# Höhere Algebra: Darstellungstheorie und homologische Algebra

Sommersemester 2017

Christoph Schweigert

Universität Hamburg
Fachbereich Mathematik
Bereich Algebra und Zahlentheorie

(Stand: 13.07.2015)

## Inhaltsverzeichnis

# Literatur:

Literatur, die ich bei der Vorbereitung häufig herangezogen habe:


- Wolfgang Soergel, Skript zur Vorlesung Algebra, erhältlich unter
  `http://home.mathematik.uni-freiburg.de/soergel/`
- Tilman Bauer, Skript zur Vorlesung Homologische Algebra, erhältlich unter
  `http://wwwmath.uni-muenster.de/u/tbauer/Homologische-Algebra/index.html`
- Jens Carsten Jantzen, Joachim Schwermer: Algebra, Springer, 2006
- Peter J. Hilton, Urs Stammbach: A course in homological algebra, Springer Graduate Texts in Mathematics, 1997
- Kenneth S. Brown: Cohomology of groups, Springer Graduate Texts in Mathematics, 1982
- Charles Weibel, An Introduction to Homological Algebra, Cambridge University Press, 1995
- Anthony Knapp, Advanced Algebra, Birkhäuser Cornerstones, Boston, 2007
- Saunders MacLane, Categories for the Working Mathematician, Springer Graduate Text in Mathematics 5, 1971.


Dieses Skript beruht auf Vorlesungen, die ich in den Wintersemestern 2008/09, 2010/11, 2013/14 und 2016/17 an der Universität Hamburg gehalten habe. Die aktuelle Version dieses Skriptes finden Sie unter
`http://www.math.uni-hamburg.de/home/schweigert/ws10/skript.pdf`
als pdf-Datei. Bitte schicken Sie Korrekturen und Bemerkungen an `christoph.schweigert@uni-hamburg.de`!

Simon Lentner, Catherine Meusburger und Thomas Nikolaus danke ich für zahlreiche Hinweise zum Skript und Diskussionen. Thomas Nikolaus danke ich auch für die Mitarbeit an den Musterlösungen. Den Hamburger Studierenden Rüdiger Brecht, Pascal Gollin, Johannes Lederich, David Lindemann, Nils Matthes, Svea-Nora Mierach, Christoph Nehring, Cora Welsch und Jan-Ole Willprecht danke ich für Hinweise zum Skript.

# 1 Moduln über Ringen

## 1.1 Grundlegende Definitionen

Ringe werden in dieser Vorlesung eine zentrale Rolle spielen. Wir wiederholen daher einige Begriffe:

***Definition 1.1.1***

*(i) Ein Ring ist eine additiv geschriebene abelsche Gruppe $(R,+)$ zusammen mit einer Abbildung*

$$\begin{array}{ccl} R\times R & \to & R \\ (x,y) & \mapsto & xy \equiv x\cdot y\ , \end{array}$$

*genannt Multiplikation, für die das Assoziativgesetz*

$$(xy)z = x(yz) \quad \text{für alle } x,y,z\in R$$

*und zwei Distributivgesetze gelten:*

$$(x_1+x_2)\cdot y = x_1\cdot y + x_2\cdot y \qquad \text{und} \quad x\cdot(y_1+y_2) = x\cdot y_1 + x\cdot y_2$$

*für alle $x, x_y, x_2, y, y_1, y_2 \in R$. Man beachte, dass $(R,\cdot)$ ein assoziatives Monoid ist.*

*(ii) Ein Ring mit Eins (oder unitärer Ring) ist ein Ring mit einem Einselement $1\in R$, so dass $1\cdot x = x\cdot 1 = x$ für alle $x\in R$ gilt.*

*(iii) Ein Ring $(R,+,\cdot)$ heißt kommutativ , wenn das Monoid $(R,\cdot)$ abelsch ist, also für alle $x,y\in R$ die Gleichung $x\cdot y = y\cdot x$ gilt.*

*(iv) Sind $R,S$ Ringe, so ist ein Ringhomomorphismus $f: R\to S$ eine Abbildung $f: R\to S$, die sowohl die Struktur einer abelschen Gruppe als auch die eines Monoids auf $R$ und $S$ respektiert:*

$$f(x+y) = f(x)+f(y) \quad \text{und} \quad f(xy) \;=\; f(x)\; f(y) \quad \text{für alle } x,y\in R\ .$$

*Im Falle unitärer Ringe fordern wir zusätzlich für Ringmorphismen*

$$f(1_R) \;=\; 1_S\,.$$

*Wir bezeichnen die Menge aller Ringhomomorphismen mit* $\mathrm{Hom}(R,S)$.

Unter einem Ring verstehen wir in dieser Vorlesung grundsätzlich einen assoziativen, nicht unbedingt kommutativen Ring mit Eins.

**Beispiele 1.1.2.**
Wichtige Beispiele für Ringe sind:

1. Der Ring $\mathbb{Z}$ der ganzen Zahlen (und allgemeiner der Ring der ganzen Zahlen in einem algebraischen Zahlkörper).

2. Körper wie die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ oder die komplexen Zahlen $\mathbb{C}$ sind insbesondere (kommutative) Ringe.

3. Für jeden kommutativen Ring $R$ ist der Polynomring $R[X]$ ein Ring; mehr dazu später.

4. Für jeden assoziativen unitären Ring $R$ ist der Ring $\mathrm{Mat}_n(R)$ der $n \times n$-Matrizen mit Einträgen in $R$ ein Ring.

5. Sei $U \subset \mathbb{R}^n$ eine offene Teilmenge. Dann bilden die reellwertigen Funktionen auf $U$ ebenso einen Ring wie die differenzierbaren oder analytischen Funktionen.

6. Der Ring $\mathbb{Z}$ der ganzen Zahlen ist der initiale unitäre Ring: für jeden (unitären) Ring $R$ gibt es genau einen Ringhomomorphismus $f$ von $\mathbb{Z}$ nach $R$, nämlich den durch $f(1) = 1_R$ festgelegten Ringhomomorphismus. In der Tat legt der Wert auf dem Erzeuger $1 \in \mathbb{Z}$ wegen $f(n) = f(\underbrace{1 + \ldots + 1}_{n-\text{mal}}) = \underbrace{f(1) + \ldots + f(1)}_{n-\text{mal}}$ den Ringhomomorphismus eindeutig fest.

7. Der terminale unitäre Ring ist der Nullring $\{0\}$, der einzige unitäre Ring in dem $1 = 0$ gilt. Für jeden Ring $R$ gibt es genau einen Ringhomomorphismus $f: R \to \{0\}$

Wir brauchen auch die Verallgemeinerung von Vektorräumen und linearen Abbildungen. Dabei müssen wir im Fall nicht-kommutativer Ringe etwas genauer sein und drei Begriffe unterscheiden:

***Definition 1.1.3***

*(i) Ein Linksmodul über einem Ring $R$ ist eine abelsche Gruppe $(M, +)$, zusammen mit einer Abbildung*

$$\begin{array}{rlll} \mu: & R \times M & \to & M \\ & (r, m) & \mapsto & \mu(r, m) \equiv r.m \equiv rm\,, \end{array}$$

*der (Skalar-)Multiplikation, so dass für alle $x, y \in R$ und $m, n \in M$ gilt:*

$$\begin{array}{rll} \mu(x, m+n) = \mu(x, m) + \mu(x, n) & \text{bzw.} & x.(m+n) = x.m + x.n \\ \mu(x+y, m) = \mu(x, m) + \mu(y, m) & \text{bzw.} & (x+y).m = x.m + y.m \\ \mu(x, \mu(y, m)) = \mu(xy, m) & \text{bzw.} & x.(y.m) = (x \cdot y).m \end{array}$$

*Die ersten beiden Gleichungen besagen, dass die Skalarmultiplikation bilinear (eigentlich besser: biadditiv) ist. Die dritte Gleichung ist ein gemischtes Assoziativitätsgesetz. Im Falle von Moduln über unitären Ringen fordern wir zusätzlich*

$$\mu(1, m) = m \quad \text{bzw.} \quad 1.m = m$$

*für alle $m \in M$.*

*(ii) Sind $M, N$ Linksmoduln über dem gleichen Ring, so nennt man eine Abbildung $f: M \to N$ einen Modulhomomorphismus, wenn sie mit Addition und Skalarmultiplikation verträglich ist:*

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

*Man nennt eine solche Abbildung auch eine $R$-lineare Abbildung. Ein bijektiver Homomorphismus von Moduln heißt Isomorphismus. Wir bezeichnen mit $\mathrm{Hom}_R(M, N)$ die Menge aller solchen Morphismen.*

*(iii) Ein Rechtsmodul über einem Ring $R$ ist eine abelsche Gruppe $(M, +)$, zusammen mit einer (Skalar-)Multiplikation*

$$\begin{array}{rlll} \mu: & M \times R & \to & M \\ & (m, r) & \mapsto & \mu(m, r) \equiv m.r \equiv mr\,, \end{array}$$

*so dass für alle $x, y \in R$ und $m, n \in M$ gilt:*

$$\begin{aligned} \mu(m+n,x) &= \mu(m,x)+\mu(n,x) \quad \text{d.h.} \quad (m+n).x = m.x+n.x \\ \mu(m,x+y) &= \mu(m,x)+\mu(m,y) \quad \text{d.h.} \quad m.(x+y) = m.x+m.y \\ \mu(m,x\cdot y) &= \mu(\mu(m,x),y) \quad \text{d.h.} \quad m.(x\cdot y) = (m.x).y \end{aligned}$$

*Im Falle unitärer Ringe fordern wir zusätzlich*

$$\mu(m,1) \;=\; m \;\; \text{d.h.} \;\; m.1 = m$$

*für alle $m \in M$.*

(iv) *Seien $R, S$ zwei Ringe, die nicht unbedingt verschieden sein müssen. Ein $R$-$S$-Bimodul ist eine abelsche Gruppe $M$, die sowohl die Struktur eines $R$-Linksmoduls $(M, \mu)$ als auch eines $S$-Rechtsmoduls $(M, \tilde{\mu})$ trägt, so dass die Bedingung*

$$\tilde{\mu}(\mu(\alpha,m),\beta) = \mu(\alpha,\tilde{\mu}(m,\beta))$$

*für alle $m \in M, \alpha \in R, \beta \in S$ erfüllt ist. In anderer Notation:*

$$(\alpha.m).\beta = \;\alpha.(m.\beta)\;.$$

(v) *Morphismen von Rechtsmoduln und von Bimoduln sind analog zu Morphismen von Linksmoduln definiert.*

**Bemerkungen 1.1.4.**
1. Wir vereinbaren die Regel "Punkt vor Strich".

2. Die Ringmultiplikation gibt jedem Ring die Struktur eines Linksmoduls, eines Rechtsmoduls und eines Bimoduls über sich selbst.

3. Ist $R$ ein Körper, so sind die $R$-Linksmoduln gerade die $R$-Vektorräume.

4. Wie bei Vektorräumen zeigt man für alle Ringe $R$ und Linksmoduln $M$

$$0_R m = 0_M \qquad \text{für alle} \quad m \in M$$

und schließt $(-1)m = -m$. Analoge Gleichungen gelten für Rechtsmoduln und Bimoduln.

Lineare Abbildungen bilden selbst wieder einen Vektorraum. Sei nun $R$ ein Ring und seien $M$ und $N$ zwei $R$-Moduln. Die Summe zweier Modulhomomorphismen $\varphi_1, \varphi_2 \in \mathrm{Hom}(M, N)$ erklärt man wie im Fall von Vektorräumen durch die Summe der Bildwerte:

$$(\varphi_1+\varphi_2)(m) := \varphi_1(m)+\varphi_2(m) \quad \text{für alle} \quad m \in M$$

und erhält so die Struktur einer abelschen Gruppe auf der Menge $\mathrm{Hom}(M, N)$. Wir werden daher in der Folge immer $\mathrm{Hom}(M, N)$ als abelsche Gruppe ansehen. Man könnte versucht sein, diese durch die Definition

$$(r.\varphi)(m) := r.\varphi(m) \quad \text{für alle} \quad m \in M$$

zu einem $R$-Modul zu machen. Aber es ist für $\lambda \in R$

$$(r\varphi)(\lambda m) = r\varphi(\lambda m) = r\lambda\varphi(m)$$

und dies müsste gleich

$$\lambda(r.\varphi)(m) = \lambda r\varphi(m)$$

sein, damit auch die Abbildung $r.\varphi$ wieder $R$-linear ist. Ist der Ring $R$ nicht kommutativ, so gilt dies im Allgemeinen nicht. Wir fassen zusammen:

**Satz 1.1.5.**
Sei $R$ ein Ring und $M, N$ seien $R$-Moduln. Dann hat $\mathrm{Hom}_R(M,N)$ stets die Struktur einer abelschen Gruppe. Ist $R$ kommutativ, so ist $\mathrm{Hom}_R(M,N)$ sogar in natürlicher Weise ein $R$-Modul.

Wir machen uns noch einige Gedanken über den Zusammenhang von Linksmoduln und Rechtsmoduln:

**Bemerkungen 1.1.6.**

1. Ist $R$ ein Ring, so bezeichnet $R^{\mathrm{opp}}$ den <u>opponierten Ring</u> : dies ist der Ring mit der gleichen zu Grunde liegenden abelschen Gruppe, aber der Multiplikation
$$(x,y) \mapsto \mu(y,x) \ .$$
Man zeige: jeder $R$-Rechtsmodul $(M,\mu)$ wird durch
$$\begin{array}{llll} \mu^{\mathrm{opp}}: & R^{\mathrm{opp}} \times M & \to & M \\ & (r,m) & \mapsto & m.r := \mu(m,r) \end{array}$$
zum $R^{\mathrm{opp}}$-Linksmodul. Umgekehrt liefert so jeder $R^{\mathrm{opp}}$-Linksmodul einen $R$-Rechtsmodul.

2. Sind $R, S$ Ringe und ist $f : R \to S$ ein Homomorphismus abelscher Gruppen mit der Eigenschaft
$$f(xy) \ = \ f(y)\, f(x) \text{ für alle } x, y \in R\,,$$
so nennt man $f$ einen <u>Antihomomorphismus</u>. Ein Antihomomorphismus ist also ein Homomorphismus von $R^{\mathrm{opp}}$ nach $S$ oder, äquivalenterweise, ein Homomorphismus von $R$ nach $S^{\mathrm{opp}}$. Die Ringe $R$ und $R^{\mathrm{opp}}$ sind also stets anti-isomorph.

3. Ein Ring $R$ ist genau dann kommutativ, wenn die Identität ein Isomorphismus von $R$ nach $R^{\mathrm{opp}}$ ist. Für einen kommutativen Ring $R$ ist wegen Bemerkung 1 jeder $R$-Linksmodul in natürlicher Weise ein $R$-Rechtsmodul und umgekehrt. Jeder $R$-Linksmodul ist sogar ein $R$-Bimodul.

4. Es gibt sehr wohl nicht-kommutative Ringe, die *isomorph* zu ihrem opponierten Ring sind, aber vermittels eines nicht-trivialen Isomorphismus. Als Beispiel betrachte den Ring $M(R, n \times n)$ der quadratischen $n \times n$ Matrizen über einem kommutativen Ring $R$. Dann liefert die Transposition einen Antiisomorphismus, denn sie dreht die Reihenfolge um:
$$(AB)^t = \ B^t \cdot A^t \ .$$

Moduln haben schon per Definition eine Addition; wir betrachten jetzt Moduln über einem kommutativen Ring $R$ mit der zusätzlichen Struktur einer Multiplikation von Modulelementen:

***Definition 1.1.7***

1. *Sei $R$ ein kommutativer Ring. Eine (assoziative) <u>$R$-Algebra</u> ist ein $R$-Modul $A$, der die Struktur eines (assoziativen) Ringes trägt, wobei die Ringaddition und die Moduladdition übereinstimmen und die Verträglichkeitsbedingung*
$$r(xy) \ = (rx)y = x(ry)$$
*für alle $x, y \in A$ und $r \in R$ gilt. Man sagt, die Multiplikation sei $R$-bilinear.*

2. *Eine Algebra $A$ heißt unitär, wenn sie als Ring unitär ist.*

**Bemerkungen 1.1.8.**

1. Zum Beispiel ist für jeden Körper $K$ der Polynomring $K[X]$ eine unitäre $K$-Algebra. Sei $E/K$ eine Körpererweiterung; dann ist $E$ insbesondere eine unitäre $K$-Algebra.

2. Man kann die Definition einer $R$-Algebra $A$ auch so fassen: es gibt einen Ringhomomorphismus $\Phi : R \to A$ mit der Eigenschaft, dass $\Phi(r)a = a\Phi(r)$ für alle $r \in R$ und $a \in A$ gilt.

   Für eine $R$-Algebra $A$ setzen wir $\Phi(r) = r.1_A$ und finden

   $$\Phi(r)a = (r.1_A) \cdot a = r.(1_A \cdot a) \ = r.a = r.(a \cdot 1_A) = a \cdot (r.1_A) = \ a \cdot \Phi(r) \ .$$

   Ist umgekehrt der Ringhomomorphismus $\Phi$ gegeben, so definieren wir eine $R$-Modulstruktur auf dem Ring $A$ durch

   $$r.a := \Phi(r) \cdot a \ ,$$

   die in der Tat $R$-bilinear ist:

   $$r.(ab) = \Phi(r)(ab) = a\Phi(r)b = a(r.b) \ .$$

**Beispiele 1.1.9.**

(i) Jede abelsche Gruppe $(G, +)$ wird zu einem $\mathbb{Z}$-Modul durch die folgende Skalarmultiplikation:

$$\begin{array}{rcl} \mathbb{Z} \times G & \to & G \\ (n,x) & \mapsto & nx = \begin{cases} \underbrace{x + \ldots + x}_{n-\text{mal}} & n > 0 \\ 0 & n = 0 \\ -|n|x & n < 0 \,. \end{cases} \end{array}$$

(ii) Sei $M$ ein $R$-Modul. Dann ist die Abbildung

$$\begin{array}{rcl} M & \to & \mathrm{Hom}_R(R, M) \\ m & \mapsto & (\varphi_m : \ r \mapsto rm) \end{array}$$

ein Isomorphismus von abelschen Gruppen. Ist der Ring $R$ *kommutativ*, so hat auch $\mathrm{Hom}_R(R, M)$ die Struktur eines $R$-Moduls. Dann ist die Abbildung wegen

$$\varphi_{rm}(s) = s.(r.m) = (s \cdot r).m = (r \cdot s).m = r.(s.m) = r\varphi_m(s)$$

sogar ein Isomorphismus von $R$-Moduln. Sein Inverses ordnet einem Homomorphismus $\varphi \in \mathrm{Hom}_R(R, M)$ sein Bild $\varphi(1) \in M$ auf der Eins zu.

Um das Beispiel in 1.1.9 (i) genauer zu untersuchen, überlegen wir uns zunächst folgendes: für jede abelsche Gruppe $(M, +)$ bilden die Gruppenendomorphismen $\mathrm{End}(M)$ einen Ring, den Endomorphismenring. Die Addition in diesem Ring ist die Addition von Abbildungungen durch Addition der Funktionswerte,

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \,.$$

Die Multiplikation im Endomorphismenring ist die Verkettung von Abbildungen, $\varphi\psi := \varphi \circ \psi$, das Einselement ist natürlich die Identität auf $M$. Endomorphismenringe sind im allgemeinen nicht kommutativ.

**Lemma 1.1.10.**
Sei $M$ eine abelsche Gruppe und $R$ ein Ring.

(i) Ist $\varphi : R \to \operatorname{End}(M)$ ein Ringhomomorphismus, so wird durch die Vorschrift

$$r.m := \varphi(r)\,.m$$

$M$ zum $R$-Modul.

(ii) Hat $M$ über die Struktur einer abelschen Gruppe hinaus die Struktur eines $R$-Moduls, so liefert die Abbildung

$$\begin{array}{rccl} \varphi: & R & \to & \operatorname{Abb}(M, M) \\ & r & \mapsto & \varphi(r) \quad \text{mit} \quad \varphi(r)m = rm \end{array}$$

einen Ringhomomorphismus mit Werten in $\operatorname{End}(M)$. Er heißt auch die Strukturabbildung oder Darstellungsabbildung des Moduls $M$.

Da es für jeden (unitären) Ring $E$ nach Beispiel 1.1.2 nur einen (unitären) Ringhomomorphismus $\mathbb{Z} \to E$ gibt, trägt jede abelsche Gruppe nur eine $\mathbb{Z}$-Modulstruktur, nämlich die in Beispiel 1.1.9 (i) angegebene.

Ein weiteres wichtiges Beispiel von Ringen sind Polynomringe und Potenzreihenringe. Wir erinnern:

***Definition 1.1.11***
*Sei $R$ ein kommutativer Ring mit Eins. Ein Paar $(A, X)$, bestehend aus einer $R$-Algebra $A$ mit Eins und einem Element $X \in A$ heißt Polynomring (korrekter wäre: Polynomalgebra) in der Unbestimmten $X$ über $R$, wenn jedes Element $f \in A$ sich* eindeutig *in der Gestalt*

$$f = r_0X^0 + r_1X^1 + \ldots + r_nX^n$$

*mit $r_0, r_1, \ldots, r_n \in R$ darstellen lässt. Hierbei setzen wir $X^0 = 1 \in A$ und verstehen die Eindeutigkeit folgendermaßen: gilt in $A$*

$$r_0 + r_1X^1 + \ldots + r_nX^n = b_0 + b_1X^1 + \ldots + b_mX^m$$

*mit $m \geq n$, so ist $r_i = b_i$ für $0 \leq i \leq n$ und $b_i = 0$ für $i > n$.*

*Man beachte, dass eine Polynomalgebra immer kommutativ ist. Die Elemente einer Polynomalgebra nennen wir auch Polynome.*

Eine Polynomalgebra über $R$ ist also ein Paar, bestehend aus einer $R$-Algebra und einem Element in dieser Algebra, genannt "Unbestimmte".

**Satz 1.1.12.** [Universelle Eigenschaft der Polynomalgebra]
Sei $A$ Polynomring in der Unbestimmten $X$ über $R$. Für jede $R$-Algebra $S$ und jede Wahl eines Elements $s \in S$ gibt es genau einen $R$-Algebrenhomomorphismus $\varphi_s : A \to S$ mit $\varphi_s(X) = s$.

**Beweis.**

- Eindeutigkeit: Da jedes Element $f \in A$ nach Definition des Polynomrings eine eindeutige Darstellung

$$f = \sum_{i=0}^{n} r_iX^i \tag{1}$$

besitzt, folgt sofort, dass

$$\varphi_s(f) = \sum_{i=0}^{n} r_i \varphi_s(X)^i = \sum_{i=0}^{n} r_i s^i \tag{2}$$

gelten muss.

- Existenz: Die so definierte Abbildung $\varphi_s$ ist wegen der Eindeutigkeit der Darstellung von $f$ wohldefiniert. $\varphi_s(X) = s$ ist aus der Definition offensichtlich. Man rechnet leicht nach, dass die so definierte Abbildung $\varphi_s$ ein $R$-Algebrenhomomorphismus ist.

$\square$

**Bemerkungen 1.1.13.**

1. Wegen der Gleichung (2) heißt $\varphi_s$ auch der zu $s \in S$ gehörende Einsetzungshomomorphismus. Man schreibt auch für ein Polynom $f \in A$

$$\varphi_s(f) = f(s) \in S \ .$$

2. Im Spezialfall des Polynomrings selbst, $(S, s) = (A, X)$ ist die Abbildung $\varphi_X$ die Identität. Es folgt die Schreibweise

$$f = \varphi_X(f) = f(X) \ ,$$

die Sie aus der Schule kennen.

3. Im Spezialfall $S = R$ erhalten wir für jedes $\lambda \in R$

$$\varphi_\lambda(f) = f(\lambda) \in R \ .$$

Ein Polynom liefert also eine Funktion $R \to R$. Man hat einen Ringhomomorphismus

$$\begin{array}{ccc} A & \to & \mathrm{Abb}(R, R) \ , \\ f & \mapsto & \tilde{f} \end{array}$$

den Auswertungshomomorphismus. Dieser ist im allgemeinen *nicht* injektiv, d.h. ein Polynom kann nicht mit der induzierten polynomialen Funktion identifiziert werden: zum Beispiel gibt es für den Körper $R = \mathbb{F}_2$ nur 4 verschiedene Funktionen $R \to R$, aber unendlich viele Polynome.

4. Je zwei Polynomringe $A, A'$ in den Unbestimmten $X$ bzw. $X'$ sind isomorph: Nach Satz 1.1.12 gibt es Algebrenhomomorphismen

$$\begin{array}{rcl} \Phi: \ A \to A' & \text{und} & \Psi: \ A' \to A \\ \text{mit} \ \ \Phi(X) = X' & \text{und} & \Psi(X') = X \ . \end{array}$$

Dann sind

$$\Psi \circ \Phi: \ A \to A \ \text{ und } \ \Phi \circ \Psi: \ A' \to A'$$

Algebrenhomomorphismen mit

$$\Psi \circ \Phi(X) = X \ \text{ und } \ \Phi \circ \Psi(X') = X'$$

Aus der Eindeutigkeitsaussage in Satz 1.1.12 folgt

$$\Psi \circ \Phi = \mathrm{id}_A \ \text{ und } \ \Phi \circ \Psi = \mathrm{id}_{A'} \ .$$

Wir haben sogar noch etwas mehr gezeigt: je zwei Polynomringe sind bis auf *eindeutigen* Isomorphismus isomorph.

5. Man muss nun noch zeigen, dass Polynomringe existieren. Eine explizite Konstruktion durch Folgen von Elementen von $R$ wird üblicherweise in der Vorlesung lineare Algebra vorgestellt.

**Beispiel 1.1.14.**
Manchmal betrachtet man auch den kommutativen Ring $R[[X]]$ der formalen Potenzreihen, dessen Elemente die Potenzreihen $\sum_{i=0}^{\infty} r_i X^i$ mit $r_i \in R$ sind. Die Multiplikation ist genauso definiert wie bei Polynomen: man beachte, dass jeder der unendlich vielen Koeffizienten des Produkts durch eine *endliche* Summe ausgedrückt wird. Ein Konvergenzbegriff ist im allgemeinen nicht gegeben. Es gibt auch keinen Auswertehomomorphismus: in eine formale Potenzreihe kann man im allgemeinen nur den Wert $0 \in R$ einsetzen und erhält den Koeffizienten $r_0 \in R$.

**Lemma 1.1.15** (Polynomringe und Endomorphismen)**.**
Sei $K$ ein Körper.

(i) Ist $M$ ein $K[X]$-Modul, so hat $M$ durch Restriktion auf die konstanten Polynome, also durch Pullback entlang der Einbettung $K \hookrightarrow K[X]$ die Struktur eines $K$-Vektorraums. Die Multiplikation mit $X \in K[X]$ ist eine $K$-lineare Abbildung $M \to M$.

(ii) Ist $M$ ein $K$-Vektorraum und $A : M \to M$ eine $K$-lineare Abbildung, so versieht die Vorschrift

$$f.m := f(A)m \qquad \text{für alle} \qquad m \in M, f \in K[X]$$

mit $f(A)$ wie in (1.1.13) erklärt den $K$-Vektorraum $M$ mit der Struktur eines $K[X]$-Moduls.

Moduln über dem Polynomring $K[X]$ über einem Körper sind also gerade $K$-Vektorräume mit einem $K$-linearen Endomorphismus. Es ist klar, wie die Situation sich verallgemeinert, wenn man den Körper $K$ durch einen kommutativen Ring ersetzt.

Dies reduziert die Endomorphismentheorie von Vektorräumen auf die Theorie der Moduln über einem Polynomring. Wichtige Polynome wie das charakteristische Polynom und das Minimalpolynom (oder allgemeiner Invarianten- oder Determinantenteiler) eines Endomorphismus finden in diesem Rahmen eine tiefere Erklärung.

Wir sehen auch, dass der Begriff des Moduls über einem Ring einen einheitlichen Rahmen für den Begriff der abelschen Gruppe und eines Vektorraums mit einem Endomorphismus bietet: beide sind Moduln über Hauptidealringen.

Wir wollen eine weitere wichtige Beispielklasse für Ringe und Moduln einführen:

***Definition 1.1.16***
*Sei $K$ ein kommutativer Ring und $G$ eine Gruppe (oder allgemeiner ein Monoid). Der Gruppenring $K[G]$ (oder allgemeiner Monoidring) ist als abelsche Gruppe die Menge aller Abbildungen*

$$f : G \to K\,,$$

*die nur für endlich viele $g \in G$ von Null verschiedene Werte annehmen. Dann lassen sich die Elemente von $K[G]$ eindeutig als Linearkombination*

$$f = \sum f(g)\delta_g \quad \textit{mit } f(g) \in K$$

*schreiben, wobei $\delta_g$ für die Abbildung steht, die auf $g \in G$ den Wert $1 \in K$ annimmt und auf allen anderen Gruppenelementen verschwindet. Wo dies nicht zu Verwirrung führt, schreiben wir auch kurz $g$ für $\delta_g$, so dass wir z.B. erhalten*

$$f = \sum f(g)g \quad \text{mit } f(g) \in K\,.$$

*Die Multiplikation im Gruppenring ist die Konvolution (oder Faltung):*

$$\left(\sum_{g\in G} a_g g\right) \star \left(\sum_{h\in G} b_h h\right) \quad = \quad \sum_{x\in G}\left(\sum_{g,h\in G, gh=x} a_g b_h\right) x\,.$$

*Man unterscheide diese Multiplikation vom kommutativen Produkt, das von der Multiplikation der Bildwerte in $K$ induziert wird. In dieses Produkt geht nur die Struktur einer Menge auf $G$ ein, bei der Konvolution dagegen die Gruppenmultiplikation: es gilt $\delta_g \star \delta_h = \delta_{gh}$.*

*Man hat einen Ringhomomorphismus*

$$\begin{array}{rcl} K & \hookrightarrow & K[G] \\ a & \mapsto & a\delta_e \ , \end{array}$$

*wobei $e$ das neutrale Element von $G$ ist, und einen Gruppenhomomorphismus*

$$\begin{array}{rcl} G & \to & K[G]^\times \\ g & \mapsto & 1g \equiv 1_K\delta_g \ , \end{array}$$

*der es erlaubt, die Gruppe $G$ als Basis des Gruppenrings $K[G]$ aufzufassen. Gruppenringe sind also Ringe mit einer ausgezeichneten Basis. Es ist klar, dass der Gruppenring $K[G]$ genau dann kommutativ ist, wenn die Gruppe $G$ abelsch ist.*

Oft spricht man über diese Situation auch in einer leicht verschiedenen Sprache:

***Definition 1.1.17***

*Eine Darstellung einer Gruppe $G$ über einem Körper $K$ ist ein Paar $(V, \rho)$, bestehend aus einem $K$-Vektorraum $V$ und einem Gruppenhomomorphismus $\rho$ in die invertierbaren $K$-linearen Abbildungen von $V$,*

$$\rho : G \to \mathrm{GL}(V) := \{\varphi \in \ \mathrm{End}_K(V), \varphi \text{ invertierbar }\}\,.$$

In Anwendungen ist der Vektorraum $V$ z.B. der Raum der Lösungen einer linearen Differentialgleichung oder der Raum der Zustände eines quantenmechanischen Systems. Die Wirkung der Gruppe beschreibt dann die Wirkung von Symmetrien. Ein Ziel der Vorlesung ist es, einen Überblick über solche Gruppenwirkungen für gegebene Gruppe $G$ und endlich-dimensionale Vektorräume $V$ zu bekommen.

**Bemerkung 1.1.18.**

(i) Gegeben eine Darstellung $(V, \rho)$, schreiben wir auch $\rho_V$ für $\rho$.

(ii) Ist $(V, \rho)$ eine Darstellung von $G$ über $K$, so ist die Abbildung

$$\begin{array}{rcl} G \times V & \to & V \\ (g, v) & \mapsto & \rho(g)v \end{array}$$

eine Operation oder Wirkung der Gruppe $G$ auf der dem Vektorraum $V$ zu Grunde liegenden Menge. Die Gruppe wirkt durch lineare Abbildungen.

(iii) Ist $G \times V \to V$ eine Operation der Gruppe $G$ auf einem $K$-Vektorraum $V$, so dass

$$g(v+w) = gv + gw \qquad g(\lambda v) = \lambda gv$$

für alle $v, w \in V, g \in G$ und $\lambda \in K$ gilt, so definiert

$$\rho(g)v = g(v)$$

eine Darstellung $\rho : G \to \mathrm{GL}(V)$.

Eine Darstellung ist also eine "Operation auf einem Vektorraum durch lineare Abbildungen".

(iv) Jeder Vektorraum $V$ trägt eine Darstellung seiner Automorphismengruppe $\mathrm{GL}(V)$ durch $\rho = \mathrm{id}_{\mathrm{GL}(V)}$.

(v) Jeder Vektorraum $V$ wird Darstellung einer beliebigen Gruppe $G$ durch die triviale Operation $\rho(g) = \mathrm{id}_V$ für alle $g \in G$.

(vi) Ist $L/K$ eine Körpererweiterung, so ist $L$, aufgefasst als $K$-Vektorraum eine Darstellung der Galoisgruppe $\mathrm{Gal}(L/K)$ über $K$.

(vii) Eine Darstellung $(V, \rho)$ der Gruppe $\mathbb{Z}$ angeben heißt, einen Automorphismus $A \in \mathrm{GL}(V)$ anzugeben, nämlich $A = \rho(1)$. Dann ist $\rho(n) = A^n$.

(viii) Darstellungen von $\mathbb{Z}/2\mathbb{Z}$ sind äquivalent zu einem Vektorraum $V$ mit einem Automorphismus $A : V \to V$, für den $A^2 = \mathrm{id}_V$ gilt. Konkret heißt dies, wenn die Charakteristik des Körpers $K$ ungleich zwei ist, dass $V$ direkte Summe der Eigenräume von $A$ zu den Eigenwerten $\pm 1$ ist,

$$V = V^+ \oplus V^- .$$

Denn jeder Vektor $v \in V$ lässt sich zerlegen zu

$$v = \frac{1}{2}(v + Av) + \frac{1}{2}(v - Av) \ ;$$

wegen

$$A\frac{1}{2}(v \pm Av) = \frac{1}{2}(Av \pm A^2 v) = \pm\frac{1}{2}(v \pm Av)$$

sind dies Eigenvektoren von $A$ zu den beiden Eigenwerten $\pm 1$.

Hat dagegen der zu Grunde liegende Körper Charakteristik 2, so gibt es nur den Eigenwert 1. Wegen $A^2 = \mathrm{id}_V$ ist das Minimalpolynom von $A$ ein Teiler von $X^2 - 1 = (X-1)^2$. Die Jordan-Blöcke haben daher Größe 1 oder 2. In der Tat gilt für einen Jordan-Block der Größe 2:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

**Lemma 1.1.19.**
Sei $G$ eine Gruppe und $K$ ein Körper. Man erhält eine Bijektion

$$\{ \text{ Darstellungen von } G \text{ über } K\} \xrightarrow{\sim} \{K[G] - \text{Moduln } \} .$$

**Beweis.**
Gegeben eine $K$-lineare $G$-Darstellung $(V, \rho)$, so definieren wir auf der dem Vektorraum $V$ zu Grunde liegenden abelschen Gruppe $(V, +)$ die Struktur eines $K[G]$-Moduls durch die skalare Multiplikation $(\sum_{g \in G} \lambda_g \delta_g).v := \sum_{g \in G} \lambda_g \rho(g)(v)$ für $v \in V$ und $\lambda_g \in K$. Man überprüfe, dass dies einen $K[G]$-Modul definiert.

Umgekehrt liefert ein $K[G]$-Modul $M$ eine abelsche Gruppe, die durch $\lambda m := (\lambda \delta_e).m$ für $m \in M$ und $\lambda \in K$ zum $K$-Vektorraum wird. Für $g \in G$ definieren wir $\rho(g) \in \mathrm{End}_K(V)$ durch $\rho(g)(v) := \lambda_g.v$ für $v \in M$. Man überprüfe, dass dies eine $K$-lineare $G$-Darstellung definiert und dass die beiden Zuordnungen zu einander invers sind. □

Allgemeiner ist für ein Monoid $G$ ein $\mathbb{Z}[G]$-Modul das gleiche wie eine abelsche Gruppe mit einer $G$-Operation durch Gruppenhomomorphismen. Den Beweis überlassen wir als Übung dem Leser.

Auch die Modulhomomorphismen von Moduln über dem Gruppenring $K[G]$ werden in der Sprache von Darstellungen anders benannt.

***Definition 1.1.20***
*Seien $V, W$ Darstellungen einer Gruppe $G$ über einem festen Körper $K$. Ein Homomorphismus von Darstellungen ist eine $K$-lineare Abbildung $f : V \to W$, für die gilt*

$$f(\rho_V(g)v) = \rho_W(g)f(v) \quad \text{für alle } g \in G\,.$$

*Ein Isomorphismus ist ein bijektiver Homomorphismus. Zwei Darstellungen heißen isomorph, wenn es einen Isomorphismus gibt.*

Wir machen weiter in der Theorie der Moduln:

***Definition 1.1.21***
*Sei $M$ ein $R$-Linksmodul und $U \subseteq M$ eine Untergruppe. Dann heißt $U$ Untermodul von $M$, falls die Skalarmultiplikation von $M$ auf $U$ definiert ist, d.h. wenn aus $m \in U$ und $r \in R$ folgt, dass $r.m \in U$ gilt.*

**Bemerkung 1.1.22.**

(i) Die Untergruppen einer abelschen Gruppe sind genau die $\mathbb{Z}$-Untermoduln.

(ii) Fasst man den Ring $R$ als Modul über sich selbst auf, so sind die $R$-Untermoduln von $R$ gerade die Ideale von $R$. Genauer gesagt sind die $R$-Links-Untermoduln die Linksideale, die $R$-Rechts-Untermoduln die Rechtsideale und die $R$-Bi-Untermoduln die beidseitigen Ideale.

(iii) Eine Teilmenge $W \subset V$ einer Darstellung $V$ heißt Unterdarstellung genau dann, wenn $W$ ein unter $G$ stabiler Untervektorraum ist; das heißt, dass aus $g \in G$ und $w \in W$ folgt, dass $gw \in W$. Beschreibt man die Darstellung $(V, \rho)$ als $K[G]$-Modul, so entsprechen die Unterdarstellungen den $K[G]$-Untermoduln.

(iv) Bild und Urbild eines Untermoduls unter einem Modulhomomorphismus sind wieder Untermoduln. Insbesondere sind Bild und Kern eines Modulhomomorphismus Untermoduln.

(v) Ist $U$ ein Untermodul von $M$, so ist $U$ ist als Untergruppe der abelschen Gruppe $M$ Normalteiler, so dass $M/U$ eine abelsche Gruppe ist.

Die Faktorgruppe $M/U$ wird zu einem $R$-Modul, dem Faktormodul oder Quotientenmodul von $M$ nach $U$ durch die folgende Skalarmultiplikation:

$$\begin{array}{rcl} R \times M/U & \to & M/U \\ (\alpha, x+U) & \mapsto & \alpha x + U \end{array}$$

Man rechne hierzu insbesondere nach, dass die Skalarmultiplikation wohldefiniert ist.

(vi) Dies soll durch das folgende Beispiel weiter illustriert werden: Sei $\mathfrak{a}$ ein Linksideal von $R$ und $M$ ein $R$-Modul, so ist

$$\mathfrak{a}M = \left\{ \sum_{\text{endl}} \alpha_i x_i \;\middle|\; \alpha_i \in \mathfrak{a}, x_i \in M \right\}$$

ein Untermodul von $M$: für $r \in R, \alpha \in \mathfrak{a}$ und $x \in M$ ist $r\alpha \in \mathfrak{a}$, da $\mathfrak{a}$ ein Linksideal ist, und somit $r(\alpha m) = (r\alpha)m \in \mathfrak{a}M$. Nach Bemerkung (v) ist dann der Quotient $M/\mathfrak{a}M$ ist ein $R$-Modul.

Ist $\mathfrak{a}$ sogar ein beidseitiges Ideal, so wird $R/\mathfrak{a}$ durch $(a+\mathfrak{a}) \cdot (a'+\mathfrak{a}) := a \cdot a' + \mathfrak{a}$ zu einem Ring. Dann ist auch die Skalarmultiplikation

$$(\alpha + \mathfrak{a})(x + \mathfrak{a}M) = \alpha x + \mathfrak{a}M$$

wohldefiniert und versieht den Quotientenmodul $M/\mathfrak{a}M$ mit der Struktur eines $R/\mathfrak{a}$-Moduls.

Dazu betrachten wir ein konkretes Beispiel: der Ring $\mathbb{Z}$ der ganzen Zahlen ist Modul über sich selbst, also ein $\mathbb{Z}$-Modul; $n\mathbb{Z}$ ist ein beidseitiges Ideal für jedes $n \in \mathbb{Z}$ und die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist ein $\mathbb{Z}$-Modul mit Skalarmultiplikation

$$n.\overline{m} = \overline{nm}$$

und natürlich auch ein $\mathbb{Z}/n\mathbb{Z}$-Modul mit $\overline{n}.\overline{m} = \overline{nm}$.

**Lemma 1.1.23** (Restriktion der Skalare/Pullback)**.**
Ist $\varphi : R \to S$ ein Ringhomomorphismus, so wird jeder $S$-Modul $(M, \mu)$ (insbesondere auch $S$ selbst) ein $R$-Modul durch $\mu \circ (\varphi \times \mathrm{id}_M)$, d.h. durch

$$r.m = \varphi(r).m\,.$$

Diese Operation heißt Restriktion der Skalare, selbst wenn $R$ nicht ein Unterring von $S$ ist, also $\varphi$ nicht injektiv ist. Man nennt auch den $R$-Modul den Pullback des $S$-Moduls $M$ entlang des Ringhomomorphismus $\varphi$.

Anders gesagt: $M$ wird durch einen Morphismus von Ringen $S \to \mathrm{End}(M)$ zu einem $S$-Modul. Dann ist

$$R \xrightarrow{\varphi} S \to \mathrm{End}(M)$$

ein Morphismus von Ringen, der $M$ zu einem $R$-Modul macht. Zum Beispiel sei $\mathfrak{a} \subset R$ ein beidseitiges Ideal von $R$, und $\mathrm{can} :\; R \to R/\mathfrak{a}$, die kanonische Surjektion, dann ist der Quotientenring $R/\mathfrak{a}$ Modul über sich selbst und durch Pullback in natürlicher Weise auch ein $R$-Modul.

**Beispiel 1.1.24.**
Wir verstehen auch so wieder, warum der Quotientenring $\mathbb{Z}/n\mathbb{Z}$ des Rings der ganzen Zahlen ein Modul über sich selbst ist.

***Definition 1.1.25***

*(i) Sei $A \subseteq M$ eine Teilmenge eines $R$-Moduls $M$. Dann bezeichnet*

$$\langle A \rangle = \left\{ \sum_{endl} \alpha_i a_i \;\middle|\; \alpha_i \in R, a_i \in A \right\}$$

*den von der Teilmenge $A$ erzeugten Untermodul von $M$. Es gilt*

$$\langle A \rangle = \bigcap_{\substack{U \subset M \text{ Untermodul} \\ A \subseteq U}} U$$

*d.h. $\langle A \rangle$ ist der kleinste Untermodul von $M$, der $A$ enthält.*

*Denn $\langle A \rangle$ ist ein Untermodul, der $A$ enthält und somit einer der Moduln, über die der Schnitt genommen wird und somit im Schnitt enthalten. Umgekehrt muss jeder Untermodul, über den der Schnitt genommen wird, auch alle Elemente des Untermoduls $\langle A \rangle$ enthalten.*

*(ii) Gilt $\langle A \rangle = M$, so heißt die Menge $A$ Erzeugendensystem des Moduls $M$. $M$ heißt endlich erzeugt, falls es ein endliches Erzeugendensystem gibt.*

*(iii) Ein Modul heißt zyklischer Modul, wenn er ein Erzeugendensystem besitzt, das aus einem Element besteht.*

Man beachte, dass nicht alle Elemente eines zyklischen Moduls auch Erzeuger sein müssen. Man überlege sich zur Übung, dass die zyklischen Gruppen auch wirklich die zyklischen $\mathbb{Z}$-Moduln sind.

**Satz 1.1.26.** (Homomorphiesätze für Moduln)

(i) Seien $M, N$ $R$-Moduln und $f : M \to N$ ein Modulhomomorphismus, so gibt es einen kanonischen Isomorphismus

$$\begin{array}{ccc} M/\ker f & \xrightarrow{\sim} & f(M) \\ x + \ker f & \mapsto & f(x) \end{array}$$

(ii) Sind $U$ und $V$ Untermoduln eines Moduls $M$, so gilt

$$(U+V)/V \quad \xrightarrow{\sim} \quad U/(U \cap V)$$

mit $U + V = \{u + v, u \in U \text{ und } v \in V\}$. Man überlege sich hierzu, dass die Abbildung

$$\begin{array}{ccc} U+V & \to & U/\, U \cap V \\ u+v & \mapsto & u + (U \cap V) \end{array}$$

wohldefiniert ist und bestimme ihren Kern.

(iii) Für jede Kette $U \subseteq V \subseteq M$ von Untermoduln ist $V/U$ Untermodul von $M/U$ und es gilt

$$(M/U)\,/\,(V/U) \quad \xrightarrow{\sim} \quad M/V\,.$$

Der Beweis dieser Sätze geht genauso wie der Beweis der entsprechenden Sätze für Vektorräume.

***Definition 1.1.27***

*(i) Sei $U$ eine Teilmenge eines $R$-Moduls $M$. Dann heißt*

$$\mathrm{Ann}\,(U) = \{\alpha \in R \mid \alpha u = 0 \quad \textit{für alle } u \in U\}$$

*der Annulator der Teilmenge $U$. Dies ist bei einem Linksmodul ein Linksideal von $R$. Den Annulator eines Elementes $x \in M$ bezeichnen wir mit*

$$\mathrm{Ann}(x) = \{\alpha \in R \,|\, \alpha x = 0\}\,.$$

*Es gilt wegen Satz 1.1.26 (i) die Isomorphie von Linksmoduln*

$$\begin{array}{ccc} R/\mathrm{Ann}(x) & \xrightarrow{\sim} & Rx \\ \overline{\alpha} & \mapsto & \alpha x\ . \end{array}$$

*Ist $U$ ein Untermodul, so ist der Annulator sogar ein beidseitiges Ideal.*

*(ii) Ein Modul $M$ heißt treu, falls $\mathrm{Ann}\ M = (0)$ ist. Wir sollten gleich bemerken, dass eine Darstellung auf einem $K$-Vektorraum $V$ treu heißt, wenn der Gruppenhomomorphismus $\rho:\ G \to \mathrm{GL}(V)$ injektiv ist. Ist $V$ als $K[G]$-Modul treu, so ist offenbar die zugehörige Darstellung treu. Denn würde $\rho(g) = \rho(g')$ für $g \neq g'$ gelten, so wäre $g - g'$ im Annulator von $V$. Die Umkehrung gilt allerdings nicht: die eindimensionale Darstellung der zyklischen Gruppe $\mathbb{Z}_2 = \{e, g\}$ mit $\rho(g) = -1$ ist treu als Gruppendarstellung, aber der zugehörige $K[G]$-Modul ist nicht treu, da das Element $e + g \in K[G]$ im Annulator liegt.*

*(iii) Ein Element $x \in M$ heißt Torsionselement, falls $\mathrm{Ann}\ (x) \neq 0$ ist. Mit Tor $M$ wird die Menge aller Torsionselemente des Moduls $M$ bezeichnet, die aber im allgemeinen kein Untermodul ist.*

*(iv) Ein Modul $M$ heißt torsionsfrei, falls Tor $M = (0)$ ist.*

In einem torsionsfreien Modul sind die Annulatoren aller von Null verschiedenen Elemente gleich Null, also insbesondere ist $\mathrm{Ann}(M) = (0)$, so dass torsionsfreie Moduln insbesondere treu sind. Die Umkehrung gilt nicht: zum Beispiel ist der Ring $R = \mathbb{Z}/6\mathbb{Z}$ als Modul über sich selbst treu, da der Ring $R$ unitär ist. Aber das Element $\overline{2}$ liegt im Annulator von $\overline{3}$, so dass $\overline{3}$ ein Torsionselement ist und der Modul Torsion hat.

**Beispiel 1.1.28.**
Über dem Ring $\mathbb{Z}$ der ganzen Zahlen ist der Modul $\mathbb{Z}$ torsionsfrei; der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ dagegen hat nur Torsionselemente.

Ein kommutativer Ring $R$ heißt integer, wenn er keine Nullteiler hat, d.h. wenn für $\alpha, \beta \in R$ aus $\alpha \cdot \beta = 0$ folgt, dass $\alpha = 0$ oder $\beta = 0$ gilt.

**Satz 1.1.29.**
Ist $M$ Modul über einem Integritätsring $R$, so ist Tor $M$ ein Untermodul von $M$ und der Quotientenmodul $M/\mathrm{Tor}\ M$ ist ein torsionsfreier $R$-Modul.

**Beweis.**

- Ist $x \in \operatorname{Tor}(M)$ ein Torsionselement, $\beta \in R$, so finden wir ein von Null verschiedenes $\alpha \in \operatorname{Ann}(x)$. Dann gilt aber $\alpha(\beta x) = (\alpha\beta)x = \beta(\alpha x) = 0$. Damit ist aber auch $\beta x \in \operatorname{Tor} M$.

- Seien nun zwei Torsionselemente vorgegeben, $x, y \in \operatorname{Tor} M$. Wir finden $\alpha, \alpha' \in R \setminus \{0\}$, so dass $\alpha x = \alpha' y = 0$. Dann ist das Produkt $\alpha\alpha' \neq 0$, da $R$ integer sein soll, und es gilt $\alpha\alpha'(x+y) = 0+0 = 0$. Also gilt auch $x+y \in \operatorname{Tor} M$. Somit ist $\operatorname{Tor}(M)$ ein Untermodul.

- Schließlich sei $x + \operatorname{Tor} M \in M/\operatorname{Tor} M$ ein Torsionselement. Wir finden wieder $\alpha \in R \setminus \{0\}$, so dass $\alpha(x + \operatorname{Tor} M) = 0$. Da dann aber $\alpha x \in \operatorname{Tor} M$ liegt, gibt es ein $\beta \in R \setminus \{0\}$ mit $\beta\alpha x = 0$. Da $R$ integer sein sollte, ist auch $\beta\alpha \neq 0$, also $x \in \operatorname{Tor} M$. Also ist der Quotient $M/\operatorname{Tor} M$ torsionsfrei.

□

## 1.2 Operationen auf Moduln, das Tensorprodukt

***Definition 1.2.1***
*Gegeben sei eine Familie $(M_\lambda)_{\lambda\in\Lambda}$ von Moduln über einem Ring $R$. Wir bilden zwei neue $R$-Moduln:*
*das* <u>*Produkt*</u>

$$\prod_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda\}$$

*und die* <u>*direkte Summe*</u>

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda,\ \textit{nur endlich viele } m_\lambda \textit{ sind nicht Null}\}.$$

*Ihre Modulstruktur über $R$ erhalten diese Mengen durch die komponentenweise Addition und die komponentenweise Multiplikation mit Skalaren aus $R$.*

**Bemerkungen 1.2.2.**

(i) Insbesondere ist $R^n = \underbrace{R \oplus \ldots \oplus R}_{n-\text{ mal}}$ für jede natürliche Zahl $n$ ein $R$-Modul.

(ii) Offensichtlich fallen für endliche Familien, $|\Lambda| < \infty$, die Begriffe der direkten Summe und des Produkts zusammen. Wir benutzen dann die Bezeichnungen $\prod_{i=1}^s M_i = M_1 \times M_2 \times \ldots \times M_s$ und $M_1 \oplus M_2 \oplus \ldots \oplus M_s$ ohne Unterschied.

(iii) Beide Begriffe können auch durch universelle Eigenschaften charakterisiert werden. Hierfür führen wir die kanonische

$$\begin{array}{ccc} \text{Injektion} & \text{bzw.} & \text{Surjektion} \\ i_\lambda : M_\lambda \hookrightarrow \bigoplus_{\mu\in\Lambda} M_\mu & & pr_\lambda : \prod_{\mu\in\Lambda} M_\mu \twoheadrightarrow M_\lambda \end{array}$$

ein. Hierbei bildet $\iota_\lambda$ das Element $m \in M_\lambda$ auf das Element in der direkten Summe ab, dessen Einträge außer in der Komponente $\lambda$ alle Null sind. Die Abbildung $pr_\lambda$ projiziert auf die Komponente $\lambda$. Beide Abbildungen sind Homomorphismen von $R$-Moduln.

Die beiden universellen Eigenschaften können nun folgendermaßen formuliert werden: ist $M$ ein beliebiger $R$-Modul, so sind die beiden Abbildungen

$$\begin{array}{rcl} \mathrm{Hom}_R\left(\oplus_{\mu\in\Lambda} M_\mu, M\right) & \longrightarrow & \prod\limits_{\mu\in\Lambda} \mathrm{Hom}_R(M_\mu, M) \\ f & \mapsto & (f \circ i_\mu)_{\mu\in\Lambda} \\ \mathrm{Hom}_R\left(M, \prod\limits_{\mu\in\Lambda} M_\mu\right) & \longrightarrow & \prod\limits_{\mu\in\Lambda} \mathrm{Hom}_R(M, M_\mu) \\ f & \mapsto & (pr_\mu \circ f)_{\mu\in\Lambda} \end{array}$$

Isomorphismen von abelschen Gruppen.

Oder anders formuliert: Eine Familie von Abbildungen von verschiedenen Moduln *in* ein und denselben Modul $M$ kann also *eindeutig* durch eine einzige Abbildung von der direkten Summe der Moduln in $M$ beschrieben werden. Im Fall des direkten Produkts kann eine Familie von Abbildungen *aus* ein und demselben Modul $M$ in verschiedene Moduln durch eine einzige Abbildung aus $M$ in das direkte Produkt eindeutig beschrieben werden.

Man sollte also die direkte Summe und das Produkt nicht als einen Modul (mit gewissen Eigenschaften) betrachten, sondern als einen Modul mit diesen Eigenschaften *zusammen* mit einer Familie von Injektionen bzw. Surjektionen. Dieser Modul mit der Familie von Morphismen ist jeweils durch die universelle Eigenschaft wieder eindeutig bis auf eindeutige Isomorphie festgelegt.

(iv) Gegeben eine Familie $(U_\lambda)_{\lambda\in\Lambda}$ von Untermoduln eines Moduls $M$, bezeichnet man den von ihrer Vereinigung erzeugten Untermodul

$$\sum_{\lambda\in\Lambda} U_\lambda := \langle\ \cup_{\lambda\in\Lambda} U_\lambda\ \rangle$$

von $M$ auch als ihre (innere) <u>Summe</u>.

Jeder Untermodul kommt mit einer Injektion $s_\lambda :\ U_\lambda \to M$; die universelle Eigenschaft der direkten Summe erlaubt es uns, diese Familie von $R$-Modulmorphismen zusammenzufassen in einen natürlichen Morphismus

$$s : \quad \oplus_{\lambda\in\Lambda} U_\lambda \to M$$

Die Summe $\sum_{\lambda\in\Lambda} U_\lambda$ ist dann das Bild des Morphismus $s$. Ist der Homomorphismus $s$ injektiv, so sagen wir, die Summe der Untermoduln sei direkt und schreiben statt $\sum_{\lambda\in\Lambda} U_\lambda$ auch $\oplus_{\lambda\in\Lambda} U_\lambda$ und sprechen von einer <u>inneren direkten Summe</u>. Die Injektivität des Modulmorphismus $s$ heißt natürlich gerade, dass wir jedes Element der inneren direkten Summe in *eindeutiger* Weise als Summe von Elementen der Untermoduln $U_\lambda$ schreiben können.

(v) Gegeben zwei Darstellungen $(V, \rho_V)$ und $(W, \rho_W)$ einer Gruppe $G$ über einem Körper $K$ definieren wir die <u>direkte Summe</u> der Darstellungen als den $K$-Vektorraum $V \oplus W$ mit der Operation $g(v, w) = (\rho_V(g)v, \rho_W(g)w)$. Genauso definiert man direkte Summen und Produkte unendlich vieler Darstellungen. Dies entspricht gerade den direkten Summen der zugehörigen Moduln über dem Gruppenring $K[G]$.

Wir brauchen auch noch den Begriff des Tensorprodukts, der vielleicht im Fall von Vektorräumen aus der linearen Algebra vertraut ist.

***Definition 1.2.3***

*Sei $M$ ein $R^{\text{opp}}$-Modul und $N$ ein $R$-Modul. Das* <u>*Tensorprodukt*</u> *$M \otimes_R N$ ist definiert als die abelsche Gruppe, die von den Paaren $m \otimes n$ mit $m \in M$ und $n \in N$ erzeugt wird modulo der Relationen*

$$\begin{array}{rlll} 0 \otimes n = & m \otimes 0 = 0 & \text{für alle} & m, n \\ (m_1 + m_2) \otimes n = & m_1 \otimes n + m_2 \otimes n & \text{für alle} & m_1, m_2, n \\ m \otimes (n_1 + n_2) = & m \otimes n_1 + m \otimes n_2 & \text{für alle} & m, n_1, n_2 \\ (m.r) \otimes n = & m \otimes (r.n) & \text{für alle} & m \in M, n \in N, r \in R \end{array}$$

**Bemerkungen 1.2.4.**

1. Man beachte, dass $M$ ein Rechtsmodul sein muss, damit die letzte Relation konsistent ist mit den Relationen, die die Modulstrukturen definieren: denn es muss gelten

$$m.(r_1 r_2) \otimes n = (m.r_1).r_2 \otimes n = m.r_1 \otimes r_2.n = m \otimes r_1.(r_2.n) = m \otimes (r_1 \cdot r_2).n \ .$$

2. Im Allgemeinen ist ein Element von $M \otimes_R N$ nicht von der Form $m \otimes n$ mit $m \in M$ und $n \in N$. Vielmehr ist es eine Summe solcher Elemente, also von der Form $\sum_i m_i \otimes n_i$ mit $m_i \in M$ und $n_i \in N$.

**Lemma 1.2.5.**
Sei $R$ ein Ring, $M$ und $M_i$ seien $R^{\text{opp}}$-Moduln und $N$ sei ein $R$-Modul. Dann gibt es ausgezeichnete Isomorphismen:

1. Sei 0 der Nullmodul. Dann gilt: $0 \otimes_R N \cong M \otimes_R 0 \cong 0$.

2. $R \otimes_R N \cong N$ und $M \otimes_R R \cong M$ als Isomorphie abelscher Gruppen.

3. $\oplus_{\lambda\in\Lambda} (M_\lambda \otimes_R N) \cong (\oplus_{\lambda\in\Lambda} M_\lambda) \otimes_R N$ und analog im zweiten Argument.

4. Sei $S$ ein weiterer Ring, $Q$ ein $S$-Modul und $P$ ein $R$-$S$-Bimodul. Dann ist $M \otimes_R P$ auf natürliche Weise ein $S^{\text{opp}}$-Modul und $P \otimes_S Q$ ein $R$-Modul und es gilt die folgende Isomorphie abelscher Gruppen:

$$(M \otimes_R P) \otimes_S Q \cong M \otimes_R (P \otimes_S Q) \ .$$

**Beweis.**
Die erste Identität folgt unmittelbar aus der ersten definierenden Relation des Tensorprodukts.

Für die zweite Identität betrachte man den Morphismus abelscher Gruppen

$$\begin{array}{ccc} M & \to & M \otimes_R R \\ m & \mapsto & m \otimes 1 \end{array} ,$$

der die Umkehrabbildung

$$\begin{array}{ccc} M \otimes_R R & \to & M \\ m \otimes r & \mapsto & m.r \end{array}$$

hat und daher ein Isomorphismus abelscher Gruppen ist.

Die Distributivität sieht man so: nach der universellen Eigenschaft der direkten Summe ist ein Morphismus

$$\Phi : \oplus_{\lambda\in\Lambda} (M_\lambda \otimes_R N) \to (\oplus_{\lambda\in\Lambda} M_\lambda) \otimes_R N$$

durch seine Einschränkung auf $M_\lambda \otimes N$ für jedes $\lambda \in \Lambda$ gegeben. Dort setzen wir auf Erzeugern $\Phi(m_\lambda \otimes n) = \iota_\lambda(m_\lambda) \otimes n$. Um die inverse Abbildung anzugeben, beachten wir, dass in $(\oplus_{\lambda\in\Lambda} M_\lambda) \otimes_R N$ jedes Element von der Form einer endlichen Summe $x = \sum_\lambda \iota_\lambda(m_\lambda) \otimes n_\lambda$ ist. Die Umkehrabbildung $\Psi$ ist dann gegeben durch $\Psi(\iota_\lambda(m_\lambda) \otimes n_\lambda) = \iota_\lambda(m_\lambda \otimes n_\lambda)$.

Die $S^{\mathrm{opp}}$-Modulstruktur auf $M \otimes_R P$ in der letzten Relation ist durch $(m \otimes p).s = m \otimes p.s$ definiert. Analog ist die $R$-Modulstruktur auf $P \otimes_S Q$ definiert. Der Isomorphismus folgt dann aus der auf Erzeugern durch

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

definierten Abbildung. □

**Beispiele 1.2.6.**

(i) Sei $R$ ein Ring und $R^n := R \oplus R \oplus \ldots \oplus R$ die $n$-fache direkte Summe von $R$. Dann gilt

$$R^m \otimes_R R^n \cong R^{mn} .$$

Dies folgt aus dem Distributivgesetz 1.2.5 (iii).

(ii) Ist $R$ ein kommutativer Ring, so gilt für die Polynomringe

$$R[X] \otimes_R R[Y] \cong R[X, Y]$$

wobei $R[X, Y]$ der Ring der Polynome in zwei Variablen ist, hier zunächst erst einmal aufgefasst als abelsche Gruppe. (Übung)

(iii) Sei $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ der $\mathbb{Z}$-Modul der ganzen Zahlen modulo $n$. Wir können ihn sowohl als Bimodul über $\mathbb{Z}$ auffassen. Dann gilt

$$\mathbb{Z}_n \otimes_\mathbb{Z} \mathbb{Z}_m \cong \mathbb{Z}_g$$

wobei $g$ der größte gemeinsame Teiler von $m$ und $n$ ist.

Denn jedes Element im Tensorprodukt lässt sich als endliche Summe

$$x = \overline{a_1} \otimes \overline{b_1} + \ldots + \overline{a_k} \otimes \overline{b_k}$$

mit $a_i, b_i \in \mathbb{Z}$ schreiben. Wegen der $\mathbb{Z}$-Bilinearität des Tensorprodukts ist

$$x = (a_1 b_1 + \ldots + a_k b_k)\,(1_{\mathbb{Z}/n\mathbb{Z}} \otimes 1_{\mathbb{Z}/m\mathbb{Z}}) ;$$

das Tensorprodukt ist also eine zyklische Gruppe. Der Gruppenhomomorphismus

$$\Phi : \begin{array}{ccc} \mathbb{Z}_n \otimes_\mathbb{Z} \mathbb{Z}_m & \to & \mathbb{Z}_g \\ \overline{k} \otimes \overline{l} & \mapsto & \overline{k \cdot l} \end{array}$$

ist wohldefiniert, weil $g = \mathrm{ggT}(m, n)$ ein Teiler von $n$ und $m$ ist. Offenbar ist $\Phi$ ein surjektiver Gruppenhomomorphismus. Ist $\Phi(a(1 \otimes 1)) = 0$, so ist $a$ ein Vielfaches des größten gemeinsamen Teilers $g$. Der euklidische Algorithmus liefert für jedes Vielfache des größten gemeinsamen Teilers $g$ ganze Zahlen $\alpha, \beta \in \mathbb{Z}$ mit $\alpha n + \beta m = a$. Somit gilt in $\mathbb{Z}_n \otimes_\mathbb{Z} \mathbb{Z}_m$

$$a(1 \otimes 1) = \alpha(\overline{n} \otimes 1) + \beta(1 \otimes \overline{m}) = 0$$

also ist der Gruppenhomomorphismus $\Phi$ auch injektiv.

(iv) Tensorieren mit $\mathbb{Q}$ über $\mathbb{Z}$ lässt Torsionselemente einer abelschen Gruppe verschwinden. In der Tat ist $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}$ für jedes $n \in \mathbb{Z}_{>0}$ gleich Null, denn es gilt für alle $i \in \mathbb{Z}$ und $q \in \mathbb{Q}$

$$[i] \otimes q = \ [(in)] \otimes \frac{q}{n} = \ [0] \otimes \frac{q}{n} = 0 \ .$$

Ist umgekehrt ein Element einer abelschen Gruppe kein Torsionselement, so erzeugt es eine Untergruppe isomorph zu $\mathbb{Z}$. Da aber Tensorieren mit $\mathbb{Q}$ Untergruppen in Untergruppen überführt (Beweis später) und $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ nach Lemma 1.2.5 (ii) gilt, verschwindet ein solches Element durch Tensorieren mit $\mathbb{Q}$ nicht.

(v) Das Tensorprodukt ist *nicht* distributiv bezüglich *unendlicher* direkter Produkte: Sei $M := \prod_{n\geq 1} \mathbb{Z}_n$. Einerseits ist nach (iv) $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ und somit gilt für das Produkt $\prod_{n\geq 1}(\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$. Sei andererseits $e \in M$ das Element, das in jeder Komponente den Eintrag 1 hat. Dann ist $e \otimes 1 \neq 0$, denn $e$ hat unendliche Ordnung in der abelschen Gruppe $M$, erzeugt also eine Untergruppe isomorph zu $\mathbb{Z}$. Es gilt aber nach Lemma 1.2.5 (ii), dass $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. Also ist das Tensorprodukt $M \otimes_{\mathbb{Z}} \mathbb{Q}$ nicht Null.

Ist $R$ sogar ein *kommutativer* Ring, so kann man das Tensorprodukt von zwei Linksmoduln $M, N$ erklären, indem man $N$ durch $m.r := r.m$ als $R$-Rechtsmodul auffasst. In diesem Fall trägt das Tensorprodukt nicht nur die Struktur einer abelschen Gruppe, sondern sogar die eines $R$-Moduls:

**Satz 1.2.7.**
Ist $R$ ein *kommutativer* Ring und sind $M, N$ zwei $R$-Moduln, so definiert

$$\mu(r, m \otimes n) \ := (r.m) \otimes n = m \otimes r.n$$

eine $R$-Modulstruktur auf $M \otimes_R \ N$.

Man hat in diesem Fall für je drei $R$-Moduln $M, N, P$ kanonische Isomorphismen

$$\begin{array}{rrcl} a_{M.N.P}: & M \otimes (N \otimes P) & \to & (M \otimes N) \otimes P \\ & m \otimes (n \otimes p) & \mapsto & (m \otimes n) \otimes p \end{array}$$

mit deren Hilfe man die $R$-Moduln $M \otimes (N \otimes P)$ und $(M \otimes N) \otimes P$ identifizieren kann. Das Tensorprodukt ist dann assoziativ.

Den Beweis überlassen wir dem Leser. Man beachte die formale Ähnlichkeit zu Hom, was für einen nicht-kommutativen Ring $R$ auch eine abelsche Gruppe, für einen kommutativen Ring aber einen $R$-Modul liefert.

Wir diskutieren noch die universelle Eigenschaft des Tensorprodukts. Sie involviert, wie im Fall von Vektorräumen, bilineare Abbildungen.

***Definition 1.2.8***
*Sei also $R$ ein Ring, $M$ ein $R^{\mathrm{opp}}$-Modul, $N$ ein $R$-Modul und $T$ eine abelsche Gruppe. Eine Abbildung $f: \ M \times N \to T$ heißt $R$-bilinear, wenn sie die folgenden Eigenschaften erfüllt:*

$$\begin{array}{rll} f(m,0) \ = f(0,n) = 0 & \textit{für alle} & m \in M, n \in N \\ f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n) & \textit{für alle} & m_1, m_2 \in M, n \in N \\ f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2) & \textit{für alle} & m \in M, n_1, n_2 \in N \\ f(m.r, n) = f(m, r.n) & \textit{für alle} & m \in M, n \in N, r \in R \end{array}$$

*Wir bezeichnen mit $\mathrm{Bil}_R(M,N,T)$ die abelsche Gruppe solcher Abbildungen.*

Die Abbildung
$$\begin{array}{rcl} M\times N & \to & M\otimes_R N \\ (m,n) & \mapsto & m\otimes n \end{array}$$
ist per Definition $R$-bilinear.

**Satz 1.2.9** (Universelle Eigenschaft des Tensorprodukts)**.**
Sei $R$ ein Ring, $M$ ein $R^{\text{opp}}$-Modul, $N$ ein $R$-Modul und $T$ eine abelsche Gruppe.

(i) Dann vermittelt die $R$-bilineare Abbildung
$$\begin{array}{rrcl} \otimes : & M\times N & \to & M\otimes N \\ & (m,n) & \mapsto & m\otimes n \end{array}$$
einen Isomorphismus von abelschen Gruppen
$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}}(M\otimes_R N, T) & \to & \mathrm{Bil}_R(M,N,T) \\ \tilde{\phi} & \mapsto & \tilde{\phi}\circ\otimes\ . \end{array}$$
Das heißt, dass jede $R$-bilineare Abbildung $\phi : M\times N \to T$ *eindeutig* durch einen Morphismus abelscher Gruppen $\tilde{\phi} : M\otimes_R N \to T$ beschrieben werden kann. Als kommutierendes Diagramm:
$$\begin{tikzcd} M\times N \arrow[r, "\otimes"] \arrow[dr, "\phi"'] & M\otimes_R N \arrow[d, dotted, "\exists!\tilde{\phi}"] \\ & T \end{tikzcd}$$

(ii) Auf der abelschen Gruppe $\mathrm{Hom}_{\mathbb{Z}}(N,T)$ ist eine natürliche $R^{\text{opp}}$-Modulstruktur definiert durch $(f.r)(n) \ := \ f(r.n)$ für $f : N\to T$, $r\in R$ und $n\in N$. In der Tat gilt
$$f.(r_1\cdot r_2)(n) \ = f((r_1\cdot r_2).n) = f(r_1.(r_2.n)) = (f.r_1)(r_2.n) = ((f.r_1).r_2))(n)$$
für alle $n\in N$.

Analog ist auf der abelschen Gruppe $\mathrm{Hom}_{\mathbb{Z}}(M,T)$ eine natürliche $R$-Linksmodulstruktur definiert durch $(r.g)(m) := g(m.r)$ für $g : M\to T$, $r\in R$ und $m\in M$.

