

Höhere Algebra: Darstellungstheorie und homologische Algebra

Wintersemester 2010/11

Christoph Schweigert

Universität Hamburg

Fachbereich Mathematik

Bereich Algebra und Zahlentheorie

(Stand: 2.2.2011)

Inhaltsverzeichnis

1	Moduln über Ringen	1
1.1	Grundlegende Definitionen	1
1.2	Operationen auf Moduln, das Tensorprodukt	14
1.3	Freie Moduln	21
1.4	Projektive, flache, teilbare und injektive Moduln	25
1.5	Einfache Moduln und Kompositionsreihen	33
2	Kategorien, Funktoren und natürliche Transformationen	40
2.1	Kategorien	40
2.2	Universelle Eigenschaften und adjungierte Funktoren	45
2.3	Abelsche Kategorien	55
2.4	Freie und kofreie Moduln	61
2.5	Pullback und Pushout	63
3	Moduln über Hauptidealringen	67
3.1	Untermuldn und Morphismen von Moduln über Hauptidealringen	67
3.2	Klassifikation von Moduln über Hauptidealringen	72
4	Darstellungstheorie	77
4.1	Halbeinfache Ringe und Kategorien	77
4.2	Strukturtheorie halbeinfacher Ringe	84
4.3	Fouriertransformation für Gruppen	87
4.4	Charaktere	91
5	Artinsche und Noethersche Moduln	101
5.1	Noethersche Moduln	101
5.2	Artinsche Moduln	105
6	Auflösungen und abgeleitete Funktoren	108
6.1	Projektive und injektive Auflösungen	109
6.2	Homologie und Homotopie	111
6.3	Das Fundamentallemma der homologischen Algebra	114
6.4	Die lange exakte Sequenz	117
6.5	Tor und Ext	121
6.6	Symmetrie von Tor und Doppelkomplexe	123
6.7	Erweiterungen von Moduln	127

7	Gruppenkohomologie	132
7.1	Definition und Beispiele	132
7.2	Funktorialität	135
7.3	Die Bar-Auflösung	137
7.4	Gruppenkohomologie und Gruppenerweiterungen	139
A	Das Zornsche Lemma	142

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 Stammach: 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.

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 schweigert@math.uni-hamburg.de! Herrn Thomas Nikolaus danke ich für zahlreiche Hinweise zum Skript, Diskussionen und Mitarbeit an den Musterlösungen. Den Hamburger Studierenden Pascal Gollin, Johannes Lederich, David Lindemann, Nils Matthes, Christoph Nehring und Cora Welsch 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

$$\begin{aligned} R \times R &\rightarrow R \\ (x, y) &\mapsto xy \equiv x \cdot y, \end{aligned}$$

genannt Multiplikation, für die das Assoziativgesetz

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

und zwei Distributivgesetze gelten:

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

für alle $x, x_1, x_2, y, y_1, y_2 \in R$. Man beachte, dass (M, \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 $R \rightarrow S$ eine Abbildung $f : R \rightarrow S$, 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 Ringmorphisamen

$$f(1_R) = 1_S.$$

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

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. 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.
5. 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 dies wegen $f(n) = \underbrace{f(1 + \dots + 1)}_{n\text{-mal}} = \underbrace{f(1) + \dots + f(1)}_{n\text{-mal}}$ den Ringhomomorphismus eindeutig fest.
6. 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 $f : R \rightarrow \{0\}$

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

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

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

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

Die ersten beiden Gleichungen besagen, dass die Skalarmultiplikation bilinear (eigentlich besser: biadditiv) ist. Die dritte Gleichung ist ein gemischtes Assoziativitätsgesetz. Im Falle unitärer Ringe 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 $f : M \rightarrow N$ einen Modulhomomorphismus, wenn sie mit Addition und Skalarmultiplikation verträglich ist:

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

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

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

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

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

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

Im Falle unitärer Ringe fordern wir zusätzlich

$$\mu(m, 1) = m \Leftrightarrow m.1 = m$$

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, μ) als auch eines S -Rechtsmoduls $(M, \tilde{\mu})$ trägt, so dass gilt

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

für alle $m \in M, \alpha \in R, \beta \in S$. 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

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

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 $\varphi_1, \varphi_2 \in \text{Hom}(M, N)$ erklärt man wie im Fall von Vektorräumen durch die Summe der Bildwerte:

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

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

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

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. Ist der Ring 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 ist $\text{Hom}_R(M, N)$ stets eine abelsche Gruppe. Ist R kommutativ, so ist $\text{Hom}_R(M, N)$ 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^{opp} den opponierten Ring : 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, μ) wird durch

$$\begin{aligned} \mu^{\text{opp}} : R^{\text{opp}} \times M &\rightarrow M \\ (r, m) &\mapsto m.r := \mu(m, r) \end{aligned}$$

zum R^{opp} -Linksmodul. Umgekehrt liefert so jeder R^{opp} -Linksmodul einen R -Rechtsmodul.

2. Sind R, S Ringe und ist $f : R \rightarrow S$ 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 Antihomomorphismus. Ein Antihomomorphismus ist also ein Homomorphismus von R^{opp} nach S oder, äquivalenterweise, ein Homomorphismus von R nach S^{opp} . Die Ringe R und R^{opp} sind also stets anti-isomorph.

3. Ein Ring R ist genau dann kommutativ, wenn die Identität ein Isomorphismus von R nach R^{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. 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 Antisomorphismus, 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:

Definition 1.1.7

1. Sei R ein kommutativer Ring. Eine (assoziative) R -Algebra 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 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 $\Phi : R \rightarrow A$ 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 $\Phi(r) = r \cdot 1_A$ und finden

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

Ist umgekehrt der Ringhomomorphismus Φ gegeben, so definieren wir eine R -Modulstruktur auf A durch

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

die in der Tat R -bilinear ist:

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

Beispiele 1.1.9.

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

$$\mathbb{Z} \times G \rightarrow G$$

$$(n, x) \mapsto nx = \begin{cases} \underbrace{x + \dots + x}_{n\text{-mal}} & n > 0 \\ 0 & n = 0 \\ -|n|x & n < 0. \end{cases}$$

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

$$M \rightarrow \text{Hom}_R(R, M)$$

$$m \mapsto (\varphi_m : r \mapsto rm)$$

ein Isomorphismus von abelschen Gruppen. Ist der Ring R kommutativ, so ist die Abbildung wegen

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

sogar ein Isomorphismus von R -Moduln. Sein Inverses ordnet einem Homomorphismus $\varphi \in \text{Hom}_R(R, M)$ sein Bild $\varphi(1)$ 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 $\text{End}(M)$ einen Ring, den Endomorphismenring. Die Addition in diesem Ring ist die Addition von Abbildungen 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 $\varphi : R \rightarrow \text{End}(M)$ ein Ringhomomorphismus, so wird durch die Vorschrift

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

M zum R -Modul.

(ii) Ist M ein R -Modul, so liefert die Abbildung

$$\begin{aligned} \varphi : R &\rightarrow \text{Abb}(M, M) \\ r &\mapsto \varphi(r) \quad \text{mit} \quad \varphi(r)m = rm \end{aligned}$$

einen Ringhomomorphismus. Er heißt auch die Strukturabbildung oder Darstellungsabbildung des Moduls.

Da es für jeden (unitären) Ring E nach Beispiel 1.1.2 nur einen (unitären) Ringhomomorphismus $\mathbb{Z} \rightarrow E$ 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. Eine R -Algebra A mit Eins heißt Polynomring (korrekter wäre: Polynomialalgebra) in der Unbestimmten X über K , wenn X ein Element von A ist und jedes Element $f \in A$ sich eindeutig in der Gestalt

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

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

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

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 Polynomialalgebra immer kommutativ ist. Die Elemente einer Polynomialalgebra nennen wir auch Polynome.

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

Satz 1.1.12. [Universelle Eigenschaft der Polynomialalgebra]

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 $\varphi_s : A \rightarrow S$ mit $\varphi_s(X) = s$.

Beweis.

- Eindeutigkeit: Da jedes Element $f \in A$ eine eindeutige Darstellung

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

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

□

Bemerkungen 1.1.13.

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

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

2. Im Spezialfall des Polynomrings selbst, $S = A$, und $s = X$ 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 gibt also eine Funktion $R \rightarrow R$. Man hat einen Ringhomomorphismus

$$\begin{aligned} A &\rightarrow \text{Abb}(R, R), \\ f &\mapsto \tilde{f} \end{aligned}$$

den Auswertehomomorphismus. 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, 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

$$\begin{aligned} \Phi : A &\rightarrow A' \quad \text{und} \quad \Psi : A' \rightarrow A \\ \text{mit } \Phi(X) &= X' \quad \text{und} \quad \Psi(X') = X. \end{aligned}$$

Dann sind

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

Algebrenhomomorphismen mit

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

Aus der Eindeutigkeitsaussage in Satz 1.1.12 folgt

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

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 man 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 die Struktur eines K -Vektorraums. Die Multiplikation mit X ist eine K -lineare Abbildung $M \rightarrow M$.
- (ii) Ist M ein K -Vektorraum und $A : M \rightarrow M$ eine K -lineare Abbildung, so versieht die Vorschrift

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

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 Moduln über einem Ring einen einheitlichen Rahmen für den Begriff der abelschen Gruppe und eines Vektorraums mit einem Endomorphismus bietet.

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

Definition 1.1.16

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

$$f : G \rightarrow K,$$

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

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

schreiben, wobei δ_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 δ_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):

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

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.

Man hat einen Ringhomomorphismus

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

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

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

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, ρ) , bestehend aus einem K -Vektorraum V und einem Gruppenhomomorphismus ρ in die invertierbaren K -linearen Abbildungen von V ,

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

In Anwendungen ist der Vektorraum V z.B. der Raum der Lösungen einer linearen Differentialgleichung oder der Raum der Zustände eines 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, ρ) , schreiben wir auch ρ_V für ρ .
- (ii) Ist (V, ρ) eine Darstellung von G über K , so ist die Abbildung

$$\begin{aligned} G \times V &\rightarrow V \\ (g, v) &\mapsto \rho(g)v \end{aligned}$$

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

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

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

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

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

eine Darstellung $\rho : G \rightarrow \text{GL}(V)$.

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

- (iv) Jeder Vektorraum V trägt eine Darstellung seiner Automorphismengruppe $\text{GL}(V)$ durch $\rho = \text{id}_{\text{GL}(V)}$.
- (v) Jeder Vektorraum V wird Darstellung einer beliebigen Gruppe G durch die triviale Operation $\rho(g) = \text{id}_V$ für alle $g \in G$.
- (vi) Ist L/K eine Körpererweiterung, so ist L , aufgefasst als K -Vektorraum eine Darstellung der Galoisgruppe $\text{Gal}(L/K)$ über K .
- (vii) Eine Darstellung (V, ρ) der Gruppe \mathbb{Z} angeben heißt, einen Automorphismus $A \in \text{GL}(V)$ 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 $A : V \rightarrow V$, für den $A^2 = \text{id}_V$ gilt. Konkret heißt dies, wenn die Charakteristik des Körpers K ungleich zwei ist, dass V direkte Summe der Eigenräume von A zu den Eigenwerten ± 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

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

sind dies Eigenvektoren von A zu den beiden Eigenwerten ± 1 .

Hat dagegen der zu Grunde liegende Körper Charakteristik 2, so gibt es nur den Eigenwert 1. Wegen $A^2 = \text{id}_V$ 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

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

durch Einschränkung der Operation von $K[G]$ zu Operationen von K und G einerseits und durch offensichtliche Ausdehnung auf $K[G]$ andererseits.

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 $f : V \rightarrow W$, 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 Unterm modul von M , falls die Skalarmultiplikation von M auf U definiert ist, d.h. wenn aus $m \in U$ und $r \in R$ folgt, dass $r \cdot m \in U$ liegt.

Bemerkung 1.1.22.

- (i) Die Untergruppen einer abelschen Gruppe sind genau die \mathbb{Z} -Unterm oduln.
- (ii) Fasst man den Ring R als Modul über sich selbst auf, so sind die R -Unterm oduln von R gerade die Ideale von R . Genauer gesagt sind die R -Links-Unterm oduln die Linksideale, die R -Rechts-Unterm oduln die Rechtsideale und die R -Bi-Unterm oduln 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, ρ) als $K[G]$ -Modul, so entsprechen die Unterdarstellungen den $K[G]$ -Unterm oduln.
- (iv) Bild und Urbild eines Unterm oduls unter einem Modulhomomorphismus sind wieder Unterm oduln. Insbesondere sind Bild und Kern eines Modulhomomorphismus Unterm oduln.
- (v) Ist U ein Unterm odul von M , so ist U als Untergruppe der abelschen Gruppe Normalteiler, so dass M/U eine abelsche Gruppe ist.

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

$$\begin{aligned} R \times M/U &\rightarrow M/U \\ (\alpha, x + U) &\mapsto \alpha x + U \end{aligned}$$

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

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

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 Ideal ist, und somit $r(\alpha m) = (r\alpha)m \in \mathfrak{a}M$. Nach Bemerkung (v) ist dann $M/\mathfrak{a}M$ ein R -Modul. Die Skalarmultiplikation

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

ist 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 Ideal für jedes $n \in \mathbb{Z}$ und die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist ein \mathbb{Z} -Modul mit Skalarmultiplikation

$$n \cdot \bar{m} = \overline{nm}$$

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

Lemma 1.1.23 (Restriktion der Skalare/Pullback).

Ist $\varphi : R \rightarrow S$ ein Ringhomomorphismus, so wird jeder S -Modul (M, μ) (insbesondere auch S selbst) ein R -Modul durch $\mu \circ (\varphi \times \text{id}_M)$, d.h. durch

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

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

Zum Beispiel sei $\mathfrak{a} \subset R$ ein beidseitiges Ideal von R , und $\text{can} : R \rightarrow R/\mathfrak{a}$, 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 $A \subseteq M$ Teilmenge eines R -Moduls M . Dann bezeichnet

$$\langle A \rangle = \left\{ \sum_{\text{endl}} \alpha_i a_i \mid \alpha_i \in R, a_i \in A \right\}$$

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 von 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 $f : M \rightarrow N$ ein Modulhomomorphismus, so gibt es einen kanonischen Isomorphismus

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

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

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

mit $U + V = \{u + v, u \in U \text{ und } v \in V\}$. Man bestimme hierzu den Kern der Abbildung

$$\begin{aligned} U + V &\rightarrow U/U \cap V \\ u + v &\mapsto u + (U \cap V) \end{aligned}$$

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

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

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

Definition 1.1.27

(i) Sei U ein R -Untermodul eines R -Moduls M . Dann heißt

$$\text{Ann}(U) = \{\alpha \in R \mid \alpha u = 0 \text{ für alle } u \in U\}$$

der Annulator des Untermoduls U . Dies ist ein (Links-)Ideal von R . Der Annulator eines Elementes $x \in M$ ist definiert als

$$\text{Ann}(x) = \{\alpha \in R \mid \alpha x = 0\}.$$

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

$$\begin{aligned} R/\text{Ann}(x) &\xrightarrow{\sim} Rx \\ \bar{\alpha} &\mapsto \alpha x \end{aligned}$$

(ii) Ein Modul M heißt treu, falls $\text{Ann } M = (0)$ ist. Wir sollten gleich bemerken, dass eine Darstellung auf einem K -Vektorraum V treu heißt, wenn der Gruppenhomomorphismus $\rho : G \rightarrow \text{GL}(V)$ 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 Darstellung, aber der zugehörige $K[G]$ -Modul ist nicht frei, da $e + g$ im Annulator liegt.

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

(iv) Ein Modul M heißt torsionsfrei, falls $\text{Tor } M = (0)$ ist.

In einem torsionsfreien Modul verschwinden alle Annulatoren, insbesondere ist $\text{Ann}(M) = (0)$, 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 er unitär ist. Aber das Element $\bar{2}$ liegt im Annulator von $\bar{3}$, so dass $\bar{3}$ 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 $\text{Tor } M$ ein Untermodul von M und $M/\text{Tor } M$ ist torsionsfreier R -Modul.

Beweis.

- Ist $x \in \text{Tor}(M)$ ein Torsionselement, $\beta \in R$, so finden wir ein von Null verschiedenes $\alpha \in \text{Ann}(x)$. Dann gilt aber $\alpha(\beta x) = (\alpha\beta)x = \beta(\alpha x) = 0$. Damit ist aber auch $\beta x \in \text{Tor } M$.
- Seien nun zwei Torsionselemente vorgegeben, $x, y \in \text{Tor } M$. 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 $x + y \in \text{Tor } M$.
- Schließlich sei $x + \text{Tor } M \in M/\text{Tor } M$ ein Torsionselement. Wir finden wieder $\alpha \in R \setminus \{0\}$, so dass $\alpha(x + \text{Tor } M) = 0$. Da dann aber $\alpha x \in \text{Tor } M$ liegt, gibt es $\beta \in R \setminus \{0\}$ mit $\beta\alpha x = 0$. Da R integer sein sollte, ist auch $\beta\alpha \neq 0$, also $x \in \text{Tor } M$. Also ist der Quotient $M/\text{Tor } M$ 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 Produkt

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

und die direkte Summe

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

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 für jedes natürliche 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 $\prod_{i=1}^s M_i = M_1 \times M_2 \times \dots \times M_s$ und $M_1 \oplus M_2 \oplus \dots \oplus M_s$ 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 i_λ das Element $m \in M_\lambda$ auf das Element in der direkten Summe ab, dessen Einträge außer in der Komponente λ alle Null sind. Die Abbildung pr_λ projiziert auf die Komponente λ . Beide Abbildungen sind Homomorphismen von Moduln.

