathrm{in}_N^{\Phi(M)}\big)\Big) \\
\big\{\text{Untermoduln von } \Psi\big(\Phi(M)\big)\big\} & \\
\downarrow \Gamma & K \mapsto \varphi_M(K) \\
\big\{\text{Untermoduln von } M\big\} &
\end{array}$$

Ist L ein Untermodul von M, so ist $\Phi(\mathrm{in}_L^M) : \Phi(L) \to \Phi(M)$ injektiv mit Bild $\Lambda(L)$. Daher existiert ein S-Isomorphismus $f : \Phi(L) \to \Lambda(L)$ mit $\Phi(\mathrm{in}_L^M) = \mathrm{in}_{\Lambda(L)}^{\Phi(M)} \circ f$. Folglich ist

$$\begin{aligned}
\Gamma\Big(\Delta\big(\Lambda(L)\big)\Big) &= \mathrm{Bld}\Big(\varphi_M \circ \Psi\big(\mathrm{in}_{\Lambda(L)}^{\Phi(M)}\big)\Big) = \mathrm{Bld}\Big(\varphi_M \circ \Psi\big(\mathrm{in}_{\Lambda(L)}^{\Phi(M)}\big) \circ \Psi(f)\Big) \\
&= \mathrm{Bld}\Big(\varphi_M \circ \Psi\big(\Phi(\mathrm{in}_L^M)\big)\Big) = \mathrm{Bld}\big(\mathrm{in}_L^M \circ \varphi_L\big) = \mathrm{Bld}\big(\mathrm{in}_M^L\big) \\
&= L\,.
\end{aligned}$$

Daher ist $\Gamma \circ \Delta \circ \Lambda = \mathrm{id}$; insbesondere ist Λ injektiv und $\Gamma \circ \Delta$ surjektiv. Da Γ bijektiv ist, ist auch Δ surjektiv. Analog ist Δ aber auch injektiv, d.h. bijektiv. Daher ist Λ bijektiv.

(i) Seien L, L' zwei Untermoduln von M. Aus $L \subseteq L'$ folgt $\mathrm{in}_L^M = \mathrm{in}_{L'}^M \circ \mathrm{in}_L^{L'}$. Daher ist $\Phi\big(\mathrm{in}_L^M\big) = \Phi\big(\mathrm{in}_{L'}^M\big) \circ \Phi\big(\mathrm{in}_L^{L'}\big)$. Danach ist

$$\Lambda(L) = \mathrm{Bld}\Big(\Phi\big(\mathrm{in}_L^M\big)\Big) \subseteq \mathrm{Bld}\Big(\Phi\big(\mathrm{in}_{L'}^M\big)\Big) = \Lambda(L')\,.$$

Aus $\Lambda(L) \subseteq \Lambda(L')$ folgt analog $\Delta\big(\Lambda(L)\big) \subseteq \Delta\big(\Lambda(L')\big)$, also

$$L = \Gamma\Big(\Delta\big(\Lambda(L)\big)\Big) \subseteq \Gamma\Big(\Delta\big(\Lambda(L')\big)\Big) = L'\,.$$

(ii) Folgt aus (i)

15.8. Bemerkung. Gegeben seien Ringe R, S, die vermöge additiver Funktoren ${}_R\mathbf{Mod} \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} {}_S\mathbf{Mod}$ Morita-äquivalent sind. Aus Satz 15.7 folgt, daß für $M \in {}_R\mathbf{Mod}$ gilt:

(i) M einfach (halbeinfach) $\iff \Phi(M)$ einfach (halbeinfach).

(ii) M unzerlegbar $\iff \Phi(M)$ unzerlegbar.

(iii) M artinsch (noethersch) $\iff \Phi(M)$ artinsch (noethersch).

Daraus ergibt sich sofort

(i) R halbeinfach $\iff S$ halbeinfach.

(ii) R artinsch (noethersch) $\iff S$ artinsch (noethersch).

Satz. *Gegeben seien Ringe R, S mit $R \approx S$. Dann ist $Z(R) \cong Z(S)$ (als Ringe).*