Mit diesen $R$-Modulstrukturen gelten die Isomorphismen von abelschen Gruppen
$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M,T)) \ \cong \mathrm{Hom}_{\mathbb{Z}}(M\otimes_R \ N, T) \cong \mathrm{Hom}_{R^{\text{opp}}}(M, \mathrm{Hom}_{\mathbb{Z}}(N,T))\,.$$

**Beweis.**
Der erste Teil folgt unmittelbar aus der Definition des Tensorprodukts. Den zweiten Teil rechnet man nach. Die letzte Aussage folgt schließlich daraus, dass alle Räume $R$-bilineare Abbildungen $M\times N \to T$ beschreiben. (Übung) □

**Bemerkung 1.2.10.**
Aus der universellen Eigenschaft des Tensorprodukts folgt die folgende Eindeutigkeitsaussage. Sei $T$ eine abelsche Gruppe und $\tau : M\times N \to T$ eine $R$-bilineare Abbildung, so dass jede bilineare Abbildung $\phi : M\times N \to T'$ sich durch Präkomposition mit $\tau$ eindeutig durch einen Homomorphismus abelscher Gruppen $\Phi^\tau : T \to T'$ ausdrücken lässt:
$$\begin{tikzcd} M\times N \arrow[r, "\tau"] \arrow[dr, "\phi"'] & T \arrow[d, dotted, "\exists!\phi^\tau"] \\ & T' \end{tikzcd}$$

Betrachten wir dieses kommutierende Diagramm für $\phi = \otimes$, vertauschen dann die Rollen von $\tau$ und $\otimes$ und hängen die beiden Diagramme aneinander, so erhalten wir das kommutierende Diagramm

$$\begin{tikzcd}
 & T \arrow[d, dotted, "\exists!\Psi_1"] \\
M \times N \arrow[ur, "\tau"] \arrow[r, "\otimes"] \arrow[dr, "\tau"'] & M \otimes_R N \arrow[d, dotted, "\exists!\Psi_2"] \\
 & T
\end{tikzcd}$$

Die vertikale Abbildung $T \to T$ rechts ist wegen der universellen Eigenschaft von $(T, \tau)$ das eindeutige $\Phi^\tau$ für $\Phi = \tau$. Sie leistet dasselbe wie die Identität, muss also gleich der Identität sein, $\Psi_2 \circ \Psi_1 = \mathrm{id}_T$. Durch Vertauschen der Rollen von $\otimes$ und $\tau$ erhält man auch $\Psi_1 \circ \Psi_2 = \mathrm{id}_{M \otimes_R N}$, so dass sowohl $\Psi_1$ und $\Psi_2$ Isomorphismen sind.

Eine wichtige Anwendung der universellen Eigenschaft des Tensorprodukts ist die Definition des Tensorprodukts von Modulmorphismen.

**Betrachtung 1.2.11.**
Sei $R$ ein Ring und sei $M \xrightarrow{\Phi} M'$ ein Morphismus von $R^{\mathrm{opp}}$-Moduln und $N \xrightarrow{\Psi} N'$ ein Morphismus von $R$-Moduln.

Wir betrachten das folgende Diagramm:

$$\begin{tikzcd}
M \times N \arrow[r, "\otimes"'] \arrow[d, "\Phi \times \Psi"] & M \otimes_R N \arrow[d, dotted, "\exists!\ \Phi\otimes\Psi"] \\
M' \times N' \arrow[r, "\otimes"'] & M' \otimes_R N'
\end{tikzcd}$$

Da die Abbildung $\otimes \circ (\Phi \times \Psi)$ offenbar $R$-bilinear ist, existiert nach der universellen Eigenschaft der Tensorprodukts ein eindeutiger Homomorphismus abelscher Gruppen $\Phi \otimes \Psi$, so dass das Diagramm kommutiert. Dieser erfüllt also

$$(\Phi \otimes \Psi)(m \otimes n) = \Phi(m) \otimes \Psi(n) \ .$$

Aus der Bilinearität von $\otimes$ folgt, dass auch das Tensorprodukt von Morphismen $\mathbb{Z}$-bilinear ist:

$$\begin{aligned}
(\Phi_1 + \Phi_2) \otimes \Psi &= \Phi_1 \otimes \Psi + \Phi_2 \otimes \Psi \\
\Phi \otimes (\Psi_1 + \Psi_2) &= \Phi \otimes \Psi_1 + \Phi \otimes \Psi_2
\end{aligned}$$

**Bemerkungen 1.2.12.**

(i) Sind $R, S$ unitäre Ringe, so sind beide insbesondere abelsche Gruppen, also $\mathbb{Z}$-Moduln. Das Tensorprodukt über $\mathbb{Z}$ liefert uns also eine abelsche Gruppe $R \otimes_{\mathbb{Z}} S$. Eine weitere, davon verschiedene, abelsche Gruppe ist das kartesische Produkt $R \times S$. Wir versehen beide Gruppen mit der Struktur eines unitären Ringes:

$$\begin{array}{rrcl}
\text{auf } R \times S & (r,s)(r',s') & := & (rr', ss') \\
\text{auf } R \otimes_{\mathbb{Z}} S & (r \otimes s)(r' \otimes s') & := & (rr') \otimes (ss') \,.
\end{array}$$

(ii) Ist $M$ ein $R$-Modul und $N$ ein $S$-Modul, so ist $M \times N$ durch $(r,s).(m,n) := (r.m, s.n)$ ein $R \times S$-Modul und $M \otimes_{\mathbb{Z}} N$ durch $r \otimes s.m \otimes n := r.m \otimes s.n$ ein $R \otimes_{\mathbb{Z}} S$-Modul.

(iii) Genauso kann man das Produkt von unendlich vielen Ringen definieren. Frage: Warum ist die unendliche direkte Summe von unitären Ringen kein unitärer Ring?

(iv) Wir erwähnen noch die universellen Eigenschaften dieser Konstruktionen:
Das Produkt $\prod_{\lambda\in\Lambda} R_\lambda$ einer beliebigen Familie von Ringen erfüllt, zusammen mit den üblichen Projektionen

$$pr_\lambda : \prod_{\mu\in\Lambda} R_\mu \to R_\lambda$$

die universelle Eigenschaft eines Produkts: für jeden Ring $S$ ist

$$\begin{array}{rcl} \mathrm{Hom}(S, \prod_{\lambda\in\Lambda} R_\lambda) & \to & \prod_{\lambda\in\Lambda} \mathrm{Hom}(S, R_\lambda) \\ f & \mapsto & (pr_\mu \circ f)_{\mu\in\Lambda} \end{array}$$

ein Isomorphismus von Mengen.

(v) Sind $R_1$ und $R_2$ kommutative Ringe, so erfüllt das Tensorprodukt $R_1 \otimes_{\mathbb{Z}} R_2$ zusammen mit den Abbildungen

$$\begin{array}{rrcl} \iota_1 : & R_1 & \to & R_1 \otimes_{\mathbb{Z}} R_2 \\ & r_1 & \mapsto & r_1 \otimes 1 \end{array} \qquad \begin{array}{rrcl} \iota_2 : & R_2 & \to & R_1 \otimes_{\mathbb{Z}} R_2 \\ & r_2 & \mapsto & 1 \otimes r_2 \end{array}$$

die eine universelle Eigenschaft, die vom gleichen Typ ist wie die der direkten Summe von Moduln: für jeden kommutativen Ring $S$ ist die Abbildung

$$\begin{array}{rcl} \mathrm{Hom}(R_1 \otimes_{\mathbb{Z}} R_2, S) & \to & \mathrm{Hom}(R_1, S) \times \mathrm{Hom}(R_2, S) \\ f & \mapsto & (f \circ \iota_1, f \circ \iota_2) \end{array}$$

ein Isomorphismus von Mengen. Man sagt dann, das Tensorprodukt sei ein Koprodukt für die kommutativen unitären Ringe. Beide Eigenschaften kommen als Übung.

## 1.3 Freie Moduln

***Definition 1.3.1***

1. *Eine Familie $(m_\lambda)_{\lambda\in\Lambda}$ von Elementen eines Moduls heißt linear unabhängig oder frei, wenn aus*

$$\sum_{\lambda\in\Lambda} r_\lambda m_\lambda = 0\,,$$

*mit einer Familie $(r_\lambda)_{\lambda\in\Lambda}$ von Elementen aus $R$, in der nur endlich viele Mitglieder von Null verschiedenen sind, folgt, dass $r_\lambda = 0$ für alle $\lambda \in \Lambda$.*

2. *Eine (nicht notwendigerweise endliche) Untermenge $S \subset M$ heißt Basis des Moduls $M$, falls $S$ linear unabhängig ist und $S$ ein Erzeugendensystem von $M$ ist, $\langle S\rangle = M$.*

3. *Ein Modul heißt frei, wenn er eine Basis besitzt.*

**Bemerkung 1.3.2.**

1. Ist $R$ ein Körper und $M$ ein Vektorraum, so ist $M$ frei, denn jeder Vektorraum besitzt eine Basis. Es gibt aber Ringe, über denen Moduln existieren, die nicht frei sind: sei $R = \mathbb{Z}$ und $M = \mathbb{Z}_2$. Wegen $2 \cdot \overline{1} = \overline{0}$ ist $\{\overline{1}\}$ nicht linear unabhängig und wegen $n.\overline{0} = \overline{0}$ für alle $n \in \mathbb{Z}$ ist $\{\overline{0}\}$ kein Erzeugendensystem.

2. Ebenso ist $\mathbb{Z}/5\mathbb{Z}$ kein freier $\mathbb{Z}$-Modul, aber natürlich ein freier $\mathbb{Z}/5\mathbb{Z}$-Modul.

3. Für jede Menge $\Lambda$ ist der Modul

$$R\Lambda := \{f : \Lambda \to R \,|\, f(\lambda) = 0 \text{ für fast alle } \lambda \in \Lambda\}$$

frei, denn die Abbildungen, die an einer Stelle in $\Lambda$ den Wert 1 annehmen und sonst den Wert Null bilden eine ausgezeichnete Basis, die wir mit $\Lambda$ identifizieren können. So kann man $\Lambda$ als Teilmenge von $R\Lambda$ auffassen.

   Man nennt ihn den von der Menge $\Lambda$ erzeugten freien $R$-Modul. Nach unseren Definitionen ist umgekehrt eine Familie $(m_\lambda)_{\lambda\in\Lambda}$ in einem Modul genau dann eine Basis, wenn die Abbildung $R\Lambda \to M$ mit $(r_\lambda) \mapsto \sum r_\lambda m_\lambda$ ein Isomorphismus von Moduln ist.

4. Ein $R$-Modul $M$ ist frei über einer Teilmenge $S \subset M$ genau dann, wenn

$$M \cong \bigoplus_{s\in S} Rs\,.$$

   In diesem Fall bildet $S$ eine Basis des Moduls. Man beachte, dass dann gilt $Rs \cong R$ als $R$-Modul.

   **Beweis.**
   Sei $(s)_{s\in S}$ eine Basis. Die Einbettungen von Untermoduln $Rs \to M$ liefern auf Grund der universellen Eigenschaft der direkten Summe aus Bemerkung 1.2.2(iii) einen Morphismus

$$\bigoplus_{s\in S} Rs \longrightarrow M$$

   von $R$-Moduln. Dieser ist surjektiv, da $\langle S\rangle = M$ gilt, und injektiv, da $S$ linear unabhängig ist. Die Umkehrung ist trivial. □

5. Ist $M$ frei und endlich erzeugt, so gibt es ein $n \in \mathbb{N}$ derart, dass

$$M \cong R^n = \underbrace{R \oplus \ldots \oplus R}_{n-\text{mal}}$$

   Denn sei $M = \langle x_1, \ldots, x_n\rangle$, also $\{x_1, \ldots, x_n\}$ ein endliches Erzeugendensystem und $S$ eine Basis, so ist jeder der endlich vielen Erzeuger $x_i$ eindeutig darstellbar

$$x_i = \sum_{\text{endl.}} \alpha_{ij} s_j \qquad \text{mit} \quad \alpha_{ij} \in R, s_j \in S\,.$$

   Es gibt also eine endliche Teilmenge von $S$, die natürlich immer noch frei ist, und die $M$ erzeugt.

6. Seien endlich viele Moduln $M_1, \ldots, M_m$ und $N_1, \ldots N_n$ über einem Ring $R$ gegeben. Dann folgt aus der universellen Eigenschaft der direkten Summe bzw. des direkten Produkts eine natürliche Identifikation

$$\mathrm{Hom}_R(M_1 \oplus \cdots \oplus M_m, N_1 \oplus \cdots \oplus N_n) \xrightarrow{\sim} \prod_{i=1}^m \mathrm{Hom}_R(M_i, \prod_{j=1}^n N_j) \xrightarrow{\sim} \prod_{i,j} \mathrm{Hom}_R(M_i, N_j)\,.$$

   Schreiben wir also die Elemente der direkten Summe $M_1 \oplus \cdots \oplus M_m$ als Spaltenvektoren, wobei der Eintrag in der $i$-ten Zeile im Modul $M_i$ liegt, so kann man jeden Homomorphismus zwischen den direkten Summen durch eine Matrix beschreiben, deren Einträge

Homomorphismen in $\mathrm{Hom}_R(M_i, N_j)$ sind. Die Komposition der Homomorphismen wird dann durch die Multiplikation der Matrizen beschrieben.

Liegen freie Moduln vor, so kann man die Moduln soweit zerlegen, dass die Matrixeinträge in $\mathrm{Hom}_R(R,R) \cong R$ liegen. Letzte Isomorphie ist durch $\phi \mapsto \phi(1)$ mit Umkehrabbildung $R \ni r \mapsto (\phi(s) := sr)$ gegeben, vergleiche Beispiel 1.1.9.

**Satz 1.3.3.**
Ist $R$ ein *kommutativer* Ring mit 1 und $M$ ein freier $R$-Modul, dann haben je zwei Basen gleiche Mächtigkeit. Diese Mächtigkeit heißt Rang des Moduls $M$. Sie kann, aber muss nicht unbedingt endlich sein. Insbesondere gilt im Falle endlicher Mächtigkeit

$$\mathrm{rang}_R M = n \iff M \cong R^n\,.$$

**Beweis.**
Sei $\mathfrak{m}$ ein maximales Ideal in $R$. Da $R$ kommutativ ist, ist der Quotient $K := R/\mathfrak{m}$ ein Körper, und nach Beispiel 1.1.22 (v) ist der Quotient $M/\mathfrak{m}M$ ein Vektorraum über $K$.

Sei $S$ eine Basis des freien Moduls $M$, also $M \cong \bigoplus_{s\in S} Rs$. Dann folgt $\mathfrak{m}M \cong \bigoplus_{s\in S} \mathfrak{m}s$, und für den Quotienten erhalten wir

$$M/\mathfrak{m}M \cong \bigoplus_{s\in S} K[s]$$

Also gilt $\dim_K(M/\mathfrak{m}M) = |S|$ und die Behauptung folgt aus der aus der linearen Algebra bekannten Tatsache, dass alle Basen eines $K$-Vektorraums gleiche Mächtigkeit haben. □

**Bemerkung 1.3.4.**
Für beliebige Ringe $R$ folgt aus $R^n \cong R^m$ als $R$-Linksmoduln im allgemeinen nicht $n = m$. Das einfachste Gegenbeispiel ist der Nullring; er ist auch der einzige kommutative Ring, der ein Gegenbeispiel liefert.

Wir geben ein interessanteres Gegenbeispiel über einem nicht-kommutativen Ring. Sei $K$ ein beliebiger Körper und $V$ der freie $K$-Vektorraum über der Menge $\mathbb{N}$ der natürlichen Zahlen. Jeder Isomorphismus von Mengen $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ liefert einen Isomorphismus von Vektorräumen $V \xrightarrow{\sim} V \oplus V$. Sei $R := \mathrm{End}_K(V)$. Dann liefert ein solcher Isomorphismus einen Isomorphismus von $R$-Moduln

$$R \;=\; \mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{Hom}_K(V \oplus V, V) \;\cong R \oplus R\;.$$

Wir geben eine Beziehung zwischen einem freien Modul und einem beliebigen Modul:

**Satz 1.3.5.**
Jeder $R$-Modul $M$ ist ein homomorphes Bild eines freien $R$-Moduls.

**Beweis.**
Wir definieren uns einen sehr großen freien Modul mit Basis $M$:

$$F := \bigoplus_{m\in M} R_m \qquad \text{mit } R_m \cong R \quad \text{für alle } m \in M\;.$$

Die Abbildung

$$\begin{aligned} F &\to M \\ (\alpha_m)_{m\in M} &\mapsto \sum_{m\in M} \alpha_m m \end{aligned}$$

ist dann ein surjektiver $R$-Modulhomomorphismus. $\square$

Für den $\mathbb{Z}$-Modul $\mathbb{Z}_5$ würden wir im Beweis des Satzes den Epimorphismus $\mathbb{Z}^5 \to \mathbb{Z}_5$ betrachten. Tatsächlich leistet aber bereits der Modulmorphismus $\mathbb{Z} \to \mathbb{Z}_5$ mit $l \mapsto l \bmod 5$ das Gewünschte.

**Satz 1.3.6.**
Seien $F$ und $M$ jeweils $R$-Moduln und sei der Modul $F$ frei. Sei $f : M \twoheadrightarrow F$ ein Epimorphismus. Dann existiert ein $R$-Modulmorphismus

$$g : F \to M$$

mit $f \circ g = \mathrm{id}_F$, und es gilt $M \cong \ker f \oplus \mathrm{Im}\, g$. Man sagt dann, dass $g$ den Epimorphismus $f$ spaltet.

Bemerkung: Natürlich ist im allgemeinen der Modulmorphismus $g$ nicht eindeutig bestimmt - schon bei Vektorräumen ist die Wahl eines Komplements nicht eindeutig.

**Beweis.**

- Sei $S$ eine Basis von $F$. Wähle ein Urbild $m_s \in f^{-1}(s) \subset M$ für jedes $s \in S$ und definiere

  $$g : F \to M$$

  durch das Bild $m_s$ für den Basisvektor $s \in S$, also

  $$\sum_{s \in S} \alpha_s s \mapsto \sum_{s \in S} \alpha_s m_s \qquad \alpha_s \in R$$

  Da $F$ ein freier Modul ist, ist die Darstellung jedes Elements von $F$ als Linearkombination der $s \in S$ eindeutig. Daher ist die Abbildung $g$ wohldefiniert und ein Homomorphismus von $R$-Moduln. Es gilt dann

  $$f \circ g(s) = f(m_s) = s \quad \text{für alle } s \in S$$

  also $f \circ g = \mathrm{id}_F$.

- Nun benutzen wir $g$, um für jedes $x \in M$ die folgende Zerlegung zu finden:

  $$x = gf(x) + (x - gf(x))\,.$$

  Offenbar liegt $gf(x) \in \mathrm{Im}\, g$, außerdem gilt

  $$f(x - gf(x)) = f(x) - f(x) = 0 \ .$$

  Also haben wir die Darstellung von $M$ als Summe von Untermoduln, $M = \ker f + \mathrm{Im}\, g$. Diese Summe ist direkt: Sei $x \in \ker f \cap \mathrm{Im}\, g$. Dann gilt $x = g(y)$ für ein $y \in F$ und $0 = f(x) = fg(y) = y$, also $y = 0$, woraus $x = 0$ folgt.

$\square$

**Korollar 1.3.7.**
Ist $N$ ein Untermodul von $M$, so dass der Quotientenmodul $M/N$ frei ist, so gibt es einen Untermodul $N'$ von $M$, so dass

$$M = N \oplus N' \quad \text{und} \quad N' \cong M/N$$

gilt. Mit anderen Worten: der Untermodul $N$ hat ein Komplement $N'$ in $M$.

**Beweis.**
Betrachte die kanonische Surjektion $f : M \twoheadrightarrow M/N$, finde mit Satz 1.3.6 einen Modulhomomorphismus $g : M/N \to M$ mit $f \circ g = \mathrm{id}_{M/N}$ und betrachte den Untermodul $N' = g(M/N)$ von $M$. Dann gilt nach Satz 1.3.6, dass $M = N \oplus N'$ und $f(N') = fg(M/N) = M/N$. Also ist die Restriktion $f_{|N'}$ surjektiv. Da außerdem gilt $\ker f|_{N'} = N' \cap N = 0$, ist $f_{|N'}$ ein Isomorphismus des Komplements $N'$ auf den Quotienten $M/N$. □

Man könnte versucht sein, freie Moduln durch die in Satz 1.3.6 beschriebene Eigenschaft zu charakterisieren. Tatsächlich sollte man sie aber durch eine universelle Eigenschaft charakterisieren, die wir in den Übungen besprechen. Die in Satz 1.3.6 beschriebene Eigenschaft hat den Vorteil, dass sie nur durch Eigenschaften von Morphismen formuliert werden kann; sie ist "kategoriell". Aber sie charakterisiert freie Moduln nicht, es gibt Moduln, die diese Eigenschaft haben ohne frei zu sein. Sie bilden die wichtige Klasse der projektiven Moduln, die Gegenstand des nächsten Unterkapitels sind.

## 1.4 Projektive, flache, teilbare und injektive Moduln

Kann man nun hoffen, Moduln, die nicht frei sind, durch freie Moduln zu verstehen? Wir wissen aus Bemerkung 1.3.2, dass der $\mathbb{Z}$-Modul $\mathbb{Z}_2$ nicht frei ist. Er ist aber Quotien des freien Moduls $\mathbb{Z}$ unter $\pi : \mathbb{Z} \to \mathbb{Z}_2$ mit $l \mapsto \bar{l}$. Der Kern von $\pi$ ist der Untermodul $2\mathbb{Z} \subset \mathbb{Z}$, der seinerseits wieder ein freier Modul ist. Also lässt sich der Modul $\mathbb{Z}_2$ als Quotient von freien Moduln schreiben. Tatsächlich brauchen wir eine etwas allgemeiner Begriffsbildung:

***Definition 1.4.1***
*Sei $R$ ein Ring. Eine Folge von $R$-Moduln und Modulmorphismen*

$$\ldots \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0 \xrightarrow{f_{-1}} M_{-1} \ldots$$

*nennen wir eine Sequenz. Eine Sequenz heißt $R$-Kettenkomplex, falls $f_i \circ f_{i+1} = 0$ für alle $i$ gilt. Eine Sequenz heißt exakt, falls $\ker(f_i) = \mathrm{Im}\,(f_{i+1})$ für alle $i$ gilt.*

**Bemerkungen 1.4.2.**

(i) Die Kettenkomplexbedingung lässt sich auch umformulieren als $\mathrm{Im}\,(f_{i+1}) \subseteq \ker(f_i)$.

(ii) Analog lassen sich endliche oder halb-unendliche Sequenzen definieren; Exaktheit wird dann nur dort gefordert, wo sie definierbar ist. Zum Beispiel ist jede 2-teilige Sequenz $M \to N$ exakt, weil es keine zusammensetzbaren Morphismen in ihr gibt.

(iii) In einem Kettenkomplex $(M_n, f_n)$ nennt man $f_n$ üblicherweise das Differenzial und verwendet den Buchstaben d. Für einen Kettenkomplex schreibt man auch $M_\bullet$, wobei der schwarze Punkt andeutet, dass es sich um einen $\mathbb{Z}$-graduierten Kettenkomplex handelt.

(iv) Von besonderem Interesse in der homologischen Algebra sind die kurzen exakten Sequenzen. Diese sind von der Form

$$0 \to M' \xrightarrow{\iota} M \xrightarrow{p} M'' \to 0 \;.$$

Die Exaktheit bei $M'$ heißt, dass $\iota$ injektiv ist. Die Exaktheit bei $M''$ heißt, dass $p$ surjektiv ist. Die Exaktheit bei $M$ kann äquivalent auch durch die beiden folgenden Isomorphien ausgedrückt werden:

$$M' \cong \mathrm{Im}\,\iota = \ker p \text{ bzw. } M'' \cong M/\ker p = M/\mathrm{Im}\,\iota = \mathrm{coker}\iota \;.$$

(v) Für jedes $n \in \mathbb{N}$ liefert die Abbildung $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ mit $x \mapsto nx$ einen injektiven Homomorphismus abelscher Gruppen. Dann ist die Sequenz abelscher Gruppen

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

exakt und erlaubt es, die zyklische Gruppe $\mathbb{Z}_n$ durch einen Homomorphismus zwischen abelschen Gruppen auszudrücken.

(vi) Kettenkomplexe treten in (fast) allen Gebieten der Mathematik auf. Aus der Differentialgeometrie ist für eine glatte Mannigfaltigkeit $X$ der Kettenkomplex $\Omega^\bullet(X)$ der glatten Differentialformen, der sogenannte de Rham Komplex, bekannt. In der Tat bilden die $p$-Formen $\Omega^p(X)$ einen Modul über dem Ring $C^\infty(X)$ der glatten Funktionen auf $X$. Das Differential ist in diesem Fall die äußere Ableitung. Exaktheit des de Rham-Komplexes heißt in diesem Fall, dass alle geschlossenen Differentialformen auch exakt sind. In der algebraischen Topologie wird einem topologischen Raum ein Kettenkomplex abelscher Gruppen als Invariante zugeordnet.

**Satz 1.4.3.**
Sei $0 \to M' \xrightarrow{\iota} M \xrightarrow{p} M'' \to 0$ eine exakte Sequenz. Dann sind die folgenden Eigenschaften äquivalent:

1. Die Injektion $\iota$ hat eine Retraktion, d.h. es gibt einen $R$-Modulmorphismus $\pi : M \to M'$ mit der Eigenschaft $\pi \circ \iota = \mathrm{id}_{M'}$.

2. Die Surjektion $p$ hat einen Schnitt, d.h. es gibt einen $R$-Modulmorphismus $s : M'' \to M$ mit der Eigenschaft $p \circ s = \mathrm{id}_{M''}$.

3. Es gibt einen Isomorphismus $\phi : M \to M' \oplus M''$ von $R$-Moduln, so dass $\phi \circ \iota = \iota_1$ und $pr_2 \circ \phi = p$ gilt.

Der Beweis kommt als Übungsaufgabe. Um die letzte Bedingung besser zu verstehen, betrachten wir das kommutative Diagramm

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\iota"] \arrow[d, equal] & M \arrow[r, "p"] \arrow[d, "\phi"] & M'' \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M' \arrow[r, "\iota_1"] & M' \oplus M'' \arrow[r, "pr_2"] & M'' \arrow[r] & 0
\end{tikzcd}$$

bei dem in der unteren Zeile die Injektion $\iota_1$ von $M'$ in die direkte Summe und die Surjektion $pr_2$ auf $M''$ des direkten Produkts steht. Man hat also in einem Sinn, den wir später noch präziser machen werden, eine Isomorphie exakter Sequenzen vorliegen.

***Definition 1.4.4***
*Von einer exakte Sequenz, die eine der drei äquivalenten Eigenschaften aus Satz 1.4.3 erfüllt, sagen wir, sie spaltet oder zerfällt. (Englisch: splits).*

**Beispiele 1.4.5.**

1. Exakte Sequenzen von Vektorräumen spalten immer, denn jeder Untervektorraum hat nach Korollar 1.3.7 ein Komplement.

2. Die exakte Sequenz von $\mathbb{Z}$-Moduln $0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0$ spaltet nicht, denn sonst wäre $\mathbb{Z}_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Freie Moduln sind für die homologische Algebra zu speziell; insbesondere können sie nicht rein kategoriell charakterisiert werden. Wir brauchen eine Vorüberlegung:

**Lemma 1.4.6.**
Sei $M$ ein $R$-Modul und

$$0 \to T' \xrightarrow{\iota} T \xrightarrow{\pi} T'' \to 0$$

eine kurze exakte Sequenz von $R$-Moduln. Dann ist auch die Sequenz von abelschen Gruppen

$$0 \to \mathrm{Hom}_R(M, T') \xrightarrow{\iota_*} \mathrm{Hom}_R(M, T) \xrightarrow{\pi_*} \mathrm{Hom}_R(M, T'')$$

exakt. Hierbei ist zum Beispiel die von $T' \xrightarrow{\iota} T$ durch Postkomposition induzierte Abbildung

$$\begin{array}{rrcl} \iota_* : & \mathrm{Hom}_R(M, T') & \to & \mathrm{Hom}_R(M, T) \\ & \phi & \mapsto & \iota \circ \phi \end{array}$$

**Beweis.**
Da $\iota : T' \to T$ injektiv ist, folgt aus $\iota_*(\phi) \stackrel{\text{def}}{=} \iota \circ \phi = \iota \circ \phi' \stackrel{\text{def}}{=} \iota_*(\phi')$, dass $\phi = \phi'$, also die Injektivität von $\iota_*$.

Liegt $\phi \in \mathrm{Hom}(M, T)$ im Bild von $\iota_*$, so gibt es $\phi' \in \mathrm{Hom}(M, T')$ mit $\phi = \iota_* \phi' = \iota \circ \phi'$. Daraus folgt aber $\pi_*(\phi) = \pi \circ \phi = \pi \circ \iota \circ \phi' = 0$, also $\phi \in \ker \pi_*$.

Sei schließlich $f \in \ker \pi_*$, also $\pi_* f(m) = \pi \circ f(m) = 0$ für alle $m \in M$. Dann ist für jedes $m \in M$ also $f(m) \in \ker \pi = \mathrm{Im}\, \iota$. Finde also für jedes $m \in M$ ein $\phi'(m) \in T'$ mit $\iota \circ \phi'(m) = f(m)$. Da $\iota$ injektiv ist, dieses Element von $T'$ sogar eindeutig bestimmt, und daher ist auch $\phi'$ ein Modulmorphismus. Also $\iota_* \phi' = f$, und $f \in \mathrm{Im}\, \iota_*$. $\square$

Wenn $\pi : T \to T''$ ein surjektiver Morphismus von Moduln ist, so ist $\pi_* : \mathrm{Hom}_R(M, T) \to \mathrm{Hom}_R(M, T'')$ nicht unbedingt ein surjektiver Morphismus abelscher Gruppen. Zum Beispiel ist $\mathbb{Z} \to \mathbb{Z}_n$ surjektiv, aber der induzierte Morphismus

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = 0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n) \cong \mathbb{Z}_n$$

ist offensichtlich nicht surjektiv.

Wir verallgemeinern nun freie Moduln zu projektiven Moduln, die durch den folgenden Satz charakterisiert werden:

**Satz 1.4.7.**
Die folgenden Aussagen über einen $R$-Modul $M$ sind äquivalent:

1. Für jedes Diagramm

$$\begin{tikzcd} & M \arrow[dl, dotted] \arrow[d] & \\ N_1 \arrow[r] & N_2 \arrow[r] & 0 \end{tikzcd}$$

   mit exakter Zeile gibt es eine Hochhebung (gepunktet gekennzeichnet), so dass das Diagramm kommutiert. (Die Hochhebung ist i.a. nicht eindeutig.)

2. Es gibt einen $R$-Modul $N$, so dass der Modul $M \oplus N$ ein freier Modul ist.

3. Jede kurze exakte Sequenz der Form
$$0 \to N' \to N \to M \to 0$$
spaltet.

4. Für jede kurze exakte Sequenz von $R$-Moduln
$$0 \to T' \to T \to T'' \to 0$$
ist auch die induzierte Sequenz von abelschen Gruppen
$$0 \to \mathrm{Hom}_R(M, T') \to \mathrm{Hom}_R(M, T) \to \mathrm{Hom}_R(M, T'') \to 0$$
exakt.

Die Formulierung dieses Satzes illustriert, dass man es in der homologischen Algebra gern vermeidet, Morphismen Namen zu geben. Man mache sich klar, dass zwar jeder Vektorraum über einem Körper, aber nicht jeder Modul diese Eigenschaften hat. Als Beispiel betrachten wir den $\mathbb{Z}$-Modul $M = \mathbb{Z}_2$.

1. Es gibt keine Hochhebung der Identität auf $M$
$$\begin{tikzcd} & \mathbb{Z}_2 \arrow[dl, dotted] \arrow[d, "\mathrm{id}"] & \\ \mathbb{Z} \arrow[r] & \mathbb{Z}_2 \arrow[r] & 0 \end{tikzcd},$$
denn der einzige Gruppenhomomorphismus $\mathbb{Z}_2 \to \mathbb{Z}$ ist der Nullmorphismus.

2. Es gibt keinen $\mathbb{Z}$-Modul der Form $M \oplus \mathbb{Z}_2$, der frei ist. Denn schon die Elemente von $\mathbb{Z}_2 \subset M \oplus \mathbb{Z}_2$ haben Torsion. Ein freier $\mathbb{Z}$-Modul ist aber von der Form $\oplus_{i \in I}\mathbb{Z}$ und hat daher keine Torsionselemente.

3. Die exakte Sequenz
$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0$$
mit eindeutigen von Null verschiedenen Gruppenhomomorphismen spaltet nicht.

4. Für die exakte Sequenz
$$0 \to \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z} \to \mathbb{Z}_2 \to 0$$
ist wegen $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) = 0$ die Sequenz $0 \to 0 \to 0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_2 \to 0$ nicht exakt.

**Beweis.**

1⇒ 3 Die Spaltung der Sequenz $0 \to N' \to N \to M \to 0$ ist gegeben durch die Hochhebung in dem Diagramm für die Identität
$$\begin{tikzcd} & M \arrow[dl, dotted] \arrow[d, "\mathrm{id}_M"] & \\ N \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

3⇒ 2 Für jeden $R$-Modul $M$ gibt es nach Satz 1.3.5 einen surjektiven $R$-Modulmorphismus von einem freien Modul $F$, zum Beispiel $F := \oplus_{m\in M} R$. Sei $F \to M$ eine solche Surjektion mit Kern $N'$. Da die exakte Sequenz $0 \to N' \to F \to M \to 0$ spaltet, gilt nach Satz 1.4.3 $F \cong M \oplus N'$ mit dem freien Modul $F$.

2⇒ 4 Zunächst beobachtet man, dass Aussage (4) immer gilt, wenn $M$ frei ist, denn dann ist $\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_R(\oplus_{i\in I} R, N) \cong \prod_{i\in I} N$ für jeden Modul $N$, wobei $I$ eine Basis des freien Moduls $M$ indiziert. Die Abbildungen sind einfach die gegebenen Abbildungen, angewandt auf jede Komponente.

Ist $M$ nun direkter Summand eines freien Moduls, ist also $M \oplus N$ frei, so ist daher die Sequenz

$$0 \to \mathrm{Hom}_R(M \oplus N, T') \to \mathrm{Hom}_R(M \oplus N, T) \to \mathrm{Hom}_R(M \oplus N, T'') \to 0$$

exakt. Nach der universellen Eigenschaft der direkten Summe aus 1.2.2(iii) ist diese exakte Sequenz aber gliedweise isomorph zu

$$\begin{aligned} &0 \to \mathrm{Hom}_R(M, T') \times \mathrm{Hom}_R(N, T') \to \mathrm{Hom}_R(M, T) \times \mathrm{Hom}_R(N, T) \\ &\to \mathrm{Hom}_R(M, T'') \times \mathrm{Hom}_R(N, T'') \to 0 \ . \end{aligned}$$

Da der Kern eines Produkts von Abbildungen das Produkt der Kerne der einzelnen Abbildungen ist, und da das Bild eines Produkts von Abbildungen das Produkt der Bilder ist, folgt daraus die Exaktheit der Sequenz in 4.

4⇒ 1 folgt, indem wir die Surjektivität des Morphismus $N_1 \to N_2$ ausnützen, um eine exakte Sequenz

$$0 \to \ker((N_1 \to N_2)) \to N_1 \to N_2 \to 0$$

zu bekommen. Dann liefert 4 die exakte Sequenz

$$0 \to \mathrm{Hom}_R(M, \ker(N_1 \to N_2)) \to \mathrm{Hom}_R(M, N_1) \to \mathrm{Hom}_R(M, N_2) \to 0$$

deren Surjektivitätsaussage genau Aussage 1 ist.

□

***Definition 1.4.8***
*Ein $R$-Modul, der eine der vier äquivalenten Eigenschaften aus Satz 1.4.7 erfüllt, heißt projektiver Modul.*

**Beispiele 1.4.9.**

1. Freie Moduln sind wegen des Kriteriums aus Satz 1.4.7 (2) projektiv. Für $R = \mathbb{Z}$ ist jeder projektive Modul frei, denn, wie wir später in Satz 3.1.1 sehen werden, sind Untermoduln von freien $\mathbb{Z}$-Moduln frei, und insbesondere sind alle direkten Summanden freier Moduln ihrerseits frei. Das gleiche gilt, wie wir auch später sehen werden, für jeden Hauptidealring $R$.

2. Für $R = R_1 \times R_2$ mit $R_2$ nicht dem Nullring ist der $R$-Modul $M = R_1$ mit $(r_1, r_2).m = r_1 \cdot m$ als direkter Summand in $R_1 \oplus R_2 = R$ projektiv, aber offensichtlich nicht frei: wegen $(0, r_2).m = 0$ für alle $r_2 \in R_2$ ist jedes Element von $M$ linear abhängig. Es gibt also gar keine linear unabhängigen Familien. Allerdings ist der Ring $R = R_1 \times R_2$ nicht nullteilerfrei.

3. Beispiele für projektive, nicht freie Moduln über nullteilerfreien Ringen $R$ erfordern etwas Zahlentheorie oder algebraische Geometrie:

   Sei $\tau := \sqrt{-5}$; betrachte den kommutativen Ring $R = \mathbb{Z}[\tau]$. Sei $M$ das von 2 und $1+\tau$ erzeugte Ideal von $R$, aufgefasst als $R$-Modul. Zunächst zeigen wir, dass der $R$-Modul $M$ nicht frei ist. Angenommen, $M$ wäre frei. Wie bei Vektorräumen ist der Rang eines freien Moduls eine untere Schranke für die Mächtigkeit eines Erzeugendensystems. (Dies sieht man z.B. indem man wie im Beweis von Satz 1.3.3 modulo einem maximalen Ideal rechnet.) Daher kann der Rang von $M$ höchstens zwei sein. Der Rang von $M$ kann aber nicht gleich 2 sein, denn in diesem Fall müssten 2 und $1+\tau$ linear unabhängig über $R$ sein, was wegen der Gleichung $3 \cdot 2 + (\tau - 1)(1+\tau) = 0$ aber nicht zutrifft.

   Also ist der Modul $M$ genau dann frei, wenn er ein Hauptideal von $R$ ist, also $M = (a)$ für ein $a \in R$ mit $a|2$ und $a|1+\tau$. Wir zeigen, dass 2 unzerlegbar im Ring $R$ ist. Dazu definiere die Normabbildung $N : R \to \mathbb{Z}$ durch $N(x + \tau y) = x^2 + 5y^2$. Die Norm ist multiplikativ, $N(a \cdot b) = N(a) \cdot N(b)$, daher $N(a)|N(2) = 4$. Also muss $N(a) = 2$ gelten. Aber für $a = x + \tau y$ ist $N(a) = x^2 + 5y^2 = 2$ unlösbar mit $x, y \in \mathbb{Z}$. Also ist der Modul nicht frei.

   Um zu zeigen, dass der Modul $M$ dennoch projektiv ist, betrachten wir die durch das Erzeugendensystem $(2, 1+\tau)$ gegebene Surjektion

   $$\begin{array}{rccl} p: & R \oplus R & \to & M \\ & (r_1, r_2) & \mapsto & r_1 2 + r_2(1+\tau) \ . \end{array}$$

   Dieser Epimorphismus hat den Schnitt:

   $$s(2x + (1+\tau)y) = (-2x - (1+\tau)y, (1-\tau)x + 3y).$$

   Also ist nach Satz 1.4.3 der Modul $M$ ein direkter Summand im freien Modul $R \oplus R$. Daher ist er nach Satz 1.4.7 projektiv.

4. Sei $X$ eine glatte Mannigfaltigkeit und $E \to X$ ein glattes Vektorbündel von endlichem Rang. Der Raum der glatten Schnitte $\Gamma(X, E)$ ist dann ein Modul über dem Ring $C^\infty(X)$ der glatten Funktionen auf $X$. Ist die Mannigfaltigkeit $X$ kompakt, so ist der Modul $\Gamma(X, E)$ projektiv. Das Serre-Swann Theorem sagt, dass dann endlich-erzeugte projektive $C^\infty(X)$-Moduln in Bijektion zu Vektorbündeln von endlichem Rang sind.

**Satz 1.4.10.**
Sei $M$ ein $R^{\mathrm{opp}}$-Modul und $0 \to N' \xrightarrow{\iota} N \xrightarrow{p} N'' \to 0$ eine kurze exakte Sequenz von $R$-Moduln.

1. Dann ist für jeden $R$-Modul die Sequenz abelscher Gruppen

   $$M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes \iota} M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes p} M \otimes_R N'' \to 0$$

   exakt.

2. Falls $M$ projektiv ist, so ist sogar die Sequenz

   $$0 \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$$

   exakt.

Man vergleiche die erste Aussage mit der Aussage in Lemma 1.4.6 für Hom.

Um zu sehen, warum bei Satz 1.4.10 keine stärkere Aussage steht, beachte, dass für jede abelsche Gruppe $A$ gilt $A \otimes_{\mathbb{Z}} \cong A/nA$. Somit ist $\mathbb{Z} \otimes \mathbb{Z}_2 \cong \mathbb{Z}_2$, aber $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Q}/2\mathbb{Q} \cong 0$. Tensoriert man

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

mit $\mathbb{Z}_2$, so erhält man $0 \to \mathbb{Z}_2 \to 0 \to 0 \to 0$, was offensichtlich nicht exakt ist.

**Beweis.**

- Für den ersten Teil muss die Exaktheit bei $M \otimes_R N''$ und bei $M \otimes_R N$ gezeigt werden. Sei $x = \sum m_i \otimes n_i'' \in M \otimes_R N''$. Da $N \to N''$ surjektiv ist, gibt es Urbilder $n_i \in N$. Dann wird das Element $\sum m_i \otimes n_i$ unter $M \otimes_R N \to M \otimes_R N'$ auf $x$ abgebildet, womit die Surjektivität gezeigt ist.

  Für die Exaktheit an der Stelle $M \otimes_R N$ betrachten wir

  $$Q := \mathrm{coker}(M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes \iota} M \otimes_R N) \equiv (M \otimes_R N)/\mathrm{Im}\,(M \otimes_R N' \to M \otimes_R N)\,.$$

  Ebenso haben wir eine Abbildung $M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes p} M \otimes_R N''$ von abelschen Gruppen. Das Bild der Abbildung $\mathrm{id}_M \otimes \iota$ liegt im Kern der Abbildung $\mathrm{id}_M \otimes p$ liegt. Daher faktorisiert diese zu einer natürlichen Abbildung

  $$\begin{array}{rcl} Q & \to & M \otimes_R N'' \\ [m \otimes n] & \mapsto & m \otimes p(n) \end{array}$$

  Wir wollen zeigen, dass diese Abbildung ein Isomorphismus ist, was nach dem Isomorphiesatz bedeutet $\mathrm{Im}\,(M \otimes_R N' \to M \otimes_R N) = \ker(M \otimes_R N \to M \otimes_R N'')$, also Exaktheit.

  Wir konstruieren dazu eine Umkehrabbildung $M \otimes_R N'' \to Q$: um das Bild von $m \otimes n''$ zu finden, wählen wir ein Urbild $n \in N$ von $n''$ und setzen $m \otimes n'' \mapsto [m \otimes n]$. Dies ist wohldefiniert: jede andere Wahl des Urbilds ist von der Form $n+k$ mit $k \in \ker(p) = \mathrm{Im}\,(\iota)$ und liefert daher die gleiche Klasse im Kokern $Q$.

  Die so definierte Abbildung ist ein Isomorphismus, denn die natürliche Abbildung $[m \otimes n] \mapsto m \otimes p(n)$ ist ein wohldefiniertes Inverses.

- Für den zweiten Teil des Satzes bleibt zu zeigen, dass injektive Abbildungen injektiv bleiben, wenn man $M \otimes_R -$ mit einem projektiven Rechtsmodul $M$ anwendet.

  Wir überlegen uns zunächst, dass die Aussage gilt, wenn $M$ nicht nur projektiv, sondern sogar frei ist, $M = \oplus_{i \in I} R$. Wegen der Distributivität von $\otimes_R$ erhalten wir in diesem Fall

  $$\begin{tikzcd} M \otimes_R N' \arrow[r, "\mathrm{id}_M \otimes \iota"] \arrow[d, "\cong"] & M \otimes_R N \arrow[d] \\ \oplus_{i \in I} N' \arrow[r, "\oplus \iota"] & \oplus_{i \in I} N \end{tikzcd}$$

  wobei die Abbildung auf der Komponente für jedes $i \in I$ durch $\iota$ gegeben ist. Hier haben wir verwendet, dass $R \otimes_R N \cong N$ für alle $N$ gilt. Die untere Zeile ist naturlich genau dann injektiv, wenn $\iota : N' \to N$ injektiv war.

Ein projektiver Modul $M$ ist nun nach Satz 1.4.7 direkter Summand eines freien Moduls $F$, also $M \oplus \tilde{M} \cong F$. Wiederum wegen der Distributivität von $\otimes_R$ kommutiert das Diagramm:

$$\begin{tikzcd} F \otimes_R N' \arrow[rr] \arrow[d, "\cong"] & & F \otimes_R N \arrow[d] \\ M \otimes_R N' \oplus \tilde{M} \otimes_R N' \arrow[rr] & & M \otimes_R N \oplus \tilde{M} \otimes_R N \end{tikzcd}$$

wobei die Abbildung als direkte Summe gegeben ist. Somit ist sie auch auf jedem Summanden injektiv.

□

Wir definieren zwei weitere Begriffe für Moduln über einem Ring:

***Definition 1.4.11***

1. *Ein $R$-Modul $M$ heißt <u>flach</u>, falls Tensorieren $- \otimes_R M$ kurze exakte Sequenzen erhält, oder äquivalent, wenn das Tensorprodukt mit $M$ die Injektivität von Abbildungen erhält.*
2. *Ein Modul heißt <u>teilbar</u>, wenn für jedes $0 \neq r \in R$ die Abbildung $M \xrightarrow{r\cdot} M$, die durch Skalarmultiplikation mit $r$ gegeben ist, surjektiv ist.*

**Beispiel 1.4.12.**
Vertauscht man im vorgehenden Satz 1.4.10 die beiden Seiten des Tensorprodukts, so folgt, dass alle projektiven Moduln flach sind. Es gibt aber auch flache Moduln, die nicht projektiv sind:

Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist flach, denn wenn $0 \to M' \to M$ injektiv ist, so ist der Kern der zusammengesetzten Abbildung $M' \to M \to M \otimes_{\mathbb{Z}} \mathbb{Q}$ mit $M \to M \otimes_{\mathbb{Z}} \mathbb{Q}$ gegeben durch $m \mapsto m \otimes 1$, nach Beispiel 1.2.6 (iv) genau die Menge der $m' \in M'$, deren Bild in $M$ ein Torsionselement ist. Wegen der Injektivität von $M' \to M$ kann das nur passieren, wenn $m'$ schon in $M$ ein Torsionselement ist, woraus aber $m' \otimes 1 = 0 \in M' \otimes_Z \mathbb{Q}$ folgt.

Andererseits ist $\mathbb{Q}$ aber nicht projektiv über $\mathbb{Z}$; andernfalls müsste es in einen freien $\mathbb{Z}$-Modul (sogar als direkter Summand) eingebettet werden können, was unmöglich ist, da $\mathbb{Q}$ als $\mathbb{Z}$-Modul teilbar ist, aber freie $\mathbb{Z}$-Moduln nicht teilbar sind.

Dual zur Definition von projektiven Moduln ist der Begriff des injektiven Moduls. Für einen Morphismus $f : T_1 \to T_2$ von $R$-Moduln betrachten wir dabei diesmal die Abbildung durch Präkomposition:

$$\begin{array}{rccc} f^* : & \mathrm{Hom}(T_2, N) & \to & \mathrm{Hom}(T_1, N) \\ & \varphi & \mapsto & \varphi \circ f \end{array}$$

Man beachte, die Reihenfolge von $T_1$ und $T_2$ in den Hom-Räumen! Den Beweis der folgenden Proposition können wir erst nach Sektion 2.4 vervollständigen.

**Satz 1.4.13.**
Die folgenden Aussagen sind äquivalent für einen $R$-Modul $M$:

1. Für jedes Diagramm

$$\begin{tikzcd} 0 \arrow[r] & N_1 \arrow[r] \arrow[d] & N \arrow[dl, dotted] \\ & M & \end{tikzcd}$$

mit exakter Zeile gibt es eine Hochhebung (gepunktet gekennzeichnet), so dass das Diagramm kommutiert.

2. Jede kurze exakte Sequenz
$$0 \to M \to N_1 \to N_2 \to 0$$
zerfällt.

3. Für jede kurze exakte Sequenz von $R$-Moduln
$$0 \to T' \to T \to T'' \to 0$$
ist auch die Sequenz von abelschen Gruppen
$$0 \to \mathrm{Hom}_R(T'', M) \to \mathrm{Hom}_R(T, M) \to \mathrm{Hom}_R(T', M) \to 0$$
exakt.

**Beweis.**
Die Implikation 1. $\Rightarrow$ 2. folgt genau wie die Implikation 1. $\Rightarrow$ 2. im Satz 1.4.7 über projektive Moduln, durch Umkehren der Pfeile. Ebenso folgt hier 3. $\Rightarrow$ 1. wie 4. $\Rightarrow$ 1. im Satz 1.4.7 über projektive Moduln.

Es fehlt aber noch das Analogon der Charakterisierung projektiver Moduln als direkter Summand eines freien Moduls. Wir gehen darauf erst in Abschnitt 2.4 ein, so dass erst danach der Beweis dieses Satzes analog zum Beweis von Satz 1.4.7 vervollständigt werden kann. □

***Definition 1.4.14***
*Ein Modul, der eine der vorstehenden Eigenschaften erfüllt, heißt injektiver Modul.*

**Satz 1.4.15** (Satz von Baer)**.**
Ein $R$-Modul $M$ ist genau dann injektiv, wenn er für jedes Ideal $\mathfrak{p}$ in $R$ und jeden Morphismus $\mathfrak{p} \to M$ von $R$-Linksmoduln die Hochhebungseigenschaft aus Satz 1.4.13 hat:

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{p} \arrow[r] \arrow[d] & R \arrow[dl, dotted] \\ & M & \end{tikzcd}$$

**Beweis.**

- Ist $M$ injektiv, so ist folgt die Hochhebungseigenschaft durch Betrachung der Eigenschaft 1 aus Satz 1.4.13 im Spezialfall der $R$-Moduln $N_1 = \mathfrak{p}$ und $N = R$.

- Die Umkehrung ist für nicht endlich erzeugte Moduln eine Anwendung des Zornschen Lemmas (vgl. Appendix A):

  Sei $0 \to N' \xrightarrow{\iota} N$ ein Monomorphismus von $R$-Moduln und $f : N' \to M$ ein beliebiger Morphismus von $R$-Moduln. Wir müssen im Diagramm

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

einen auf ganz $N$ definierten Morphismus $g$ finden, so dass das Diagramm kommutiert. Wir sagen dann, $g$ setze $f$ vom Untermodul $N'$ auf den größeren Modul $N$ fort. Dazu betrachten wir die Menge aller Fortsetzungen,

$$X = \{(K,g) | N' \subseteq K \subseteq N, g : K \to M \text{ ist Fortsetzung von } f\} \; .$$

Die Menge $X$ enthält die triviale Fortsetzung $(N', f)$, ist also nicht leer. Wir definieren eine partielle Ordnung auf $X$ durch

$$(K,g) \leq (K',g') \overset{\text{def}}{\iff} K \subseteq K' \text{ und } g'|_K = g \, .$$

Man sieht leicht, dass jede total geordnete Teilmenge von $X$ die Vereinigung als obere Schranke hat. Nach dem Zornschen Lemma hat $X$ ein maximales Element $g_0 : K_0 \to M$, und wir müssen zeigen, dass für dieses maximale Element $K_0 = N$ gilt.

Andernfalls finden wir $n \in N \setminus K_0$ und setzen $\mathfrak{p} := \{r \in R | r.n \in K_0\}$. Dieses Ideal ist nicht das Nullideal, denn sonst wäre die innere Summe $K' := K_0 + Rn$ direkt. Dann könnten wir $g_0$ auf $K'$ durch irgend einen Wert in $M$ für $n$ weiter fortsetzen, im Widerspruch zur Maximalität von $K_0$.

Nun betrachten wir den Modulmorphismus $g_0 \circ n : \mathfrak{p} \xrightarrow{.n} K_0 \xrightarrow{g_0} M$. Nach Voraussetzung kann dieser fortgesetzt werden zu einem Modulmorphismus $\tilde{g} : R \to M$. Betrachte nun auf $K' = K_0 + Rn \subset N$ die Fortsetzung $g'(k + rn) = g_0(k) + \tilde{g}(r)$. Man beachte, dass $g'$ deswegen wohldefiniert ist, weil $\tilde{g}$ eine Fortsetzung von $g \circ n$ ist, also auf dem Schnitt $\mathfrak{p} \cong Rn \cap K_0$ mit $g_0$ übereinstimmt. Damit ist aber $(K', g') > (K_0, g_0)$, ein Widerspruch zur Maximalität von $(K_0, g_0)$.

□

**Korollar 1.4.16.**
Ein Modul $M$ über einem Hauptidealring $R$ ist genau dann injektiv, wenn er teilbar ist, d.h. wenn die Multiplikation mit jedem Ringelement $r \in R \setminus \{0\}$ surjektiv ist.

**Beweis.**

- Wir zeigen dazu, dass ein $R$-Modul genau dann teilbar ist, wenn er die Hochhebungseigenschaft aus dem Satz von Baer 1.4.15 hat. Im Hauptidealring $R$ sind alle Ideale von der Form $\mathfrak{p} = (\alpha)$ mit $\alpha \in R$. Betrachte also das Diagramm

$$\begin{tikzcd} 0 \arrow[r] & (\alpha) \arrow[r] \arrow[d, "\phi"'] & R \arrow[dl, dotted, "\tilde{\phi}"] \\ & M & \end{tikzcd}$$

  Dann ist $\phi$ festgelegt durch seinen Wert $\phi(\alpha)$ auf dem Erzeuger $\alpha$ des Hauptideals und ebenso $\tilde{\phi}$ durch seinen Wert auf dem Erzeuger $1 \in R$.

- Ist der Modul $M$ teilbar, so finden wir ein $\tilde{m} \in M$ mit $\alpha.\tilde{m} = \phi(\alpha)$. Wir legen den Morphismus $\tilde{\phi}$ durch den Wert $\tilde{\phi}(1) := \tilde{m}$ auf dem Erzeuger $1 \in R$ fest. Dann gilt für $\alpha$ die Gleichung $\tilde{\phi}(\alpha) = \alpha\tilde{\phi}(1) \;\; = \alpha\tilde{m} = \phi(\alpha)$. Also gilt $\tilde{\phi}|_{(\alpha)} = \phi$. Daher haben teilbare $R$-Moduln die Hochhebungseigenschaft für Ideale und sind nach dem Satz von Baer 1.4.15 injektiv.

- Sei umgekehrt der Modul $M$ injektiv und erfülle somit nach Satz 1.4.13 die Hochhebungseigenschaft. Um zu sehen, dass $M$ teilbar ist, geben wir uns $\alpha \in R \setminus \{0\}$ und $m \in M$ vor und suchen ein $\tilde{m} \in M$ mit $\alpha\tilde{m} = m$. Dazu betrachte das vorstehende Diagramm mit $\phi$ definiert durch $\phi(\alpha) = m$, finde $\tilde{\phi}$ mit der Hochhebungseigenschaft und setze $\tilde{m} := \tilde{\phi}(1) \in M$.

□

Insbesondere ist eine abelsche Gruppe als $\mathbb{Z}$-Modul genau dann injektiv, wenn sie teilbar ist, d.h. wenn die Multiplikation mit $n \in \mathbb{Z} \setminus \{0\}$ surjektiv ist. Beispiele injektiver abelscher Gruppen sind die teilbaren Gruppen $\mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$, Gegenbeispiele sind freie Moduln.

## 1.5 Einfache Moduln und Kompositionsreihen

Wir haben nun schon mit freien, projektiven, injektiven und flachen Moduln mehrere Klassen von Moduln kennengelernt. Wir wollen nun noch zum Abschluss einfache Moduln kennenlernen; vielleicht wider Erwarten ist deren Struktur aber gar nicht "einfach".

***Definition 1.5.1***

1. *Ein Modul $M$ über einem Ring heißt <u>einfach</u>, wenn er nicht Null ist und außer den Untermoduln $M$ und dem Nullmodul keine Untermoduln hat.*

2. *Entsprechend heißt eine Darstellung $V$ einer Gruppe $G$ <u>irreduzibel</u> oder <u>einfach</u>, wenn $V \neq 0$ gilt und $0$ und $V$ die einzigen Unterdarstellungen sind.*

3. *Ein Modul $M$ über einem Ring heißt <u>unzerlegbar</u>, wenn er nicht Null ist und es keine zwei vom Nullmodul verschiedenen Untermoduln $N_1$ und $N_2$ gibt, so dass $M = N_1 \oplus N_2$ gilt.*

4. *Entsprechend heißt eine Darstellung $V$ von $G$ <u>unzerlegbar</u>, wenn $V$ nicht der Nullraum ist und es keine zwei von Null verschiedenen Unterdarstellungen $W_1, W_2 \subset V$ gibt, so dass $V$ die innere direkte Summe ist:*
$$V = W_1 \oplus W_2 \,.$$

**Lemma 1.5.2.**

1. Sei $R$ ein Ring und $M$ ein $R$-Modul. Dann ist $M$ genau dann einfach, wenn jedes $x \in M$ mit $x \neq 0$ ein Erzeuger von $M$ ist. Insbesondere sind einfache Moduln zyklisch.

2. Für jeden Erzeuger $m$ eines zyklischen Moduls $M$ definiert
$$\begin{array}{rccc} \phi_m : & R & \to & M \\ & r & \mapsto & r.m \end{array}$$
eine Surjektion. Deren Kern ist ein *maximales* Linksideal von $R$ genau dann, wenn $M$ einfach ist.

**Beweis.**

1. Sei $M$ einfacher Modul. Betrachte für $x \in M$, $x \neq 0$ den von $x$ erzeugten Untermodul. Offenbar $1.x = x \in \langle x \rangle$, so dass dieser Untermodul nicht Null ist. Da $M$ keine nicht-trivialen Untermoduln hat, muss $\langle x \rangle = M$ gelten.

   Sei umgekehrt jedes nicht-verschwindende $x \in M$ Erzeuger. Angenommen, $U \subset M$ ist ein beliebiger von $(0)$ verschiedener Untermodul. Wähle $x \in U$ mit $x \neq 0$; dies ist ein Erzeuger von $M$ und daher $M = \langle x \rangle \subset U$. Also ist $U = M$ und $M$ hat keine nicht-trivialen Untermoduln.

2. Sei $M$ einfach; angenommen, der Kern ist kein maximales Linksideal, $\ker \phi_m \subsetneq \mathfrak{m} \subsetneq R$; dann ist $\phi_m(\mathfrak{m}) \subsetneq M$ ein nicht-trivialer Untermodul von $M$, im Widerspruch dazu, dass $M$ einfach sein soll.

   Sei umgekehrt $\ker \phi_m$ maximal, aber $0 \subsetneq U \subsetneq M$ ein echter Untermodul. Dann gilt $\ker \phi_m \subsetneq \phi_m^{-1} U \subsetneq R$, im Widerspruch zur Maximalität des Ideals $\ker \phi_m \subset R$.

□

Warnung: es gilt aber nicht, dass jeder zyklische Modul einfach ist. Zum Beispiel ist der $\mathbb{Z}$-Modul $\mathbb{Z}_6$ zyklisch, aber wegen des chinesischen Restsatzes $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ nicht einfach. Als weiteres Gegenbeispiel betrachte man den Polynomring $R = K[X]$ über einem Körper $K$ und den $R$-Modul, der durch einen $K$-Vektorraum mit einem Endomorphismus mit einem einzigen Jordan-Block von Länge größer gleich zwei gegeben ist.

**Beispiele 1.5.3.**

(i) Darstellungen von Gruppen auf einem $K$-Vektorraum der Dimension 1 sind irreduzibel.

(ii) Ist $\operatorname{char} K \neq 2$ so hat die Gruppe $\mathbb{Z}_2$ zwei irreduzible eindimensionale Darstellungen $K_\pm$. Jede endlich-dimensionale Darstellung ist nach Beispiel 1.1.18 (viii) vollständig reduzibel, d.h. isomorph zu genau einer Darstellung der Gestalt

$$K_+^m \oplus K_-^n \quad \text{mit } m, n \in \mathbb{N}\,.$$

(iii) Ist $\operatorname{char} K = 2$, so ist die triviale eindimensionale Darstellung $K$ irreduzibel und die zweidimensionale Darstellung $P$ unzerlegbar, aber nicht irreduzibel. Jede endlich-dimensionale Darstellung ist isomorph zu

$$K^n \oplus P^m \quad \text{mit} \quad n, m \in \mathbb{N}\,.$$

Die Darstellung $P$ ist übrigens ein freier Modul vom Rang 1 und somit projektiv und zyklisch.

**Lemma 1.5.4.**
Sei $R$ ein Ring, $E$ ein einfacher $R$-Modul und $M$ ein beliebiger $R$-Modul.

(i) Jeder Homomorphismus $E \to M$ ist injektiv oder Null. Denn der Kern ist ein Untermodul von $E$.

(ii) Jeder Homomorphismus $M \to E$ ist surjektiv oder Null. Denn das Bild ist ein Untermodul von $E$.

(iii) Der Endomorphismenring $\operatorname{End}_R(E)$ ist ein Divisionsring, d.h. alle von Null verschiedenen Endomorphismen sind invertibel.

**Satz 1.5.5** (Schursches Lemma).
Sei $K$ ein algebraisch abgeschlossener Körper und $A$ eine $K$-Algebra. Sei $M$ ein einfacher $A$-Modul, der als $K$-Vektorraum endlich-dimensional ist, $\dim_K M < \infty$.

Dann besitzt $M$ außer den Skalaren keine Endomorphismen:

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \mathrm{End}_A(M) \\ \lambda & \mapsto & \lambda \mathrm{id}_M \end{array} .$$

**Beweis.**
Da $M$ nach Annahme einfach ist, gilt insbesondere $M \neq 0$. Jeder Endomorphismus $\varphi \in \mathrm{End}_A(M)$ hat also wegen $\dim_K M < \infty$ und da $K$ algebraisch abgeschlossen ist, wenigstens einen Eigenwert $\lambda$. Der entsprechende Eigenraum ist als Kern des Homomorphismus von Moduln $\varphi - \lambda\, \mathrm{id}_M$ ein Untermodul $M$. Da $M$ einfach sein soll, muss der Kern gleich $M$ sein, also $\varphi = \lambda\, \mathrm{id}_M$. □

**Bemerkungen 1.5.6.**

1. Für eine endliche Gruppe $G$ ist die Gruppenalgebra $K[G]$ endlich-dimensional über $K$ und somit nach Lemma 1.5.2 auch jede irreduzible Darstellung $V$ als Quotient von $K[G]$. Man muss dann also nicht mehr die Endlichdimensionalität von $V$ eigens voraussetzen.

2. Jede endlich-dimensionale irreduzible Darstellung einer *abelschen* Gruppe über einem algebraisch abgeschlossenen Körper ist eindimensional. Denn jedes Gruppenelement $g \in G$ operiert auf einer endlich-dimensionalen Darstellung durch einen Endomorphismus $\rho(g)$ der Darstellung:

$$\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g) \quad \text{für alle} \quad h \in G .$$

   Nach dem Schurschen Lemma 1.5.5 operieren somit alle Gruppenelemente durch Vielfache der Identität, so dass wir die Darstellung in eine direkte Summe eindimensionaler Unterdarstellungen zerlegen können.

3. Wir betrachten ein Beispiel über dem Körper der reellen Zahlen. Die Gruppe der vierten Einheitswurzeln in den komplexen Zahlen, $G = \{\pm 1 \pm \mathrm{i}\} \cong \mathbb{Z}_4$ operiert durch Multiplikation auf dem zwei-dimensionalen $\mathbb{R}$-Vektorraum $V = \dot{\mathbb{C}}$. Dies gibt eine irreduzible reelle Darstellung von $G$ auf $\dot{\mathbb{C}}$, aber es gilt auch

$$K = \mathbb{R} \subsetneq \mathrm{End}_G(V) \cong \mathbb{C}$$

   als $\mathbb{R}$-Algebra. Aber der Körper $\mathbb{R}$ ist nicht algebraisch abgeschlossen, so dass wir das Schursche Lemma 1.5.5 nicht anwenden können. Man beachte aber, dass im Einklang mit Lemma 1.5.4 der Endomorphismenring $\mathbb{C}$ ein Schiefkörper über dem Körper $\mathbb{R}$ ist.

4. Sei $K \subset L$ eine echte Körpererweiterung. Dann trägt der $K$-Vektorraum $V = L$ eine Darstellung der Gruppe $G = L^\times$ über $K$. Jedes Element von $L \setminus \{0\}$ ist ein Erzeuger für die $L^\times$-Wirkung, also ist die Darstellung nach Lemma 1.5.2 irreduzibel. In diesem Beispiel ist

$$\mathrm{End}_G V = L \;,$$

   was natürlich ungleich $K$ ist, selbst wenn $K$ algebraisch abgeschlossen ist. Aber für algebraisch abgeschlossenes $K$ ist eine echte Körpererweiterung $L/K$ nicht endlich-dimensional!

Es stellt sich die Frage, wie man Moduln aus einfachen Moduln aufbauen kann. Dies führt zu der folgenden Definition:

***Definition 1.5.7***
*Sei $R$ ein Ring und $M$ ein $R$-Modul. $M$ heißt von endlicher Länge genau dann, wenn es eine* endliche *Kette von Untermoduln*

$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0$$

*gibt, so dass alle Quotientenmoduln $M_i/M_{i-1}$ einfach sind. Eine solche Kette heißt Kompositionsreihe von $M$, die Moduln $M_i/M_{i-1}$ heißen Subquotienten der Kompositionsreihe. Die minimal mögliche Länge $r$ einer Kompositionsreihe heißt Länge des Moduls $M$.*

*Wir sehen gleich, dass eine Version des Satzes von Jordan-Hölder für Moduln gilt. Die Subquotienten sind bis auf Reihenfolge eindeutig und heißen Kompositionsfaktoren des Moduls $M$.*

Dazu brauchen wir das wichtige

**Lemma 1.5.8** (Neunerlemma).
Gegeben sei ein Diagramm von Moduln mit kurzen exakten Zeilen:

$$\begin{tikzcd}
A' \arrow[r, hook, "\iota_1"'] \arrow[d, "\varphi_1"'] & A \arrow[r, two heads, "\pi_1"'] \arrow[d, "\varphi_2"'] & A'' \arrow[d, "\varphi_3"'] \\
B' \arrow[r, hook, "\iota_2"'] \arrow[d, "\psi_1"'] & B \arrow[r, two heads, "\pi_2"'] \arrow[d, "\psi_2"'] & B'' \arrow[d, "\psi_3"'] \\
C' \arrow[r, hook, "\iota_3"'] & C \arrow[r, two heads, "\pi_3"'] & C''
\end{tikzcd}$$

und es seien die senkrechten Kompositionen null:

$$\psi_i \circ \varphi_i = 0 \quad \text{für } i = 1, 2, 3 \; .$$

Das Diagramm sei kommutativ in dem Sinne, dass alle 4 Quadrate kommutieren. Dann gilt: Sind zwei der Spalten kurze exakte Sequenzen, so ist auch die dritte Spalte eine kurze exakte Sequenz.

**Beweis.**
Wir behandeln das Beispiel, in dem die linke und die mittlere Spalte exakt sind.

- Die Surjektivität von $\psi_3$ folgt aus der Kommutativität des rechten unteren Quadrats, $\psi_3 \circ \pi_2 = \pi_3 \circ \psi_2$. Daher

  $$\mathrm{Im}\,(\psi_3) \supseteq \mathrm{Im}\,(\psi_3 \circ \pi_2) = \mathrm{Im}\,(\pi_3 \circ \psi_2) = C'' \, ,$$

  da $\pi_3$ und $\psi_2$ surjektiv sind.

- Um die Injektivität von $\varphi_3$ zu zeigen, betrachten wir $a'' \in A''$, so dass $\varphi_3(a'') = 0$. Wegen der Surjektivität von $\pi_1$ finden wir ein Urbild $a \in A$ unter $\pi_1$:

  $$\pi_1(a) = a'' \, .$$

Definiere $b := \varphi_2(a) \in B$. Dieses Element hat zwei Eigenschaften:

$$\begin{aligned} \psi_2(b) &= \psi_2 \circ \varphi_2(a) = 0 \quad \text{wegen } \psi_2 \circ \varphi_2 = 0 \\ \pi_2(b) &= \pi_2 \varphi_2(a) = \varphi_3 \pi_1(a) = \varphi_3(a'') = 0 \ . \end{aligned}$$

Die letzte Eigenschaft erlaubt es, die Exaktheit der zweiten Zeile zu benutzen, um ein $b' \in B'$ zu finden, so dass

$$b = \iota_2(b')$$

und die erste Eigenschaft impliziert dann

$$\psi_2 \circ \iota_2(b') = \psi_2(b) = 0 = \iota_3 \circ \psi_1(b') \, .$$

Da $\iota_3$ injektiv ist, folgt $\psi_1(b') = 0$. Jetzt können wir die Exaktheit der ersten Spalte ausnützen und finden ein Urbild von $b'$ in $A'$, also

$$b' = \varphi_1(a') \quad \text{mit} \quad a' \in A'.$$

Wir rechnen $\varphi_2 \circ \iota_1(a') = \iota_2 \varphi_1(a') = \iota_2(b') = b = \varphi_2(a)$. Nun war aber $\varphi_2$ als injektiv vorausgesetzt, also gilt $i_1(a') = a$. Das erlaubt uns die Rechnung $a'' = \pi_1(a) = \pi_1 i_1(a') = 0$, was zeigt, dass $\varphi_3$ injektiv ist.