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

$$\begin{array}{ccc}
 \text{Hom}_R(\bigoplus_{\mu \in \Lambda} M_\mu, M) & \longrightarrow & \prod_{\mu \in \Lambda} \text{Hom}_R(M_\mu, M) \\
 f & \mapsto & (f \circ i_\mu)_{\mu \in \Lambda} \\
 \\
 \text{Hom}_R\left(M, \prod_{\mu \in \Lambda} M_\mu\right) & \longrightarrow & \prod_{\mu \in \Lambda} \text{Hom}_R(M, M_\mu) \\
 f & \mapsto & (pr_\mu \circ f)_{\mu \in \Lambda}
 \end{array}$$

Isomorphismen von Moduln.

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

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

auch als ihre Summe.

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

$$s : \bigoplus_{\lambda \in \Lambda} U_\lambda \rightarrow M$$

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 $\bigoplus_{\lambda \in \Lambda} U_\lambda$ und sprechen von einer inneren direkten Summe. Die Injektivität von s heißt natürlich gerade, dass wir jedes Element der inneren direkten Summe in eindeutiger Weise als Summe von Elementen der Untermoduln U_λ schreiben können.

- (v) Gegeben zwei Darstellungen (V, ρ_V) und (W, ρ_W) einer Gruppe G über einem Körper K definieren wir die direkte Summe 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^{opp} -Modul und N ein R -Modul. Das Tensorprodukt $M \otimes_R N$ 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

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

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

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

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^{opp} -Moduln und N sei ein R -Modul. Dann gilt:

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. $\bigoplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N) \cong (\bigoplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N$ 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^{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

$$\begin{aligned} M &\rightarrow M \otimes_R R \\ m &\mapsto m \otimes 1 , \end{aligned}$$

der die Umkehrabbildung

$$\begin{aligned} M \otimes_R R &\rightarrow M \\ m \otimes r &\mapsto m.r \end{aligned}$$

hat und daher ein Isomorphismus ist.

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

$$\Phi : \bigoplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N) \rightarrow (\bigoplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N$$

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 $(\bigoplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N$ jedes Element von der Form einer endlichen Summe $x = \sum_\lambda \iota_\lambda(m_\lambda) \otimes n$ ist. Die Umkehrabbildung Ψ ist dann gegeben durch $\Psi(\iota_\lambda(m_\lambda) \otimes n) = \iota_\lambda(m_\lambda \otimes n)$.

Die S^{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 $R^n := R \oplus R \oplus \dots \oplus R$ 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 . 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

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

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

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

das Tensorprodukt ist also eine zyklische Gruppe. Der Gruppenhomomorphismus

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

ist wohldefiniert, weil g ein Teiler von n und m ist. Offenbar ist Φ ein surjektiver Gruppenhomomorphismus. Ist $\Phi(a(1 \otimes 1)) = 0$, so ist a ein Vielfaches des ggT g . Der euklidische Algorithmus liefert für jedes Vielfache des ggT 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 Φ auch injektiv.

- (iv) Tensorieren mit \mathbb{Q} über \mathbb{Z} lässt Torsionselemente einer abelschen Gruppe verschwinden. In der Tat ist $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 gilt $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$, 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 $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ und somit $\prod_{n \geq 1} \mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. 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 $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$.

Ist R sogar ein kommutativer Ring, so kann man das Tensorprodukt von zwei Linksmoduln M, N erklären, indem man N 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

$$\begin{aligned} \alpha_{M,N,P} : M \otimes (N \otimes P) &\rightarrow (M \otimes N) \otimes P \\ m \otimes (n \otimes p) &\mapsto (m \otimes n) \otimes p \end{aligned}$$

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 ein R -Modul ist.

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^{opp} -Modul, N ein R -Modul und T eine abelsche Gruppe. Eine Abbildung $f : M \times N \rightarrow T$ heißt R -bilinear, wenn sie die folgenden Eigenschaften erfüllt:

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

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

Die Abbildung

$$\begin{aligned} M \times N &\rightarrow M \otimes_R N \\ (m, n) &\mapsto m \otimes n \end{aligned}$$

ist per Definition R -bilinear.

Satz 1.2.9 (Universelle Eigenschaft des Tensorprodukts).

Sei R ein Ring, M ein R^{opp} -Modul, N ein R -Modul und T eine abelsche Gruppe.

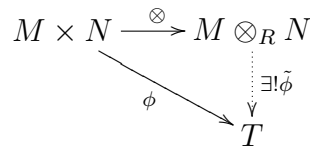
(i) Dann vermittelt die R -bilineare Abbildung

$$\begin{aligned} \otimes : M \times N &\rightarrow M \otimes N \\ (m, n) &\mapsto m \otimes n \end{aligned}$$

einen Isomorphismus von abelschen Gruppen

$$\begin{aligned} \text{Hom}_{\mathbb{Z}}(M \otimes_R N, T) &\rightarrow \text{Bil}_R(M, N, T) \\ \tilde{\phi} &\mapsto \tilde{\phi} \circ \otimes . \end{aligned}$$

Das heißt, dass jede R -bilineare Abbildung $\phi : M \times N \rightarrow T$ eindeutig durch einen Morphismus abelscher Gruppen $\tilde{\phi} : M \otimes_R N \rightarrow T$ beschrieben werden kann. Als kommutierendes Diagramm:



(ii) Auf der abelschen Gruppe $\text{Hom}_{\mathbb{Z}}(N, T)$ ist eine natürliche R^{opp} -Modulstruktur definiert durch $(f.r)(n) := f(r.n)$ für $f := N \rightarrow T$, $r \in R$ 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 $\text{Hom}_{\mathbb{Z}}(M, T)$ eine natürliche R -Modulstruktur definiert durch $(r.g)(m) := g(m.r)$ für $g := M \rightarrow T$, $r \in R$ und $m \in M$.

Mit diesen R -Modulstrukturen gelten die Isomorphismen

$$\text{Hom}_R(N, \text{Hom}_{\mathbb{Z}}(M, T)) \cong \text{Hom}_{\mathbb{Z}}(M \otimes_R N, T) \cong \text{Hom}_{R^{\text{opp}}}(M, \text{Hom}_{\mathbb{Z}}(N, T)).$$

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 $M \times N \rightarrow T$ beschreiben. (Übung) \square

Bemerkung 1.2.10.

Aus der universellen Eigenschaft des Tensorprodukts folgt die folgende Eindeutigkeitsaussage. Sei T eine abelsche Gruppe und $\tau : M \times N \rightarrow T$ eine R -bilineare Abbildung, so dass jede bilineare Abbildung $\phi : M \times N \rightarrow T'$ sich vermittels τ eindeutig durch einen Homomorphismus abelscher Gruppen $\Phi^\tau : T \rightarrow T'$ ausdrücken lässt:

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau} & T \\ & \searrow \phi & \downarrow \exists! \phi^\tau \\ & & T' \end{array}$$

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

$$\begin{array}{ccccc} & & & & T \\ & & & & \downarrow \exists! \Psi_1 \\ M \times N & \xrightarrow{\tau} & & & M \otimes_R N \\ & \searrow \otimes & & & \downarrow \exists! \Psi_2 \\ & & & & T \end{array}$$

Die vertikale Abbildung $T \rightarrow T$ rechts ist wegen der universellen Eigenschaft von (T, τ) das eindeutige Φ^τ für $\Phi = \tau$. Sie leistet dasselbe wie die Identität, muss also gleich der Identität sein, $\Psi_2 \circ \Psi_1 = \text{id}_T$. Durch Vertauschen der Rollen von \otimes und τ erhält man auch $\Psi_1 \circ \Psi_2 = \text{id}_{M \otimes_R N}$, so dass sowohl Ψ_1 und Ψ_2 Isomorphismen sind.

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

Betrachtung 1.2.11.

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

Wir betrachten das folgende Diagramm:

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_R N \\ \downarrow \Phi \times \Psi & & \downarrow \Phi \otimes \Psi \\ M' \times N' & \xrightarrow{\otimes} & M' \otimes_R N' \end{array}$$

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:

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

(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

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

die universelle Eigenschaft eines Produkts: für jeden Ring S ist

$$\begin{aligned}\text{Hom}(S, \prod_{\lambda \in \Lambda} R_{\lambda}) & \rightarrow \prod_{\lambda \in \Lambda} \text{Hom}(S, R_{\lambda}) \\ f & \mapsto (pr_{\mu} \circ f)_{\mu \in \Lambda}\end{aligned}$$

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

$$\begin{aligned}\iota_1 : R_1 & \rightarrow R_1 \otimes_{\mathbb{Z}} R_2 & \iota_2 : R_2 & \rightarrow R_1 \otimes_{\mathbb{Z}} R_2 \\ r_1 & \mapsto r_1 \otimes 1 & r_2 & \mapsto 1 \otimes r_2\end{aligned}$$

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

$$\begin{aligned}\text{Hom}(R_1 \otimes_{\mathbb{Z}} R_2, S) & \rightarrow \text{Hom}(R_1, S) \times \text{Hom}(R_2, S) \\ f & \mapsto (f \circ \iota_1, f \circ \iota_2)\end{aligned}$$

ein Isomorphismus von Mengen. Man sagt dann, das Tensorprodukt sei ein Koproduct 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 verschieden sind, folgt, dass $r_\lambda = 0$ für alle λ .

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 Moduln, die nicht frei sind: sei $R = \mathbb{Z}$ und $M = \mathbb{Z}_2$. Wegen $2 \cdot \bar{1} = \bar{0}$ ist $\{\bar{1}\}$ nicht linear unabhängig und wegen $n\bar{0} = \bar{0}$ ist $\{\bar{0}\}$ 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 Λ ist der Modul

$$R\Lambda := \{f : \Lambda \rightarrow R \mid f(\lambda) = 0 \text{ für fast alle } \lambda\}$$

frei, denn die Abbildungen, die an einer Stelle den Wert 1 annehmen und sonst den Wert Null bilden eine Basis. Man nennt ihn den von der Menge Λ 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 $R\Lambda \rightarrow M$ mit $(r_\lambda) \mapsto \sum r_\lambda m_\lambda$ ein Isomorphismus ist.

4. Ein R -Modul M ist frei über S genau dann, wenn

$$M \cong \bigoplus_{s \in S} R_s.$$

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

Beweis.

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

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

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

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

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

Denn sei $M = \langle x_1, \dots, x_n \rangle$ und S eine Basis, so ist jedes x_i eindeutig darstellbar

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

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, \dots, M_m und N_1, \dots, N_n über einem Ring R gegeben. Dann folgt aus der universellen Eigenschaft der direkten Summe bzw. des direkten Produkts eine natürliche Identifikation

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

Schreiben wir also die Elemente der direkten Summe $M_1 \oplus \dots \oplus M_m$ 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 $\text{Hom}_R(M_i, N_j)$ 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 $\text{Hom}_R(R, R) \cong R$ 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 von M . Sie kann, aber muss nicht unbedingt endlich sein. Insbesondere gilt im Falle endlicher Mächtigkeit

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

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 $M/\mathfrak{m}M$ ein Vektorraum über K .

Sei S eine Basis von 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. \square

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 \mathbb{N} . Jeder Isomorphismus von Mengen $\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ liefert einen Isomorphismus von Vektorräumen $V \rightarrow V \oplus V$. Sei $R := \text{End}_K(V)$. Dann liefert ein solcher Isomorphismus einen Isomorphismus von R -Moduln

$$R = \text{End}_K(V) \rightarrow \text{Hom}_K(V \oplus V, V) \cong R \oplus R .$$

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 :

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

Die Abbildung

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

ist dann ein surjektiver R -Modulhomomorphismus. □

Satz 1.3.6.

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

$$g : F \rightarrow M$$

mit $f \circ g = \text{id}_F$, und es gilt $M \cong \ker f \oplus g(F)$. 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 $m_s \in M$ für jedes $s \in S$ und definiere

$$g : F \rightarrow M$$

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

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

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

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

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

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

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

Offenbar liegt $gf(x) \in g(F)$, außerdem gilt

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

Also haben wir die Darstellung von M als Summe von Untermoduln, $M = \ker f + g(F)$. Diese Summe ist direkt: Sei $x \in \ker f \cap g(F)$. 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

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 "kategorial". 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.

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 $g : M/N \rightarrow M$ mit $f \circ g = \text{id}_{M/N}$ 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 $f|_{N'}$ surjektiv. Da außerdem gilt $\ker f|_{N'} = N' \cap N = 0$, ist $f|_{N'}$ ein Isomorphismus von N' nach M/N . \square

1.4 Projektive, flache, teilbare und injektive Moduln

Definition 1.4.1

Sei R ein Ring. Eine Folge von R -Moduln und Modulmorphismen

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

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

Bemerkungen 1.4.2.

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

- (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 $M \rightarrow N$ 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

$$0 \rightarrow M' \xrightarrow{\iota} M \xrightarrow{p} M'' \rightarrow 0 .$$

Die Exaktheit bei M' heißt, dass ι injektiv ist. Die Exaktheit bei M'' heißt, dass p surjektiv ist. Die Exaktheit bei M kann äquivalent auch durch die beiden folgenden Isomorphismen ausgedrückt werden:

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

Satz 1.4.3.

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

1. ι hat eine Retraktion, d.h. es gibt einen R -Modulmorphismus $\pi : M \rightarrow M'$ mit der Eigenschaft $\pi \circ \iota = \text{id}_{M'}$.
2. p hat einen Schnitt, d.h. es gibt einen R -Modulmorphismus $s : M'' \rightarrow M$ mit der Eigenschaft $p \circ s = \text{id}_{M''}$.
3. Es gibt einen Isomorphismus $\phi : M \rightarrow M' \oplus M''$ von R -Moduln, so dass $\phi \circ \iota = \iota_1$ und $\text{pr}_2 \circ \phi = p$ gilt.

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\iota} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \parallel & & \downarrow \phi & & \parallel & & \\ 0 & \longrightarrow & M' & \xrightarrow{\iota_1} & M' \oplus M'' & \xrightarrow{\text{pr}_2} & M'' & \longrightarrow & 0 \end{array}$$

bei dem in der unteren Zeile die Injektion ι_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 exakten Sequenz, die eine der drei äquivalenten Eigenschaften aus Satz 1.4.3 erfüllt, sagen wir, sie spaltet oder zerfällt. (Englisch: splits).

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

Lemma 1.4.5.

Sei M ein R -Modul und

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

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

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

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

$$\begin{aligned} \iota_* : \text{Hom}_R(M, T') &\rightarrow \text{Hom}_R(M, T) \\ \phi &\mapsto \iota \circ \phi \end{aligned}$$

Beweis.

Da $\iota : T' \rightarrow T$ injektiv ist, folgt aus $\iota_*(\phi) = \iota \circ \phi = \iota \circ \phi' = \iota_*(\phi')$, dass $\phi = \phi'$, also die Injektivität von ι_* .

Liegt $\phi \in \text{Hom}(M, T)$ im Bild von ι_* , so gibt es $\phi' \in \text{Hom}(M, T')$ 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 $f(m) \in \ker \pi = \text{Im } \iota$. Finde also für jedes $m \in M$ ein $\phi'(m) \in T'$ mit $\iota \circ \phi'(m) = f(m)$. Da ι injektiv ist, dieses Element von T' sogar eindeutig bestimmt, und daher ist auch ϕ' ein Modulmorphismus. Also $\iota_*\phi' = f$, und $f \in \text{Im } \iota_*$. \square

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

Satz 1.4.6.

Die folgenden Aussagen über einen R -Modul M sind äquivalent:

1. Für jedes Diagramm

$$\begin{array}{ccccc} & & M & & \\ & \swarrow \text{---} & \downarrow & & \\ N_1 & \longrightarrow & N_2 & \longrightarrow & 0 \end{array}$$

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 $M \oplus N$ frei ist.
3. Jede kurze exakte Sequenz der Form

$$0 \rightarrow N' \rightarrow N \rightarrow M \rightarrow 0$$

zerfällt.

4. Für jede kurze exakte Sequenz von Moduln

$$0 \rightarrow T' \rightarrow T \rightarrow T'' \rightarrow 0$$

ist auch die Sequenz von abelschen Gruppen

$$0 \rightarrow \text{Hom}_R(M, T') \rightarrow \text{Hom}_R(M, T) \rightarrow \text{Hom}_R(M, T'') \rightarrow 0$$

exakt.

Die Formulierung dieses Satzes illustriert, dass man es in der homologischen Algebra gern vermeidet, Morphismen Namen zu geben.

Beweis.

1 \Rightarrow 3 Die Spaltung ist gegeben durch die Hochhebung in dem Diagramm

$$\begin{array}{ccccc}
 & & M & & \\
 & \swarrow \text{dotted} & \downarrow \text{id} & & \\
 N & \longrightarrow & M & \longrightarrow & 0
 \end{array}$$

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

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

$$0 \rightarrow \text{Hom}_R(M \oplus N, T') \rightarrow \text{Hom}_R(M \oplus N, T) \rightarrow \text{Hom}_R(M \oplus N, T'') \rightarrow 0$$

exakt. Nach der universellen Eigenschaft der direkten Summe ist diese exakte Sequenz aber gliedweise isomorph zu

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

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 \Rightarrow 1 folgt, indem wir die Surjektivität ausnützen, um eine exakte Sequenz

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

zu bekommen. Dann liefert 4 die exakte Sequenz

$$0 \rightarrow \text{Hom}_R(M, \ker(N_1 \rightarrow N_2)) \rightarrow \text{Hom}_R(M, N_1) \rightarrow \text{Hom}_R(M, N_2) \rightarrow 0$$

der Surjektivitätsaussage genau Aussage 1 ist.