Beweis. Wir wählen einen Morita-Kontext $(R, S, P, Q, \sigma, \tau)$ mit surjektiven σ, τ. Für $r \in Z(R)$ ist die Abbildung $\varrho_r : P \to P$, $p \mapsto pr$, ein R-Homomorphismus mit $\varphi\big(\varrho_r(p)\big) = \varphi(pr) = \varphi(p)r = \varrho_r\big(\varphi(p)\big)$ für $\varphi \in \mathrm{End}_R(P)$, $p \in P$. Folglich ist $\varrho_r \in Z\big(\mathrm{End}_R(P)\big)$. Nach Satz 15.5 (v) existiert also genau ein Element $\zeta(r) \in Z(S)$ mit $\zeta(r)p = \zeta_r(p) = pr$ für $p \in P$. Analog existiert zu jedem $s \in Z(S)$ genau ein Element $\eta(s) \in Z(R)$ mit $p\eta(s) = sp$ für $p \in P$. Für $r \in Z(R)$ und $p \in P$ ist dann $pr = \zeta(r)p = p\eta\big(\zeta(r)\big)$, d.h. $p\Big(r - \eta\big(\zeta(r)\big)\Big) = 0$. Da P ein R-Progenerator ist, folgt $r - \eta\big(\zeta(r)\big) = 0$, d.h. $\eta\big(\zeta(r)\big) = r$. Analog ist $\zeta\big(\eta(s)\big) = s$ für $s \in Z(S)$. Daher sind $\zeta : Z(R) \to Z(S)$ und $\eta : Z(S) \to Z(R)$ zueinander inverse bijektive Abbildungen. Man rechnet leicht nach, daß ζ ein Ringisomorphismus ist.

15.9. Bemerkung. Für kommutative Ringe R, S gilt also nach Satz 15.8: $R \cong S \iff R \approx S$. Das gleiche gilt, falls R, S lokale Ringe sind; denn ist P ein S-Progenerator mit $R^\circ \cong \mathrm{End}_S(P)$, so ist P frei, also $P \cong S^n$ für ein $n \in \mathbb{N}$ und damit $R^\circ \cong \mathrm{End}_S(S^n) \cong \mathrm{Mat}(n, S)^\circ$, d.h. $R \cong \mathrm{Mat}(n, S)$. Da R lokal ist, folgt $n = 1$, denn sonst ist

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} + \begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

in $\mathrm{Mat}(n, S)$.

Satz. *Sei $R \approx S$ vermöge additiver Funktoren ${}_R\mathbf{Mod} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} {}_S\mathbf{Mod}$. Dann ist die Abbildung*

$$I \mapsto \Gamma(I) := \mathrm{Ann}_S\left(\Phi\left({}^{R}\!/_{I}\right)\right)$$

eine Bijektion zwischen der Menge der Ideale in R und der Menge der Ideale in S. Für Ideale I, I' in R gilt dabei

(i) $I \subseteq I' \iff \Gamma(I) \subseteq \Gamma(I')$.

(ii) $\Gamma(I \overset{+}{\cap} I') = \Gamma(I) \overset{+}{\cap} \Gamma(I')$.

Beweis. Offenbar ist $\Gamma(I)$ für jedes Ideal I in R ein Ideal in S. Analog ist $\Delta\big(\Gamma(J)\big) := \mathrm{Ann}_R\Big(\Psi\big({}^S/_J\big)\Big)$ für jedes Ideal $J \in S$ ein Ideal in R. Ferner hat man einen R-Epimorphismus

$$f : \coprod_{x\in\Psi\left({}^S/_J\right)} {}^R/_{\Delta(J)} \to \Psi\left({}^S/_J\right)\ , \quad \big(r_x + \Delta(J)\big) \mapsto \sum_{x\in\Psi\left({}^S/_J\right)} r_x x\ ,$$

und einen R-Monomorphismus

$$g : {}^R/_{\Delta(J)} \to \prod_{x\in\Psi\left({}^S/_J\right)} \Psi\left({}^S/_J\right)\ , \quad r + \Delta(J) \mapsto (rx)_{x\in\Psi(S/J)}\ .$$

Anwendung von Φ macht daraus einen S-Epimorphismus

$$\coprod_x \Phi\left({}^R/_{\Delta(J)}\right) \cong \Phi\Big(\coprod_x {}^R/_{\Delta(J)}\Big) \to \Phi\left(\Psi\left({}^S/_J\right)\right) \cong {}^S/_J$$

und einen S-Monomorphismus

$$\Phi\left({}^R/_{\Delta(J)}\right) \to \Phi\left(\prod_x \Psi\left({}^S/_J\right)\right) \cong \prod_x \Phi\left(\Psi\left({}^S/_J\right)\right) \cong \prod_x {}^S/_J\ .$$

Daher ist $J = \mathrm{Ann}_S\left({}^S/_J\right) = \mathrm{Ann}_S\Big(\Phi\big({}^R/_{\Delta(J)}\big)\Big) = \Gamma\big(\Delta(J)\big)$. Analog ist $\Delta\big(\Gamma(I)\big) = I$ für jedes Ideal I in R.