- Im $\varphi_3 \subset \ker\ \psi_3$ war schon vorausgesetzt. Sei also $b'' \in \ker \psi_3$. Da $\pi_2$ surjektiv ist, finden wir ein Urbild $b \in B$, so dass $\pi_2(b) = b''$. Wir rechnen

  $$0 = \psi_3(b'') = \psi_3 \circ \pi_2(b) = \pi_3 \circ \psi_2(b) \, ,$$

  was aber wegen der Exaktheit der dritten Zeile impliziert, dass $c := \psi_2(b)$ sich schreiben lässt als $i_3(c') = c$. Da $\psi_1$ surjektiv ist, finden wir ein Urbild $b' \in B'$, also $\psi_1(b') = c'$. Wir betrachten nun die Differenz $x_b := -\iota_2(b') + b \in B$:

  $$\begin{aligned} \pi_2(x_b) &= -\pi_2 \circ \iota_2(b') + \pi_2(b) = \pi_2(b) = b'' \\ \psi_2(x_b) &= -\psi_2 \iota_2(b') + \psi_2(b) = -\iota_3 \psi_1(b') + c \\ &= -\iota_3(c') + c = -c + c = 0. \end{aligned}$$

  Wegen der letzten Gleichung und der Exaktheit der zweiten Spalte gibt es $a \in A$, so dass $\varphi_2(a) = x_b$. Setze $a'' := \pi_1(a)$ und rechne

  $$\varphi_3(a'') = \varphi_3 \circ \pi_1(a) = \pi_2 \circ \varphi_2(a) = \pi_2(x_b) = b'' \, .$$

  Daher gilt $b'' \in \operatorname{Im} \varphi_3$; auch die rechte Spalte ist exakt.

□

**Satz 1.5.9** (Jordan-Hölder)**.**

(i) Mit einem Modul $M$ hat auch jeder Untermodul $N \subset M$ und jeder Quotient $M/N$ von $M$ endliche Länge, und es gilt

$$\ell(M) = \ell(M/N) + \ell(N)$$

(ii) Je zwei Kompositionsreihen eines Moduls endlicher Länge haben dieselbe Länge und bis auf Reihenfolge isomorphe Subquotienten.

Sind also
$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0$$
und
$$M = \tilde{M}_s \supset \tilde{M}_{s-1} \supset \ldots \supset \tilde{M}_0 = 0$$
zwei Kompositionsreihen eines Moduls $M$, so gilt $r = s$ und es gibt eine Permutation $\sigma \in S_r$ mit
$$\tilde{M}_i/\tilde{M}_{i-1} \cong M_{\sigma i}/M_{\sigma i-1} \quad \text{für alle } i\,.$$

**Beweis.**
Sei $M$ ein $R$-Modul mit Kompositionsreihe
$$M = M_r \supset \ldots \supset M_0 = 0$$
und $N \subset M$ ein Untermodul. Wir betrachten die kanonische Surjektion
$$\text{can}: \quad M \twoheadrightarrow \overline{M} := M/N$$
und die Untermoduln
$$N_i := M_i \cap N \subset N \qquad \text{und } \overline{M}_i := \text{can}\,(M_i) \subset \overline{M}$$
Im kommutierenden Diagramm:
$$\begin{array}{ccccc}
N_{i-1} & \hookrightarrow & N_i & \twoheadrightarrow & N_i/N_{i-1} \\
\downarrow & & \downarrow & & \downarrow \\
M_{i-1} & \hookrightarrow & M_i & \twoheadrightarrow & M_i/M_{i-1} \\
\downarrow & & \downarrow & & \downarrow \\
\overline{M}_{i-1} & \hookrightarrow & \overline{M}_i & \twoheadrightarrow & \overline{M}_i/\overline{M}_{i-1}
\end{array}$$
sind die Zeilen exakt, die ersten zwei Spalten auch. Nach dem Neunerlemma 1.5.8 erhalten wir für jedes $i = 1, \ldots r$ eine kurze exakte Sequenz
$$N_i/N_{i-1} \quad \hookrightarrow \quad M_i/M_{i-1} \twoheadrightarrow \overline{M}_i/\overline{M}_{i-1}\,. \tag{3}$$

Da der Quotientenmodul $M_i/M_{i-1}$ als Kompositionsfaktor von $M$ einfach ist, sind auch die Quotientenmoduln $N_i/N_{i-1}$ und $\overline{M}_i/\overline{M}_{i-1}$ als Untermoduln oder Quotientenmoduln eines einfachen Moduln entweder Null oder einfach. Genauer ist $N_i/N_{i-1}$ genau dann Null, wenn $\overline{M}_i/\overline{M}_{i-1}$ ein einfacher Modul ist und umgekehrt. Lässt man die Moduln weg, für die der Quotient Null ist, so bilden also die verbleibenden $N_i$ eine Kompositionsreihe für den Untermodul $N$ und die verbleibenden $\overline{M}_i/\overline{M}_{i-1}$ eine Kompositionsreihe für den Quotienten $M/N$. Es folgt daraus, dass alle Untermoduln und alle Quotienten von $M$ endliche Länge haben. Aus der kurzen exakten Sequenz (3) folgt dann sofort
$$\ell(N) + \ell(M/N) = \ell(M)\,.$$
(ii) folgt mit vollständiger Induktion nach der Länge des Moduls. Der Induktionsanfang $\ell(M) = 1$ ist trivial. Betrachte nun zwei Kompositionsreihen für den Modul $M$:
$$\begin{array}{ccl}
M & \supset & X \supset \cdots \supset (0) \\
M & \supset & Y \supset \cdots \supset (0)
\end{array}$$

Gilt $X = Y$, so wendet man direkt die Induktionsvoraussetzung an. Andernfalls betrachte die kanonische Surjektion

$$\pi : M \to M/Y\,.$$

Der Modul $M/Y$ ist einfach, daher folgt $\pi(X) = M/Y$. Denn wäre $\pi(X) = 0$, so wäre $X \subset Y$, aber nach Lemma 1.5.2.2 ist $X$ als Kern der Surjektion auf einen einfachen Modul maximal; also $X = Y$. Also vermittelt $\pi$ einen Isomorphismus von Moduln

$$X/(X \cap Y) \cong M/Y\,. \tag{4}$$

Durch Vertauschen von $X$ und $Y$ findet man analog

$$Y/(X \cap Y) \cong M/X\,. \tag{5}$$

Wir wählen jetzt eine Kompositionsreihe des Durchschnitts $X \cap Y$ und vergleichen die vier Kompositionsreihen von $M$:

$$\begin{array}{lcl} M & \supset & X \supset \cdots \supset (0) \\ M & \supset & X \supset (X \cap Y) \supset \cdots \supset (0) \\ M & \supset & Y \supset (X \cap Y) \supset \cdots \supset (0) \\ M & \supset & Y \supset \cdots \supset (0)\;\;. \end{array}$$

Die erste und die zweite Kompositionsreihe sind nach Induktionsvoraussetzung, angewandt auf den Modul $X$, äquivalent. Aus dem gleichen Grund sind auch die dritte und vierte Kompositionsreihe äquivalent. Die Äquivalenz der zweiten und der dritten Kompositionsreihe folgt aus den Isomorphismen (4) und (5). □

**Korollar 1.5.10.**
Sei $R$ ein Ring, der als Linksmodul über sich selbst endliche Länge hat. Jeder einfache $R$-Modul $M$ ist dann ein Quotient von $R$, aufgefasst als Linksmodul über sich selbst, und tritt somit in jeder Kompositionsreihe von $R$ als Subquotient auf.

**Beweis.**
Nach Lemma 1.5.2 liefert jeder Erzeuger eine Surjektion $\varphi : R \twoheadrightarrow M$. Es gibt daher eine Kompositionsreihe der Form $R \supsetneq \ker \varphi \supsetneq \ldots$, in der $R/\ker\varphi \cong M$ als Kompositionsfaktor auftritt. Nach dem Satz von Jordan-Hölder 1.5.9 tritt $M$ in allen Kompositionsreihen von $R$ als Subquotient auf. □

**Korollar 1.5.11.**
Sei $R$ ein Ring, der einen Körper $K$ als Teilring hat. Ist $R$ endlich dimensional über $K$, so gibt es bis auf Isomorphismus höchstens $\dim_K R$ verschiedene einfache $R$-Moduln.

**Beweis.**
Jeder $R$-Modul $M$ ist durch Einschränkung der skalaren Multiplikation auf den Teilring $K$ auch ein $K$-Vektorraum, also gilt $\dim_K M \geq 1$. Daher gilt

$$\ell(M) \leq \dim_K(M)\,.$$

Da nach Korollar 1.5.10 jeder einfache Modul in allen Kompositionsreihen als Subquotient auftritt, gibt es höchstens $\ell(R)$ verschiedene einfache $R$-Moduln. □

Die Aussage gilt natürlich insbesondere für endlich-dimensionale $K$-Algebren und somit für die Gruppenalgebra einer endlichen Gruppe aus Definition 1.1.16.

**Satz 1.5.12.**
Sei $G$ eine endliche Gruppe und $K$ ein Körper. So gibt es bis höchstens $|G|$ verschiedene Isomorphieklassen von irreduziblen Darstellungen von $G$ über $K$.

**Beweis.**
Nach Lemma 1.1.19 fassen wir Darstellungen von $G$ als Moduln über dem Gruppenring $K[G]$ auf. Die Behauptung folgt dann direkt aus Korollar 1.5.11, da $\dim_K K[G] = |G|$. □

# 2 Kategorien, Funktoren und natürliche Transformationen

Wir wollen in diesem Kapitel einige Sprechweisen einführen, die es erlauben, sehr kompakt über Konstruktionen für Moduln über Ringen (und gleichzeitig über ähnliche Konstruktionen in vielen anderen Gebieten der Mathematik) zu sprechen. Entscheidend ist hierbei, dass man über mathematische Strukturen und die zugehörigen strukturerhaltenden Abbildungen gleichzeitig betrachtet.

## 2.1 Kategorien

***Definition 2.1.1***
*Eine Kategorie $\mathcal{C}$ besteht aus einer Klasse $\mathrm{ob}\,\mathcal{C}$ von Objekten und einer Klasse $\mathrm{mor}\,\mathcal{C}$ von Morphismen, zusammen mit den folgenden Strukturabbildungen:*

1. *Einer Identitätsabbildung* $\mathrm{id} : \mathrm{ob}\,\mathcal{C} \to \mathrm{mor}\,\mathcal{C}$
2. *Quell- und Zielabbildungen* $s, t : \mathrm{mor}\,\mathcal{C} \to \mathrm{ob}\,\mathcal{C}$
3. *Einer Kompositionsabbildung* $\circ : \mathrm{mor}\,\mathcal{C} \times_{\mathrm{ob}\,\mathcal{C}} \mathrm{mor}\,\mathcal{C} \to \mathrm{mor}\,\mathcal{C}$. *Hierbei besteht das Urbild aus denjenigen Paaren $(x, y) \in \mathrm{mor}\,\mathcal{C} \times \mathrm{mor}\,\mathcal{C}$, für die $s(x) = t(y)$ gilt.*

*Diese Abbildungen müssen folgende Axiome erfüllen:*

1. $\mathrm{Hom}_{\mathcal{C}}(a, b) := \{f \in \mathrm{mor}\,\mathcal{C} \mid s(f) = a, t(f) = b\}$ *ist eine* Menge *und keine echte Klasse.*
2. $s \circ \mathrm{id} = t \circ \mathrm{id} = \mathrm{id}_{\mathrm{ob}\,\mathcal{C}}$
   *("Quelle und Ziel der Identität auf einem Objekt $X$ ist $X$ selbst.")*
3. $s(f \circ g) = s(g)$, $t(f \circ g) = t(f)$
   *("Ziel einer Komposition ist das Ziel der zuletzt angewandten Funktion, Quelle ist die Quelle der zuerst angewandten Funktion.")*

4. $\mathrm{id}_{t(f)} \circ f = f$, $f \circ \mathrm{id}_{s(f)} = f$.
*("Komposition mit Identitätsmorphismen ist die Identität.")*

5. $f \circ (g \circ h) = (f \circ g) \circ h$, *wann immer die Kompositionen von Morphismen definiert sind (Assoziativität).*

**Beispiele 2.1.2.**

1. Die Kategorie Set der Mengen, deren Objekte Mengen und deren Morphismen Abbildungen von Mengen sind.

2. Ähnlich definiert man die Kategorie Grp der Gruppen, Ab der abelschen Gruppen, sowie für einen kommutativen Ring $R$ die Kategorie $\mathrm{Alg}_R$ der $R$-Algebren und $\mathrm{Alg}_R^1$ der unitären $R$-Algebren.

   Für Ringe $R$ und $S$ definiert man die Kategorien $R-$Mod der $R$-Linksmoduln, Mod$-R$ der $R$-Rechtsmoduln und $R-S-$Bimod der $R$-$S$-Bimoduln. Mit $\mathrm{vect}_K$ bezeichnen wir die Kategorie der Vektorräume über einem Körper $K$.

3. Top: die Objekte sind topologische Räume und die Morphismen sind stetige Abbildungen.

4. Bilden die Objekte keine echte Klasse, sondern sogar eine Menge, so heißt die Kategorie klein.

5. Die leere Kategorie und die Kategorie mit genau einem Objekt und dem dazugehörigen Identitätsmorphismus sind die beiden kleinsten Kategorien. Allgemein ist für jedes Objekt jeder Kategorie $\mathrm{Hom}(a, a)$ ein unitäres assoziatives Monoid. Kategorien mit einem Objekt sind also in Bijektion zu unitären Monoiden.

   Gruppen sind in Bijektion zu Kategorien mit einem Objekt, in denen alle Morphismen Isomorphismen sind. Für eine Gruppe $G$ bezeichnen wir die zugehörige Kategorie mit einem Objekt mit $*//G$. Daher heißen Kategorien, in denen alle Morphismen Isomorphismen sind auch Gruppoide.

6. Partiell geordnete Mengen: Sei $(X, \leq)$ eine partiell geordnete Menge, aufgefasst als Kategorie $\underline{X}$, deren Objekte die Element von $X$ sind und $\mathrm{Hom}_{\underline{X}}(x, y)$ ist die einelementige Menge, falls $x \leq y$ gilt, und leer sonst. Die Komposition ist damit eindeutig, denn es gibt immer höchstens eine Abbildung zwischen zwei Objekten.

***Definition 2.1.3***
*Seien $\mathcal{C}, \mathcal{D}$ Kategorien.*

(i) *Die Kategorie $\mathcal{C}^{\mathrm{opp}}$ ist die Kategorie mit denselben Objekten wie $\mathcal{C}$, aber Morphismen* $\mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(a, b) := \mathrm{Hom}_{\mathcal{C}}(b, a)$ *und der Komposition* $f \circ_{\mathrm{opp}} g := g \circ_{\mathcal{C}} f$ .

(ii) *Die Kategorie $\mathcal{C} \coprod \mathcal{D}$ ist die Kategorie, deren Objekte und Morphismen die disjunkten Vereinigungen der Objekte bzw. der Morphismen von $\mathcal{C}$ und von $\mathcal{D}$ sind.*

(iii) *Genauso ist $\mathcal{C} \times \mathcal{D}$ die kartesische Produktkategorie. Klar ist, dass auch unendliche disjunkte Vereinigungen bzw. Produkte konstruierbar sind.*

Wir müssen als nächstes “Abbildungen” zwischen Kategorien einführen. Sie müssen auf Objekten und Morphismen wirken.

***Definition 2.1.4***
*Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ ordnet jedem Objekt $c$ von $\mathcal{C}$ ein Objekt $F(c)$ von $\mathcal{D}$ zu, sowie jedem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$ einen Morphismus $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(c), F(c'))$. Es muss gelten:*

1. $F(\mathrm{id}_c) = \mathrm{id}_{F(c)}$.
2. $F(f \circ g) = F(f) \circ F(g)$.

*Einen Funktor $F : \mathcal{C} \to \mathcal{D}^{\mathrm{opp}}$ nennt man auch einen kontravarianten Funktor von $\mathcal{C}$ nach $\mathcal{D}$.*

Natürlich ist das das gleiche wie ein Funktor $F : \mathcal{C}^{\mathrm{opp}} \to \mathcal{D}$; ein kontravarianter Funktor “dreht Pfeile um”.

**Beispiele 2.1.5.**

1. Der Funktor $U : R\text{−Mod} \to \mathrm{Ab}$, der einem $R$-Modul die zugrundeliegende abelsche Gruppe zuordnet. Funktoren dieser Art heißen Vergissfunktoren.
2. Ein Funktor $F_\rho : *//G \to \mathrm{vect}_K$ ist dasselbe wir eine $K$-lineare Darstellung der Gruppe $G$.
3. Jeder Ringhomomorphismus $\Phi : \ R \to S$ liefert durch Restriktion der Skalare nach Lemma 1.1.23 einen Funktor $S\text{−Mod} \to R\text{−Mod}$. Man kann zum Beispiel in dieser Weise wegen $\mathbb{R} \hookrightarrow \mathbb{C}$ jeden komplexen Vektorraum durch Einschränkung der Skalare als reellen Vektorraum ansehen.
4. Der Funktor $F = -^* : \ \mathrm{vect}(K) \to \mathrm{vect}(K)^{\mathrm{opp}}$, der jedem Vektorraum seinen Dualraum zuordnet, $F(V) = V^*$, und jeder linearen Abbildung die duale Abbildung, $F(f) = f^*$.
5. Der Funktor $F =^{**}\!: \ \mathrm{vect}(K) \to \mathrm{vect}(K)$, der jedem Vektorraum seinen Bidualraum zuordnet, $F(V) = V^{**}$ und jeder Abbildung die biduale Abbildung, $F(f) = f^{**}$.
6. Der Funktor $\coprod : \mathrm{Set} \times \mathrm{Set} \to \mathrm{Set}$, der zwei Mengen $X, Y$ die disjunkte Vereinigung $X \coprod Y$ zuordnet, ebenso der Funktor $\prod$, der zwei Mengen das kartesische Produkt zuordnet.
7. Der Funktor $\otimes_R : R^{\mathrm{opp}}\text{−Mod} \times R\text{−Mod} \to \mathrm{Ab}$.
8. Sei $\mathcal{C}$ eine beliebige Kategorie. Für jedes Objekt $W$ in $\mathcal{C}$ definieren wir einen kovarianten Funktor
$$\mathrm{Hom}(W, -) \ : \ \mathcal{C} \to \mathrm{Set}$$
auf Objekten durch
$$\mathrm{Hom}(W, -) : \quad X \mapsto \mathrm{Hom}_{\mathcal{C}}(W, X) \ .$$
Einem Morphismus $X \xrightarrow{\varphi} Y$ ordnet dieser Funktor die Abbildung von Mengen durch Präkomposition
$$\begin{array}{rccc} \varphi_* : & \mathrm{Hom}_{\mathcal{C}}(W, X) & \to & \mathrm{Hom}_{\mathcal{C}}(W, Y) \\ & f & \mapsto & \varphi \circ f \ . \end{array}$$
zu. Man rechnet leicht nach, dass alle Eigenschaften eines Funktors erfüllt sind.

9. Sei wieder $\mathcal{C}$ eine beliebige Kategorie. Für jedes Objekt $W$ in $\mathcal{C}$ definieren wir einen kontravarianten Funktor, also einen Funktor

$$\mathrm{Hom}(-, W) : \ \mathcal{C} \to \mathrm{Set}^{\mathrm{opp}}$$

auf Objekten durch

$$\mathrm{Hom}(-, W) : X \to \mathrm{Hom}_{\mathcal{C}}(X, W) \ .$$

Einem Morphismus $X \xrightarrow{\varphi} Y$ ordnet dieser Funktor die Abbildung von Mengen durch Postkomposition

$$\begin{array}{llll} \varphi^* : & \mathrm{Hom}_{\mathcal{C}}(Y, W) & \to & \mathrm{Hom}_{\mathcal{C}}(X, W) \\ & f & \mapsto & f \circ \varphi \ . \end{array}$$

zu.

10. Wenn man für $\mathcal{C}$ die Kategorie $R-$Mod der Moduln über einem Ring $R$ betrachtet, so hat die Morphismenmenge $\mathrm{Hom}_{\mathcal{C}}(\cdot, \cdot)$ sogar die Struktur einer abelschen Gruppe. In diesem Fall liefern $\mathrm{Hom}(-, W)$ und $\mathrm{Hom}(W, -)$ Funktoren in die Kategorie der abelschen Gruppen, bzw. deren opponierte Kategorie. Ist der Ring $R$ kommutativ, so erhält man sogar Funktoren in die Kategorie der $R$-Moduln.

***Definition 2.1.6***
*Zwei Kategorien $\mathcal{C}, \mathcal{D}$ heißen isomorph, wenn es zwei Funktoren $F : \mathcal{C} \to \mathcal{D}$ und $G : \mathcal{D} \to \mathcal{C}$ gibt, so dass $G \circ F$ der Identitätsfunktor auf $\mathcal{C}$ und $F \circ G$ der Identitätsfunktor auf $\mathcal{D}$ ist.*

**Bemerkungen 2.1.7.**

1. Wir kennen schon Beispiele isomorpher Kategorien:

   – Für jeden Ring $R$ sind die Kategorie der $R$-Rechtsmoduln und die Kategorie der $R^{\mathrm{opp}}$-Linksmoduln isomorph, vergleiche Bemerkung 1.1.6.

   – Für jeden Körper $K$ sind die Kategorie der $K[X]$-Moduln und die Kategorie der $K$-Vektorräume mit einem $K$-linearen Endomorphismus isomorph, vergleiche Lemma 1.1.15.

   – Für jeden Körper $K$ und jede Gruppe $G$ sind die Kategorie der $K$-linearen $G$-Darstellungen und die Kategorie der $K[G]$-Moduln isomorph, vgl. Lemma 1.1.19.

2. Isomorphie von Kategorien ist, wie wir sehen werden, ein zu enger Begriff.

Um Kategorien angemessen vergleichen zu können ist es wichtig, dass es auch noch Strukturen gibt, die Beziehungen zwischen Funktoren herstellen. Wir erinnern daran, dass ein Funktor $F_\rho : *//G \to \mathrm{vect}_K$ eine $K$-lineare Darstellung beschreibt und es Morphismen von Darstellungen gibt.

Betrachten wir als weiteres Beispiel für einen Körper $K$ die Kategorie $\mathrm{vect}(K)$ der $K$-Vektorräume. Sowohl die Identität als auch der Bidualfunktor $-^{**}$ sind Endofunktoren

$$\mathrm{id}, -^{**} : \qquad \mathrm{vect}(K) \to \mathrm{vect}(K) \ .$$

Für jedes Objekt in der Kategorie, also jeden $K$-Vektorraum $V$ haben wir eine lineare Abbildung

$$\begin{array}{llll} \iota_V : & V & \mapsto & V^{**} \\ & v & \mapsto & (\varphi \mapsto \varphi(v)) \end{array}$$

die sogar ein Isomorphismus ist, wenn $V$ endlich-dimensional ist. Mit ihrer Hilfe identifiziert man oft einen endlich-dimensionalen Vektorraum und seinen Bidualraum. Wir stellen also eine Beziehung zwischen den zwei Funktoren id und $-^{**}$ her, indem wir für jedes Objekt der Kategorie einen Morphismus zwischen den Bildern des Objekts unter den beiden Funktoren finden. Allerdings gibt es Beziehungen zwischen diesen Morphismen. Dies führt uns auf die folgende Definition.

***Definition 2.1.8***

1. *Sind $F, G$ Funktoren von einer Kategorie $\mathcal{C}$ nach einer Kategorie $\mathcal{D}$, so ist eine natürliche Transformation $N : F \to G$, manchmal auch $F \Rightarrow G$ geschrieben, eine Vorschrift, die jedem Objekt $c$ in der Kategorie $\mathcal{C}$ einen Morphismus $N_c : F(c) \to G(c)$ in der Kategorie $\mathcal{D}$ zuordnet, so dass für jeden Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$ in der Kategorie $\mathcal{C}$ das folgende Diagramm in der Kategorie $\mathcal{D}$ kommutiert:*

$$\begin{tikzcd} F(c) \arrow[r, "N_c"] \arrow[d, "F(f)"] & G(c) \arrow[d, "G(f)"] \\ F(c') \arrow[r, "N_{c'}"] & G(c') \end{tikzcd}$$

2. *Sind alle Morphismen $N_c$, die in einer natürlichen Transformation auftreten, Isomorphismen in der Kategorie $\mathcal{D}$, so spricht man auch von einem natürlichen Isomorphismus.*

**Beispiele 2.1.9.**

1. Für die Einschränkungen der beiden Endofunktoren

$$\mathrm{id}, -^{**} : \qquad \mathrm{vect}_f(K) \to \mathrm{vect}_f(K)$$

auf die Unterkategorie $\mathrm{vect}_f(K)$ der endlich-dimensionalen $K$-Vektorräume bilden die oben angegebenen Isomorphismen einen natürlichen Isomorphismus $\mathrm{id} \to -^{**}$.

2. Für eine kleine Kategorie $\mathcal{C}$ und eine beliebige Kategorie $\mathcal{D}$, kann man die Funktorkategorie $[\mathcal{C}, \mathcal{D}]$ betrachten, deren Objekte Funktoren $F : \mathcal{C} \to \mathcal{D}$ sind und deren Morphismen natürliche Transformationen zwischen den Funktoren sind. Man rechne nach, dass alle Axiome einer Kategorie erfüllt sind!

3. Als Beispiel betrachten wir für $\mathcal{C}$ die total geordnete Menge $[n] := \{0, ..., n\}$, die wir wie in Beispiel 2.1.2.6 als kleine Kategorie auffassen. Ein Funktor $[n] \to R-\mathrm{Mod}$ ist dann das Gleiche wie eine Sequenz $R_0 \to R_1 \to \ldots \to R_n$ von $R$-Moduln. Eine natürliche Transformation zwischen zwei solchen Funktoren $R$ und $S$ ist ein kommutierendes Diagramm der Form

$$\begin{array}{ccccccc} R_0 & \to & R_1 \to & \ldots & \to & R_n \\ \downarrow & & \downarrow & & & \downarrow \\ S_0 & \to & S_1 \to & \ldots & \to & S_n \end{array}$$

Es ist somit klar, wann wir zwei Sequenzen (und damit auch zwei Komplexe) als isomorph auffassen.

Als Anwendung wollen wir den Begriff der Isomorphie von Kategorien abschwächen. Dazu beachten wir, dass es nie natürlich ist, zu fordern, dass zwei Objekte einer Kategorie gleich sind, nur Isomorphie ist eine natürliche Forderung. Für eine kleine Kategorie $\mathcal{C}$ bilden die Funktoren

$\mathcal{C} \to \mathcal{D}$ nach Beispiel 2.1.9 eine Kategorie, die Funktorkategorie. Entsprechend ist es auch nicht natürlich, zu fordern, dass die Kompositionen $F \circ G$ und $G \circ F$ zweier Funktoren gleich einem Identitätsfunktor sind.

***Definition 2.1.10***
*Seien $F : \mathcal{C} \to \mathcal{D}$ und $G : \mathcal{D} \to \mathcal{C}$ zwei Funktoren zwischen zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$. Dann heißen $F$ und $G$ Äquivalenzen von Kategorien, falls es natürliche Isomorphismen*

$$\epsilon : G \circ F \to \mathrm{id}_{\mathcal{C}} \quad \textit{und} \quad \eta : \mathrm{id}_{\mathcal{D}} \to F \circ G \ ,$$

*gibt.*

Wir wollen die Äquivalenz von Kategorien noch etwas anders fassen.

***Definition 2.1.11***

1. *Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heißt volltreu, wenn alle Abbildungen $F : \mathrm{Hom}_{\mathcal{C}}(c, d) \to \mathrm{Hom}_{\mathcal{D}}(F(c), F(d))$ auf Hom-Räumen Isomorphismen von Mengen sind.*

2. *Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heißt wesentlich surjektiv , wenn es für jedes Objekt $d$ von $\mathcal{D}$ ein Objekt $c$ in $\mathcal{C}$ gibt, so dass $F(c)$ und $d$ isomorph sind, $F(c) \cong d$.*

Wir zeigen nun:

**Satz 2.1.12.**
Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ vermittelt genau dann eine Äquivalenz von Kategorien, wenn $F$ volltreu und wesentlich surjektiv ist.

**Beweis.**

- Sei $F$ eine Äquivalenz von Kategorien mit Funktor $G : \mathcal{D} \to \mathcal{C}$ und natürlichen Isomorphismen $\eta : \mathrm{id}_{\mathcal{D}} \xrightarrow{\sim} FG$ und $\epsilon : GF \xrightarrow{\sim} \mathrm{id}_{\mathcal{C}}$. Dann gibt es für jedes Objekt $W \in \mathcal{D}$ einen Isomorphismus $\eta_W : W \xrightarrow{\sim} FG(W)$, woraus folgt, dass der Funktor $F$ wesentlich surjektiv ist.

- Für jeden Morphismus $V \xrightarrow{f} V'$ in $\mathcal{C}$ liefert die Natürlichkeit von $\epsilon$ ein kommutierendes Diagramm

$$\begin{tikzcd} GF(V) \arrow[r, "\sim", "\epsilon_V"'] \arrow[d, "GF(f)"'] & V \arrow[d, "f"] \\ GF(V') \arrow[r, "\sim", "\epsilon_{V'}"'] & V' \end{tikzcd} \ . \tag{6}$$

  Aus $F(f_1) = F(f_2)$ folgt $G(F(f_1)) = G(F(f_2))$. Hieraus folgt mit (6) sofort $f_1 = f_2$, so dass der Funktor $F$ treu ist. Mit Hilfe des natürlichen Isomorphismus $\eta$ folgt ebenso, dass auch der Funktor $G$ treu ist.

- Um zu zeigen, dass der Funktor $F$ voll ist, geben wir uns einen Morphismus $g : F(V) \to F(V')$ in $\mathcal{D}$ vor. Setze $f := \epsilon_{V'} \circ G(g)\epsilon_V^{-1} : V \to V'$. Wir erhalten dann aus dem kommutierenden Diagram (6) die Identität

$$\epsilon_{V'} \circ G(F(f))\epsilon_V^{-1} \overset{(6)}{=} f = \epsilon_{V'} \circ G(g)\epsilon_V^{-1}$$

  und somit $GF(f) = G(g)$. Da $G$ treu, also auf Morphismen injektiv ist, folgt $F(f) = g$. Also ist der Funktor $F$ voll. Ähnlich folgt, dass auch der Funktor $G$ voll ist.

- Sei nun umgekehrt $F : \mathcal{C} \to \mathcal{D}$ ein wesentlich surjektiver, volltreuer Funktor. Für jedes vorgegebene Objekt $W \in \mathcal{D}$ können wir wegen der wesentlichen Surjektivität von $F$ ein Objekt $G(W)$ in $\mathcal{C}$ und einen Isomorphismus $\eta_W : W \xrightarrow{\sim} F(G(W))$ wählen. Man beachte, dass hier das Auswahlaxiom eingeht, wenn man ein Objekt $G(W)$ auswählt.

  Für einen Morphismus $g : W \to W'$ in $\mathcal{D}$ betrachte

  $$\eta_{W'} \circ g \circ \eta_W^{-1} : FG(W) \to W \to W' \to FG(W') \ .$$

  Da der Funktor $F$ als volltreu vorausgesetzt wurde, gibt es einen eindeutigen Morphismus $G(g) : G(W) \to G(W')$, der unter $F$ auf $\eta_{W'} \circ g \circ \eta_W^{-1}$ abgebildet wird. Es folgt leicht, dass so ein Funktor $G$ definiert wird und dass $\eta : \mathrm{id}_\mathcal{D} \to FG$ eine natürliche Transformation ist.

- Wir müssen nur noch eine natürliche Isomorphie $\epsilon_G : GF \to \mathrm{id}_\mathcal{C}$ definieren. Für $V \in \mathcal{C}$ haben wir einen Isomorphismus

  $$\eta_{F(V)} : \quad F(V) \to FGF(V)$$

  und somit $\eta^{-1}_{F(V)} : FGF(V) \to F(V)$. Da $F$ als volltreu vorausgesetzt wurde, definiere $\epsilon_V : GF(V) \xrightarrow{\sim} V$ als das eindeutige Urbild des Morphismus $\eta^{-1}_{F(V)}$ unter $F$. Man überzeugt sich, dass dies einen natürlichen Isomorphismus definiert.

$\square$

**Beispiele 2.1.13.**

1. Wir geben ein Beispiel für zwei äquivalente Kategorien an: die Kategorie $\mathrm{vect}_f(K)$ der endlich-dimensionalen $K$-Vektorräume ist äquivalent zu der Kategorie mit einem Objekt $[n]$ für jedes $n \in \mathbb{N}$ – darunter kann man sich die Vektorräume $K^n$ vorstellen – und mit Matrizen als Morphismen $\mathrm{Hom}([n],[m]) := M(n \times m, K)$. Man beachte, dass nur die Kategorie $\mathrm{vect}_f(K)$ die Eigenschaft hat, dass die Homomorphismenräume wieder Objekte in der Kategorie, also Vektorräume, sind. Deshalb lässt sich in der zweiten Kategorie der duale Vektorraum nicht wie üblich definieren. Für praktische Rechnungen greift man aber doch manchmal auf sie zurück.

2. Ein Erzeuger einer Kategorie $\mathcal{C}$ ist ein Objekt $X$, so dass der Funktor $\mathrm{Hom}(X, -)$ treu ist. Seien $A$ und $B$ Ringe. Dann sind die folgenden Aussagen äquivalent:

   (a) Die Kategorien $A$-mod und $B$-mod der Linksmoduln sind äquivalent.

   (b) Die Kategorien $A^{\mathrm{opp}}$ -mod und $B^{\mathrm{opp}}$-mod sind äquivalent.

   (c) Es gibt einen endlich-erzeugten projektiven Erzeuger $P$ von $A$-mod und einen Ring-Isomorphismus $B \cong \mathrm{End}_A(P)$.

   Für den Beweis dieser Aussage, die als Moritas Theorem bekannt ist, verweisen wir auf die Literatur.

## 2.2 Universelle Eigenschaften und adjungierte Funktoren

Wir wollen uns nun in etwas abstrakterer Weise mit universellen Eigenschaften beschäftigen. Um ein gutes Beispiel zu bekommen, verallgemeinern wir erst einmal die Definition von direkter Summe und Produkt von Moduln.

***Definition 2.2.1***

*Sei $\mathcal{C}$ eine Kategorie und $(a_\lambda)_{\lambda\in\Lambda}$ eine Familie von Objekten in $\mathcal{C}$. Ein Objekt $c \in \mathcal{C}$ zusammen mit Morphismen $\iota_\lambda : a_\lambda \to c$ heißt <u>Koprodukt</u> der Familie $(a_\lambda)$, und $c$ wird mit $\coprod_{\lambda\in\Lambda} a_\lambda$ bezeichnet, wenn für jedes Objekt $d$ von $\mathcal{C}$ die Morphismen einen Isomorphismus von Mengen induzieren:*

$$\begin{array}{rcl} \mathrm{Hom}_{\mathcal{C}}(c,d) & \xrightarrow{\sim} & \prod_{\lambda\in\Lambda} \mathrm{Hom}_{\mathcal{C}}(a_\lambda, d) \\ f & \mapsto & (f \circ \iota_\lambda)_{\lambda\in\Lambda} \,. \end{array}$$

**Bemerkungen 2.2.2.**

1. Wir drücken die definierende Eigenschaft des Koprodukts noch einmal anders aus und beschränken uns der Einfachheit halber auf den Fall des Koprodukts von zwei Objekten $a, b$. Dann ist das Koprodukt $c$ ein Objekt mit zwei Morphismen $a \to c$ und $b \to c$, so dass es für jedes Paar von Morphismen $b \to d$ und $a \to d$ einen *eindeutigen* Morphismus $c \to d$ gibt für den das Diagramm

$$\begin{tikzcd} & a \arrow[d] \arrow[ddr] & \\ b \arrow[r] \arrow[drr] & c \arrow[dr, dashed] & \\ & & d \end{tikzcd}$$

   kommutiert.

2. Analog ist das <u>Produkt</u> $c = \prod_{\lambda\in\Lambda} a_\lambda$ definiert. Es ist ein Objekt $c$, zusammen mit einer Familie von Morphismen $pr_\lambda : c \to a_\lambda$, so dass für jedes Objekt $d$ von $\mathcal{C}$ die Abbildung

$$\begin{array}{rcl} \mathrm{Hom}_{\mathcal{C}}(d,c) & \to & \prod_{\lambda\in\Lambda} \mathrm{Hom}_{\mathcal{C}}(d, a_\lambda) \\ f & \mapsto & (pr_\lambda \circ f)_{\lambda\in\Lambda} \end{array}$$

   ein Isomorphismus von Mengen ist. Wieder als Diagramm im Falle des Produkts $c$ von zwei Objekten $a$ und $b$

$$\begin{tikzcd} d \arrow[dr, dashed] \arrow[drr] \arrow[ddr] & & \\ & c \arrow[r] \arrow[d] & a \\ & b & \end{tikzcd}$$

3. Es gibt Kategorien, in denen nicht alle Produkte und Koprodukte existieren. Aber wenn solche existieren, so folgt aus der universellen Eigenschaft, dass sie bis auf eindeutige Isomorphie eindeutig sind.

4. Wir bringen noch einige Beispiele:

   (a) In der Kategorie der $R$-Moduln sind die direkte Summe und das direkte Produkt aus Definition 1.2.1 das kategorielle Koprodukt bzw. Produkt. Dies ist der Inhalt der Bemerkung 1.2.2 (ii).

   (b) Das kartesische Produkt von Ringen ist auch ein kategorielles Produkt in der Kategorie der Ringe. Das Tensorprodukt dagegen ist das Koprodukt in der Kategorie der *kommutativen* Ringe, nicht aber in der Kategorie aller Ringe.

Wir betrachten die direkte Summe und das direkte Produkt einer Familie $(X_\lambda)_{\lambda\in\Lambda}$ von Moduln über einem gegebenen Ring $R$, also $X \in \mathcal{D} = R$-mod noch etwas formaler. Dazu sei

$$\mathcal{C} := \prod_{\lambda\in\Lambda} \mathcal{D}$$

die Produktkategorie aus Definition 2.1.3, deren Objekte $\Lambda$-Tupel von Objekten Moduln sind. Ein Morphismus $(X_\lambda)_{\lambda\in\Lambda} \to (Y_\lambda)_{\lambda\in\Lambda}$ ist ein $\Lambda$-Tupel von $R$-Modulmorphismen $f_\lambda : X_\lambda \to Y_\lambda$.

In der universellen Eigenschaft sowohl der direkten Summe als auch des Produkts tritt ein beliebiges, aber festes Objekt in allen Faktoren eines Produktes von Hom-Mengen auf. Wir führen daher den Diagonalenfunktor ein,

$$\begin{array}{rcl} \Delta : \mathcal{D} & \to & \mathcal{C} \\ X & \mapsto & (X, X, \dots, X) = (X)_{\lambda\in\Lambda} \end{array}$$

der einem Objekt $X$ die konstante Familie zuordnet und einem Morphismus $X \xrightarrow{f} Y$ die konstante Familie von Morphismen, $\Delta(f) = (f)_{\lambda\in\Lambda}$.

Wir nehmen an, dass in der Kategorie $\mathcal{D}$ alle direkten Summen und alle Produkte definiert sind. Dies ist zum Beispiel der Fall, wenn $\mathcal{D}$ die Kategorie $R-$Mod für einen Ring $R$ ist. Die direkte Summe bzw. das direkte Produkt von Moduln und Modulmorphismen liefern dann Funktoren

$$\prod, \coprod : \mathcal{C} \to \mathcal{D} \ .$$

Die universelle Eigenschaft des Koprodukts besagt dann, dass es für jedes Objekt $c \in \mathcal{C}$ - also für jede Familie von Objekten in $\mathcal{D}$ – und für jedes Objekt $d \in \mathcal{D}$ Isomorphismen von Hom-Mengen gibt:

$$\mathrm{Hom}_{\mathcal{D}}(\coprod c, d) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(c, \Delta d) \quad ;$$

im Falle des Produkts haben wir dagegen Isomorphismen

$$\mathrm{Hom}_{\mathcal{D}}(d, \prod c) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(\Delta d, c) \quad .$$

Dies führt uns auf die folgende Definition:

***Definition 2.2.3***

1. *Seien $\mathcal{C}$ und $\mathcal{D}$ beliebige Kategorien. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heißt linksadjungiert zu einem Funktor $G : \mathcal{D} \to \mathcal{C}$ falls es für je zwei Objekte $c$ in $\mathcal{C}$ und $d$ in $\mathcal{D}$ einen Isomorphismus von Mengen*

   $$\Phi_{c,d} : \ \mathrm{Hom}_{\mathcal{C}}(c, Gd) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(Fc, d)$$

   *mit der folgenden natürlichen Eigenschaft gibt.*

   *Für jeden Homomorphismus $c' \xrightarrow{f} c$ in $\mathcal{C}$ und $d \xrightarrow{g} d'$ in $\mathcal{D}$ betrachte für $\varphi \in \mathrm{Hom}_{\mathcal{D}}(Fc, d)$ den Morphismus*

   $$\mathrm{Hom}(Ff, g)(\varphi) := Fc' \xrightarrow{Ff} Fc \xrightarrow{\varphi} d \xrightarrow{g} d' \in \mathrm{Hom}_{\mathcal{D}}(Fc', d')$$

   *und für $\varphi \in \mathrm{Hom}_{\mathcal{C}}(c, Gd)$ den Morphismus*

   $$\mathrm{Hom}(f, Gg)(\varphi) := c' \xrightarrow{f} c \xrightarrow{\varphi} Gd \xrightarrow{Gg} Gd' \in \mathrm{Hom}_{\mathcal{C}}(c', Gd') \ .$$

*Die natürliche Eigenschaft ist dann die Verträglichkeitsforderung mit Morphismen, dass das Diagramm*

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(c, Gd) & \xrightarrow[\mathrm{Hom}(f,Gg)]{} & \mathrm{Hom}_{\mathcal{C}}(c', Gd') \\ \downarrow{\scriptstyle \Phi_{c,d}} & & {\scriptstyle \Phi_{c',d'}}\downarrow \\ \mathrm{Hom}_{\mathcal{D}}(Fc, d) & \xrightarrow[\mathrm{Hom}(Ff,g)]{} & \mathrm{Hom}_{\mathcal{D}}(Fc', d') \end{array}$$

*für alle Morphismen $f, g$ kommutiert.*

2. *Man schreibt dann $F \dashv G$ und sagt auch, der Funktor $G$ sei rechtsadjungiert zu $F$.*

**Beispiele 2.2.4.**

1. Wir haben schon gesehen, dass das Koprodukt ein linksadjungierter Funktor zum Diagonalenfunktor ist und das Produkt ein rechtsadjungierter Funktor zum Diagonalenfunktor.

2. Wir betrachten den Vergissfunktor

$$U: \ \mathrm{vect}(K) \to \mathrm{Set} \ ,$$

der jedem Vektorraum die unterliegende Menge zuweist. Sein linksadjungierter Funktor muss jeder Menge einen Vektorraum zuordnen. Wir behaupten, dass dies das freie Erzeugnis ist,

$$F: \ \mathrm{Set} \to \mathrm{vect}(K)\,,$$

das einer Menge $M$ den von ihr erzeugten $K$-Vektorraum $F(M)$ der Abbildungen $f: M \to K$ zuordnet, die nur für endlich viele Elemente von $M$ einen Wert ungleich Null annehmen. Dieser Vektorraum hat eine kanonische Basis, die in Bijektion zu den Elementen von $M$ ist. Eine Abbildung $f: M \to N$ von Mengen wird dabei auf diejenige lineare Abbildung $F(M) \to F(N)$ abgebildet, die den Basisvektor $\delta_m$ mit $m \in M$ der kanonischen Basis von $F(M)$ auf den Basisvektor $\delta_{f(m)}$ der kanonischen Basis von $F(N)$ abbildet.

Wir haben dann für jede Menge $M$ und jeden $K$-Vektorraum $V$ einen Isomorphismus von Mengen

$$\begin{array}{rccl} \Phi_{M,V}: & \mathrm{Hom}_{\mathrm{Set}}(M, U(V)) & \to & \mathrm{Hom}_K(F(M), V) \\ & \varphi & \mapsto & \Phi_{M,V}(\varphi) \end{array}$$

mit

$$\Phi_{M,V}(\varphi)(\sum_{m\in M} \lambda_m m) := \sum_{m\in M} \lambda_m \varphi(m) \ .$$

Insbesondere finden wir, dass für jeden $K$-Vektorraum $V$ die einelementige Menge $\mathrm{Hom}_{\mathrm{Set}}(\emptyset, G(V))$ isomorph zum Raum der linearen Abbildungen $\mathrm{Hom}_K(F(\emptyset), V)$ sein muss. Der einzige $K$-Vektorraum aber, von dem es genau eine lineare Abbildung in jeden $K$-Vektorraum $V$ gibt, ist der Nullvektorraum, $F(\emptyset) = \{0\}$. Dies führt zu der Einsicht, dass Nullvektorraum von der leeren Menge erzeugt wird.

3. Ein ähnliches Beispiel ist der Vergissfunktor $U: Gr \to \mathrm{Set}$, der einer Gruppe die zu Grunde liegende Menge zuordnet. Hier gibt es ebenfalls einen linksadjungierten Funktor, nämlich den Funktor $F$, der einer Menge die von ihr erzeugte freie Gruppe zuordnet.

Die Kategorie *Ab* der abelschen Gruppen ist eine Unterkategorie der Kategorie *Gr* aller Gruppen, auf die wir den Vergissfunktor einschränken können. Der linkadjungierte Funktor ist nun ein Funktor $F': \ \mathrm{Set} \to Ab$ und ordnet einer Menge die freie *abelsche* Gruppe zu. Er ist von dem oben beschriebenen linksadjungierten Funktor verschieden.

Wir lernen also, dass freie Erzeugnisse als Bilder des zu einem Vergissfunktor linksadjungierten Funktors definiert werden sollen.

4. Es gibt aber auch Vergissfunktoren, die keinen linksadjungierten Funktor haben. Als Beispiel nehmen wir den Vergissfunktor $U$ von der Kategorie von Körpern in die Kategorie von Mengen. Gäbe es einen linksajungierten Funktor, so würde dieser einer Menge $M$ einen Körper $K(M)$ zuordnen. Natürlich können wir auch speziell für $M = \emptyset$ wählen. Wir würden dann einen Körper $K = K(\emptyset)$ suchen, so dass für jeden Körper $L$ eine Bijektion von Mengen

$$\mathrm{Hom}_{\mathrm{Field}}(K, L) \cong \mathrm{Hom}_{\mathrm{Set}}(\emptyset, U(L)) \cong \star$$

existiert. Da nichttriviale Körperhomomorphismen injektiv sind, muss der gesuchte Körper Unterkörper jedes Körper sein. Ein solcher Körper existiert nicht: der Primkörper hängt von der Charakteristik von $L$ ab. (Anders formuliert: in der Kategorie von Mengen gibt es ein initiales Objekt, die leere Menge. In der Kategorie aller Körper gibt es kein initiales Objekt.) Es gibt also keinen "frei erzeugten Körper".

5. Der Inklusionsfunktor $I : Ab \to Grp$ der abelschen Gruppen in alle Gruppen hat einen linksadjungierten Funktor, nämlich $(-)_{\mathrm{ab}} : Grp \to Ab$, der einer Gruppe $G$ ihre Abelisierung $G_{ab} := G/[G, G]$ zuordnet. Denn es gilt:

$$\mathrm{Hom}_{Grp}(G, I(A)) \cong \mathrm{Hom}_{Ab}(G_{ab}, A) \ .$$

Hat ein Funktor Adjungierte, so hat er zusätzliche Eigenschaften, wie wir zum Beispiel in Satz 2.2.11 sehen werden.

Wir betrachten noch ein anderes Beispiel aus der Modultheorie:

**Beispiel 2.2.5.**
Seien $R, S$ (unitäre) Ringe und $\phi : R \to S$ ein Ringhomomorphismus. (Ist $\phi$ injektiv, so ist $R$ ein Unterring von $S$.) Dann liefert der Pullback bzw. die Restriktion der Skalare wie in Beispiel 2.1.5.2 einen Vergissfunktor

$$U : S-\mathrm{Mod} \to R-\mathrm{Mod} \ .$$

Wir untersuchen seine adjungierten Funktoren.

1. Um einen linksadjungierten Funktor $F : R-\mathrm{Mod} \to S-\mathrm{Mod}$ zu bekommen, setzen wir auf Objekten $F(M) = S \otimes_R M$, wobei $S$ durch Pullback entlang $\phi$ zum Rechtmodul über $R$ wird und die Linkswirkung von $S$ auf $S \otimes_R M$ erklärt ist durch die Multiplikation in $S$, also $s'.(s \otimes m) := (s' \cdot s) \otimes m$. Auf Morphismen setzen wir $F(f) = \mathrm{id}_S \otimes_R f$. Dieser Funktor heißt <u>Skalarenerweiterung</u> oder <u>Induktion</u>.

   Um zu sehen, dass $F$ wirklich ein linksadjungierter Funktor von $U$ ist, betrachten wir für $M \in R-\mathrm{Mod}$ und $N \in S-\mathrm{Mod}$ die folgenden beiden Morphismen abelscher Gruppen:

$$\begin{array}{rcl} \mathrm{Hom}_R(M, U(N)) & \stackrel{\sim}{\to} & \mathrm{Hom}_S(S \otimes_R M, N) \\ f & \mapsto & (s \otimes m \mapsto s.f(m)) \end{array}$$

   und

$$\begin{array}{rcl} \mathrm{Hom}_S(S \otimes_R M, N) & \stackrel{\sim}{\to} & \mathrm{Hom}_R(M, U(N)) \\ g & \mapsto & (m \mapsto g(1_S \otimes m)) \ . \end{array}$$

   Man überlegt sich leicht, dass diese zueinander invers sind und die Natürlichkeitseigenschaft aus Definition 2.2.3 haben.

2. Um den rechtadjungierten Funktor $G : R{-}\mathrm{Mod} \to S{-}\mathrm{Mod}$ zum Pullback-Funktor $U$ zu finden, setzen wir auf Objekten

$$G(M) = \mathrm{Hom}_R(S, M)$$

Hierbei wird $S$ durch Pullback entlang $\phi$ als $R$-Modul gesehen; $G(M)$ wird zum $S$-Linksmodul durch die Rechtswirkung von $S$ auf sich selbst, $(s.\varphi)(s') := \varphi(s' \cdot s)$ für $\varphi \in \mathrm{Hom}_R(S, M)$. Der Funktor $G$ heißt auch Koinduktion.

Um zu sehen, dass $G$ wirklich ein rechtsadjungierter Funktor von $U$ ist, betrachten wir für $M \in R{-}\mathrm{Mod}$ und $N \in S{-}\mathrm{Mod}$ die beiden folgenden Morphismen abelscher Gruppen

$$\begin{array}{rcl} \mathrm{Hom}_R(U(N), M) & \xrightarrow{\sim} & \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) \\ f & \mapsto & (\, n \mapsto (s \mapsto f(sn))) \end{array}$$

mit inverser Abbildung

$$\begin{array}{rcl} \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) & \xrightarrow{\sim} & \mathrm{Hom}_R(U(N), M) \\ g & \mapsto & (n \mapsto g(n)(1_S)) \ . \end{array}$$

Man überlegt sich leicht, dass diese zueinander invers sind und die Natürlichkeitseigenschaft der Definition 2.2.3 haben.

3. Seien $R, S$ Ringe und $B$ ein $S-R$-Bimodul. Dann haben wir einen Funktor

$$\begin{array}{rcl} \tilde{B} : R{-}\mathrm{Mod} & \to & S{-}\mathrm{Mod} \\ N & \mapsto & B \otimes_R N \end{array}$$

der Linksadjungiert zum Funktor

$$\begin{array}{rcl} S{-}\mathrm{Mod} & \to & R{-}\mathrm{Mod} \\ Q & \mapsto & \mathrm{Hom}_S(B, Q) \end{array}$$

ist. Tensorprodukte und Hom-Funktoren sind zueinander adjungiert.

Es ist manchmal nützlich, die folgende Umformulierung der Definition adjungierter Funktoren zur Verfügung zu haben:

**Betrachtung 2.2.6.**

1. Seien $F \dashv G$ adjungierte Funktoren. Aus der Definition folgt, dass es insbesondere Isomorphismen

$$\mathrm{Hom}_{\mathcal{C}}(G(d), G(d)) \cong \mathrm{Hom}_{\mathcal{D}}(F(G(d)), d)$$

und

$$\mathrm{Hom}_{\mathcal{D}}(F(c), F(c)) \cong \mathrm{Hom}_{\mathcal{C}}(c, G(F(c)))$$

gibt. Die Bilder der Identität auf $G(d)$ bzw. $F(c)$ unter diesen Isomorphismen setzen sich zusammen zu natürlichen Transformationen

$$\epsilon : F \circ G \to \mathrm{id}_{\mathcal{D}} \quad \text{und} \quad \eta : \mathrm{id}_{\mathcal{C}} \to G \circ F \ .$$

(Man beachte die unterschiedliche Reihenfolge der Funktoren $G$ und $F$.) Diese haben die Eigenschaft, dass für alle Objekte $c$ in $\mathcal{C}$ und $d$ in $\mathcal{D}$ die Morphismen

$$G(d) \xrightarrow{\eta_{G(d)}} (GF)\,G(d) = \ G(FG)(d) \xrightarrow{G(\epsilon_d)} G(d)$$

und

$$F(c) \xrightarrow{F(\eta_c)} F(GF)(c) = (FG)F(c) \xrightarrow{\epsilon_{F(c)}} F(c)$$

Identitätsmorphismen sind. Für einen Beweis dieser Aussagen verweisen wir auf S. Mac Lane, Categories for the working mathematician, Springer, New York, 1971, Chapter IV.

2. Umgekehrt kann man aus den natürlichen Transformationen $\epsilon$ und $\eta$ die Adjunktionsisomorphismen gewinnen durch

$$\mathrm{Hom}_{\mathcal{C}}(c, G(d)) \xrightarrow{F} \mathrm{Hom}_{\mathcal{D}}(F(c), F(G(d)) \xrightarrow{(\epsilon_d)_*} \mathrm{Hom}_{\mathcal{D}}(F(c), d)$$

   und ihre Inversen durch

$$\mathrm{Hom}_{\mathcal{D}}(F(c), d) \xrightarrow{G} \mathrm{Hom}_{\mathcal{C}}(G(F(c)), G(d)) \xrightarrow{\eta_d^*} \mathrm{Hom}_{\mathcal{C}}(c, G(d)) .$$

3. Wir können nun auch sagen, dass ein Paar adjungierter Funktoren $F \dashv G$ genau dann eine Äquivalenz von Kategorien liefert, falls $\epsilon$ und $\eta$ natürliche *Iso*morphismen sind.

Um ein wichtiges Hilfsmittel aus der Kategorientheorie zu bekommen, beschäftigen wir uns nun mit Funktoren in die Kategorie Set der Mengen. Für jedes Objekt $c$ einer Kategorie $\mathcal{C}$ haben wir einen Funktor nach Set, für den wir die Bezeichnung

$$y_c := \mathrm{Hom}_{\mathcal{C}}(c, -) : \mathcal{C} \to \mathrm{Set}$$

einführen. Dies ist eine spezielle Klasse von Funktoren $\mathcal{C} \to \mathrm{Set}$.

***Definition 2.2.7***
*Sei $\mathcal{C}$ eine Kategorie. Ein Funktor $F : \mathcal{C} \to \mathrm{Set}$ heißt darstellbar, wenn er natürlich isomorph zu einem Funktor $y_c$ für ein Objekt $c$ ist. Wir sagen dann auch, das Objekt $c$ stelle den Funktor $F$ dar und nennen $c$ ein darstellendes Objekt.*

**Beispiele 2.2.8.**

1. Sei $F : \mathrm{Ring} \to \mathrm{Set}$ der Vergessensfunktor, der jedem Ring die zu Grunde liegende Menge zuordnet. Dann haben wir die Isomorphie von Mengen

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[X], R) & \to & R \\ \varphi & \mapsto & \varphi(X) \ , \end{array}$$

   so dass der Polynomring $\mathbb{Z}[X]$ den Vergessensfunktor darstellt.

2. Sei $F : \mathrm{Ring} \to \mathrm{Set}$ der Funktor, der einem Ring $R$ die Menge der Einheiten $R^\times$ zuordnet. Dieser Funktor wird dargestellt durch den Quotientenring $\mathbb{Z}[X, Y]/(XY - 1)$. In der Tat ist

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[X, Y]/(XY - 1), R) & \to & R^\times \\ \varphi & \mapsto & \varphi(X) \ , \end{array}$$

   ein Isomorphismus von Mengen, dessen Umkehrabbildung für $r \in R^\times$ der Ringmorphismus $X \mapsto r, Y \mapsto r^{-1}$ ist.

Es ist eine wichtige Technik, Objekte konstruieren, indem man erst einen Funktor nach Set einführt und dann nachweist, dass dieser darstellbar ist. Man möchte dann natürlich wissen, dass das darstellende Objekt eindeutig ist. Dies folgt aus dem folgenden Lemma über Funktoren in die Kategorie Set, das insgesamt eine zentrale Rolle in der Kategorientheorie spielt:

**Lemma 2.2.9** (Yoneda-Lemma)**.**

1. Sei $\mathcal{C}$ eine Kategorie, $F : \mathcal{C} \to \mathrm{Set}$ ein Funktor und $c \in \mathcal{C}$ ein Objekt. Dann bilden die natürlichen Transformationen $\mathrm{Hom}(y_c, F)$ eine Menge.

2. Betrachte die Abbildung

$$\begin{array}{lclcl} \mathrm{Hom}(y_c, F) & \to & \mathrm{Hom}_{\mathrm{Set}}(y_c(c), F(c)) \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\mathrm{Set}}(\mathrm{Hom}_{\mathcal{C}}(c,c), F(c)) & \to & F(c) \\ N & \mapsto & N_c & \mapsto & N_c(\mathrm{id}_c) \ , \end{array}$$

wobei der erste Pfeil die Projektion der natürlichen Transformation auf ihre Komponente in $c$ ist und der letzte Pfeil das Einsetzen von $\mathrm{id}_c$ ist. Diese Abbildung ist eine Bijektion von Mengen.

**Beweis.**
Ist $N : y_c \to F$ eine natürliche Transformation, so kommutiert nach Definition für jeden Morphismus $f : c \to c'$ in $\mathcal{C}$ das Diagramm

$$\begin{tikzcd} y_c(c) \arrow[r, "y_c(f)"] \arrow[d, "N_c"] & y_c(c') \arrow[d, "N_{c'}"] \\ F(c) \arrow[r, "F(f)"] & F(c') \end{tikzcd}$$

Indem wir das Bild von $\mathrm{id}_c \in y_c(c) = \mathrm{Hom}_{\mathcal{C}}(c, c)$ durch das Diagramm verfolgen, sehen wir mit

$$N_{c'}(y_c(f)(\mathrm{id}_c)) = \ N_{c'}(f_*\mathrm{id}_c) = N_{c'}(f)$$

dass die Gleichung

$$N_{c'}(f) = F(f)(N_c(\mathrm{id}_c))$$

für alle $f \in \mathrm{Hom}(c, c') = y_c(c')$ gilt. Somit hängt die natürliche Transformation $N$ einzig von dem Element $N_c(\mathrm{id}_c) \in F(c)$ ab, womit die Injektivität der Yoneda-Abbildung gezeigt ist.

Umgekehrt liefert jedes Element $x \in F(c)$ für jedes Objekt $c$ der Kategorie $\mathcal{C}$ eine Abbildung von Mengen

$$\begin{array}{rcl} \mathrm{Hom}_{\mathcal{C}}(c, c') = y_c(c') & \to & F(c') \\ f & \mapsto & {}^xN(f) := \ F(f)(x) \ , \end{array}$$

die sich zu einer natürlichen Transformation ${}^xN : \ y_c \to F$ von Funktoren $\mathcal{C} \to \mathrm{Set}$ zusammensetzen. □

Das Yoneda-Lemma hat viele Folgerungen. Zunächst benutzen wir es in der folgenden Betrachtung:

**Betrachtung 2.2.10.**

1. Sei auch der Funktor $F$ von der Form $F = y_{c'} = \mathrm{Hom}(c', -)$. Dann finden wir Isomorphien

$$\mathrm{Hom}(c', c) \ \cong F(c) \cong \mathrm{Hom}(y_c, y_{c'})$$

Hierbei wird der Morphismus $f \in \mathrm{Hom}(c', c)$ auf die natürliche Transformation $y_c \to y_{c'}$ abgebildet, die auf dem Objekt $d$ wirkt durch

$$\begin{array}{rrcl} f^* : & \mathrm{Hom}(c', d) & \to & \mathrm{Hom}(c, d) \\ & \varphi & \mapsto & \varphi \circ f \end{array}$$

Daher sind die Funktoren $\mathrm{Hom}(c', -)$ und $\mathrm{Hom}(c, -)$ genau dann isomorph, wenn die Objekte $c$ und $c'$ isomorph sind.

2. Insbesondere gilt: ist ein Funktor $F : \mathcal{C} \to \mathrm{Set}$ darstellbar, so ist das darstellende Objekt eindeutig bis auf Isomorphie.

3. Indem wir die gleiche Betrachtung auf den Funktor

$$\mathrm{Hom}(-, d) : \mathcal{C}^{\mathrm{opp}} \to \mathrm{Set}$$

anwenden, finden wir auch, dass auch die Funktoren $\mathrm{Hom}(-, d)$ und $\mathrm{Hom}(-, d')$ genau dann isomorph sind, wenn die Objekte $d$ und $d'$ isomorph sind.

Wir wenden dies nun an im Beweis von

**Satz 2.2.11.**
Sei $F : \mathcal{C} \to \mathcal{D}$ ein Funktor, der einen linksadjungierten Funktor $G$ besitzt. Dann vertauscht $F$ mit Produkten. Ist $G : \mathcal{D} \to \mathcal{C}$ ein Funktor, der einen rechtsadjungierten Funktor $F$ besitzt, so vertauscht $G$ mit Koprodukten.

**Beweis.**
Es gibt für jedes Objekt $d$ von $\mathcal{D}$ ausgezeichnete Isomorphismen

$$\begin{array}{rcll}
\mathrm{Hom}_{\mathcal{D}}(d, F(\prod_i c_i)) & \cong & \mathrm{Hom}_{\mathcal{C}}(G(d), \prod_i c_i) & \text{da } G \dashv F \\
& \cong & \prod_i \mathrm{Hom}_{\mathcal{C}}(G(d), c_i) & \text{univ. Eigen. des direkten Produkts} \\
& \cong & \prod_i \mathrm{Hom}_{\mathcal{D}}(d, F(c_i)) & \text{da } G \dashv F \\
& \cong & \mathrm{Hom}_{\mathcal{D}}(d, \prod_i F(c_i)) & \text{univ. Eigen. des direkten Produkts.}
\end{array}$$

Dies liefert für jedes Objekt $d$ in der Kategorie $\mathcal{D}$ ausgezeichnete Isomorphismen. Man überlegt sich leicht, dass diese sich zu einer natürlichen Transformation vom Funktor

$$\mathrm{Hom}_{\mathcal{D}}(-, F(\prod_i c_i)) : \mathcal{D}^{\mathrm{opp}} \to \mathrm{Set}$$

zum Funktor

$$\mathrm{Hom}_{\mathcal{D}}(-, \prod_i F(c_i)) : \mathcal{D}^{\mathrm{opp}} \to \mathrm{Set}$$

zusammensetzen.

Daraus folgt die Isomorphie der Funktoren $\mathrm{Hom}_{\mathcal{D}}(-, F(\prod_i c_i))$ und $\mathrm{Hom}_{\mathcal{D}}(-, \prod_i F(c_i))$ und somit mit Betrachtung 2.2.10.1 , dass $F(\prod_i c_i) \cong \prod_i F(c_i)$ gilt. Analog geht der Beweis für Koprodukte. □

Wir bringen auch gleich eine weitere Folgerung aus dem Yoneda-Lemma 2.2.9:

**Satz 2.2.12.**
Besitzt ein Funktor $G : \mathcal{D} \to \mathcal{C}$ einen linksadjungierten Funktor, so ist dieser bis auf natürlichen Isomorphismus eindeutig bestimmt. Ebenso sind natürlich auch rechtsadjungierte Funktoren in der gleichen Weise eindeutig, wenn sie existieren.

**Beweis.**
Seien $F, F' : \mathcal{C} \to \mathcal{D}$ zwei Linksadjungierte zu $G$. Dann gibt es für alle Objekte $c \in \mathcal{C}$ und $d \in \mathcal{D}$ ausgezeichnete Isomorphismen

$$\mathrm{Hom}_{\mathcal{D}}(F(c), d) \cong \mathrm{Hom}_{\mathcal{C}}(c, G(d)) \cong \mathrm{Hom}_{\mathcal{D}}(F'(c), d)\,.$$

Die Isomorphismen erfüllen wieder die Natürlichkeitseigenschaft. Wir erhalten also einen natürlichen Isomorphismus $y_{F(c)} \to y_{F'(c)}$, der nach der Folgerung 2.2.10 aus dem Yoneda-Lemma von einem (Iso-)Morphismus $F'(c) \to F(c)$ herrührt. □

Wir wollen nun noch abschließend universelle Eigenschaften in der Sprache von Kategorien und Funktoren und den Zusammenhang zu adjungierten Funktoren diskutieren. Unsere Situation ist die folgende: wir starten mit einem Funktor $U : \mathcal{D} \to \mathcal{C}$. Hierbei ist die Kategorie $\mathcal{D}$ oft die "bessere" Kategorie, z.B. wenn $U$ ein Vergissfunktor ist. Als Beispiel betrachten wir für $\mathcal{D}$ die Kategorie der Vektorräume und für $\mathcal{C}$ die Kategorie der Mengen. Wir wollen nun ein Objekt $X \in \mathcal{C}$ verbessern durch ein Objekt $A_X \in \mathcal{D}$, etwa eine Menge $X$ linearisieren durch den von ihr frei erzeugten Vektorraum $A_X$. Man beachte, dass der frei erzeugte Vektorraum $A_X$ mit einem Morphismus $\varphi : X \to A_X$ von Mengen kommt. Die universelle Eigenschaft besagt nun, dass man auch für jeden Vektorraum $B$ jeden anderen Morphismus $\varphi : X \to U(B)$ von *Mengen* aus $X$ heraus eindeutig zu einem Morphismus $A_X \to B$ von Vektorräumen verbessern kann, also hier linearisieren kann.

***Definition 2.2.13***
*Seien $\mathcal{C}, \mathcal{D}$ Kategorien und $U : \mathcal{D} \to \mathcal{C}$ ein Funktor. Sei $X_0$ ein Objekt in $\mathcal{C}$.*

1. *Ein <u>initialer universeller Morphismus</u> von $X_0$ nach $U$ ist ein Paar $(A_{X_0}, \varphi_0)$, bestehend aus einem (verbesserten) Objekt $A_{X_0}$ in $\mathcal{D}$ und einem Morphismus $\varphi_0 : X_0 \to U(A_{X_0})$ in $\mathcal{C}$ (in der ursprünglichen Kategorie), so dass die folgende <u>universelle Eigenschaft</u> gilt:*

   *Für jedes Objekt $B$ von $\mathcal{D}$ und jeden Morphismus $f : X_0 \to U(B)$ in $\mathcal{C}$ gibt es einen eindeutigen (verbesserten) Morphismus $\tilde{f} : A_X \to B$ in $\mathcal{D}$, so dass das folgende Diagramm in $\mathcal{C}$ kommutiert:*

$$\begin{tikzcd} X_0 \arrow[r, "\varphi_0"] \arrow[dr, "f"'] & U(A_{X_0}) \arrow[d, dashed, "U(\tilde{f})"] \\ & U(B) \end{tikzcd} \qquad \begin{tikzcd} A_{X_0} \arrow[d, dashed, "\exists!\, \tilde{f}"] \\ B \end{tikzcd}$$

   *in $\mathcal{C}$      in $\mathcal{D}$*

2. *Ein <u>terminaler universeller Morphismus</u> von $U$ nach einem einem Objekt $X$ in $\mathcal{C}$ ist ein Paar $(A_X, \varphi)$, bestehend aus einem Objekt $A_X$ in $\mathcal{D}$ und einem Morphismus $\varphi : U(A_X) \to X$ in $\mathcal{C}$, so dass die folgende <u>universelle Eigenschaft</u> gilt:*

   *Für jedes Objekt $B$ von $\mathcal{D}$ und jeden Morphismus $f : U(B) \to X$ in $\mathcal{C}$ gibt es einen eindeutigen Morphismus $\tilde{f} : B \to A_X$ in $\mathcal{D}$, so dass das folgende Diagramm in $\mathcal{C}$ kommutiert:*

$$\begin{tikzcd} U(B) \arrow[d, dashed, "U(\tilde{f})"'] \arrow[dr, "f"] & \\ U(A_X) \arrow[r, "\varphi"'] & X \end{tikzcd} \qquad \begin{tikzcd} B \arrow[d, dashed, "\exists!\, \tilde{f}"] \\ A_X \end{tikzcd}$$

   *in $\mathcal{C}$      in $\mathcal{D}$*

Um die Beziehung zu adjungierten Funktoren zu sehen, beachten wir,dass wir z.B. für einen initialen universellen Morphismus eine Bijektion $\mathrm{Hom}_{\mathcal{C}}(X_0, U(B)) \cong \mathrm{Hom}_{\mathcal{D}}(A_{X_0}, B)$ haben. Ein zu $U$ linksadjungierter Funktor liefert also für jedes $X_0$ einen initialen universellen Morphismus.

**Beispiele 2.2.14.**

1. Um die universelle Eigenschaft des Polynomrings – Einsetzen – zu verstehen, betrachten wir den Vergissfunktor
$$U: \; K\text{-Alg} \to \mathrm{Set} \; .$$
Wir wollen nun den initialen universellen Morphismus für die einelementige Menge $\bullet$ untersuchen. Dies ist ein Objekt in $K$-Alg, also eine $K$-Algebra $R$, mit einem Morphismus von Mengen $\bullet \to U(R)$, d.h. einem Element $X \in R$.

   Die universelle Eigenschaft ist nun die Forderung, dass es für jede $K$-Algebra $S$ und einen Morphismus von Mengen $\bullet \to U(S)$, also für jedes Paar bestehend aus einer $K$-Algebra $S$ und einem Element $a \in S$, einen eindeutigen Morphismus $f: R \to S$ von $K$-Algebren geben muss, so dass $\bullet \to U(R) \stackrel{U(f)}{\to} U(S)$ gleich $\bullet \to S$ ist, also dass $f(X) = a$ gilt.