□

Definition 1.4.7

Ein R -Modul, der eine der vier äquivalenten Eigenschaften aus Satz 1.4.6 erfüllt, heißt projektiver Modul.

Beispiele 1.4.8.

1. Freie Moduln sind wegen Satz 1.4.6 (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 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.
3. Beispiele für projektive, nicht freie Moduln über nullteilerfreien Ringen R sind etwas schwieriger zu finden, wenn man nicht auf algebraisch-geometrische Methoden zurückgreifen will.

Sei $\tau := \sqrt{-5}$; betrachte den kommutativen Ring $R = \mathbb{Z}[\tau]$. Sei M das von 2 und $1 + \tau$ erzeugte Ideal, aufgefasst als R -Modul. Zunächst zeigen wir, dass M nicht frei ist. Angenommen, M wäre frei. Wie bei Vektorräumen ist der Rang eines freien Moduls ist 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.) Dann kann der Rang von M höchstens zwei sein. Dann kann der Rang nicht 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 M genau dann frei, wenn es ein Hauptideal ist, also $M = (a)$ für ein $a \in R$ mit $a|2$ und $a|1 + \tau$. Wir zeigen, dass 2 unzerlegbar in R ist. Dazu definiere die Normabbildung $N : R \rightarrow \mathbb{Z}$ 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 $x, y \in \mathbb{Z}$.

Um zu zeigen, dass M dennoch projektiv ist, betrachten wir die durch das Erzeugendensystem gegebene Surjektion

$$p : R \oplus R \rightarrow M \\ (r_1, r_2) \mapsto r_1 2 + r_2 (1 + \tau) .$$

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 direkter Summand im freien Modul $R \oplus R$, daher nach Satz 1.4.6 projektiv.

Satz 1.4.9.

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

1. Dann ist die Sequenz abelscher Gruppen

$$M \otimes_R N' \rightarrow M \otimes_R N \rightarrow M \otimes_R N'' \rightarrow 0$$

immer exakt.

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

$$0 \rightarrow M \otimes_R N' \rightarrow M \otimes_R N \rightarrow M \otimes_R N'' \rightarrow 0$$

exakt.

Man vergleiche die erste Aussage mit der Aussage in Lemma 1.4.5.

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 $N \rightarrow N''$ surjektiv ist, gibt es Urbilder $n_i \in N$. Dann wird das Element $\sum m_i \otimes n_i$ unter $M \otimes_R N \rightarrow M \otimes_R N'$ auf x abgebildet, womit die Surjektivität gezeigt ist.

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

$$Q := \text{coker}(M \otimes_R N' \rightarrow M \otimes_R N) \cong (M \otimes_R N) / \text{Im}(M \otimes_R N' \rightarrow M \otimes_R N).$$

Tensorieren wir die Abbildung $p : N \rightarrow N''$ mit der Identität id_M , so bekommen wir eine Abbildung $M \otimes_R N \rightarrow M \otimes_R N''$. In gleicher Weise bekommen wir eine Abbildung $M \otimes_R N' \rightarrow M \otimes_R N$, deren Bild offenbar im Kern der ersten Abbildung $\text{id}_M \otimes p$ liegt. Daher faktorisiert diese zu einer natürlichen Abbildung

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

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

Wir konstruieren dazu eine Umkehrabbildung $M \otimes_R N'' \rightarrow Q$: 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 $k \in \ker(p) = \text{Im}(\iota)$ und liefert daher die gleiche Klasse im Kokern Q .

Die so definierte Abbildung ist ein Isomorphismus, denn die natürliche Abbildung ist ein $[m \otimes n] \mapsto m \otimes p(n)$ 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 Modul M anwendet. Wegen der Distributivität von \otimes_R und da projektive Moduln direkte Summanden freier Moduln sind, vgl. Satz 1.4.6 (2), dürfen wir annehmen, dass M sogar frei ist, also $M = \oplus_{i \in I} R$. Wiederum wegen der Distributivität kommutiert das Diagramm:

$$\begin{array}{ccc} M \otimes_R N' & \longrightarrow & M \otimes_R N \\ \downarrow \cong & & \downarrow \\ \oplus_{i \in I} N' & \longrightarrow & \oplus_{i \in I} N \end{array}$$

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

□

Wir definieren daher zwei weitere Begriffe für Moduln über einem Ring:

Definition 1.4.10

1. Ein R -Modul M heißt flach, falls Tensorieren $- \otimes_R M$ kurze exakte Sequenzen erhält, oder äquivalent, wenn er das Tensorprodukt mit M die Injektivität von Abbildungen erhält.

2. Ein Modul heißt teilbar, wenn für jedes $0 \neq r \in R$ die Abbildung $M \xrightarrow{r} M$, die durch Skalarmultiplikation mit r gegeben ist, surjektiv ist.

Beispiel 1.4.11.

Vertauscht man im vorgehenden Satz 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 $0 \rightarrow M' \rightarrow M$ injektiv ist, so ist der Kern der zusammengesetzten Abbildung $M' \rightarrow M \rightarrow M \otimes_{\mathbb{Z}} \mathbb{Q}$ mit $M \rightarrow M \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 $M' \rightarrow M$ kann das nur passieren, wenn m' selbst schon ein Torsionselement ist, woraus aber $m' = 0 \in M' \otimes_{\mathbb{Z}} \mathbb{Q}$ folgt.

Andererseits ist \mathbb{Q} aber nicht projektiv über \mathbb{Z} ; andernfalls müsste es in einen freien \mathbb{Z} -Modul 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 $f : T_1 \rightarrow T_2$ von R -Moduln betrachten wir dabei diesmal die Abbildung

$$f^* : \text{Hom}(T_2, N) \rightarrow \text{Hom}(T_1, N) \\ \varphi \mapsto \varphi \circ f$$

Man beachte, die Reihenfolge von T_1 und T_2 in den Hom-Räumen! Der Beweis der folgenden Proposition ist völlig analog zum Beweis von Satz 1.4.6 und wird hier nicht mehr wiederholt

Satz 1.4.12.

Die folgenden Aussagen sind äquivalent für einen R -Modul M :

1. Für jedes Diagramm

$$\begin{array}{ccccc} 0 & \longrightarrow & N_1 & \longrightarrow & N \\ & & \downarrow & \swarrow \text{dotted} & \\ & & M & & \end{array}$$

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

2. Jede kurze exakte Sequenz

$$0 \rightarrow M \rightarrow N_1 \rightarrow N_2 \rightarrow 0$$

zerfällt.

3. Für jede kurze exakte Sequenz

$$0 \rightarrow T' \rightarrow T \rightarrow T'' \rightarrow 0$$

ist auch die Sequenz

$$0 \rightarrow \text{Hom}_R(T'', M) \rightarrow \text{Hom}_R(T, M) \rightarrow \text{Hom}_R(T', M) \rightarrow 0$$

exakt.

Es fehlt noch das Analogon der Charakterisierung projektiver Moduln als direkter Summanden freier Moduln. Wir gehen darauf erst in Abschnitt 2.4 ein.

Definition 1.4.13

Ein Modul, der eine der vorstehenden Eigenschaften erfüllt, heißt injektiver Modul.

Satz 1.4.14 (Satz von Baer).

Ein R -Modul M ist genau dann injektiv, wenn er für jedes Ideal \mathfrak{p} in R und jeden Morphismus $\mathfrak{p} \rightarrow M$ von R -Linksmoduln die Hochhebungseigenschaft hat:

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathfrak{p} & \longrightarrow & R \\ & & \downarrow & \swarrow & \\ & & M & & \end{array}$$

Beweis.

- Ist M injektiv, so folgt die Hochhebungseigenschaft durch Betrachtung der Eigenschaft 1 aus Satz 1.4.12 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 $0 \rightarrow N' \xrightarrow{\iota} N$ ein Monomorphismus von R -Moduln und $f : N' \rightarrow M$ ein beliebiger Morphismus von R -Moduln. Wir müssen im Diagramm

$$\begin{array}{ccccc} 0 & \longrightarrow & N' & \xrightarrow{\iota} & N \\ & & \downarrow f & \swarrow g & \\ & & M & & \end{array}$$

einen 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

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

Sie enthält die Fortsetzung (N', f) , ist also nicht leer. Wir definieren eine partielle Ordnung durch

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

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

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

Nun betrachten wir den Modulmorphismus $\mathfrak{p} \xrightarrow{g_0 \circ n} M = \mathfrak{p} \xrightarrow{\cdot n} K_0 \xrightarrow{g_0} M$. Nach Voraussetzung kann dieser fortgesetzt werden zu einem Modulmorphismus $\tilde{g} : R \rightarrow M$. Sei nun

$$K' = K_0 + Rn \subset N; g'(k + rn) = g_0(k) + \tilde{g}(r).$$

Man beachte, dass g' deswegen wohldefiniert ist, weil \tilde{g} eine Fortsetzung von $g \circ n$ ist, also auf dem Schnitt $\mathfrak{p} = Rn \cap K_0$ mit g_0 übereinstimmt. Damit ist aber $(K', g') > (K_0, g_0)$, ein Widerspruch zur Maximalität von (K, g) .

□

Korollar 1.4.15.

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 hat. Im Hauptidealring R sind alle Ideale von der Form $\mathfrak{p} = (\alpha)$ mit $\alpha \in R$. Betrachte also das Diagramm

$$\begin{array}{ccccc} 0 & \longrightarrow & (\alpha) & \longrightarrow & R \\ & & \downarrow \phi & \swarrow \tilde{\phi} & \\ & & M & & \end{array}$$

Dann ist ϕ festgelegt durch seinen Wert $\phi(\alpha)$ auf dem Erzeuger α des Hauptideals und ebenso $\tilde{\phi}$ durch seinen Wert auf $1 \in R$. Ist M teilbar, so finden wir ein $\tilde{m} \in M$ mit $\alpha \cdot \tilde{m} = \phi(\alpha)$. Wir legen den Morphismus $\tilde{\phi}$ durch den Wert $\tilde{\phi}(1) := \tilde{m}$ auf dem Erzeuger $1 \in R$ fest. Dann gilt für $\alpha \neq 0$ 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 und sind nach dem Satz von Baer 1.4.14 injektiv.

Sei umgekehrt der Modul M injektiv und erfülle somit nach Satz 1.4.12 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 ϕ definiert durch $\phi(\alpha) = m$, finde $\tilde{\phi}$ mit der Hochhebungseigenschaft und setze $\tilde{m} := \tilde{\phi}(1)$. □

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} .

1.5 Einfache Moduln und Kompositionsreihen

Definition 1.5.1

1. Ein Modul M über einem Ring heißt einfach, 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 irreduzibel oder einfach, wenn $V \neq 0$ gilt und 0 und V die einzigen Unterdarstellungen sind.
3. Ein Modul M über einem Ring heißt unzerlegbar, 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 unzerlegbar, 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

$$\begin{aligned} \ker \phi_m : R &\rightarrow M \\ r &\mapsto r.m \end{aligned}$$

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, gilt $\langle x \rangle = M$.

Sei umgekehrt jedes nicht-verschwindende $x \in M$ Erzeuger. Angenommen, $U \subset M$ ist ein 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 von $\ker \phi_m$.

□

Warnung: es gilt aber nicht, dass jeder zyklische Modul einfach ist. Als 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 über einem Körper K auf einem Vektorraum der Dimension 1 sind irreduzibel.
- (ii) Ist $\text{char } K \neq 2$ 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 $\text{char } K = 2$, so ist die triviale eindimensionale Darstellung K irreduzibel und die zweidimensionale Darstellung P unzerlegbar, aber nicht irreduzibel. Jede endlich-dimensionale Darstellung ist isomorph zu

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

Lemma 1.5.4.

Sei R ein Ring, E einfacher R -Modul und M beliebiger R -Modul

- (i) Jeder Homomorphismus $E \rightarrow M$ ist injektiv oder Null. Denn der Kern ist ein Untermodul von E .
- (ii) Jeder Homomorphismus $M \rightarrow E$ ist surjektiv oder Null. Denn das Bild ist ein Untermodul von E .
- (iii) Der Endomorphismenring $\text{End}_R(E)$ 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:

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

Beweis.

Da M nach Annahme einfach ist, gilt insbesondere $M \neq 0$. Jeder Endomorphismus $\varphi \in \text{End}_A(M)$ hat also wenigstens einen Eigenwert λ . Der entsprechende Eigenraum ist als Kern des Homomorphismus von Moduln $\varphi - \lambda \text{id}_M$ ein Untermodul M . Da M einfach sein soll, muss der Kern gleich M sein, also $\varphi = \lambda \text{id}_M$. \square

Bemerkungen 1.5.6.

1. Es ist klar, dass eine analoge Aussage auch für Moduln über einem Ring R gilt, der einen algebraisch abgeschlossenen Körper K als Unterring enthält, wenn der Modul als Vektorraum über K endlich-dimensional ist.
2. Setzt man die Gruppe G als endlich voraus, so ist die Gruppenalgebra $K[G]$ endlich-dimensional über K und somit auch jede irreduzible Darstellung V als Quotient von $K[G]$. Man muss dann also nicht mehr die Endlichdimensionalität von V eigens voraussetzen.
3. Jede endlich-dimensionale irreduzible Darstellung einer abelschen Gruppe über einem algebraisch abgeschlossenen Körper ist eindimensional. Denn jedes Gruppenelement $g \in G$ operiert in diesem Fall durch einen Endomorphismus $\rho(g)$ der Darstellung:

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

Nach dem Schurschen Lemma 1.5.5 operieren somit alle Gruppenelemente durch Vielfache der Identität, so dass wir in eindimensionale Unterdarstellungen zerlegen können.

4. Die Gruppe der vierten Einheitswurzeln in den komplexen Zahlen, $G = \{\pm 1 \pm i\} \cong \mathbb{Z}_4$ operiert durch Multiplikation auf dem zwei-dimensionalen \mathbb{R} -Vektorraum \mathbb{C} . Dies gibt eine irreduzible reelle Darstellung von G auf \mathbb{C} , aber es gilt auch

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

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

5. Sei $K \subset L$ eine echte Körpererweiterung. Dann trägt der K -Vektorraum $V = L$ eine irreduzible Darstellung der Gruppe $G = L^\times$ über K , denn jedes Element von $L \setminus \{0\}$ ist Erzeuger für die L^\times -Wirkung. In diesem Beispiel ist

$$\text{End}_G V = L ,$$

was natürlich ungleich K ist, selbst wenn K algebraisch abgeschlossen ist. Aber für algebraisch abgeschlossenes K ist eine echte Körpererweiterung L/K sicher nicht endlichdimensional!

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

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

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 auch Kompositionsfaktoren des Moduls M .

Dazu brauchen wir das wichtige

Lemma 1.5.8 (Neunerlemma).

Gegeben sei ein Diagramm von Moduln mit kurzen exakten Zeilen:

$$\begin{array}{ccccc} A' & \xrightarrow{\iota_1} & A & \twoheadrightarrow & A'' \\ \varphi_1 \downarrow & & \varphi_2 \downarrow & & \varphi_3 \downarrow \\ B' & \xrightarrow{\iota_2} & B & \twoheadrightarrow & B'' \\ \psi_1 \downarrow & & \psi_2 \downarrow & & \psi_3 \downarrow \\ C' & \xrightarrow{\iota_3} & C & \twoheadrightarrow & C'' \end{array}$$

und es seien die senkrechten Kompositionen null:

$$\psi_i \circ \varphi_i = 0.$$

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 beiden linken Spalten exakt sind.

- Die Surjektivität von ψ_3 folgt aus der Kommutativität des rechten unteren Quadrats, $\psi_3 \circ \pi_2 = \pi_3 \circ \psi_2$. Daher

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

da π_3 und ψ_2 surjektiv sind.

- Um die Injektivität von φ_3 zu zeigen, betrachten wir $a'' \in A''$, so dass $\varphi_3(a'') = 0$. Wegen der Surjektivität von π_1 finden wir ein Urbild unter π_1 :

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

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

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

Die letzte Eigenschaft erlaubt es, die Exaktheit der zweiten Zeile zu benutzen, um $b' \in B'$ 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 ι_3 injektiv ist, folgt $\psi_1(b') = 0$. Jetzt können wir die Exaktheit der ersten Spalte ausnützen und finden ein Urbild 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 φ_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 φ_3 injektiv ist.