(i) Seien I, I' Ideale in R mit $I \subseteq I'$. Dann ist $h : {}^R/_I \to {}^R/_{I'}$, $r + I \mapsto r + I'$ ein R-Epimorphismus. Folglich ist $\Phi(h) : \Phi\left({}^R/_I\right) \to \Phi\left({}^R/_{I'}\right)$ ein S-Epimorphismus, d.h. $\Gamma(I) = \mathrm{Ann}_S\Big(\Phi\big({}^R/_I\big)\Big) \subseteq \mathrm{Ann}_S\Big(\Phi\big({}^R/_{I'}\big)\Big) = \Gamma(I')$.
Analog ist $\Delta(J) \subseteq \Delta(J')$ für beliebige Ideale J, J' in S mit $J \subseteq J'$.

(ii) Folgt aus (i).

15.10. Bemerkung. Sei $R \approx S$ wie in Satz 15.9. Dann gilt:

(i) R einfach $\Longleftrightarrow$ S einfach.

(ii) $\Gamma\big(J(R)\big) = J(S)$; für jeden einfachen S-Modul N ist $\Psi(N)$ ein einfacher R-Modul, d.h. $J(R)\cdot\Psi(N) = 0$. Es existiert also ein R-Epimorphismus $f : {}^R/_{J(R)} \to \Psi(N)$. Daher ist $\Phi(f) : \Phi\left({}^R/_{J(R)}\right) \to \Phi\big(\Psi(N)\big) \cong N$ ein S-Epimorphismus. Folglich ist

$$\Gamma\big(J(R)\big) = \mathrm{Ann}_S\left(\Phi\left({}^R/_{J(R)}\right)\right) \subseteq \mathrm{Ann}_S(N)\ .$$

Da dies für *jeden* einfachen S-Modul N gilt, folgt:

$$\Gamma\big(J(R)\big) \subseteq J(S)\ .$$

Analog ist $\Delta\big(J(S)\big) \subseteq J(R)$. Insgesamt ist also $\Gamma\big(J(R)\big) \subseteq J(S) = \Gamma\Big(\Delta\big(J(S)\big)\Big) \subseteq \Gamma\big(J(R)\big)$, d.h. $\Gamma\big(J(R)\big) = J(S)$.

(iii) $\Gamma(I\cdot I') = \Gamma(I)\cdot\Gamma(I')$ für alle Ideale I, I' in R; dies werden wir nicht beweisen. Daraus folgt, daß ein Ideal I in R genau dann ein Primideal ist, wenn $\Gamma(I)$ ein Primideal in S ist. Insbesondere bildet Γ das Primradikal von R auf das Primradikal von S ab.

(iv) Ein Ideal I in R ist nach (iii) genau dann nilpotent, wenn $\Gamma(I)$ nilpotent ist. Es ist unbekannt, ob dies entsprechend für Nilideale gilt.

(v) Eine Folge $\mathcal{E} : 0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ in ${}_R\mathbf{Mod}$ ist genau dann exakt, wenn die Folge $\Phi(\mathcal{E}) : 0 \longrightarrow \Phi(L) \xrightarrow{\Phi(f)} \Phi(M) \xrightarrow{\Phi(g)} \Phi(N) \longrightarrow 0$ exaktist; ist nämlich $\mathcal{E}$ exakt, so ist f injektiv, g surjektiv und $\mathrm{Bld}(f) = \mathrm{Ker}(g)$. Daher ist $\Phi(f)$ injektiv, $\Phi(g)$ surjektiv und $\Phi(g) \circ \Phi(f) = \Phi(g \circ f) = \Phi(0) = 0$, d.h. $\mathrm{Bld}\big(\Phi(f)\big) \subseteq \mathrm{Ker}\big(\Phi(g)\big) = K$. Zum Beweis der umgekehrten Inklusion sei $i : K \to \Phi(M)$ die Inklusionsabbildung und $\varphi : \Psi \circ \Phi \Rightarrow \mathrm{Id}_{{}_R\mathbf{Mod}}$ eine natürliche Äquivalenz. Dann ist

$$\begin{aligned} g \circ \varphi_M \circ \Psi(i) &= \varphi_N \circ \Psi\big(\Phi(g)\big) \circ \Psi(i) \\ &= \varphi_N \circ \underbrace{\big(\Phi(g) \circ i\big)}_{=0} = 0\ , \end{aligned}$$

d.h. $\mathrm{Bld}\big(\varphi_M \circ \Psi(i)\big) \subseteq \mathrm{Ker}(g) = \mathrm{Bld}(f)$. Daher existiert ein $h \in \mathrm{Hom}_R\big(\Psi(K), L\big)$ mit $f \circ h = \varphi_M \circ \Psi(i)$, d.h.