2. Für das Tensorprodukt betrachten wir den natürlichen Isomorphismus
$$\mathrm{Hom}_K(W \otimes V, Y) \cong \mathrm{Hom}_K(W, \mathrm{Hom}_K(V, Y)) \; ,$$
der daraus folgt, dass beide Räume bilineare Abilldungen $W \times V \to Y$ beschreiben. Wir schreiben dies um mit Hilfe der Funktoren
$$\begin{array}{rccc} U = y_V = \mathrm{Hom}(V, -): & \mathrm{vect}(K) & \to & \mathrm{vect}(K) \\ & W & \mapsto & \mathrm{Hom}_K(V, W) \end{array}$$
und
$$\begin{array}{rccc} T_V := - \otimes V: & \mathrm{vect}(K) & \to & \mathrm{vect}(K) \\ & W & \mapsto & W \otimes V \end{array}$$
und finden
$$\mathrm{Hom}_K(T_V(W), Y) \cong \mathrm{Hom}_K(W, y_V(Y))) \; .$$
Tensorieren ist also ein linksadjugierter Funktor zum Hom-Funktor.

   Das universelle Objekt von $W$ nach $y_V = \mathrm{Hom}(V, -)$ ist dann das Tensorprodukt $W \otimes V$ mit universellem Morphismus
$$\begin{array}{rccc} \varphi: & W & \to & \mathrm{Hom}_K(V, W \otimes V) \\ & w & \mapsto & \varphi_w \end{array}$$
mit $\varphi_w(v) := w \otimes v$.

**Bemerkungen 2.2.15.**

(i) Universelle Eigenschaften definieren wie gewohnt Objekte bis auf eindeutigen Isomorphismus. Gelingt es zu zeigen, dass zwei verschiedene Objekte die gleiche universelle Eigenschaft haben, so müssen diese insbesondere isomorph sein.

(ii) Universelle Konstruktionen sind funktoriell: sei $(A_{X_1}, \varphi_1)$ ein universeller Morphismus von $X_1$ nach $U$ und $(A_{X_2}, \varphi_2)$ ein universeller Morphismus von $X_2$ nach $U$. Um einen Funktor $X \mapsto A_X$ auch auf Morphismen zu definieren, betrachte einen Morphismus $h: \; X_1 \to X_2$ in $\mathcal{C}$.

   Aus Definition 2.2.13, angewandt auf den Morphismus $\varphi_2 \circ h$ in $\mathcal{C}$, folgt, dass für jeden Morphismus $h: \; X_1 \to X_2$ in $\mathcal{C}$ ein eindeutig bestimmter Morphismus $\widetilde{\varphi_2 \circ h}: A_{X_1} \to A_{X_2}$ existiert, so dass in $\mathcal{C}$ das Diagramm
$$\begin{tikzcd} X_1 \arrow[r, "\varphi_1"'] \arrow[d, "h"'] & U(A_{X_1}) \arrow[d, dashed, "U(\widetilde{\varphi_2 \circ h})"] \\ X_2 \arrow[r, "\varphi_2"'] & U(A_{X_2}) \end{tikzcd}$$

kommutiert. Existiert ein universeller Morphismus für *jedes* Objekt $X$ von $\mathcal{C}$, so definiert $X_i \mapsto A_{X_i}$ und $h \mapsto \widetilde{\varphi_2 \circ h}$ einen (Verbesserungs-)Funktor $V$ von $\mathcal{C}$ nach $\mathcal{D}$ und die Morphismen $\varphi_i$ liefern eine natürliche Transformation vom Identitätsfunktor nach $U \circ V$. Es folgt leicht, dass dann die Funktoren $U, V$ adjungiert sind, $V \dashv U$.

Wir haben schon umgekehrt gesehen, dass jedes Paar adjungierter Funktoren universelle Morphismen für *alle* Objekte liefert. Universelle Konstruktionen geben nur adjungierte Funktoren, wenn für *jedes* Objekt von $\mathcal{C}$ ein universeller Morphismus existiert.

## 2.3 Abelsche Kategorien

Wir fangen damit an, dass wir für die Morphismen-Mengen einer Kategorie mehr algebraische Struktur fordern. Zum Beispiel waren in der Kategorie $R-$Mod die Homomorphismen-Mengen sogar abelsche Gruppen. Es ist natürlich, dann auch eine Klasse von Funktoren einzuführen, die diese Struktur respektiert.

***Definition 2.3.1***

1. *Eine Kategorie $\mathcal{C}$ heißt <u>additiv</u>, falls*
   (a) *Alle* Hom*-Mengen abelsche Gruppen sind und die Komposition $\circ$ bilinear ist.*
   (b) *In $\mathcal{C}$ alle endlichen Produkte und Koprodukte existieren.*
2. *Seien $\mathcal{C}$ und $\mathcal{D}$ additive Kategorien. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heißt <u>additiv</u>, wenn für jedes Paar $X, Y$ von Objekten von $\mathcal{C}$ die Abbildung $F : \mathrm{Hom}_\mathcal{C}(X, Y) \to \mathrm{Hom}_\mathcal{D}(F(X), F(Y))$ ein Gruppenhomomorphismus ist.*

Wir wissen nach den Überlegungen des vorangegangenen Abschnitts, dass der zweite Punkt bedeutet, dass der Diagonalenfunktor $\Delta : \mathcal{C} \to \prod_{i\in I} \mathcal{C}$ für endliche Indexmengen $I$ den Koproduktfunktor $\coprod_{i\in I}$ als linksadjungierten und den Produktfunktor $\prod_{i\in I}$ als rechtsadjungierten Funktor hat.

**Bemerkung 2.3.2.**
Man beachte, dass für eine additive Kategorie auch die Existenz des leeren Produkts und Koprodukts gefordert ist.

- Betrachten wir das leere Koprodukt $\coprod_\emptyset$, das ein Objekt in $\mathcal{C}$ ist. Für jedes beliebige Objekt $M$ von $\mathcal{C}$ gibt es eine eindeutig bestimmte Familie von Morphismen nach $M$, die durch die leere Menge indiziert wird, nämlich die leere Familie. Nach der universellen Eigenschaft des Koprodukts gibt sie einen eindeutig bestimmten Morphismus $\coprod_\emptyset \to M$. Dies zeigt, dass $\coprod_\emptyset$ ein <u>initiales Objekt</u> in $\mathcal{C}$ ist. Dies ist ein Objekt $0 \in \mathcal{C}$, aus dem heraus genau ein Morphismus in jedes Objekt von $\mathcal{C}$ geht.
- Analog folgt, dass das leere Produkt von Mengen ein <u>terminales Objekt</u> $\star \in \mathcal{C}$ ist.
- Nun hat insbesondere der Hom-Raum $\mathrm{Hom}_\mathcal{C}(0, 0) = \{0\}$ nur ein Element, das gleich der Identität $\mathrm{id}_0$ auf dem initialen Objekt 0 sein muss. Gleichzeitig ist $\mathrm{id}_0$ das neutrale Element $0_0$ für die abelsche Gruppenstruktur auf $\mathrm{Hom}_\mathcal{C}(0, 0)$. Also gilt $\mathrm{id}_0 = 0_0$.

  Für einen beliebigen Morphismus $c \xrightarrow{f} 0$ folgt daher aus der Bilinearität der Verknüpfung $f = \mathrm{id}_0 \circ f = 0_0 \circ f = 0 \in \mathrm{Hom}_\mathcal{C}(c, 0)$ für alle Objekte $c \in \mathcal{C}$. Daher bestehen die Homomorphismen nur aus dem neutralen Element, $\mathrm{Hom}_\mathcal{C}(c, 0) = \{0\}$. Damit ist das initiale

Objekt 0 in einer additiven Kategorie auch terminal, $0 \cong \star$. Kategorien mit isomorphen terminalem und initialem Objekt heißen auch punktierte Kategorien. Additive Kategorien sind also punktiert.

- In jeder punktierten Kategorie finden wir für jedes Paar von Objekten $X, Y$ einen Morphismus $X \xrightarrow{0} 0 \xrightarrow{0} Y \in \mathrm{Hom}(X, Y)$. Man überlege sich, dass dieser Morphismus in einer additiven Kategorie gleich dem neutralen Element der abelschen Gruppe $\mathrm{Hom}(X, Y)$ ist.

**Bemerkung 2.3.3.**
Wir überlegen uns nun, ob es eine Eigenschaft oder eine Struktur einer Kategorie ist, additiv zu sein.

- Punktiert zu sein ist eine Eigenschaft einer Kategorie.
- In jeder punktierten Kategorie gibt es einen kanonischen Morphismus

  $$\coprod_{i \in I} X_i \to \prod_{i \in I} X_i$$

  vom Koprodukt ins Produkt. Dazu geben wir eine Familie von Morphismen

  $$f_{ij}: \ X_i \to X_j$$

  an: diese ist $0 : X_i \to X_j$ für $i \neq j$ und $\mathrm{id}_{X_i}$ im Falle gleicher Indizes.

  Wenn dieser Morphismus die Eigenschaft hat, für endliche Familien $I$ ein Isomorphismus zu sein, so definiert für zwei Morphismen $f, g : A \to B$

  $$A \xrightarrow{(\mathrm{id}_A, \mathrm{id}_A)} A \prod A = A \coprod A \xrightarrow{(f,g)} B$$

  eine Struktur eines abelschen Monoids, so dass die Komposition bilinear ist. Eine Gruppe zu sein ist wiederum eine Eigenschaft eines abelschen Monoids. Dies ist aber die einzig mögliche Komposition, siehe z.B. Borceux, Handbook of Categorical Algebra II: Categories and Structures, Proposition 1.2.7.

  Somit ist es für eine gegebene Kategorie eine *Eigenschaft*, eine additive Kategorie zu sein, und es bedarf keiner Wahl einer Struktur.
- Ist umgekehrt auf den Hom-Mengen einer Kategorie die Struktur von abelschen Monoiden gegeben und existieren z.B. Koprodukte, dann ist die Kategorie erstens punktiert und zweitens sind die Koprodukte auch Produkte (bzw. Produkte Koprodukte).

***Definition 2.3.4***

*(i) Sei $f : a \to b$ ein Morphismus in einer additiven Kategorie $\mathcal{C}$. Ein Morphismus $\iota : k \to a$ heißt Kern von $f$, und wir schreiben $\iota = \ker(f)$, falls $f \circ \iota = 0$ gilt und für jeden Morphismus $d \xrightarrow{g} a$, für den die Verkettung $f \circ g = 0$ verschwindet, es einen eindeutigen Morphismus $d \to k$ gibt, so dass das Diagramm*

$$\begin{tikzcd}
k \arrow[r, "\iota"] & a \arrow[r, "f"] & b \\
& d \arrow[ul, dashed, "\exists!"] \arrow[u, "g"] \arrow[ur, "0"'] &
\end{tikzcd}$$

*kommutiert. Äquivalent dazu können wir auch fordern, dass für alle Objekte $d$ die Sequenz abelscher Gruppen*

$$0 \to \mathrm{Hom}_{\mathcal{C}}(d,k) \xrightarrow{\iota_*} \mathrm{Hom}_{\mathcal{C}}(d,a) \xrightarrow{f_*} \mathrm{Hom}_{\mathcal{C}}(d,b)$$

*exakt ist.*

*(ii) Analog heißt ein Morphismus $p : b \to c$ Kokern von $f$, und wir schreiben $p = \mathrm{coker}(f)$, falls für alle Objekte $d$ die folgende Sequenz abelscher Gruppen exakt ist:*

$$0 \to \mathrm{Hom}_{\mathcal{C}}(c,d) \xrightarrow{p^*} \mathrm{Hom}_{\mathcal{C}}(b,d) \xrightarrow{f^*} \mathrm{Hom}_{\mathcal{C}}(a,d)\ .$$

*Als Diagramm*

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[dr, "0"'] & b \arrow[r, "p"] \arrow[d] & c \arrow[dl, dashed, "\exists!"] \\ & d & \end{tikzcd}$$

Wiederum hat nicht in jeder Kategorie jeder Morphismus einen Kern bzw. Kokern.

***Definition 2.3.5***
*Sei $\mathcal{C}$ eine Kategorie.*

1. *Ein Morphismus $\iota : a \to b$ heißt Monomorphismus, wenn aus $\iota \circ f = \iota \circ f'$ für alle passenden Morphismen $f$ und $f'$ folgt, dass $f = f'$ gilt. (In einer additiven Kategorie reicht es, dies für den Spezialfall $f' = 0$ zu fordern.)*

2. *Ein Morphismus $p : a \to b$ heißt Epimorphismus, wenn aus $f \circ p = f' \circ p$ für alle passenden Morphismen $f, f'$ folgt, dass $f = f'$ gilt.*

Wir überzeugen uns von der folgenden Tatsache:

**Lemma 2.3.6.**
Sei $\mathcal{C}$ eine additive Kategorie. Sei $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ ein Morphismus, der einen Kern $K \xrightarrow{\iota} A$ besitzt. Dann ist der Kern $\iota$ ein Monomorphismus. Dual, wenn $f$ einen Kokern besitzt, so ist der Kokern ein Epimorphismus.

**Beweis.**
Für ein beliebiges Objekt $X$ betrachte den Nullmorphismus $X \xrightarrow{0} A$. Nach der universellen Eigenschaft des Kerns gibt es einen eindeutigen Morphismus $\phi$, so dass das Diagramm

$$\begin{tikzcd} \ker f \arrow[r] & A \arrow[r, "f"] & B \\ & X \arrow[ul, dashed, "\exists\phi"] \arrow[u, "0"'] \arrow[ur, "0"'] & \end{tikzcd}$$

kommutiert. Da auch mit $\phi = 0$ das Diagramm kommutiert, muss $\phi$ der Nullmorphismus sein. Hat man also $X \xrightarrow{g} \ker f$ mit $\ker f \circ g = 0$, so ist notwendigerweise $g = 0$, also ist $\ker f$ ein Monomorphismus. □

***Definition 2.3.7***
*Sei $\mathcal{C}$ eine Kategorie. Eine additive Kategorie heißt abelsche Kategorie, falls jeder Morphismus einen Kern und einen Kokern hat, und folgende Kompatibilitätsbedingung gegeben ist:*

– *Für jeden Monomorphismus $\iota : a \to b$ gilt $\iota = \ker(\operatorname{coker}(\iota))$. Im Diagramm für den Monomorphismus*

$$\begin{tikzcd} a \arrow[r, "\iota"] & b \arrow[r, "\operatorname{coker}\iota"] & \operatorname{coker}\iota \\ & \ker\operatorname{coker}\iota \arrow[u, "\ker"] & \end{tikzcd}$$

*müssen also der linke horizontale Pfeil und der vertikale Pfeil die gleiche universelle Eigenschaft haben.*

– *Für jeden Epimorphismus $p : a \to b$ gilt $p = \operatorname{coker}(\ker(p))$.*

Für eine gegebene Kategorie ist es wieder eine Eigenschaft, eine abelsche Kategorie zu sein, und es bedarf keiner Wahl einer Struktur.

***Definition 2.3.8***
*Lässt sich ein Morphismus einer beliebigen Kategorie $f : a \to b$ zerlegen als $f = \iota \circ p$, wobei $p : a \to x$ ein Epimorphismus und $\iota : x \to b$ ein Monomorphismus ist, so nennt man das Objekt $x$ ein* <u>Bild</u> *von $f$ und schreibt $x = \mathrm{Im}\,(f)$.*

**Bemerkungen 2.3.9.**

1. Wie immer bei Objekten, die durch universelle Eigenschaften definiert sind, zeigt man, dass Kerne, Kokerne und Bilder bis auf eindeutige Isomorphie eindeutig bestimmt sind, wenn sie existieren.

2. In abelschen Kategorien kann man jeden Morphismus $f$ in der Form $f = \iota \circ p$ mit $\iota$ Monomorphismus und $p$ Epimorphismus zerlegen, so dass das Bild existiert.

   Hierzu betrachte den Kern des Kokerns:

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[dr, dashed, "e"'] & b \arrow[r, "\operatorname{coker}(f)"] & \operatorname{coker}(f) \\ & \ker\left(\operatorname{coker}(f)\right) \arrow[u, "\ker"] & \end{tikzcd}$$

   Weil $\operatorname{coker}(f) \circ f = 0$ gilt, gibt es einen eindeutigen Morphismus $e$ nach nach der universellen Eigenschaft des Kerns.

   Es ist noch zu zeigen, dass $e$ ein Epimorphismus ist. Für den recht technischen Beweis verweisen wir auf Knapp, Advanced Algebra, p. 239 ff oder Mac Lane, VIII.3. Dort wird auch gezeigt, dass $e = \operatorname{coker}(\ker f)$ gilt und dass die Faktoriserung (und somit das Bild) funktoriell sind.

   Damit können wir exakte Sequenzen in allgemeinen abelschen Kategorien einführen.

**Beispiele 2.3.10.**

1. Wir betrachten die Kategorie $\mathrm{Ab}_{fr}$ der endlich erzeugten *freien* abelschen Gruppen mit Gruppenhomomorphismen als Morphismen.

   • Untergruppen von endlich erzeugten freien abelschen Gruppen sind, wie wir sehen werden, wieder endlich erzeugt und frei. Daher sind die Kerne in $\mathrm{Ab}_{fr}$ die Kerne in der Kategorie Ab der abelschen Gruppen.

- Das Bild von Torsionselementen in einer freien abelschen Gruppe ist immer Null. Betrachte das Diagramm in der Kategorie Ab der abelschen Gruppen:

$$\begin{tikzcd} a \arrow[r, "f"] & b \arrow[r, "\mathrm{coker} f"] \arrow[d] & \mathrm{coker}(f) \arrow[dl, dashed] \\ & x & \end{tikzcd}$$

  In unserem Fall ist $x$ stets eine freie abelsche Gruppe. Daher faktorisiert der gestrichelte Morphismus über die torsionsfreie Gruppe $\mathrm{coker}(f)/\mathrm{Tor}$. Der Kokern einer Abbildung $f : M' \to M$ in $\mathcal{C}$ ist daher gegeben durch die freie Gruppe $\mathrm{coker}(f)/\mathrm{Tor}$, d.h. durch die Quotientengruppe nach der Untergruppe aller Torsionselemente.

- Die Kategorie $\mathrm{Ab}_{fr}$ hat also alle Kerne und Kokerne. Man muss aber aufpassen: betrachte für $0 \neq n \in \mathbb{Z}$ die Multiplikationsabbildung $\iota_n : \mathbb{Z} \to \mathbb{Z}$; sie hat trivialen Kern und Kokern. Daher ist das Bild dieser Abbildung in $\mathcal{C}$ die Identitätsabbildung $\mathbb{Z} \to \mathbb{Z}$. $\iota_n$ ist als injektive Abbildung der unterliegenden Mengen ein Monomorphismus, aber $\ker(\mathrm{coker}(\iota_n)) = \mathrm{id}_{\mathbb{Z}} \neq \iota_n$. Also ist $\mathrm{Ab}_{fr}$ *keine* abelsche Kategorie.

2. Für jeden Ring $R$ ist die Kategorie der $R$-Moduln abelsch, denn Kerne und Kokerne sind auf der Ebene der zu Grunde liegenden abelschen Gruppen definiert.

   Es gilt auch eine Umkehrung, das Theorem über die volle Einbettung: jede kleine abelsche Kategorie kann voll eingebettet werden in die Kategorie von Moduln über einem geeigneten Ring, so dass Exaktheitsbeziehungen erhalten sind, siehe etwa B. Mitchell, Theory of categories, Academic Press 1965, London-New York, p. 151.

3. Ist $\mathcal{C}$ eine abelsche Kategorie, so ist auch die opponierte Kategorie $\mathcal{C}^{opp}$ abelsch, denn Kerne in $\mathcal{C}^{opp}$ sind Kokerne in $\mathcal{C}$ und umgekehrt. Allgemein ist die Kategoriensprache so gehalten, dass ein $X$ in $\mathcal{C}$ einem Ko-$X$ in $\mathcal{C}^{opp}$ entspricht.

Wir haben somit in abelschen Kategorien alle Begriffe, um exakte Sequenzen einzuführen. Damit bilden abelsche Kategorien einen natürlichen Rahmen für homologische Algebra.

***Definition 2.3.11***
*Sei $F : \mathcal{C} \to \mathcal{D}$ ein additiver Funktor zwischen abelschen Kategorien. Ist $0 \to a' \to a \to a'' \to 0$ eine beliebige kurze exakte Sequenz in $\mathcal{C}$, so heißt $F$*
*halbexakt,* *falls $F(a') \to F(a) \to F(a'')$ für alle exakten Sequenzen in $\mathcal{C}$ exakt ist;*
*linksexakt,* *falls $0 = F(0) \to F(a') \to F(a) \to F(a'')$ exakt ist;*
*rechtsexakt,* *falls $F(a') \to F(a) \to F(a'') \to 0$ für alle exakten Sequenzen in $\mathcal{C}$ exakt ist;*
*exakt,* *falls $0 \to F(a') \to F(a) \to F(a'') \to 0$ für alle exakten Sequenzen in $\mathcal{C}$ exakt ist.*

**Beispiele 2.3.12.**

1. Die Funktoren $\coprod$ und $\prod : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ sind, wenn sie existieren, exakt, vgl. dazu den Beweis von 1.4.7, Schritt 2 $\Rightarrow$ 4. Nach Bemerkung 2.3.2 sind dann Produkt und Koprodukt gleich.

2. Sei $M$ ein $R$-Rechtsmodul. Der Funktor $M \otimes_R - : R{-}\mathrm{Mod} \to \mathrm{Ab}$ ist rechtsexakt nach Satz 1.4.10. Er ist exakt genau dann, wenn der Modul $M$ flach ist, vgl. Definition 1.4.11.

3. Sei $M$ ein $R$-Modul. Der Funktor $\mathrm{Hom}_R(M, -) : R{-}\mathrm{Mod} \to \mathrm{Ab}$ ist linksexakt. Er ist genau dann exakt, wenn der Modul $M$ projektiv ist, vgl. Satz 1.4.7.

4. Sei $M$ ein $R$-Modul. Der Funktor $\mathrm{Hom}_R(-, M) : (R\text{–Mod})^{\mathrm{opp}} \to Ab$ ist linksexakt. Er ist genau dann exakt, wenn der Modul $M$ injektiv ist, vgl. Satz 1.4.13.

Wir kommen dadurch zu den folgenden allgemeinen Definitionen für abelsche Kategorien:

***Definition 2.3.13***

1. *Ein Objekt $U$ einer abelschen Kategorie heißt projektiv, wenn der Funktor $\mathrm{Hom}(U, -) : \mathcal{C} \to Ab$ exakt ist.*

2. *Eine abelsche Kategorie $\mathcal{C}$ heißt halbeinfach , wenn jedes Objekt $U$ von $\mathcal{C}$ projektiv ist, d.h. wenn alle Funktoren $\mathrm{Hom}(U, -)$ exakt sind.*

3. *Ein Objekt $U$ einer abelschen Kategorie heißt injektiv, wenn der Funktor $\mathrm{Hom}(-, U) : \mathcal{C}^{\mathrm{opp}} \to Ab$ exakt ist.*

4. *Hat die abelsche Kategorie $\mathcal{C}$ ein Tensorprodukt $\otimes$ mit ähnlichen Eigenschaften wie das Tensorprodukt von Moduln über Ringen, so heißt ein Objekt $U$ flach, wenn der Funktor $U \otimes - : \mathcal{C} \to Ab$ exakt ist.*

In dieser abstrakten Sprache werden wir später homologische Algebra entwickeln, die das Studium halbexakter Funktoren zum Thema hat. Hierbei werden die Funktoren $\otimes$ und Hom im Vordergrund stehen. Mit Hilfe des vollen Einbettungssatzes aus Satz 2.3.10.2 ist klar, dass Aussagen wie das Neunerlemma 1.5.8 in beliebigen abelschen Kategorien gelten.

**Bemerkung 2.3.14.**

1. Man kann projektive und injektive Objekte nicht nur in abelschen Kategorien definieren. Sei $\mathcal{C}$ eine beliebige Kategorie. Ein Objekt $P \in \mathcal{C}$ heißt projektiv, wenn für jeden Epimorphismus $e : M \to N$ und jeden Morphismus $f : P \to N$ es eine Hochhebung $\tilde{f} : P \to M$ gibt mit $e \circ \tilde{f} = f$. Injektive Objekte sind dual definiert.

2. In der Kategorie der Mengen ist jedes Objekt $M$ injektiv: betrachte für eine Teilmenge $N_1 \subset N_2$ und einen Morphismus $f : N_1 \to M$ das Diagramm

$$\begin{tikzcd} N_1 \arrow[r] \arrow[d, "f"'] & N_2 \arrow[dl, dashed] \\ M & \end{tikzcd}$$

   Dann kann offensichtlich die Abbildung $f$ auf die Obermenge fortgesetzt werden. In anderen mathematischen Kontexten ist die Existenz von Fortsetzungen aber keinesfalls selbstverständlich!

3. Die Aussage, dass jedes Objekt in der Kategorie der Mengen projektiv ist, ist äquivalent zum Auswahlaxiom.

   Gelte das Auswahlaxiom; wähle mit Hilfe des Auswahlaxioms für einen vorgegebenen Epimorphismus $e : M \to N$ einen Schnitt $s : N \to M$, d.h. $e \circ s = \mathrm{id}_N$. Für einen beliebigen Morphismus $f : P \to N$ setze dann $\tilde{f} := s \circ f$. Dann gilt $e \circ \tilde{f} = e \circ s \circ f = f$, was zeigt, dass jedes Objekt $P$ projektiv ist.

   Ist umgekehrt jedes Objekt projektiv, so betrachte für einen gegebenen Epimorphismus $e : M \to N$ den Morphismus $f = \mathrm{id}_N$ und finde durch die Hebungseigenschaft für die

Identität einen Schnitt von $e$, als Diagramm:

$$\begin{tikzcd} & N \arrow[d, "\mathrm{id}"] & \\ M \arrow[r, "e"] & N \arrow[r] & 0 \end{tikzcd}$$

## 2.4 Freie und kofreie Moduln

Wir haben nun die Begriffe zur Verfügung, um eine Charakterisierung von injektiven Moduln geben, die dual ist zu der Charakterisierung projektiver Moduln als direkter Summanden freier Moduln.

Hierzu brauchen wir das folgende Lemma:

**Lemma 2.4.1.**
Sei $(M_i)_{i \in I}$ eine Familie von Objekten einer abelschen Kategorie $\mathcal{C}$.

1. Das Koprodukt $\coprod_{i \in I} M_i$ der Familie ist genau dann projektiv, wenn jeder Summand $M_i$ projektiv ist.

2. Das Produkt $\prod_{i \in I} M_i$ der Familie ist genau dann injektiv, wenn jeder Faktor $M_i$ injektiv ist.

**Beweis.**
Wir zeigen nur die zweite Aussage über injektive Objekte. Die erste Aussage benutzt ganz entsprechend die universelle Eigenschaft der direkten Summe.

Wir zeigen, dass der Funktor $\mathrm{Hom}(-, \prod_{i \in I} M_i)$ genau dann exakt ist, wenn alle $M_i$ injektiv sind. Dazu wenden wir den Funktor auf eine exakte Sequenz

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

an und erhalten aufgrund der universellen Eigenschaft des Produktes die Sequenz abelscher Gruppen:

$$0 \to \prod_{i \in I} \mathrm{Hom}_R(C, M_i) \to \prod_{i \in I} \mathrm{Hom}_R(B, M_i) \to \prod_{i \in I} \mathrm{Hom}_R(A, M_i) \to 0$$

Diese ist offenbar genau dann exakt, wenn die einzelnen Sequenzen

$$0 \to \mathrm{Hom}(C, M_i) \to \mathrm{Hom}(B, M_i) \to \mathrm{Hom}(A, M_i) \to 0$$

für alle $i$ exakt sind, also wenn alle Objekte $M_i$ projektiv sind. $\square$

***Definition 2.4.2***
*Sei $R$ ein Ring.*

1. *Ein $R$-Modul $\tilde{R}$ heißt regulär, wenn er projektiv ist und für jeden $R$-Modul eine exakte Sequenz*

$$\oplus_{i \in I} \tilde{R} \to M \;\; \to 0$$

*mit einer geeigneten Familie $I$ existiert. Jeden Modul der Form $\oplus_{i \in I} \tilde{R}$ nennen wir einen freien Modul zu $\tilde{R}$.*

2. *Ein $R$-Modul $R^*$ heißt koregulär, wenn er injektiv ist und für jeden $R$-Modul eine exakte Sequenz*
$$0 \to M \to \prod_{i\in I} R^*$$
*mit einer geeigneten Familie $I$ existiert. Jeden Modul der Form $\prod_{i\in I} R^*$ nennen wir einen kofreien Modul zu $R^*$.*

Wegen Lemma 2.4.1.2 sind freie Moduln projektiv und kofreie Moduln injektiv.

**Beispiele 2.4.3.**

1. $R$ selbst ist regulär; ebenso direkte Summen von Kopien von $R$.

2. Die abelsche Gruppe $R^* := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ wird durch die Rechtswirkung von $R$ auf sich selbst zum $R$-Modul, vgl. Satz 1.2.9 (ii).

   - Wir überlegen uns zunächst, dass für jede teilbare abelsche Gruppe $D$ der bezüglich des Morphismus $\mathbb{Z} \to R$ zum $\mathbb{Z}$-Modul $D$ koinduzierte $R$-Modul $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ injektiv ist. Denn Satz 1.2.9 (iii) impliziert die Isomorphie von Funktoren $R-\mathrm{Mod} \to \mathrm{Ab}$
   $$\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \cong \mathrm{Hom}_{\mathbb{Z}}(R \otimes_R -, D) \cong \mathrm{Hom}_{\mathbb{Z}}(-, D)\,.$$
   Man beachte, dass beim letzten Funktor der Vergissfunktor von $R$-Moduln zu abelschen Gruppen im ersten Argument angewandt werden muss. Anders gesagt, der Koinduktionsfunktor ist rechtsadjungiert zum Vergessensfunktor $R-\mathrm{Mod} \to \mathrm{Ab}$.
   Da $D$ teilbar ist, ist die abelsche Gruppe $D$ nach Korollar 1.4.16 injektiv in der Kategorie der $\mathbb{Z}$-Moduln. Also ist der Funktor auf der rechten Seite exakt. Somit ist auch der Funktor auf der linken Seite exakt und somit der $R$-Modul $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ injektiv.
   - Als zweites wollen wir uns überlegen, dass jeder $R$-Modul $M$ injektiv in ein Produkt von Kopien des Moduls $R^*$ abgebildet werden kann. Dazu erinnern wir uns an die Tatsache aus Beispiel 2.2.5, dass die Koinduktion der rechtsadjungierte Funktor zum Vergessensfunktor ist, es also eine Isomorphie von abelschen Gruppen
   $$(*) \qquad \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$$
   gibt.
   Da die abelsche Gruppe $\mathbb{Q}/\mathbb{Z}$ Torsionselemente beliebiger Ordnung enthält, existiert für jede abelsche Gruppe $M$ ein nichtverschwindender Gruppenhomomorphismus nach $\mathbb{Q}/\mathbb{Z}$.
   Daraus folgt wegen des Adjunktionsisomorphismus $(*)$, dass es für jeden vom Nullmodul verschiedenen $R$-Modul $M$ einen nicht-verschwindenden Morphismus von $R$-Moduln $M \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) \equiv R^*$ gibt.
   - Als nächsten Zwischenschritt verschaffen wir uns jetzt einen Morphismus von $R$-Moduln $M \to R^*$, der wenigstens auf einem vorgegebenen Element $0 \neq m \in M$ nicht verschwindet. Sei dazu $\langle m \rangle$ der von $m$ erzeugte Untermodul. Es gibt nach der verangegangenen Überlegung insbesondere einen nicht-verschwindenden Morphismus $\alpha_m : \langle m \rangle \to R^*$. Da der Modul $R^*$ injektiv ist, gibt es eine Ausdehnung $\beta_m$ auf $M$, so dass das Diagramm
   $$\begin{tikzcd} 0 \arrow[r] & \langle m \rangle \arrow[r] \arrow[d, "\alpha_m"'] & M \arrow[dl, dashed, "\beta_m"] \\ & R^* & \end{tikzcd}$$

kommutiert. Dann gilt $\beta_m(m) = \alpha_m(m) \neq 0$.

- Im letzten Schritt verwenden wir die universelle Eigenschaft des Produkts, um alle Homomorphismen $\beta_m$ zu einem einzigen zusammenzufassen:

$$\beta : \ M \to \prod_{m \in M \setminus \{0\}} R^* \ .$$

  Für diesen gilt $\beta(m) \neq 0$, da der Morphismus $\beta_m$ in die $m$-te Komponente für $m$ einen von Null verschiedenen Wert liefert. Also ist $\beta$ injektiv und somit ein Monomorphismus.

**Satz 2.4.4.**

1. Sei $\tilde{R}$ regulär. Dann ist ein $R$-Modul $M$ genau dann projektiv, wenn er direkter Summand in einer direkten Summe $\oplus_{i \in I} \tilde{R}$ ist.

2. Sei $R^*$ koregulär. Dann ist $M$ genau dann injektiv, wenn er direkter Faktor in einem Produkt $\prod_{i \in I} R^*$ ist.

**Beweis.**
Wir beweisen nur die zweite Aussage, die erste Aussage ist dual (und im Spezialfall $\tilde{R} = R$ bekannt). Ist $M$ injektiv, so spaltet die exakte Sequenz $0 \to M \to \prod_{i \in I} R^*$, also ist $M$ direkter Faktor des Produkts. Umgekehrt ist $\prod_{i \in I} R^*$ nach Lemma 2.4.1 injektiv als Produkt injektiver Moduln. Gilt $M \times M' \cong \prod_{i \in I} R^*$, so folgt wegen des gleichen Lemmas aus der Injektivität der rechten Seite die Injektivität von $M$. □

Der Leser möge nun den Beweis von Satz 1.4.13 über die verschiedenen Charakterisierungen injektiver Moduln vervollständigen.

## 2.5 Pullback und Pushout

Die universellen Eigenschaften von Produkten und Koprodukten haben eine wichtige Verallgemeinerung. Hierzu sei $\mathcal{C}$ eine additive Kategorie, die nicht unbedingt abelsch ist.

***Definition 2.5.1***

1. *Die Kategorie der Hakendiagramme in $\mathcal{C}$ hat als Objekte Diagramme der Form*

$$\Gamma := \qquad \begin{tikzcd} & X \arrow[d, "f"] \\ Y \arrow[r, "g"'] & M \end{tikzcd} \ .$$

   *Als Morphismen von Hakendiagrammen betrachten wir kommutierende Diagramme der Form*

$$\begin{tikzcd} & X \arrow[d] \arrow[drr, dotted] & & \\ Y \arrow[r] \arrow[dr, dotted] & M \arrow[drr, dotted] & & X' \arrow[d] \\ & Y' \arrow[rr] & & M' \end{tikzcd} \ .$$

2. *Für ein gegebenes Hakendiagramm $\Gamma$ betrachten wir eine Kategorie $\mathcal{C}_\Gamma$, deren Objekte kommutierende Diagramme $\Gamma(W)$ der Form*

$$\begin{tikzcd} W \arrow[r] \arrow[d] & X \arrow[d, "f"] \\ Y \arrow[r, "g"'] & M \end{tikzcd}$$

*Die Morphismen $\Gamma(W') \to \Gamma(W)$ sind Morphismen $W' \to W$, so dass das folgende Diagramm kommutiert:*

$$\begin{tikzcd} W' \arrow[dr] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & W \arrow[r] \arrow[d] & X \arrow[d] \\ & Y \arrow[r] & M \end{tikzcd}$$

*Ein terminales Objekt in der Kategorie $\mathcal{C}_\Gamma$ heißt ein Pullback für das Hakendiagramm $\Gamma$. Es erfüllt also die folgende universelle Eigenschaft: für jedes Diagramm $\Gamma(W)$ über dem Hakendiagramm $\Gamma$ gibt es genau einen Morphismus $W \to Z$ in $\mathcal{C}$, so dass das Diagramm*

$$\begin{tikzcd} W \arrow[dr, dashed, "\exists!"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & Z \arrow[r] \arrow[d] & X \arrow[d] \\ & Y \arrow[r] & M \end{tikzcd}$$

*kommutiert. Wir schreiben dann auch $Z = X \times_M Y = X\ {}_f\!\times_g Y$ oder*

$$\begin{tikzcd} Z \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & X \arrow[d, "f"] \\ Y \arrow[r, "g"'] & M \end{tikzcd}$$

**Bemerkungen 2.5.2.**

1. Da sie durch universelle Eigenschaften definiert sind, sind Pullbacks eindeutig bis auf eindeutige Isomorphie, wenn sie existieren.

2. Sei $M$ ein Objekt in einer Kategorie C. Die Überkategorie $\mathcal{C} \downarrow M$ der Objekte über $M$ ist definiert als die Kategorie, deren Objekte Paare $(X, f_X)$ sind, mit $X$ einem Objekt in $\mathcal{C}$ und einem Morphismus $f_X : X \to M$, und deren Morphismen kommutierende Diagramme

$$\begin{tikzcd} X \arrow[rr, "\varphi"] \arrow[dr, "f_X"'] & & Y \arrow[dl, "f_Y"] \\ & M & \end{tikzcd}$$

sind. Die Pullbacks $\cdot \times_M \cdot$ sind dann genau die Produkte in der Überkategorie über $M$. Sie werden daher auch Faserprodukte über $M$ genannt.

3. In den Kategorien Set, Top, Ab, $R-$Mod ist der Pullback gegeben durch

$$X \times_M Y = X\ {}_f\!\times_g Y = \{(x,y) \,|\, x \in X,\ y \in Y, \quad f(x) = g(y)\}\ .$$

Der Strukturmorphismus $X \times_M Y \to X$ ist die (Einschränkung der) Projektion $(x,y) \mapsto x$ auf die erste Komponente, der Strukturmorphismus $X \times_M Y \to X$ ist die (Einschränkung der) Projektion $(x,y) \mapsto y$. Der Morphismus $Z \to X \times_M Y$, der durch zwei geeignete Morphismen $\varphi : Z \to X$ und $\psi : Z \to Y$ induziert wird, ist gegeben durch $z \mapsto (\varphi(z), \psi(z))$.

Dies ist ein Beispiel eines <u>Differenzkerns</u>: seien $f, g : \ N \to M$ zwei Morphismen. Dann ist der Differenzkern ein Morphismus $\mathrm{Eq} \to N$, so dass im Diagramm

$$\begin{tikzcd}
\mathrm{Eq} \arrow[r] & N \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & M \\
& X \arrow[ul, dashed, "\exists! \tilde h"] \arrow[u, "h"] \arrow[ur, "0"'] &
\end{tikzcd}$$

für jeden Morphismus $h$ mit $f \circ h = g \circ h$ ein eindeutiger Morphismus $\tilde h : X \to \mathrm{Eq}$ existiert. In einer additiven Kategorie ist der Differenzkern gerade der Kern der Differenzabbildung $\delta(x,y) := f(x) - g(y)$.

In den Kategorien Set, Top, Ab, $R-$Mod ist der Pullback also der Differenzkern

$$X \times_M Y = X\ {}_f\!\times_g Y = \mathrm{Eq}(\ X \times Y \overset{f \circ pr_1}{\underset{g \circ pr_2}{\rightrightarrows}} M\ )\ .$$

4. Wenn Pullbacks existieren, liefern sie einen Funktor von der Kategorie der Hakendiagramme in $\mathcal{C}$ nach $\mathcal{C}$. Um den Funktor auf Morphismen zu definieren, betrachten wir das kommutierende Diagramm

$$\begin{tikzcd}
X \times_M Y \arrow[r] \arrow[d] & X \arrow[d] \arrow[dr, dashed] & \\
Y \arrow[r] \arrow[dr, dashed] & M \arrow[dr, dashed] & X' \arrow[d] \\
& Y' \arrow[r] & M'
\end{tikzcd}$$

Die äußeren Pfeile liefern übereinstimmende Morphismen $X \times_Y X \to Y \to Y' \to M'$ und $X \times_Y X \to X \to X' \to M$, die nach der universellen Eigenschaft des Pullbacks $X' \times_{M'} Y'$ einen eindeutigen Morphismus $X \times_M Y \to X' \times_{M'} Y'$ induzieren.

5. Im Falle der Existenz von Pullbacks liefert ein Morphismus $M \xrightarrow{g} M'$ einen Funktor der Überkategorien

$$g^* : \mathcal{C} \downarrow M' \to \mathcal{C} \downarrow M$$

liefert, der das Objekt $X \to M'$ auf das Objekt $X \times_{M'} M \to M$ in der Kategorie $\mathcal{C} \downarrow M$ abbildet:

$$\begin{tikzcd}
g^*(X) = X \times_{M'} M \arrow[r] \arrow[d] & X \arrow[d] \\
M \arrow[r, "g"] & M'
\end{tikzcd}$$

Wir nennen dann $g^*$ auch den <u>Pullbackfunktor</u> zu dem Morphismus $g$.

6. Falls in dem Diagramm

$$\begin{tikzcd} X_2 \arrow[r] \arrow[d] & X_1 \arrow[r] \arrow[d] & X_0 \arrow[d] \\ M_2 \arrow[r] & M_1 \arrow[r] & M_0 \end{tikzcd}$$

die beiden kleinen Diagramme Pullback-Diagramme sind, so auch das große. Es gilt also

$$(X_0 \times_{M_0} M_1) \times_{M_1} M_2 \cong X_0 \times_{M_0} M_2 \ .$$

Dazu betrachten wir das Diagramm

$$\begin{tikzcd} Y \arrow[dr, dashed] \arrow[drr, dashed, bend left] \arrow[drrr, bend left] \arrow[ddr, bend right] & & & \\ & (X_0 \times_{M_0} M_1) \times_{M_1} M_2 \arrow[r] \arrow[d] & X_0 \times_{M_0} M_1 \arrow[r] \arrow[d] & X_0 \arrow[d] \\ & M_2 \arrow[r, "f_1"] & M_1 \arrow[r, "f_0"] & M_0 \end{tikzcd}$$

für ein beliebiges Objekt $Y$ und geben uns Morphismen $Y \to X_0$ und $Y \to M_2$ vor, so dass das äußerste Rechteck kommutiert. Die Pullback-Eigenschaft des rechten Diagramms, angewandt auf die Morphismen $Y \to X_0$ und $Y \to M_2 \xrightarrow{f_1} M_1$ liefert uns einen eindeutigen Morphismus $Y \to X_0 \times_{M_0} M_1$. Auf diesen und auf $Y \to M_2$ wenden wir nun die Pullback-Eigenschaft des rechten Diagramms an und erhalten einen eindeutigen Morphismus $Y \to (X_0 \times_{M_0} M_1) \times_{M_1} M_2$, der zeigt, dass auch das große Diagramm ein Pullback-Diagramm ist.

7. Dieses Resultat hat eine wichtige Uminterpretation für die Pullbackfunktoren aus 5.: gegeben Morphismen $M_2 \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0$, gibt es eine ausgezeichnete natürliche Isomorphismen

$$(f_0 \circ f_1)^* \Rightarrow f_1^* \circ f_0^* \ .$$

Man beachte, dass hier i.a. keine Gleichheit von Funktoren vorliegt. Man kann zeigen, dass dann die sogenannte Kohärenzbedingung gilt, dass das folgende Diagramm von natürlichen Transformationen kommutiert

$$\begin{tikzcd} (f_0 \circ f_1 \circ f_2)^* \arrow[r, Rightarrow] \arrow[d, Rightarrow] & f_2^* \circ (f_0 \circ f_1)^* \arrow[d, Rightarrow] \\ (f_1 \circ f_2)^* \circ f_0^* \arrow[r, Rightarrow] & f_2^* \circ f_1^* \circ f_0^* \ . \end{tikzcd}$$

***Definition 2.5.3***

*Dual zum Pullback definieren wir den* <u>Pushout</u> *eines Diagramms*

$$\begin{tikzcd} N \arrow[r, "f"] \arrow[d, "g"'] & A \\ B & \end{tikzcd}$$

*als Diagramm*

$$\begin{tikzcd} N \arrow[r, "f"] \arrow[d, "g"'] & A \arrow[d] \\ B \arrow[r] & W \end{tikzcd}$$

*geschrieben $W = A \sqcup_N B$ mit der dualen universellen Eigenschaft.*

**Bemerkung 2.5.4.**

1. Man definiert die Kategorie $N \downarrow \mathcal{C}$ der Objekte unter $N$ als die Kategorie, deren Objekte Paare $(X, f)$ sind mit $f : N \to X$. Die Pushouts sind dann gerade die Koprodukte in der Unter-Kategorie. Sie werden auch amalgamierte Summen genannt.

2. In der Kategorie $R-$Mod ist der Pushout gegeben durch den Quotientenmodul

$$A \sqcup_N B = A \oplus B/(f(n), 0) \sim (0, g(n)) \ .$$

Der Strukturmorphismus $A \to A \sqcup_N B$ ist die Injektion $a \mapsto [a, b]$ in die erste Komponente. Der Morphismus $A \sqcup_N B \to Z$, der durch zwei geeignete Morphismen $f : A \to Z$ und $g : B \to Z$ induziert wird, ist gegeben durch $[a, b] \mapsto f(a) + g(b)$. Man überlege sich, dass er auf dem Quotienten wohldefiniert ist.

Allgemeiner ist der Pushout gleich dem Differenzkokern der Abbildungen

$$A \sqcup_N B := \mathrm{CoEq}(\ N \underset{g}{\overset{f}{\rightrightarrows}} A \coprod B\ )$$

in das Koprodukt, wenn dieser existiert.

3. Alle Aussagen zum Pullback haben offensichtliche Entsprechungen für das Pushout.

# 3 Moduln über Hauptidealringen

Unser Ziel in diesem Abschnitt ist es, endlich erzeugte Moduln über Hauptidealringen vollständig zu beschreiben. Nach Körpern sind Hauptidealringe die nächst einfache Klasse von Ringen. (Man erinnere sich daran, dass Hauptidealringe insbesondere kommutativ und nullteilerfrei sind.) Beispiele sind der Ring $\mathbb{Z}$ der ganzen Zahlen und der Polynomring $K[X]$ über einem Körper. Es stellt sich heraus, dass auch hier eine vollständige Beschreibung aller endlich erzeugten Moduln zu erreichen ist.

## 3.1 Untermoduln und Morphismen von Moduln über Hauptidealringen

**Satz 3.1.1.**
Sei $M$ ein freier Modul über einem Hauptidealring $R$. Dann ist auch jeder Untermodul $U$ von $M$ frei. Hat $M$ endlichen Rang, so gilt $\mathrm{rang}(U) \leq \mathrm{rang}(M)$.

Das Beispiel $n\mathbb{Z} \subsetneq \mathbb{Z}$ von $\mathbb{Z}$-Moduln zeigt, dass auch bei *echten* Untermoduln Gleichheit des Rangs auftreten kann.

**Beweis.**
Wir führen den Beweis nur für den Fall, dass der Rang von $M$ endlich ist, durch Induktion nach $\mathrm{rang} M =: n$. Im allgemeinen Fall benutzt man das Zornsche Lemma.

- Für $n = 0$ ist $M = 0$, also ist nichts zu zeigen.

- Für $n = 1$ betrachten wir einen Untermodul $I \subset R$, also ein Ideal. Dies ist ein Hauptideal, $I = (a)$, hat also ein Erzeugendensystem aus einem Element. Wegen der Nullteilerfreiheit ist die Familie $(a)$ frei, also eine Basis von $I$. Somit ist jeder Untermodul von $R$ frei vom Rang 1.

- Sei $\{x_1, \ldots, x_n\}$ eine Basis von $M$. Dann ist die Familie $(x_1, \ldots, x_{n-1})$ frei und somit der von ihr erzeugte Untermodul $M' = \langle x_1, \ldots, x_{n-1} \rangle$ von $M$ frei vom Rang $n-1$. Die Linearform
$$\begin{array}{rccc} f: & M & \to & R \\ \sum_{i=1}^n \lambda_i x_i & & \mapsto & \lambda_n \end{array}$$
liefert eine exakte Sequenz
$$0 \to M' \to M \xrightarrow{f} R \to 0 \ .$$
Für jeden Untermodul $U \subset M$ gibt dies eine exakte Sequenz
$$0 \to M' \cap U \to U \to f(U) \to 0 \ .$$
Der Untermodul $f(U) \subset R$ ist frei und vom Rang 1 nach dem Induktionsanfang, also spaltet nach Satz 1.3.6 die Sequenz:
$$U \cong (M' \cap U) \oplus f(U) \ .$$
Der Untermodul $M' \cap U$ ist frei nach Induktionsannahme und vom Rang $\leq n-1$. Somit folgt die Behauptung.

□

**Korollar 3.1.2.**
Jeder projektive Modul über einem Hauptidealring ist frei.

**Beweis.**
Jeder projektive Modul ist direkter Summand eines freien Moduls und damit insbesondere Untermodul eines freien Moduls. Diese sind aber nach Satz 3.1.1 bei Moduln über Hauptidealringen wieder freie Moduln. □

**Betrachtung 3.1.3.**

- Sei nun $M$ ein endlich erzeugter Modul über einem Hauptidealring $R$. Wie für jeden endlich erzeugten Modul über einem beliebigen Ring können wir eine Surjektion
$$p : R^m \twoheadrightarrow M$$
mit einem geeigneten $m \in \mathbb{N}$ finden. Da der Ring $R$ ein Hauptidealring ist, ist das Ideal $\ker p$ nach Satz 3.1.1 endlich erzeugt und frei, $\ker p \cong R^n$. Betrachte die Abbildung $\ker p : R^n \to R^m$ von freien Moduln. Wir finden einen Isomorphismus
$$M \cong R^m / \ker p \cong \operatorname{coker} \ker p \ .$$
Dies heißt, dass wir den endlich erzeugten Modul $M$ ausschließlich durch den Morphismus $\ker p$ zwischen zwei endlich erzeugten *freien* Moduln verstehen können.

- Man beachte, dass es hier wesentlich ist, dass wir mit freien und nicht mit projektiven Moduln arbeiten können. Es gibt wesentlich mehr Ringe, die die Eigenschaft haben, dass jeder Untermodul eines projektiven Moduls projektiv ist. Solche Ringe werden erblich genannt. Ein endlich erzeugter Modul über einem erblichen Ring ist stets Kokern eines Morphismus von endlich erzeugten projektiven Moduln. Solche Morphismen sind allerdings nicht so einfach zu beschreiben wie die zwischen freien Moduln.

Daher müssen wir nun Sätze über Morphismen von freien Moduln bereitstellen, die zum Teil bekannte Sätze der linearen Algebra verallgemeinern.

Sei $R$ ein Ring mit Eins. Wie über Körpern haben wir auch bei Ringen eine natürliche Bijektion von Hom-Räumen freier Moduln zu Matrizen mit Einträgen in $R$,

$$M: \quad \mathrm{Hom}_R(R^n, R^m) \to M(m \times n, R)$$

vgl. Bemerkung 1.3.2.6. Die Spalten der Matrix $M(f) = (a_{ij})$ sind die Bilder unter $f$ der Vektoren $e_1, \ldots, e_n$ der Standardbasis des Moduls $R^n$. In Formeln:

$$f(e_j) \;=\; \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} .$$

Für einen beliebigen Ring $R$ betrachten wir die Matrizen mit Einträgen in $R$ als abelsche Gruppe bezüglich der Matrizenaddition. Dann ist $M$ ein Isomorphismus von abelschen Gruppen. Die Matrizenmultiplikation entspricht dann der Verknüpfung von Abbildungen. Ein $R$-Modulmorphismus $\varphi$ ist genau dann ein Isomorphismus, wenn die Matrix $M(\varphi)$ invertibel ist.

Ist der Ring $R$ kommutativ, so versehen wir die Matrizen durch Linksmultiplikation aller Einträge mit einem Element aus $R$ mit der Struktur eines $R$-Moduls. Dann ist $M$ ein Isomorphismus von $R$-Moduln.

***Definition 3.1.4***
*Ist der Ring $R$* kommutativ*, so bilden wir für quadratische Matrizen $A = (a_{ij}) \in M(n \times n, R)$ mit $n \neq 0$ die Determinante durch die Vorschrift*

$$\det A = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)} .$$

Man kann natürlich die gleiche Formel auch für Matrizen mit Einträgen in einem nichtkommutativen Ring betrachten. Aber dann gilt die Formel $\det A \cdot \det B = \det AB$ nicht mehr, und der Begriff wird nutzlos.

**Satz 3.1.5.**
Sei $R$ ein kommutativer Ring.

(i) Für je zwei quadratische Matrizen $A, B \in M(n \times n, R)$ gilt

$$\det A \cdot \det B = \det AB$$

(ii) Genau dann ist die quadratische Matrix $A$ invertierbar in $M(n \times n, R)$, wenn ihre Determinante eine Einheit in $R$ ist, also $\det A \in R^\times$.

**Beweis.**

(i) Der Beweis der Multiplikativität der Determinante ist für Matzrizen mit Einträgen in einem Körper aus der linearen Algebra vertraut. Da der Integritätsbereich

$$\mathbb{Z}[X_{ij}, Y_{ij}]_{1 \le i,j \le n}$$

ein Unterring seines Quotientenkörpers ist, ist die auch die Determinante mit Einträgen in diesem Integritätsbereich multiplikativ. In diese abstrakte Identität können wir dann für $X_{ij}$ und $Y_{ij}$ Elemente eines beliebigen kommutativen Rings einsetzen, und die Behauptung folgt.

(ii) Ist $A$ invertierbar, so gilt wegen der Multiplikativität $\det A \cdot \det A^{-1} = 1$, also ist die Determinante eine Einheit in $R$. Umgekehrt betrachte die adjungierte Matrix mit Einträgen

$$A^{\#}_{ij} := (-1)^{i+j} \det A^{ji}$$

wobei $A^{ji}$ die $(n-1) \times (n-1)$-Matrix bezeichnet, die aus $A$ durch Streichung der $j$-ten Zeile und $i$-ten Spalte entsteht. Für Matrizen mit Einträgen in einem Körper zeigt man in der linearen Algebra die Identität

$$A^{\#} A = (\det A) I \,.$$

Sie überträgt man wie im ersten Teil des Beweises auf beliebige kommutative Ringe $R$.

□

Wir können nun den folgenden Satz aus der linearen Algebra für endlich erzeugte *freie* Moduln über Hauptidealringen verallgemeinern:

**Satz 3.1.6** (Elementarteilersatz)**.**
Sei $R$ ein Hauptidealring und $f : M \to N$ ein Homomorphismus zwischen zwei *freien* $R$-Moduln von endlichem Rang $m$ bzw. $n$.

(i) Es gibt eine Diagonalmatrix $D \in M(n \times m, R)$ für deren Einträge die Teilbarkeitsbeziehung

$$d_{11} \,|\, d_{22} \,|\, d_{33} \ldots \,|\, d_{rr}$$

gilt, wobei $r = \min(n, m)$ ist, und Isomorphismen $M \cong R^m$, $N \cong R^n$, so dass das Diagramm

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \wr\| & & \wr\| \\ R^m & \xrightarrow{D} & R^n \end{array}$$

kommutiert.

(ii) Die Diagonaleinträge $d_{ii}$ sind eindeutig bis auf Assoziiertheit im Ring $R$.

**Beweis.**

- Wir dürfen $M = R^m$ und $N = R^n$ annehmen. $f$ wird dann durch eine Matrix $A \in M(n \times m, R)$ beschrieben. Wir suchen invertible quadratische Matrizen

$$X \in M(n \times n, R)\,, \quad Y \in M(m \times m, R)\ ,$$

so dass das Produkt $XAY$ die beschriebene Diagonalform hat.

- Für eine Matrix $A$ bezeichne $\langle A \rangle \subset R$ das von den Einträgen der Matrix erzeugte Ideal. Für jede Matrix $X$ folgt aus der Beziehung für die Matrixelemente

$$(XA)_{ij} = \sum_k x_{ik} a_{kj}$$

sofort die Inklusionsbeziehung

$$\langle XA \rangle \subseteq \langle A \rangle$$

für die Ideale. Ist $X$ invertierbar, so bekommt man auch die umgekehrte Inklusion, also

$$\langle XA \rangle = \langle A \rangle\,.$$

- Wir werden ein Verfahren angeben, das im Fall einer echten Inklusion $\langle a_{11} \rangle \subsetneqq \langle A \rangle$ invertierbare Matrizen $X$ und $Y$ liefert, so dass das kleinere Ideal echt größer wird, $\langle (XAY)_{11} \rangle \supsetneqq \langle a_{11} \rangle$. So vergrößern wir schrittweise das Hauptideal, das vom Matrixelement in der linken oberen Ecke der Matrix erzeugt wird. In jedem Hauptidealring liegen nun wegen der Eindeutigkeit der Primzahlzerlegung nur endlich viele verschiedene Ideale $\mathfrak{a}$ zwischen zwei gegebenen Idealen, $\mathfrak{a}_0 \subseteq \mathfrak{a} \subseteq \mathfrak{a}_1$. Daher haben wir nach endlich vielen Schritten das Ideal $\langle A \rangle$ erreicht und finden somit invertierbare Matrizen $\tilde{X}$ und $\tilde{Y}$, so dass

$$\langle (\tilde{X} A \tilde{Y})_{11} \rangle = \langle A \rangle\,.$$

Jetzt kann man Spalten- und Zeilenoperationen ausführen, die alle Elemente der ersten Zeile und Spalte eliminieren, ohne das Element in der linken oberen Ecke zu verändern: da $a_{11}$ nun alle Einträge teilt, kann man geeignete Vielfache der erste Zeile bzw. Spalte zu jeder anderen Zeile bzw. Spalte addieren. So finden wir invertierbare Matrizen $\hat{X}$ und $\hat{Y}$ derart, dass in der Matrix $\hat{X}\ A\ \hat{Y}$ außer einem Eintrag $d_{11}$ in der linken oberen Ecke in der ersten Zeile und Spalte nur Nullen stehen, und dass zusätzlich gilt $\langle d_{11} \rangle = \langle A \rangle$, d.h. $d_{11}$ teilt alle weiteren Einträge.

Induktiv räumt man danach ebenso auch die endlich vielen weiteren Zeilen und Spalten auf.

- Für das Verfahren zur Vergrößerung des Ideals, das von dem Matrixelement in der linken oberen Ecke erzeugt wird, unterscheiden wir drei Fälle

  (a) $a_{11}$ teilt nicht alle Elemente in der ersten Zeile, etwa teilt $a_{11}$ nicht das Element $a_{12}$. Schreibe das Ideal $\langle a_{11}, a_{12} \rangle$ im Hauptidealring $R$ als Hauptideal:

$$\langle a_{11}, a_{12} \rangle = \langle d \rangle \quad \text{mit} \quad d \neq 0\,.$$

Dies erlaubt es uns, $x, y, \lambda, \mu \in R$ zu finden, so dass gilt:

$$\begin{aligned} d &= x a_{11} + y a_{12} \\ a_{11} &= d\lambda \\ a_{12} &= d\mu\,. \end{aligned}$$

Da Hauptidealringe nullteilerfrei sind, folgt hieraus insbesondere $1 = x\lambda + y\mu$. Wir betrachten nun das Produkt der folgenden zwei Matrizen:

$$\left(\begin{array}{cc|c} a_{11} & a_{12} & \\ & & * \\ * & * & \\ \hline & * & * \end{array}\right) \quad \left(\begin{array}{cc|c} x & -\mu & \\ & & 0 \\ y & \lambda & \\ \hline & 0 & I \end{array}\right) = \left(\begin{array}{cc|c} d & * & \\ & & * \\ * & * & \\ \hline & * & * \end{array}\right)$$

Die rechte Matrix $Y$ auf der linken Seite hat Determinante Eins, ist also nach Satz 3.1.5 invertierbar. Da das Ideal $\langle d \rangle$ das Ideal $\langle a_{11} \rangle$ echt enthält, haben wir mit $X$ der Identität ein Paar $X, Y$ von Matrizen gefunden, welches das Gewünschte leistet.

(b) Völlig analog läuft das Argument, falls $a_{11}$ nicht alle Elemente der ersten Spalte teilt.

(c) Teilt $a_{11}$ alle Elemente der ersten Zeile und Spalte, so kann man zwar schon diese durch elementare Transformationen eliminieren. Wegen $\langle a_{11} \rangle \neq \langle A \rangle$ kann $a_{11}$ aber nicht alle Einträge von $A$ teilen. Durch Addition einer geeigneten Zeile zur ersten Zeile muss man deshalb erst wieder die Situation in (a) herstellen und fährt wie dort fort.

- Es bleibt, die Eindeutigkeit der erhaltenen Diagonalmatrix zu zeigen. Sei $J_i(A)$ für $i \geq 1$ das von den Determinanten der $i \times i$-Untermatrizen von $A$ erzeugte Ideal von $R$. Offenbar gilt wieder

$$J_i(XA) \subseteq J_i(A)$$

für jede Matrix $X$, also Gleichheit der Ideale für eine invertierbare Matrix $X$. Es folgt

$$J_i(A) = \langle d_{11} d_{22} \cdots d_{ii} \rangle$$

und somit die Eindeutigkeit der Diagonalelemente $d_{ii}$ bis auf Assoziiertheit.

□

## 3.2 Klassifikation von Moduln über Hauptidealringen

Wir finden nun sehr einfach eine explizite Beschreibung endlich erzeugter Moduln über einem Hauptidealring. Wir beginnen mit einem Existenzsatz:

**Lemma 3.2.1.**
Sei $M$ ein endlich erzeugter Modul über einem Hauptidealring $R$. Dann gibt es eine aufsteigende Kette $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r \subsetneqq R$ von Idealen von $R$, so dass

$$M \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r \,.$$

Hierbei ist $\mathfrak{a}_i = 0$ ist zugelassen und $R/0 \cong R$ als $R$-Modul.

**Beweis.**
Wir hatten schon in Betrachtung 3.1.3 gesehen, dass es einen Morphismus $f : R^n \to R^m$ von endlich erzeugten freien Moduln gibt, so dass $M$ isomorph zum Kokern von $f$ ist.

Der Elementarteilersatz 3.1.6 erlaubt es uns, invertierbare Abbildungen $X, Y$ zu finden, so dass das Diagramm

$$\begin{tikzcd} R^n \arrow[r, "f"] & R^m \arrow[d, "Y"] \\ R^n \arrow[u, "X"] \arrow[r, "D"] & R^m \end{tikzcd}$$

kommutiert und $D$ eine Diagonalmatrix ist, deren Elemente die Teilbarkeitsbeziehung $d_{11}|d_{22}|\dots|d_{rr}$ mit $r = \min(m,n)$ erfüllen. Es folgt die Isomorphie von $R$-Moduln:

$$M \cong R^m/\mathrm{Im}\ D \cong R/d_{11}R \times \cdots \times R/d_{rr}R \times R^{m-r}$$

Schließlich dürfen wir Faktoren mit $d_{ii} \in R^\times$ weglassen. Hieraus folgt die Existenz der angegebenen Zerlegung. □

Das folgende Theorem fasst nun diese Überlegungen zusammen und stellt fest, dass die Beschreibung eindeutig ist. Wir geben zwei äquivalente Formulierungen.

**Theorem 3.2.2.**
Sei $M$ ein endlich erzeugter Modul über einem Hauptidealring $R$.

(i) Dann gibt es genau eine aufsteigende Kette $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r$ von Idealen in $R$, so dass

$$M \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_r \ .$$

(ii) Dann gibt es Primpotenzen $q_1, \dots, q_t$ in $R$ derart, dass gilt

$$M \cong R^s \times R/q_1R \times \cdots \times R/q_tR\,. \tag{7}$$

Dann ist $s \in \mathbb{N}_0$ wohlbestimmt, d.h. es hängt nicht von der Wahl der Zerlegung (7) ab, und die Primpotenzen $q_i$ sind wohlbestimmt bis auf Einheiten und Reihenfolge.

**Beweis.**

- Die Existenz einer Zerlegung wie in (i) hatten wir schon in Lemma 3.2.1 gezeigt. Die Existenzaussage in (ii) folgt aus dieser Existenzaussage, indem wir für $\mathfrak{a}_i \neq 0$ einen Erzeuger $\alpha_i$ wählen, $\mathfrak{a}_i = (\alpha_i)$, und diesen als Produkt von teilerfremden Primpotenzen schreiben:
$$\alpha_i = \prod_j q_j^{(i)} \ .$$
Dann wenden wir den chinesischen Restsatz an:
$$R/\mathfrak{a}_i \cong R/(q_1^{(i)}) \times R/(q_2^{(i)}) \times \cdots \times R/(q_s^{(i)})\,.$$

- Umgekehrt kann man die Eindeutigkeitsaussage in (i) auf die Eindeutigkeitsaussage in (ii) zurückführen, indem man wiederum den chinesischen Restsatz anwendet. Es bleibt also nur, die Eindeutigkeitsaussage in (ii) zu beweisen. Die Idee ist, Eindeutigkeitsaussagen auf die Eindeutigkeit der Dimension von Vektorräumen über den verschiedenen Körpern zurückzuführen, die mit dem Hauptidealring $R$ zusammenhängen.

- Wir beginnen mit der Eindeutigkeit des Rangs des freien Anteils. Sei $Q := \mathrm{Quot}(R)$ der Quotientenkörper von $R$. Dann ist $\mathrm{Hom}_R(M,Q)$ ein $Q$-Vektorraum. Nach der universellen Eigenschaft 1.2.2 (i) der direkten Summe ist
$$\mathrm{Hom}_R(M,Q) \cong \mathrm{Hom}_R(R/q_1R,Q) \times \cdots \times \mathrm{Hom}_R(R/q_tR,Q) \times \mathrm{Hom}_R(R,Q)^s\,.$$
Nach Satz 1.1.9 (iv) ist $\mathrm{Hom}_R(R,Q) \cong Q$. Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal von $R$. Dann ist wegen der universellen Eigenschaft des Quotientenmoduls
$$\mathrm{Hom}_R(R/\mathfrak{a},Q) \cong \{f \in \mathrm{Hom}_R(R,Q) \mid f|_{\mathfrak{a}} = 0\} \ .$$

Jeder Modulhomomorphismus $f : R \to Q$, der nicht verschwindet, ist injektiv: sei $f(1) \neq 0$. Dann folgt für alle $m \neq 0$ im Ring $R$ aus $f(m) = mf(1)$, dass auch $f(m) \neq 0$ gilt, da der Quotientenkörper $Q$ nullteilerfrei ist. Also enthält die rechte Seite nur den Nullmorphismus, so dass für $\mathfrak{a} \neq 0$ gilt

$$\mathrm{Hom}_R(R/\mathfrak{a}, Q) = 0\,.$$

Es folgt

$$s = \dim_Q \mathrm{Hom}_R(M, Q)\,,$$

also hängt der Rang $s$ des freien Anteils nicht von der Zerlegung (7) in (ii) ab.

- Wir verwenden eine ähnliche Strategie, um auch die Unabhängigkeit der Primzahlpotenzen zu zeigen. Dafür betrachten wir für jedes feste irreduzible $p \in R$ den Restklassenkörper $R/pR$.

  Sei $M$ ein $R$-Modul. Für jedes $n \geq 1$ ist der Quotient $p^{n-1}M/p^nM$ ein $(R/pR)$-Vektorraum. Definiere

  $$d_p^n(M) := \dim_{R/pR}(p^{n-1}M/p^nM)\,.$$

  Offenbar gilt

  $$d_p^n(M \oplus N) = d_p^n(M) + d_p^n(N)\,.$$

  Wir berechnen $d_p^n(M)$ in drei verschiedenen Fällen:

  1. Wir berechnen zunächst $d_p^n(R)$.
     Die Multiplikation mit $p^{n-1}$ liefert eine Surjektion, die wir mit einer kanonischen Surjektion verketten:

     $$R \overset{\cdot p^{n-1}}{\twoheadrightarrow} p^{n-1}R \twoheadrightarrow p^{n-1}R/p^nR\,.$$

     Wir bekommen dadurch einen Isomorphismus von $R/pR$-Vektorräumen

     $$R/pR \xrightarrow{\sim} p^{n-1}R/p^nR\,.$$

     Daraus schliessen wir für alle $n \in \mathbb{N}$, dass für $R$ als Linksmodul über sich selbst gilt

     $$d_p^n(R) = \dim_{R/pR}(p^{n-1}R/p^nR) = 1\,.$$

  2. Als Nächstes betrachten wir Moduln der Form $R/p^mR$.
     Für $n > m$ ist $p^{n-1}(R/p^mR) = 0$. Für $n \leq m$ finden wir ähnlich eine Surjektion

     $$\begin{aligned} R \twoheadrightarrow R/p^mR \overset{\cdot p^{n-1}}{\twoheadrightarrow}\ & p^{n-1}(R/p^mR) \twoheadrightarrow \\ & p^{n-1}(R/p^mR)/p^n(R/p^mR) \end{aligned}$$

     mit Kern $pR$. Also gilt

     $$d_p^n(R/p^mR) = \begin{cases} 0 & \text{für} \quad n > m \\ 1 & \text{für} \quad n \leq m\,. \end{cases}$$

  3. Schließlich betrachten wir Moduln der Form $R/\tilde{p}^mR$, wobei $\tilde{p}$ ein Primelement ist, das nicht zu $p$ assoziiert ist.
     Dann ist die Restklasse von $p$ eine Einheit im Restklassenring

     $$\tilde{R} := R/\tilde{p}^mR\,.$$

     Also ist die Multiplikation mit $p^n$ ein Isomorphismus auf $\tilde{R}$ und

     $$d_p^n(R/\tilde{p}^mR) = \dim_{R/pR}(\tilde{R}/\tilde{R}) = 0\,.$$

Aus diesen drei Berechnungen folgt

$$d_p^n(M) = s + |\{i \,|\, p^n \quad \text{teilt} \quad q_i\}| ,$$

so dass die Eindeutigkeit der $q_i$ bis auf Assoziiertheit und Reihenfolge aus der Eindeutigkeit der Dimensionen $d_p^n(M)$ folgt.

□

**Korollar 3.2.3.**

1. Jeder endlich erzeugte Modul $M$ über einem Hauptidealring $R$ ist direkte Summe seines Torsionsuntermoduls mit einem freien Modul,

$$M \cong \text{Tor}\ (M) \oplus R^s .$$

2. Ein endlich erzeugter torsionsfreier Modul über einem Hauptidealring ist frei. (Umgekehrt sind natürlich freie Moduln für jeden Ring torsionsfrei.)

Man beachte, dass die Zerlegung in einer direkte Summe *nicht* kanonisch ist: wohl bilden die Torsionselemente einen Untermodul, aber der freie Anteil liegt nicht als Untermodul eindeutig fest.

Wir wollen diese Strukturaussagen nun in zwei wichtigen Spezialfällen explizit machen: für abelsche Gruppen, also $\mathbb{Z}$-Moduln und für $K$-Vektorräume mit Endomorphismen, also $K[X]$-Moduln.

**Korollar 3.2.4.**
Sei $G$ eine endlich erzeugte abelsche Gruppe, also endlich erzeugte Moduln über dem Hauptidealring $\mathbb{Z}$.