- Im $\varphi_3 \subset \ker \psi_3$ war schon vorausgesetzt. Sei also $b'' \in \ker \psi_3$. Da π_2 surjektiv ist, finden wir $b \in B$, 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 ψ_1 surjektiv ist, finden wir ein Urbild $b' \in B'$ in B' , $\psi_1(b') = c'$. 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 $b'' \in \text{Im } \varphi_3$; 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

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

und

$$M = \tilde{M}_s \supset \tilde{M}_{s-1} \supset \dots \supset \tilde{M}_0 = 0$$

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

$$M = M_r \supset \dots \supset M_0 = 0$$

und $N \subset M$ ein Untermodul. Wir betrachten die kanonischen Surjektionen

$$\text{can} : M \rightarrow \overline{M} := M/N$$

und die Untermoduln

$$N_i := M_i \cap N \subset N \quad \text{und} \quad \overline{M}_i := \text{can}(M_i) \subset \overline{M}$$

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 kurze exakte Sequenzen

$$N_i/N_{i-1} \hookrightarrow M_i/M_{i-1} \twoheadrightarrow \overline{M}_i/\overline{M}_{i-1}. \tag{3}$$

Ist $N \neq 0$, so gibt es wenigstens ein i mit $N_i/N_{i-1} \neq 0$. Da M_i/M_{i-1} einfach ist, folgt aus der Exaktheit von (3), dass $\overline{M}_i/\overline{M}_{i-1} = 0$. Also gilt für alle Quotienten

$$\ell(M/N) < \ell(M)$$

und ebenso gilt für jeden echten Untermodul

$$\ell(N) < \ell(M).$$

Damit ist aber $\ell(M)$ auch gleich dem Maximum der Längen von Ketten echt absteigender Untermoduln von M . Es folgt daraus, dass alle Untermoduln und alle Quotienten endliche Länge haben. Aus (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 :

$$\begin{aligned} M &\supset X \supset \cdots \supset (0) \\ M &\supset Y \supset \cdots \supset (0) \end{aligned}$$

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

$$\pi : M \rightarrow M/Y.$$

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 π einen Isomorphismus von Moduln

$$X/(X \cap Y) \cong M/Y. \quad (4)$$

Durch Vertauschen von M und N findet man analog

$$Y/(X \cap Y) \cong M/X. \quad (5)$$

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

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

Die erste und die zweite Kompositionsreihe sind nach Induktionsvoraussetzung, angewandt auf 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). \square

Korollar 1.5.10.

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

Beweis.

Sei $a \in M$ und $a \neq 0$. Dann ist der von a erzeugte Untermodul $\langle a \rangle$ ungleich Null, also $\langle a \rangle = M$, da ein einfacher Modul keine nicht-trivialen Untermoduln hat. Wir haben daher eine Surjektion

$$\begin{aligned} \varphi : R &\rightarrow M \\ \lambda &\mapsto \lambda a \end{aligned}$$

Nach dem Homomorphiesatz ist $M \cong R/\ker\varphi$; also ist jeder einfache R -Modul Quotient von R , tritt also in einer Kompositionsreihe der Form $R \supseteq \ker\varphi \supseteq \dots$ und damit in allen Kompositionsreihen von R als Subquotient auf. \square

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 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. \square

Wir wenden nun unsere Einsichten auf den Gruppenring aus Definition 1.1.16 an.

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 $\dim_K K[G] = |G|$. \square

2 Kategorien, Funktoren und natürliche Transformationen

Wir wollen in diesem Kapitel einige Sprechweisen einführen, die es erlauben, sehr kompakt über Moduln über Ringen (und viele andere Gebiete 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 $\text{ob } \mathcal{C}$ von Objekten und einer Klasse $\text{mor } \mathcal{C}$ von Morphismen, zusammen mit den folgenden Strukturabbildungen:

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

Diese Abbildungen müssen folgende Axiome erfüllen:

1. $\text{Hom}_{\mathcal{C}}(a, b) := \{f \in \text{mor } \mathcal{C} \mid s(f) = a, t(f) = b\}$ ist eine Menge und keine echte Klasse.

2. $s \circ \text{id} = t \circ \text{id} = \text{id}_{\text{ob } C}$
 (“Quelle und Ziel der Identität auf einem Objekt X ist X selbst.”)
3. $s(a \circ b) = s(b)$, $t(a \circ b) = t(a)$
 (“Ziel einer Komposition ist das Ziel der zuletzt angewandten Funktion, Quelle ist die Quelle der zuerst angewandten Funktion.”)
4. $\text{id}_{t(f)} \circ f = f$, $f \circ \text{id}_{s(f)} = f$.
 (“Komposition mit Identitätsmorphisamen 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, *R-Mod* der *R*-Linksmoduln, *Mod-R* der *R*-Rechtsmoduln und *R-S-Bimod* der *R-S*-Bimoduln, sowie die Kategorie *Alg_R* der *R*-Algebren.
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 $\text{Hom}(a, a)$ 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. 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 $\text{Hom}_{\underline{X}}(x, y)$ 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}^{opp} ist die Kategorie mit denselben Objekten wie \mathcal{C} , aber Morphismen $\text{Hom}_{\mathcal{C}^{\text{opp}}}(a, b) := \text{Hom}_{\mathcal{C}}(b, a)$ und der Komposition $f \circ_{\text{opp}} g := g \circ_{\mathcal{C}} f$.
- (ii) Die Kategorie $\mathcal{C} \amalg \mathcal{D}$ 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 $F : \mathcal{C} \rightarrow \mathcal{D}$ ordnet jedem Objekt c von \mathcal{C} ein Objekt $F(c)$ von \mathcal{D} zu, sowie jedem Morphismus $f \in \text{Hom}_{\mathcal{C}}(c, c')$ einen Morphismus $F(f) \in \text{Hom}_{\mathcal{D}}(F(c), F(c'))$. Es muss gelten:

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

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

Beispiele 2.1.5.

1. Der Funktor $U : R\text{-Mod} \rightarrow \text{Ab}$, der einem R -Modul die zugrundeliegende abelsche Gruppe zuordnet. Funktoren dieser Art heißen Vergissfunktoren.
2. Jeder Ringhomomorphismus $\Phi : R \rightarrow S$ liefert durch Restriktion der Skalare nach Lemma 1.1.23 einen Funktor $S\text{-Mod} \rightarrow R\text{-Mod}$. Man kann zum Beispiel in dieser Weise wegen $\mathbb{R} \hookrightarrow \mathbb{C}$ jeden komplexen Vektorraum als reellen Vektorraum ansehen.
3. Der Funktor $F = -^* : \text{vect}(K) \rightarrow \text{vect}(K)^{\text{opp}}$, der jedem Vektorraum seinen Dualraum zuordnet, $F(V) = V^*$, und jeder linearen Abbildung die duale Abbildung, $F(f) = f^*$.
4. Der Funktor $F = -^{**} : \text{vect}(K) \rightarrow \text{vect}(K)$, der jedem Vektorraum seinen Bidualraum zuordnet, $F(V) = V^{**}$ und jeder Abbildung die biduale Abbildung, $F(f) = f^{**}$.
5. Der Funktor $\coprod : \text{Set} \times \text{Set} \rightarrow \text{Set}$, der zwei Mengen X, Y die disjunkte Vereinigung $X \coprod Y$ zuordnet, ebenso der Funktor \prod , der zwei Mengen das kartesische Produkt zuordnet.
6. Der Funktor $\otimes_R : R^{\text{opp}}\text{-Mod} \times R\text{-Mod} \rightarrow \text{Ab}$.
7. Sei \mathcal{C} eine beliebige Kategorie. Für jedes Objekt W in \mathcal{C} definieren wir einen kovarianten Funktor

$$\text{Hom}(W, -) : \mathcal{C} \rightarrow \text{Set}$$

auf Objekten durch

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

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

$$\varphi_* : \begin{array}{ccc} \text{Hom}_{\mathcal{C}}(W, X) & \rightarrow & \text{Hom}_{\mathcal{C}}(W, Y) \\ f & \mapsto & \varphi \circ f . \end{array}$$

zu. Man rechnet leicht nach, dass alle Eigenschaften eines Funktors erfüllt sind.

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

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

auf Objekten durch

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

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

$$\begin{aligned} \varphi^* : \text{Hom}_{\mathcal{C}}(Y, W) &\rightarrow \text{Hom}_{\mathcal{C}}(X, W) \\ f &\mapsto f \circ \varphi . \end{aligned}$$

zu.

9. Wenn man für \mathcal{C} die Kategorie $\text{vect}(K)$ der K -Vektorräume betrachtet, so hat die Morphismenmenge $\text{Hom}_{\mathcal{C}}(\cdot, \cdot)$ sogar die Struktur eines K -Vektorraums. In diesem Fall liefern $\text{Hom}(-, W)$ und $\text{Hom}(W, -)$ Funktoren in die Kategorie der K -Vektorräume, bzw. deren opponierte Kategorie.

Definition 2.1.6

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

Bemerkungen 2.1.7.

- Wir kennen schon Beispiele isomorpher Kategorien:
 - Für jeden Ring R sind die Kategorie der R -Rechtsmoduln und die Kategorie der R^{opp} -Linksmoduln isomorph.
 - Für jeden Körper K sind die Kategorie der $K[X]$ -Moduln und die Kategorie der K -Vektorräume mit einem K -linearen Endomorphismus isomorph.
 - Für jeden Körper K und jede Gruppe G sind die Kategorie der K -linearen G -Darstellungen und die Kategorie der $K[G]$ -Moduln isomorph.
- 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. Betrachten wir dafür als Beispiel für einen Körper K die Kategorie $\text{vect}(K)$ der K -Vektorräume. Sowohl die Identität als auch der Bidualfunktork $-^{**}$ sind Endofunktoren

$$\text{id}, -^{**} : \text{vect}(K) \rightarrow \text{vect}(K) .$$

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

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

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. Dies führt uns auf die folgende Definition.

Definition 2.1.8

- Sind F, G Funktoren von einer Kategorie \mathcal{C} nach einer Kategorie \mathcal{D} , so ist eine natürliche Transformation $N : F \rightarrow G$, manchmal auch $F \Rightarrow G$ geschrieben, eine Vorschrift, die jedem Objekt c in der Kategorie \mathcal{C} einen Morphismus $N_c : F(c) \rightarrow G(c)$ in der

Kategorie \mathcal{D} zuordnet, so dass für jeden Morphismus $f \in \text{Hom}_{\mathcal{C}}(c, c')$ in der Kategorie \mathcal{C} das folgende Diagramm in der Kategorie \mathcal{D} kommutiert:

$$\begin{array}{ccc} F(c) & \xrightarrow{N_c} & G(c) \\ \downarrow F(f) & & \downarrow G(f) \\ F(c') & \xrightarrow{N_{c'}} & G(c') \end{array}$$

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

$$\text{id}, -^{**} : \text{vect}_f(K) \rightarrow \text{vect}_f(K)$$

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

2. Für eine kleine Kategorie \mathcal{C} und eine beliebige Kategorie \mathcal{D} , kann man die Funktorkategorie betrachten, deren Objekte Funktoren $F : \mathcal{C} \rightarrow \mathcal{D}$ 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 $[n] := \{0, \dots, n\}$, die wir wie in Beispiel 2.1.2.6 als kleine Kategorie auffassen. Ein Funktor $[n] \rightarrow R\text{-Mod}$ ist dann das Gleiche wie eine Sequenz $R_0 \rightarrow R_1 \rightarrow \dots \rightarrow R_n$ von R -Moduln. Eine natürliche Transformation zwischen zwei solchen Funktoren R und S ist ein kommutierendes Diagramm der Form

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

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:

Definition 2.1.10

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

$$\epsilon : F \circ G \rightarrow \text{id}_{\mathcal{D}} \quad \text{und} \quad \eta : \text{id}_{\mathcal{C}} \rightarrow G \circ F,$$

gibt.

Wir wollen die Äquivalenz von Kategorien noch etwas anders fassen.

Definition 2.1.11

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

2. Ein Funktor $F : \mathcal{C} \rightarrow \mathcal{D}$ 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, $F(c) \cong d$.

Man kann nun zeigen:

Satz 2.1.12.

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

Für den Beweis verweisen wir etwa auf Kassel, Quantum groups, Proposition XI.1.5. Man beachte, dass in den Beweis das Auswahlaxiom eingeht, wenn man Urbilder findet.

Beispiele 2.1.13.

1. Wir geben ein Beispiel für zwei äquivalente Kategorien an: die Kategorie $\text{vect}_f(K)$ 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 $\text{Hom}([n], [m]) := M(n \times m, K)$. Man beachte, dass nur $\text{vect}_f(K)$ 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 $\text{Hom}(X, -)$ treu ist. Seien A und B Ringe. Dann sind die folgenden Aussagen äquivalent:

- (a) Die Kategorien $A - \text{mod}$ und $B - \text{mod}$ der Linksmoduln sind äquivalent.
- (b) Die Kategorien $A^{\text{opp}} - \text{mod}$ und $B^{\text{opp}} - \text{mod}$ der Linksmoduln sind äquivalent.
- (c) Ein Erzeuger einer Kategorie \mathcal{C} ist ein Objekt X , so dass der Funktor $\text{Hom}(X, -)$ treu ist. Es gibt einen endlich-erzeugten projektiven Erzeuger P von $A - \text{mod}$ und einen Ring-Isomorphismus $B \cong \text{End}_A(P)$.

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.

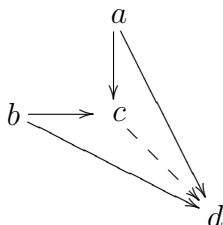
Definition 2.2.1

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 $\iota_\lambda : a_\lambda \rightarrow c$ heißt Koprodukt der a_λ , 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:

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

Bemerkungen 2.2.2.

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

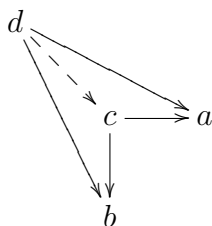


kommutiert.

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

$$\begin{aligned} \text{Hom}_{\mathcal{C}}(d, c) &\rightarrow \prod_{\lambda \in \Lambda} \text{Hom}_{\mathcal{C}}(d, a_\lambda) \\ f &\mapsto (pr_\lambda \circ f)_{\lambda \in \Lambda} \end{aligned}$$

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



3. Es gibt Kategorien, in denen nicht alle Produkte und Koproducte 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 das kategorielle Koproduct bzw. Produkte. Dies ist der Inhalt der Bemerkung 1.2.2 (ii).
- (b) Das kartesische Produkt von Ringen ist auch ein kategorielles Produkt. Das Tensorprodukt dagegen ist das Koproduct 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 Objekten einer Kategorie \mathcal{D} noch etwas formaler. Dazu sei

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

die Produktkategorie, deren Objekte Λ -Tupel von Objekten von \mathcal{D} sind. Ein Morphismus $(X_\lambda)_{\lambda \in \Lambda} \rightarrow (Y_\lambda)_{\lambda \in \Lambda}$ ist ein Λ -Tupel von Morphismen $f_\lambda : X_\lambda \rightarrow Y_\lambda$ in \mathcal{D} .

In der universellen Eigenschaft sowohl der direkten Summe als auch des Produkts tritt dieses als Objekt in allen Faktoren eines Produktes von Hom-Räumen auf. Wir führen daher den Diagonalfunktor ein,

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

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 $R\text{-Mod}$ für einen Ring R ist. Die direkte Summe bzw. das direkte Produkt liefern dann Funktoren

$$\prod, \coprod : \mathcal{C} \rightarrow \mathcal{D},$$

weil sie nach Annahme für *jede* Familie von Objekten definiert sind. 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-Räumen gibt:

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

im Falle des Produkts haben wir Isomorphismen

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

Dies führt uns auf die folgende Definition:

Definition 2.2.3

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

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

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 $\varphi \in \text{Hom}_{\mathcal{D}}(Fc, d)$ den Morphismus

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

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

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

Die natürliche Eigenschaft ist dann die Forderung, dass das Diagramm

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

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.

- Wir haben schon gesehen, dass das Koprodukt ein linksadjungierter Fuunktor zum Diagonalenfunktor ist und das Produkt ein rechtsadjungierter Funktor zum Diagonalenfunktor.
- Wir betrachten den Vergissfunktor

$$U : \text{vect}(K) \rightarrow \text{Set} ,$$

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

$$F : \text{Set} \rightarrow \text{vect}(K) ,$$

das einer Menge M den von ihr erzeugten K -Vektorraum $F(M)$ der Abbildungen $f : M \rightarrow K$ zuordnet, die nur für endlich viele Elemente von M einen Wert ungleich Null annehmen. Eine Abbildung $f : M \rightarrow N$ von Mengen wird dabei auf diejenige lineare Abbildung $F(M) \rightarrow F(N)$ abgebildet, die den Basisvektor δ_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

$$\begin{aligned} \Phi_{M,V} : \text{Hom}_{\text{Set}}(M, U(V)) &\rightarrow \text{Hom}_K(F(M), V) \\ \varphi &\mapsto \Phi_{M,V}(\varphi) \end{aligned}$$

mit

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

Insbesondere finden wir, dass für jeden K -Vektorraum V die einelementige Menge $\text{Hom}_{\text{Set}}(\emptyset, U(V))$ isomorph zu $\text{Hom}_K(F(\emptyset), V)$ 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 Mengen erzeugt wird.

- Ein ähnliches Beispiel ist der Vergissfunktor $U : \text{Gr} \rightarrow \text{Set}$, 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 linksadjungierte Funktor ist nun ein Funktor $F' : \text{Set} \rightarrow \text{Ab}$ und ordnet einer Menge die freie abelsche Gruppe zu. Er ist von dem oben beschriebenen linksadjungierten Funktor verschieden.

- 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. Wir würden dann einen Körper K suchen, so dass für jeden Körper L eine Bijektion von Mengen

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

existiert. Da 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. (Es ist klar, was hinter diesem Beispiel steckt: in der Kategorie von Mengen gibt es ein initiales Objekt, die leere Menge. In der Kategorie aller Körper gibt es kein initiales Objekt.)