$$\Psi(i) = \varphi_M^{-1} \circ f \circ h = \Psi\big(\Phi(f)\big) \circ \varphi_L^{-1} \circ h = \underbrace{\Psi\big(\Phi(f)\big) \circ \Psi(k)}_{=\Psi\left(\Phi(f)\circ k\right)}$$

für ein $k \in \mathrm{Hom}_S\big(K, \Phi(L)\big)$. Daher ist $i = \Phi(f) \circ k$ und $\mathrm{Ker}\big(\Phi(g)\big) = K = \mathrm{Bld}(i) \subseteq \mathrm{Bld}\big(\Phi(f)\big)$. Damit ist gezeigt, daß $\Phi(\mathcal{E})$ exakt ist.
Ist umgekehrt $\Phi(\mathcal{E})$ exakt, so auch analog $\Psi\big(\Phi(\mathcal{E})\big)$, und man hat ein kommutatives Diagramm

$$\begin{tikzcd} 0 \arrow[r] & \Psi\big(\Phi(L)\big) \arrow[r, "\Psi(\Phi(f))"] \arrow[d, "\varphi_L"] & \Psi\big(\Phi(M)\big) \arrow[r, "\Psi(\Phi(g))"] \arrow[d, "\varphi_M"] & \Psi\big(\Phi(N)\big) \arrow[r] \arrow[d, "\varphi_N"] & 0 \\ 0 \arrow[r] & L \arrow[r, "f"] & M \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

Es folgt leicht, daß $\mathcal{E}$ exakt ist.

Satz. *Im Fall $R \approx S$ gilt*

$$R \textit{ semiperfekt} \iff S \textit{ semiperfekt}\ .$$

Beweis. Sei R semiperfekt. Wir wählen additive Funktoren ${}_R\mathbf{Mod} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} {}_S\mathbf{Mod}$ mit $\Psi \circ \Phi \sim \mathrm{Id}_{{}_R\mathbf{Mod}}$ und $\Phi \circ \Psi \sim \mathrm{Id}_{{}_S\mathbf{Mod}}$. Ist N ein endlich erzeugter S-Modul, so ist $\Psi(N)$ ein endlich erzeugter R-Modul, hat also eine projektive Decke $f : P \to \Psi(N)$. Damit ist $\Phi(f) : \Phi(P) \to \Phi\big(\Psi(N)\big) \cong N$ ein S-Epimorphismus, und $\Phi(P)$ ist projektiv. Daher genügt zu zeigen, daß $\mathrm{Ker}\big(\Phi(f)\big)$ überflüssig in $\Phi(P)$ ist.
Zum Beweis betrachten wir die exakte Folge

$$0 \longrightarrow \mathrm{Ker}(f) \overset{\mathrm{in}}{\hookrightarrow} P \xrightarrow{f} \Psi(N) \longrightarrow 0$$

in ${}_R\mathbf{Mod}$. Nach der obigen Bemerkung ist

$$0 \longrightarrow \Phi\big(\mathrm{Ker}(f)\big) \xrightarrow{\Phi(\mathrm{in})} \Phi(P) \xrightarrow{\Phi(f)} \Phi\big(\Psi(N)\big) \longrightarrow 0$$

exakt in ${}_S\mathbf{Mod}$. Daher ist $\mathrm{Ker}\big(\Phi(f)\big) = \mathrm{Bld}\big(\Phi(\mathrm{in})\big) = \Lambda\big(\mathrm{Ker}(f)\big)$ in der Notation von Satz 15.7. Da $\mathrm{Ker}(f)$ überflüssig in P ist, folgt aus Satz 15.7, daß $\Lambda\big(\mathrm{Ker}(f)\big)$ überflüssig in $\Phi(P)$ ist.

16 Die Picardgruppe eines Ringes

Sei R ein Ring.

16.1. Definition. Ein R-R-Bimodul P heißt **invertierbar**, falls ein R-R-Bimodul Q existiert mit $P \otimes_R Q \cong R$ und $Q \otimes_R P \cong R$ (als R-R-Bimodul).

Satz. *Für jeden invertierbaren R-R-Bimodul P gilt:*

(i) $\mathrm{End}_R(P_R) \cong R$ *und* $\mathrm{End}_R({}_RP) \cong R^\circ$ *(als Ringe).*

(ii) $\mathrm{End}_{R,R}(P) \cong Z(R)$ *(als Ring).*

(iii) ${}_RP$ *und* P_R *sind R-Progeneratoren.*

(iv) $P \otimes_R \mathrm{Hom}_R(P,R) \cong R$ *und* $\mathrm{Hom}_R(P,R) \otimes_R P \cong R$ *(als R-R-Bimoduln).*

Beweis. Sei Q wie in der Definition. Wir wählen R-R-Isomorphismen $\varphi : P \otimes_R Q \to R$ und $\psi : Q \otimes_R P \to R$ und Elemente $x_1, \ldots, x_k \in P$, $y_1, \ldots, y_k \in Q$ mit $\varphi\big(\sum_{i=1}^k x_i \otimes y_i\big) = 1_R$.