1. Dann gibt es genau eine Folge von natürlichen Zahlen $d_1, d_2, \ldots, d_s \in \{0, 2, 3, 4, \ldots\}$ mit $d_i | d_{i+1}$ für $i = 1, \ldots, s-1$, derart, dass gilt

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s}$$

   Hierbei beachte man, dass $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} \ \cong\ \mathbb{Z}$ zugelassen ist.

2. Dann gibt es Primzahlpotenzen $q_1, \ldots, q_t$ und eine natürliche Zahl $r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t} \times \mathbb{Z}^r$$

   Die natürliche Zahl $r$ wird durch $G$ eindeutig festgelegt. Sie heißt auch der Rang von $G$. Die Primzahlpotenzen sind eindeutig bis auf die Reihenfolge.

Auch hier sind die freien Faktoren in den Zerlegungen nicht eindeutig als Untergruppen von $G$. Die angegebenen Isomorphismen sind *nicht* kanonisch, d.h. nicht in eindeutiger Weise ausgezeichnet.

**Betrachtung 3.2.5.**

- Sei nun $V$ ein endlich-dimensionaler $K$-Vektorraum und $A \in \text{End}_K(V)$ ein Endomorphismus. Dann ist $V$ nach Lemma 1.1.15 ein $K[X]$-Modul, der endlich erzeugt ist, da schon die Vektorraumdimension endlich ist. Aus Dimensionsgründen verschwindet der freie Anteil als $K[X]$-Modul. Wir finden daher Hauptideale $\mathfrak{a}_i = (f_i)$ wie in Theorem 3.2.2, wobei wir die Erzeuger $f_i \in K[X]$ dadurch eindeutig festlegen, dass wir fordern, dass sie normierte Polynome sind.

- Dadurch haben wir jedem Endomorphismus eine Folge normierter Polynome $f_1, \dots, f_r$ zugeordnet, die die Teilbarkeitsbeziehung $f_i | f_{i-1}$ erfüllen. Diese Polynome heißen die Invariantenteiler des Endomorphismus $A$.

- Für jede Restklasse $\overline{v} \in K[X]/\ \mathfrak{a}_i$ folgt
$$f_1.\overline{v} = \overline{f_1 \cdot v} = 0 \ ,$$
also $f_1(A) = 0$. Umgekehrt wirken auf dem Summanden $K[X]/(f_1)$ genau die Vielfachen von $f_1$ durch Null. Daher ist $f_1$ das normierte Polynom kleinsten Grades, für das $f(A) = 0$ gilt, also das Minimalpolynom von $A$.

- Wir geben noch für jeden Summanden der Gestalt $K[X]/(f)$ die Wirkung des Endomorphismus explizit an. Dazu sei
$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \, .$$
Wähle als $K$-Basis von $K[X]/(f)$ die Restklassen $b_i := \overline{X^i}$ mit $i = 0, \dots n-1$. Dann gilt $X.b_i = b_{i+1}$ für $i = 0, \dots n-2$ und $X.b_{n-1} = -\sum_{i=0}^{n-1} a_i b_i$. Wir finden also, dass die Matrix
$$B_f := \begin{pmatrix} 0 & 0 & & & -a_0 \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix} \in M(n \times n, K)$$
die sogenannte Begleitmatrix des Polynoms $f$ in der genannten Basis den Endomorphismus beschreibt. Die so erhaltene Normalform heißt auch Frobeniussche Normalform des Endomorphismus.

Der Spezialfall algebraisch abgeschlossener Körper ist besonders wichtig.

**Korollar 3.2.6** (Jordansche Normalform)**.**
Sei $K$ ein algebraisch abgeschlossener Körper, $V$ ein endlich-dimensionaler $K$-Vektorraum und $A : V \to V$ ein Endomorphismus von $V$. So gibt es eine Basis von $V$, in der $A$ blockdiagonal ist, wobei in jedem Block die Diagonaleinträge konstant sind, nur 1 auf der ersten oberen Nebendiagonale steht und sonst alle Einträge null sind.

**Beweis.**
Da $K$ algebraisch abgeschlossen ist, sind die Primelemente bis auf Assoziiertheit gegeben durch Linearfaktoren. Finde daher nach Theorem 3.2.2 (ii) einen Isomorphismus von $K[X]$-Moduln
$$V \cong K[X]/(X-\lambda_1)^{n_1} \times \cdots \times K[X]/(X-\lambda_t)^{n_t}$$
mit $n_i \in \mathbb{N}$ und $\lambda_i \in K$ für $i = 1, \dots, n$. In jedem Summanden der rechten Seite wähle als Basis die Restklassen der Polynome
$$1, (X-\lambda), (X-\lambda)^2, \dots, (X-\lambda)^{n-1} \, .$$
Wegen
$$X(X-\lambda)^i = \lambda(X-\lambda)^i + (X-\lambda)^{i+1}$$
hat die Multiplikation mit $X$, also die Wirkung von $A$ auf $V$, in der angegebenen Basis die angegebene Form. □

Ähnlich folgen Normalformen für algebraisch nicht abgeschlossene Körper, zum Beispiel für $\mathbb{R}$ (siehe etwa H.J. Kowalski, Lineare Algebra, de Gruyter, Satz 35.8).

# 4 Darstellungstheorie

## 4.1 Halbeinfache Ringe und Kategorien

Es ist nun an der Zeit, auch die Moduln über Gruppenringen endlicher Gruppen etwas näher zu untersuchen. Hierbei sei $K$ ein Körper beliebiger Charakteristik und $G$ eine endliche Gruppe; mit $R := K[G]$ bezeichnen wir den Gruppenring von $G$ über $K$.

Wir beginnen mit einer allgemeinen Definition:

***Definition 4.1.1***
*Ein Ring $R$ heißt selbstinjektiv, wenn $R$ als Linksmodul über sich selbst koregulär im Sinne von Definition 2.4.2 ist.*

Für endlich erzeugte Moduln über selbstinjektiven Ringen gilt die folgende wichtige Aussage:

**Satz 4.1.2.**
Sei $R$ ein selbstinjektiver Ring. Dann ist ein endlich erzeugter $R$-Modul genau dann projektiv, wenn er injektiv ist.

**Beweis.**
Wir betrachten die folgende Kette von Implikationen:

$$\begin{aligned} M \text{ projektiv } &\Leftrightarrow M \text{ direkter Summand in } \textstyle\bigoplus_{\text{endl.}} R \\ &\Leftrightarrow M \text{ direkter Faktor in } \textstyle\prod_{\text{endl.}} R \\ &\Leftrightarrow M \;\text{ injektiv} \end{aligned}$$

Die erste und letzte Implikation folgen dabei sofort aus Satz 2.4.4. Die Endlichkeit folgt, weil wir im Beweis von Satz 1.3.5 für einen endlich erzeugten Modul $M$ einen freien Modul von endlichem Rang wählen können. □

Unser Ziel ist der folgende Satz:

**Satz 4.1.3.**
Sei $K$ ein beliebiger Körper und $G$ eine endliche Gruppe. Dann ist der Gruppenring $R = K[G]$ selbstinjektiv. Insbesondere ist eine endlich-dimensionale $G$-Darstellung auf einem $K$-Vektorraum genau dann projektiv, wenn sie injektiv ist.

Bei diesem Satz ist sowohl wesentlich, dass $K$ ein Körper ist und auch, dass die Gruppe $G$ endlich ist. Wir beweisen zunächst

**Lemma 4.1.4.**
Sei $R$ eine $K$-Algebra. Wir bezeichnen mit $R^*$ den $R$-Modul $R^* := \mathrm{Hom}_K(R, K)$, der durch die Rechtswirkung von $R$ auf sich selbst induziert wird. Dann ist der $R$-Modul $R^*$ injektiv.

**Beweis.**
Der Beweis läuft wie in Beispiel 2.4.3.2: Wir wollen dazu die Äquivalenz der Funktoren $\mathrm{Hom}_R(-, R^*)$ und $\mathrm{Hom}_K(-, K)$ zeigen. Für einen beliebigen $R$-Modul $M$ gilt:

$$\mathrm{Hom}_R(M, R^*) \stackrel{\text{def}}{=} \mathrm{Hom}_R(M, \mathrm{Hom}_K(R, K)) \cong \mathrm{Hom}_K(R \otimes_R M, K) \cong \mathrm{Hom}_K(M, K)\,.$$

Die zweite Isomorphie folgt, da beide Räume $K$-bilineare Abbildungen $M \times R \to K$ beschreiben. Im letzten Ausdruck ist implizit ein Vergessensfunktor von $R$-Moduln auf $K$-Vektorräume.

Also haben wir die Äquivalenz von Funktoren $\mathrm{Hom}_R(-, R^*)$ und $\mathrm{Hom}_K(-, K)$. Der Funktor $\mathrm{Hom}_K(-, K)$ ist exakt, da der Körper $K$ als Modul über sich selbst injektiv ist. Man beachte, dass in diesem Schritt eingeht, dass wir den Gruppenring über einem Körper betrachten. Wegen der Isomorphie der Funktoren ist auch $\mathrm{Hom}_R(-, R^*)$ exakt, also $R^*$ ist injektiv. □

Auch die anderen Argumente von Beispiel 2.4.3 lassen sich verallgemeinern, und man schließt, dass $R^*$ koregulär ist. Der Beweis von Satz 4.1.3 folgt nun aus dem folgenden Lemma.

**Lemma 4.1.5.**
Sei $G$ eine endliche Gruppe und $R = K[G]$. Dann ist die $K$-lineare Abbildung

$$\begin{array}{rccl} \Phi: & R^* & \to & R \\ & f & \mapsto & \sum_{g\in G} f(g)g^{-1}, \end{array}$$

ein Isomorphismus von $R$-Moduln. Hierbei ist $(g)_{g\in G}$ die ausgezeichnete Basis von $K[G]$.

Insbesondere sind für den Gruppenring einer endlichen Gruppe die Moduln $R$ und $R^*$ isomorph. In Anlehnung an eine bei Hopf-Algebren übliche Terminologie nennen wir $\Phi$ die Frobenius-Abbildung.

**Beweis.**
Wir rechnen nach, dass $\Phi$ ein Morphismus von $R$-Moduln ist: für $g_0 \in G$ gilt

$$\Phi(g_0.f) = \sum_{g\in G} f(gg_0)g^{-1} = \sum_{\tilde{g}\in G} f(\tilde{g})g_0\tilde{g}^{-1} = g_0\Phi(f) \; .$$

Die Abbildung $\Phi$ ist surjektiv, denn ein Urbild von $g \in R$ ist gegeben durch $\delta_{g^{-1}} \in R^*$ mit $\delta_g(g') = \delta_{g,g'}$. Man beachte, dass die Summe deswegen sinnvoll ist, weil die Gruppe endlich ist. Also ist die Abbildung $\Phi$ ein Isomorphismus von $R$-Moduln. □

Man kann sich nun fragen, ob die Situation eintreten kann, dass *alle* Darstellungen einer endlichen Gruppe auf einem $K$-Vektorraum projektiv sind, also die Kategorie halbeinfach im Sinne von Definition 2.3.13 ist. Wir wollen Kategorien von Moduln über einem Ring, in denen alle Objekte projektiv sind, erst etwas näher untersuchen.

***Definition 4.1.6***

*(i) Ein Modul heißt halbeinfach, , wenn jeder Untermodul $U$ von $M$ ein* Komplement *$D$ besitzt, d.h. es zu jedem Untermodul $U$ einen Untermodul $D$ mit $D \oplus U = M$ gibt.*

*(ii) Ein Ring heißt halbeinfach genau dann, wenn er halbeinfach ist als Linksmodul über sich selbst.*

Jeder Vektorraum - also jeder Modul über einem Körper – ist offensichtlich halbeinfach. Über jedem Ring ist der Nullmodul $M = 0$ halbeinfach.

Da wir nur Linksmoduln benutzt haben, um zu definieren, wann ein Ring halbeinfach ist, sollte man besser von links-halbeinfach sprechen. Wir werden aber in Korollar 4.2.5 sehen, dass jeder linkshalbeinfache Ring auch rechtshalbeinfach ist.

**Satz 4.1.7.**
Sei $R$ ein Ring und $M$ ein $R$-Modul. Dann sind äquivalent:

(i) $M$ ist (innere) direkte Summe von einfachen Untermoduln.

(ii) $M$ ist eine (nicht-notwendig direkte) Summe von einfachen Untermoduln.

(iii) $M$ ist halbeinfach, also jeder Untermodul $U$ von $M$ besitzt ein Komplement $D$.

**Beweis.**

(i) $\Rightarrow$ (ii) ist klar nach Definition.

(ii) $\Rightarrow$ (iii) Sei $M = \sum\limits_{i\in I} M_i$ Summe einfacher Untermoduln $M_i$. Für jede Teilmenge $J \subset I$ bezeichnen wir die zugehörige innere Summe von Untermoduln mit

$$M_J := \sum_{i\in J} M_i\,.$$

$U$ sei der Untermodul, für den wir ein Komplement suchen. Nun finden wir mit Hilfe des Zornschen Lemmas unter allen Teilmengen $J \subset I$ mit $M_J \cap U = 0$ eine bezüglich Inklusion maximale Teilmenge $J$. Wir behaupten, dass

$$M_J + U = M$$

gilt. Diese Summe ist dann wegen der Bedingung $M_J \cap U = 0$ an die Indexmenge $J$ direkt. Wäre $M_J + U$ ein echter Untermodul von $M$, so gäbe es wenigstens ein $M_i \not\subset M_J + U$. Da der Modul $M_i$ einfach ist, ist entweder $M_i \cap (M_J + U) = M_i$ oder der Nullmodul, also

$$M_i \cap (M_J + U) = 0\,.$$

Damit gilt aber auch $(M_i + M_J) \cap U = 0$, im Widerspruch zur Maximalität von $J$.

(iii) $\Rightarrow$ (ii)

Wir überlegen uns zunächst, dass die Eigenschaft (iii) sich auch auf Untermoduln vererbt. Seien $U \subset N \subset M$ Untermoduln, $V$ ein Komplement von $U$ in $M$, so ist $V \cap N$ Komplement von $U$ in $N$.

Wir setzen nun $S$ gleich der Summe aller einfachen Untermoduln von $M$. Hat $M$ keine einfachen Untermoduln, so bedeutet dies $S = 0$. Gälte $S \neq M$, so finden wir wegen (iii) ein Komplement $D$ von $S$, das ungleich Null ist.

Angenommen also, es wäre $D \neq 0$. Sei $D \ni d \neq 0$, und $Rd$ der Untermodul von $D$, der von $d$ erzeugt ist. Die echten Untermoduln eines Moduls bilden eine nicht-leere, induktiv geordnete Menge, denn als obere Schranke einer total geordneten Teilmenge von Untermoduln können wir ihre Vereinigung nehmen. Mit Hilfe von Zorns Lemma finden wir somit im Modul $Rd$ einen maximalen Untermodul $U'$. Weil auch der Untermodul $Rd$ von $M$ die Bedingung (iii) erfüllt, finden wir ein Komplement $Rd = U' \oplus E$. Dann ist $E \cong Rd/U'$ und somit wegen der Maximalität von $U'$ nach Lemma 1.5.2.2 in $Rd$ einfach. Nach Definition von $S$ ist dann aber $E \subset S$, im Widerspruch zu $E \subset Rd \subset D$ und $D \cap S = 0$.

(ii) $\Rightarrow$ (i)

Es gilt $M = \sum_{i\in I} M_i$ mit einfachen Moduln $M_i$. Sei $X$ die Menge aller Teilmengen $J \subset I$, so dass die Summe $M_J = \sum_{j\in J} M_j$ direkt ist. Wegen $\emptyset \in X$ ist diese Menge nicht leer.

Wir zeigen, dass $X$ induktiv geordnet ist. Sei $Y$ eine total geordnete nicht-leere Teilmenge von $X$. Setze $I_0 := \cup_{I'\in Y} I'$. Wenn wir zeigen $I_0 \in X$, dann ist $I_0$ eine obere Schranke für $Y$ in $X$.

Nun ist die Summe $M_{I_0}$ genau dann direkt, wenn für jede endliche Teilmenge $I_1 \subset I_0$ die Summe direkt ist. Weil $Y$ aber total geordnet ist, gibt es zu jedem *endlichen* $I_1$ ein $I' \in Y$ mit $I_1 \subset I'$. Wegen $Y \subset X$ ist die Summe $M_{I'}$ direkt, also erst recht die kleinere Summe $M_{I_1}$. Es folgt, dass die Summe $M_{I_0}$ direkt ist, also $I_0 \in X$.

Nach dem Zornschen Lemma finden wir ein maximales Element $J \in X$ und behaupten $M_J = M$. Dazu reicht es aus, $M_i \subset M_J$ für alle $i \in I$ zu zeigen. Angenommen, dies gälte nicht für $i_0$, dann ist $M_{i_0} \cap M_J$ ein echter Untermodul von $M_{i_0}$. Weil $M_{i_0}$ einfach ist, folgt $M_{i_0} \cap M_J = 0$, also ist die Summe $M_{i_0} \oplus M_J$ direkt, im Widerspruch zur Maximalität von $J$.

□

**Korollar 4.1.8.**
Jeder Quotient und jeder Untermodul eines halbeinfachen Moduls ist halbeinfach.

**Beweis.**
Für einen gegebenen Untermodul $U \subset M$ betrachte die kanonische Surjektion $M \to M/U$. Das Bild eines einfachen Untermoduls von $M$ ist dann entweder Null oder isomorph zum einfachen Untermodul. Daher ist der Quotient $M/U$ eine Summe einfacher Untermoduln, nach Satz 4.1.7 also halbeinfach.

Wiederum nach Satz 4.1.7 finden wir ein Komplement $D$ zu $U$. Damit ist der Untermodul isomorph zu einem Quotienten, $U \cong M/D$, und nach dem vorangegangenen Resultat selbst halbeinfach. □

**Korollar 4.1.9.**
Sei $R$ ein Ring. Dann sind die folgenden Aussagen äquivalent.

1. Der Ring $R$ ist halbeinfach, d.h. als Linksmodul über sich selbst direkte Summe einfacher Untermoduln.

2. Jeder $R$-Modul ist halbeinfach, d.h. jeder $R$-Modul ist direkte Summe einfacher Untermoduln.

3. Die Kategorie $R-$Mod ist halbeinfach im Sinne von Definition 2.3.13, d.h. alle $R$-Moduln sind projektiv.

**Beweis.**

3.⇒ 2. Sei die Kategorie $R-$Mod halbeinfach und $M$ ein $R$-Modul. Für jeden Untermodul $U \subset M$ hat man eine kurze exakte Sequenz

$$0 \to U \to M \to M/U \to 0 \ ,$$

die nach Satz 1.4.7 spaltet, weil der Modul $M/U$ projektiv ist. Nach Satz 1.4.3 hat dann der Untermodul $U$ ein Komplement in $M$.

2.⇒ 1. Diese Richtung ist trivial, da 1. ein Spezialfall von 2. ist.

1.$\Rightarrow$ 3. Es ist zu zeigen, dass jeder $R$-Modul $M$ projektiv ist, also direkter Summand eines freien $R$-Moduls $F$ ist. Nach Satz 1.3.5 ist $M$ homomorphes Bild eines freien Moduls $F$, betrachte also die exakte Sequenz

$$0 \to \ker \pi \to F \xrightarrow{\pi} M \to 0$$

Der Ring $R$ ist nach Annahme halbeinfach, und somit auch $F$ als direkte Summe. Nach Satz 4.1.7 hat $\ker \pi$ ein Komplement, das isomorph zu $M$ ist, $F \cong M \oplus \ker \pi$. Also ist $M$ projektiv.

□

**Satz 4.1.10.**
Sei $R$ ein halbeinfacher Ring. Dann hat $R$ als $R$-Modul endliche Länge und jeder einfache $R$-Modul ist isomorph zu einem einfachen Untermodul von $R$. Insbesondere gibt es nur endlich viele einfache $R$-Moduln bis auf Isomorphie.

**Beweis.**
Finde eine Zerlegung von $R$ als direkte Summe einfacher $R$-Moduln, $R = \oplus M_i$ mit $M_i$ einfach. Als Ring mit Eins ist $R$ zyklisch als Modul über sich selbst mit Erzeuger $1 \in R = \oplus M_i$. Der Erzeuger kann aber nur in endlich vielen Summanden eine von Null verschiedene Komponente haben also hat $R$ endliche Länge. Für einen beliebigen einfachen Modul $M$ betrachte einen Erzeuger $x \in M$ und die Surjektion

$$\begin{array}{rcl} R \cong \oplus M_i & \to & M \\ r & \mapsto & rx \end{array}$$

Dies entspricht einer Familie $(M_i \to M)$ von Modulmorphismen. Da die Abbildung surjektiv ist, muss wenigstens eine der Abbildungen $M_i$ ungleich Null sein. Sie ist nach dem Schurschen Lemma 1.5.5 ein Isomorphismus, so dass wir $M$ mit einem Untermodul von $R$ identifizieren können. □

***Definition 4.1.11***

1. *Sei $R$ ein Ring und $M$ ein $R$-Modul. Gegeben ein einfacher $R$-Modul $E$, bezeichnen wir mit $M_E \subset M$ die Summe aller zu $E$ isomorphen Untermoduln von $M$ und nennen sie die isotypische Komponente von $M$ vom Typ $E$.*

2. *Das Erzeugnis aller einfachen Untermoduln eines Moduls heißt der Sockel von $M$ und wird mit $\mathrm{soc}(M)$ bezeichnet.*

**Satz 4.1.12** (Zerlegung in isotypische Komponenten)**.**

1. Der Sockel ist der größte halbeinfache Untermodul von $M$. Insbesondere ist ein Modul genau dann halbeinfach, wenn er gleich seinem Sockel ist.

2. Sei $R$ ein Ring und $\mathrm{irr}(R)$ ein Repräsentantensystem für die Isomorphieklassen einfacher $R$-Moduln. Dann zerfällt der Sockel $\mathrm{soc}(M)$ als direkte Summe seiner isotypischen Komponenten:

$$\mathrm{soc}(M) = \bigoplus_{E \in \mathrm{irr}(R)} M_E\,.$$

**Beweis.**

- Da der Sockel Summe einfacher Moduln ist, ist er nach Satz 4.1.7 halbeinfach.
- Da soc$(M)$ halbeinfach ist, muss nur gezeigt werden, dass die Summe der isotypischen Komponenten direkt ist, dass also gilt

  $$M_E \cap \sum_{F\neq E} M_F = 0$$

  für alle $E$. Dazu reicht es, zu zeigen, dass jeder einfache Untermodul in einer Summe einfacher Untermoduln zu einem der Summanden isomorph ist. Denn dann ist jeder einfache Untermodul von $M_E$ isomorph zu $E$, aber kein einfacher Untermodul von $\sum_{F\neq E} M_F$ kann isomorph zu $E$ sein. Also ist der Schnitt trivial.

  Sei also $E$ ein einfacher Untermodul in einer Summe $M := \sum_{j\in J} M_j$ einfacher Moduln. Da aber die Summe $\sum_{j\in J} M_j$ halbeinfach ist, ist der einfache Untermodul $E$ auch ein Quotient dieser Summe. Wie im Beweis von 4.1.10 schließt man, dass $E$ auch isomorph zu einem einfachen direkten Summanden in $M$ ist.

□

Wir können nun eine Bedingung angeben, unter der die Kategorie der Darstellungen einer endlichen Gruppe $G$ auf $K$-Vektorräumen halbeinfach ist.

**Satz 4.1.13** (Maschke)**.**
Sei $G$ eine endliche Gruppe und $K$ ein Körper, dessen Charakteristik nicht die Gruppenordnung $|G|$ teilt. Dann ist die Kategorie von Darstellungen von $G$ auf $K$-Vektorräumen halbeinfach.

Es gibt eine einfache Beweistechnik im Fall $K=\mathbb{R}$ oder $K=\mathbb{C}$; da diese oft auf andere Situationen verallgemeinert wird, behandeln wir zunächst diesen Spezialfall. Sie beruht in diesem Fall auf dem folgenden Lemma.

**Lemma 4.1.14.**
Ist $V$ eine Darstellung von $G$ über $\mathbb{R}$ oder $\mathbb{C}$ der endlichen Gruppe $G$, so gibt es auf $V$ ein $G$-invariantes Skalarprodukt, bzw. für $K=\mathbb{C}$ ein hermitesches Skalarprodukt, d.h. es gilt $(gv,gw)=(v,w)$ für alle Elemente $g\in G$.

**Beweis.**
Wir wählen auf $V$ irgendein Skalarprodukt $b: V\times V\to\mathbb{C}$, zum Beispiel, indem wir eine beliebige Basis zur Orthonormalbasis deklarieren. Dann definiert

$$(v,w) := \sum_{g\in G} b(gv,gw)$$

ein $G$-invariantes Skalarprodukt. Dieses ist offensichtlich sesquilinear und positiv definit, denn $(v,v)=\sum_{g\in G}(gv,gv)$ ist als endliche Summe positiver reeller Zahlen positiv. Die $G$-Invarianz folgt aus

$$(gv,gw) = \sum_{\tilde g\in G} b(\tilde g gv,\tilde g gw) = (v,w) \quad .$$

□

**Beweis.**
des Satzes von Maschke 4.1.13 für $K = \mathbb{R}$ oder $K = \mathbb{C}$ und Darstellungen endlicher Dimension. Ist $W \subset V$ eine Unterdarstellung, so existiert ein orthogonales Komplement $W^\perp \subset V$, weil $V$ endlich-dimensional ist. Unter einem invarianten Skalarprodukt ist $W^\perp$ eine Unterdarstellung: denn aus $(v, w) = 0$ für alle $w \in W$ folgt wegen der Invarianz auch $(gv, w) = (v, g^{-1}w) = 0$, für alle $g \in G$ und $w \in W$. Wir haben also die folgende orthogonale Zerlegung in Unterdarstellungen:

$$V = W \oplus W^\perp .$$

Da Komplemente existieren, folgt die Halbeinfachheit aus Satz 4.1.7. □

Diese Technik heißt auch "Weyls Unitaritätstrick". Im Falle unendlich-dimensionaler Skalarproduktsräume muss man zusätzlich die Vollständigkeit des Unterraums $W$ voraussetzen, damit ein orthogonales Komplement existiert. Der allgemeine Fall, d.h. allgemeinere Körper und auch Darstellungen unendlicher Dimension, braucht mehr Begriffe, die wir jetzt einführen.

**Beweis.**
des Satzes von Maschke 4.1.13 im allgemeinen Fall. Es reicht wieder nach Satz 4.1.7 zu zeigen, dass jeder Untermodul $W$ von $V$ ein Komplement besitzt.

- Ist $i : W \hookrightarrow V$ eine Unterdarstellung, so finden wir eine Retraktion in der Kategorie von $K$-Vektorräumen, d.h. eine $K$-lineare Abbildung

  $$\pi \,:\, V \to W$$

  so dass $\pi \circ i = \mathrm{id}_W$. Das Problem ist, dass $\pi$ nur eine Abbildung von Vektorräumen, aber nicht von $G$-Darstellungen ist. Die Idee ist nun, die Abbildung durch Mittelung über die Gruppe $G$ so zu verbessern, dass sie mit der Wirkung von $G$ vertauscht. Betrachte daher die Abbildung $\psi :\ V \to W$:

  $$\psi = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1}$$

  Diese Definition macht natürlich nur dann Sinn, wenn die Charakteristik von $K$ die Gruppenordnung nicht teilt. Man vergleiche den Ausdruck mit dem Beweis von Satz 4.1.3, wo auch eine Summe über Gruppenelemente auftritt, bei der $g$ und $g^{-1}$ paarweise auftreten.

- Wir rechnen nun für $h \in G$ beliebig:

  $$h \circ \psi = \frac{1}{|G|} \sum_{g \in G} hg \circ \pi \circ g^{-1} = \frac{1}{|G|} \sum_{\tilde{g} \in G} \tilde{g} \circ \pi \circ \tilde{g}^{-1} h = \psi \circ h \ ,$$

  wobei wir substituierten $\tilde{g} := hg$. Also ist $\psi \in \mathrm{Hom}_G(V, W)$. Außerdem gilt weiterhin

  $$\psi \circ i = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1} \circ i = \sum_{g \in G} \frac{1}{|G|} g \circ \pi \circ i \circ g^{-1} = \mathrm{id}_W \ ,$$

  wobei wir in der zweiten Gleichheit ausnutzten, dass $i$ ein $G$-Morphismus ist, und im dritten Schritt $\pi \circ \iota = \mathrm{id}_W$. Hier wird auch klar, warum wir durch die Gruppenordnung $|G|$ dividieren mussten, was eine Einschränkung an die Charakteristik des Körpers liefert.

- Nach Satz 1.4.3 ist nun $V$ die innere direkte Summe von $\iota(W)$ und $\ker \psi$.

□

Damit ist im allgemeinen Fall, wenn $\mathrm{char}(K)$ nicht die Gruppenordnung $|G|$ teilt, das Verständnis der Darstellungstheorie einer endlichen Gruppe $G$ auf $K$-Vektorräumen reduziert auf das Verständnis einfacher Darstellungen und damit nach Satz 4.1.10 auf das Verständnis der Zerlegung des Gruppenrings in einfache Linksmoduln.

## 4.2 Strukturtheorie halbeinfacher Ringe

Halbeinfache Ringe bzw. halbeinfache Algebren über einem Körper können ganz explizit beschrieben werden. Diese Beschreibung werden wir bei der Untersuchung von halbeinfachen Gruppenringen im nächsten Abschnitt verwenden.

Wir erinnern an das Schursche Lemma 1.5.5: jeder Homomorphismus $\Phi : M_1 \to M_2$ ist injektiv oder Null, wenn $M_1$ einfacher Modul ist, und ist surjektiv oder Null, wenn $M_2$ einfacher Modul ist.

**Korollar 4.2.1.**

1. Für jeden einfachen $R$-Modul $M$ ist der Endomorphismenring $\mathrm{End}_R(M)$ ein Divisionsring, d.h. ein Ring, in dem jedes von Null verschiedene Element ein multiplikatives Inverses hat.

2. Homomorphismen zwischen halbeinfachen Moduln erhalten die isotypische Komponente.

3. Wenn $R$ kommutativ ist, ist für jedes Ideal $I \subset R$ der Quotient $R/I$ ein Ring. Dann gilt die Isomorphie von Ringen

$$\mathrm{End}_R(R/I) \cong \mathrm{End}_{R/I}(R/I) \cong R/I \ .$$

   Der Modul $R/I$ ist genau dann einfach, wenn das Linksideal $I$ maximal ist, cf. Lemma 1.5.2. Der Endomorphismenring eines einfachen Moduln über einem *kommutativen* Ring ist also sogar ein Körper.

Ein endlich erzeugter halbeinfacher Modul $M$ hat stets endliche Länge. Denn sei $e_1, \ldots e_n$ ein endliches Erzeugendensystem von $M$. Jeder der endlich vielen Erzeuger hat nur in endlich vielen Summanden der Zerlegung $M \cong M_1 \oplus \ldots \oplus M_r$ in einfache Moduln eine von Null verschiedene Komponente. Es können also nur endlich viele Komponenten getroffen werden.

**Satz 4.2.2.**
Sei $R$ ein Ring und $M$ ein endlich erzeugter halbeinfacher $R$-Modul. Dann ist der Endomorphismenring $\mathrm{End}_R(M)$ isomorph zu einem endlichen Produkt von Matrizenringen über Divisionsringen.

**Beweis.**
Da der Modul $M$ halbeinfach ist, betrachte nach Satz 4.1.12 die Zerlegung $M \cong \oplus_{i=1}^k M_i^{n_i}$ in isotypische Komponenten mit $n_i \in \mathbb{N}$ und $M_i$ paarweise nicht isomorphen einfachen $R$-Moduln. Da der Modul endlich erzeugt ist, ist dies eine endliche direkte Summe. Dann gilt

$$\mathrm{End}_R(M) = \oplus_{ij}\mathrm{Hom}(M_i^{n_i}, M_j^{n_j}) \cong \oplus_i M(n_i \times n_i, \mathrm{End}_R(M_i)) \ .$$

Nach Korollar 4.2.1.1 aus dem Schurschen Lemma ist $\mathrm{End}_R(M_i)$ ein Divisionsring. □

**Theorem 4.2.3** (Theorem von Wedderburn).
Jeder halbeinfache Ring $R$ ist isomorph zu einem endlichen Produkt von Matrizenringen über Divisionsringen. Ist $R$ kommutativ, so ist jeder halbeinfache Ring $R$ isomorph zu einem endlichen Produkt von Körpern.

**Beweis.**
Da $R$ halbeinfach ist, hat $R$ als Linksmodul über sich selbst nach Satz 4.1.10 endliche Länge. Daher ist nach Satz 4.2.2

$$\mathrm{End}_R(R) \cong \prod_i M(n_i \times n_i, D_i)$$

für gewisse $n_i \in \mathbb{N}$ und gewisse Divisionsringe $D_i$. Es gibt aber für jeden Ring $R$ einen Isomorphismus durch Rechtsmultiplikation,

$$\begin{array}{ccc} R^{\mathrm{opp}} & \xrightarrow{\sim} & \mathrm{End}_R(R) \\ r & \mapsto & (\varphi_r : \; x \mapsto xr) \end{array}$$

und daher

$$R \cong (R^{\mathrm{opp}})^{\mathrm{opp}} \cong \prod_i M(n_i \times n_i, D_i)^{\mathrm{opp}} \cong \prod_i M(n_i \times n_i, D_i^{\mathrm{opp}}) \ ,$$

wobei die letzte Isomorphie durch Transposition der $n_\times n_i$-Matrizen folgt. □

**Bemerkung 4.2.4.**
Die Zerlegung eines halbeinfachen Rings $R$

$$R \cong \prod_i M(n_i \times n_i, D_i)$$

ist eindeutig bis auf Reihenfolge.

**Korollar 4.2.5.**
Ein Ring ist genau dann rechts-halbeinfach, wenn er links-halbeinfach ist.

Arbeiten wir statt mit allgemeinen Ringen mit Algebren über Körpern, so können wir für einen algebraisch abgeschlossenen Körper $K$ die halbeinfachen $K$-Algebren explizit angeben. Dafür brauchen wir das folgende Lemma:

**Lemma 4.2.6.**
Sei $F$ ein algebraisch abgeschlossener Körper. Wenn $D$ eine endlich-dimensionale Divisionsalgebra über dem Körper $F$ ist, so gilt $D = F$.

**Beweis.**
Für jedes Element $x \in D$ ist die Familie $(1, x, \ldots x^m)$ mit $m := \dim_F D$ linear abhängig über dem Körper $F$. Es gibt also ein normiertes Polynom $f \in F[X]$ mit $f(x) = 0$. Wir wählen ein solches Polynom $f$ von minimalen Grad. Wäre $f$ reduzibel, $f = f_1 \cdot f_2$, so würde $0 = f_1(x) \cdot f_2(x)$ gelten mit nicht-konstanten Polynomen strikt kleineren Grads als $f$. Da $D$ eine Divisionsalgebra ist, folgt daraus $f_1(x) = 0$ oder $f_2(x) = 0$. Dies ist im Widerspruch zur Minimalitätsannahme für $f$.

Da $F$ algebraisch abgeschlossen ist, ist $f$ als irreduzibles Polynom ein Linearfaktor, $f(X) = X - a$ mit $a \in F$. Daher ist $x = a$ und daher $D = F$. □

Über dem algebraisch nicht abgeschlossenen Körper $\mathbb{R}$ dagegen gibt es verschiedenen Divisionsalgebren: die Körper $\mathbb{R}$ und $\mathbb{C}$ und die Quaternionen $\mathbb{H}$ als nicht-kommutative Divisionsalgebra.

Es folgt nun unmittelbar aus Theorem 4.2.3:

**Korollar 4.2.7.**
Sei $K$ ein algebraisch abgeschlossener Körper. Jede halbeinfache $K$-Algebra ist isomorph zu einem endlichen Produkt von Matrizenringen mit Einträgen in $K$.

Wir ziehen mit Hilfe von Lemma 4.2.6 gleich eine einfache Folgerung aus dem Schurschen Lemma 4.2.1.1:

**Korollar 4.2.8.**
Sei $K$ ein algebraisch abgeschlossener Körper und $R$ eine $K$-Algebra. Sei $M$ ein einfacher $R$-Modul endlicher Dimension. Dann ist

$$\begin{array}{rcl} K & \xrightarrow{\sim} & \mathrm{End}_R(M) \\ \lambda & \mapsto & \lambda \mathrm{id}_M \end{array}$$

ein Isomorphismus.

**Beweis.**
Da $K$ ein Körper ist, wissen wir, dass die Abbildung injektiv ist. Andererseits ist $\mathrm{End}_R(M)$ als Divisionsalgebra über dem algebraisch abgeschlossenen Körper $K$ nach Lemma 4.2.6 isomorph zu $K$. Somit ist die $K$-lineare Abbildung auch surjektiv. □

Wir wollen aus dem Theorem von Wedderburn 4.2.3 auch die Darstellungstheorie halbeinfacher Ringe ablesen.

**Korollar 4.2.9.**
Die Isomorphieklassen von einfachen Darstellungen eines halbeinfachen Rings sind in Bijektion zu den einzelnen Faktoren; nur der entsprechende Faktor wirkt auf der einfachen Darstellung nicht durch Null. Zum Faktor $M(n_i \times n_i, D_i)$ gehört eine einfache Darstellung, die durch Multiplikation der Matrix mit einem Spaltenvektor in $(D_i)^n$ definiert ist.

## 4.3 Fouriertransformation für Gruppen

Wir wollen nicht von vornherein voraussetzen, dass die Gruppenalgebra einer endlichen Gruppe $G$ über einem Körper $K$ halbeinfach ist, und brauchen daher ein weiteres Hilfsmittel. Sei $M$ ein $R$-Modul. Dann ist $M$ auch ein Modul über dem Ring $\mathrm{End}_R(M)$:

$$\begin{array}{rcl} \mathrm{End}_R(M) \times M & \to & M \\ (\varphi, m) & \mapsto & \varphi(m)\ . \end{array}$$

Jedes Ringelement $x \in R$ gibt durch Skalarmultiplikation

$$\begin{array}{rrcl} \lambda_x : & M & \to & M \\ & m & \mapsto & x.m \end{array}$$

ein Element von $\mathrm{End}(M)$, das natürlich mit jedem $\varphi \in \mathrm{End}_R(M)$ vertauscht, also in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ liegt. Wir haben insbesondere einen Ringhomomorphismus

$$\varphi_{\mathrm{Jac}} : R \to \mathrm{End}_{\mathrm{End}_R(M)}(M)\,.$$

**Satz 4.3.1.** (Jacobsonscher Dichtesatz)
Sei $R$ ein Ring und $M$ ein *halbeinfacher* $R$-Modul. Wir geben uns $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ und endlich viele Elemente $m_1, \ldots, m_r \in M$ des halbeinfachen Moduls vor. Dann gibt es stets ein $x \in R$ mit $f(m_i) = xm_i$ für alle $i$.

Diese Aussage wird oft zusammengefasst, indem man sagt, dass das Bild $\varphi_{\mathrm{Jac}}(R)$ in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ dicht sei: Wir können also die Wirkung jedes Morphismus $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ auf endlich vielen Elementen des Moduls wiedergeben durch die Multiplikation mit einem Skalar $x \in R$.

**Beweis.**
Wir betrachten zunächst den Fall $r = 1$, also eines Elements $m_1 \in M$. Da $M$ halbeinfach ist, hat der Untermodul $Rm_1 \subset M$ nach Satz 4.1.7 ein Komplement $D$. Betrachte also eine Zerlegung

$$M = Rm_1 \oplus D \ .$$

Die idempotente Abbildung

$$\pi : M \twoheadrightarrow Rm_1 \hookrightarrow M,$$

die als Verkettung von kanonischer Surjektion und kanonischer Injektion definiert ist, liegt im Endomorphismenring $\mathrm{End}_R(M)$. Da $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ liegen soll, gilt

$$f \circ \pi = \pi \circ f\,,$$

also gilt

$$f(m_1) = f \circ \pi(m_1) = \pi \circ f(m_1)\,.$$

Daraus folgt $f(m_1) \in Rm_1$. Es gibt also ein Element $x \in R$, so dass

$$f(m_1) = xm_1\,.$$

Für den allgemeinen Fall $r > 1$ betrachten wir die endliche direkte Summe

$$(m_1, \ldots, m_r) \in M \oplus \ldots \oplus M \ ,$$

die ein halbeinfacher $R$-Modul ist, und die Abbildung

$$f \times f \times \ldots \times f\,,$$

die in der Tat mit allen Elementen von

$$\mathrm{End}_R(M \oplus \ldots \oplus M) \cong M(r \times r, \mathrm{End}_R M)$$

kommutiert und wenden den Fall $r = 1$ an. □

**Korollar 4.3.2** (Satz von Wedderburn)**.**
Ist $K$ ein *algebraisch abgeschlossener* Körper und ist $A$ ein Teilring von $M(n \times n, K)$, so dass $K^n$ einfach ist als $A$-Modul, so ist $A$ schon der ganze Matrizenring,

$$A = M(n \times n, K)\,.$$

**Beweis.**
Da $K$ algebraisch abgeschlossen ist und $K^n$ ein einfacher $A$-Modul sein soll, ist nach dem Korollar 4.2.8 aus dem Schurschen Lemma $\mathrm{End}_A(K^n) \cong K$. Als einfacher $A$-Modul ist $K^n$ auch halbeinfach; nach dem Dichtesatz 4.3.1 ist nun $A$ dicht in $\mathrm{End}_{\mathrm{End}_A(K^n)}(K^n) = \mathrm{End}_K(K^n)$. Da $K^n$ von endlich vielen $m_i \in K^n$ als $K$-Vektorraum erzeugt wird, reicht es, die lineare Abbildung auf endlich vielen Werten festzulegen. Es folgt die Surjektivität von $\varphi_{\mathrm{Jac}} : A \to \mathrm{End}_K(K^n)$. $\square$

**Bemerkung 4.3.3.**
Man kann den Satz von Wedderburn auch koordinatenfrei formulieren: Ist $K$ ein algebraisch abgeschlossener Körper und $V$ ein endlich-dimensionaler $K$-Vektorraum und $A \subset \mathrm{End}_K(V)$ ein Teilring derart, dass $V$ einfach ist als $A$-Modul, so gilt bereits $A = \mathrm{End}_K(V)$. In dieser Sprache lässt sich die Notwendigkeit der Bedingung "algebraisch abgeschlossen" besonders gut einsehen: ist $K \subset L$ eine endliche Körpererweiterung und betrachten wir den Teilring $L \subset \mathrm{End}_K(L)$, wobei ein Element aus $L$ durch Linksmultiplikation auf $L$ wirkt. Dann ist $L$ als Körper ein einfacher $L$-Modul über sich selbst, aber im Fall $K \neq L$ gilt schon aus Dimensionsgründen $L \neq \mathrm{End}_K(L)$.

**Korollar 4.3.4.**
Sei $K$ ein algebraisch abgeschlossener Körper und $V$ eine irreduzible endlich-dimensionale Darstellung der Gruppe $G$ über $K$. So definiert die Operation von $G$ auf $V$ eine Surjektion

$$K[G] \twoheadrightarrow \mathrm{End}_K(V)$$

**Beweis.**
Wende den Satz von Wedderburn, Korollar 4.3.2, auf das Bild von $K[G]$ in $\mathrm{End}_K(V)$ an. $\square$

**Satz 4.3.5** (Fouriertransformation)**.**
Sei $K$ ein algebraisch abgeschlossener Körper beliebiger Charakteristik und $G$ eine endliche Gruppe. Seien $L_1, \ldots, L_r$ Repräsentanten der Isomorphieklassen irreduzibler Darstellungen von $G$

(i) Die Operation von $G$ definiert eine Surjektion von Ringen

$$F : K[G] \twoheadrightarrow (\mathrm{End}_K L_1) \times \cdots \times (\mathrm{End}_K L_r)\,. \tag{8}$$

(ii) Teilt die Charakteristik des Körpers $K$ nicht die Gruppenordnung $|G|$, so ist dies sogar ein Isomorphismus von Ringen.

**Beweis.**
(i) Der halbeinfache $K[G]$-Modul $M := L_1 \oplus \cdots \oplus L_r$ hat, da $K$ abgeschlossen ist, den Endomorphismenring

$$\mathrm{End}_{K[G]}(L_1 \oplus \cdots \oplus L_r) = K \times K \times \cdots \times K\,.$$

Somit ist

$$\mathrm{End}_{\mathrm{End}_{K[G]}}(M) = \mathrm{End}_{K \times \ldots K}(M) = \mathrm{End}_K(L_1) \times \ldots \mathrm{End}_K(L_r)$$

und die Surjektivität folgt wieder aus dem Dichtesatz 4.3.1.

(ii) Teilt die Charakteristik von $K$ nicht die Gruppenordnung, so ist nach dem Satz von Maschke 4.1.13 der Gruppenring $K[G]$ halbeinfach, also direkte Summe einfacher Unterdarstellungen. Dann folgt die Isomorphie aus dem Theorem von Wedderburn 4.2.3. Alternativ betrachtet man $a \in K[G]$ im Kern der Surjektion. Dann ist auch die Linksmultiplikation mit $a$ die Nullabbildung auf jedem einfachen Modul, und somit auch auf jedem halbeinfachen Modul und damit insbesondere auf dem regulären Modul $K[G]$. Daraus folgt mit $a = \sum \lambda_g g$ auch $ae = 0$, also $\lambda_g = 0$ für alle Gruppenelemente $g \in G$, mithin $a = 0$.

□

Offensichtlich ist es ein wichtiges Ziel, für einen gegebenen Körper $K$ und eine gegebene Gruppe $G$ alle irreduziblen Darstellungen zu beschreiben. (Man möchte dann auch noch Tensorprodukte von Darstellungen beschreiben können.) Man beachte, dass diese Information nicht ausreicht, um den Gruppenring als Ring zu kennen, wenn dieser nicht halbeinfach ist, also wenn $\mathrm{char}(K)$ die Gruppenordnung $|G|$ teilt. In allen anderen Fällen, insbesondere in Charakteristik Null, reicht aber diese Information aus. Wir wollen erste Informationen über irreduzible Darstellungen im halbeinfachen Fall sammeln.

Aus Satz 4.3.5 folgt sofort:

**Korollar 4.3.6.**
Sei $K$ ein algebraisch abgeschlossener Körper und $G$ eine endliche Gruppe, deren Gruppenordnung nicht durch die Charakteristik von $K$ geteilt wird. Seien $L_1, \ldots, L_r$ Repräsentanten der Isomorphieklassen einfacher Darstellungen. Dann gilt

$$|G| = (\dim_K L_1)^2 + (\dim_K L_2)^2 + \cdots + (\dim_K L_r)^2$$

**Korollar 4.3.7.**
Unter den gleichen Voraussetzungen gilt: Es gibt bis auf Isomorphie genauso viele einfache Darstellungen von $G$ wie Konjugationsklassen in $G$.

**Beweis.**
Das Zentrum $Z(R)$ eines Ringes ist

$$Z(R) := \{z \in R \,|\, za = az \quad \text{für alle } a \in R\}\,.$$

Es ist ein kommutativer Teilring von $R$. Achtung: im allgemeinen ist das Zentrum $Z(K[G])$ des Gruppenrings $K[G]$ einer Gruppe $G$ etwas anderes als der Gruppenring des Zentrums $Z(G)$ der Gruppe; es gilt aber $K[Z(G)] \subseteq Z(K[G])$.

Nach Satz 4.3.5 ist für den Gruppenring einer endlichen Gruppe $\dim_K Z(K[G])$ gleich der Zahl inäquivalenter irreduzibler Darstellungen,

$$\dim_K Z(K[G]) = \ |\text{Isoklassen einfacher Darstellungen}|\ .$$

Für ein Element im Zentrum $Z(K[G])$ des Gruppenrings machen wir den Ansatz $z = \sum\limits_h \lambda_h \delta_h$ mit $\lambda_h \in K$. Durch den Vergleich von

$$\begin{aligned} zg &= \sum_{h\in G} \lambda_h h \cdot g = \sum_{h \in G} \lambda_{hg^{-1}} h \\ gz &= \sum_{h\in G} \lambda_{g^{-1}h} h\,. \end{aligned}$$

finden wir $\lambda_{ghg^{-1}} = \lambda_h$ für alle $g, h \in G$. Man muss also nur für jede Konjugationsklasse von $G$ einen Wert für den Koeffizienten wählen, daher ist auch

$$\dim_K Z(K[G]) = \ |\text{Konjugationsklassen}|\ .$$

Durch Vergleich der beiden Formeln für $\dim_K Z(K[G])$ ergibt sich die Behauptung des Korollars. □

**Bemerkung 4.3.8.**
Wir wollen noch die Beziehung zur Fouriertransformation erklären. Betrachten wir dafür die abelsche Gruppe aller komplexen Zahlen vom Betrag Eins,

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}\,.$$

Man kann zeigen, dass alle irreduziblen, stetigen, endlich-dimensionalen Darstellungen eindimensional sind und Repräsentanten für alle Isomorphieklassen beschrieben werden durch den Gruppenhomomorphismus

$$\begin{array}{rccl} L_n: & S^1 & \to & \mathrm{GL}(1,\mathbb{C}) \cong \mathbb{C}^\times \qquad \text{für } n \in \mathbb{Z}\,. \\ & z & \mapsto & z^n \end{array}$$

Als Analogon des Gruppenrings betrachten wir stetige komplexwertige Funktionen auf $S^1$, $C^0(S^1)$, die wir natürlich mit den periodischen Funktionen auf $\mathbb{R}$ identifizieren dürfen. Das Produkt ist hierbei durch die Faltung

$$f| * g(h) = \int f(hx)g(x^{-1})\mathrm{d}x$$

gegeben, vgl. Definition 1.1.16. Die stetige Funktion $f \in C^0(S^1)$ operiert auf einer stetigen endlich-dimensionalen Darstellung $V$ durch

$$fv = \int_{S^1} f(z)\rho_V(z)(v)\,dz \qquad \text{für} \qquad v \in V$$

insbesondere also auf der irreduziblen Darstellung $L_n$ durch Multiplikation mit

$$\int_{S^1} f(z)z^n\,\mathrm{d}z \in \mathbb{C}\ ,$$

was genau die Fourierkoeffizienten von $f$ sind. Die Abbildung aus Satz 4.3.5

$$C^0(S^1) \xrightarrow{\sim} \prod_{n\in\mathbb{Z}} \mathrm{End}_{\mathbb{C}} L_n \cong \prod_{n\in\mathbb{Z}} \mathbb{C}$$

ordnet einer Funktion $f \in C^0(S^1)$ also gerade die Folge ihrer Fourierkoeffizienten zu.

## 4.4 Charaktere

In diesem Abschnitt sei $K$ ein algebraisch abgeschlossener Körper und $G$ eine endliche Gruppe, so dass $\operatorname{char} K$ die Gruppenordnung $|G|$ nicht teilt. Es gilt dann nach Satz 4.3.5 die Isomorphie von Ringen

$$F: K[G] \xrightarrow{\sim} (\mathrm{End}_K L_1) \times \cdots \times (\mathrm{End}_K L_r)\,.$$

***Definition 4.4.1***
*Sei $L$ eine einfache Darstellung von $G$. Wegen des Isomorphismus aus Satz 4.3.5 gibt es genau ein Element $e_L \in K[G]$, das durch die Identität auf $L$ operiert und durch Null auf jeder einfachen Darstellung $M$ von $G$, die nicht zu $L$ isomorph ist:*

$$e_L : M \to M = \begin{cases} \mathrm{id}_M & \textit{falls} \quad M \cong L \\ 0 & \textit{falls} \quad M \textit{ einfach}, \ M \ncong L \end{cases}$$

*Dieses Element*

$$e_L = F^{-1}\Big(\mathrm{id}_{\mathrm{End}_K L}\Big) \in K[G]$$

*heißt Projektor oder Idempotent zur einfachen Darstellung $L$.*

**Lemma 4.4.2.**
Seien $(L_i)_{i=1\ldots r}$ Repräsentanten der Isomorphieklassen irreduzibler Darstellungen von $G$ und $e_i \in K[G]$ die zugehörigen idempotenten Elemente des Gruppenrings. Dann gilt

$$e_i \cdot e_j = \delta_{ij} e_i$$
$$1 = e_1 + \cdots + e_r$$

und die Familie $(e_i)_{i=1,\ldots r}$ der idempotenten Elemente bildet eine Basis des Zentrums von $K[G]$.

**Beweis.**
folgt sofort aus Satz 4.3.5 über die Fouriertransformation. □

Wir wollen die Idempotenten explizit angeben und brauchen dafür die folgende Definition:

***Definition 4.4.3***
*Für eine endlich-dimensionale Darstellung einer Gruppe $G$ auf einem $K$-Vektorraum $V$ definiert man ihren Charakter*

$$\chi_V : G \to K$$

*durch $\chi_V(g) = \mathrm{Tr}_V\, g \equiv \mathrm{Tr}_V\, \rho(g)$ als Funktion auf der Gruppe $G$ und somit auf der ausgezeichneten Basis der Gruppenalgebra $K[G]$. Man kann diese Funktion zu einer Linearform auf dem Gruppenring fortsetzen, die wir ebenfalls mit $\chi_V \in K[G]^*$ bezeichnen:*

$$\chi_V : \quad K[G] \to K$$

*Es gilt wegen der Linearität der Spur $\chi_V(h) = \mathrm{Tr}_V h$ für jedes $h \in K[G]$.*

**Beispiel 4.4.4.**
Die Gruppenalgebra $K[G]$ ist, wie jeder Ring, ein Modul über sich selbst, der sogenannte reguläre Modul. Explizit ist diese diese Linkswirkung gegeben durch

$$\begin{aligned} \rho(g) : K[G] &\to K[G] \\ \rho(g)\Big(\sum_{h \in G} \lambda_h h\Big) &= \sum_{h \in G} \lambda_h \, gh\,. \end{aligned}$$

Damit berechnen wir den Charakter des regulären Moduls zu

$$\chi_{K[G]}(g) = \mathrm{Tr}_{K[G]} \rho(g) = \begin{cases} |G| & \text{für } g = e \\ 0 & \text{sonst.} \end{cases}$$

Wir erinnern ferner an den Isomorphismus von $K[G]$-Moduln aus Lemma 4.1.5, die Frobenius-Abbildung:

$$\begin{array}{rcl} \Phi: \ K[G]^* & \to & K[G] \\ f & \mapsto & \sum_{g\in G} f(g)g^{-1} \,. \end{array}$$

**Theorem 4.4.5** (Charakter-Projektor-Formel)**.**
Zwischen dem Charakter $\chi_L \in K[G]^*$ und dem Projektor $e_L \in K[G]$ zu einer einfachen Darstellung $L$ stellt die Frobenius-Abbildung $\Phi$ die Beziehung

$$e_L = \frac{\dim_K L}{|G|}\, \Phi(\chi_L)$$

her.

**Beweis.**
Für jeden $K[G]$-Modul $M$ haben wir einen Ringhomomorphismus $K[G] \to \mathrm{End}_K(M)$ und können somit eine Abbildung

$$\tau_M : \quad K[G]^* \xrightarrow{\Phi} K[G] \to \mathrm{End}_K(M)$$

betrachten. Für eine beliebige Funktion $f \in K[G]^*$ finden wir mit Hilfe des Charakters des regulären Moduls aus Beispiel 4.4.4

$$(*) \qquad \mathrm{Tr}_{\,K[G]} \big(\rho(g)\tau_{K[G]}(f)\big) = \sum_{h\in G} f(h) \mathrm{Tr}_{\,K[G]}\; gh^{-1} = |G| f(g) \ .$$

Wir suchen diejenige Funktion $f_i \in K[G]^*$, deren Bild unter der Frobenius-Abbildung $\Phi$ der $i$-te Projektor ist, $\Phi(f_i) = e_i$. Für diese Funktion gilt für jeden $K[G]$-Modul $L$ die Gleichung $\tau_L(f_i) = \rho_L(e_i)$.

Indem wir erst Gleichung $(*)$ und dann im zweiten Schritt den Isomorphismus aus Satz 4.3.5 anwenden, finden wir

$$\begin{aligned} f_i(g) &= \frac{1}{|G|} \mathrm{Tr}_{\,K[G]} \rho(g)\tau_{K[G]}(f_i) \\ &= \frac{1}{|G|} \sum_{j=1}^{r} \mathrm{Tr}_{\,\mathrm{End}_K(L_j)} (\rho_{L_j}(g))_* \circ \rho_{L_j}(e_i)_* \ . \end{aligned} \tag{9}$$

Die rechte Seite wertet man leicht mit Hilfe des folgenden elementaren Lemmas aus der linearen Algebra aus: □

**Lemma 4.4.6.**
Ist $L$ ein endlich-dimensionaler $K$-Vektorraum und $A : L \to L$ eine $K$-lineare Abbildung, so gilt für die Spur der durch Präkomposition induzierten Abbildung

$$\begin{array}{rcl} A_* : \ \mathrm{End}_K L & \to & \mathrm{End}_K L \\ \varphi & \mapsto & A \circ \varphi \end{array}$$

die Beziehung

$$\mathrm{Tr}_{\,\mathrm{End}_K L} A_* = \dim_K L \cdot \mathrm{Tr}_{\,L} A$$

**Beweis.**
Ohne Beschränkung der Allgemeinheit sei $L = K^n$. Dann ist $\mathrm{End}_K(K^n) \cong M(n \times n, K)$. Die zu $A$ gehörige Matrix muss von links mit einer beliebigen $n \times n$ Matrix multipliziert werden. Dabei multipliziert man jeden Spaltenvektor dieser Matrix für sich mit $A$. Also operiert $A_*$ auf jeder Spalte der $n \times n$-Matrix wie $A$ auf $K^n$ selbst. Daher ist die Matrix von $A_*$ blockdiagonal mit $n$ Blöcken der Gestalt $A$. □

Weiter im **Beweis** von Satz 4.4.5:
Aus Gleichung (9) folgt sofort

$$f_i(g) = \sum_{j=1}^{r} \frac{\dim_K L_j}{|G|} \mathrm{Tr}_{\,L_j}(\rho(g)) \circ \rho_{L_j}(e_i) = \frac{\dim_K L_i}{|G|} \chi_i(g) \,. \qquad \square$$

**Bemerkungen 4.4.7.**
Aus den aus der linearen Algebra bekannten Eigenschaften der Spur folgt sofort:

(i) Der Charakter ist auf Konjugationsklassen konstant, also eine Klassenfunktion:

$$\chi_L(ghg^{-1}) = \chi_L(h) \quad \text{für alle} \quad g, h \in G$$

Wir fassen durch lineare Fortsetzung den Raum der Klassenfunktionen als einen Untervektorraum des Dualraums $K[G]^*$ auf.

(ii) Sind $V$ und $W$ Darstellungen von $G$, so gilt für ihre direkte Summe $\chi_{V\oplus W} = \chi_V + \chi_W$.

(iii) Sind $V$ und $W$ jeweils $G$-Darstellungen, so wird das Tensorprodukt der Vektorräume $V \otimes_K W$ zur $G$-Darstellung durch

$$g(v \otimes w) := (gv) \otimes (gw) \,.$$

Es gilt

$$\chi_{V\otimes W} = \chi_V \cdot \chi_W \,.$$

Warnung: dieses Tensorprodukt sollte nicht verwechselt werden mit dem Tensorprodukt $V \otimes_{K[G]} W$, das lediglich die Struktur eines $K$-Vektorraums trägt und in diesem Fall ein Quotient des Vektorraums $V \otimes_K W$ ist.

(iv) Für eine $G$-Darstellung $V$ nennen wir den Dualraum $V^* = \mathrm{Hom}_K(V, K)$ mit der Wirkung

$$(g\lambda)(v) = \lambda(g^{-1}v) \quad \text{für } \lambda \in V^*, g \in G \,, v \in V$$

die kontragrediente Darstellung. Es gilt

$$\chi_{V^*}(g) = \chi_V(g^{-1}) \,.$$

Um mehr über Charaktere zu lernen, definieren wir auf $K[G]^*$ ein weiteres Produkt, indem wir die Frobenius-Abbildung zum Morphismus von Algebren

$$K[G]^* \to K[G]^{\mathrm{opp}}$$

erklären. Dieses Produkt ist im Allgemeinen nicht kommutativ.

***Definition 4.4.8***
*Für zwei Funktionen $f_1, f_2 \in K[G]^*$ definieren wir das* <u>*Konvolutionsprodukt*</u> *durch*

$$\begin{aligned} f_1 \star f_2(h) &:= \Phi^{-1}(\Phi(f_1) \cdot \Phi(f_2))(h) \\ &= \Phi^{-1}(\textstyle\sum_{h_1,h_2 \in G} f_1(h_1) f_2(h_2) h_1^{-1} h_2^{-1})(h) = \textstyle\sum_{h_1 \cdot h_2 = h} f_1(h_1) \cdot f_2(h_2) \ . \end{aligned}$$

**Lemma 4.4.9.**
Sei $(L_i)$ ein Repräsentantensystem für die Isomorphieklassen einfacher Darstellungen einer endlichen Gruppe $G$ auf einem $K$-Vektorraum. Dann gilt für das Konvolutionsprodukt der Charaktere

$$\chi_{L_i} \star \chi_{L_j} = \delta_{ij} \frac{|G|}{\dim_K L_i} \quad \chi_{L_i}$$

**Beweis.**
Die Beziehung in der Gruppenalgebra $K[G]$

$$e_{L_i} \cdot e_{L_j} = \delta_{ij} e_{L_i}$$

für die Projektoren führt wegen $\chi_L = \frac{|G|}{\dim_K L} \Phi^{-1}(e_L)$ zu der behaupteten Beziehung

$$\chi_{L_i} \star \chi_{L_j} = \frac{|G|^2}{\dim_K L_i \dim_K L_j} \Phi^{-1}(e_{L_i} \cdot e_{L_j}) \ = \frac{|G|^2}{\dim_K L_i \dim_K L_j} \delta_{ij} \Phi^{-1}(e_{L_i}) = \delta_{ij} \frac{|G|}{\dim_K L_i} \ \chi_{L_i} \ .$$

□

**Satz 4.4.10.**
Sei $G$ eine endliche Gruppe und $K$ ein Körper der Charakteristik Null. Dann teilt die Dimension jeder einfachen $G$-Darstellung die Gruppenordnung $|G|$.

**Beweis.**
Sei $L$ eine einfache Darstellung. Sei $n = |G|$ die Gruppenordnung. Dann gilt $g^n = 1$ für alle $g \in G$. Da der Wert $\chi_L(g)$ des Charakters als Spur die Summe der Eigenwerte von $\rho(g)$ ist, liegt $\chi_L(g)$ im Ring $\mathbb{Z}[\zeta]$, mit $\zeta$ einer primitiven $n$-ten Einheitswurzel.

Sei $I \subset \mathbb{Z}[\zeta]$ das von den Werten der Charaktere erzeugte Ideal. Aus Lemma 4.4.9 folgt die Inklusion

$$I \supset \frac{|G|}{\dim_K L} \ I \ .$$

Aus der Zahlentheorie ist bekannt, dass $\mathbb{Z}[\zeta]$ eine endlich erzeugte torsionsfreie abelsche Gruppe ist. Nach Satz 3.1.1 ist auch die Untergruppe $I$ endlich erzeugt frei und daher torsionsfrei. Daher ist $I \cong \mathbb{Z}^r$ für ein $r \in \mathbb{N}$. Daher muss

$$\frac{|G|}{\dim_K L} \in \mathbb{Z}$$

gelten, denn nur die Skalarierung mit einer ganzen Zahl bildet ein Gitter wieder auf sich ab. □

**Satz 4.4.11.**
Betrachte auf dem Vektorraum $K[G]^*$ die symmetrische Bilinearform

$$(\varphi, \psi) := \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1})$$

Dann bilden die Charaktere eine Orthonormalbasis für den Raum der Klassenfunktionen bezüglich dieser Bilinearform.

**Beweis.**
Nach Definition 4.4.8 des Konvolutionsprodukts gilt

$$(\varphi, \psi) = \frac{1}{|G|}(\varphi * \psi)(e)$$

mit $e \in G$ dem neutralen Element. Sei $(L_i)$ ein Repräsentantensystem für die Isomorphieklassen einfacher Darstellungen. Wertet man die Gleichheit in Lemma 4.4.9 auf dem neutralen Element $e$ aus und beachtet

$$\chi_L(e) = \mathrm{Tr}\,{}_L\rho(e) = \mathrm{Tr}\,{}_L\mathrm{id}_L = \dim_K L\,,$$

so folgt

$$(\chi_{L_i}, \chi_{L_j}) = \delta_{ij}\ \frac{1}{|G|}\ \frac{|G|}{\dim_K L_j}\ \ \chi_{L_j}(e) = \delta_{ij}\ .$$

Insbesondere sind die Charaktere einfacher Darstellungen linear unabhängig im Raum der Klassenfunktionen. Wegen Korollar 4.3.6 bilden die Charaktere der irreduziblen Darstellungen eine Basis für den gesamten Raum der Klassenfunktionen. □

Ist die Gruppenalgebra $K[G]$ nicht halbeinfach, so spannen die Charaktere nur einen echten Unterraum des Raums der Klassenfunktionen auf.

**Korollar 4.4.12.**
Zwei endlich-dimensionale Darstellungen einer endlichen Gruppe über einem algebraisch abgeschlossenen Körper der Charakteristik Null sind genau dann isomorph, wenn sie denselben Charakter haben.

**Beweis.**
Da die Gruppenalgebra nach dem Satz von Maschke 4.1.13 halbeinfach ist, ist nach Korollar 4.1.9 jede endlich-dimensionale Darstellung endliche direkte Summe einfacher Darstellungen. Wir können die Vielfachheit, mit der eine vorgegebene irreduzible Darstellung $L$ in einer Zerlegung der Darstellung $V$ als direkte Summe irreduzibler Darstellungen auftritt, berechnen: gilt $V = \oplus_{i=1}^r n_i L_i$, so folgt für den Charater $\chi_V = \sum_{i=1}^r n_i \chi_{L_i}$ und daher $(\chi_L, \chi_V) = n_L$.

Haben also zwei Darstellungen den gleichen Charakter, so treten die irreduziblen Darstellungen mit gleichen Multiplizitäten $n_i$ auf, und beide Darstellungen sind zur direkten Summe $\oplus_{i=1}^r n_i L_i$ isomorph. □

Es gibt natürlich auch eine umgekehrte Version der Orthogonalitätsbeziehungen aus Satz 4.1.13, bei der über die $r$ verschiedenen irreduziblen Charaktere von $G$ summiert wird.

**Korollar 4.4.13.**
Sei $s \in G$ und sei $c(s)$ die Anzahl der Gruppenelemente in der Konjugationsklasse von $s$. Dann gilt

$$\sum_{i=1}^{r} \chi_i(s)\chi_i(s^{-1}) = \frac{|G|}{c(s)} \ ;$$

ist $t \in G$ nicht konjugiert zu $s$, so gilt

$$\sum_{i=1}^{r} \chi_i(s)\chi_i(t^{-1}) = 0 \ .$$

**Beweis.**
Für $s \in G$ sei $f_s$ die Klassenfunktion, die auf der Konjugationklasse des Gruppenelements $s$ gleich Eins ist und auf allen anderen Konjugationsklassen verschwindet. Da die Charaktere nach Satz 4.4.11 eine Orthonormalbasis für die Klassenfunktionen bilden, können wir entwickeln

$$f_s = \sum_{i=1}^{r} \lambda_i \chi_i \qquad \text{mit Koeffizienten} \qquad \lambda_i = (f_s, \chi_i) = \frac{c(s)}{|G|} \chi_i(s^{-1}).$$

Daher folgt

$$f_s(t) = \frac{c(s)}{|G|} \sum_{i=1}^{r} \chi_i(s^{-1})\chi_i(t) \ .$$

□

Wir betrachten noch spezieller den Fall komplexer Gruppenalgebren.

**Korollar 4.4.14.**
Betrachtet man auf dem Dual der komplexen Gruppenalgebra $\mathbb{C}[G]$ das hermitesche Skalarprodukt $\langle \cdot, \cdot \rangle$, das gegeben ist durch

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)} \, ,$$

so bilden die einfachen Charaktere eine Orthonormalbasis im Raum der Klassenfunktionen.

**Beweis.**

- Wir zeigen für jeden Charakter $\chi = \chi_V$ über $\mathbb{C}$

  $$\chi(g^{-1}) = \overline{\chi(g)} \, .$$

  Zu jedem komplexen Vektorraum $(V, +, \cdot)$ gibt es einen anderen komplexen Vektorraum $(\overline{V}, +, *)$: als abelsche Gruppe sind beide Vektorräume gleich, $(V, +) = (\overline{V}, +)$, aber die Skalarmultiplikation ist mit der Konjugation getwistet:

  $$\lambda * v := \overline{\lambda} \cdot v \qquad \text{für alle } \lambda \in \mathbb{C}, v \in V \, .$$

  Hierbei ist $\overline{\lambda}$ die zu $\lambda$ konjugierte komplexe Zahl.

- Ist $V$ eine $G$-Darstellung, so auch $\overline{V}$ mit der gleichen Abbildung eine $G$-Darstellung. Bezüglich einer fest gewählten Basis von $V$ wird sie aber durch die Matrix mit komplex konjugierten Einträgen dargestellt. Daher gilt

  $$\chi_{\overline{V}}(g) = \overline{\chi_V(g)} \, .$$

- Andererseits wissen wir aus Bemerkung 4.4.7(iv), dass für die kontragrediente Darstellung gilt
$$\chi_{V^*}(g) = \chi_V(g^{-1})$$
Es reicht also aus, einen Isomorphismus von $G$-Darstellungen
$$V^* \cong \overline{V}$$
anzugeben. Nach Lemma 4.1.14 gibt es ein $G$-invariantes hermitesches Skalarprodukt auf $V$. Wir definieren eine lineare Abbildung
$$\iota : V^* \to \overline{V}$$
auf $\varphi \in V^*$ durch
$$\varphi(v) = \langle v, \iota(\varphi)\rangle$$
für alle $v \in V$. Da $\langle\cdot,\cdot\rangle$ nicht ausgeartet ist, ist dies eine Bijektion. $\iota$ ist sogar ein $G$-Morphismus, denn für alle $g \in G$, $v \in V$ und $\varphi \in V^*$ gilt:
$$\langle v, \iota(g\varphi)\rangle = g\varphi(v) = \varphi(g^{-1}v) = \langle g^{-1}v, \iota(\varphi)\rangle = \langle v, g\iota(\varphi)\rangle\ .$$
Hierbei benutzen wir die Definition von $\iota$, die Wirkung von $g$ auf $V^*$, wiederum die Definition von $\iota$ und die $G$-Invarianz des Skalarprodukts.