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

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

Hat ein Funktor Adjungierte, so hat er gute Eigenschaften, und oft kann man ihn studieren, indem man die (manchmal einfacheren) adjungierten Funktoren studiert. Wir werden das sehen, wenn wir noch etwas mehr Begriffe zur Verfügung haben.

Wir betrachten noch ein anderes Beispiel aus der Modultheorie:

Beispiel 2.2.5.

Seien R, S Ringe und $\phi : R \rightarrow S$ ein Ringhomomorphismus. Dann liefert der Pullback bzw. die Restriktion der Skalare wie in Beispiel 2.1.5.2 einen Vergissfunktor

$$U : S\text{-Mod} \rightarrow R\text{-Mod} .$$

Wir untersuchen seine adjungierten Funktoren.

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

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

$$\begin{aligned} \text{Hom}_R(M, U(N)) &\xrightarrow{\sim} \text{Hom}_S(S \otimes_R M, N) \\ f &\mapsto (s \otimes m \mapsto s \cdot f(m)) \end{aligned}$$

und

$$\begin{aligned} \text{Hom}_S(S \otimes_R M, N) &\xrightarrow{\sim} \text{Hom}_R(M, U(N)) \\ g &\mapsto (m \mapsto g(1_S \otimes m)) . \end{aligned}$$

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

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

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

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

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

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

mit inverser Abbildung

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

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

3. Man kann diese Überlegungen noch leicht etwas verallgemeinern: Seien R, S Ringe und B ein $S - R$ -Bimodul. Dann haben wir einen Funktor

$$\begin{aligned} \tilde{B} : R\text{-Mod} &\rightarrow S\text{-Mod} \\ N &\mapsto B \otimes_R N \end{aligned}$$

der Linksadjungiert zum Funktor

$$\begin{aligned} S\text{-Mod} &\rightarrow R\text{-Mod} \\ Q &\mapsto \text{Hom}_S(B, Q) \end{aligned}$$

ist.

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

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

und

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

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

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

(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

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

Identitätsmorphisme 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 ϵ und η die Adjunktionsisomorphismen gewinnen durch

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

und ihre Inversen durch

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

3. Wir können nun auch sagen, dass ein Paar adjungierter Funktoren $F \dashv G$ genau dann eine Äquivalenz von Kategorien ist, falls ϵ und η natürliche Isomorphismen sind.

Wir müssen uns nun mit Funktoren in die Kategorie Set beschäftigen. Für jedes Objekt c einer Kategorie \mathcal{C} haben wir einen Funktor nach Set , für den wir die Bezeichnung

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

einführen.

Definition 2.2.7

Sei \mathcal{C} eine Kategorie. Ein Funktor $F : \mathcal{C} \rightarrow \text{Set}$ 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.

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 wichtige Rolle in der Kategorientheorie spielt:

Lemma 2.2.8 (Yoneda-Lemma).

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

$$\begin{array}{ccccc} \text{Hom}(y_c, F) & \rightarrow & \text{Hom}_{\text{Set}}(y_c(c), F(c)) = \text{Hom}_{\text{Set}}(\text{Hom}_{\mathcal{C}}(c, c), F(c)) & \rightarrow & F(c) \\ N & \mapsto & N_c & \mapsto & N_c(\text{id}_c) \end{array},$$

wobei der erste Pfeil der natürliche Morphismus auf c und der letzte Pfeil das Einsetzen von id_c ist. Diese Abbildung ist eine Bijektion von Mengen.

Beweis.

Ist $N : y_c \rightarrow F$ eine natürliche Transformation, so kommutiert nach Definition für jeden Morphismus $f : c \rightarrow c'$ das Diagramm

$$\begin{array}{ccc} y_c(c) & \xrightarrow{y_c(f)} & y_c(c') \\ \downarrow N_c & & \downarrow N_{c'} \\ F(c) & \xrightarrow{F(f)} & F(c') \end{array}$$

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

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

dass die Gleichung

$$N_{c'}(f) = F(f)(N_c(\text{id}_c))$$

gilt. Somit hängt die natürliche Transformation N einzig von $N_c(\text{id}_c)$ ab, womit die Injektivität der Yoneda-Abbildung gezeigt ist.

Umgekehrt liefert jedes $x \in F(c)$ für jedes Objekt c der Kategorie \mathcal{C} eine Abbildung von Mengen

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(c, c') = y_c(c') & \rightarrow & F(c') \\ f & \mapsto & {}^x N(f) := F(f)(x) \end{array}$$

die sich zu einer natürlichen Transformation $\eta : y_c \rightarrow F$ von Funktoren $\mathcal{C} \rightarrow \text{Set}$ zusammensetzen. \square

Das Yoneda-Lemma hat viele Folgerungen. Zunächst benutzen wir es in der folgenden Betrachtung:

Betrachtung 2.2.9.

1. Sei auch der Funktor F von der Form $F = y_{c'} = \text{Hom}(c', -)$. Dann finden wir Isomorphismen

$$\text{Hom}(c', c) \cong F(c) \cong \text{Hom}(y_c, y_{c'})$$

Hierbei wird der Morphismus $f \in \text{Hom}(c', c)$ auf die natürliche Transformation $y_c \rightarrow y_{c'}$ abgebildet, die auf dem Objekt d wirkt durch

$$\begin{aligned} f^* : \text{Hom}(c', d) &\rightarrow \text{Hom}(c, d) \\ \varphi &\mapsto \varphi \circ f \end{aligned}$$

Daher sind die Funktoren $\text{Hom}(c', -)$ und $\text{Hom}(c, -)$ genau dann isomorph, wenn die Objekte c und c' isomorph sind.

2. Insbesondere gilt: ist ein Funktor $F : \mathcal{C} \rightarrow \text{Set}$ darstellbar, so ist das darstellende Objekt eindeutig bis auf Isomorphie.
3. Indem wir die gleiche Betrachtung auf den Funktor

$$\text{Hom}(-, d) : \mathcal{C}^{\text{opp}} \rightarrow \text{Set}$$

anwenden, finden wir auch, dass auch die Funktoren $\text{Hom}(-, d)$ und $\text{Hom}(-, d')$ genau dann isomorph sind, wenn die Objekte d und d' isomorph sind.

Wir wenden dies nun an im Beweis von

Satz 2.2.10.

Sei $F : \mathcal{C} \rightarrow \mathcal{D}$ ein Funktor, der einen linksadjungierten Funktor G besitzt. Dann vertauscht F mit Produkten und G mit Koproducten.

Beweis.

Es gilt für alle Objekte d von \mathcal{D}

$$\begin{aligned} \text{Hom}_{\mathcal{D}}(d, F(\prod_i c_i)) &\cong \text{Hom}_{\mathcal{C}}(G(d), \prod_i c_i) && \text{da } G \dashv F \\ &\cong \prod_i \text{Hom}_{\mathcal{C}}(G(d), c_i) && \text{univ. Eigen. des direkten Produkts} \\ &\cong \prod_i \text{Hom}_{\mathcal{D}}(d, F(c_i)) && \text{da } G \dashv F \\ &\cong \text{Hom}_{\mathcal{D}}(d, \prod_i F(c_i)) && \text{univ. Eigen. des direkten Produkts.} \end{aligned}$$

Dies liefert für jedes Objekt d in der Kategorie \mathcal{D} Isomorphismen. Man überlegt sich leicht, dass diese sich zu einer natürlichen Transformation vom Funktor

$$\text{Hom}_{\mathcal{D}}(-, F(\prod_i c_i)) : \mathcal{D}^{\text{opp}} \rightarrow \text{Set}$$

zum Funktor

$$\text{Hom}_{\mathcal{D}}(-, \prod_i F(c_i)) : \mathcal{D}^{\text{opp}} \rightarrow \text{Set}$$

zusammensetzen.

Daraus folgt die Isomorphie der Funktoren $\text{Hom}_{\mathcal{D}}(-, F(\prod_i c_i))$ und $\text{Hom}_{\mathcal{D}}(-, \prod_i F(c_i))$ und somit mit Betrachtung 2.2.9.1, dass $F(\prod_i c_i) \cong \prod_i F(c_i)$ gilt. Analog geht der Beweis für Koprodukte. \square

Wir bringen auch gleich eine weitere Folgerung aus dem Yoneda-Lemma 2.2.8:

Satz 2.2.11.

Besitzt ein Funktor $G : \mathcal{D} \rightarrow \mathcal{C}$ einen linksadjungierten Funktor, so ist dieser bis auf natürlichen Isomorphismus eindeutig bestimmt. Ebenso sind natürlich auch rechtsadjungierte Functoren in der gleichen Weise eindeutig, wenn sie existieren.

Beweis.

Seien $F, F' : \mathcal{C} \rightarrow \mathcal{D}$ zwei Linksadjungierte zu G . Dann gilt für alle Objekte $c \in \mathcal{C}$ und $d \in \mathcal{D}$ die Isomorphie

$$\text{Hom}_{\mathcal{D}}(F(c), d) \cong \text{Hom}_{\mathcal{C}}(c, G(d)) \cong \text{Hom}_{\mathcal{D}}(F'(c), d).$$

Die Isomorphismen erfüllen wieder die Natürlichkeitseigenschaft. Wir erhalten also einen natürlichen Isomorphismus $y_{F(c)} \rightarrow y_{F'(c)}$, der nach der Folgerung 2.2.9 aus dem Yoneda-Lemma von einem (Iso-)Morphismus $F'(c) \rightarrow F(c)$ herrührt. \square

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 $U : \mathcal{D} \rightarrow \mathcal{C}$. Hierbei ist die Kategorie \mathcal{D} oft die "bessere" Kategorie, z.B. wenn U ein Vergissfunktors 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 die von ihr frei erzeugten Vektorraum A_X . Man beachte, dass dieser mit einem Morphismus $\varphi : X \rightarrow A_X$ von Mengen kommt. Die universelle Eigenschaft besagt nun, dass man auch für jeden Vektorraum B jeden anderen Morphismus $\varphi : X \rightarrow U(B)$ von Mengen eindeutig zu einem Morphismus $A_X \rightarrow B$ von Vektorräumen verbessern kann, also hier linearisieren kann.

Definition 2.2.12

Seien \mathcal{C}, \mathcal{D} Kategorien und $U : \mathcal{D} \rightarrow \mathcal{C}$ ein Funktor. Sei X_0 ein Objekt in \mathcal{C} .

1. Ein initialer universeller Morphismus von X_0 nach U ist ein Paar (A_{X_0}, φ) , bestehend aus einem (verbesserten) Objekt A_{X_0} in \mathcal{D} und einem Morphismus $\varphi_0 : X_0 \rightarrow U(A_{X_0})$ in \mathcal{C} (in der ursprünglichen Kategorie), so dass die folgende universelle Eigenschaft gilt:

Für jedes Objekt B von \mathcal{D} und jeden Morphismus $f : X_0 \rightarrow U(B)$ in \mathcal{C} gibt es einen eindeutigen (verbesserten) Morphismus $\tilde{f} : A_{X_0} \rightarrow B$ in \mathcal{D} , so dass das folgende Diagramm in \mathcal{C} kommutiert:

$$\begin{array}{ccc} X_0 & \xrightarrow{\varphi_0} & U(A_{X_0}) & & A_{X_0} \\ & \searrow f & \downarrow U(\tilde{f}) & & \downarrow \exists! \tilde{f} \\ & & U(B) & & B \end{array}$$

in \mathcal{C}

in \mathcal{D}

2. Ein terminaler universeller Morphismus von U nach einem Objekt X in \mathcal{C} ist ein Paar (A_X, φ) , bestehend aus einem Objekt A_X in \mathcal{D} und einem Morphismus $\varphi : U(A_X) \rightarrow X$ in \mathcal{C} , so dass die folgende universelle Eigenschaft gilt:

Für jedes Objekt B von \mathcal{D} und jeden Morphismus $f : U(B) \rightarrow X$ in \mathcal{C} gibt es einen eindeutigen Morphismus $\tilde{f} : B \rightarrow A_X$ in \mathcal{D} , so dass das folgende Diagramm in \mathcal{C} kommutiert:

$$\begin{array}{ccc}
 U(B) & & B \\
 \downarrow U(\tilde{f}) & \searrow f & \downarrow \exists! \tilde{f} \\
 U(A_X) & \xrightarrow{\varphi} & X \\
 & & \downarrow \\
 & & A_X
 \end{array}$$

in \mathcal{C} in \mathcal{D}

Beispiele 2.2.13.

1. Um die universelle Eigenschaft des Polynomrings – Einsetzen – zu verstehen, betrachten wir den Vergissfunktork

$$U : K\text{-Alg} \rightarrow \text{Set} .$$

Wir wollen nun den initialen universellen Morphismus für die einelementige Menge \bullet untersuchen. Dies ist ein Objekt in $K\text{-Alg}$, also eine K -Algebra R , mit einem Morphismus von Mengen $\bullet \rightarrow U(R)$, 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 $\bullet \rightarrow U(S)$, also für jedes Paar bestehend aus einer K -Algebra S und einem Element $a \in S$, einen eindeutigen Morphismus $f : R \rightarrow S$ von K -Algebren geben muss, so dass $\bullet \rightarrow U(R) \xrightarrow{U(f)} U(S)$ gleich $\bullet \rightarrow S$ ist, also dass $f(X) = a$ gilt.

2. Für das Tensorprodukt betrachten wir vereinfachend nur den Fall von K -Vektorräumen und nur ein Argument und halten das andere Argument, einen K -Vektorraum V , fest. Dann können wir $\mathcal{C} = \mathcal{D} = \text{vect}(K)$ setzen. Wir betrachten dann den Funktor

$$\begin{array}{ccc}
 U = y_V = \text{Hom}(V, -) : & \text{vect}(K) & \rightarrow \text{vect}(K) \\
 & W & \mapsto \text{Hom}_K(V, W)
 \end{array}$$

Das universelle Objekt von W nach $y_V = \text{Hom}(V, -)$ ist dann das Tensorprodukt $W \otimes V$ mit universellem Morphismus

$$\begin{array}{ccc}
 \varphi : & W & \rightarrow \text{Hom}_K(V, W \otimes V) \\
 & w & \mapsto \varphi_w
 \end{array}$$

mit $\varphi_w(v) := w \otimes v$. Dafür brauchen wir für jeden K -Vektorraum Y und jede lineare Abbildung $f : W \rightarrow \text{Hom}_K(V, Y)$, also $f \in \text{Hom}_K(W, \text{Hom}_K(V, Y))$ eine lineare Abbildung $g : W \otimes V \rightarrow Y$. Eine solche existiert wegen der natürlichen Isomorphie

$$\text{Hom}_K(W \otimes V, Y) \cong \text{Hom}_K(W, \text{Hom}_K(V, Y)) .$$

Denn beide Räume beschreiben bilineare Abbildungen $W \times V \rightarrow Y$. Wenn $\beta : W \times V \rightarrow Y$ eine bilineare Abbildung ist, so ist für jedes $w \in W$ die Abbildung $\beta(w, \cdot)$ eine lineare Abbildung in $\text{Hom}_K(V, Y)$. Dies liefert den gewünschten Isomorphismus.

Bemerkungen 2.2.14.

- (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}, φ_1) ein universeller Morphismus von X_1 nach U und (A_{X_2}, φ_2) ein universeller Morphismus von X_2 nach U . Aus Definition 2.2.12, angewandt auf den Morphismus $\varphi_2 \circ h$ in \mathcal{C} , folgt, dass für jeden Morphismus $h : X_1 \rightarrow X_2$ in \mathcal{C} ein eindeutig bestimmter Morphismus $\tilde{h} : A_{X_1} \rightarrow A_{X_2}$ existiert, so dass in \mathcal{C} das Diagramm*

$$\begin{array}{ccc} X_1 & \xrightarrow{\varphi_1} & U(A_{X_1}) \\ h \downarrow & & \downarrow U(\tilde{h}) \\ X_2 & \xrightarrow{\varphi_2} & U(A_{X_2}) \end{array}$$

kommutiert. Existiert ein universeller Morphismus für jedes Objekt X von \mathcal{C} , so definiert $X_i \mapsto A_{X_i}$ und $h \mapsto \tilde{h}$ einen Funktor V von \mathcal{C} nach \mathcal{D} und die Morphismen φ_i liefern eine natürliche Transformation vom Identitätsfunktor nach $U \circ V$. Man kann zeigen, dass dann die Funktoren U, V adjungiert sind.

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. Es ist natürlich, dann auch eine Klasse von Funktoren einzuführen, die diese Struktur respektiert.

Definition 2.3.1

1. Eine Kategorie \mathcal{C} heißt additiv, 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 $F : \mathcal{C} \rightarrow \mathcal{D}$ heißt additiv, wenn für jedes Paar X, Y von Objekten von \mathcal{C} die Abbildung $F : \text{Hom}_{\mathcal{C}}(X, Y) \rightarrow \text{Hom}_{\mathcal{D}}(F(X), F(Y))$ ein Homomorphismus von abelschen Gruppen ist.