(i) Wir definieren $\vartheta : R \to \mathrm{End}_R(P_R)$ durch $[\vartheta(r)](p) = rp$ für $r \in R$, $p \in P$. Dann ist ϑ ein Ringhomomorphismus. Im Fall $r \in \mathrm{Ker}(\vartheta)$ ist $rP = 0$; insbesondere ist also

$$r = r1 = \sum_{i=1}^k r\varphi(x_i \otimes y_i) = \sum_{i=1}^k \varphi(\underbrace{rx_i}_{=0} \otimes y_i) = 0\,.$$

Daher ist ϑ injektiv. Für $f \in \mathrm{End}_R(P_R)$ ist $f \otimes \mathrm{id}_Q \in \mathrm{End}_R(P \otimes_R Q)$,

$$\begin{tikzcd}
P \otimes_R Q \arrow[r, "\varphi"] \arrow[d, "f \otimes \mathrm{id}_Q"] & R \arrow[d] \\
P \otimes_R Q \arrow[r, "\varphi"] & R
\end{tikzcd}$$

also $\varphi\circ(f\otimes\mathrm{id}_Q)\circ\varphi^{-1} \in \mathrm{End}_R(R_R)$. Daher existiert $r \in R$ mit $\big[\varphi\circ(f\otimes\mathrm{id}_Q)\otimes\varphi^{-1}\big](x) = rx$ für $x \in R$, d.h. $\big[\varphi \circ (f \otimes \mathrm{id}_Q)\big](y) = r\varphi(y) = \varphi(ry)$ für $y \in P \otimes_R Q$. Folglich ist $(f \otimes \mathrm{id}_Q)(y) = ry$ für $y \in P \otimes_R Q$; insbesondere ist

$$\begin{aligned}
(f \otimes \mathrm{id}_Q)(p \otimes q) &= r(p \otimes q) = (rp) \otimes q \\
&= \big[\vartheta(r)\big](p) \otimes q = \big[\vartheta(r) \otimes \mathrm{id}_Q\big](p \otimes q)
\end{aligned}$$

für alle $p \in P$, $q \in Q$, d.h. $f \otimes \mathrm{id}_Q = \vartheta(r) \otimes \mathrm{id}_Q$. Daher ist $f \otimes \mathrm{id}_Q \otimes \mathrm{id}_P = \vartheta(r) \otimes \mathrm{id}_Q \otimes \mathrm{id}_P$.

$$\begin{tikzcd}
P \otimes_R Q \otimes_R P \arrow[r, "\mathrm{id}_P \otimes\psi"] \arrow[d, swap, "\vartheta(r) \otimes \mathrm{id}_Q \otimes \mathrm{id}_P"] \arrow[d, "f \otimes \mathrm{id}_Q \otimes \mathrm{id}_P"] & P \otimes_R R \arrow[r, "\mu"] \arrow[d, swap, "\vartheta(r) \otimes \mathrm{id}_R"] \arrow[d, "f \otimes \mathrm{id}_R"] & P \arrow[d, swap, "\vartheta(r)"] \arrow[d, "f"] \\
P \otimes_R Q \otimes_R P \arrow[r, "\mathrm{id}_P \otimes\psi"] & P \otimes_R R \arrow[r, "\mu"] & P
\end{tikzcd}$$

Da beide Diagramme kommutieren, folgt $f = \vartheta(r)$.

(ii) Für $z \in Z(R)$ ist die Abbildung $\vartheta(z) : P \to P$, $p \mapsto zp$, ein R-R-Endomorphismus von P. Daher ist die Einschränkung von ϑ ein Ringmonomorphismus $Z(R) \to \mathrm{End}_{R,R}(P)$. Ist $f \in \mathrm{End}_{R,R}(P)$, so existiert nach (i) ein $r \in R$ mit $f(p) = rp$ für $p \in P$. Für $a \in R$, $p \in P$ ist also $arp = af(p) = f(ap) = rap$. Daher ist

$$\begin{aligned} ar = ar1 = ar\varphi\Big(\sum_{i=1}^{k} x_i \otimes y_i\Big) &= \sum_{i=1}^{k} \varphi(arx_i \otimes y_i) \\ = \sum_{i=1}^{k} \varphi(rax_i \otimes y_i) = ra\varphi\Big(\sum_{i=1}^{k} x_i \otimes y_i\Big) &= ra \,. \end{aligned}$$

Daher ist $r \in Z(R)$.