□

**Bemerkung 4.4.15.**
Die Werte der Charaktere der irreduziblen komplexen Darstellungen einer endlichen Gruppe $G$ werden in der Form einer Charaktertafel zusammengefasst. Die Spalten solch einer Tafel werden durch Repräsentanten von Konjugationsklassen, die Zeilen durch irreduzible Darstellungen indiziert. In der Tafel stehen die Werte des Charakters der entsprechenden irreduziblen Darstellung auf Elementen der entsprechenden Konjugationsklasse. Über den Konjugationsklassen wird meist in einer eigenen Zeile deren Kardinalität angegeben, damit auch das Skalarprodukt auf dem Raum der Klassenfunktionen aus der Tafel hervorgeht.

**Beispiele 4.4.16.**

1. Die irreduziblen komplexen Darstellungen der symmetrischen Gruppe $S_3$ sind die triviale Darstellung triv, die Signumsdarstellung sig und die Darstellung spieg als zweidimensionale Spiegelungsgruppe, bei der die drei ungeraden Permutationen durch Spiegelungen an drei Ursprungsgeraden operieren, die paarweise den Winkel $60^0$ einschließen. Zeichnen wir zwei ungerade Permutationen $s, t \in S_3$ aus, so sind die Elemente von $S_3 = \{e, s, t, sts, ts, st\}$. Die Charaktertafel hat die Gestalt

| | 1 | 3 | 2 |
|---|---|---|---|
| | $e$ | $s, t, sts$ | $ts, st$ |
| triv | 1 | 1 | 1 |
| sig | 1 | $-1$ | 1 |
| spieg | 2 | 0 | $-1$ |

Um sich vom der Richtigkeit der unteren Zeile zu überzeugen, beachte man, dass jede Spiegelung an einer Geraden in der Ebene Spur Null hat, jede ebene Drehung um $120^0$ jedoch Spur $-1 = \zeta_3 + \overline{\zeta}_3$ mit $\zeta_3$ einer primitiven dritten Einheitswurzel. Die Orthogonalitätsrelationen aus den Korollaren 4.4.14 und 4.4.13 überprüfe man als Übung.

2. Die eindimensionalen komplexen irreduziblen Darstellungen einer zyklischen Gruppe $C_n = \langle g \rangle$ mit einem Erzeuger $g$ und Relation $g^n = e$ finden wir mit dem Ansatz $\rho(g) = w$ mit $w \in GL(1, \mathbb{C}) \cong \mathbb{C}^\times$. Aus der Relation folgt $1 = \rho(g^n) = \rho(g)^n = w^n$. Wir finden daher $n$ eindimensionale irreduzible Darstellungen mit Charakter

$$\chi_h(g^k) = \exp(2\pi \mathrm{i} \frac{kh}{n}) \ ,$$

wobei wir $h$ mod $n$ betrachten. Die Charaktere sind offenbar orthogonal, da gilt

$$\frac{1}{n} \sum_{k=0}^{n-1} \mathrm{e}^{\frac{2\pi \mathrm{i} k}{n}(h-h')} = \delta_{h,h'}^{\bmod n\mathbb{Z}} \ .$$

Für das Tensorprodukt dieser Darstellungen sehen wir sofort $\chi_h \chi_{h'} = \chi_{h+h' \bmod n}$. Wir haben so alle irreduziblen Darstellungen gefunden: in einer abelschen Gruppe sind alle Konjugationsklassen einelementig, es gibt also für eine endliche abelsche Gruppe so viele Isomorphieklassen einfacher Darstellungen wie Gruppenelemente. Die Quadratsumme der Dimensionen der $n$ eindimensionalen Darstellungen sind offenbar gleich der Gruppenordnung $|C_n| = n$.

3. Die Diedergruppe $D_n$ ist definiert als die Symmetriegruppe des regulären $n$-Ecks. Sie enthält die Drehungen um Vielfache von $\frac{2\pi}{n}$ als zyklische Untergruppe der Ordnung $n$. Außerdem enthält sie $n$ Geradenspiegelungen. Als Erzeuger wählen wir die Drehung $r$ um $\frac{2\pi}{n}$ und eine Geradenspiegelung $s$. Dann gelten die Relationen

$$r^n = 1, \quad s^2 = 1 \quad \text{und } rs = sr^{-1} \ .$$

Die Gruppenelemente sind von der Form $r^k, sr^k$ mit $k$ mod $n$. Es gibt also $2n$ Gruppenelemente.

Wir nehmen nun an, dass $n$ gerade ist. Dann gibt es offenbar vier Isomorphieklassen eindimensionaler Darstellungen

| | $r^k$ | $sr^k$ |
|---|---|---|
| $\psi_1$ | $1$ | $1$ |
| $\psi_2$ | $1$ | $-1$ |
| $\psi_3$ | $(-1)^k$ | $(-1)^k$ |
| $\psi_4$ | $(-1)^k$ | $(-1)^{k+1}$ |

wobei $k$ modulo $n$ zu nehmen ist. Um zwei-dimensionale Darstellungen zu finden, wählen wir eine primitve $n$-te Einheitswurzel $w := \exp(2\pi \mathrm{i}/n)$ und setzen für $h \in \mathbb{Z}$:

$$\rho^{(h)}(r^k) = \begin{pmatrix} w^{hk} & 0 \\ 0 & w^{-hk} \end{pmatrix} \qquad \rho^{(h)}(sr^k) = \begin{pmatrix} 0 & w^{-hk} \\ w^{hk} & 0 \end{pmatrix}$$

Man sieht sofort, dass wir $h$ nur modulo $n$ betrachten müssen. Ferner liefert das Vertauschen der Basisvektoren $e_1$ und $e_2$ der Standardbasis den Isomorphismus $\rho^{(h)} \cong \rho^{(n-h)}$. Die Darstellungen $\rho^{(0)}$ und $\rho^{(n/2)}$ sind zerlegbar, denn alle Matrizen haben die gemeinsamen Eigenvektoren $e_1 \pm e_2$. Daher gilt die folgende Zerlegung in eindimensionale Darstellungen:

$$\rho^{(0)} \cong \psi_1 \oplus \psi_2 \quad \rho^{(n/2)} \cong \psi_3 \oplus \psi_4 \ .$$

Für $0 < h < n/2$ sind die Darstellungen $\rho^{(h)}$ irreduzibel, da die Matrix $\rho^{(h)}(r)$ diagonalisierbar mit verschiedenen Eigenwerten ist, so dass die Diagonalmatrix und die Außerdiagonalmatrix $\rho^{(h)}(s)$ nicht gleichzeitig diagonalisierbar sein können. Wir finden daher weitere Charaktere

$$\chi_h(r^k) = 2\cos\frac{2\pi kh}{n} \qquad \chi_h(sr^k) \ = 0 \quad \text{für} \quad 1, \ldots, n/2-1\,.$$

Man rechnet nach, dass die Charaktere alle orthogonal im Sinne von Satz 4.4.11 sind, womit klar ist, dass die Darstellungen paarweise nicht isomorph sind. Insbesondere folgt aus der Quadratsumme der Dimensionen

$$|D_n| \ = 2n = \ 4 \cdot 1^2 + (n/2-1)\cdot 2^2 \ ,$$

dass wir alle $n/2+3$ Isomorphieklassen von Darstellungen gefunden haben. Auch die Anzahl der Konjugationsklassen

$$\{e\}, \quad \{r^{n/2}\}, \quad \{r^k, r^{-k}\} \qquad k = 1, \ldots, \frac{n}{2}-1$$

und die beiden Konjugationsklassen von Spiegelungen an Geraden durch Kantenmitten bzw. durch Ecken $\{sr^i\}$ mit $i$ gerade bzw. ungerade stimmt mit der Zahl der Isomorphieklassen überein.

Für ungerades $n$ findet man nur zwei eindimensionale Darstellungen und die Charaktertafel

| | $r^k$ | $sr^k$ |
|---|---|---|
| $\psi_1$ | 1 | 1 |
| $\psi_2$ | 1 | $-1$ |
| $\chi_h$ | $2\cos\frac{2\pi kh}{n}$ | 0 mit $0 < h < \frac{n}{2}$ |

Im Fall von ungeradem $n$ gibt es nur eine Konjugationsklasse von Spiegelungen.

4. Die alternierende Gruppe $A_4$ kann identifiziert werden mit den Rotationssymmetrien eines regulären Tetraeders, die wir uns mit $1, 2, 3, 4$ numeriert vorstellen. Die 12 Elemente bestehen aus

   - dem neutralen Element,
   - drei Doppeltranspositionen

     $$x := (12)(34) \quad y := (13)(24) \quad z := (14)(23)\ ,$$

     die eine normale Untergruppe $H \subset A_4$ isomorph zur Kleinschen Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ erzeugen und geometrisch Drehungen des Tetraeders um $\pi$ um eine Achse durch die Mittelpunkte zweier gegenüberliegender Seiten entsprechen.
   - Schließlich gibt es noch 8 zyklische Permutationen der Ordnung 3, die geometrisch einer Rotation um $\frac{2\pi}{3}$ um eine Achse durch einen der vier Vertizes und den Schwerpunkt der gegenüberliegenden Dreiecksseite entsprechen.

   Wählen wir die Drehung $t := (123)4$, so finden wir vier Konjugationsklassen:

   $$\{1\} \quad \{x, y, z\} \quad \{t, tx, ty, tz\} \quad \{t^2, t^2x, t^2y, t^2z\}\ .$$

   Sei $K := \{e, t, t^2\} \cong \mathbb{Z}_3$ eine zyklische Untergruppe von $A_4$, so finden wir also die kurze exakte Sequenz von Gruppen

   $$1 \to H \to A_4 \to K \to 1\,,$$

wobei die Surjektion auf $K$ Kern $\{1, x, y, z\}$ hat.

Die Charaktere von drei eindimensionalen irreduziblen Darstellungen finden wir durch Zurückziehen der drei irreduziblen Charaktere der zyklischen Gruppe $K$. Den vierten Charakter finden wir mit Hilfe der Orthogonalitätsrelationen:

$$\begin{array}{c|cccc} & 1 & 3 & 4 & 4 \\ & 1 & x & t & t^2 \\ \hline \chi_0 & 1 & 1 & 1 & 1 \\ \chi_1 & 1 & 1 & w & w^2 \\ \chi_2 & 1 & 1 & w^2 & w \\ \psi & 3 & -1 & 0 & 0 \end{array}$$

wobei $w$ eine primitive dritte Einheitswurzel ist. Wieder überprüft man leicht die restlichen Orthogonalitätsrelationen.

Wir beschreiben abschließend die irreduzible dreidimensionale Darstellung: $A_4$ operiert als Untergruppe von $S_4$ auf $\mathbb{C}^4 = \mathbb{C}(e_1, e_2, e_3, e_4)$ durch Permutation der Elemente der Standardbasis. Das orthogonale Komplement der trivialen Unterdarstellung $\mathbb{C}(e_1 + e_2 + e_3 + e_4)$ ist die gesuchte dreidimensionale irreduzible Darstellung.

Wir wollen abschließend noch einmal komplexe Darstellungen einer endlichen Gruppe betrachten.

***Definition 4.4.17***

(i) *Die Quaternionen sind die reelle* 4*-dimensionale assoziative unitäre Algebra* $\mathbb{H}$ *mit Basis* $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$, *wobei die Multiplikation auf den Basiselementen durch die Relationen*

$$\begin{aligned} \mathrm{i}^2 &= \mathrm{j}^2 = \mathrm{k}^2 = -1 \\ \mathrm{ij} &= \mathrm{k}\,. \end{aligned}$$

*erklärt ist.*

(ii) *Einen* $\mathbb{H}$*-Modul nennen wir auch kurz einen* $\mathbb{H}$*-Vektorraum oder quaternionischen Vektorraum.*

Die Algebra $\mathbb{H}$ der Quaternionen ist ein Schiefkörper, auch Divisionsalgebra genannt, denn jedes $a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{k} \in \mathbb{H} \setminus \{0\}$ hat ein Inverses, $\frac{1}{\sum_i a_i^2}(a_0 - a_1\mathrm{i} - a_2\mathrm{j} - a_3\mathrm{k})$. Ein klassisches Resultat von Frobenius besagt, dass es nur drei reelle Schiefkörper gibt: die Körper $\mathbb{R}$ der reellen und $\mathbb{C}$ der komplexen Zahlen sowie die Quaternionen.

Die Benennung "quaternionischer Vektorraum" findet eine Rechtfertigung durch den folgenden Satz, aus dem hervorgeht, dass alle $\mathbb{H}$-Moduln isomorph zu direkten Summen eines einzigen irreduziblen $\mathbb{H}$-Moduls sind.

**Satz 4.4.18.**
Sei $D$ ein Divisionsring und $V$ ein endlich erzeugter $D$-Modul. Dann ist der Ring $\mathrm{End}_D(V)$ halbeinfach und alle einfachen $\mathrm{End}_D(V)$-Moduln sind isomorph.

**Beweis.**
Wie in der linearen Algebra zeigt man, dass $V$ eine endliche $D$-Basis hat. Wähle eine $D$-Basis $(e_1, \ldots e_n)$ von $V$ und betrachte

$$\begin{aligned} R := \mathrm{End}_D(V) &\to V \oplus \ldots V \\ f &\mapsto (f(e_1), \ldots f(e_n))\ , \end{aligned}$$

was ein Homomorphismus von $R$-Moduln ist. Da eine $D$-lineare Abbildung eindeutig auf einer Basis festgelegt werden kann, ist der Morphismus injektiv und surjektiv, also ein Isomorphismus von $R$-Moduln. Da $V$ als $\mathrm{End}_D(V)$-Modul einfach, also auch halbeinfach ist, ist der Ring $\mathrm{End}_D(V)$ halbeinfach. Nach Satz 4.1.10 ist jeder einfache $\mathrm{End}_D(V)$-Modul isomorph zu einem Untermodul von $\mathrm{End}_D(V)$, also isomorph zu $V$. Jeder $\mathrm{End}_D(V)$-Modul ist somit direkte Summe einfacher $\mathrm{End}_D(V)$-Moduln, nämlich von Kopien von $V$. □

Die Verbindung zu komplexen Vektorräumen stellt das folgende Lemma her:

**Lemma 4.4.19.**
Ein $\mathbb{H}$-Modul ist äquivalent zu einem komplexen Vektorraum $V$ mit einer antilinearen Abbildung $J$, für deren Quadrat $J^2 = -\mathrm{id}_V$ gilt.

**Beweis.**
Sei $V$ ein $\mathbb{H}$-Modul. Die Wirkung mit $\mathrm{i} \in \mathbb{H}$ liefert dann die Skalarmultiplikation mit der imaginären Einheit von $\mathbb{C}$ und versieht $V$ mit der Struktur eines komplexen Vektorraums. Setze $J(v) = \mathrm{j}v$. Die Eigenschaften von $J$ folgen durch Nachrechnen.

Liegt umgekehrt ein komplexer Vektorraum $V$ mit einer antilinearen Abbildung $J$ vor, so definiert man die Wirkung des Quaternions i durch die Wirkung von $\mathrm{i} \in \mathbb{C}$ und des Quaternions j durch die Wirkung von $J$. Die Wirkung von $\mathrm{k} = \mathrm{ij}$ liegt dann fest. □

**Satz 4.4.20.**
Sei $G$ eine Gruppe und $V$ eine einfache Darstellung von $G$ über $\mathbb{C}$ von endlicher Dimension. So sind wir in genau einem der drei Fälle:

(a) $V$ entsteht aus einer einfachen reellen Darstellung $V_\mathbb{R}$ durch Erweiterung der Skalare, d.h.

$$V = \mathbb{C} \otimes_\mathbb{R} V_\mathbb{R} = \mathrm{Ind}_\mathbb{R}^\mathbb{C}(V_\mathbb{R}) \ .$$

Man sagt dann, $V$ sei von reellem Typ.

(b) $V$ entsteht aus einer einfachen quaternionalen Darstellung $V_\mathbb{H}$ auf einem $\mathbb{H}$-Modul durch Restriktion der Skalare auf $\mathbb{C} \subset \mathbb{H}$, d.h.

$$V = \mathrm{Res}_\mathbb{C}^\mathbb{H} V_\mathbb{H} \quad .$$

Man sagt dann auch, $V$ sei von quaternionalem Typ.

(c) $V$ ist nicht isomorph zu $\overline{V}$. In diesem Fall sagt man auch, $V$ sei von komplexem Typ.

**Beweis.**

- Ist $V \cong \overline{V}$, so gilt nach dem Schurschen Lemma 1.5.5

$$\dim_\mathbb{C} \ \mathrm{Hom}_G(V, \overline{V}) = 1 \, ;$$

sind die Moduln $V$ und $\overline{V}$ nicht isomorph, so gibt es keine nicht-verschwindenden $G$-Morphismen.

Für einen von Null verschiedenen Homomorphismus $J \in \mathrm{Hom}_G(V, \overline{V})$ gilt

$$Jav = \overline{a}Jv \qquad \text{für alle} \quad a \in \mathbb{C}, v \in V$$

d.h. $J$ ist antilinear. Wenden wir die reell-lineare Abbildung, die $J$ zu Grunde liegt, zweimal an, so erhalten wir eine komplex lineare Abbildung, auf die wir das Schursche Lemma anwenden können. Daher ist

$$J^2 = \lambda \mathrm{id}_V \quad \text{mit } \lambda \in \mathbb{C}^\times .$$

Wegen

$$\lambda J v = J^3 v = J(J^2 v) = J\lambda v = \overline{\lambda} J v$$

gilt $\lambda = \overline{\lambda}$, also ist $\lambda$ reell, $\lambda \in \mathbb{R}$. Ersetzen wir $J$ durch ein komplexes Vielfaches $J'$, also $J' = zJ$ mit $z \in \mathbb{C}^\times$, so ist

$$(J')^2 = zJzJ = |z|^2 J^2 = |z|^2 \lambda \,\mathrm{id}_V .$$

Wir finden also im Fall $V \cong \overline{V}$ einen antilinearen $G$-Isomorphismus $J$, für den entweder gilt
$(a)$ $J^2 = \mathrm{id}_V$ oder $(b)$ $J^2 = -\mathrm{id}_V$.

- Im Falle $(a)$ betrachten wir den reellen Untervektorraum der $J$-Fixpunkte $V^J \subset V$. Weil die Endomorphismen $\rho_g$ mit $J$ vertauschen, trägt dieser eine reelle $G$-Darstellung: es gilt

$$J\rho_g v = \ \rho_g J v = \ \rho_g v$$

und somit ist für jedes $g \in G$ auch $\rho_g v \in V^J$. Die Abbildung

$$\begin{array}{ccc} V^J \otimes_{\mathbb{R}} \mathbb{C} & \to & V \\ v \otimes_{\mathbb{R}} (\lambda_1 + \mathrm{i}\lambda_2) & \mapsto & \lambda_1 v + \lambda_2 \mathrm{i} v \end{array}$$

mit $\lambda_1, \lambda_2 \in \mathbb{R}$ ist dann ein Isomorphismus von komplexen $G$-Darstellungen. (Auf der linken Seite operiert $G$ nicht-trivial nur auf $V^J$ und trivial auf $\mathbb{C}$.) Im Falle $(b)$ definiert $J$ nach Lemma 4.4.19 auf $V$ die Struktur eines $\mathbb{H}$-Vektorraums.

□

Man kann an Hand der Charaktertafel entscheiden, welcher Typ von Darstellung vorliegt, vgl. Serre, Linear Representations of Finite Groups, Springer Graduate Text 48, Proposition 39: der Ausdruck $\frac{1}{|G|}\sum_{g\in G}\chi(g^2)$ nimmt den Wert 1 für reelle, $-1$ für quaternionale und 0 für komplexe Darstellungen an.

# 5 Artinsche und Noethersche Moduln

## 5.1 Noethersche Moduln

Sei $R$ ein Ring mit Eins.

**Satz 5.1.1.**
Für einen $R$-(Links)Modul $M$ sind folgende Bedingungen äquivalent.

(i) Jede aufsteigende Kette $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq N_{k+1} \subseteq \ldots$ von Untermoduln von $M$ wird stationär, d.h. es gibt einen Index $k$, so dass $N_i = N_k$ für alle $i \geq k$. Man sagt auch kurz, $M$ erfülle eine aufsteigende Kettenbedingung.

(ii) Jede nicht-leere Teilmenge von Untermoduln von $M$ besitzt bezüglich der Inklusion ein maximales Element.

(iii) Jeder Untermodul von $M$ ist endlich erzeugt.

**Definition 5.1.2**

*(i) Ein $R$-Modul $M$, der eine der Bedingungen aus 5.1.1 erfüllt, heißt noetherscher (Links-)Modul.*

*(ii) Ein Ring $R$ heißt (links-)noethersch, wenn er als Modul über sich selbst noethersch ist.*

*(iii) Man definiert analog noethersche Rechtsmoduln und rechtsnoethersche Ringe.*

*(iv) Ein Ring heißt noethersch, wenn er sowohl links- als auch rechtsnoethersch ist.*

Es gilt nicht, dass ein linksnoetherscher Ring automatisch auch rechtsnoethersch ist. Ein Gegenbeispiel hierzu kommt in den Übungen.

**Beweis.**
(von 5.1.1)

(i) ⇒ (ii) Jede nicht-leere Menge $X$ von Untermoduln ist bezüglich Inklusion induktiv geordnet: denn sei $N_1 \subseteq N_2 \subseteq \dots$ eine Kette in $X$, so ist $\bigcup_i N_i = N_k \in X$ nach (i) eine obere Schranke für die Familie $\{N_i\}$. Die Existenz eines maximalen Elements folgt nun aus dem Zornschen Lemma.

(ii) ⇒ (iii) Sei $N \subseteq M$ Untermodul. Wir betrachten die Menge

$$X := \{N' | N' \subseteq N \quad \text{Untermodul von}\, M, N' \,\text{endlich erzeugt}\}$$

Zumindest der Nullmodul liegt in $X$, $0 \in X$, also ist $X$ nicht leer. Sei $N_0 \in X$ ein maximales Element. Wir behaupten, dass dann $N_0 = N$ gilt. Denn wäre $x \in N \backslash N_0$, so wäre $\langle N_0, x\rangle \in X$ und das Erzeugnis $\langle N_0, x\rangle \supsetneq N_0$ wäre immer noch endlich erzeugt, im Widerspruch zur Maximalität von $N_0$.

(iii) ⇒ (i) Sei $N_1 \subseteq N_2 \subseteq \dots$ eine Kette von Untermoduln. Ihre Vereinigung $N' := \bigcup_i N_i$ ist ein Untermodul und nach Voraussetzung (iii) endlich erzeugt:

$$N' = \langle x_1, \dots, x_r\rangle$$

Daher gibt es $k \in \mathbb{N}$ so dass $x_i \in N_k$ für alle $i = 1, \dots r$. Hieraus folgt $N' \subseteq N_k$, die Kette der Untermoduln wird also stationär.

□

**Beispiele 5.1.3.**

1. Ist $R$ eine Algebra über einem Körper $K$, so ist jeder $R$-Modul, der endlich dimensional über $K$ ist, noethersch. Ist $R$ selbst eine endlich dimensionale Algebra über einem Körper, so ist $R$ noethersch.

2. Halbeinfache Ringe sind nach Satz 4.1.10 noethersch.

3. Die Untermoduln eines Ringes sind seine Ideale, die im Falle eines Hauptidealrings sogar von nur einem Element erzeugt werden, also insbesondere endlich erzeugt sind. Nach Satz 5.1.1 sind also Hauptidealringe noethersch.

4. Wir geben ein Beispiel eines Ringes, der nicht noethersch ist:

$$\begin{aligned} R &= \{f(X) \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\} \\ &= \{m + Xg \mid m \in \mathbb{Z}, g \in \mathbb{Q}[X]\} \end{aligned}$$

Jede Untergruppe $G$ von $(\mathbb{Q}, +)$ gibt ein Ideal

$$A_G := GX + X^2\mathbb{Q}[X]$$

von $R$. Betrachte für jedes $i \in \mathbb{N}$ die Untergruppe $G_i := \left\{\frac{m}{i}, m \in \mathbb{Z}\right\}$. Wir bekommen so eine unendliche aufsteigende Kette von Idealen

$$A_{G_2} \subset A_{G_4} \subset A_{G_8} \subset \dots .$$

in $R$. Beispiele für noethersche Ringe folgen unmittelbar aus Korollar 5.1.7 unten.

**Satz 5.1.4.**

(i) Untermoduln und epimorphe Bilder noetherscher Moduln sind noethersch.

(ii) Ist $U$ ein Untermodul und sind $U$ und $M/U$ noethersch, so ist auch $M$ noethersch.

**Beweis.**

(i) Sei $M$ noethersch, $U$ Untermodul von $M$. Jeder Untermodul $U'$ von $U$ ist auch Untermodul von $M$, also endlich erzeugt. Also sind auch Untermoduln noetherscher Moduln endlich erzeugt.

Sei $M'$ ein epimorphes Bild von $M$, also $f : M \twoheadrightarrow M'$, also $M' \cong M/\ker f$. Sei ferner $V$ ein Untermodul von $M'$ und $f^{-1}(V)$ das Urbild von $V$ unter der Surjektion $f$. Dann ist $f^{-1}(V)$ als Untermodul des noetherschen Moduls $M$ endlich erzeugt:

$$f^{-1}(V) = \langle v_1, \dots, v_r \rangle \quad \text{mit } v_i \in M\,.$$

Hieraus folgt

$$V = \langle v_1 + \ker f, \dots, v_r + \ker f \rangle\,,$$

also ist auch der Untermodul $V$ von $M$ endlich erzeugt. Damit ist auch das epimorphe Bild $M'$ noethersch.

(ii) Sei $N_1 \subseteq N_2 \subseteq \dots$ eine aufsteigende Kette von Untermoduln in $M$. Wir erhalten durch die kanonische Surjektion $p : M \twoheadrightarrow M/U$ eine aufsteigende Kette von Untermoduln in $M/U$

$$(N_1 + U)/U \subseteq (N_2 + U)/U \subseteq \dots$$

und durch Schnitt mit $U$ eine aufsteigende Kette von Untermoduln in $U$:

$$N_1 \cap U \subseteq N_2 \cap U \subseteq \dots$$

Da sowohl $U$ als auch $M/U$ noethersch sein sollen, gibt es ein $k \in \mathbb{N}$, so dass

$$N_k + U = N_{k+1} + U = \dots$$

und $N_k \cap U = N_{k+1} \cap U = \dots$

Daraus folgt aber $N_k = N_{k+1}$. Denn sei $x \in N_{k+1}$, dann folgt aus der Stationarität der Kette im Quotientenmodul, dass man $x$ schreiben kann in der Form $x = y + u$ mit $y \in N_k$ und $u \in U$. Somit liegt $u = x - y \in U \cap N_{k+1} = U \cap N_k \subset N_k$. Daraus folgt aber $x \in N_k$.

$\square$

**Korollar 5.1.5.**
Endliche direkte Summen noetherscher Moduln sind noethersch.

**Beweis.**
Seien $U, V$ noethersche Moduln. Dann ist auch $(U \oplus V)/V \cong U$ noethersch. Aus Satz 5.1.4(ii) folgt nun, dass auch die direkte Summe $U \oplus V$ noethersch ist. $\square$

**Satz 5.1.6.**
Ein Modul über einem noetherschen Ring ist genau dann noethersch, wenn er endlich erzeugt ist.

**Beweis.**
Jeder noethersche Modul ist als Untermodul seiner selbst endlich erzeugt. Sei umgekehrt $M = \langle a_1, \ldots, a_r \rangle$ und sei $F := R^r$. Betrachte die Surjektion

$$\begin{aligned} F = R^r &\twoheadrightarrow M \\ (\alpha_1, \alpha_2, \ldots, \alpha_r) &\mapsto \sum_{i=1}^{r} \alpha_i a_i \end{aligned}$$

Nach Satz 5.1.5 ist die direkte Summe $R^r$ noethersch, nach Satz 5.1.4 (i) ist $M$ als epimorphes Bild eines noetherschen Moduls noethersch. $\square$

**Korollar 5.1.7.**

1. Endlich erzeugte Moduln über Hauptidealringen sind noethersch.
2. Die endlich erzeugten abelsche Gruppen sind die noetherschen $\mathbb{Z}$-Moduln.
3. Jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt.

**Beweis.**

1. Aus Satz 5.1.6 folgt sofort, dass endlich erzeugte Moduln über Hauptidealringen noethersch sind.
2. Da $\mathbb{Z}$ ein Hauptidealring ist, ist dies ein Spezialfall von (ii).
3. Folgt aus Satz 5.1.1, da eine Untergruppe einer abelschen Gruppe auch ein $\mathbb{Z}$-Untermodul ist.

$\square$

**Satz 5.1.8** (Hilbertscher Basissatz)**.**
Sei $R$ ein kommutativer Ring. Ist $R$ noethersch, so ist auch der Polynomring $R[X]$ noethersch.

**Beweis.**
Sei $I \subset R[X]$ ein Ideal. Sei $\mathfrak{a}_i \subset R$ das Ideal, das aus den höchsten Koeffizienten, den Leitkoeffizienten, aller Polynome vom Grad $i$ im Ideal $I$ besteht. Die Multiplikation mit dem Monom $X$ zeigt die folgende Inklusion von Idealen von $R$:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \ldots .$$

Für diese aufsteigende Idealkette im noetherschen Ring $R$ gibt es ein $j$, so dass gilt

$$\mathfrak{a}_j = \mathfrak{a}_{j+1} = \ldots .$$

Jedes der endlich vielen Ideale $\mathfrak{a}_i$ mit $i \leq j$ ist nach Satz 5.1.6 als Ideal des noetherschen Rings $R$ endlich erzeugt. Wähle also endlich viele Polynome aus $I$, deren Leitkoeffizienten alle Ideale $\mathfrak{a}_i$ von $R$ erzeugen.

Die Gesamtheit dieser Polynome erzeugt das Ideal $I$ im Polynomring: sei $p \in I$ vom Grad $n$, so finde $\alpha_i \in R$ mit zugehörigem Polynom $p_i$, so dass $p$ und das Polynom $\sum_i \alpha_i p_i X^{n_i}$ den gleichen Leitkoeffizienten haben. Ihre Differenz $p - \sum_i \alpha_i p_i X^{n_i}$ hat also Grad kleiner gleich $n-1$. Induktiv schließt man weiter. □

## 5.2 Artinsche Moduln

Artinsche Moduln verhalten sich in vielerlei Hinsicht ähnlich zu noetherschen Moduln. Wir fassen uns daher kurz.

***Definition 5.2.1***

1. *Ein $R$-Modul heißt artinsch, wenn es für jede absteigende Kette $M_0 \supset M_1 \supset M_2 \cdots$ von Untermoduln in $M$ einen Index $n$ gibt, so dass $M_i = M_n$ für alle $i \geq n$ gilt. Man sagt auch kurz, $M$ erfülle eine absteigende Kettenbedingung.*

2. *Ein Ring heißt linksartinsch, wenn er als Linksmodul über sich selbst artinsch ist.*

3. *Man definiert analog artinsche Rechtsmoduln und rechtsartinsche Ringe.*

4. *Ein Ring heißt artinsch, wenn er sowohl links- als auch rechtssartinsch ist.*

**Beispiele 5.2.2.**

1. Ist $R$ eine Algebra über einem Körper $K$, so ist jeder $R$-Modul, der endlich dimensional über $K$ ist, artinsch. Ist $R$ selbst eine endlich dimensionale Algebra über einem Körper, so ist $R$ artinsch.

2. Der Ring $\mathbb{Z}$ ist nicht artinsch, wie die Kette $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots$ zeigt. Für jedes positive $n \in \mathbb{Z}$ ist der Ring $\mathbb{Z}/n\mathbb{Z}$ endlich und daher artinsch. (Der Ring $\mathbb{Z}$ ist aber noethersch, da er Hauptidealring ist.)

Man kann zeigen:

**Satz 5.2.3.**

1. Es seien $M$ ein $R$-Modul und $N$ ein Untermodul von $M$. Dann ist $M$ genau dann artinsch, wenn $M/N$ und $N$ artinsch sind.

2. Es seien $M_1, M_2, \dots, M_r$ Moduln über $R$. Dann ist die direkte Summe $\oplus_{i=1}^r M_i$ genau dann artinsch, wenn alle Summanden $M_i$ artinsch sind.

3. Jeder endlich erzeugte Modul über einem linksartinschen Ring ist artinsch.

**Bemerkung 5.2.4.**

- Man überlegt sich leicht: Ein $R$-Modul ist genau dann endlich erzeugt, wenn zu jeder Familie $(M_i)_{i\in I}$ von Untermoduln mit $\sum_{i\in I} M_i = M$ eine endliche Teilmenge $J \subset I$ existiert, so dass $M = \sum_{j\in J} M_j$ gilt. Ist $M$ endlich erzeugt, $M = \langle x_1, \dots x_r\rangle$, so finde Untermoduln $M_i$ mit $x_i \in M_i$. Dann ist offenbar $M = \sum_{i=1}^r M_i$. Für die umgekehrte Richtung benutze man, dass $M = \sum_{m\in M} Rm$ und finde eine endliche Teilmenge von $M$, die $M$ erzeugt.

- Dual dazu definiert man nun: Ein $R$-Modul $M$ heißt <u>endlich koerzeugt</u>, wenn es zu jeder Familie $(M_i)_{i\in I}$ von Untermoduln mit $\cap_{i\in I} M_i = 0$ eine endliche Teilmenge $J \subset I$ mit $\cap_{j\in J} M_j = 0$ gibt.

- Ist $N$ ein Untermodul eines $R$-Moduls $M$, so folgt aus dieser Definition, dass der Quotientenmodul $M/N$ genau dann endlich koerzeugt ist, wenn es zu jeder Familie $(M_i)_{i\in I}$ von Untermoduln von $M$ mit $\cap_{i\in I} M_i = N$ eine endliche Teilmenge $J \subset I$ mit $\cap_{j\in J} M_j = N$ gibt.

**Satz 5.2.5.**
Sei $M$ ein $R$-Modul. Dann sind die folgenden Aussagen äquivalent:

(i) $M$ ist artinsch.

(ii) Jede nicht-leere Menge von Untermoduln von $M$ enthält ein minimales Element.

(iii) Jeder Faktormodul von $M$ ist endlich koerzeugt.

**Beweis.**

$(i) \Rightarrow (ii)$ beweist man ähnlich wie die entsprechende Aussage $(i) \Rightarrow (ii)$ in Satz 5.1.1 für noethersche Moduln.

$(ii) \Rightarrow (iii)$ Seien $N$ und $(M_i)_{i\in I}$ Untermoduln von $M$ mit $N = \cap_{i\in I} M_i$. Setze $X = \{\cap_{j\in J} M_j | J \subset I \text{ endlich}\}$. Nach Voraussetzung enthält $X$ ein minimales Element $N_1$. Es gilt offenbar $N_1 \supset N$. Wäre diese Inklusion echt, so gäbe es $x \in N_1 \setminus N$ Wegen $N = \cap_{i\in I} M_i$ gibt es ein $i \in I$ mit $x \notin M_i$, also $x \notin N_2 = N_1 \cap M_i$. Wir haben also $N_2 \in X$ und $N_2 \subsetneq N_1$: Widerspruch!

$(iii) \Rightarrow (i)$ Für eine absteigende Kette $M_0 \supset M_1 \supset M_2 \supset \cdots$ von Untermoduln von $M$ setze man $N := \cap_{i\in\mathbb{N}} M_i$. Weil $M/N$ endlich koerzeugt ist, gibt es eine endliche Teilmenge $J \subset \mathbb{N}$ mit $N = \cap_{j\in J} M_j$. Ist nun $n := \max(J)$, so folgt $N = M_n$, also $M_i = M_n$ für alle $i \geq n$.

□

Wir erwähnen abschließend noch ohne Beweis den folgenden Satz von Hopkins: Ein linksartinscher Ring ist auch linksnoethersch. (Die Umkehrung gilt aber nicht, wie das Beispiel des Rings $\mathbb{Z}$ der ganzen Zahlen zeigt.)

***Definition 5.2.6***
*Ein Ring heißt <u>einfach</u>, wenn er keine nicht-trivialen beidseitigen Ideale hat.*

Achtung: ein Ring, der einfach als Modul über sich selbst ist, ist immer ein einfacher Ring. Denn die Untermoduln sind gerade die Linksideale, und der Modul hat keine nicht-trivialen Untermoduln. Also gibt es keine nicht-trivialen Linksideale, und daher erst recht keine nicht-trivialen beidseitigen Ideale. Die Umkehrung gilt nicht: es gibt einfache Ringe, die nicht einfach als Moduln über sich selbst sind.

**Theorem 5.2.7.**
Für einen Ring $R$ sind äquivalent

1. $R$ ist ein einfacher artinscher Ring.
2. $R$ ist isomorph zu einem Matrizenring über einem Divisionsring.
3. $R$ ist halbeinfach und alle einfachen $R$-Moduln sind isomorph.
4. $R$ ist halbeinfach als $R$-Modul und in der Zerlegung von $R$ als Linksmodul tritt nur eine Isomorphieklasse einfacher Moduln auf.
5. $R$ ist artinsch und hat einen treuen einfachen Modul.

**Beweis.**
Wir beschränken uns darauf, die Implikation (5) $\Rightarrow$ (4) und (1) $\Rightarrow$ (5) zu zeigen. Der Rest sind einfache Folgerungen aus Definitionen und dem Wedderburnschen Strukturtheorem 4.2.3.

(5) $\Rightarrow$ (4) Betrachte für den treuen Modul $M$ ind für alle $n$ alle $R$-Modulmorphismen

$$R \to M^n \ .$$

Die Kerne dieser Morphismen sind (Links-)Ideale von $R$; da $R$ artinsch ist, können wir einen Morphismus $f$ mit minimalem Kern wählen.

Wir zeigen, dass dieses $f$ injektiv ist. Denn wäre $r \in R \setminus \{0\}$ mit $f(r) = 0$, so könnten wir den treuen Modul $M$ benutzen, um ein $m \in M$ zu finden mit $r.m \neq 0$. Dann hätte aber

$$\begin{array}{rcl} R & \to & M^n \oplus M \\ r & \mapsto & (f(r), r.m) \end{array}$$

einen kleineren Kern als $f$, im Widerspruch zur Minimalitätsannahme für den Kern von $f$. Also ist $R$ ein Untermodul des homogenen (d.h. nur eine isotypische Komponente ist nicht-trivial) halbeinfachen Moduls $M^n$ und selbst homogen und halbeinfach.

(1) $\Rightarrow$ (5) Für jeden $R$-Modul $M$ ist der Annulator $\mathrm{Ann}(M)$ ein beidseitiges Ideal. Da $R$ einfach ist und $1 \notin \mathrm{Ann}(M)$, verschwindet der Annulator und sogar jeder $R$-Modul ist treu.

Da $R$ artinsch ist, existieren einfache Moduln: jede absteigende Kette von Idealen wird konstant und das kleinste auftretende Ideal ist ein einfacher Modul.

□

**Korollar 5.2.8.**
Sei $K$ ein Körper und $R$ eine $K$-Algebra. Sei $M$ ein einfacher $R$-Modul mit $\dim_K M < \infty$, für den $\mathrm{End}_K(M) = K\mathrm{id}_M$ gilt. (Das ist zum Beispiel immer der Fall, wenn $K$ algebraisch abgeschlossen ist.) Dann ist die Strukturabbildung

$$R \to \mathrm{End}_K(M)$$

surjektiv.

**Beweis.**
Wir faktorisieren die Strukturabbildung

$$\begin{tikzcd} R \arrow[r] \arrow[d] & \mathrm{End}_K(M) \\ R/\mathrm{Ann}(M) \arrow[ur] & \end{tikzcd}$$

Dann ist $M$ ein treuer $R/\mathrm{Ann}(M)$-Modul, so dass die Abbildung $R/\mathrm{Ann}(M) \to \mathrm{End}_K(M)$ injektiv ist. Somit ist $R/\mathrm{Ann}(M)$ als $K$-Algebra endlich-dimensional und insbesondere artinsch. Damit ist $R/\mathrm{Ann}(M)$ ein artinscher Ring, der einfach ist, da $M$ einfacher Modul ist. Nach dem Struktursatz Theorem 5.2.7.2 gilt $R/\mathrm{Ann}(M) \cong \mathrm{End}_K(M)$. □

Wir ziehen noch eine Schlussfolgerung:

**Korollar 5.2.9.**
Sei $K$ ein Körper und $R$ eine einfache, endlich-dimensionale $K$-Algebra, $\dim_K R = n$, deren Zentrum gleich $K1_R$ ist. Dann gilt der folgende Isomorphismus von Ringen:

$$R \otimes_K R^{\mathrm{opp}} \cong M(n \times n, K) \ .$$

**Beweis.**
$R$ ist als $R-R$-Bimodul ein $R \otimes_K R^{\mathrm{opp}}$-Modul. Da die beidseitigen Ideale gerade die $R \otimes_K R^{\mathrm{opp}}$-Untermoduln sind, der Ring $R$ aber einfach ist, ist $R$ als $R \otimes_K R^{\mathrm{opp}}$-Modul einfach.

Nun gilt

$$\begin{array}{rcl} \mathrm{End}_{R\otimes_K R^{\mathrm{opp}}} R & \to & Z(R) \\ f & \mapsto & f(1) \ , \end{array}$$

denn $r.f(1) = f(r \cdot 1) = f(1 \cdot r) = f(1).r$ für alle $r \in R$. Wir haben also die Isomorphie

$$\mathrm{End}_{R\otimes_K R^{\mathrm{opp}}} R \cong Z(R) \cong K \ .$$

Nach dem vorangegangenen Korollar ist dann

$$R \otimes_K R^{\mathrm{opp}} \to \mathrm{End}_K(R) \cong M(n \times n, K)$$

surjektiv. Bild und Urbild sind $K$-Vektorräume der gleichen Dimension $n^2$, daher ist die Abbildung sogar ein Isomorphismus. □

# 6 Auflösungen und abgeleitete Funktoren

Der Funktor $\mathrm{Hom}(U, -)$ ist genau dann exakt, wenn $U$ ein projektives Objekts einer abelschen Kategorie ist; ähnlich ist $\mathrm{Hom}(-, U)$ genau dann exakt, wenn $U$ ein injektives Objekt ist. Der Funktor $U \otimes -$ ist genau für die flachen Objekte einer abelschen Tensorkategorie exakt. Wir wollen nun diese Funktoren auf allgemeinen Objekten untersuchen.

## 6.1 Projektive und injektive Auflösungen

***Definition 6.1.1***

1. *Eine abelsche Kategorie $\mathcal{C}$ hat genug projektive Objekte, falls es für jedes Objekt $M \in \mathcal{C}$ einen Epimorphismus $P \to M \to 0$ aus einem projektiven Objekt $P$ gibt.*

2. *Sie hat genug injektive Objekte, falls es für jedes Objekt $M$ einen Monomorphismus $0 \to M \to I$ in ein injektives Objekt $I$ gibt.*

**Beispiele 6.1.2.**

1. Für jeden Ring $R$ hat die Kategorie $R-$Mod genug projektive und injektive Objekte. Dies folgt aus der Tatsache, dass jeder Modul Untermodul eines kofreien Moduls und Bild eines freien Moduls ist, vgl. Satz 2.4.4.

2. Die Kategorie $\mathrm{Ab}_{fin}$ der *endlichen* abelschen Gruppen hat überhaupt keine projektiven und injektiven Objekte, insbesondere nicht genug.

   Bei der Argumentation müssen wir etwas acht geben: $\mathrm{Ab}_{fin}$ ist eine volle Unterkategorie von Ab, aber im Allgemeinen sind die projektiven oder injektiven Objekte einer Unterkategorie nicht einfach diejenigen projektiven oder injektiven Objekte, die in der Unterkategorie liegen. Zum Beispiel ist jeder Vektorraum über dem Körper $\mathbb{Z}_2$ eine abelsche Gruppe, daher ist $\mathrm{vect}_{\mathbb{Z}_2} \subset \mathrm{Ab}$ eine Unterkategorie. Jeder Vektorraum ist frei und daher projektiv. Insbesondere ist $\mathbb{Z}_2$ selbst in $\mathrm{vect} - \mathbb{Z}_2$ projektiv, nicht aber in Ab.

   Dazu überlegen wir uns zunächst, dass für jedes $n \in \mathbb{N}$ die kurze exakte Sequenz

   $$0 \to \mathbb{Z}_n \to \mathbb{Z}_{n^2} \to \mathbb{Z}_n \to 0$$

   nicht spaltet. Daher ist die zyklische Gruppe $\mathbb{Z}_n$ weder projektiv noch injektiv. Jede endliche abelsche Gruppe $A$ lässt sich nach Korollar 3.2.4 schreiben als $A = \bigoplus \mathbb{Z}_{n_i} \equiv \prod \mathbb{Z}_{n_i}$, ist also als Summe nicht projektiver Moduln nach Lemma 2.4.1 nicht projektiv, bzw. als Produkt nicht injektiver Moduln nach dem gleichen Lemma auch nicht injektiv in der Kategorie der endlichen abelschen Gruppen.

3. Die Kategorie der endlich erzeugten abelschen Gruppen hat zwar genug projektive Objekte (die freie abelsche Gruppe auf einem endlichen Erzeugendensystem ist projektiv und bildet surjektiv auf eine solche Gruppe ab), aber keine injektiven Objekte. Eine endlich erzeugte abelsche Gruppe $A$ lässt sich nach Korollar 3.2.4 als endliches Produkt $\prod \mathbb{Z}_{n_i} \times \mathbb{Z}^n$ schreiben. Sie ist nach Lemma 2.4.1 injektiv in Ab, wenn jeder Faktor injektiv ist. Nach Korollar 1.4.16 sind aber die injektiven abelschen Gruppen genau die teilbaren abelschen Gruppen; die Faktoren $\mathbb{Z}$ und $\mathbb{Z}_n$ sind aber nicht teilbar.

***Definition 6.1.3***
*Sei $M$ ein Objekt in einer abelschen Kategorie $\mathcal{C}$.*

1. *Eine projektive Auflösung von $M$ ist eine exakte Sequenz*

   $$\cdots \to P_i \to P_{i-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

   *in der alle Objekte (außer natürlich $M$) projektiv sind. Der Morphismus $P_0 \to M$ wird auch Augmentation genannt.*

2. *Eine <u>injektive Auflösung</u> ist eine exakte Sequenz*

$$0 \to M \to Q_0 \to Q_1 \to \cdots \ ,$$

*in der alle Objekte $Q_i$ injektiv sind.*

Freie Auflösungen sind Spezialfälle projektiver Auflösungen. Wir haben schon in Betrachtung 3.1.3 gesehen, dass Moduln über Hauptidealringen freie Auflösungen der Länge 1 besitzen,

$$0 \to F_1 \to F_0 \to M \ \to 0 \ .$$

**Lemma 6.1.4.**
Hat eine Kategorie $\mathcal{C}$ genug Projektive, so hat jedes Objekt von $\mathcal{C}$ eine projektive Auflösung. Hat $\mathcal{C}$ genug Injektive, so hat jedes Objekt eine injektive Auflösung.

**Beweis.**
Wir beweisen nur die Aussage über projektive Auflösungen; denn die Aussage über injektive Auflösungen ist die entsprechende Aussage in $\mathcal{C}^{\mathrm{opp}}$. Zunächst existiert ein Epimorphismus $P_0 \to M \to 0$, da $\mathcal{C}$ genug Projektive hat. Sei $K_0 := \ker(P_0 \to M)$. Das Objekt $K_0$ ist im Allgemeinen nicht projektiv, aber wir können einen Epimorphismus $P_1 \to K_0$ von einem projektiven Objekt $P_1$ finden. Damit ist die resultierende Sequenz

$$\begin{tikzcd}
P_1 \arrow[rr] \arrow[dr] & & P_0 \arrow[r] & M \arrow[r] & 0 \\
& K_0 \arrow[ur] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

exakt. Iteriert man dieses Verfahren, erhält man offensichtlich eine projektive Auflösung. □

**Bemerkung 6.1.5.**
Um Auflösungen zu motivieren, wollen wir lineare Gleichungssysteme diskutieren. Sei $K$ ein kommutativer Ring und $A$ eine $K$-Algebra. Sei $S$ ein beliebiger $A$-Modul, $B \in M(q \times p, A)$ eine Matrix und $(v_i)_{i=1,\ldots,q}$ eine Familie von Elementen in $S$. Dann suchen wir Lösungen $(u_j)_{j=1,\ldots p}$ mit $u_j \in S$ des inhomogenen linearen Gleichungssystems mit Werten in $S$

$$(*) \qquad \sum_{j=1}^{p} B_{ij} u_j = v_i \quad \text{mit} \quad i = 1, \ldots, q \ .$$

- Als Beispiel können wir für $K$ einen Körper wählen und den Polynomring $A = K[X_1, \ldots, X_s]$ in mehreren Variablen über einem Körper betrachten. Für jedes $s$-Tupel $(q_1, \ldots, q_s) \in K^s$ haben wir durch Einsetzen einen Auswertehomomorphismus $ev_{(q_1,\ldots,q_s)} : A = K[X_1, \ldots, X_s] \to K$. Zieht man die durch Skalarmultiplikation gegebene $K$-Modulstruktur auf $S = K^n$ entlang $ev_{(q_1,\ldots,q_s)}$ zurück, so erhält man auf $K^n$ eine $A$-Modulstruktur. Das homogene lineare Gleichungssystem zu $(*)$ ist dann ein Gleichungssystem, das polynomial von $s$ Parametern in $K$ abhängt.

- In einem anderen Beispiel ist $K = \mathbb{R}$ und $A$ die Algebra der reelwertigen glatten Funktionen auf einer glatten Mannigfaltigkeit $X$. Ist $X$ kompakt, so sind die projektiven endlicherzeugten $A$-Moduln gerade die Räume glatter Schnitte in Vektorbündeln über $X$. Sei $B$ ein linearer Differentialoperator; hat die Mannigfaltigkeit $X$ eine Metrik, etwa der Laplace-Operator. Dann suchen wir Lösungen des inhomogenen Systems linearer Differentialgleichungen $Bu = v$.

Wir fassen die Matrix $B$ durch Rechtsmultiplikation als Morphismus von freien $A$-Moduln auf:

$$F_1 = A^q \xrightarrow{\cdot B} F_0 = A^p$$

und betrachten nun den Quotientenmodul $M := F_0/\mathrm{Im}\, B$. Er kommt mit einer kanonischen Surjektion $\psi : A^p \to M$, so dass wir eine exakte Sequenz bekommen

$$F_1 = A^q \xrightarrow{B} F_0 = A^p \xrightarrow{\psi} M \to 0 \ .$$

Wenden wir für einen gegebenen $A$-Modul $S$ den kontravarianten linksexakten Funktor $\mathrm{Hom}_A(-, S)$ auf diese exakte Sequenz an, so finden wir die exakte Sequenz

$$0 \to \mathrm{Hom}_A(M, S) \to S^p \xrightarrow{B\cdot} S^q \ ,$$

wobei nun $B$ durch Linksmultiplikation wirkt. Insbesondere ist der $K$-Modul $\mathrm{Hom}_A(M, S)$ isomorph zum Kern und somit gleich dem Lösungsraum des homogenen Gleichungssystems mit Werten im Modul $S$. Man kann daher den Quotientenmodul $M = A^p/A^qB$ als eine "koordinatenfreie" Version des homogenen linearen Gleichungssystems ansehen, das aus der freien Auflösung von $M$ kommt. Die Homomorphismen aus dem Quotientenmodul $M$ in einen Modul $S$ geben den Lösungsraum zum homogenen Gleichungssystem für den Modul $S$. Man beachte: wählt man die Standardbasis $(e_i)_{i=1,\dots p}$ $A^p$ und setzt $u_i := \psi(e_i)$, dann hat $M$ die Erzeuger $(u_i)_{i=1,\dots p}$ modulo der Relationen $\sum_{j=1}^p B_{ij}u_j$ für $i = 1, \dots, q$.

Wir nehmen nun an, $A$ ist linksnoethersch. Dies ist zum Beispiel für den Polynomring $A = K[X_1, \dots, X_s]$ für einen Körper $K$ der Fall. Dann ist $\ker B$ als Untermodul eines endlich erzeugten Moduls endlich erzeugt. Wir finden einen endlich-erzeugten freien Modul $F_2 = A^r$ und eine Surjektion $F_2 \to \ker B$. Wir konstruieren so eine Auflösung

$$(**) \qquad F_2 \xrightarrow{X} F_1 = A^q \xrightarrow{B} F_0 = A^p \to M \to 0$$

durch endlich-erzeugte freie Moduln, die insbesondere eine projektive Auflösung ist.

Wir finden wiederum durch Anwenden des linksexakten kontravarianten Hom-Funktors einen Kettenkomplex

$$0 \to \mathrm{Hom}_A(M, S) \to S^p \xrightarrow{B\cdot} S^q \xrightarrow{X\cdot} S^r \ .$$

Eine notwendige Bedingung dafür, dass das inhomogene lineare Gleichungssystem $(*)$ eine Lösung hat, ist somit dass $Xv = 0$ gilt.

Betrachten wir mit Hilfe des Komplexes $(**)$ die homogene lineare Gleichung, die durch $B$ gegeben ist. Die Bilder von $r$ Erzeugenden von $F_2$ erzeugen den Lösungsraum des homogenen Gleichungssystems $Bu = 0$ in $F_0$. Über Ringen, im Gegensatz zu Körpern, ist dies aber im Allgemeinen eine Überparametrisierung: denn im allgemeinen geht die freie Auflösung geht weiter:

$$\cdots F_3 \to F_2 = R^r \xrightarrow{X} F_1 = R^q \xrightarrow{B} F_0 = R^p \to R^p/BR^q \to 0 \ .$$

Die Elemente des Moduls $F_3$ beschreiben also Abhängigkeiten zwischen Parametrisierungen; sie heißen Syzygien. Man kann zeigen, dass für den Ring $K[X_1, \dots, X_s]$ die freie Auflösung so gewählt werden kann, dass sie nach $s$ Schritten abbricht. Für einen Hauptidealring wie $K[X]$ wissen wir schon aus Betrachtung 3.1.3, dass freie Auflösungen der Länge 1 existieren.

## 6.2 Homologie und Homotopie

Wir bezeichnen mit $Ch_{\mathcal{C}}$ die Kategorie der Kettenkomplexe in einer abelschen Kategorie $\mathcal{C}$. Kettenkomplexe wurden in Definition 1.4.1 eingeführt. Die Morphismen sind hierbei die "Leitern" von Morphismen in $\mathcal{C}$, also kommutative Diagramme

$$\begin{tikzcd}
\cdots \arrow[r, "d_{n+1}"] & C_{n+1} \arrow[r, "d_n"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "d_{n-1}"] \arrow[d, "f_n"] & \cdots \\
\cdots \arrow[r, "d_{n+1}"] & D_{n+1} \arrow[r, "d_n"] & D_n \arrow[r, "d_{n-1}"] & \cdots
\end{tikzcd}$$

**Bemerkungen 6.2.1.**

1. Es gibt natürlich interessante Unterkategorien: etwa die der Kettenkomplexe, die nur in nicht-negativem oder nicht-positivem Grad nicht verschwinden, oder die beschr änkten Kettenkomplexe, für die nur endlich viele Objekte $C_i$ nicht das Nullobjekt in der abelschen Kategorie $\mathcal{C}$ sind. Der Einfachheit halber werden wir im Folgenden alle Morphismen in einem Kettenkomplex nur mit $d$ bezeichnen.

2. In einer Übungsaufgabe können Sie zeigen, dass die Kategorie $Ch_{\mathcal{C}}$ abelsch ist.

***Definition 6.2.2***

1. *Sei $(C_\bullet, d_\bullet) \in Ch_{\mathcal{C}}$. Die i-Zykel sind definiert als $Z_i(C_\bullet, d_\bullet) := \ker(d_{i-1}) \subset C_i$.*

2. *Die i-Ränder $B_i(C_\bullet, d_\bullet)$ sind definiert als das Bild von $d_i$ in $C_i$.*

3. *Das Bild $B_i$ ist ein Unterobjekt der Ketten $C_i$. Wegen der Kettenkomplexbedingung $d^2 = 0$ verschwindet die Komposition der Einbettung $B_i \xrightarrow{\iota} C_i$ mit dem Differential $C_i \xrightarrow{d} C_{i-1}$. Daher faktorisiert die Einbettung über den Kern $Z_i$ von $d$*

$$\begin{tikzcd}
B_i \arrow[r, "\iota"] \arrow[dr, dashed] & C_i \arrow[r, "d"] & C_{i-1} \\
& Z_i \arrow[u, "\ker d"'] &
\end{tikzcd}$$

*mit einem Monomorphismus. Die Ränder sind also ein Unterobjekt der Zykel. Die i-te Homologie des Komplexes $C_\bullet$ ist definiert als Kokern dieses Monomorphismus.*

*Realisieren wir die abelsche Kategorie explizit als volle Unterkategorie einer Kategorie von Moduln über einem Ring, so können wir auch mit Elementen rechnen. Die Zykel in $Z_i$ sind dann die Elemente*

$$Z_i := \{c_i \in C_i \mid d_{i-1}c_i = 0\}$$

*und die Ränder*

$$B_i := \{c_i \in C_i \mid \exists\, b_{i+1} \in C_{i+1} \text{ so dass } d_i b_{i+1} = c_i \ \} \ .$$

*Dann sind Ränder insbesondere Zykel, denn aus $c_i = d_i b_{i+1}$ folgt $d_{i-1}c_i = d_{i-1} \circ d_i b_{i+1} = 0$. Die Homologie ist dann der Quotient*

$$H_i(C_\bullet, d_\bullet) := Z_i/B_i = \ker(d_{i-1})/\mathrm{Im}\,(d_i) \ .$$

4. *Ein Kettenkomplex $C_\bullet$ heißt azyklisch , wenn $H_n(C_\bullet) = 0$ für $n \geq 1$ gilt.*

**Bemerkungen 6.2.3.**

1. Für jedes $n \in \mathbb{Z}$ ist die Zuordnung $H_n : Ch_\mathcal{C} \to \mathcal{C}$ ein Funktor, denn jede Abbildung von Kettenkomplexen bildet Kerne von $d$ auf Kerne von $d$ und Bilder von $d$ auf Bilder von $d$ ab. Für einen Kettenmorphismus $f$ wird üblicherweise $f_n$ statt $H_n(f)$ geschrieben.

2. Sei $P_\bullet \to M \to 0$ eine projektive Auflösung eines Objekts $M \in \mathcal{C}$. Dann ist der Komplex $P_\bullet \to 0$ azyklisch. Seine nullte Homologie ist $P_0/(\mathrm{Im}\,(P_1 \to P_0) = P_0/\ker(P_0 \to M) \cong M$.

3. Sei $C_\bullet$ ein Kettenkomplex, der in nicht-negativen Graden konzentriert ist, der also endet mit $\ldots \to C_1 \to C_0 \to 0$. Dann gilt $H_0(C_\bullet) = C_0/\mathrm{Im}\,(C_1 \to C_0)$ und wir haben durch die kanonische Surjektion auf den Quotienten einen surjektiven Morphismus $C_0 \to H_0(C_\bullet)$. Offenbar ist dann

$$\cdots \to C_n \to C_{n-1} \to \cdots \to C_0 \to H_0(C_\bullet) \to 0$$

ein Komplex. Dieser augementierte Komplex ist genau dann exakt, wenn der Kettenkomplex $C_\bullet$ azyklisch ist.

4. Die Bezeichnungen Zykel und Rand stammen aus der Topologie. Dort lässt sich $d_\bullet$ oft interpretieren als der geometrische Rand eines Objektes, z.B. einer Mannigfaltigkeit, und ein Zykel ist ein Objekt ohne Rand.

5. Betrachten wir als Beispiel einen Ring $R$ und ein Element $x \in R$. Dann können wir aus der Rechtsmultiplikation mit $x$ einen Kettenkomplex

$$0 \to R \xrightarrow{\cdot x} R \to 0$$

konstruieren. Dann ist $H_0(C_\bullet) = R/R.x$ und $H_1(C_\bullet) = \{r \in R | r.x = 0\} = \mathrm{Ann}(x)$.

6. Als etwas komplizierteres Beispiel betrachten wir für beliebige Elemente $a, b \in R$ eines kommutativen Rings $R$ den Komplex

$$0 \longrightarrow R \xrightarrow{X} R^2 \xrightarrow{A} R \longrightarrow 0$$

mit Matrizen

$$A = (a, b) \quad \text{und} \quad X = \begin{pmatrix} -b \\ a \end{pmatrix}$$

Dann ist $H_0(C_\bullet) = R/(ax + by)$ ein Maß für die Nicht-Trivialität der inhomogenen linearen Gleichung $ax + by = c$. Die Homologie $H_1(C_\bullet) = \{(r_1, r_2) \in R^2 | r_1 a + r_2 b = 0\}/ \{(-\lambda b, \lambda a)\}$ ist der Raum der Lösungen der homogenen linearen Gleichung modulo der trivialen Lösungen.

7. Es ist oft üblich, die Graduierung der Kettenkomplexe umzudrehen, d.h. die Abbildungen gehen nun von $C_i$ nach $C_{i+1}$, und die resultierende Homologie dann Kohomologie zu nennen. Der Einfachheit halber drehen wir nichts um und definieren die Kohomologie als $H^i(C_\bullet, d_\bullet) := H_{-i}(C_\bullet, d_\bullet)$ und definieren auch $C^i = C_{-i}$.

8. Man beachte, dass ein Komplex genau dann exakt ist, wenn seine Homologie verschwindet. Die Homologie misst also die Abweichung von der Exaktheit.

9. Es kann passieren, dass eine Abbildung zwischen zwei Kettenkomplexen zwar kein Isomorphismus ist, aber einen solchen in Homologie induziert. Hier ist ein Beispiel für $\mathcal{C} = Ab$:

$$\begin{tikzcd} \cdots \arrow[r] & 0 \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r, "2"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \cdots \\ \cdots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \mathbb{Z}_2 \arrow[r] & 0 \arrow[r] & \cdots \\ \text{Grad} & 2 & 1 & 0 & -1 & \end{tikzcd}$$

In beiden Fällen ist $H_0 = \mathbb{Z}_2$, und alle anderen Homologiegruppen verschwinden. Ein Morphismus von Kettenkomplexen $f_\bullet : C_\bullet \to D_\bullet$, der in jedem Grad in Homologie einen Isomorphismus $H_n(f) : \; H_n(C_\bullet) \xrightarrow{\sim} H_n(D_\bullet)$ induziert, heißt Quasi-Isomorphismus von Komplexen.

Eine Unterklasse von Homologieisomorphismen sind durch Kettenhomotopieäquivalenzen gegeben.

***Definition 6.2.4***

1. *Seien $f, g : C_\bullet \to D_\bullet$ zwei Kettenabbildungen. Eine Folge von Abbildungen $h_n : C_{n-1} \to D_n$ mit der Eigenschaft*
$$f - g = h \circ d + d \circ h$$
*heißt (Ketten-)homotopie von $g$ nach $f$. Graphisch:*

$$\begin{tikzcd} \cdots & \arrow[r] & C_{n+1} \arrow[r] \arrow[d] \arrow[dll, dashed] & C_n \arrow[r] \arrow[d] \arrow[dl, dashed] & C_{n-1} \arrow[r] \arrow[d] \arrow[dl, dashed] & C_{n-2} \arrow[r] \arrow[d] \arrow[dl, dashed] & \cdots \\ \cdots & \arrow[r] & D_{n+1} \arrow[r] & D_n \arrow[r] & D_{n-1} \arrow[r] & D_{n-2} \arrow[r] & \cdots \end{tikzcd}$$

*wobei an den vertikalen Pfeilen $(f-g)_n$ und an den diagonalen Pfeilen $h_n$ steht. Man beachte, dass hier* kein *kommutierendes Diagramm vorliegt. Existiert eine Kettenhomotopie zwischen $f$ und $g$, so nennen wir die beiden Abbildungen (ketten-)homotop und schreiben $f \simeq g$.*

2. *Sind $f : C_\bullet \to D_\bullet$ und $g : D_\bullet \to C_\bullet$ Kettenabbildungen mit der Eigenschaft $f \circ g \simeq \mathrm{id}_{D_\bullet}$ und $g \circ f \simeq \mathrm{id}_{C_\bullet}$, so nennen wir die Komplexe $C_\bullet$ und $D_\bullet$ (ketten-)homotopieäquivalent und schreiben $C_\bullet \simeq D_\bullet$. Dies definiert eine Äquivalenzrelation auf Kettenkomplexen.*

**Bemerkungen 6.2.5.**

1. Eine Kettenhomotopie ist natürlich schon aus Gradgründen keine Kettenabbildung.

2. Die folgende Überlegung gibt einen Hinweis darauf, warum es sinnvoll ist, Kettenhomotopien einzuführen. Wir betrachten nur Kettenkomplexe $C_\bullet$ und $D_\bullet$ von Moduln, die in den Graden 1 und 0 konzentriert sind. Wir ordnen dem Kettenkomplex $C_\bullet$ die Kategorie $\mathcal{C}(C_\bullet)$ zu, deren Objekte die Elemente von $C_0$ sind mit Morphismen $\mathrm{Hom}(c', c) := \{c_1 \in C_1 \,|\, dc_1 = c - c'\}$. Die Komposition von Morphismen ist die Addition in $C_1$.

Dann liefert jede Kettenabbildung $f_\bullet : C_\bullet \to D_\bullet$ einen Funktor

$$\mathcal{C}(f) : \mathcal{C}(C_\bullet) \ \to \mathcal{C}(D_\bullet)$$

Dieser bildet das Objekt $c_0 \in C_0$ auf das Objekt $f(c_0) \in D_0$ ab und den Morphismus $c_0' \xrightarrow{c_1} c_0$ auf $f(c_0') \xrightarrow{f(c_1)} f(c_0)$. In der Tat gilt $f(c_1) \in \mathrm{Hom}\,(f(c_0), f(c_0'))$, denn

$$df(c_1) = f(dc_1) = f(c_0 - c_0') = f(c_0) - f(c_0') \quad .$$

Seien $f, g : C_\bullet \to D_\bullet$ Morphismen von Kettenkomplexen. Eine Kettenhomotopie $h : g \rightsquigarrow f$ liefert dann eine natürliche Transformation $\mathcal{C}(h) : \mathcal{C}(g) \Rightarrow \mathcal{C}(f)$. Die einzige nichttriviale Abbildung bei so kurzen Kettenkomplexen ist nämlich $h_0 : C_0 \to D_1$. Wegen

$$f(c_0) - g(c_0) = h_{-1}(dc_0) + dh_0(c_0) = dh_0(c_0)$$

ist $h_0(c_0) \in \mathrm{Hom}(g(c_0), f(c_0))$. Ausserdem folgt für einen Morphismus $c_1 \in \mathrm{Hom}(c_0', c_0)$ aus der Gleichung

$$f(c_1) - g(c_1) = h_0(dc_1) + dh_1(c_1) = h_0(dc_1) = h_0(c_0) - h_0(c_0')$$

die Kommutativität des Diagramms in $\mathcal{C}(D_\bullet)$

$$\begin{tikzcd}
g(c_0') \arrow[r, "g(c_1)"] \arrow[d, "h_0(c_0')"'] & g(c_0) \arrow[d, "h_0(c_0)"] \\
f(c_0') \arrow[r, "f(c_1)"'] & f(c_0)
\end{tikzcd}$$

**Satz 6.2.6.**

1. Kettenhomotope Abbildungen induzieren die gleiche Abbildung in Homologie.

2. Kettenhomotopieäquivalenzen induzieren Isomorphismen in Homologie.

**Beweis.**
Offensichtlich folgt die zweite Aussage sofort aus der ersten und der Definition 6.2.4.2.

Sei also eine Kettenhomotopie $h$ gegeben. Wir müssen zeigen, dass $\hat{h} := (h \circ d + d \circ h)$ die Nullabbildung in Homologie induziert. Schränken wir $\hat{h}_n$ auf die Zykel ein, so gilt offensichtlich: $\hat{h}_{|\ker d} = d \circ h$. Damit gilt aber auch, dass $\hat{h}_{|\ker d} \subseteq \mathrm{Im}\, d$, und somit $\hat{h}_* = 0$ in Homologie. □

In Beispiel 6.2.3.9 ist der Kettenhomomorphismus, der einen Homologieisomorphismus induziert, allerdings keine Kettenhomotopieäquivalenz: alle Kettenabbildungen von dem unteren Komplex in den oberen sind null, also kann es kein Inverses bis auf Homotopie geben.

## 6.3 Das Fundamentallemma der homologischen Algebra

Die folgende Aussage ist zentral für die gesamte homologische Algebra:

**Satz 6.3.1.**
Sei $f : M \to N$ ein Morphismus in einer abelschen Kategorie, $P_\bullet \to M \to 0$ ein Kettenkomplex aus projektiven Objekten und $N_\bullet \to N \to 0$ eine beliebige exakte Sequenz.

1. Dann gibt es eine Fortsetzung $f_\bullet : P_\bullet \to N_\bullet$ von $f$ zu einem Morphismus von Kettenkomplexen.

2. Je zwei solche Fortsetzungen $f_\bullet, f'_\bullet$ sind kettenhomotop.

Analoge Aussagen gelten natürlich auch für injektive Auflösungen.

**Beweis.**

- Betrachte das Diagramm

$$\begin{tikzcd} P_0 \arrow[r, "d"] \arrow[d, dashed] & M \arrow[d, "f"] & \\ N_0 \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

  Da $P_0$ projektiv ist, gibt es ein Fortsetzung des Morphismus $f \circ d$ zu $P_0 \to N_0$, so dass das entstehende Diagramm kommutiert. Diese Fortsetzung ist im Allgemeinen nicht eindeutig. Bezeichnet $M' \subset P_0$ den Kern der oberen horizontalen Abbildung, also den Kern des Differentials, und $N' \subset N_0$ den Kern der unteren, so betrachten wir die Einschränkung der Abbildung $P_0 \to N_0$ auf $M'$. Sei $x \in \ker d = M'$, dann gilt $df_0(x) = f_1(dx) = f_1(0) = 0$, also erhalten wir durch Restriktion auf $\ker d$ eine Abbildung $f' : M' \to N'$. Wir haben also ein neues Diagramm

$$\begin{tikzcd} P_1 \arrow[r] \arrow[d, dashed] & M' \arrow[d, "f'"] & \\ N_1 \arrow[r] & N' \arrow[r] & 0 \end{tikzcd}$$

  in dem die untere Zeile wiederum exakt ist. Da auch $P_1$ nach Voraussetzung projektiv ist, kann man in der gleichen Weise wie vorhin fortfahren und erhält einen Morphismus $P_1 \to N_1$. Insgesamt finden wir eine Fortsetzung über die gesamten Auflösungen.