Wir wissen nach den Überlegungen des vorangegangenen Abschnitts, dass der zweite Punkt bedeutet, dass der Diagonalfunktor $\Delta : \mathcal{C} \rightarrow \prod_{i \in I} \mathcal{C}$ 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 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 Koproducts gibt sie einen eindeutig bestimmten Morphismus $\coprod_0 \rightarrow M$. Dies zeigt, dass \coprod_0 ein initiales Objekt 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 terminales Objekt $\star \in \mathcal{C}$ ist.
- Nun gilt $\text{Hom}_{\mathcal{C}}(0, 0) = \{0\}$, denn dieser Hom-Raum enthält nur ein Objekt, das gleich der Identität id_0 auf dem initialen Objekt 0 sein muss. Gleichzeitig ist es id_0 neutrale Element 0 für die abelsche Gruppenstruktur auf $\text{Hom}_{\mathcal{C}}(0, 0)$. Also gilt $\text{id}_0 = 0$.

Für einen beliebigen Morphismus $c \xrightarrow{f} 0$ folgt aber aus der Bilinearität der Verknüpfung $f = \text{id}_0 \circ f = 0_0 \circ f = 0$ für alle Objekte $c \in \mathcal{C}$. Daher bestehen die Homomorphismen nur aus dem neutralen Element, $\text{Hom}_{\mathcal{C}}(c, 0) = \{0\}$. 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.

- In jeder punktierten Kategorien gibt es einen kanonischen Morphismus

$$\prod_{i \in I} X_i \rightarrow \prod_{i \in I} X_i$$

vom Koproduct ins Produkt. Dazu geben wir eine Familie von Morphismen

$$f_{ij} : X_i \rightarrow X_j$$

an: diese ist $0 : X_i \rightarrow X_j$ für $i \neq j$ und id_{X_i} im Falle gleicher Indizes.

Wenn dieser Morphismus ein Isomorphismus ist, bekommen wir automatisch auf allen Hom-Mengen die Struktur eines abelschen Monoids, sodass die Komposition bilinear ist.

Ist umgekehrt auf den Hom-Mengen einer Kategorie die Struktur von abelschen Monoiden gegeben und existieren z.B. Koproducte, dann ist die Kategorie erstens punktiert und zweitens sind die Koproducte auch Produkte (bzw. Produkte Koproducte).

Somit ist es für eine gegebene Kategorie eine Eigenschaft, eine additive Kategorie zu sein, und es bedarf keiner Wahl einer Struktur.

- Allgemeiner finden wir für jedes Paar von Objekten X, Y einer additiven Kategorie einen Morphismus $X \xrightarrow{0} 0 \xrightarrow{0} Y \in \text{Hom}(X, Y)$. Man überlege sich, dass dieser Morphismus gleich dem neutralen Element der abelschen Gruppe $\text{Hom}(X, Y)$ ist.

Definition 2.3.3

- (i) Sei $f : a \rightarrow b$ ein Morphismus in einer additiven Kategorie \mathcal{C} . Ein Morphismus $\iota : k \rightarrow a$ 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 $d \rightarrow k$ gibt, so dass das Diagramm

$$\begin{array}{ccccc} k & \xrightarrow{\iota} & a & \xrightarrow{f} & b \\ & \swarrow \exists! & \uparrow g & & \\ & & d & & \end{array}$$

kommutiert. Äquivalent dazu können wir auch fordern, dass für alle Objekte d die Sequenz abelscher Gruppen

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(d, k) \xrightarrow{\iota^*} \text{Hom}_{\mathcal{C}}(d, a) \xrightarrow{f^*} \text{Hom}_{\mathcal{C}}(d, b)$$

exakt ist.

(ii) Analog heißt ein Morphismus $p : b \rightarrow c$ Kokern von f , und wir schreiben $p = \text{coker}(f)$, falls für alle Objekte d die folgende Sequenz abelscher Gruppen exakt ist:

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(c, d) \xrightarrow{p^*} \text{Hom}_{\mathcal{C}}(b, d) \xrightarrow{f^*} \text{Hom}_{\mathcal{C}}(a, d) .$$

Als Diagramm

$$\begin{array}{ccccc} a & \xrightarrow{f} & b & \xrightarrow{p} & c \\ & & \downarrow & \swarrow \exists! & \\ & & d & & \end{array}$$

Wiederum hat nicht in jeder Kategorie jeder Morphismus einen Kern bzw. Kokern.

Definition 2.3.4

Sei \mathcal{C} eine Kategorie.

1. Ein Morphismus $\iota : a \rightarrow b$ 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 $f' = 0$ zu fordern.)
2. Ein Morphismus $p : a \rightarrow b$ 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 2.3.5.

Sei \mathcal{C} eine additive Kategorie. Sei $f \in \text{Hom}_{\mathcal{C}}(A, B)$ ein Morphismus, der einen Kern $K \xrightarrow{\iota} A$ besitzt. Dann ist ι ein Monomorphismus. Dual, wenn f einen Kokern besitzt, so ist dieser 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 ϕ , so dass das Diagramm

$$\begin{array}{ccccc} \ker f & \xrightarrow{f} & A & \xrightarrow{f} & B \\ & \swarrow \phi & \uparrow 0 & & \\ & & X & & \end{array}$$

kommutiert. Da auch mit $\phi = 0$ das Diagramm kommutiert, muss ϕ 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. \square

Definition 2.3.6

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 $\iota : a \rightarrow b$ gilt $\iota = \ker(\text{coker}(\iota))$.

- Für jeden Epimorphismus $p : a \rightarrow b$ gilt $p = \text{coker}(\ker(p))$. Im Diagramm für den Monomorphismus

$$\begin{array}{ccccc}
 a & \xrightarrow{\iota} & b & \xrightarrow{\text{coker}\iota} & \text{coker}\iota \\
 & & \uparrow \text{ker} & & \\
 & & \text{ker coker}\iota & &
 \end{array}$$

müssen also der linke horizontale Pfeil und der vertikale Pfeil übereinstimmen.

Für eine gegebene Kategorie ist es wieder eine Eigenschaft, eine abelsche Kategorie zu sein, und es bedarf keiner Wahl einer Struktur.

Definition 2.3.7

- Lässt sich ein Morphismus einer beliebigen Kategorie $f : a \rightarrow b$ zerlegen als $f = \iota \circ p$, wobei $p : a \rightarrow x$ ein Epimorphismus und $\iota : x \rightarrow b$ ein Monomorphismus ist, so nennt man das Objekt x ein Bild von f und schreibt $x = \text{Im}(f)$.
- Lässt sich umgekehrt $f = p \circ \iota$ schreiben, wobei $\iota : a \rightarrow x$ ein Monomorphismus und $p : x \rightarrow b$ ein Epimorphismus ist, so nennt man das Objekt x ein Kobild von f und schreibt $x = \text{coim}(f)$.

Bemerkungen 2.3.8.

- Wie immer bei Objekten, die durch universelle Eigenschaften definiert sind, zeigt man, dass Kerne, Kokerne, Bilder und Kobilder bis auf eindeutige Isomorphie eindeutig bestimmt sind, wenn sie existieren.
- In abelschen Kategorien existieren Bilder und Kobilder stets: das Bild ist der Kern des Kokerns, und das Kobild ist der Kokern des Kerns. Als Diagramm für das Bild:

$$\begin{array}{ccccc}
 a & \xrightarrow{f} & b & \xrightarrow{\text{coker}(f)} & \text{coker}(f) \\
 & \searrow \tilde{f} & \uparrow \text{ker} & & \\
 & & \text{ker(coker}(f)) & &
 \end{array}$$

Der Morphismus \tilde{f} existiert hierbei nach der universellen Eigenschaft des Kerns, da $\text{ker}(\text{coker}(f)) \circ f = 0$ gilt. Es ist noch zu zeigen, dass \tilde{f} ein Epimorphismus ist. Für den recht technischen Beweis verweisen wir auf Knapp, *Advanced Algebra*, p. 239 ff. Damit können wir exakte Sequenzen in allgemeinen abelschen Kategorien einführen.

Beispiele 2.3.9.

- Wir betrachten die Kategorie \mathcal{C} 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 \mathcal{C} die Kerne in der Kategorie Ab der abelschen Gruppen.

- Das Bild von Torsionselementen in einer freien abelschen Gruppe ist immer Null. Betrachte das Diagramm

$$\begin{array}{ccccc}
 a & \xrightarrow{f} & b & \xrightarrow{\text{coker} f} & \text{coker}(f) \\
 & & \downarrow & \swarrow & \\
 & & x & &
 \end{array}$$

In unserem Fall ist x stets eine freie abelsche Gruppe. Daher faktorisiert der gestrichelte Morphismus auf die torsionsfreie Gruppe $\text{coker}(f)/\text{Tor}$. Der Kokern einer Abbildung $f : M' \rightarrow M$ in \mathcal{C} ist daher gegeben durch die freie Gruppe $\text{coker}(f)/\text{Tor}$, d.h. durch die Quotientengruppe nach der Untergruppe aller Torsionselemente.

- Die Kategorie \mathcal{C} hat also alle Kerne und Kokerne. Man muss aber aufpassen: betrachte für $0 \neq n \in \mathbb{Z}$ die Multiplikationsabbildung $\iota_n : \mathbb{Z} \rightarrow \mathbb{Z}$; sie hat trivialen Kern und Kokern. Daher ist das Bild dieser Abbildung in \mathcal{C} die Identitätsabbildung $\mathbb{Z} \rightarrow \mathbb{Z}$. ι_n ist als injektive Abbildung der unterliegenden Mengen ein Monomorphismus, aber $\ker(\text{coker}(\iota_n)) = \text{id}_{\mathbb{Z}} \neq \iota_n$. Also ist \mathcal{C} 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 $\text{Ko-}X$ in \mathcal{C}^{opp} entspricht.

Definition 2.3.10

1. Ein Funktor $F : \mathcal{C} \rightarrow \mathcal{D}$ zwischen abelschen Kategorien heißt additiv, falls $F : \text{Hom}_{\mathcal{C}}(c, c') \rightarrow \text{Hom}_{\mathcal{D}}(F(c), F(c'))$ ein Homomorphismus von abelschen Gruppen ist.
2. Sei $F : \mathcal{C} \rightarrow \mathcal{D}$ ein additiver Funktor zwischen abelschen Kategorien. Ist $0 \rightarrow a' \rightarrow a \rightarrow a'' \rightarrow 0$ eine beliebige kurze exakte Sequenz in \mathcal{C} , so heißt F
 - halbexakt, falls $F(a') \rightarrow F(a) \rightarrow F(a'')$ für alle exakten Sequenzen in \mathcal{C} exakt ist;
 - linksexakt, falls $0 = F(0) \rightarrow F(a') \rightarrow F(a) \rightarrow F(a'')$ exakt ist;
 - rechtsexakt, falls $F(a') \rightarrow F(a) \rightarrow F(a'') \rightarrow 0$ für alle exakten Sequenzen in \mathcal{C} exakt ist;
 - exakt, falls $0 \rightarrow F(a') \rightarrow F(a) \rightarrow F(a'') \rightarrow 0$ für alle exakten Sequenzen in \mathcal{C} exakt ist.

Beispiele 2.3.11.

1. Die Funktoren \coprod und $\prod : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ sind, wenn sie existieren, exakt, vgl. dazu den Beweis von 1.4.6, Schritt 2 \Rightarrow 4. Nach Bemerkung 2.3.2 sind dann Produkt und Koprodukt gleich.
2. Sei M ein R -Rechtsmodul. Der Funktor $M \otimes_R - : R\text{-Mod} \rightarrow \text{Ab}$ ist rechtsexakt nach Satz 1.4.9. Er ist exakt genau dann, wenn der Modul M flach ist, vgl. Definition 1.4.10.
3. Sei M ein R -Modul. Der Funktor $\text{Hom}_R(M, -) : R\text{-Mod} \rightarrow \text{Ab}$ ist linksexakt. Er ist genau dann exakt, wenn der Modul M projektiv ist, vgl. Satz 1.4.6.

4. Sei M ein R -Modul. Der Funktor $\text{Hom}_R(-, M) : (R\text{-Mod})^{\text{opp}} \rightarrow \text{Ab}$ ist linksexakt. Er ist genau dann exakt, wenn der Modul M injektiv ist, vgl. Satz 1.4.12.

Wir kommen dadurch zu den folgenden allgemeinen Definitionen für abelsche Kategorien:

Definition 2.3.12

1. Ein Objekt U einer abelschen Kategorie heißt projektiv, wenn der Funktor $\text{Hom}(U, -) : \mathcal{C} \rightarrow \text{Ab}$ exakt ist.
2. Eine abelsche Kategorie \mathcal{C} heißt halbeinfach, wenn jedes Objekt U von \mathcal{C} projektiv ist, d.h. wenn alle Funktoren $\text{Hom}(U, -)$ exakt sind.
3. Ein Objekt U einer abelschen Kategorie heißt injektiv, wenn der Funktor $\text{Hom}(-, U) : \mathcal{C}^{\text{opp}} \rightarrow \text{Ab}$ 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 $U \otimes - : \mathcal{C} \rightarrow \text{Ab}$ 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 2.3.9.3 ist klar, dass Aussagen wie das Neunerlemma 1.5.8 in beliebigen abelschen Kategorien gelten.

Bemerkung 2.3.13.

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 $e : M \rightarrow N$ und jeden Morphismus $f : P \rightarrow N$ es eine Hochhebung $\tilde{f} : P \rightarrow M$ gibt mit $e \circ \tilde{f} = f$. Injektive Objekte sind dual definiert.
2. In der Kategorie der Mengen ist jedes Objekt injektiv.
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 beliebigen Epimorphismus $e : M \rightarrow N$ einen Schnitt $s : N \rightarrow M$, d.h. $e \circ s = \text{id}_N$. Für einen beliebigen Morphismus $f : P \rightarrow N$ 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 $e : M \rightarrow N$ den Morphismus $f = \text{id}_N$ und finde durch die Hebungseigenschaft für die Identität einen Schnitt von e , als Diagramm:

$$\begin{array}{ccccc}
 & & N & & \\
 & & \downarrow \text{id} & & \\
 M^e & \longrightarrow & N & \longrightarrow & 0
 \end{array}$$

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. Dann ist das Koproduct $\coprod_{i \in I} M_i$ genau dann projektiv, wenn jeder Summand M_i projektiv ist.
2. Dann ist das Produkt $\prod_{i \in I} M_i$ 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 $\text{Hom}(-, \prod_{i \in I} M_i)$ genau dann exakt ist, wenn alle M_i projektiv sind. Dazu wenden wir den Funktor auf eine exakte Sequenz

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

an und erhalten aufgrund der universellen Eigenschaft des Produktes die Sequenz abelscher Gruppen:

$$0 \rightarrow \prod_{i \in I} \text{Hom}_R(C, M_i) \rightarrow \prod_{i \in I} \text{Hom}_R(B, M_i) \rightarrow \prod_{i \in I} \text{Hom}_R(A, M_i) \rightarrow 0$$

Diese ist offenbar genau dann exakt, wenn die einzelnen Sequenzen

$$0 \rightarrow \text{Hom}(C, M_i) \rightarrow \text{Hom}(B, M_i) \rightarrow \text{Hom}(A, M_i) \rightarrow 0$$

für alle i exakt sind, i.e. alle Objekte M_i projektiv sind. □

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

$$\oplus_{i \in I} \tilde{R} \rightarrow M \rightarrow 0$$

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

$$0 \rightarrow M \rightarrow \prod_{i \in I} R^*$$

mit einer geeigneten Familie I existiert. Jeden Modul der Form $\prod_{i \in I} R^*$ nennen wir einen kofreien Modul zu \tilde{R} . Er ist wegen Lemma 2.4.1 injektiv.

Beispiele 2.4.3.

1. R selbst ist regulär; ebenso direkte Summen von Kopien von R .
2. Die abelsche Gruppe $R^* := \text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ 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 bezüglich des Morphismus $\mathbb{Z} \rightarrow R$ koinduzierte R -Modul $\text{Hom}_{\mathbb{Z}}(R, D)$ injektiv ist. Denn Satz 1.2.9 (iii) impliziert die Isomorphie von Funktoren

$$\text{Hom}_R(-, \text{Hom}_{\mathbb{Z}}(R, D)) \cong \text{Hom}_{\mathbb{Z}}(R \otimes_R -, D) \cong \text{Hom}_{\mathbb{Z}}(-, D).$$

Man beachte, dass beim letzten Funktor der Vergissfunktors von R -Moduln zu abelschen Gruppen im ersten Argument angewandt werden muss. Da D teilbar ist, ist die abelsche Gruppe D 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 der Modul $\text{Hom}_{\mathbb{Z}}(R, D)$ injektiv.

- Als zweites wollen wir uns überlegen, dass jeder R -Modul M injektiv in ein Produkt von Kopien von R^* abgebildet werden kann. Dazu erinnern wir uns an die Tatsache aus Beispiel 2.2.5, dass die Konduktion der rechtsadjungierte Funktor zum Vergessensfunktors ist, es also eine Isomorphie von abelschen Gruppen

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

gibt.

- Da die abelsche Gruppe \mathbb{Q}/\mathbb{Z} Torsionselemente beliebiger Ordnung enthält, existiert für jede abelsche Gruppe M ein nichtverschwindender Gruppensomorphismus nach \mathbb{Q}/\mathbb{Z} .

Daraus folgt mit der vorangegangenen Überlegung, dass es für jeden vom Nullmodul verschiedenen R -Modul M einen nicht-verschwindenden Morphismus von R -Moduln $M \rightarrow \text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) \cong R^*$ gibt.