(iii) Wir betrachten das Diagramm

$$\begin{tikzcd} P \otimes_R Q \otimes_R P \arrow[r, "\varphi \otimes \mathrm{id}_P"] \arrow[d, "\mathrm{id}_P \otimes \psi"] & R \otimes_R P \arrow[d, "\alpha"] \\ P \otimes_R R \arrow[r, "\beta"] & P \end{tikzcd}$$

wobei α, β durch die Multiplikation induziert werden. Das Diagramm ist nicht unbedingt kommutativ. Aber:

$$u := \beta \circ (\mathrm{id}_P \otimes \psi) \circ (\varphi \otimes \mathrm{id}_P)^{-1} \circ \alpha^{-1}$$

ist ein R-R-Automorphismus. Nach (ii) existiert also eine Einheit $z \in Z(R)$ mit $u(p) = zp$ für $p \in P$. Ersetzen wir also φ durch $\varphi' : P \otimes_R Q \to R$, $y \mapsto z\varphi(y)$, so kommutiert das obige Diagramm.
Als nächstes betrachten wir

$$\begin{tikzcd} Q \otimes_R P \otimes_R Q \arrow[r, "\psi \otimes \mathrm{id}_Q"] \arrow[d, "\mathrm{id}_R \otimes \varphi'"] & R \otimes_R Q \arrow[d, "\alpha'"] \\ Q \otimes_R R \arrow[r, "\beta'"] & Q \end{tikzcd}$$

Wir zeigen, daß dieses Diagramm „automatisch" kommutiert. Dazu seien $p \in P$, $q, q' \in Q$.

$$\begin{aligned} d &:= \big[\alpha' \circ (\psi \otimes \mathrm{id}_Q)\big](q \otimes p \otimes q') - \big[\beta' \circ (\mathrm{id}_Q \otimes \varphi')\big](q \otimes p \otimes q') \\ &= \psi(q \otimes p)q' - q\varphi'(p \otimes q') \in Q \,. \end{aligned}$$

Für $p' \in P$ gilt wegen der Kommutativität des ersten Diagramms:

$$\begin{aligned} \psi(d \otimes p') &= \psi(q \otimes p)\psi(q' \otimes p') - \psi\big(q \otimes \varphi'(p \otimes q')p'\big) \\ &= \psi\big(q \otimes p\psi(q' \otimes p')\big) - \psi\big(q \otimes p\psi(q' \otimes p')\big) \\ &= 0 \,. \end{aligned}$$

Daher ist $d \otimes p' = 0$ für alle $p' \in P$ und es folgt leicht $d = 0$. Es sind also beide Diagramme kommutativ. Daher ist $(R, R, P, Q, \varphi, \psi)$ ein Morita-Kontext mit surjektiven φ, ψ. Der Rest folgt aus Satz 15.5.

16.2. Bemerkung. Für jeden R-R-Bimodul M bezeichnen wir mit $[M]$ seine Isomorphieklasse. Aus 16.1 folgt, daß die Isomorphieklassen invertierbarer R-R-Bimoduln eine Gruppe mit Multiplikation

$$[M] \cdot [N] = [M \otimes_R N] \, ,$$

Einselement $[R]$ und $[M]^{-1} = \big[\mathrm{Hom}_R(M,R)\big]$ bilden. (Dabei beachte man, daß dies überhaupt eine Menge ist, da invertierbare Bimoduln endlich erzeugt sind.) Diese Gruppe nennt man die **Picardgruppe** von R. Man schreibt $\mathrm{Pic}(R)$. In der Regel ist $\mathrm{Pic}(R)$ nicht kommutativ.
Die Picardgruppe $\mathrm{Pic}(R)$ hängt eng mit der Automorphismengruppe $\mathrm{Aut}(R)$ des Rings R zusammen. Wir erinnern uns, daß für $u \in U(R)$ die Abbildung

$$\mathrm{ad}_u : R \to R \, , \quad r \mapsto uru^{-1} \, ,$$

ein Automorphismus von R ist. Die so entstehende Abbdildung

$$\mathrm{ad} : U(R) \to \mathrm{Aut}(R) \, , \quad u \mapsto \mathrm{ad}_u \, ,$$

ist ein Gruppenhomomorphismus mit Kern $Z(R)$. Das Bild von ad ist eine Untergruppe von $\mathrm{Aut}(R)$, die man mit $\mathrm{Inn}(R)$ bezeichnet. Es ist also $\mathrm{Inn}(R) = \big\{\mathrm{ad}_u : u \in U(R)\big\}$. Die Elemente in $\mathrm{Inn}(R)$ bezeichnet man als **innere Automorphismen** von R.