- Für den zweiten Teil der Aussage genügt es zu zeigen, dass jede Hochhebung $f_\bullet$ der Nullabbildung $M \xrightarrow{0} N$ kettenhomotop zur Nullabbildung auf dem Kettenkomplex ist, d.h. es gibt eine Kettenhomotopie $h$, so dass $f = h \circ d + d \circ h$ gilt. Betrachte das Leiterdiagramm:

$$\begin{tikzcd} {} \arrow[r] & P_0 \arrow[r, "d"] \arrow[d, "f_0"] & M \arrow[d, "0"] & \\ N_1 \arrow[r, "d"'] & N_0 \arrow[r, "d"'] & N \arrow[r] & 0 \end{tikzcd}$$

  Da $d \circ f_0 = 0 \circ d = 0$ gilt, liefert $f_0$ einen Morphismus $P_0 \to \ker(N_0 \to N)$. Wegen der Exaktheit der Sequenz $N_\bullet$ ist der Morphismus $N_1 \to \ker(N_0 \to N)$ surjektiv. Im Diagramm

$$\begin{tikzcd} & P_0 \arrow[dl, dashed, "h_0"'] \arrow[d] & \\ N_1 \arrow[r] & \ker(N_0 \to N) \arrow[r] & 0 \end{tikzcd}$$

  erhalten wir wegen der Projektivität von $P_0$ eine Hochhebung $h_0 : P_0 \to N_1$ über $N_1 \to \ker(N_0 \to N) \to 0$, so dass $d \circ h_0 = f_0$. Ähnlich wie vorher lässt sich das Argument jetzt für den Morphismus $f_1 - h_0 \circ d$ wiederholen:

$$\begin{tikzcd}
 & P_1 \arrow[r, "d"] \arrow[d, "f_1"] \arrow[dl, dashed] & P_0 \arrow[d, "f_0"] \arrow[dl, "h_0"'] & \\
N_2 \arrow[r, "d"'] & N_1 \arrow[r, "d"'] & \ker d \arrow[r] & 0
\end{tikzcd}$$

Beachte, dass in dem Quadrat nur das untere Dreieck kommutiert! Es gilt aber $d \circ (f_1 - h_0 \circ d) = d \circ f_1 - f_0 \circ d = 0$. Damit lässt sich $f_1 - h_0 \circ d$ zu einer Abbildung $h_1$ nach $N_2$ hochheben, so dass $d \circ h_1 + h_0 \circ d = f_1$ gilt. Iteriert man die Konstruktion, ist der Beweis vollständig.

□

**Korollar 6.3.2.**
Je zwei projektive (injektive) Auflösungen eines Objekts sind kettenhomotopie-äquivalent.

**Beweis.**
Seien $P_\bullet$ und $P'_\bullet$ zwei projektive Auflösungen eines Objekts $M \in \mathcal{C}$. Dann können wir wegen Satz 6.3.1.1 die Identität auf $M$ fortsetzen zu Morphismen von Kettenkomplexen $f : P_\bullet \to P'_\bullet$ und $f' : P'_\bullet \to P_\bullet$. Dann ist aber auch $f \circ f'$ eine Fortsetzung der Identität $\mathrm{id}_M$ zu einem Endomorphismus des Kettenkomplexes $P'_\bullet$. Eine andere Fortsetung der Identität $\mathrm{id}_M$ ist natürlich die Identität in jedem Grad. Nach Satz 6.3.1.2 sind diese beiden Fortsetzungen kettenhomotop. Somit stellen $f, f'$ eine Kettenhomotopieäquivalenz dar. □

Die Idee ist nun, Objekte der Kategorie $\mathcal{C}$ durch Kettenkomplexe von besseren, d.h. hier projektiven oder injektiven Objekten zu ersetzen. Wie wir gerade gesehen haben, können auch die Morphismen bis auf Kettenhomotopie geliftet werden.

Sei nun $F$ ein additiver Funktor, $F : \mathcal{C} \to \mathcal{D}$. Durch termweise Anwendung von $F$ auf einen Kettenkomplex $P_\bullet$ in $Ch_\mathcal{C}$ erhält man wegen der Additivität von $F$ wiederum einen Kettenkomplex $F(P_\bullet)$. Selbst wenn $P_\bullet$ exakt ist, ist der Kettenkomplex $F(P_\bullet)$ im Allgemeinen nur dann exakt, wenn der Funktor $F$ exakt ist.

***Definition 6.3.3***
*Seien $\mathcal{C}, \mathcal{D}$ abelsche Kategorien und $F : \mathcal{C} \to \mathcal{D}$ ein additiver Funktor.*

1. *Hat $\mathcal{C}$ genug Projektive, so sind die <u>linksabgeleiteten</u> Funktoren $L_nF : \mathcal{C} \to \mathcal{D}$ von F auf Objekten gegeben durch die Homologie des Komplexes $F(P_\bullet)$:*

   $$L_nF(X) := H_n(F(P_\bullet)) \ ,$$

   *wobei $P_\bullet \to X$ eine beliebige projektive Auflösung von $X$ ist.*

2. *Hat $\mathcal{C}$ genug Injektive, so sind die <u>(rechts-)abgeleiteten Funktoren</u> $R^nF : \mathcal{C} \to \mathcal{D}$ analog auf Objekten definiert:*

   $$R^nF(X) := H^n(F(I_\bullet)) \ ,$$

   *wobei $X \to I_\bullet$ eine injektive Auflösung ist.*

**Bemerkungen 6.3.4.**

- Die abgeleiteten Funktoren verschwinden, wenn der Funktor $F$ exakt ist.
- Wegen des Fundamentallemmas 6.3.1 sind die abgeleiteten Funktoren bis auf Isomorphie wohldefiniert: denn wenn $P_\bullet$ und $P'_\bullet$ zwei verschiedene projektive Auflösungen sind, so gibt es nach Korollar 6.3.2 eine Kettenhomotopieäquivalenz $P_\bullet \simeq P'_\bullet$; deren Bild unter $F$ liefert eine Kettenhomotopieäquivalenz $F(P_\bullet) \simeq F(P_\bullet)$. Aus Satz 6.2.6 folgt dann, dass die Homologiegruppen isomorph sind.
- Aus dem Fundamentallemma 6.3.1 folgt auch, dass die abgeleiteten Funktoren wirklich Funktoren sind, also auch auf Morphismen definiert sind. Denn ist $f : X \to Y$ ein Morphismus, so kann man $f$ bis auf Homotopie in eindeutiger Weise zu einem Morphismus $f_\bullet : P_\bullet \to Q_\bullet$ der projektiven Auflösungen $P_\bullet$ und $Q_\bullet$ hochheben. Damit erhält man einen Morphismus $F(f_\bullet) : F(P_\bullet) \to F(Q_\bullet)$ von Kettenkomplexen, der wiederum einen Morphismus $F(f_\bullet)_*$ auf der Homologie induziert. Aus Satz 6.2.2 folgt, dass dieser nicht von der Wahl der Liftung $f_\bullet$ abhängt. Dass die Funktoraxiome erfüllt sind, überprüft man leicht.

**Lemma 6.3.5.**
Sei ein Funktor $F$ rechtsexakt; dann gilt $L_0F = F$. Sei $F$ linksexakt; dann gilt $R^0F = F$.

**Beweis.**
Wir zeigen nur den ersten Teil der Aussage. Ist $P_\bullet \to X$ eine projektive Auflösung, so impliziert die Rechtsexaktheit von $F$, dass die Sequenz

$$F(P_1) \to F(P_0) \to F(X) \to 0$$

exakt ist. Also gilt mit Hilfe des Homomorphiesatzes

$$F(X) \cong F(P_0)/(\ker(F(P_0) \to F(X)) \cong F(P_0)/\mathrm{Im}\,(F(P_1)) = H_0(F(P_\bullet)) \ .$$

□

Wir werden ab sofort linksabgeleitete Funktoren nur für einen rechtsexakten Funktor und rechtsabgeleitete Funktoren nur für einen linksexakten Funktor betrachten.

## 6.4 Die lange exakte Sequenz

Wir haben bereits in Lemma 6.3.5 gesehen, dass die abgeleiteten Funktoren $L_nF$ bzw. $R^nF$ verschwinden, wenn der Funktor $F$ exakt ist. Um Aussagen im Fall zu machen, wenn die abgeleiteten Funktoren nicht verschwinden, brauchen wir die lange exakte Sequenz von abgeleiteten Funktoren. Wir brauchen dazu einige Vorbereitungen.

**Lemma 6.4.1** (Schlangenlemma)**.**
Das folgende Diagramm in einer abelschen Kategorie $\mathcal{C}$ sei kommutativ mit exakten Zeilen:

$$(*) \qquad \begin{tikzcd} & M' \arrow[r, "\iota"] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "\iota"] & N \arrow[r] & N'' & \end{tikzcd}$$

Dann gibt es eine exakte Sequenz

$$\ker f' \to \ker f \to \ker f'' \xrightarrow{\partial} \mathrm{coker} f' \to \mathrm{coker} f \to \mathrm{coker} f''$$

mit einem Morphismus $\partial$, der im Beweis beschrieben wird. Der Name "Schlangenlemma" erklärt sich, wenn man oben die Zeile $\ker f' \to \ker f \to \ker f''$ und unten die Zeile $\mathrm{coker} f' \to \mathrm{coker} f \to \mathrm{coker} f''$ hinzunimmt:

$$
\begin{tikzcd}
 & \ker f' \arrow[r] \arrow[d] & \ker f \arrow[r] \arrow[d] & \ker f'' \arrow[d] \arrow[dddll, dashed, rounded corners] & \\
 & M' \arrow[r, "\iota"] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\iota"] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[d] & \\
 & \mathrm{coker} f' \arrow[r] & \mathrm{coker} f \arrow[r] & \mathrm{coker} f'' &
\end{tikzcd}
$$

Ist $M' \to M$ ein Monomorphismus, so auch $\ker f' \to \ker f$. Ist $N \to N''$ Epimorphismus, so auch $\mathrm{coker} f \to \mathrm{coker} f''$.

**Beweis.**
Durch Diagrammjagd, wobei wir nach dem vollen Einbettungssatz voraussetzen dürfen, dass $\mathcal{C}$ eine volle abelsche Unterkategorie von Moduln über einem Ring $R$ ist. Für Beweise solcher Lemmata, die Diagrammjagd vermeiden, verweisen wir auf Saunders MacLane, Categories for the Working Mathematician, p. 202 ff.

- Zunächst zur Konstruktion von $\partial$. Sei $m'' \in \ker f''$. Da $M \to M''$ surjektiv ist, gibt es ein Urbild $m_0 \in M$, und wegen der Exaktheit bei $M$ hat jedes andere solche Urbild die Form $m = m_0 + \iota(m')$ für $m' \in M'$. Nun wird $f(m_0) \in N$ unter $N \to N''$ nach 0 abgebildet, denn es war $m'' \in \ker f''$. Aus der Exaktheit der unteren Zeile an beiden Stellen folgt, dass es ein eindeutiges $n_0' \in N'$ gibt mit $n_0' \mapsto f(m_0)$. Hätten wir an Stelle von $m_0 \in M$ mit $m := m_0 + \iota(m')$ mit $m' \in M'$ gearbeitet, so wäre wegen $N' \ni n_0' + f'(m') \mapsto f(m) \in N$ das Element $n_0' + f'(m')$ ein Urbild von $f(m)$. Somit ist die Klasse $[n_0'] =: \partial(m'')$ wohldefiniert bis auf ein Bild unter $f'$, also wohldefiniert in $\mathrm{coker} f'$. Nach Konstruktion ist $\partial$ ein Modulmorphismus.

- Zum Beweis der Exaktheit können wir uns auf zwei Stellen beschränken, z.B. Exaktheit bei $\ker f$ und Exaktheit bei $\ker f''$. Die Zusatzaussage über die Injektivität von $\ker f' \to \ker f$ ist offensichtlich, und die Exaktheit bei $\mathrm{coker} f'$ und $\mathrm{coker} f$ und die Zusatzaussage über die Surjektivität folgen dann durch Übergang zu der opponierten Kategorie $\mathcal{C}^{\mathrm{opp}}$.

- Exaktheit bei $\ker f$. Aus der Exaktheit der oberen Zeile folgt sofort, dass das Bild von $\ker f' \to \ker f$ im Kern von $\ker f \to \ker f''$ liegt. Sei $m \in \ker f$ mit $m \mapsto 0 \in M''$. Wegen der Exaktheit der oberen Zeile gibt es ein Urbild $m' \in M'$, von dem aber noch gezeigt werden muss, dass es im Untermodul $\ker f' \subset M'$ liegt. Aus $f(m) = 0$ folgt $f'(m') \mapsto 0 \in N$. Da die untere Zeile exakt ist, ist $\iota : N' \to N$ injektiv; also muss schon $f'(m') = 0$ sein.

- Exaktheit bei $\ker f''$. Wir verwenden die Bezeichnungen von Elementen aus dem ersten Teil des Beweises, wo die Schlangenabbildung konstruiert wurde. Zunächst zeigen wir, dass die Komposition $\ker f \to \ker f'' \xrightarrow{\partial} \mathrm{coker} f'$ null ist. Ist $m'' \in M''$ das Bild eines

Elements $m \in \ker f$ unter $M \to M''$, so ist $f(m) = 0$ und es gilt nach Konstruktion von $\partial$, dass $\partial(m'') = 0$.

Sei nun $m'' \in \ker \partial \cap \ker f''$; gesucht ist ein Urbild in $\ker f$. Wir finden wegen der Exaktheit der oberen Zeile ein Urbild $m \in M$, das aber nicht unbedingt in $\ker f$ liegt. Aber $f(m) \in N$ hat ein Urbild $n'$ in $N'$, da $f(m) \mapsto 0 \in N''$. Da nach Annahme $\partial(m'') = 0$ gilt, gibt es ein Urbild $m' \in M'$ von $n'$. Sei $m_0$ das Bild von $m'$ in $M$, also $m_0 = \iota(m')$. Die Differenz $\delta := m - m_0 \in M$ hat das gleiche Bild in $M''$ wie $m$, also das vorgegebene $m''$. Es gilt aber auch

$$f(\delta) = f(m) - f(m_0) = f(m) - \iota f'(m') = f(m) - \iota n' = 0 \ .$$

Im letzten Schritt wurde benutzt, dass $n'$ ein Urbild von $f(m) \in N$ ist. Also ist $\delta$ das gesuchte Urbild von $m''$ in $\ker f$.

$\square$

**Bemerkung 6.4.2** (Natürlichkeit)**.**
Aus der Konstruktion folgt, dass der Schlangenmorphismus $\partial$ natürlich ist, d.h., wenn wir einen Morphismus von Diagrammen $D_1 \to D_2$ der Form $(*)$ in Satz 6.4.1 haben, so kommutiert das Diagramm

$$\begin{tikzcd}
\ker(f''_{D_1} : M''_{D_1} \to N''_{D_1}) \arrow[r, "\partial"] \arrow[d] & \mathrm{coker}(f'_{D_1} : M'_{D_1} \to N'_{D_1}) \arrow[d] \\
\ker(f''_{D_2} : M''_{D_2} \to N''_{D_2}) \arrow[r, "\partial"] & \mathrm{coker}(f'_{D_2} : M'_{D_2} \to N'_{D_2})
\end{tikzcd}$$

Die Kategorie der Kettenkomplexe $Ch_{\mathcal{C}}$ einer abelschen Kategorie ist wieder eine abelsche Kategorie. Daher ist klar, was eine kurze exakte Sequenz

$$0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$$

von Kettenkomplexen ist. Insbesondere gilt für eine exakte Sequenz von Kettenkomplexen, dass für jedes $n$ die Sequenz $0 \to M'_n \to M_n \to M''_n \to 0$ exakt ist.

**Satz 6.4.3.**
Ist $0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$ eine kurze exakte Sequenz von Kettenkomplexen in $\mathcal{C}$, so gibt es eine lange exakte Sequenz

$$\cdots \to H_i(M'_\bullet) \to H_i(M_\bullet) \to H_i(M''_\bullet) \xrightarrow{\partial} H_{i-1}(M'_\bullet) \to \cdots$$

in Homologie.

**Beweis.**
Wir nehmen wieder an, dass $\mathcal{C}$ eine volle Unterkategorie der Kategorie der $R$-Moduln über einem Ring $R$ ist. Das kommutierende Diagramm

$$\begin{tikzcd}
0 \arrow[r] & M'_n \arrow[r] \arrow[d, "d"'] & M_n \arrow[r] \arrow[d, "d"'] & M''_n \arrow[r] \arrow[d, "d"'] & 0 \\
0 \arrow[r] & M'_{n-1} \arrow[r] & M_{n-1} \arrow[r] & M''_{n-1} \arrow[r] & 0
\end{tikzcd}$$

zusammen mit dem Schlangenlemma 6.4.1 liefert, weil der Kern des Differentials $d$ gerade die Zykel und das Bild die Ränder sind, eine lange exakte Sequenz

$$0 \to Z_n M' \to Z_n M \to Z_n M'' \to \frac{M'_{n-1}}{B_{n-1}M'} \to \frac{M_{n-1}}{B_{n-1}M} \to \frac{M''_{n-1}}{B_{n-1}M''} \to 0$$

Daher sind die Zeilen exakt in dem kommutierenden Diagramm

$$\begin{tikzcd} & M'_n/B_nM' \arrow[r] \arrow[d, "d"] & M_n/B_nM \arrow[r] \arrow[d, "d"] & M''_n/B_nM'' \arrow[r] \arrow[d, "d"] & 0 \\ 0 \arrow[r] & Z_{n-1}M' \arrow[r] & Z_{n-1}M \arrow[r] & Z_{n-1}M'' & \end{tikzcd}$$

In diesem Diagramm gilt $\ker d = H_n$ und $\operatorname{coker} d = H_{n-1}$. Also liefert eine erneute Anwendung des Schlangenlemmas 6.4.1 die lange exakte Sequenz in Homologie. □

**Satz 6.4.4** (Hufeisenlemma)**.**

1. Sei $\mathcal{C}$ eine abelsche Kategorie mit genug Injektiven, $\mathcal{D}$ eine beliebige abelsche Kategorie und $F : \mathcal{C} \to \mathcal{D}$ ein linksexakter additiver Funktor. Sei

$$0 \to M' \xrightarrow{\iota} M \xrightarrow{p} M'' \to 0$$

eine kurze exakte Sequenz in $\mathcal{C}$. Dann gibt es eine lange exakte Sequenz in $\mathcal{D}$

$$0 \to R^0F(M') \to \cdots \to R^iF(M') \xrightarrow{R^iF(\iota)} R^iF(M) \xrightarrow{R^iF(p)} R^iF(M'') \xrightarrow{\partial} R^{i+1}F(M') \to \cdots$$

2. Hat $\mathcal{C}$ genug Projektive und ist der Funktor $F$ rechtsexakt, dann gibt es eine lange exakte Sequenz in $\mathcal{D}$

$$\cdots \to L_iF(M') \xrightarrow{L_iF(\iota)} L_iF(M) \xrightarrow{L_iF(p)} L_iF(M'') \xrightarrow{\partial} L_{i-1}F(M') \xrightarrow{\iota_*} \cdots \to L_0F(M'') \to 0$$

Der Homomorphismus $\partial$ heißt Verbindungshomomorphismus.

**Beweis.**
Um abgeleitete Funktoren zu berechnen, müssen wir projektive Auflösungen von $P'_\bullet \to M', P_\bullet \to M$ und $P''_\bullet \to M''$ betrachten. Um Satz 6.4.3 anwenden zu können, sollen aber diese Auflösungen eine kurze exakte Sequenz $0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$ von Kettenkomplexen bilden, d.h. es soll das Diagramm

$$\begin{tikzcd} & P'_n \arrow[r] \arrow[d] & P_n \arrow[r] \arrow[d] & P''_n \arrow[d] & \\ & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\ & P'_0 \arrow[r] \arrow[d, "\epsilon'"'] & P_0 \arrow[r] \arrow[d, "\epsilon"'] & P''_0 \arrow[d, "\epsilon''"'] & \\ 0 \arrow[r] & M' \arrow[r, "\iota"] & M \arrow[r] & M'' \arrow[r] & 0 \end{tikzcd}$$

kommutieren. Hierbei sind $\epsilon'$ und $\epsilon''$ die Augmentationen aus der projektiven Auflösung von $M'$ bzw. $M''$. Dann folgt die Behauptung aus Satz 6.4.3.

Dazu wählen wir uns zwei projektive Auflösungen $P'_\bullet \to M'$ und $P''_\bullet \to M''$ und setzen $P_0 := P'_0 \oplus P''_0$. Wir betrachten auf der ersten Komponente $\iota \circ \epsilon' : P'_0 \to M$. Für die zweite Komponente beachten wir, dass $M \to M''$ surjektiv ist, und benutzen die Projektivität von $P''_0$, um $\epsilon''$ zu einem Morphismus $P''_0 \to M$ zu heben. Zusammen erhalten wir einen Morphismus $\epsilon : P_0 = P'_0 \oplus P''_0 \to M$, so dass das Diagramm

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker(\epsilon') \arrow[r] \arrow[d] & \ker(\epsilon) \arrow[r] \arrow[d] & \ker(\epsilon'') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P'_0 \arrow[r] \arrow[d, "\epsilon'"] & P_0 \arrow[r] \arrow[d, "\epsilon"] & P''_0 \arrow[r] \arrow[d, "\epsilon''"] & 0 \\
0 \arrow[r] & M' \arrow[r, "\iota"] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

kommutiert. Die beiden unteren Zeilen sind exakt. Aus dem Schlangenlemma folgt, dass die obere Zeile exakt ist und $\mathrm{coker}(\epsilon) = 0$, so dass $P_0 \to M$ surjektiv ist.

Damit haben wir die erste Etage aufgefüllt. Wir erhalten nun die Situation

$$\begin{tikzcd}
 & {} \arrow[d] & & {} \arrow[d] & \\
 & P'_0 \arrow[d] & & P''_0 \arrow[d] & \\
0 \arrow[r] & \ker(\epsilon') \arrow[r] \arrow[d] & \ker(\epsilon) \arrow[r] \arrow[d] & \ker(\epsilon'') \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

die wieder ein Hufeisen ist, und fahren induktiv fort. □

**Bemerkungen 6.4.5.**

1. Die rechtsabgeleiteten Funktoren eines linksexakten Funktors verschwinden genau dann, wenn der Funktor $F$ exakt ist. Die Exaktheit von $F$ folgt hierbei aus dem Verschwinden von $R^1F$ bzw. $L_1F$, vgl. auch die Übungen.

2. Aus der Natürlichkeit der Schlangenabbildung kann man auch hier Natürlichkeitsaussagen ableiten: wenn

$$\begin{tikzcd}
0 \arrow[r] & M'_\bullet \arrow[r] \arrow[d] & M_\bullet \arrow[r] \arrow[d] & M''_\bullet \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N'_\bullet \arrow[r] & N_\bullet \arrow[r] & N''_\bullet \arrow[r] & 0
\end{tikzcd}$$

ein kommutierendes Diagramm von exakten Sequenzen von Kettenkomplexen ist, so erhalten wir einen Morphismus zwischen den zugehörgen langen exakten Sequenzen aus Satz 6.4.3, also eine kommutierende Leiter

$$\begin{tikzcd}
\cdots H_i(M'_\bullet) \arrow[r] \arrow[d] & H_i(M_\bullet) \arrow[r] \arrow[d] & H_i(M''_\bullet) \arrow[r, "\partial"] \arrow[d] & H_{i-1}(M'_\bullet) \arrow[r] \arrow[d] & \cdots \\
\cdots H_i(N'_\bullet) \arrow[r] & H_i(N_\bullet) \arrow[r] & H_i(N''_\bullet) \arrow[r, "\partial"] & H_{i-1}(N'_\bullet) \arrow[r] & \cdots
\end{tikzcd}$$

Wenn

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0
\end{tikzcd}$$

ein kommutatives Diagramm mit kurzen exakten Zeilen in einer Kategorie $\mathcal{C}$ mit genug Projektiven ist, so kommutiert auch die induzierte Leiter aus Satz 6.4.4

$$\begin{tikzcd}
\cdots \arrow[r] & L_iF(M') \arrow[r, "\iota_*"] \arrow[d] & L_iF(M) \arrow[r, "p_*"] \arrow[d] & L_iF(M'') \arrow[r, "\partial"] \arrow[d] & L_{i-1}F(M') \arrow[r, "\iota_*"] \arrow[d] & \cdots \arrow[r] & L_0F(M'') \rightarrow 0 \\
\cdots \arrow[r] & L_iF(N') \arrow[r, "\iota_*"] & L_iF(N) \arrow[r, "p_*"] & L_iF(N'') \arrow[r, "\partial"] & L_{i-1}F(N') \arrow[r, "\iota_*"] & \cdots \arrow[r] & L_0F(N'') \rightarrow 0
\end{tikzcd}$$

## 6.5 Tor und Ext

Die wichtigsten abgeleiteten Funktoren sind die Ableitungen des Tensorprodukts und des Hom-Funktors.

***Definition 6.5.1***
*Sei $R$ ein Ring.*

1. *Definiere zu einem $R$-Rechtsmodul $X$ einen Funktor $F_X : R-\mathrm{Mod} \to \mathrm{Ab}$ durch $F_X(Y) := X \otimes_R Y$. Dieser Funktor ist rechtsexakt (vgl. Beispiele 2.3.12.3). Seine linksabgeleiteten Funktoren bezeichnen wir mit*
$$\mathrm{Tor}_n^R(X,Y) := L_nF_X(Y) \ .$$

2. *Definiere zu einem $R$-Modul $X$ einen Funktor $G_X : (R-\mathrm{Mod})^{\mathrm{opp}} \to \mathrm{Ab}$ durch $G_X(Y) := \mathrm{Hom}_R(Y,X)$. $G_X$ ist linksexakt (vgl. Beispiele 2.3.12.5). Seine rechtsabgeleiteten Funktoren bezeichnen wir mit*
$$\mathrm{Ext}_R^n(Y,X) := R^nG_X(Y) \ .$$

In der Definition von Ext wird eine injektive Auflösung in $(R-\mathrm{Mod})^{\mathrm{opp}}$ verwendet. Dies ist aber tatsächlich das gleiche wie eine projektive Auflösung in $R-\mathrm{Mod}$.

Folgende Beobachtungen folgen sofort aus den Definitionen:

- $\mathrm{Tor}_n^R(X,Y) = 0$ für alle $Y$ und für alle $n > 0$ genau dann, wenn der Rechtsmodul $X$ flach ist.
- $\mathrm{Ext}_R^n(Y,X) = 0$ für alle $Y$ und für alle $n > 0$ genau dann, wenn der Modul $X$ injektiv ist.
- Tor und Ext sind nicht nur Funktoren in der Variablen $Y$, sondern auch in $X$.

**Beispiele 6.5.2.**

1. Sei $R = \mathbb{Z}$ und $Y = \mathbb{Z}_n$. Eine freie und daher auch projektive Auflösung des $\mathbb{Z}$-Moduls $Y = \mathbb{Z}_n$ ist gegeben durch den augmentierten Komplex

$$0 \to \mathbb{Z} \stackrel{n\cdot}{\to} \mathbb{Z} \to \mathbb{Z}_n \to 0\,.$$

Wir berechnen nun $\mathrm{Tor}_k^{\mathbb{Z}}(X,Y)$ für den $\mathbb{Z}$-Modul $X = \mathbb{Z}_m$. Wegen $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}_m$ liefert Tensorieren der zugehörigen projektiven Auflösung mit $\mathbb{Z}_m$ den Komplex

$$0 \to \mathbb{Z}_m \stackrel{n\cdot}{\to} \mathbb{Z}_m \to 0\ ,$$

dessen Homologie $\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n)$ ergibt:

$$\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \begin{cases} \mathbb{Z}_{\mathrm{ggT}(m,n)}; & \text{falls } k = 0,1 \\ 0; \ \text{sonst.} \end{cases}$$

Dazu schreibe $n = g \cdot x$ mit $g := \mathrm{ggT}(m,n)$ und $x \in \mathbb{N}$. Die Multiplikation mit der zu $m$ teilerfremden Zahl $x$ wirkt auf $\mathbb{Z}_m$ als Isomorphismus. $\ker n\cdot = \ker g\cdot$ sind alle Vielfachen von $m/g$, also eine zyklische Gruppe der Ordnung $g$. Der Kokern $\mathrm{coker} n\cdot = \mathrm{coker} g\cdot$ ist der Quotient von $\mathbb{Z}_m$ modulo aller Vielfachen von $g$, also ebenfalls eine zyklische Gruppe der Ordnung $g$.

Nach Lemma 6.3.5 muss Tor für $k = 0$ mit dem ursprünglichen Funktor übereinstimmen: $\mathrm{Tor}_0(X,Y) = X \otimes_{\mathbb{Z}} Y$, vgl. Beispiel 1.2.6(iii).

In der Tat verschwinden die höheren (d.h. $k \geq 2$) Tor-Gruppen über $\mathbb{Z}$ für alle $\mathbb{Z}$-Moduln: weil $\mathbb{Z}$ ein Hauptidealring ist, kann man nach Bemerkung 3.1.3 stets eine freie Auflösung konstruieren, die in den Graden 0 und 1 konzentriert ist.

Wir berechnen auch noch $\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n)$ als Homologie des Komplexes

$$0 \to \mathbb{Z} \stackrel{n\cdot}{\to} \mathbb{Z} \to 0$$

und finden

$$\mathrm{Tor}_0^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n) \cong \mathbb{Z}_n \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_n \quad \text{und} \quad \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n) = 0\ .$$

Der Funktor $\mathrm{Tor}_1(-, \mathbb{Z}_n)$ kann nur dann auf endlich erzeugten abelschen Gruppen nicht verschwinden, wenn sie einen Torsionsanteil haben, daher sein Name.

2. Eine sehr ähnliche Rechnung zeigt, dass

$$\mathrm{Ext}_{\mathbb{Z}}^k(\mathbb{Z}_m, \mathbb{Z}_n) \cong \begin{cases} \mathbb{Z}_{\mathrm{ggT}(m,n)}; & \text{falls } k = 0,1 \\ 0; \ \text{sonst.} \end{cases}$$

Die Bezeichnung Ext können wir erst in Kapitel 6.7 erklären.

3. In dem folgenden Beispiel gibt es unendlich viele nichttriviale Tor-Gruppen: Sei $R = \mathbb{Z}[t]/(t^n - 1)$ der Gruppenring der zyklischen Gruppe $\mathbb{Z}_n$ über den ganzen Zahlen. Wähle $R$-Moduln $X = Y = \mathbb{Z}$ mit trivialer Modulstruktur $t.m = m$. Wir behaupten, dass eine projektive (und sogar freie) Auflösung gegeben ist durch den projektiven Anteil des augmentierten Komplex

$$\cdots \stackrel{N}{\to} R \stackrel{1-t}{\to} R \stackrel{N}{\to} R \stackrel{1-t}{\to} R \stackrel{\epsilon}{\to} \mathbb{Z} \to 0$$

wobei $\epsilon$ definiert ist durch Einsetzen von 1, also $\epsilon(t) = 1$ und $N := 1 + t + \cdots + t^{n-1}$. Man rechnet nämlich leicht nach, dass $(1-t)N = 1 - t^n$ gilt, also ein Kettenkomplex vorliegt. Wir zeigen Exaktheit: die Klasse eines Polynoms $f \in \mathbb{Z}[t]$ im Quotientenring $R$ verschwindet genau dann, wenn $f$ ein Vielfaches von $1 - t^n$ ist. Der Ring $\mathbb{Z}[t]$ ist nach dem Satz von Gauß faktoriell. Daher ist ein Vielfaches von $N$ genau dann ein Vielfaches von $1 - t^n$, wenn es auch durch $1 - t$ geteilt wird. Der Komplex ist also exakt.

Nach Tensorieren der projektiven Auflösung über $R$ mit $\mathbb{Z}$ mit der gleichen $R$-Modulstruktur mit der trivialen Modulstruktur erhält man in allen Graden $R \otimes_R \mathbb{Z} \cong \mathbb{Z}$. Die von $1 - t$ induzierte Abbildung wird durch Einsetzen von $t = 1$ zu Null, die von der Multiplikation mit $N$ induzierte Abbildung wird die Multiplikation mit $n \in \mathbb{N}$. Also ergibt sich der Komplex

$$\cdots \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0\,.$$

Somit gilt

$$\mathrm{Tor}_k^R(\mathbb{Z}, \mathbb{Z}) \cong \begin{cases} \mathbb{Z}; & \text{falls } k = 0 \text{ (vgl. Lemma 6.3.5)} \\ \mathbb{Z}_n; & \text{falls } k \text{ ungerade} \\ 0 & \text{falls } k > 0 \text{ gerade.} \end{cases}$$

4. Es ist klar, dass für einen freien $\mathbb{Z}$-Modul $A$ gilt $\mathrm{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$. Ob umgekehrt aus $\mathrm{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$ folgt, dass der $\mathbb{Z}$-Modul $A$ frei ist, ist eine überraschend subtile Frage, deren Antwort von der zu Grunde gelegten Mengenlehre abhängt (Hilton-Stammbach, Second Edition, Seite 330 “note to the third corrected printing”).

## 6.6 Symmetrie von Tor und Doppelkomplexe

Es liegt nahe, eine zweite Variante $\mathrm{Tor}'$ von Tor zu definieren, indem man die erste Variable projektiv auflöst. Ähnlich gibt es eine Variante $\mathrm{Ext}'$ von Ext, bei der für festes $X'$ die links-abgeleiteten Funktoren des linkssexakten Funktors $\mathrm{Hom}_R(X, -) : R\mathrm{-Mod} \to Ab$ betrachtet werden.

Wir zeigen die Isomorphie von Tor und $\mathrm{Tor}'$, indem wir zeigen, dass Tor zu einem dritten Funktor $\widetilde{\mathrm{Tor}}$ isomorph ist, der offensichtlich symmetrisch in seinen beiden Variablen ist; analoge Aussagen gelten für Ext. Dazu benötigen wir Doppelkomplexe.

***Definition 6.6.1***

1. *Die Kategorie der Doppelkomplexe in einer abelschen Kategorie $\mathcal{C}$ hat als Objekte Tripel $(X_{ij}, d_h, d_v)$ bestehend aus Objekten $X_{ij}$ für $i, j \in \mathbb{Z}$ von $\mathcal{C}$ und Morphismen $d_h : X_{ij} \to X_{i-1,j}$ und $d_v : X_{ij} \to X_{i,j-1}$ so dass gilt*

$$d_h d_v = -d_v d_h \quad d_h d_h = d_v d_v = 0\,.$$

*Die Summe $i + j$ heißt der Totalgrad des Objekts $X_{ij}$.*

2. *Die Morphismen von Doppelkomplexen sind gegeben durch Familien von Morphismen $f_{ij} : X_{ij} \to Y_{ij}$, die mit den Differentialen $d_h$ und $d_v$ kommutieren.*

3. *Mit Hilfe von Koprodukt und Produkt assoziiert man zu einem Doppelkomplex zwei einfache Komplexe*

$$|X_{\bullet\bullet}|_n := \coprod_{i+j=n} X_{ij} \qquad (\mathrm{Tot} X_{\bullet\bullet})_n := \prod_{i+j=n} X_{ij}$$

*wobei die Differentiale in beiden Fällen gegeben sind durch $d = d_h + d_v$. Beide Komplexe werden als Totalkomplex bezeichnet.*

**Bemerkung 6.6.2.**

1. Man beachte, dass die bei Doppelkomplexen übliche Indizierung von Zeilen und Spalten nicht die von Matrizen gewohnte ist!

2. Das Diagramm

$$\begin{tikzcd} X_{i,j} \arrow[r, "d_h"] \arrow[d, "d_v"] & X_{i-1,j} \arrow[d, "d_v"] \\ X_{i,j-1} \arrow[r, "d_h"] & X_{i-1,j-1} \end{tikzcd}$$

kommutiert also *nicht*. Die Schiefkommutativität der Differenziale, $d_h d_v = -d_v d_h$, stellt vielmehr sicher, dass die Totalkomplexe $|X|$ und $\mathrm{Tot}X$ wieder Kettenkomplexe sind: Ist $x \in X_{ij}$, so gilt für $d = d_h + d_v$

$$d(dx) = d(d_h x + d_v x) = d_h d_h x + d_h d_v x + d_v d_h x + d_v d_v x = 0\,.$$

***Definition 6.6.3***

1. *Sei $R$ ein Ring. Seien $(P_\bullet, d)$ ein $R^{\mathrm{opp}}$-Kettenkomplex und $(Q_\bullet, d)$ ein $R$-Kettenkomplex. Definiere einen Doppelkomplex $(P \otimes_R Q)_{\bullet,\bullet}$ von $\mathbb{Z}$-Moduln durch*

$$(P \otimes_R Q)_{i,j} := P_i \otimes_R Q_j \ ,$$

*wobei die Abbildungen für $p \in P_i, q \in Q_j$ gegeben sind durch $d_h(p \otimes q) = d(p) \otimes q$ und $d_v(p \otimes q) = (-1)^i p \otimes d(q)$. Wir nennen $i$ den <u>Grad</u> von $p$ und schreiben $|p| = i$. Wenn wir abstrakt den Grad von $d$ mit $-1$ definieren, da $d$ von $P_n$ nach $P_{n-1}$ geht, so ist die obige Vorzeichenkonvention ein Sonderfall von folgender Konvention, der sogenannten <u>Koszulregel</u>:*

> *Immer, wenn ein Element vom Grad $i$ an einem Element vom Grad $j$ vorbeigeschoben wird, wird ein Vorzeichen $(-1)^{ij}$ eingeführt.*

2. *Wir nennen dann den Totalkomplex $|P \otimes_R Q|$ das Tensorprodukt der Kettenkomplexe $P_\bullet$ und $Q_\bullet$.*

3. *Sei $(P_\bullet, d)$ ein $R$-Kettenkomplex, so definiere einen Doppelkomplex $\mathrm{Hom}_R(P,Q)_{\bullet\bullet}$ von abelschen Gruppen durch*

$$\mathrm{Hom}_R(P,Q)_{i,j} := \mathrm{Hom}_R(P_i, Q_j) \ .$$

*Hierbei sind die Differentiale des Doppelkomplexes natürlich durch Vorschalten und Nachschalten der Differentiale von $P_\bullet$ und $Q_\bullet$ gegeben.*

**Bemerkung 6.6.4.**

Tensorprodukte von Kettenkomplexen treten zum Beispiel im folgenden Problem auf: seien $X$ und $Y$ topologische Räume. Singuläre Homologie ordnet diesen Kettenkomplexe $C_\bullet(X)$ und $C_\bullet(Y)$ zu. Das Eilenberg-Zilber Theorem besagt, dass der Kettenkomplex $C_\bullet(X \times Y)$ des kartesischen Produkts kettenhomotop zum Tensorproduktkomplex $C_\bullet(X) \otimes C_\bullet(Y)$ ist.

Wir benötigen noch einen Hilfssatz, um Totalkomplexe zu untersuchen:

**Lemma 6.6.5.**
Sei $X_{\bullet\bullet}$ ein Doppelkomplex in einer abelschen Kategorie $\mathcal{C}$. Falls für jedes $j \in \mathbb{Z}$ gilt, dass der Zeilenkomplex $X_{\bullet,j}$ exakt ist, so ist

1. der Totalkomplex $|X|$ exakt, falls es ein $N \in \mathbb{Z}$ gibt, so dass $X_{ij} = 0$ für alle Zeilen $j < N$ gilt;

2. der Totalkomplex $\mathrm{Tot}X$ exakt, falls es ein $N \in \mathbb{Z}$ gibt, so dass gilt $X_{ij} = 0$ für alle Spalten $i < N$.

Die Bedingungen (1) und (2) sind natürlich immer erfüllt, falls $X$ in beiden Indizes nicht-negativ graduiert ist. Beide Bedingungen sind keine notwendigen Bedingungen; man sagt, sie stellen die "Konvergenz" sicher.

**Beweis.**

- Für den Beweis von (1) dürfen wir ohne Einschränkung annehmen, dass $N = 0$ gilt, ansonsten kann der Komplex vertikal verschoben werden. Ebenso ist es genug, Exaktheit des Totalkomplexes an der Stelle $|X|_0$ zu zeigen, denn durch Rechts- oder Linksverschiebung von $X$ kann jeder andere Totalgrad in Totalgrad Null geschoben werden.

  Es gilt
  $$|X|_0 = \oplus_{n\in\mathbb{Z}} X_{-n,n} = \oplus_{n\geq 0} X_{-n,n} \ .$$
  Sei $x = (x_{n_0}, x_{n_0-1}, \ldots, x_0) \in |X|_0$ ein Element, mit $x_n \in X_{-n,n}$, für das $d(x) = 0$ gilt. Wegen $d_h x_n \in X_{-n-1,n}$ und $d_v x_n \in X_{-n,n-1}$ bedeutet dies für die homogenen Komponenten
  $$d_v(x_i) + d_h(x_{i-1}) = 0 \text{ in } X_{-i,i-1} \text{ für } 0 \leq i \leq n_0 + 1 \ . \qquad (*)$$
  Da $x_{n_0+1} = 0$ gilt, ist für $i = n_0 + 1$ speziell
  $$d_h(x_{n_0}) = 0 \ .$$
  Da die Zeilen nach Voraussetzung exakt sind, folgt aus $d_h(x_{n_0}) = 0$, dass es ein $y_{n_0} \in X_{-n_0+1,n_0}$ gibt mit $d_h(y_{n_0}) = x_{n_0}$.

  Wir finden nun induktiv Elemente $y_n \in X_{-n+1,n}$, so dass gilt
  $$\begin{array}{rcl} d_h(y_{n_0}) & = & x_{n_0} \\ d_h(y_i) & = & x_i - d_v(y_{i+1}) \text{ für } 0 \leq i < n_0 \end{array}$$
  Denn es gilt für $0 \leq i < n_0$
  $$d_h(x_i - d_v(y_{i+1})) = d_h(x_i) + d_v d_h(y_{i+1}) \stackrel{\text{I.A.}}{=} d_h x_i + d_v x_{i+1} - d_v d_v(y_{i+2}) \stackrel{(*)}{=} 0 \ ,$$
  so dass wir wegen der Exaktheit der Zeilen $y_i \in X_{-i+1,i}$ finden mit
  $$d_h y_i = x_i - d_v y_{i+1} \ .$$
  Damit ist mit $y = (y_{n_0}, ..., y_0) \in |X|_1$ ein Element mit $d(y) = x$ gefunden. Der Totalkomplex $|X|$ ist somit exakt.

- Beim Beweis der Aussage über $\mathrm{Tot}(X)$ nehmen wir $N = 0$ an und betrachten $(\ldots, x_{-2}, x_{-1}, x_0) \in (\mathrm{Tot}X)_0$, wobei die Folge unendlich viele nicht-verschwindende Einträge $x_i \in X_{-i,i}$ haben kann. Wir erhalten wiederum Gleichungen $d_v(x_i) + d_h(x_{i-1}) = 0$ für alle $i \leq 0$. Aus der Abbruchbedingung folgt, dass die 0-te Gleichung die Form $d_h x_0 = 0$ hat, so dass wir auf Grund der Exaktheit der Zeilen ein $y_0 \in X_{1,0}$ finden mit $d_h y_0 = x_0$. So löst man wie oben sukzessive weiter und erhält eine Folge von $y_i \in X_{-i+1,i}$, die unendlich viele nicht-triviale Einträge haben kann, was ja für ein Element von $\mathrm{Tot}X$ erlaubt ist.

$\square$

Sei $P_\bullet \to X$ eine projektive Auflösung von $R^{\mathrm{opp}}$-Moduln, $Q_\bullet \to Y$ eine projektive Auflösung von $R$-Moduln. Um einen in beiden Auflösungen symmetrischen Komplex zu bekommen, betrachten wir das Tensorprodukt der Auflösungen und die Homologie des zugehörigen Totalkomplexes und setzen

$$\widetilde{\mathrm{Tor}}_n^R(X,Y) := H_n(|P \otimes_R Q|) \ .$$

**Satz 6.6.6.**
Für einen $R$-Rechtsmodul $X$ und einen $R$-Linksmodul $Y$ gilt

$$\mathrm{Tor}_n^R(X,Y) = \widetilde{\mathrm{Tor}}_n^R(X,Y) \ .$$

Da $\widetilde{\mathrm{Tor}}_n^R(X,Y)$ durch einen Doppelkomplex konstruiert wurde, der in beiden Argumenten symmetrisch ist, folgt, dass wir auch den anderen Tensoranden hätten projektiv auflösen können.

**Beweis.**

- Seien $P_\bullet \to X$ und $Q_\bullet \to Y$ projektive Auflösungen. Wir bezeichnen mit $\tilde{P}_\bullet$ den augmentierten Komplex mit $\tilde{P}_n := P_n$ für $n \geq 0$ und $P_{-1} = X$. Der augmentierte Komplex $\tilde{P}_\bullet$ ist exakt, und da $Q_i$ projektiv für jedes $i$ ist, ist nach Satz 1.4.10 auch jedes $Q_i$ flach und somit der Doppelkomplex $\tilde{P} \otimes_R Q$ zeilenweise exakt. Nach Lemma 6.6.5 ist damit der Totalkomplex $|\tilde{P} \otimes Q|$ ebenfalls exakt.

- Trivialerweise ist
$$0 \to X[-1] \to \tilde{P}_\bullet \to P_\bullet \to 0$$
eine kurze exakte Sequenz von Komplexen, wobei $X[-1]$ den Komplex bezeichnet, der in Grad $-1$ den Modul $X$ enthält und 0 überall sonst ist. Da $Q_i$ projektiv ist, liefert Tensorieren mit $Q_\bullet$ eine exakte Sequenz von Doppelkomplexen. Da der Funktor $|-|$, der Doppelkomplexe auf Komplexe abbildet, exakt ist, erhalten wir eine kurze exakte Sequenz von Totalkomplexen
$$0 \to |X[-1] \otimes Q| \to |\tilde{P} \otimes Q| \to |P \otimes Q| \to 0$$
Da der mittlere Komplex $\tilde{P} \otimes_R Q$, wie im ersten Schritt gesehen, exakt ist, also seine Homologie verschwindet, zerfällt die dazu nach Satz 6.4.3 gehörige lange exakte Sequenz für $n \geq 0$ in Stücke, die vom Verbindungshomomorphismus geliefert werden:
$$0 \to H_n|P \otimes Q| \to H_{n-1}|X[-1] \otimes Q| \to 0 \ ,$$
also in Isomorphismen.

- Wir bestimmen die abelschen Gruppe in Bild und Urbild des Isomorphismus: nach Definition von $\widetilde{\mathrm{Tor}}$ gilt für die abelsche Gruppe im Urbild
$$H_n|P \otimes Q| = \widetilde{\mathrm{Tor}}_n^R(X,Y) \ ;$$
für die abelsche Gruppe im Bild finden wir nach Definition von Tor
$$H_{n-1}|X[-1] \otimes Q| = H_n(X \otimes Q) = \mathrm{Tor}_n^R(X,Y) \ .$$
Damit ist die Isomorphie der Funktoren Tor und $\widetilde{\mathrm{Tor}}$ gezeigt.

□

Wenn der Ring $R$ kommutativ ist, sind die beiden Tensorprodukte $X \otimes_R Y$ und $Y \otimes_R X$ definiert und isomorph durch Vertauschung der Faktoren. Seien $P_\bullet \to X$ und $Q_\bullet \to X$ projektive Auflösungen. Dann haben wir die die Isomorphie

$$\begin{array}{rcll} P \otimes Q & \to & Q \otimes P & \\ v_p \otimes w_q & \mapsto & (-1)^{pq} w_q \otimes v_p & \text{für } v_p \in P_p \text{ und } w_q \in Q_q \end{array}$$

von Doppelkomplexen. Wir finden somit

$$\begin{array}{rcl} \mathrm{Tor}_*^R(X,Y) & \cong & \widetilde{\mathrm{Tor}}_*^R(X,Y) = H_*(|P \otimes_R Q|) \\ & \cong & H_*(|Q \otimes_R P|) = \widetilde{\mathrm{Tor}}_*^R(X,Y) = \mathrm{Tor}_*^R(Y,X) \end{array}$$

Also ist im Falle eines *kommutativen* Rings $R$ auch der abgeleitete Funktor $\mathrm{Tor}_*^R$ kommutativ in den beiden Argumenten.

Im Fall von Ext können wir auch statt das erste Argument projektiv das zweite Argument injektiv auflösen:

**Satz 6.6.7.**
Seien $X, Y \in R-\mathrm{Mod}$ und $Y \to I_\bullet$ eine injektive Auflösung und $P_\bullet \to X$ eine projektive Auflösung. Setze:

$$\mathrm{Ext}'^n_R(X,Y) := H^n(\mathrm{Hom}_R(X, I_\bullet)) \text{ und } \widetilde{\mathrm{Ext}}^n_R(X,Y) := H_n(\mathrm{TotHom}_R(P_\bullet, I_\bullet)) \ .$$

Hierbei graduieren wir den Komplex abelscher Gruppen mit

$$\mathrm{Hom}(P_\bullet, I_\bullet)_{i,j} := \mathrm{Hom}(P_{-i}, I_j) \ .$$

Dann gilt

$$\mathrm{Ext}^n_R(X,Y) \cong \widetilde{\mathrm{Ext}}^n_R(X,Y) \cong \mathrm{Ext}'^n_R(X,Y)$$

**Beweis.**
Übung. □

## 6.7 Erweiterungen von Moduln

Während die Bezeichnung “Tor” sich nach Beispiel 6.5.2 mit der Torsion in abelschen Gruppen erklären lässt, ist bisher unklar geblieben, wofür “Ext” steht. In diesem Abschnitt wird eine alternative Definition von Ext-Gruppen durch Äquivalenzklassen von Erweiterungen (extensions) von $R$-Moduln durch andere $R$-Moduln vorgestellt, die auf Yoneda zurückgeht.

Sei $\mathcal{C}$ eine abelsche Kategorie und seien $M, N$ zwei Objekte in $\mathcal{C}$. Betrachte für $n \geq 1$ die Mengen von *exakten* Sequenzen

$$\mathrm{Ex}^n(M,N) = \{0 \to N \to X_{n-1} \to X_{n-2} \to \cdots X_0 \to M \to 0\}/\sim \ ,$$

wobei $\sim$ die Äquivalenzrelation ist, die erzeugt wird von $E \sim E'$, wenn es eine Leiterabbildung $E \to E'$ gibt, die auf den $M$- und $N$-Einträgen die Identität ist. Es reicht hier nicht aus, nur Isomorphie auf den Einträgen von $M$ und $N$ zu fordern. Man beachte, dass aus dem

Neunerlemma 1.5.8 im Falle $n = 1$ folgt, dass der Morphismus $X_0 \to X_0'$ ein Isomorphismus ist. Im allgemeinen sind die Leiterabbildungen jedoch keine Isomorphismen.

Wir wollen nun $\mathrm{Ex}^n$ zu einem Funktor $\mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathrm{Set}$ machen. (In Lemma 6.7.2 werden wir dann sehen, dass er Werte in abelschen Gruppen annimmt.) Um den Funktor auf Morphismen zu definieren, seien gegeben eine Erweiterung

$$E = (0 \to N \to X_\bullet \to M \to 0) \in \mathrm{Ex}^\bullet(M, N)$$

und Morphismen

$$f : M' \to M \quad \text{und} \quad g : N \to N' .$$

Betrachte für $f$ das Pullback-Diagramm

$$\begin{tikzcd}
X_1 \arrow[dr, dashed] \arrow[drr, bend left, "0"] \arrow[ddr, bend right, "d"'] & & \\
& X_0 \times_M M' \arrow[r] \arrow[d] & M' \arrow[d, "f"] \\
& X_0 \arrow[r, "d"] & M
\end{tikzcd}$$

wobei der Morphismus $X_1 \to X_0 \to M$ aus der exakten Sequenz $E$ kommt und daher gleich Null ist. Betrachte den Komplex

$$f^*E : \quad 0 \to N \to X_{n-1} \to \cdots \to X_1 \to X_0 \times_M M' \to M' \to 0$$

Dual definieren wir durch einen Pushout unter $N$, vgl. Abschnitt 2.5, einen Komplex

$$g_*E : \quad 0 \to N' \to X_{n-1} \sqcup_N N' \to X_{n-2} \to \cdots \to X_0 \to M \to 0 .$$

**Lemma 6.7.1.**

1. Die Komplexe $f^*E$ und $g_*E$ sind wieder exakt. Ihre Äquivalenzklasse hängt nicht von der Wahl des Repräsentanten für die Äquivalenzklasse in Ex ab.

2. Wir erhalten so einen Funktor $\mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathrm{Set}$.

**Beweis.**

1. Für die Wohldefiniertheit muss gezeigt werden, dass $f^*$ nicht vom Repräsentanten $E$ der Äquivalenzklasse abhängt. Sei also

$$\begin{tikzcd}
E : 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & X_\bullet \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
E' : 0 \arrow[r] & N \arrow[r] & X_\bullet' \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

eine elementare Äquivalenz von exakten Sequenzen und $f : M' \to M$ ein Morphismus. Dann erhalten wir auf Grund der Funktorialität 2.5.2 (4) des Pullbacks eine Abbildung

$$X_0 \times_M M' \to X_0' \times_M M' ,$$

die zusammen mit den anderen Morphismen $X_i \to X_i'$ eine elementare Äquivalenz zwischen $f^*E$ und $f^*E'$ liefert. Das duale Argument wenden wir auf $g_*$ an.

2. Außerdem müssen wir uns überlegen, dass der eben konstruierte Komplex $f^*E$ exakt und somit eine Erweiterung ist.

   – Die Abbildung $X \times_M M' \to M'$ ist surjektiv, denn zu $m' \in M'$ finde $x \in X_0$ mit $f(m') = dx$, da $d : X_0 \to M$ surjektiv ist. $(x, m')$ ist dann das Urbild von $m' \in M'$ im Faserprodukt $X_0 \times_M M'$.

   – Der Morphismus $X_1 \to X_0 \times_M \ M'$ ist $x \mapsto (dx, 0)$, was wegen $d(dx) = 0 = f(0)$ wirklich im Faserprodukt $X_0 \times_M \ M'$ liegt. Daher ist
   $$\ker(X_1 \to X_0 \times_M \ M') = \ker(X_1 \to X_0) = \mathrm{Im}\,(X_2 \to X_1) \quad .$$

   – Schließlich enthält $\ker(X_0 \times_M \ M' \to M')$ die Elemente von $X_0 \times_M \ M'$ der Form $(x, 0)$. Für diese muss aber $dx = f(0) = 0$ gelten. Wegen der Exaktheit von $E$ ist dann aber $x \in \mathrm{Im}\,(X_1 \to X_0)$ und somit $(x, 0) \in \mathrm{Im}\,(X_1 \to X_0 \times_M \ M')$.

   Das Argument für die Exaktheit des Komplexes $g_*E$ ist wieder dual.

3. Nun zum zweiten Teil des Lemmas, der Funktorialität: seien $M_2 \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0$ zwei Morphismen; es ist zu zeigen, dass $(f_0 \circ f_1)^* = f_1^* \circ f_0^*$ gilt. Dies folgt sofort aus dem kanonischen Isomorphismus
   $$(X_0 \times_{M_0} M_1) \times_{M_1} M_2 \cong X_0 \times_{M_0} M_2 \ ,$$
   vergleiche Bemerkung 2.5.2 (5).

4. Wir müssen nun noch zeigen, dass $f^*g_* = g_*f^*$ ist für $f : M' \to M$ und $g : N \to N'$. Das ist klar für $n \geq 2$, da die beiden Funktoren dann auf verschiedenen Teilen der exakten Sequenz operieren. Aber für $n = 1$ folgt aus dem Diagramm
   $$\begin{tikzcd}
   & N \arrow[dl, "g"'] \arrow[d, "d"] \arrow[dr, "0"] & \\
   N' \arrow[dr, "0"'] & X \arrow[d, "d"] & M' \arrow[dl, "f"] \\
   & M &
   \end{tikzcd}$$
   der Isomorphismus
   $$(X \times_M M') \sqcup_N N' \cong (X \sqcup_N N') \times_N M'$$
   den man am besten elementweise nachrechnet, und der eine Äquivalenz der Sequenzen $f^*g_*E$ und $g_*f^*E$ erzeugt.

$\square$

Wir wollen nun noch die Mengen $\mathrm{Ex}^n$ mit der Struktur von abelschen Gruppen versehen. Seien $E, E' \in \mathrm{Ex}^n(M, N)$. Für $n \geq 2$ betrachten wir das Pullback-Diagramm

$$\begin{tikzcd}
X_1 \oplus X_1' \arrow[dr, dashed] \arrow[drr, bend left, "d' \circ pr_2"] \arrow[ddr, bend right, "d \circ pr_1"'] & & \\
& X_0 \times_M \ X_0' \arrow[r] \arrow[d] & X_0' \arrow[d, "d'"] \\
& X_0 \arrow[r, "d"'] & M
\end{tikzcd}$$

und das duale Pushout-Diagramm. Wir definieren einen Komplex $E+E'$ durch direkte Summen und den gestrichelten Morphismus im Diagramm:

$$E+E' : 0 \to N \to X_{n-1} \sqcup_N X'_{n-1} \to X_{n-2} \oplus X'_{n-2} \to \cdots \to X_1 \oplus X'_1 \to X_0 \times_M X'_0 \to M \to 0 \ .$$

Im Fall $n = 1$ müssen wir den mittleren Term des Komplexes $E + E'$ definieren als

$$\{(x, x') \in X \oplus X' | d(x) = d'(x')\}/(d(n), 0) \sim (0, d'(n))(n \in N) \ .$$

**Lemma 6.7.2.**
Die Mengen $\mathrm{Ex}^n(M, N)$ erhalten so eine wohldefinierte abelsche Gruppenstruktur.

**Beweis.**

- Zunächst zeigen wir die Exaktheit des Komplexes $E + E'$.
  - Die Exaktheit ist klar bei den mittleren (direkten Summen-)Gruppen.
  - Exaktheit bei $M$ ist Surjektivität: gegeben $m \in M$, finde $x_0 \in X_0$ und $x'_0 \in X'_0$ mit $dx_0 = m$ und $d'x'_0 = m$, wegen der Surjektivität in den Erweiterungen $E, E'$. Dann ist $(x_0, x'_0)$ das gewünschte Urbild.
  - Zur Exaktheit bei $X_0 \times_M X'_0$: Der Kern in $X_0 \times_M X'_0$ ist genau $\ker(X_0 \to M) \times_M \ker(X'_0 \to M) = \mathrm{Im}\,(X_1 \oplus X'_1 \to X_0 \times_M X'_0)$.
  - Die Exaktheit bei $N$ und bei $X_{n-1} \sqcup_N X'_{n-1}$ folgt dual.
- Die Assoziativität und Kommutativität der Summen ist aus der Definition sofort ersichtlich. Wir beschreiben das neutrale Element; dieses ist für $n \geq 2$ gegeben durch

  $$0 \to N \xrightarrow{\mathrm{id}} N \to 0 \to \cdots \to M \xrightarrow{\mathrm{id}} M \to 0$$

  bzw. für $n = 1$ durch die zerfallende kurze exakte Sequenz.
- Den Beweis für die Existenz von Inversen lassen wir aus.

□

Der folgende Satz erklärt die Bezeichnung Ext. Gleichzeitig macht er Erweiterungen von Moduln durch projektive Auflösungen berechenbar.

**Satz 6.7.3.**
Hat die Kategorie $\mathcal{C}$ genug Projektive, so gibt es einen natürlichen Isomorphismus von Funktoren $\mathrm{Ex}^n \cong \mathrm{Ext}^n$.

**Beweis.**

- Sei $P_\bullet \to M$ eine projektive Auflösung von $M$. Sei $E \in \mathrm{Ex}^n(M, N)$. Dann hat nach dem Fundamentallemma 6.3.1 das Hochhebungsproblem für die Identitität $\mathrm{id}_M$

$$\begin{tikzcd}
\cdots \arrow[r] & P_{n+1} \arrow[r, "d"] \arrow[d, dotted] & P_n \arrow[r] \arrow[d, dotted, "f_n"] & P_{n-1} \arrow[r] \arrow[d, dotted, "f_{n-1}"] & P_{n-2} \arrow[r] \arrow[d, dotted, "f_{n-2}"] & \cdots \arrow[r] & P_0 \arrow[r] \arrow[d, dotted, "f_0"] & M \arrow[r] \arrow[d, equal] & 0 \\
E: & 0 \arrow[r] & N \arrow[r] & X_{n-1} \arrow[r] & X_{n-2} \arrow[r] & \cdots \arrow[r] & X_0 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

eine Lösung. Wegen der Kommutativität des Quadrats ganz links außen gilt $f_n \circ d = 0$, also liegt

$$f_n \in \ker(\mathrm{Hom}(P_n, N) \xrightarrow{d^*} \mathrm{Hom}(P_{n+1}, N)) \ .$$

Wir können daher die Klasse

$$\Phi(E) := [f_n] \in \mathrm{Ext}^n(M, N)$$

betrachten.

- Wir zeigen zunächst, dass $\Phi(E) \in \mathrm{Ext}^n(M, N)$ wohldefiniert ist: das Element hängt weder von der Wahl der Hochhebung $f_\bullet$ der Identität $\mathrm{id}_M$ noch von der Wahl der Erweiterung $E$ innerhalb einer Äquivalenzklasse ab. Dann zeigen wir, dass $\Phi : \mathrm{Ex}^n(M, N) \to \mathrm{Ext}^n(M, N)$ ein Isomorphismus von abelschen Gruppen ist.

  Das Fundamentallemma 6.3.1 garantiert eine Hochhebung $f_n : P_n \to N$, die eindeutig bis auf Homotopie ist. Das heißt, jede weitere Lösung ist von der Form $f_n + H \circ d = f_n + d^*(H)$, wobei $H : P_{n-1} \to N$ Teil einer Kettenhomotopie ist. Da dies keinen Unterschied in Homologie macht, ist die erste Wohldefiniertheit gezeigt.

  Also ist die Klasse von $f_n$ in $H^n(\mathrm{Hom}(P_\bullet, N)) = \mathrm{Ext}^n(M, N)$ wohldefiniert, wenn wir zeigen können, dass sie invariant unter der Äquivalenzrelation in Ex ist. Ist aber $E \to E'$ eine elementare Äquivalenz, so können wir für diese die Hochhebung $P_\bullet \to E'$ der Identität speziell so wählen, dass es die Hochhebung $P_\bullet \to E$ von $\mathrm{id}_M$ ist, gefolgt von der Äquivalenzabbildung $E \to E'$. Da diese per Definition die Identität auf $N$ ist, erhalten wir das gleiche Element in $\mathrm{Ext}^n$.

- Wir wollen eine Umkehrabbildung von $\Phi$ konstruieren. Sei dazu $f : P_n \to N$ ein Repräsentant eines Elementes von $\mathrm{Ext}^n(M, N)$. Betrachte das Pushout-Diagramm

$$\begin{tikzcd}
P_n \arrow[r, "d"] \arrow[d, "f"'] & P_{n-1} \arrow[d] \arrow[ddr, bend left, "d"] & \\
N \arrow[r] \arrow[drr, bend right, "0"'] & N \sqcup_{P_n} P_{n-1} \arrow[dr, dashed] & \\
 & & P_{n-2}
\end{tikzcd}$$

  und konstruiere daraus mit Argumenten dual zu denen im Beweis von Lemma 6.7.2 eine exakte Sequenz

$$0 \to N \to N \sqcup_{P_n} P_{n-1} \to P_{n-2} \to P_{n-3} \to \cdots \to P_0 \to M \to 0 \ .$$

  Sie bestimmt ein Element in $\mathrm{Ex}^n$. Es ist klar, dass die Komposition Ext $\to$ Ex $\to$ Ext die Identität ist; die andere Richtung ist gegeben durch das folgende Diagramm, das eine Äquivalenz in Ex angibt:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & N \sqcup_{P_n} P_{n-1} \arrow[r] \arrow[d, "{(d, f_{n-1})}"] & P_{n-2} \arrow[r] \arrow[d, "f_{n-2}"] & \cdots \arrow[r] & P_0 \arrow[r] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r, "d"] & X_{n-1} \arrow[r, "d"] & X_{n-2} \arrow[r] & \cdots \arrow[r] & X_0 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

- Es ist klar, dass unter $\Phi$ die Null in $\mathrm{Ex}^n$ auf die Null in $\mathrm{Ext}^n$ abgebildet wird, denn wir können als Hochhebung auf $P_n$ den Nullmorphismus wählen.

- Wir müssen nun noch zeigen, dass die Bijektion zwischen $\mathrm{Ext}^n$ und $\mathrm{Ex}^n$ die Addition respektiert. Dazu beobachten wir zunächst, dass wir die Addition in $\mathrm{Ext}^n$ wie folgt charakterisieren können.

  Sei $\Delta : M \to M \oplus M$ die Diagonalenabbildung und $\Sigma : N \oplus N \to N$ die Summenabbildung, so ist

$$\mathrm{Hom}(M,N) \oplus \mathrm{Hom}(M,N) \to \mathrm{Hom}(M \oplus M, N \oplus N) \xrightarrow{\Sigma_* \Delta^*} \mathrm{Hom}(M,N)$$

  wegen

$$\Sigma \circ (f,g) \circ \Delta(m) = \Sigma\,(f(m), g(m)) = f(m) + g(m)$$

  die Addition der abelschen Gruppe $\mathrm{Hom}(M,N)$ und ebenso

$$\mathrm{Ext}(M,N) \oplus \mathrm{Ext}(M,N) \to \mathrm{Ext}(M \oplus M, N \oplus N) \xrightarrow{\Sigma_* \Delta^*} \mathrm{Ext}(M,N)$$

  die Addition der abelschen Gruppe $\mathrm{Ext}(M,N)$: es gilt

$$\Sigma_* \Delta^* (f \oplus g) = f + g \ .$$

  Für $\mathrm{Ex}^n$ wurde die Funktorialität in Lemma 6.7.1 für $\Delta^*$ durch ein Pullback und für $\Sigma_*$ durch einen Pushforward definiert. Genau diese Operationen treten aber auch in der Definition der Summe in Lemma 6.7.2 auf. Daher gilt auch in $\mathrm{Ex}^n$:

$$E + E' \cong \Sigma_* \Delta^* (E \oplus E') \ ,$$

  wobei $E \oplus E'$ die direkte Summensequenz von $N \oplus N$ nach $M \oplus M$ ist. Wählen wir eine projektive Auflösung $P_\bullet$ von $M$, so können wir in dem Diagramm

$$\begin{tikzcd}
 & \cdots \arrow[r] & P_n \oplus P_n \arrow[r] \arrow[d, "{(f_n, f'_n)}"] & \cdots \arrow[r] & P_0 \oplus P_0 \arrow[r] \arrow[d, "{(f_n, f'_n)}"] & M \oplus M \arrow[r] \arrow[d, equal] & 0 \\
E \oplus E' : & & N \oplus N \arrow[r] & \cdots \arrow[r] & X_0 \oplus X'_0 \arrow[r] & M \oplus M \arrow[r] & 0
\end{tikzcd}$$

  die Hochhebung als die direkte Summe der Hochhebungen $f, f'$ definieren, die zu $E$ bzw. $E'$ gehören. Die Anwendung von $\Sigma_* \Delta^*$ zeigt dann die Additivität.

□

**Beispiel 6.7.4.**
Sei $p$ eine Primzahl; dann gilt nach Beispiel 6.5.2 in der Kategorie der abelschen Gruppen $\mathrm{Ext}^1_{Ab}(\mathbb{Z}_p, \mathbb{Z}_p) = \mathbb{Z}_p$. Wir wissen also, dass es $p$ Äquivalenzklassen von Erweiterungen

$$0 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p \to 0$$

geben muss. Für die nicht-trivialen Gruppenelemente von $\mathrm{Ext}^1_{Ab}(\mathbb{Z}_p, \mathbb{Z}_p)$ ist $G \cong \mathbb{Z}_{p^2}$, für das neutrale Element $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Die Darstellung durch den Yoneda-Ext erlaubt es uns, noch mehr Struktur auf die Gesamtheit der Gruppen $\mathrm{Ext}^*(M,N)$ zu finden. Ist $E \in \mathrm{Ex}^n(M,N), E' \in \mathrm{Ex}^m(Q,M)$ mit $m > 0$ und

$n > 0$, so liefert die Komposition $X_0 \to M \to X'_{m-1}$ einen Morphismus. Aus der Exaktheit von $X_1 \to X_0 \to M \to 0$ und $0 \to M \to X'_{m-1}$ folgt, dass

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & X_{n-1} \arrow[r] & \cdots \arrow[r] & X_0 \arrow[r] \arrow[dr] & X'_{m-1} \arrow[r] & \cdots \arrow[r] & X'_0 \arrow[r] & Q \\ & & & & & M \arrow[u] & & & \end{tikzcd} ,$$

wieder eine Erweiterung ist.

Wir definieren $\mathrm{Ex}^0(M,N)$ als $\mathrm{Hom}(M,N)$; die Multiplikation $\mathrm{Ex}^0 \times \mathrm{Ex}^0 \to \mathrm{Ex}^0$ ist dann einfach die Komposition von Morphismen. Ferner setzen wir

$$\begin{array}{rcl} \mathrm{Ex}^0 \times \mathrm{Ex}^n & \to & \mathrm{Ex}^0 \\ (f,E) & \mapsto & f^*E \end{array}$$

bzw.

$$\begin{array}{rcl} \mathrm{Ex}^n \times \mathrm{Ex}^0 & \to & \mathrm{Ex}^0 \\ (E,g) & \mapsto & g_*E \end{array}$$

**Satz 6.7.5** (Yoneda-Produkt).
Ist $E \in \mathrm{Ex}^n(M,N), E' \in \mathrm{Ex}^m(Q,M)$, so definiere das Yoneda-Produkt $EE' \in \mathrm{Ex}^{n+m}(Q,N)$ durch die Erweiterung

$$0 \to N \to X_{n-1} \to \cdots \to X_0 \to X'_{m-1} \to \cdots \to X'_0 \to Q \ ,$$

Die Abbildung $(E,E') \mapsto E \cdot E'$ ist eine wohldefinierte, bilineare, assoziative Multiplikation.

**Beweis.**
Die Assoziativität für $n,m > 0$ ist sofort klar. Ebenso die Wohldefiniertheit, denn zwei elementare Äquivalenzen können zu einer Äquivalenz des Produktes zusammengeklebt werden.