- Als nächsten Zwischenschritt verschaffen wir uns jetzt einen Morphismus von R -Moduln $M \rightarrow R^*$, 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 vorangegangenen Überlegung insbesondere einen nicht-verschwindenden Morphismus $\alpha_m : \langle m \rangle \rightarrow R^*$. Da R^* injektiv ist, gibt es eine Ausdehnung β_m auf M , so dass das Diagramm

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle m \rangle & \longrightarrow & M \\ & & \alpha_m \downarrow & \swarrow \beta_m & \\ & & R^* & & \end{array}$$

kommutiert. Dann gilt $\beta_m(m) = \alpha_m(m) \neq 0$.

- Im letzten Schritt verwenden wir die universelle Eigenschaft des Produkts, um alle Homomorphismen β_m zu einem einzigen zusammenzufassen:

$$\beta : M \rightarrow \prod_{m \in M \setminus \{0\}} R^* .$$

Für diesen gilt $\beta(m) \neq 0$, da der Morphismus β_m in die m -te Komponente für m einen von Null verschiedenen Wert liefert. Also ist β injektiv und somit ein Monomorphismus.

Satz 2.4.4.

1. Sei \tilde{R} regulär. Dann ist ein R -Modul genau dann projektiv, wenn er direkter Summand in einer direkten Summe $\bigoplus_{i \in I} \tilde{R}$ ist.
2. Sei R^* koregulär. Dann ist 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. Ist M injektiv, so spaltet die exakte Sequenz $0 \rightarrow M \rightarrow \prod_{i \in I} R^*$, 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 . \square

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

$$\Gamma := \begin{array}{ccc} & X & \\ & \downarrow f & \\ Y & \xrightarrow{g} & M \end{array} .$$

Als Morphismen von Hakendiagrammen betrachten wir kommutierende Diagramme der Form

$$\begin{array}{ccccc} & X & & & \\ & \downarrow & \searrow & & \\ Y & \longrightarrow & M & & X' \\ & \searrow & \downarrow & \swarrow & \\ & Y' & \longrightarrow & M' & \end{array} .$$

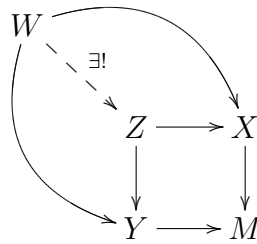
2. Für ein gegebenes Hakendiagramm Γ betrachten wir eine Kategorie \mathcal{C}_Γ , deren Objekte kommutierende Diagramme $\Gamma(W)$ der Form

$$\begin{array}{ccc} W & \longrightarrow & X \\ \downarrow & & \downarrow f \\ Y & \xrightarrow{g} & M \end{array}$$

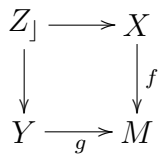
Die Morphismen $\Gamma(W') \rightarrow \Gamma(W)$ sind Morphismen $W' \rightarrow W$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} & & & & \\ & & & & \\ & & & & \\ W' & \searrow & & \searrow & \\ & & W & \longrightarrow & X \\ & \searrow & \downarrow & & \downarrow f \\ & & Y & \longrightarrow & M \\ & \swarrow & & \swarrow & \\ & & & & \end{array}$$

Ein terminales Objekt in der Kategorie \mathcal{C}_Γ heißt ein Pullback für das Hakendiagramm Γ . Es erfüllt also die folgende universelle Eigenschaft: für jedes Diagramm $\Gamma(W)$ über dem Hakendiagramm Γ gibt es genau einen Morphismus $W \rightarrow Z$ in \mathcal{C} , so dass das Diagramm

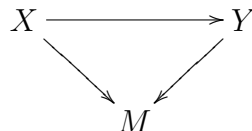


kommutiert. Wir schreiben dann auch $Z = X \times_M Y = X \times_f \times_g Y$ oder



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 \mathcal{C} . Die Überkategorie $\mathcal{C} \downarrow M$ der Objekte über M ist definiert als die Kategorie, deren Objekte Paare (X, f) sind mit X einem Objekt in \mathcal{C} und einem Morphismus $f : X \rightarrow M$, und deren Morphismen kommutierende Diagramme



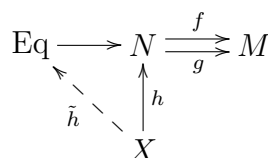
sind. Die Pullbacks $\cdot \times_M \cdot$ sind dann genau die Produkte in der Überkategorie über M . Sie werden daher auch Faserprodukte über M genannt.

3. In den Kategorien $\text{Set}, \text{Top}, \text{Ab}, R\text{-Mod}$ ist der Pullback gegeben durch

$$X \times_M Y := \{(x, y) \mid x \in X, y \in Y, f(x) = g(y)\}.$$

Der Strukturmorphismus $X \times_M Y \rightarrow X$ ist die Projektion $(x, y) \mapsto x$ auf die erste Komponente, der Strukturmorphismus $X \times_M Y \rightarrow Y$ ist die Projektion $(x, y) \mapsto y$. Der Morphismus $Z \rightarrow X \times_M Y$, der durch zwei geeignete Morphismen $f : Z \rightarrow X$ und $g : Z \rightarrow Y$ induziert wird, ist gegeben durch $z \mapsto (f(z), g(z))$.

Dies ist ein Beispiel eines Differenzkerns: seien $f, g : N \rightarrow M$ zwei Morphismen. Dann ist der Differenzkern ein Morphismus $\text{Eq} \rightarrow N$, so dass im Diagramm



für jeden Morphismus h mit $f \circ h = g \circ h$ ein eindeutiger Morphismus $\tilde{h} : X \rightarrow \text{Eq}$ existiert. In einer additiven Kategorie ist der Differenzkern gerade der Kern der Differenzabbildung $\delta(x, y) := f(x) - g(y)$.

In den Kategorien $\text{Set}, \text{Top}, \text{Ab}, R\text{-Mod}$ ist der Pullback also der Differenzkern

$$X \times_M Y := \text{Eq} \left(X \times Y \begin{array}{c} \xrightarrow{f \circ pr_1} \\ \xrightarrow{g \circ pr_2} \end{array} M \right) .$$

4. Wenn Pullbacks existieren, liefern sie einen Funktor von der Kategorie der Hakendiagramme in \mathcal{C} nach \mathcal{C} . Hierzu betrachten wir das kommutierende Diagramm

$$\begin{array}{ccccc} X \times_M Y & \longrightarrow & X & & \\ \downarrow & & \downarrow & \searrow & \\ Y & \longrightarrow & M & & X' \\ & \searrow & \downarrow & \searrow & \downarrow \\ & & Y' & \longrightarrow & M' \end{array} .$$

Die äußeren Pfeile liefern übereinstimmende Morphismen $X \times_Y X \rightarrow Y' \rightarrow M$ und $X \times_Y X \rightarrow X' \rightarrow M$, die nach der universellen Eigenschaft des Pullbacks $X' \times_M Y'$ einen eindeutigen Morphismus $X \times_M Y \rightarrow X' \times_M Y'$ induzieren.

5. Wir sehen auch, dass im Falle der Existenz von Pullbacks ein Morphismus $M \xrightarrow{g} M'$ einen Funktor der Überkategorien

$$g^* : \mathcal{C} \downarrow M' \rightarrow \mathcal{C} \downarrow M$$

liefert, der das Objekt $X \rightarrow M'$ auf das Objekt $X \times_{M'} M \rightarrow M$ in der Kategorie $\mathcal{C} \downarrow M$ abbildet:

$$f^*(X) = \begin{array}{ccc} X \times_{M'} M & \longrightarrow & X \\ \downarrow & & \downarrow \\ M & \xrightarrow{g} & M' \end{array}$$

Wir nennen dann g^* auch den Pullbackfunktor zu dem Morphismus g .

6. Falls in dem Diagramm

$$\begin{array}{ccccc} X_2 & \longrightarrow & X_1 & \longrightarrow & X_0 \\ \downarrow & & \downarrow & & \downarrow \\ M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 \end{array}$$

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

$$\begin{array}{ccccc} Y & & & & \\ \downarrow & \searrow & & \searrow & \\ (X_0 \times_{M_0} M_1) \times_{M_1} M_2 & \longrightarrow & X_0 \times_{M_0} M_1 & \longrightarrow & X_0 \\ \downarrow & & \downarrow & & \downarrow \\ M_2 & \xrightarrow{f_1} & M_1 & \xrightarrow{f_0} & M_0 \end{array}$$

für ein beliebiges Objekt Y und geben uns Morphismen $Y \rightarrow X_0$ und $Y \rightarrow M_2$ vor, so dass das äußerste Rechteck kommutiert. Die Pullback-Eigenschaft des rechten Diagramms, angewandt auf die Morphismen $Y \rightarrow X_0$ und $Y \rightarrow M_2 \xrightarrow{f_1} M_1$ liefert uns einen eindeutigen Morphismus $Y \rightarrow X_0 \times_{M_0} M_1$. Auf diesen und auf $Y \rightarrow M_2$ wenden wir nun die Pullback-Eigenschaft des rechten Diagramms an und erhalten einen eindeutigen Morphismus $Y \rightarrow (X_0 \times_{M_0} M_1) \times_{M_1} M_2$, der zeigt, dass auch das große Diagramm ein Pullback-Diagramm ist.

7. Dieses Resultat hat eine wichtige Uminterpretation für die Pullbackfunktoren: gegeben Morphismen $M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2$, gibt es eine ausgezeichnete natürliche Transformation

$$(f_0 \circ f_1)^* \Rightarrow f_1^* \circ f_0^* .$$

Man beachte, dass hier i.a. keine Gleichheit vorliegt. Man kann zeigen, dass dann die sogenannte Kohärenzbedingung gilt, dass das folgende Diagramm von natürlichen Transformationen kommutiert

$$\begin{array}{ccc} (f_0 \circ f_1 \circ f_2)^* & \Longrightarrow & f_2^* \circ (f_0 \circ f_1)^* \\ \Downarrow & & \Downarrow \\ (f_1 \circ f_2)^* \circ f_0^* & \Longrightarrow & f_2^* \circ f_1^* \circ f_0^* \end{array}$$

Definition 2.5.3

Dual zum Pullback definieren wir den Pushout eines Diagramms

$$\begin{array}{ccc} N & \xrightarrow{f} & A \\ g \downarrow & & \\ & & B \end{array}$$

als Diagramm

$$\begin{array}{ccc} N & \xrightarrow{f} & A \\ g \downarrow & & \downarrow \\ B & \longrightarrow & W \end{array}$$

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 $f : N \rightarrow X$. Die Pushouts sind dann gerade die Koproducte in der Unter-Kategorie. Sie werden auch amalgamierte Summen genannt.
2. In der Kategorie $R\text{-Mod}$ ist der Pushout gegeben durch den Quotientenmodul

$$A \sqcup_N B = A \oplus B / (f(n), 0) \sim (0, g(n)) .$$

Der Strukturmorphismus $A \rightarrow A \sqcup_N B$ ist die Injektion $a \mapsto [a, b]$ in die erste Komponente. Der Morphismus $A \sqcup_N B \rightarrow Z$, der durch zwei geeignete Morphismen $f : A \rightarrow Z$ und $g : B \rightarrow Z$ 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 Differenzkern der Abbildungen

$$A \sqcup_N B := \text{CoEq}(N \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} A \amalg B)$$

in das Koproduct, 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. Es stellt sich heraus, dass auch hier eine vollständige Beschreibung zu erreichen ist. Dazu müssen wir zunächst etwas mehr über die interne Struktur dieser Ringe lernen.

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 $\text{rang}(U) \leq \text{rang}(M)$.

Das Beispiel $n\mathbb{Z} \subsetneq \mathbb{Z}$ von \mathbb{Z} -Moduln zeigt, dass auch bei echten Untermoduln Gleichheit auftreten kann.

Beweis.

Wir führen den Beweis nur für den Fall, dass der Rang von M endlich ist, durch Induktion nach $\text{rang} M =: n$. Im allgemeinen Fall benutzt man das Zornsche Lemma. Für $n = 0$ ist $M = 0$, also ist nichts zu zeigen. Sei $\{x_1, \dots, x_n\}$ eine Basis von M . Die Teilmenge von R

$$\mathfrak{a} := \left\{ \beta \in R \mid \text{es gibt } \beta_2, \dots, \beta_n \in R, \text{ so dass } \beta x_1 + \sum_{i=2}^n \beta_i x_i \in U \right\}$$

ist ein Ideal von R und daher im Hauptidealring R von der Form $\mathfrak{a} = (\alpha_1)$. Fixiere irgendwelche $\alpha_2, \dots, \alpha_n \in R$, so dass

$$\alpha_1 x_1 + \sum_{i=2}^n \alpha_i x_i \in U .$$

Wir nennen diese Linearkombination u ; beachte $u \in U$.

Da $\{x_i\}$ eine Basis von M ist, besitzt jedes $v \in U$ eine (eindeutige) Darstellung

$$v = \rho_1 x_1 + \sum_{i=2}^n \rho_i x_i \quad \text{mit } \rho_i \in R .$$

Offenbar liegt dann aber $\rho_1 \in \mathfrak{a}$, ist also von der Form $\rho_1 = \rho \alpha_1$ mit $\rho \in R$. Wir bezeichnen mit

$$M' = \langle x_2, \dots, x_n \rangle$$

den freien Untermodul von M vom Rang $n - 1$. Dann liegt

$$v - \rho u \in U \cap M' =: U' .$$

Nach Induktionsannahme ist der Untermodul U' von M' frei vom Rang $t \leq n - 1$. Sei also

$$\{y_1, \dots, y_t\}$$

eine Basis des Untermoduls U' von M' .

Ist $\alpha_1 = 0$, so ist $\mathfrak{a} = 0$. Dann liegt u in U' und es ist $U' = U$, also ist U frei vom Rang $< n$. Sei also $\alpha_1 \neq 0$. Wir behaupten, dass in diesem Fall $\{u, y_1, \dots, y_t\}$ eine Basis des Untermoduls U ist. Damit ist dieser Untermodul dann auch frei vom Rang $t + 1 \leq n$.

Für beliebiges $v \in U$ fanden wir oben ein $\rho \in R$, so dass

$$v - \rho u \in U'$$

gilt. Also ist $\{u, y_1, \dots, y_t\}$ ein Erzeugendensystem von U , $\langle u, y_1, \dots, y_t \rangle = U$. Um die lineare Unabhängigkeit des Erzeugendensystems zu sehen, betrachte die Linearkombination

$$0 = \gamma u + \sum_{i=1}^t \mu_i y_i \quad \text{mit} \quad \gamma, \mu_i \in R.$$

Wir stellen die Elemente u, y_i des Erzeugendensystems als Linearkombination der Basisvektoren x_i von M dar und erhalten die Gleichung

$$0 = \gamma \alpha_1 x_1 + \sum_{i=2}^n \mu'_i x_i.$$

mit gewissen $\mu'_i \in R$, da $y_i \in U' \subset M' = \langle x_2, \dots, x_n \rangle$. Aus der linearen Unabhängigkeit der Familie $\{x_i\}$ folgt $\gamma \alpha_1 = 0$. Da ein Hauptidealring integer ist, folgt $\gamma = 0$. Da die y_i nach Voraussetzung linear unabhängig sind, folgt dann auch $\mu_i = 0$. \square

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 bei Hauptidealringen wieder freie Moduln. \square

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

$$p : R^n \twoheadrightarrow M$$

mit einem geeigneten $n \in \mathbb{N}$ 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 $\ker p : R^n \rightarrow R^n$ von freien Moduln. Wir finden einen Isomorphismus

$$M \cong R^n / \ker p \cong \text{coker } \ker p .$$

Dies heißt, dass wir den endlich erzeugten Modul M ausschließlich durch den Morphismus $\ker p$ zwischen 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 freie 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 ,

$$M : \text{Hom}_R(R^n, R^m) \rightarrow M(m \times n, R)$$

vgl. Bemerkung 1.3.2 6. Die Spalten der Matrix $M(f) = (a_{ij})$ sind die Bilder unter f der Vektoren e_1, \dots, 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 f ein Isomorphismus von abelschen Gruppen. Die Matrizenmultiplikation entspricht dann der Verknüpfung von Abbildungen. Ein R -Modulmorphismus φ 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 f ein Morphismus 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

$$\det A = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

Man kann natürlich die gleiche Formel auch für Matrizen mit Einträgen in einem nicht-kommutativen 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 Matrizen mit Einträgen in einem Körper aus der linearen Algebra vertraut. Da der Integritätsbereich

$$\mathbb{Z}[X_{ij}, Y_{ij}]_{1 \leq i, j \leq n}$$

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 $f : M \rightarrow N$ 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

$$d_{11} \mid d_{22} \mid d_{33} \dots \mid d_{rr}$$

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 XAY die gewünschte 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 $\langle a_{11} \rangle \subsetneq \langle A \rangle$ invertierbare Matrizen X und Y liefert, so dass das Ideal echt größer wird, $\langle (XAY)_{11} \rangle \supsetneq \langle a_{11} \rangle$. 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 ersten 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 weiteren Zeilen und Spalten auf.