16.3. Bemerkung. Für einen R-R-Bimodul M und Ringautomorphismen $\alpha, \beta \in \mathrm{Aut}(R)$ definiert man einen neuen R-R-Bimodul ${}_\alpha M_\beta$ folgendermaßen: Als abelsche Gruppe ist ${}_\alpha M_\beta$ gleich M, aber die Multiplikation auf ${}_\alpha M_\beta$ wird gegeben durch $r \bullet m = \alpha(r)m$, $m \bullet r = m\beta(r)$ für $r \in R$, $m \in M$. Offenbar ist ${}_{\mathrm{id}}M_{\mathrm{id}} = M$. Wir wenden jetzt diese Konstruktion auf $M = R$ an.

Satz. *Für $\alpha, \beta, \gamma \in \mathrm{Aut}(R)$ gilt:*

(i) Die Abbildung ${}_\alpha R_\beta \to {}_{\gamma\circ\alpha}R_{\gamma\circ\beta}$ ist ein R-R-Isomorphismus.

(ii) Die Abbildung ${}_{\mathrm{id}}R_\alpha \otimes_R {}_{\mathrm{id}}R_\beta \to {}_{\mathrm{id}}R_{\alpha\circ\beta}$, $x \otimes y \mapsto x\alpha(y)$, ist ein R-R-Isomorphismus.

(iii) Die Abbildung $\delta : \mathrm{Aut}(R) \to \mathrm{Pic}(R)$, $\alpha \mapsto \big[{}_{\mathrm{id}}R_\alpha\big]$, ist ein Gruppenhomomorphismus.

(iv) $\mathrm{Ker}(\delta) = \mathrm{Inn}(R)$.

Beweis.

(i) , (ii) Nachrechnen!

(iii) Folgt aus (ii).

(iv) Sei ${}_{\mathrm{id}}R_\alpha \cong {}_{\mathrm{id}}R_{\mathrm{id}}$ und $f : {}_{\mathrm{id}}R_\alpha \to {}_{\mathrm{id}}R_{\mathrm{id}}$ ein R-R-Isomorphismus. Dann ist f insbesondere ein Isomorphismus von R-Linksmoduln. Für $r \in R$ ist also $f(r) = f(r1) = rf(1) = ru$ mit $u := f(1) \in U(R)$. Andererseits ist $\alpha(r)u = f\big(\alpha(r)\big) = f(1 \bullet r) = f(1)r = ur$, also $\alpha(r) = uru^{-1}$ für $r \in R$. Daher ist $\alpha \in \mathrm{Inn}(R)$. Umgekehrt zeigt man, daß jeder innere Automorphismen von R im Kern von δ liegt.

16.4. Bemerkung. Aus 16.3 folgt, daß $\mathrm{Inn}(R)$ ein Normalteiler in $\mathrm{Aut}(R)$ ist. Die Faktorgruppe $\mathrm{Aut}(R)/\mathrm{Inn}(R)$ bezeichnet man mit $\mathrm{Out}(R)$. Man nennt $\mathrm{Out}(R)$ die **äußere Automorphismengruppe** von R. Nach dem Homomorphiesatz für Gruppen ist also $\mathrm{Out}(R)$ zu der Untergruppe $\mathrm{Bld}(\delta)$ von $\mathrm{Pic}(R)$ isomorph.

Satz. *In der obigen Situation gilt:*

$$\mathrm{Bld}(\delta) = \left\{[P] \in \mathrm{Pic}(R) : {}_RP \cong {}_RR\right\} .$$

Beweis. Offenbar gilt „$\subseteq$". Sei umgekehrt $[P] \in \mathrm{Pic}(R)$ mit ${}_RP \cong {}_RR$. Sei $f : {}_RP \to {}_RR$ ein R-Isomorphismus. Für $r \in R$ ist die Abbildung $g_r : {}_RP \to {}_RP$, $p \mapsto pr$, ein R-Homomorphismus. Daher ist $f \circ g_r \circ f^{-1} : {}_RR \to {}_RR$ ein R-Homomorphismus. Folglich existiert genau ein $\alpha(r) \in R$ mit $(f \circ g_r \circ f^{-1})(x) = x\alpha(r)$. Dann ist also $f(y)\alpha(r) = (f \circ g_r)(y) = f(yr)$ für $y \in P$. Daraus folgt leicht, daß α ein Ringautomorphismus und $f : {}_RP_R \to {}_{\mathrm{id}}R_\alpha$ ein R-R-Isomorphismus ist.