Die Assoziativität für den Fall, dass $n = 0$ oder $m = 0$ gilt, entspricht dann genau der Funktorialität von $\mathrm{Ex}^n$ aus Lemma 6.7.1. □

## 6.8 Die Künneth-Formel

Wir hatten in Definition 6.6.3.2 das Tensorprodukt von Kettenkomplexen $X_\bullet$ und $Y_\bullet$ von $R$-Moduln als Totalkomplex $|X_\bullet \otimes_R Y_\bullet|$ definiert. Wir wollen die Homologie eines solchen Tensorprodukts $C_\bullet \otimes_R D_\bullet$ durch die Homologien von $C_\bullet$ und $D_\bullet$ ausdrücken. Wir müssen uns hierbei auf den Fall beschränken, dass $R$ ein Hauptidealring ist. Insbesondere ist dann $R$ kommutativ.

**Beispiel 6.8.1.**
Sei $R = \mathbb{Z}$ und seien $C_\bullet = D_\bullet$ in Grad Null konzentrierte Komplexe mit Eintrag $\mathbb{Z}_2$. Sei $C'_\bullet$ der Komplex mit $\mathbb{Z}$ in Grad 0,1 und $0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to 0$. Dann haben nach Beispiel 6.2.3 die quasiisomorphen Komplexe $C_\bullet$ und $C'_\bullet$ isomorphe Homologie,

$$H_p(C_\bullet) = H_p(C'_\bullet) \quad \text{für alle } p \in \mathbb{Z} \ .$$

Es ist $H_1(C_\bullet \otimes D_\bullet) = 0$, aber $H_1(C'_\bullet \otimes D_\bullet) = \mathbb{Z}_2$ wegen

$$C'_\bullet \otimes D_\bullet : 0 \to \mathbb{Z}_2 \xrightarrow{0} \mathbb{Z}_2 \to 0 \ .$$

Das Tensorprodukt der quasiisomorphen Komplexe $C_\bullet$ und $C'_\bullet$ mit dem Komplex $D_\bullet$ ist nicht quasiisomorph. Das Tensorprodukt ist also nicht verträglich mit Quasiisomorphisen und daher für komplexe ein schlechter Begriff.

Insbesondere reicht die Homologie der Komplexe nicht aus, um die Homologie des Tensorprodukts zu bestimmen.

Wir machen im folgenden Theorem daher mehr Annahmen, die insbesondere in Beispiel 6.8.1 die in einem Grad konzentrierten Torsionsgruppen eliminieren.

**Theorem 6.8.2** (Künneth)**.**
Seien $C_\bullet, D_\bullet$ Kettenkomplexe von Moduln über einem Hauptidealring $R$. Sei einer der Komplexe flach, d.h. alle involvierten Moduln sind flach. Dann gibt es eine natürliche kurze exakte Sequenz

$$0 \to \bigoplus_{p+q=n} H_p(C_\bullet) \otimes_R H_q(D_\bullet) \xrightarrow{\zeta} H_n(C_\bullet \otimes D_\bullet) \to \bigoplus_{p+q=n-1} \mathrm{Tor}_1^R(H_p(C_\bullet), H_q(D_\bullet)) \to 0 ,$$

wobei $\zeta$ durch die Inklusion

$$Z_p(C_\bullet) \otimes_R Z_q(D_\bullet) \to Z_{p+q}(C_\bullet \otimes_R D_\bullet)$$

von Zykeln erzeugt wird. Die Sequenz spaltet, aber nicht natürlich.

**Beweis.**

- Wegen der Isomorphie von Tensorproduktkomplexen über dem Ring $R$

$$\begin{array}{rcl} C_\bullet \otimes_R D_\bullet & \to & D_\bullet \otimes_R C_\bullet \\ c \otimes d & \mapsto & (-1)^{pq} d \otimes c \qquad \text{für } c \in C_p \text{ und } d \in D_q \end{array}$$

  können wir ohne Verlust der Allgemeinheit annehmen, dass der Komplex $C_\bullet$ flach ist.

- Wir führen für Zykel und Ränder die Bezeichnungen ein

$$\begin{array}{ll} Z_p := Z_p(C_\bullet) & B_p := B_p(C_\bullet) \\ \overline{Z}_p := Z_p(D_\bullet) & \overline{B}_p := B_p(D_\bullet) \end{array}$$

  und betrachten die dazu gehörigen Komplexe mit verschwindendem Differential. Wir erhalten eine exakte Sequenz von Komplexen

$$0 \to Z_\bullet \xrightarrow{\iota} C_\bullet \xrightarrow{\partial} B[-1]_\bullet \to 0 .$$

  Da $R$ ein Hauptidealring ist, sind alle Komplexe wieder flach, da sie aus Unterobjekten flacher Objekte bestehen. Wir erhalten wie im Beweis von Satz 6.6.6 eine exakte Sequenz von Komplexen

$$0 \to Z_\bullet \otimes_R D_\bullet \xrightarrow{\iota\otimes\mathrm{id}} C_\bullet \otimes_R D_\bullet \xrightarrow{\partial\otimes\mathrm{id}} B[-1]_\bullet \otimes_R D_\bullet \to 0 .$$

  Hieraus erhalten wir nach Satz 6.4.3 eine lange exakte Sequenz in Homologie, die wir symbolisch so schreiben:

$$\begin{tikzcd} H(Z_\bullet \otimes_R D_\bullet) \arrow[rr, "(\iota\otimes\mathrm{id})_*"] & & H(C_\bullet \otimes_R D_\bullet) \arrow[dl, "(\partial\otimes\mathrm{id})_*"] \\ & H(B_\bullet[-1] \otimes_R D_\bullet) \arrow[ul, "\omega"] & \end{tikzcd} ,$$

  wobei alle Morphismen Grad 0 haben, außer dem Morphismus $\omega$, der vom Verbindungshomomorphismus erzeugt wird und der Grad $-1$ hat. Machen wir die Gradverschiebung bei $B_\bullet$ rückgängig, so erhalten wir Grad 0 für $\omega$ und $-1$ für $\partial$.

- Wir analysieren die Homologie $H(B[-1]\otimes_R D_\bullet)$. Im ersten Tensoranden ist das Differential trivial, so dass wir (nach Änderung von Vorzeichen) mit dem Differential $\mathrm{id}\otimes\partial$ arbeiten können. Weil $B_n$ für alle $n$ flach ist, sind Kern und Bild dieses Differentials Tensorprodukte des Kerns und Bilds des Differentials in $D_\bullet$. Daher gilt

$$H_n(B[-1]_\bullet \otimes_R D_\bullet) = (B_\bullet \otimes_R H(D_\bullet))_{n-1}$$

Analog folgt

$$H_n(Z_\bullet \otimes_R D_\bullet) = (Z_\bullet \otimes_R H(D_\bullet))_n \ .$$

Somit erhalten wir eine lange exakte Sequenz in Homologie

$$\begin{tikzcd} Z_\bullet \otimes_R H(D_\bullet) \arrow[rr, "(\iota\otimes \mathrm{id})_*"] & & H(C_\bullet \otimes_R D_\bullet) \arrow[dl, "(\partial\otimes\mathrm{id})_*"] \\ & B_\bullet \otimes_R H(D_\bullet) \arrow[ul, "\omega"] & \end{tikzcd} \qquad (*)$$

- Wir müssen nun noch den Morphismus $\omega$ analysieren, der vom Verbindungshomomorphismus herkommt. Stellen wir $\partial c\otimes[z]\in B\otimes_R H(D_\bullet)$ durch $\partial c\otimes z$ dar, so zeigt sich, dass $\omega(\partial c\otimes[z])$ die Homologieklasse von $\partial c\otimes z$ in $Z_\bullet\otimes H(D_\bullet)$ ist und $\omega$ somit durch die Inklusion $B_\bullet\to Z_\bullet$ erzeugt wird.

  Damit ist klar, dass $(\iota\otimes\mathrm{id})_*$ die Abbildung $H(C_\bullet)\otimes_R H(D_\bullet)\xrightarrow{\zeta} H_n(C_\bullet\otimes D_\bullet)$ induziert, wenn man modulo Rändern rechnet, also modulo dem Bild von $\omega$.

- Wir brauchen eine weitere exakte Sequenz: tensoriert man die kurze exakte Sequenz

$$0\to B_\bullet\to Z_\bullet\to H(C_\bullet)\to 0$$

mit $H(D_\bullet)$ und beachtet, dass $\mathrm{Tor}_1^R(Z_\bullet, H(D_\bullet))=0$, weil der Komplex $Z_\bullet$ flach ist, so erhält man aus der langen exakten Sequenz in Homologie die exakte Sequenz

$$0\to \mathrm{Tor}_1^R(H(C_\bullet),H(D_\bullet))\to B_\bullet\otimes_R H(D_\bullet)\xrightarrow{\omega} Z_\bullet\otimes_R H(D_\bullet)\to H(C_\bullet)\otimes_R H(D_\bullet)\to 0 \quad (**)$$

von Komplexen.

  Nach $(*)$ ist der Kern von $\zeta$ das Bild von $\omega$. Daher ist $Z_\bullet\otimes_R H(D_\bullet)/\ker\zeta = \mathrm{coker}\omega \overset{(**)}{=} H(C_\bullet)\otimes_R H(D_\bullet)$ und wir finden Injektivität

$$0\to H(C_\bullet)\otimes_R H(D_\bullet)\xrightarrow{\zeta} H(C_\bullet\otimes_R D_\bullet)\ .$$

  Wir müssen noch den Kokern von $\zeta$ bestimmen. Wir finden

$$\begin{aligned} \mathrm{coker}\zeta &= H(C_\bullet\otimes_R D_\bullet)/\mathrm{Im}\,\zeta \overset{(*)}{=} H(C_\bullet\otimes_R D_\bullet)/\ker(\partial\otimes\mathrm{id})_* \\ &\overset{(H)}{=} \mathrm{Im}\,(\partial\otimes\mathrm{id})_* \overset{(*)}{=} \ker\omega \overset{(**)}{=} \mathrm{Tor}_1^R(H(C_\bullet),H(D_\bullet))\ . \end{aligned}$$

  wobei wir bei $(H)$ den Homomorphiesatz angewendet haben.

- Für den Beweis, dass die Künneth-Sequenz spaltet, verweisen wir auf Hilton-Stammbach, V.2.

□

Ein wichtiger Spezialfall ist der, wenn $C_\bullet$ flach ist und $D_\bullet$ ein $R$-Modul $A$, konzentriert in Grad 0.

**Korollar 6.8.3** (Universelles Koeffiziententheorem in Homologie).
Sei $R$ ein Hauptidealring, $C_\bullet$ ein flacher Kettenkomplex von $R$-Moduln und $A$ ein $R$-Modul. Dann gibt es eine natürliche kurze exakte Sequenz

$$0 \to H_n(C_\bullet) \otimes_R A \xrightarrow{\zeta} H_n(C_\bullet \otimes_R A) \to \mathrm{Tor}_1^R(H_{n-1}(C_\bullet), A) \to 0 \ .$$

Diese exakte Sequenz spaltet, und zwar natürlich in $A$, aber nicht natürlich in $C_\bullet$.

**Beweis.**
Es bleibt die Natürlichkeitsaussage zu zeigen, für die wir wieder auf Hilton-Stammbach verweigen. □

Wir halten auch entsprechende Theorem für Ext fest, für deren Beweis wir auf Hilton-Stammbach, §V.3 verweisen:

**Theorem 6.8.4.**
Seien $C_\bullet, D_\bullet$ Kettenkomplexe von Moduln über einem Hauptidealring $R$. Sei der Komplex $C_\bullet$ frei. Dann gibt es eine natürliche kurze exakte Sequenz

$$0 \to \prod_{q-p=n+1} \mathrm{Ext}_R^1(H_p(C_\bullet), H_q(D_\bullet)) \to H_n(\mathrm{Hom}_R(C_\bullet, D_\bullet) \xrightarrow{\zeta} \bigoplus_{q-p=n} \mathrm{Hom}_R(H_p(C_\bullet), H_q(D_\bullet)) \to 0 \ ,$$

wobei $\zeta$ den Morphismus $f \in Z_n(\mathrm{Hom}_R(C_\bullet, D_\bullet))$ auf den induzierten Morphismus $F_n : H_n(C_\bullet) \to H_n(D_\bullet)$ abbildet. Die Sequenz spaltet, aber nicht natürlich.

Wir erhalten analog das

**Korollar 6.8.5** (Universelles Koeffiziententheorem in Kohomologie).
Sei $R$ ein Hauptidealring, $C_\bullet$ ein freier Kettenkomplex von $R$-Moduln und $B$ ein $R$-Modul. Dann gibt es eine natürliche kurze exakte Sequenz

$$0 \to \mathrm{Ext}_R^1(H_{n-1}(C_\bullet), B) \to H^n(\mathrm{Hom}_R(C_\bullet, B)) \xrightarrow{\zeta} \mathrm{Hom}_R(H_n(C_\bullet), B) \to 0 \ .$$

Diese exakte Sequenz spaltet, und zwar natürlich in $B$, aber nicht natürlich in $C_\bullet$.

# 7 Gruppenkohomologie

## 7.1 Definition und Beispiele

Sei $G$ eine Gruppe. Unter einem $G$-Modul verstehen wir in diesem Kapitel der Kürze halber einen $\mathbb{Z}[G]$-Modul. Dies ist natürlich nichts anderes als eine abelsche Gruppe $M$ zusammen mit einer $G$-Operation $G \to \mathrm{Aut}_{\mathbb{Z}}(M)$ durch Morphismen abelscher Gruppen. Ist $A$ eine abelsche Gruppe, so verstehen wir $A$ auch als $G$-Modul mit der trivialen Operation, $\rho(g) = \mathrm{id}_A$ für alle $g \in G$.

Wir definieren zunächst:

***Definition 7.1.1***
*Die Invarianten $M^G$ eines $G$-Moduls $M$ sind die Fixpunkte der $G$-Operation:*

$$M^G = \{m \in M | g.m = m \text{ für alle } g \in G\} \ .$$

*Die Koinvarianten $M_G$ sind definiert als Quotient*

$$M_G = M/(gm - m | g \in G, m \in M) \ .$$

Wir machen Invarianten und Koinvarianten zu additiven Funktoren

$$(-)^G, (-)_G : \mathbb{Z}[G]\text{−Mod} \to Ab \ ,$$

die auf einem $\mathbb{Z}[G]$-Modulmorphismus $f : M \to N$ folgendermaßen definiert sind. Aus $g.m = m$ für alle $g \in G$ folgt $g.f(m) = f(g.m) = f(m)$ für alle $g \in G$, so dass die Einschränkung von $f$ auf die Invarianten ein Homomorphismus $f^G : M^G \to N^G$ abelscher Gruppen liefert. Weil $f(gm - m) = gf(m) - f(m)$ gilt, faktorisiert der Homomorphismus $M \xrightarrow{f} N \xrightarrow{\text{can}} N_G$ auf einen Homomorphismus abelscher Gruppen $f_G : M_G \to N_G$ auf den Koinvarianten,

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\text{can}"] & N \arrow[d, "\text{can}"] \\ M_G \arrow[r, dashed] & N_G \end{tikzcd}$$

**Lemma 7.1.2.**
Es gibt natürliche Isomorphismen $M^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ und $M_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$, wobei die abelsche Gruppe $\mathbb{Z}$ mit der trivialen Links- bzw. Rechtsmodulstruktur versehen wird. Insbesondere ist nach Beispiel 2.3.12.4 der Invariantenfunktor $(-)^G$ linksexakt und der Koinvariantenfunktor $(-)_G$ rechtsexakt nach Beispiel 2.3.12.3.

**Beweis.**
Für den ersten Isomorphismus beachte, dass ein Element aus $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M)$ durch das Bild des Erzeugers $1 \in \mathbb{Z}$ eindeutig festgelegt ist. Damit der Homomorphismus in $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \subset \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M)$ liegt, muss für alle $g \in G$ gelten $g.f(1) = f(g.1) = f(1)$. Also $f(1) \in M^G$ gelten. Umgekehrt definiert jedes solche $x \in M^G$ einen Morphismus in $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Für den zweiten Isomorphismus betrachte die surjektive Abbildung

$$\begin{array}{rcl} \phi : M & \to & \mathbb{Z} \otimes_{\mathbb{Z}[G]} M \\ m & \mapsto & 1 \otimes m \end{array}$$

Da in der abelschen Gruppe $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M$ gilt

$$1 \otimes (gm - m) = (1.g) \otimes m - 1 \otimes m = 0 \ ,$$

faktorisiert die Abbildung $\phi$ auf den Quotienten $M_G$, also die Koinvarianten. $\phi$ und somit auch die induzierte Abbildung ist surjektiv. Es ist klar, dass $1 \otimes m$ und $1 \otimes m'$ genau dann gleich sind, wenn $m \in M$ und $m' \in M$ die gleiche Klasse in den Koinvarianten bestimmen. □

***Definition 7.1.3***
*Sei $M$ ein $\mathbb{Z}[G]$-Modul.*

1. *Die $n$-te Homologie der Gruppe $G$ mit Koeffizienten im $\mathbb{Z}[G]$-Modul $M$ ist definiert als der $n$-te linksabgeleitete Funktor der Koinvarianten:*

$$H_n(G; M) := (L_n(-)_G)(M) \ = \ \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M) \ .$$

2. *Die Kohomologie der Gruppe $G$ mit Koeffizienten im $\mathbb{Z}[G]$-Modul $M$ ist definiert als*

$$H^n(G;M) := (R^n(-)^G)(M) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M) \ .$$

*Ist $M$ der triviale $G$-Modul $\mathbb{Z}$, so schreiben wir auch kürzer $H_n(G) := H_n(G,\mathbb{Z})$ und $H^n(G) := H^n(G,\mathbb{Z})$.*

**Bemerkung 7.1.4.**
Die Definitionen gehen auch durch, wenn man statt einer Gruppe $G$ ein Monoid betrachtet. Aber wirkungsvolle Methoden funktionieren nur für Gruppen, daher beschränken wir uns hier schon auf Gruppen.

**Beispiel 7.1.5.** (Homologie einer zyklischen Gruppe $C_n$)

1. Sei $G = C_n = \langle t \rangle$ eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ mit Erzeuger $t \in G$. Dann ist $R := \mathbb{Z}[G] \cong \mathbb{Z}[t]/(t^n - 1)$, und die Homologie wurde schon in Beispiel 6.5.2.3 berechnet:

$$H_k(C_n) \cong \begin{cases} \mathbb{Z}, & \text{falls } k = 0\,; \\ \mathbb{Z}_n, & \text{falls } k \text{ ungerade} \\ 0, & \text{sonst.} \end{cases} ;$$

2. Betrachten wir nun für die Koeffizienten die abelsche Gruppe $A = \mathbb{Z}_n$ mit der trivialen $\mathbb{Z}[G]$-Modulstruktur. Nach Tensorieren der Auflösung aus Beispiel 6.5.2.3

$$\cdots \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

mit $N := 1 + t + \cdots + t^{n-1}$ aus Beispiel 6.5.2.3 mit $\mathbb{Z}_n$ ergibt sich der Komplex

$$\ldots \xrightarrow{0} \mathbb{Z}_n \xrightarrow{0} \mathbb{Z}_n \to 0$$

und somit $H_k(C_n; \mathbb{Z}_n) \cong \mathbb{Z}_n$ für alle $k \geq 0$.

3. Betrachten wir den Fall beliebiger Moduln über einer zyklischen Gruppe $C_n$: Sei $M$ ein $C_n$-Modul. Das Bild der Multiplikation mit $N = 1 + t + \cdots + t^{n-1}$ ist wegen $gN = N$ für alle $g \in C_n$ in den Invarianten $M^G$. Die Multiplikation liefert daher eine Abbildung $M \to M^G$. Da außerdem $Ngm = Nm$ für alle $g \in C_n$ gilt, folgt, dass die Multiplikation mit $N$ auf eine sogenannte Normabbildung $\bar{N} : M_G \to M^G$ auf dem Quotienten $M_G$ faktorisiert.

   Es gilt im Falle einer zyklischen Gruppe mit Erzeuger $t$ für die Invarianten bzw. Koinvarianten

$$\ker(1-t) = M^G \quad \text{bzw.} \quad M/\mathrm{Im}\,(1-t) = M_G$$

   und daher

$$\ker N/\mathrm{Im}\,(1-t) = \ker \bar{N} \quad \text{bzw.} \quad \ker(1-t)/\mathrm{Im}\, N = M^G/\mathrm{Im}\, \bar{N} = \mathrm{coker}\bar{N} \ .$$

   Nach Tensorieren der Auflösung aus Beispiel 6.5.2.3 mit $M$ erhalten wir den Komplex

$$\cdots M \xrightarrow{1-t} M \xrightarrow{N} M \xrightarrow{1-t} M \to 0$$

   und somit

$$H_k(\mathbb{Z}_n; M) \cong \begin{cases} M/\mathrm{Im}\,(1-t) = M_G, & \text{falls } k = 0 \text{ (vgl. Lemma 6.3.5);} \\ \ker(1-t)/\mathrm{Im}\, N = \mathrm{coker}\bar{N}, & \text{falls } k \text{ ungerade;} \\ \ker N/\mathrm{Im}\,(1-t) = \ker \bar{N}, & \text{falls } k > 0 \text{ und } k \text{ gerade.} \end{cases}$$

4. Ebenso können wir die Kohomologie ausrechnen. Indem wir $\mathrm{Hom}_R(-, M)$ auf die Auflösung aus Beispiel 6.5.2.3 anwenden, erhalten wir den Komplex

$$0 \to M \stackrel{1-t}{\to} M \stackrel{N}{\to} M \stackrel{1-t}{\to} M \stackrel{N}{\to} \cdots$$

und somit

$$H^k(\mathbb{Z}_n; M) \cong \begin{cases} \ker(1-t) = M^G & \text{falls } k = 0 \text{ (vgl. Lemma 6.3.5);} \\ \ker N/\mathrm{Im}\,(1-t) = \ker \bar{N}, & \text{falls } k \text{ ungerade;} \\ \ker(1-t)/\mathrm{Im}\, N = \mathrm{coker}\bar{N}, & \text{falls } k > 0 \text{ gerade.} \end{cases}$$

**Beispiel 7.1.6** (Homologie der freien abelschen Gruppe $\mathbb{Z}$).
Der Gruppenring der Gruppe $G = \mathbb{Z}$ ist $\mathbb{Z}[G] \cong \mathbb{Z}[t, t^{-1}]$, also der Ring der Laurentpolynome $a_m t^m + \cdots + a_n t^n$ mit $m \leq n \in \mathbb{Z}$ und $a_n \in \mathbb{Z}$. Eine freie Auflösung des trivialen Moduls auf $\mathbb{Z}$ als $\mathbb{Z}[G]$-Modul ist gegeben durch den augmentierten Komplex

$$0 \to \mathbb{Z}[t, t^{-1}] \stackrel{1-t}{\to} \mathbb{Z}[t, t^{-1}] \stackrel{t \mapsto 1}{\to} \mathbb{Z} \to 0 \quad .$$

Tensoriert man die entsprechende Auflösung mit einem Modul $M$ über $\mathbb{Z}[G]$, so erhält man den Komplex

$$0 \to M \stackrel{1-t}{\to} M \to 0$$

aus dem folgt

$$H_0(G; M) = M/\mathrm{Im}\,(1-t) = M_G \quad \text{und} \quad H_1(G; M) = \ker(1-t) = M^G \ .$$

Das Ergebnis für $H_0(G, M)$ stimmt wieder mit Lemma 6.3.5 überein. Die Anwendung von $\mathrm{Hom}_{\mathbb{Z}}(-, M)$ liefert den gleichen Komplex mit anderer Graduierung und daher

$$H_0(G; M) = H^1(G; M) = M_G \text{ und } H_1(G; M) = H^0(G; M) = M^G \ .$$

Alle höhere Homologie und Kohomologie ist null, weil die Auflösung des trivialen $\mathbb{Z}[G]$-Moduls $\mathbb{Z}$ Länge 2 hat.

**Bemerkung 7.1.7** (Satz von Maschke).
Wir wollen den Satz von Maschke als Konsequenz einer Aussage über Kohomologiegruppen von Gruppen verstehen. Sei $G$ eine endliche Gruppe und $K$ ein Körper, dessen Charakteristik nicht die Gruppenordnung $|G|$ teilt. Man kann dann recht direkt zeigen (cf. Hilton-Stammbach, Lemma VI.16.7), dass dann für *jeden* $K[G]$-Modul $W$ und alle $n \geq 1$ gilt $H^n(G, W) = 0$. Wir zeigen, dass aus diesem Verschwindungssatz der Satz von Maschke 4.1.13 folgt.

Denn sei

$$0 \to V' \to V \to V'' \to 0$$

eine beliebige kurze exakte Sequenz von $K[G]$-Moduln. Wir wollen zeigen, dass dann die induzierte Sequenz

$$0 \to \mathrm{Hom}_G(V'', V') \to \mathrm{Hom}_G(V, V') \to \mathrm{Hom}_G(V', V') \to 0$$

exakt ist. Denn dann liefert das Urbild der Identität $\mathrm{id}_{V'}$ eine Retraktion $V \to V'$ von $K[G]$-Moduln, so dass die exakte Sequenz $0 \to V' \to V \to V'' \to 0$ spaltet, vgl. Satz 1.4.3. Dazu betrachten wir die entsprechende kurze exakte Sequenz von $K$-Vektorräumen,

$$0 \to \mathrm{Hom}_K(V'', V') \to \mathrm{Hom}_K(V, V') \to \mathrm{Hom}_K(V', V') \to 0 \ ,$$

die wir als exakte Sequenz von $K[G]$-Moduln ansehen. Die $G$-Wirkung auf den Vektorräumen linearer Abbildungen ist hierbei gegeben durch

$$\begin{array}{rcl} K[G] \times \mathrm{Hom}_K(V,W) & \to & \mathrm{Hom}_K(V,W) \\ (g,\varphi) & \mapsto & g.\varphi(-) + \varphi(g^{-1}.-) \ . \end{array}$$

Da die Elemente von $\mathrm{Hom}_G(V,W)$ genau die $G$-Invarianten im $K[G]$-Modul $\mathrm{Hom}_K(V,W)$ sind, müssen wir zeigen, dass die Sequenz der Invarianten

$$0 \to H^0(G, \mathrm{Hom}_K(V',V')) \to H^0(G, \mathrm{Hom}_K(V,V')) \to H^0(G, \mathrm{Hom}_K(V'',V')) \to 0$$

exakt ist. Dies aber folgt mit Hilfe der langen exakten Sequenz 6.4.4 aus $H^1(G,W) = 0$ mit dem $K[G]$-Modul $W = \mathrm{Hom}_K(V',V')$.

## 7.2 Funktorialität

Homologie und Kohomologie sind Funktoren, allerdings muss man bei der Definition sorgfältig sein.

***Definition 7.2.1***
*Sei $GrpMod$ die Kategorie, deren Objekte Paare sind, bestehend aus einer Gruppe $G$ und einem $G$-Modul $M$, und deren Morphismen definiert sind durch*

$$\begin{array}{l} \mathrm{Hom}_{GrpMod}((G,M),(G',M')) \\ := \{\alpha : G \to G', f : M \to M' | f(g.m) = \alpha(g)f(m) \text{ und } \alpha \text{ Gruppenhomomorphismus}\} \ . \end{array}$$

**Bemerkungen 7.2.2.**

1. Ein Morphismus $(\alpha, f) : (G,M) \to (G',N)$ ist also ein Morphismus $f : M \to \alpha^* N$ von $K[G]$-Moduln, wobei $\alpha^* N$ der $K[G]$-Modul ist, der durch Pullback entlang $\alpha$, also Restriktion der Skalare, aus $N$ entsteht.

2. Für festes $G$ kann die Kategorie $\mathrm{Mod}_{\mathbb{Z}[G]}$ als Unterkategorie von $GrpMod$ aufgefasst werden. Diese Unterkategorie ist nicht voll, da es in $GrpMod$ mehr Morphismen gibt, nämlich die mit $\alpha \neq \mathrm{id}_G$. Homologie ist ein Funktor auf dieser Unterkategorie, wegen der Funktorialität von Tor im zweiten Argument.

3. Andererseits kann man eine abelsche Gruppe $M$ festhalten und $Grp \hookrightarrow GrpMod$ als eine Unterkategorie auffassen, indem die Gruppe $G$ abgebildet wird auf $(G,M)$ mit der trivialen $G$-Modulstruktur auf $M$. Ist gezeigt, dass Gruppenhomologie ein Funktor ist, so erhält man für jeden Gruppenmorphismus $\alpha : G \to H$ eine induzierte Abbildung $\alpha_* : H_i(G) \to H_i(H)$ auf der Gruppenhomologie mit trivialen Koeffizienten.

**Satz 7.2.3.**
Gruppenhomologie ist in jedem Grad ein Funktor $GrpMod \to Ab$.

**Beweis.**
Sei $(\alpha, f) : (G,M) \to (H,N)$ ein Morphismus $GrpMod$. Wähle projektive Auflösungen $P_\bullet \to M$ über dem Ring $\mathbb{Z}[G]$ und $Q_\bullet \to N$ über $\mathbb{Z}[H]$. Wir können alle $H$-Moduln $Q_n$ in $Q_\bullet$ entlang

$\alpha$ zu $G$-Moduln zurückziehen und so $Q_\bullet$ als $\mathbb{Z}[G]$-Modulkomplex auffassen mit der gleichen Abbildung als Differential. Dieser Komplex ist dann zwar nicht mehr projektiv; da aber das Differenzial unverändert ist, ist der Komplex immer noch azyklisch. Wegen des Fundamentallemmas 6.3.1 gibt es eine bis auf Homotopie eindeutige Hochhebung $f_\bullet : P_\bullet \to \alpha^*(Q)_\bullet$ des Morphismus $f : M \to \alpha^*(N)$ von $G$-Moduln. Diese induziert einen Morphismus von Komplexen abelscher Gruppen

$$\mathrm{id} \otimes f_\bullet : \quad \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_\bullet \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \alpha^*(Q)_\bullet \ .$$

Da die Homologie der rechten Seite wegen $\mathbb{Z} \otimes_{\mathbb{Z}[G]} \alpha^*(Q)_\bullet = \mathbb{Z} \otimes_{\mathbb{Z}[H]} Q_\bullet$ gleich $H_i(H;N)$ ist, erhalten wir somit eine wohldefinierte Abbildung $(\alpha, f)_* : H_i(G;M) \to H_i(H;N)$. Die Funktorialität folgt aus der Eindeutigkeit der Hochhebung bis auf Homotopie. □

**Beispiel 7.2.4.**
Wir zeigen, dass die vom surjektiven Gruppenhomomorphismus $\alpha : \mathbb{Z} \to \mathbb{Z}_n$ induzierte Abbildung auf der Homologiegruppe $H_1(-;\mathbb{Z})$ surjektiv ist. Wir betrachten die Standardauflösungen aus den Beispielen 7.1.5 und 7.1.6 und eine offensichtliche Hochhebung der Identität auf dem trivialen Modul $\mathbb{Z}$:

$$\begin{tikzcd}
 & 0 \arrow[r] & \mathbb{Z}[t,t^{-1}] \arrow[r, "1-t"] \arrow[d, "t\mapsto t"] & \mathbb{Z}[t,t^{-1}] \arrow[r] \arrow[d, "t\mapsto t"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
\cdots \arrow[rr, "N"] & & \mathbb{Z}[t]/(t^n-1) \arrow[r, "1-t"] & \mathbb{Z}[t]/(t^n-1) \arrow[r] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Durch Übergang zu den Koinvarianten auf den Auflösungen erhalten wir den Morphismus von Komplexen

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "0"] \arrow[d, equal] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
\cdots \arrow[r, "n"] & \mathbb{Z} \arrow[r, "0"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

also ist die Abbildung auf $H_1(-,\mathbb{Z})$ die Standardreduktion $\mathbb{Z} \to \mathbb{Z}_n$ von abelschen Gruppen.

**Satz 7.2.5.**
Sei $G$ eine Gruppe und $M$ ein $G$-Modul. Sei $g_0 \in G$ und betrachte den Automorphismus $(\alpha, f) : M \to M$ in *GrpMod*, der gegeben ist durch $\alpha(g) := g_0 g g_0^{-1}$ und $f(m) := g_0.m.$ [1] Dieser indzuiert die Identität in Homologie, $(\alpha, f)_* = \mathrm{id}_{H_*(G;M)}$.

**Beweis.**
Sei $P_\bullet \to M$ eine projektive Auflösung von $M$ über dem Ring $\mathbb{Z}[G]$. Definiere einen Automorphismus von $P_\bullet$ durch $\tau(x) = g_0.x$ für $x \in P_n$, für alle $n$. Dann ist $\tau$ ein Automorphismus von Kettenkomplexen, der den Morphismus $f : M \to M$ fortsetzt, also kann der Morphismus $(\alpha, f)_*$ auf der Homologie berechnet werden als die von $\tau$ induzierte Abbildung in Homologie. Aber nach Tensorieren mit dem trivialen Modul $\mathbb{Z}$, auf dem insbesondere $g_0$ trivial wirkt, ist

$$\mathrm{id}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \tau : \quad \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_n \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_n$$

die Identität. □

[1] Dann gilt $f(gm) = g_0 gm = g_0 g g_0^{-1} g_0 m = \alpha(g) f(m)$.

**Bemerkung 7.2.6.**
Ist $G$ eine Gruppe, so nennt man die Automorphismen, die sich durch Konjugation darstellen lassen, die inneren Automorphismen; diese bilden einen Normalteiler $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$. Die Quotientengruppe $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ heißt die Gruppe der äußeren Automorphismen. Der Satz 7.2.5 zeigt, dass die Gruppenhomologie $H_*(G)$ eine Operation der Quotientengruppe $\mathrm{Out}(G)$ trägt.

## 7.3 Die Bar-Auflösung

In den bisherigen Beispielen haben wir stets Auflösungen ad hoc konstruiert. Die Frage liegt nahe, ob es eine kanonische, funktorielle Art gibt, eine Auflösung eines Moduls über $\mathbb{Z}[G]$ zu erzeugen. Die Antwort ist ja, aber für explizite Berechnungen der gesamten Gruppenhomologie eignet sie sich selten, weil sie sehr groß ist.

***Definition 7.3.1***
*Sei $R$ ein Ring und $M$ ein $R$-Modul. Um den Bar-Komplex $B_\bullet(R;M)$ einzuführen, betrachte für $n \geq 0$ die abelschen Gruppen*

$$B_n(R;M) := R^{\otimes n+1} \otimes_{\mathbb{Z}} M \equiv R \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} \ M.$$

*Wir führen aus historischen Gründen die Schreibweise $a|b$ für $a \otimes b$ ein; sie gibt dem Bar-Komplex seinen Namen. Wir versehen die abelsche Gruppe $B_n(R;M)$ mit einer $R$-Modulstruktur durch Linksmultiplikation*

$$r.(r_0|\cdots|r_n|m) := rr_0|r_1|\cdots|r_n|m \ .$$

*Schließlich führen wir noch Differentiale $d : B_n(R,M) \to B_{n-1}(R,M)$ ein durch*

$$d := \sum_{i=0}^{n} (-1)^i d_i \quad \text{mit} \quad d_i(r_0|\cdots|r_n|m) := r_0|\cdots|r_i r_{i+1}|\cdots|r_n|m \ ,$$

*mit $r_i \in R$ für $i \leq n$ und $r_{n+1} \in M$.*

**Satz 7.3.2.**
Die Sequenz $B_\bullet(R;M)$ ist eine Auflösung von $M$ über $R$, also ein exakter Komplex von $R$-Moduln mit Surjektion auf $M$.

**Beweis.**
Um zu zeigen, dass $B_\bullet(R;M)$ ein Komplex ist, beachten wir, dass

$$d_i \circ d_j = d_j \circ d_{i+1} \text{ falls } i \geq j \qquad\qquad (*)$$

gilt. Man mache sich klar, dass in diese Gleichung für $i = j+1$ die Assoziativität der Multiplikation in $R$ und die Moduleigenschaft von $M$ eingehen. Hieraus folgt

$$\begin{aligned}
d \circ d &\overset{\text{def}}{=} \textstyle\sum_{i=0}^{n-1} \sum_{j=0}^{n} (-1)^{i+j} d_i \circ d_j \\
&= \textstyle\sum_{i=0}^{n-1} \sum_{j=0}^{i} (-1)^{i+j} d_i \circ d_j + \sum_{i=0}^{n-1} \sum_{j=i+1}^{n} (-1)^{i+j} d_i \circ d_j \\
&\overset{(*)}{=} \textstyle\sum_{i=1}^{n} \sum_{j=0}^{i-1} (-1)^{i+j-1} d_j \circ d_i + \sum_{i=0}^{n-1} \sum_{j=i+1}^{n} (-1)^{i+j} d_i \circ d_j \\
&= \textstyle\sum_{j=0}^{n-1} \sum_{i=j+1}^{n} (-1)^{i+j-1} d_j \circ d_i + \sum_{i=0}^{n-1} \sum_{j=i+1}^{n} (-1)^{i+j} d_i \circ d_j = 0 \ .
\end{aligned}$$

Hierbei wurde die Summe zuerst aufgespalten, dann die obige Relation $(*)$ auf den ersten Summanden angewandt und schließlich die erste Summe umsortiert.

Es bleibt zu zeigen, dass der Komplex $B_\bullet(R;M)$ exakt ist. Dazu konstruieren wir eine Kettenkontraktion, also einen Kettennullhomotopie, $h : B_n(R;M) \to B_{n+1}(R;M)$, so dass $h \circ d + d \circ h = \mathrm{id}$ gilt. Wir benutzen dafür die Eins $1 \in R$ und setzen

$$h(r_0|\cdots|r_n) := 1|r_0|\cdots|r_n \ .$$

Dann gilt $h \circ d_i = d_{i+1} \circ h$ für $i = 0, \ldots, n$ und damit

$$d \circ h + h \circ d \stackrel{\text{def}}{=} \sum_{i=0}^{n+1} (-1)^i d_i \circ h + \sum_{i=0}^{n} (-1)^i h \circ d_i = d_0 \circ h = \mathrm{id}\,.$$

□

**Bemerkungen 7.3.3.**

1. Der $R$-Modul $B_n(R,M)$ ist nicht unbedingt projektiv; ist zum Beispiel $R = \mathbb{Z}$ und $M = \mathbb{Z}_n$, so ist $B_n(R;M) = R^{\otimes n+1} \otimes_{\mathbb{Z}} \mathbb{Z}_n = \mathbb{Z}_n$. Sind aber der Ring $R$ und der Modul $M$ als abelsche Gruppen frei, so ist auch $B_n(R;M)$ ein freier $R$-Modul für alle $n$, und wir haben eine freie und somit insbesondere projektive Auflösung gefunden.
2. Gruppenringe $R = \tilde{R}[G]$ sind immer frei als abelsche Gruppen, wenn der Grundring $\tilde{R}$ als abelsche Gruppe frei ist.
3. Allgemeiner gilt, wenn $K$ ein kommutativer Grundring ist, $R$ eine $K$-Algebra, und wenn alle Tensorprodukte in $B_n(R;M)$ statt über $\mathbb{Z}$ über $K$ gebildet werden, dass $B_n(R;M)$ ein freier $R$-Modul ist, wenn $R$ und $M$ freie $K$-Moduln sind. Für den Fall, dass $K$ ein Körper ist, ist dies natürlich immer erfüllt.

Wir können nun die erste Homologiegruppe mit einer klassischen algebraischen Größe identifizieren. Dazu erinnern wir an die Abelisierung:

**Beispiel 7.3.4** (Erste Homologiegruppe)**.**

- Dazu erinnern wir an die Abelisierung: Sei $G$ eine beliebige Gruppe, und bezeichne $G_{ab}$ die Abelisierung, d.h. den maximalen abelschen Quotienten von $G$. Es gilt $G_{ab} = G/G'$, wobei $G'$ der Normalteiler ist, der von den Kommutatoren $[x,y] := xyx^{-1}y^{-1}$ mit $x, y \in G$ erzeugt wird.

  Nach Beispiel 2.2.4.5 ist die Abelisierung der linksadjungierte Funktor zur Einbettung $Ab \to Grp$, so dass für jede abelsche Gruppe $A$ gilt

  $$\mathrm{Hom}_{Grp}(G,A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{ab},A)\ .$$

  Die entsprechende universelle Eigenschaft legt $G_{ab}$ bis auf eindeutige Isomorphie fest.

- Wir behaupten, dass für alle Gruppen gilt $H_1(G;\mathbb{Z}) \cong G_{ab}$. Um dies zu sehen, betrachten wir den Anfang der Bar-Auflösung des trivialen Moduls $\mathbb{Z}$ über $\mathbb{Z}[G]$ und beachten, dass gilt

  $$B_n(\mathbb{Z}[G],\mathbb{Z}) = \mathbb{Z}[G]^{\otimes_{\mathbb{Z}} n+1} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}[G]^{\otimes n+1}$$

so dass die ersten Differentiale wie folgt definiert sind:

$$\begin{tikzcd}
\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] \arrow[r] & \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] \arrow[r] & \mathbb{Z}[G] \\
g_0|g_1|g_2 \arrow[r, mapsto] & g_0g_1|g_2 - g_0|g_1g_2 + g_0|g_1 & \\
 & g_0|g_1 \arrow[r, mapsto] & g_0g_1 - g_0
\end{tikzcd}$$

Man beachte, dass auf dem trivialen Modul das Element rechts außen trivial wirkt. Da $\mathbb{Z}$ ein freier $\mathbb{Z}$-Modul ist, haben wir eine freie Auflösung des trivialen $\mathbb{Z}[G]$-Moduls $\mathbb{Z}$ gefunden. Um die Homologie $H_1(G, \mathbb{Z})$ mit Koeffizienten im trivialen Modul $\mathbb{Z}$ zu finden, tensorieren wir diese Sequenz von links mit dem trivialen $\mathbb{Z}[G]$-Modul $\mathbb{Z}$ über $\mathbb{Z}[G]$ und erhalten

$$\begin{tikzcd}
\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] \arrow[r] & \mathbb{Z}[G] \arrow[r] & \mathbb{Z} \\
g_1|g_2 \arrow[r, mapsto] & g_2 - g_1g_2 + g_1 & \\
 & g \arrow[r, mapsto] & 0
\end{tikzcd}$$

Also ist

$$H_1(G;\mathbb{Z}) = \mathbb{Z}[G]/(g_1 + g_2 - g_1g_2 | g_1, g_2 \in G) \ .$$

- Nun ist die Abbildung

$$G \to \mathbb{Z}[G] \stackrel{\text{can}}{\to} \mathbb{Z}[G]/(g_1 + g_2 - g_1g_2 | g_1, g_2 \in G) \cong H_1(G;\mathbb{Z})$$

  ein Epimorphismus von Gruppen. Denn im Quotienten ist die Klasse von $ng \in \mathbb{Z}[G]$ gleich der Klasse des Gruppenelements $g^n$. Es genügt nun, für diese Abbildung die universelle Eigenschaft der Abelisierung nachzuweisen, dass jeder Gruppenmorphismus $f : G \to A$ in eine abelsche Gruppe eindeutig durch $H_1(G;\mathbb{Z})$ faktorisiert. Da $A$ abelsch ist, kann man $f$ auf *eindeutige* Weise zu einem Homomorphismus $\mathbb{Z}[G] \to A$ fortsetzen, nämlich durch $\sum_g a_g g \mapsto \sum_g a_g f(g)$. Unter dieser Abbildung geht ein Element der Form $g_1 + g_2 - g_1g_2$ nach null, weil $f$ ein Gruppenhomomorphismus ist. Daher erfüllt $H_1(G;\mathbb{Z})$ die universelle Eigenschaft 2.2.4.3 der Abelisierung.

## 7.4 Gruppenkohomologie und Gruppenerweiterungen

**Betrachtung 7.4.1.**

1. Sei $G' \lhd G$ ein Normalteiler in einer Gruppe $G$ mit Quotientengruppe $G''$. Wir erlauben uns, dies in Form einer exakten Sequenz $1 \to G' \to G \to G'' \to 1$ zu notieren, obwohl die Kategorie der Gruppen nicht abelsch ist. Wir nennen in diesem Fall $G$ eine Erweiterung von $G''$ durch $G'$. Zwei Erweiterungen heißen äquivalent, falls es ein kommutatives Diagramm von Gruppenhomomorphismen gibt:

$$\begin{tikzcd}
 & & G_1 \arrow[dd, "f"] \arrow[dr] & & \\
1 \arrow[r] & G' \arrow[ur] \arrow[dr] & & G'' \arrow[r] & 1 \\
 & & G_2 \arrow[ur] & &
\end{tikzcd}$$

In diesem Fall ist $f$ automatisch ein Isomorphismus. Zunächst folgt aus Kommutativität des rechten Dreieckes $\ker f \subset \ker(G_1 \to G'')$. Ist $x \in \ker f \subset \ker(G_1 \to G'') = \mathrm{Im}\,(G' \to G_1)$, so finde ein Urbild $y \in G'$, das injektiv in $G_2$ abbildet wird. Dort ist aber das Bild $f(x)$ das neutrale Element, also sind auch $y \in G'$ und daher $x \in G_1$ jeweils das neutrale Element. Daher ist $f$ injektiv.

Um die Surjektivität zu sehen, finde für das Bild $x'' \in G''$ eines vorgebenen Elements $x_2 \in G_2$ ein Urbild $x_1 \in G_1$. Dann haben $f(x_1)$ und $x_2$ das gleiche Bild in $G''$, daher ist $f(x_1)x_2^{-1} \in \ker(G_2 \to \ G'') = \mathrm{Im}\,(G' \to G_2)$. Also $f(x_1) = x_2\iota_2(g') = x_2 f(\iota_1 g')$ für ein $g' \in G'$. Es ist $x_2 = f(x_1\iota_1(g')^{-1})$ und $f$ surjektiv.

2. Ist eine Erweiterung $1 \to G' \to G \to G'' \to 1$ mit *abelschem* Normalteiler $G'$ gegeben, so operiert die Quotientengruppe $G''$, die nicht unbedingt abelsch sein muss, auf der abelschen Gruppe $G'$ wie folgt. Sei $g \in G$ ein Urbild von $g'' \in G''$. Wir setzen für $g_0 \in G'$

$$g''.g_0 := g g_0 g^{-1} \ .$$

Da $G'$ ein Normalteiler ist, liegt $g''.g_0$ wieder in $G'$. Die Wahl des Urbilds $g$ von $g''$ ist unerheblich, denn zwei solche Wahlen unterscheiden sich durch ein Element der abelschen Gruppe $G'$, und Konjugation mit Elementen von $G'$ ist die Identität auf $G'$.

3. Umgekehrt lässt sich aus jeder Operation $\alpha : G'' \to \mathrm{Aut}(G')$ von $G''$ auf *einer beliebigen Gruppe* $G'$ durch Gruppenautomorphismen eine Erweiterung $G = G' \rtimes_\alpha G''$, das <u>semi-direkte Produkt</u>, bilden. Die zu Grunde liegende Menge von $G$ ist $G' \times G''$, und die Multiplikation ist definiert durch

$$(g_1', g_1'') \cdot (g_2', g_2'') := (g_1'(g_1''.g_2'), g_1''g_2'') \ .$$

Man erhält so eine Gruppe $G' \rtimes G''$. Die Gruppenhomomorphismen

$$\begin{array}{ccc} G' & \to & G' \rtimes G'' \\ g' & \mapsto & (g', e) \end{array}$$

und

$$\begin{array}{ccc} G' \rtimes G'' & \to & G'' \\ (g', g'') & \mapsto & g'' \end{array}$$

geben eine Erweiterung $1 \to G' \to G' \rtimes G'' \to G'' \to 1$. Insbesondere ist $G'$ ein Normalteiler. Die Merkregel für die Richtung des Zeichens $\rtimes$: die Spitze des Dreiecks zeigt in Richtung des Normalteilers). Man rechne nach, dass die Konjugation mit $(e, g'')$ in $G' \rtimes G''$ den Automorphismus $\alpha$ liefert:

$$(e, g'')(g', e)(e, g'')^{-1} = (\alpha(g'')(g'), e) \ .$$

4. Die Erweiterung $1 \to G' \to G' \rtimes G'' \to G'' \to 1$ zerfällt, denn der Gruppenhomomorphismus $s_0 : G'' \stackrel{g'' \mapsto (1,g'')}{\longrightarrow} G' \rtimes G''$ ist ein Schnitt. Zwei Schnitte $s_1, s_2 : G'' \to G' \rtimes G''$ heißen äquivalent, falls sie sich nur durch Konjugation mit einem Element aus $G'$ unterscheiden, d.h. falls $s_2(g'') = g's_1(g'')(g')^{-1}$ für ein $g' \in G'$ und für alle $g'' \in G''$ gilt.

5. Folgende natürliche Fragen stellen sich:

   - Zerfallen alle Erweiterungen, so dass semidirekte Produkte vorliegen? Wenn nein, wie lassen sie sich bis auf Äquivalenz bestimmen?

- Ist $s_0$ der einzig mögliche Schnitt? Wenn nein, wie lässt sich die Menge aller Schnitte bis auf Äquivalenz beschreiben?

6. Gruppenkohomologie beantwortet beide Fragen, zumindest für abelsche Normalteiler $G'$. Wir betrachten zunächst den zweiten Punkt. Ein Schnitt $s = (\delta, \mathrm{id}) : G'' \to G' \rtimes G''$ muss die Identität auf der zweiten Koordinate sein. Wir schreiben die erste Komponente mit Werten in der abelschen Gruppe $G'$ additiv. Dann muss ein Schnitt ein Gruppenhomomorphismus sein,

$$(\delta g_1'', g_1'') \cdot (\delta g_2'', g_2'') = (\delta g_1'' + g_1''.\delta g_2'', g_1'' g_2'') \overset{!}{=} (\delta(g_1'' g_2''), g_1'' g_2'') \ ,$$

also muss die Funktion $\delta : G'' \to G'$, die den Schnitt $s$ festlegt, die Gleichung

$$\delta(g_1'' g_2'') = \delta(g_1'') + g_1''.\delta(g_2'') \ . \tag{10}$$

erfüllen.

7. Wenn zwei Funktionen $\delta_1, \delta_2 : G'' \to G'$ beide die Gleichung (10) erfüllen, dann auch die Summe $\delta_1 + \delta_2$; dies definiert also eine abelsche Gruppenstruktur auf der Menge aller Schnitte. Ein Schnitt $\delta$ ist genau dann äquivalent zum Nullschnitt $s_0$, wenn es ein $g' \in G'$ gibt, so dass

$$\delta(g'') = g' - g''.(g') \quad \text{für alle } g'' \in G'' \ .$$

**Satz 7.4.2.**
Sei $G'$ eine abelsche Gruppe; sei $G''$ eine Gruppe, die durch Gruppenautomorphismen auf $G'$ operiere. Die Gruppe der Schnitte $G'' \to G' \rtimes_\alpha G''$ ist dann isomorph zu $H^1(G'', G')$, wobei die abelsche Gruppe $G'$ über die $G''$-Operation $\alpha$ als $G''$-Modul gesehen wird.

**Beweis.**

- Wir betrachten wie in Beispiel 7.3.4 die Bar-Auflösung des trivialen $G''$-Moduls $\mathbb{Z}$ und studieren den Komplex abelscher Gruppen mit

$$C^n := \mathrm{Hom}_{\mathbb{Z}[G'']}(\mathbb{Z}[G'']^{\otimes n+1}, G') \ .$$

Dann gilt nach Definition von Gruppenkohomologie $H^n(G'', G') = H^n(C^\bullet)$. Eine 1-Kokette $C^1$ ist ein $\mathbb{Z}[G'']$-linearer Morphismus mit Werten in der abelschen Gruppe $G'$,

$$f : \mathbb{Z}[G''] \otimes_{\mathbb{Z}} \mathbb{Z}[G''] \to G' \quad .$$

Wegen des Isomorphismus für induzierte $\mathbb{Z}[G]$-Moduln

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}[G'']}(\mathbb{Z}[G''] \otimes_{\mathbb{Z}} \mathbb{Z}[G''], G') & \to & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G''], G') \\ f & \mapsto & s(-) = f(1, -) \end{array}$$

ist diese Funktion äquivalent zu einem $\mathbb{Z}$-linearen Morphismus $s : \mathbb{Z}[G''] \to G'$. Die Umkehrabbildung ist $f(g_1''|g_2'') = g_1''.s(g_2'')$. Der Morphismus abelscher Gruppen $s : \mathbb{Z}[G''] \to G'$ ist wiederum durch seine Werte auf der Basis $G'' \subset \mathbb{Z}[G'']$ festgelegt und daher äquivalent zu einer Funktion $\delta : G'' \to G'$. Die Funktion $f$ ist wegen der Auflösung aus 7.3.4 genau dann ein Kozykel, wenn

$$0 = df(g_0''|g_1''|g_2'') = f(g_0'' g_1''|g_2'') - f(g_0''|g_1'' g_2'') + f(g_0''|g_1'')$$

gilt, also falls mit $g_0'' = 1$ für die Funktion $\delta$ gilt

$$0 = g_1''\delta(g_2'') - \delta(g_1'' g_2') + \delta(g_1'') \ . \tag{11}$$

Also falls $\delta$ die Gleichung (10) erfüllt.

- Ferner ist $f$ genau dann ein Korand, wenn es einen $\mathbb{Z}[G]$-linearen Morphismus $\tilde{f}:\mathbb{Z}[G]\to G'$ gibt mit
$$f(g_0''|g_1'') = \tilde{f}(g_0'') - \tilde{f}(g_1'') ,$$
also falls es ein $g' = \tilde{f}(1) \in G'$ gibt, so dass
$$\delta(g_1'') = f(1, g_1'') = \tilde{f}(1) - \tilde{f}(g_1'') = g' - g_1''(g') . \tag{12}$$
Genau dann ist aber nach 7.4.1.7 der zugehörige Schnitt äquivalent zum Nullschnitt.

□

Wir beschreiben als Vorbereitung für Satz 7.4.3 auch noch die Elemente der Kohomologiegruppe $H^2(G'', G')$ als Äquivalenzklassen von Funktionen $f : G'' \times G'' \to G'$ mit
$$(df)(g_1'', g_2'', g_3'') = g_1''.f(g_2'', g_3'') - f(g_1''g_2'', g_3'') + f(g_1'', g_2''g_3'') - f(g_1'', g_2'') = 0 , \tag{13}$$
modulo der Identifikation von Funktionen, die sich um einen Ausdruck der Form
$$da(g_1'', g_2'') := a(g_1'') - a(g_1''g_2'') + g_1''.a(g_2'')$$
mit einer Funktion $a : G'' \to G'$ unterscheiden.

**Satz 7.4.3.**
Sei $G''$ eine Gruppe, die auf der abelschen Gruppe $G'$ durch Gruppenautomorphismen operiert. Dann gibt es eine Bijektion von der Menge der Erweiterungen von $G''$ durch $G'$ modulo Äquivalenz wie in 7.4.1.1 nach $H^2(G'', G')$, wobei die abelsche Gruppe $G'$ durch die $G''$-Operation zum $G''$-Modul wird.

**Beweis.**
- Sei $E : 1 \to G' \to G \to G'' \to 1$ eine solche Erweiterung. Im Allgemeinen gibt es keinen Schnitt $G'' \to G$, der ein Gruppenhomomorphismus ist. Wir wählen daher einen Schnitt $s : G'' \to G$ von Mengen. Dann ist $s(g_1'')s(g_2'')s(g_1''g_2'')^{-1}$ in $\ker(G \to G'') = \mathrm{Im}\,(G' \to G) \cong G'$. Wir definieren daher die Funktion
$$\begin{array}{rcl} f_{E,s} : G'' \times G'' & \to & G' \\ (g_1'', g_2'') & \mapsto & s(g_1'')s(g_2'')s(g_1''g_2'')^{-1} . \end{array}$$
Man rechnet nach, dass Kozykelbedingung (13) erfüllt ist; daher definiert $f_{E,s}$ eine Klasse in $H^2(G'', G')$.

- Ist $s' : G'' \to G$ ein anderer Schnitt für die gleiche Erweiterung, so setze $a := s's^{-1} : G'' \to G'$. Damit ist
$$\begin{array}{rcl} (f_{E,s'} - f_{E,s})(g_1'', g_2'') & = & a(g_1'')s(g_1'')a(g_2'')s(g_2'')s(g_1''g_2'')^{-1}a(g_1''g_2'')^{-1}s(g_1''g_2'')s(g_2'')^{-1}s(g_1'')^{-1} \\ & = & a(g_1'')s(g_1'')a(g_2'')s(g_1'')^{-1}a(g_1''g_2'')^{-1} \\ & = & a(g_1'') - a(g_1''g_2'') + g_1''.a(g_2'') = (da)(g_1'', g_2'') . \end{array}$$
Hierbei wurde die letzte Zeile additiv geschrieben, da alle Terme in der abelschen Untergruppe $G'$ liegen. Die Klasse von $f$ in $H^2(G'', G')$ hängt also nicht von der Wahl des Schnitts $s$ ab. Man rechnet nach, dass äquivalente Erweiterungen dieselbe Funktion $f$ ergeben.

- Umgekehrt sei eine beliebige Funktion $f : G'' \times G'' \to G'$ gegeben. Wir versuchen, eine Gruppenstruktur $G_f$ auf der Menge $G' \times G''$ durch

$$(g_1', g_1'')(g_2', g_2'') := (g_1' + g_1''.g_2' + f(g_1'', g_2''), g_1''g_2'')$$

zu definieren. Die Projektion $G_f \to G''$ ergibt eine kurze exakte Sequenz $E_f : 1 \to G' \to G_f \to G'' \to 1$. Man rechnet leicht nach, dass es stets Inverse in $G_f$ gibt. Die Assoziativität der Multiplikation ist dagegen nicht automatisch:

$$\begin{aligned}
[(g_1', g_1'')(g_2', g_2'')](g_3', g_3'') &= (g_1' + g_1''.g_2' + f(g_1'', g_2''), g_1''g_2'') \cdot (g_3', g_3'') \\
&= (g_1' + g_1''.g_2' + f(g_1'', g_2'') + (g_1''g_2'').g_3' + f(g_1''g_2'', g_3''), g_1''g_2''g_3'') \; . \\
(g_1', g_1'')[(g_2', g_2'')(g_3', g_3'')] &= (g_1', g_1'')(g_2' + g_2''.g_3' + f(g_2'', g_3''), g_2''g_3'') \\
&= (g_1' + g_1''.(g_2' + g_2''.g_3' + f(g_2'', g_3'')) + f(g_1'', g_2''g_3''), g_1''g_2''g_3'')
\end{aligned}$$

Die Komponente in $G'$ der Differenz der beiden Ausdrücke ist:

$$g_1''f(g_2'', g_3'') - f(g_1''g_2'', g_3'') + f(g_1'', g_2''g_3'') - f(g_1'', g_2'') = (df)(g_1'', g_2'', g_3'') \; .$$

Also definiert $f$ genau dann eine Gruppenstruktur, wenn $df = 0$ gilt. Ist $f = f_{E,s}$, so ist $E_f$ äquivalent zu $E$, und somit erhalten wir eine Bijektion

$$\left\{ \begin{array}{l} \text{Erweiterungen von } G'' \text{ durch } G' \\ \text{modulo Äquivalenz} \end{array} \right\} \cong \left\{ \begin{array}{l} \text{Funktionen } f : G'' \times G'' \to G' \text{ mit } df = 0 \\ \text{modulo Funktionen } da \text{ für } a : G'' \to G' \end{array} \right\} .$$

Die rechte Seite ist nach der vorangegangenen Betrachtung mit der Bar-Auflösung genau $H^2(G'', G')$.

□

**Betrachtung 7.4.4.**

- Sei $K/k$ eine Galoiserweiterung und $G := \mathrm{Gal}(K/k)$ die Galoisgruppe. Dann heißen die Gruppen $H^n(G, K^*)$ die Galois-Kohomologiegruppen der Erweiterung $K/k$ mit Koeffizienten in $K^*$.

- Eine Version von Hilberts Theorem 90 besagt, dass $H^0(G, K^*) = k^*$ und $H^1(G, K^*) = 1$ gilt.

- Eine Funktion $\varphi : G \to K^*$, die eine Klasse in $H^1(G, K^*) = 1$ repräsentiert, erfüllt nach Geichung (11) die Gleichung

$$\varphi(\sigma\tau) = \tau\left(\varphi(\sigma)\right)\varphi(\tau) \; . \qquad (*)$$

Klassisch nennt man eine solche Funktion einen gekreuzten Homomorphismus. Sie ist nach Gleichung (12) genau dann ein Korand, wenn es ein Element $\alpha \in K^*$ gibt, so dass

$$\varphi(\sigma) = \frac{\alpha}{\sigma(\alpha)}$$

gilt. Man sagt dann, der gekreuzte Homomorphismus spalte. Hilberts Theorem 90 besagt, dass dies für endliche Galoiserweiterungen der Fall ist.

- Ist die Körpererweiterung zyklisch, d.h. $G = \langle\sigma\rangle$, so ist für jeden gekreuzten Homomorphismus $\varphi$

$$\begin{aligned} N(\varphi(\sigma)) &\overset{\text{def}}{=} \sigma^{n-1}(\varphi(\sigma))\ldots\sigma^2(\varphi(\sigma))\cdot\sigma(\varphi(\sigma))\cdot\varphi(\sigma) \\ &\overset{(*)}{=} \sigma^{n-1}(\varphi(\sigma))\ldots\sigma^2(\varphi(\sigma))\cdot\varphi(\sigma^2) \\ &\overset{(*)}{=} \sigma^{n-1}(\varphi(\sigma))\ldots\varphi(\sigma^2) = \varphi(\sigma^n) = 1 \end{aligned}$$

  Man sieht auch leicht, dass umgekehrt es für jedes Element $\gamma \in K$ mit Norm $N(\gamma) = 1$ einen eindeutigen gekreuzten Homomorphismus gibt, der auf dem Erzeuger durch $\varphi(\sigma) = \gamma$ definiert ist.

- Damit folgt für zyklische Körpererweiterungen die klassische Aussage: ein Element $\gamma \in K^*$ hat genau dann Norm 1, wenn es einen gekreuzten Homomorphismus mit $\varphi(\sigma) = \gamma$ gibt, also ein $\alpha \in K^*$ gibt mit $\gamma = \varphi(\sigma) = \frac{\alpha}{\sigma(\alpha)}$.

Auch die Kohomologie $H^2(G, K^*)$ hat klassische Anwendungen. Für Hintergrund zu den folgenden Bemerkungen verweisen wir auf B. Farb und R.K. Dennis, *Noncommutative Algebra*, Springer Graduate Texts in Mathematics 144, 1993.

***Definition 7.4.5***

1. *Eine Algebra $A$ über einem kommutativen Ring $R$ heißt <u>zentral</u>, wenn für ihr Zentrum $Z(A) = R$ gilt.*

2. *Eine Algebra heißt <u>zentral einfach</u>, wenn Sie zentral und einfach ist, d.h. zentral ist und keine beidseitigen Ideale hat.*

**Beispiele 7.4.6.**

1. Die Quaternionen $\mathbb{H}$ sind eine zentral einfache $\mathbb{R}$-Algebra.

2. Jede volle Matrixalgebra $M(n \times n, k)$ über einem Körper $k$ ist zentral einfach.

3. Eine echte Körpererweiterung $K/k$ ist nicht zentral einfach, denn es gilt $Z(K) = K \supsetneq k$.

4. Divisionsalgebren sind nicht unbedingt zentral einfach, z.B. ist die reelle Divisionsalgebra $\mathbb{C}$ nicht halbeinfach.

**Bemerkungen 7.4.7.**

1. Sind $R$ und $S$ zentral einfache Algebren, dann auch $R \otimes S$. (Zum Beispiel sind die Algebren $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$ und $M(n \times n, k) \otimes S$ für jede zentral einfache Algebra zentral einfach.

2. Für eine endlich-dimensionale zentral einfache $k$-Algebra $R$ gilt $R \otimes R^{\text{opp}} \cong M(n \times n, k)$ mit $n := \dim_k R$.

3. Sei $D$ eine Divisionsalgebra über $k$. Eine Körpererweiterung $K/k$ so dass $D_K := D \otimes_k K \cong M(n \times n, K)$ heißt ein Zerfällungskörper für $D$.

   Jeder maximale Unterkörper $K \subset D$ ist ein Zerfällungskörper von $D$ und es gilt $[K : k] =: n$.

***Definition 7.4.8***

1. *Seien $S$ und $T$ endlich-dimensionale zentral einfach $k$-Algebren. Wir sagen, $S$ und $T$ sind ähnlich, $S \sim T$, wenn eine der äquivalenten Bedingungen gilt:*

   *(a) Gilt $S \cong M(n \times n, D)$ und $T \cong M(m \times m,\ E)$ mit Divisionsalgebren $D, E$, so ist $D \cong E$.*

   *(b) Es gibt $m, n$, so dass $S \otimes_k M_m(k) \cong T \otimes_k M_n(k)$ gilt.*

   *(c) Es gibt $m.n$, so dass $M_m(S) \cong M_n(T)$ gilt.*

2. *Die Brauer-Gruppe $Br(k)$ eines Körpers $k$ ist die Menge der Äquivalenzklassen eindliche-dimensionaler einfacher $k$-Algebren unter Ähnlichkeit. Die Gruppenoperation wird durch das Tensorprodukt induziert, die Klasse $[k]$ gibt das neutrale Element.*

Die Brauergruppe klassifiziert Divisionsalgebren in dem Sinne, dass jedes Element von $Br(k)$ einer anderen Divisionsalgebra entspricht. Sie ist abelsch.

**Beispiele 7.4.9.**

1. Es gilt $Br(k) = 0$, wenn $k$ ein algebraisch abgeschlossener Körper ist, denn dann gibt es keine nicht-trivialen Divisionsalgebren.

2. Für einen endlichen Körper $k$ gilt $Br(k) = 0$. Insbesondere ist jeder endliche Divisionsring kommutativ (Wedderburnsches Theorem).

3. Es gilt $Br(\mathbb{R}) \cong \mathbb{Z}_2$. Ein Repräsentant des Erzeugers sind die Quaternionen $\mathbb{H}$. In der Tat gilt $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M(4 \times 4, \mathbb{R})$.

**Bemerkung 7.4.10.**

1. Für jede Körpererweiterung $K/k$ gibt es einen Homomorphismus, der durch Skalarenerweiterung gegeben ist:
$$\begin{array}{rcl} Br(k) & \to & Br(K) \\ {[S]} & \mapsto & [S_K] := [S \otimes_k K] \end{array}$$

2. Die relative Brauergruppe ist
$$Br(K/k) = \ker(Br(k) \to Br(K))$$
also die Menge endlich-dimensionalen zentralen Divisionsalgebren über $k$, die über $K$ zerfallen.

3. Man kann zeigen, dass für jede Divisionsalgebra $D$ mit Zentrum $k$ und $\dim_k D = n^2$, es eine endliche Galois-Erweiterung $K/k$ gibt, so dass $D$ über $K$ zerfällt.

4. Folglich ist $Br(k) = \cup Br(K/k)$, wobei $K$ über alle endlichen Galois-Erweiterungen von $k$ läuft.

5. Es gilt der folgende Isomorphismus von Gruppen
$$Br(K/k) = H^2(\mathrm{Gal}(K/k), K^*)$$
Wir bemerken hier, dass für einen 2-Kozykel $a_{\sigma,\tau}$ mit $\sigma, \tau \in G := \mathrm{Gal}(K/k)$ der über $G$ frei erzeugte $K$-Vektorraum mit Multiplikation
$$(\alpha e_\sigma) \cdot (\beta e_\tau) := \alpha\sigma(\beta) a_{\sigma,\tau} e_{\sigma\tau}$$
eine zentral einfache Algebra ist.

Sei $S$ eine zentral einfache Algebra und $K$ ein Körper, über dem $S$ zerfällt.. Man beobachtet zunächst, dass für jedes $\sigma \in G$ es $x_\sigma \in S$ gibt mit

$$\sigma(a) = x_\sigma \cdot a \cdot x_\sigma^{-1} \ ,$$

wobei die $x_\sigma$ bis auf Faktoren in $K$ eindeutig sind. Daher gibt es eine Funktion $a : G \times G \to K^*$ mit

$$x_\sigma x_\tau = a(\sigma, \tau) x_{\sigma\tau} \ .$$

Aus der Assoziativität der Multiplikation der $x_\sigma$

$$x_\rho a(\sigma, \tau) \cdot x_{\sigma\tau} = a(\rho, \sigma) x_{\rho\sigma} \cdot x_\tau$$

und somit

$$\rho(a(\rho, \sigma)) a(\rho, \sigma\tau) x_{\rho\sigma\tau} = a(\rho, \sigma) a(\rho\sigma, \tau) x_{\rho\sigma\tau}$$

folgt, dass $a$ die Gleichung (13) erfüllt, also eine Klasse in $H^2(G, K^*)$ definiert. Man zeigt dann noch, dass die Familie $(x_\sigma)_{\sigma \in G}$ eine $K$-Basis von $S$ bildet.

# A Das Zornsche Lemma

Sei $S$ eine Menge. Wir erinnern an die folgenden Begriffe und Resultate der Mengenlehre:

(i) Eine partielle Ordnung auf $S$ ist eine Relation $x \leq y$ mit den folgenden Eigenschaften:

$$x \leq x \qquad \text{Reflexivität}$$

$$x \leq y \ \wedge \ y \leq z \ \Rightarrow \ x \leq z \qquad \text{Transitivität}$$

$$x \leq y \ \wedge \ y \leq x \ \Rightarrow \ x = y \qquad \text{Antisymmetrie}\,.$$

(ii) Eine Totalordnung auf $S$ ist eine partielle Ordnung, für die je zwei Elemente vergleichbar sind:

$$x, y \in S \quad \Rightarrow \quad x \leq y \quad \text{oder} \quad y \leq x\,.$$

(iii) Sei $S$ partiell geordnet, $T \subset S$ Teilmenge.

Ein Element $b \in S$ heißt eine obere Schranke der Teilmenge $T$, falls

$$x \leq b \quad \text{für alle} \quad x \in T\,.$$

(iv) Sei $S$ partiell geordnet. Ein Element $m \in S$ heißt ein maximales Element, falls

$$m \leq x \quad \Rightarrow \quad m = x\,.$$

Das maximale Element muss nicht eindeutig sein. Als Beispiel betrachte die Menge der Ideale des Rings $\mathbb{Z}$ mit Teilordnung durch Inklusion. In ihr sind alle Primideale $(p)$ mit $p$ Primzahl maximal.

(v) Eine partiell geordnete Menge $S$ heißt induktiv geordnet, falls jede nicht–leere, total geordnete Teilmenge von $S$ eine obere Schranke besitzt.

(vi) Zornsches Lemma Sei $S$ eine nicht–leere, induktiv geordnete Menge. Dann besitzt $S$ maximale Elemente.

# Index