16.5. Bemerkung. Für $[P] \in \mathrm{Pic}(R)$ und $z \in Z(R)$ ist die Abbildung $P \to P$, $p \mapsto pz$, ein R-R-Endomorphismus. Nach Satz 16.1 (ii) existiert also ein Element $\alpha_P(z) \in Z(R)$ mit $pz = \alpha_P(z)p$ für $p \in P$. Man rechnet leicht nach, daß $\alpha_P : Z(R) \to Z(R)$ ein Ringautomorphismus ist. Außerdem rechnet man nach, daß die Abbildung $\eta : \mathrm{Pic}(R) \to \mathrm{Aut}\big(Z(R)\big)$, $[P] \mapsto \alpha_P$, ein wohldefinierter Gruppenhomomorphismus ist. Ein Element $[P] \in \mathrm{Pic}(R)$ liegt genau dann im Kern von η, wenn $zp = pz$ für alle $p \in P$, $z \in Z(R)$ gilt. Man setzt $\mathrm{Picent}(R) = \mathrm{Ker}(\eta)$. Nach dem Homomorphiesatz für Gruppen ist $\mathrm{Pic}(R)/\mathrm{Picent}(R)$ zu einer Untergruppe von $\mathrm{Aut}\big(Z(R)\big)$ isomorph. Ist R kommutativ und $P = {}_{\mathrm{id}}R_\alpha$ für ein $\alpha \in \mathrm{Aut}(R)$, so ist $p \bullet z = p\alpha(z) = \alpha(z)p$ für $p \in R$ und $z \in Z(R) = R$, d.h. $\alpha_P = \alpha$. Für einen kommutativen Ring R ist also $\eta : \mathrm{Pic}(R) \to \mathrm{Aut}(R)$ surjektiv; insbesondere ist dann $\mathrm{Aut}(R) \cong \mathrm{Pic}(R)/\mathrm{Picent}(R)$.
Ist R ein „Dedekind-Ring" (z.B. der Ring der ganzen algebraischen Zahlen in einem algebraischen Zahlkörper), so ist $\mathrm{Picent}(R)$ isomorph zur sogenannten „Klassengruppe" von R. Diese ist ein zentrales Objekt in der algebraischen Zahlentheorie.

Satz. *Für Morita-äquivalente Ringe R, S gilt stets:* $\mathrm{Pic}(R) \cong \mathrm{Pic}(S)$ *und* $\mathrm{Picent}(R) \cong \mathrm{Picent}(S)$.

Beweis. Wir wählen einen Morita-Kontext $(R, S, P, Q, \sigma, \tau)$ mit surjektiven σ, τ. Für $[M] \in \mathrm{Pic}(R)$ ist dann $[P \otimes_R M \otimes_R Q] \in \mathrm{Pic}(S)$ wegen

$$(P \otimes_R M \otimes_R Q) \otimes_S \big(P \otimes_R \mathrm{Hom}_R(M, R) \otimes_R Q\big) \cong \cdots \cong S$$

und

$$\big(P \otimes_R \mathrm{Hom}_R(M, R) \otimes_R Q\big) \otimes_S (P \otimes_R M \otimes_R Q) \cong \cdots \cong S .$$

Offenbar ist die Abbildung $\mathrm{Pic}(R) \to \mathrm{Pic}(S)$, $[M] \mapsto [P \otimes_R M \otimes_R Q]$ ein Homomorphismus von Gruppen. Analog kommt man zurück. Also ist $\mathrm{Pic}(R) \cong \mathrm{Pic}(S)$. Sei jetzt $[M] \in \mathrm{Picent}(R)$, d.h. $zm = mz$ für $m \in M$, $z \in Z(R)$. Nach Satz 15.8 existiert ein Ringisomorphismus $\zeta : Z(R) \to Z(S)$ mit $\zeta(z)p = pz$ für $z \in Z(R)$, $p \in P$. Daher gilt:

$$p \otimes zq = pz \otimes q = \zeta(z)p \otimes q = \zeta(z)(p \otimes q) = (p \otimes q)\zeta(z) = p \otimes q\zeta(z)$$

für $p \in P$, $q \in Q$, $z \in Z(R)$. Daraus folgt wie üblich: $zq = q\zeta(z)$ für $q \in Q$, $z \in Z(R)$. Daher ist

$$\begin{aligned}
\zeta(z)[p \otimes m \otimes q] &= \zeta(z)p \otimes m \otimes q = pz \otimes m \otimes q \\
&= p \otimes zm \otimes q = p \otimes mz \otimes q \\
&= p \otimes m \otimes zq = p \otimes m \otimes q\zeta(z) \\
&= [p \otimes m \otimes q]\zeta(z)
\end{aligned}$$

für $z \in Z(R)$, $p \in P$, $m \in M$, $q \in Q$, d.h. $[P \otimes_R M \otimes_R Q] \in \mathrm{Picent}(S)$.

16.6. Bemerkungen.

(i) Aus $R \approx S$ folgt i.a. nicht $\mathrm{Aut}(R) \cong \mathrm{Aut}(S)$ oder $\mathrm{Out}(R) \cong \mathrm{Out}(S)$.

(ii) Man kann zeigen, daß $\mathrm{Picent}(R) = 1$ ist, falls R halbeinfach ist. Dabei benötigt man den Satz von Skolem-Noether.

Index