- Für das Verfahren zur Vergrößerung des Ideals 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:

$$\begin{aligned} d &= xa_{11} + ya_{12} \\ a_{11} &= d\lambda \\ a_{12} &= d\mu. \end{aligned}$$

Da Hauptidealringe nullteilerfrei sind, folgt hieraus insbesondere $1 = x\lambda + y\mu$. Wir betrachten nun das Produkt der folgenden zwei Matrizen:

$$\left(\begin{array}{cc|c} a_{11} & a_{12} & * \\ * & * & * \\ \hline & * & * \end{array} \right) \left(\begin{array}{cc|c} x & -\mu & 0 \\ y & \lambda & I \\ \hline & & \end{array} \right) = \left(\begin{array}{cc|c} d & * & * \\ * & * & * \\ \hline & * & * \end{array} \right)$$

Die rechte Matrix Y auf der linken Seite hat Determinante Eins, ist also in R 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 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r \subsetneq R$ von Idealen von R , so dass

$$M \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r.$$

Hierbei ist $\mathfrak{a} = 0$ ist zugelassen und $R/0 \cong R$ als R -Modul.

Beweis.

Wir hatten schon in Betrachtung 3.1.3 gesehen, dass es einen Morphismus $f : R^n \rightarrow R^m$ 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

$$\begin{array}{ccc} R^n & \xrightarrow{f} & R^m \\ X \uparrow & & \downarrow Y \\ R^n & \xrightarrow{D} & R^m \end{array}$$

kommutiert und D eine Diagonalmatrix ist, deren Element die Teilbarkeitsbeziehung $d_{11}|d_{22}|\dots|d_{rr}$ mit $r = \min(m, n)$ erfüllen. Es folgt die Isomorphie von R -Moduln:

$$M \cong R^m / \text{Im } D \cong R/d_{11}R \times \dots \times R/d_{rr}R \times R^{m-r}$$

Schließlich dürfen wir Faktoren mit $d_{ii} \in R^\times$ weglassen. Hieraus folgt die Existenz der angegebenen Zerlegung. \square

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 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots \subseteq \mathfrak{a}_r$ von Idealen in R , so dass

$$M \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \dots \times R/\mathfrak{a}_r .$$

(ii) Dann gibt es Primpotenzen q_1, \dots, q_t in R derart, dass gilt

$$M \cong R^s \times R/q_1R \times \dots \times R/q_tR . \tag{6}$$

Dann ist $s \in \mathbb{N}_0$ wohlbestimmt, d.h. es hängt nicht von der Wahl der Zerlegung (6) 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 α_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:

$$R/\alpha_i \cong R/q_1^{(i)} \times R/q_2^{(i)} \times \dots \times R/q_s^{(i)} .$$

- 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 $Q := \text{Quot}(R)$ der Quotientenkörper von R . Dann ist $\text{Hom}_R(M, Q)$ ein Q -Vektorraum. Nach der universellen Eigenschaft 1.2.2 (i) der direkten Summe ist

$$\text{Hom}_R(M, Q) \cong \text{Hom}_R(R/q_1R, Q) \times \dots \times \text{Hom}_R(R/q_tR, Q) \times \text{Hom}_R(R, Q)^s .$$

Nach Satz 1.1.9 (iv) ist $\text{Hom}_R(R, Q) \cong Q$. Sei \mathfrak{a} ein von Null verschiedenes Ideal von R . Dann ist wegen der universellen Eigenschaft des Quotientenmoduls

$$\text{Hom}_R(R/\mathfrak{a}, Q) \cong \{f \in \text{Hom}_R(R, Q) \mid f|_{\mathfrak{a}} = 0\} .$$

Jeder Modulhomomorphismus $f : R \rightarrow Q$, 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 Nullmorphimus, 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 (6) ab.

- Wir verwenden eine ähnliche Strategie, um auch die Unabhängigkeit der Primzahlpotenzen zu zeigen. Dafür betrachten wir für $p \in R$ irreduzibel 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:

$$R \xrightarrow{p^{n-1}} p^{n-1}R \twoheadrightarrow p^{n-1}R/p^nR.$$

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^nR .

Für $m > n$ ist $p^{n-1}(R/p^mR) = 0$. Für $m \leq n$ finden wir ähnlich eine Surjektion

$$R \twoheadrightarrow R/p^mR \xrightarrow{p^{n-1}} p^{n-1}(R/p^mR) \twoheadrightarrow p^{n-1}(R/p^mR)/p^n(R/p^mR)$$

mit Kern pR . Also gilt

$$d_p^n(R/p^mR) = \begin{cases} 0 & \text{für } m > n \\ 1 & \text{für } m \leq n. \end{cases}$$

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

$$d_p^n(M) = s + |\{i \mid q_i \text{ teilt } p^n\}|,$$

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 nur als Quotient 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.

1. Dann gibt es genau eine Folge von natürlichen Zahlen $d_1, d_2, \dots, d_s \in \{0, 2, 3, 4, \dots\}$ mit $d_i \mid d_{i+1}$ für $i = 1, \dots, s-1$, derart, dass gilt

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_s}$$

Hierbei beachte man, dass $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ zugelassen ist.

2. Dann gibt es Primzahlpotenzen q_1, \dots, q_t und eine natürliche Zahl $r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}_{q_1} \times \dots \times \mathbb{Z}_{q_t} \times \mathbb{Z}^r$$

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 keinesfalls eindeutig als Untergruppen von G . Mit anderen Worten: 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 Invariantenteiler des Endomorphismus A .

- Für jedes $\bar{v} \in K[X]/\mathfrak{a}_i$ folgt

$$f_r \cdot \bar{v} = \overline{f_r \cdot v} = 0,$$

also $f_r(A) = 0$. Umgekehrt wirken auf dem Summanden $K[X]/(f_r)$ genau die Vielfachen von f_r durch Null. Daher ist f_r das Polynom kleinsten Grades, für das $f(A) = 0$ gilt, also das Minimalpolynom von A .

- Wir geben noch für jeden Summanden $K[X]/(f)$ die Wirkung des Endomorphismus explizit an. Dazu sei

$$f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0.$$

Wähle als K -Basis von $K[X]/(f)$ die Restklassen $b_i := \overline{X^i}$ mit $i = 0, \dots, n-1$. Dann gilt $X \cdot b_i = b_{i+1}$ für $i = 0, \dots, n-1$ und $X \cdot b_{n-1} = -\sum_{i=0}^{n-1} a_i b_i$. 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 $A : V \rightarrow V$ 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 einen Isomorphismus von $K[X]$ -Moduln

$$V \cong K[X]/(X - \lambda_1)^{n_1} \times \dots \times K[X]/(X - \lambda_t)^{n_t}$$

mit $n_i \in \mathbb{N}$ und $\lambda_i \in K$ für $i = 1, \dots, t$. 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. \square

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 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 Inklusionen:

$$\begin{aligned} M \text{ projektiv} &\Leftrightarrow M \text{ direkter Summand in } \bigoplus_{\text{endl.}} R \\ &\Leftrightarrow M \text{ direkter Summand in } \prod_{\text{endl.}} R \\ &\Leftrightarrow M \text{ injektiv} \end{aligned}$$

Die erste und letzte Inklusion folgen dabei sofort aus Satz 2.4.4. □

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 $R^* := \text{Hom}_K(R, K)$, der durch die Rechtswirkung von R auf sich selbst induziert wird. Dann ist der R -Modul R^* injektiv.

Beweis.

Wir wollen dazu die Äquivalenz der Funktoren $\text{Hom}_R(-, R^*)$ und $\text{Hom}_K(-, K)$ zeigen. Für einen beliebigen R -Modul M gilt:

$$\text{Hom}_R(M, R^*) \equiv \text{Hom}_R(M, \text{Hom}_K(R, K)) \cong \text{Hom}_K(R \otimes_R M, K) \cong \text{Hom}_K(M, K).$$

Die zweite Isomorphie folgt, da beide Räume K -bilineare Abbildungen $M \times R \rightarrow K$ beschreiben. Im letzten Ausdruck ist implizit ein Vergessensfunktorkontrahent von R -Moduln auf K -Vektorräumen. Also haben wir die Äquivalenz von Funktoren $\text{Hom}_R(-, R^*)$ und $\text{Hom}_K(-, K)$. Der Funktor $\text{Hom}_K(-, K)$ ist exakt, da der Körper K als Modul über sich selbst injektiv ist. Man beachte,

dass in diesem Schritt einget, dass wir über einem Körper arbeiten. Wegen der Isomorphie der Funktoren ist auch $\text{Hom}_R(-, R^*)$ exakt, also R^* ist injektiv. \square

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. Dann ist die K -lineare Abbildung

$$\begin{aligned} \Phi : R^* &\rightarrow R \\ f &\mapsto \sum_{g \in G} f(\delta_g) \delta_{g^{-1}}, \end{aligned}$$

ein Isomorphismus von R -Moduln. Hierbei ist δ_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 Φ die Frobenius-Abbildung.

Beweis.

Wir rechnen nach, dass Φ ein Morphismus von R -Moduln ist: für $g_0 \in G$ gilt

$$\Phi(g_0 \cdot f) = \sum_{g \in G} f(\delta_{g g_0}) \delta_{g^{-1}} = \sum_{\tilde{g} \in G} f(\delta_{\tilde{g}}) \delta_{g_0 \tilde{g}^{-1}} = g_0 \Phi(f).$$

Die Abbildung Φ ist surjektiv, denn ein Urbild von $g \in R$ ist gegeben durch $\delta_g \in R^*$ mit $\delta_g(g') = \delta_{gg'}$. Man beachte, dass die Summe deswegen sinnvoll ist, weil die Gruppe endlich ist. Also ist die Abbildung Φ ein Isomorphismus von R -Moduln. \square

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 2.3.12 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 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 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 $M = \sum_{i \in I} M_i$ Summe einfacher Untermoduln M_i . Für jede Teilmenge $J \subset I$ betrachten wir die inner Summe von Untermoduln

$$M_J := \sum_{i \in J} M_i.$$

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 $M_J \oplus U$ echter Untermodul von M , so gäbe es wenigstens ein $M_i \not\subset M_J \oplus U$. 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, es ist $D \neq 0$. 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 Modul Rd 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' in Rd einfach. Nach Definition von S ist dann aber $U' \subset S$, 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 sicher 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 kleiner 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 $M \rightarrow M/U$. 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 $R\text{-Mod}$ ist halbeinfach, d.h. alle R -Moduln sind projektiv.*

Beweis.

3. \Rightarrow 2. Sei die Kategorie $R\text{-Mod}$ halbeinfach und M ein R -Modul. Für jeden Untermodul $U \subset M$ hat man eine kurze exakte Sequenz

$$0 \rightarrow U \rightarrow M \rightarrow M/U \rightarrow 0,$$

die nach Satz 1.4.3 spaltet, weil der Modul M/U projektiv ist. Nach Satz 1.4.3 hat dann der Untermodul U ein Komplement in M .

2. \Rightarrow 1. Diese Richtung ist trivial, da 1. ein Spezialfall von 2. ist.

1. \Rightarrow 3. Es ist zu zeigen, dass jeder Modul M projektiv ist, also direkter Summand eines freien Moduls F ist. Nach Satz 1.3.5 ist M homomorphes Bild eines freien Moduls F , betrachte also die exakte Sequenz

$$0 \rightarrow \ker \pi \rightarrow F \xrightarrow{\pi} M \rightarrow 0$$

Der Ring R ist nach Annahme halbeinfach, und somit auch F als direkte Summe. Somit 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, $R = \bigoplus M_i$ mit M_i einfach. Als Ring mit Eins ist R zyklisch als Modul über sich selbst, also endlich erzeugt, hat also endliche Länge. Für einen beliebigen einfachen Modul M betrachte einen Erzeuger $x \in M$ und die Surjektion

$$\begin{aligned} R \cong \bigoplus M_i &\rightarrow M \\ r &\mapsto rx \end{aligned}$$

Dies entspricht einer Familie $(M_i \rightarrow M)$ von Modulmorphisimen. Da M einfach ist, muss wenigstens eine der Abbildungen M_i ungleich Null sein. Sie ist nach dem Schurschen Lemma 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 $\text{soc}(M)$ 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 $\text{irr}(R)$ ein Repräsentantensystem für die Isomorphieklassen einfacher R -Moduln. Dann zerfällt der Sockel $\text{soc}(M)$ als direkte Summe seiner isotypischen Komponenten:

$$\text{soc}(M) = \bigoplus_{E \in \text{irr}(R)} M_E.$$

Beweis.

- Da der Sockel Summe einfacher Moduln ist, ist er nach Satz 4.1.7 halbeinfach.
- Da $\text{soc}(M)$ 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 leer.

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 $b : V \times V \rightarrow \mathbb{C}$, 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, denn es gilt

$$(gv, gw) = \sum_{\tilde{g} \in G} b(\tilde{g}gv, \tilde{g}gw) = (v, w) \quad .$$

□

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 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 nun aus Satz 4.1.7. \square

Diese Technik heißt auch “Weyls Unitaritätstrick”. Im Falle unendlich-dimensionaler Skalarprodukträume 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

$$\pi : V \rightarrow W$$

so dass $\pi \circ i = \text{id}_W$. Das Problem ist, dass π 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 $\psi : V \rightarrow W$:

$$\psi = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1}$$

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 $\psi \in \text{Hom}_G(V, W)$. Außerdem gilt weiterhin

$$\psi \circ i = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1} \circ i = \sum_{g \in G} \frac{1}{|G|} g \circ \pi \circ i \circ g^{-1} = \text{id}_W,$$

wobei wir in der zweiten Gleichheit ausnutzten, dass i ein G -Morphismus ist, und im dritten Schritt $\pi \circ i = \text{id}_W$. 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 $\ker \psi$.

\square

Damit ist im allgemeinen Fall, wenn $\text{char}(K)$ 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

Es stellt sich heraus, dass halbeinfache Ringe bzw. halbeinfache Algebren über einem Körper sehr einfach klassifiziert werden können. Dies wird uns bei der Untersuchung von Gruppenringen im halbeinfachen Fall sehr helfen.

Wir erinnern an das Schursche Lemma: jeder Homomorphismus $\Phi : M_1 \rightarrow M_2$ 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 $\text{End}_R(M)$ 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

$$\text{End}_R(R/I) \cong \text{End}_{R/I}(R/I) \cong R/I$$

d.h. der Endomorphismenring ist im Falle einfacher Moduln über einem kommutativen Ring sogar ein Körper.

Wir überlegen als Nächstes, warum der Endomorphismenring so wichtig ist:

Betrachtung 4.2.2.

Sei M ein R -Modul. Dann ist $\text{End}_R(M)$ ein Ring, dessen Multiplikation die Hintereinanderausführung von Endomorphismen ist. Durch

$$\begin{aligned} \text{End}_R(M) \times M &\rightarrow M \\ (\varphi, m) &\mapsto \varphi(m) \end{aligned}$$

wird M auch ein $\text{End}_R(M)$ -Modul. Jedes $x \in R$ gibt durch Skalarmultiplikation

$$\begin{aligned} \lambda_x : M &\rightarrow M \\ m &\mapsto x.m \end{aligned}$$

ein Element von $\text{End}(M)$, das natürlich mit jedem $\varphi \in \text{End}_R(M)$ vertauscht, also in $\text{End}_{\text{End}_R(M)}(M)$ liegt. Wir haben insbesondere einen Ringhomomorphismus

$$\varphi_{\text{Jac}} : R \rightarrow \text{End}_{\text{End}_R(M)}(M).$$

Wir werden dies benutzen, um einen halbeinfachen Ring R durch die Endomorphismenringe von R -Moduln zu untersuchen. Dabei treten Divisionsringe auf. Wir überlegen uns daher:

Satz 4.2.3.

Sei V ein Modul über einem Divisionsring D und $R := \text{End}_D(V)$. Der Ringhomomorphismus

$$\begin{aligned} \varphi_{\text{Jac}} : D &\rightarrow \text{End}_R(V) \\ d &\mapsto \lambda_d, \end{aligned}$$

wobei $\lambda_d(v) := d.v$ die Skalarmultiplikation mit $d \in D$ ist, ist dann ein Isomorphismus von Ringen.

Beweis.

$d_1v = d_2v$ heißt $(d_1 - d_2)v = 0$. Da für Divisionsringe aus $dv = 0$ mit $d \neq 0$ durch Multiplikation mit d^{-1} folgt $v = 1 \cdot v = d^{-1}dv = 0$, ist die Abbildung offensichtlich injektiv.

Wir überlegen uns zunächst, dass jedes $v \in V$ mit $v \neq 0$ zyklisch für V als R -Modul ist. In der Tat: wir können für jedes $w \in V$ ein $\Phi \in R = \text{End}_D(V)$ finden, so dass $w = \Phi(v)$. (Dies macht man sich klar wie bei Vektorräumen, indem man v zu einer D -Basis von V ergänzt und eine Abbildung auf dieser Basis vorschreibt.)

Um Surjektivität zu zeigen, geben wir uns nun ein $T \in \text{End}_R(V)$ vor. Da V als R -Modul zyklisch ist, können wir T schon allein durch seine Wirkung auf einem $v \in V \setminus \{0\}$ beschreiben. Wir wollen also ein $d \in D$ finden, so dass für dieses v gilt $Tv = dv$. Betrachte dazu einen Projektionsoperator $p : V \rightarrow Dv$ mit $p \in \text{End}_D(V) \cong R$. Einen solchen Projektionsoperator finden wir zum Beispiel, indem wir v zu einer D -Basis von V ergänzen. Wegen $p \in R$ folgt nun aber mit $T \in \text{End}_R(V)$

$$Tv = Tpv = pTv \in Dv$$

und somit die Existenz eines gesuchten d . □

Lemma 4.2.4.

Sei F ein algebraisch abgeschlossener Körper. Wenn D eine endlich-dimensionale Divisionsalgebra über F ist, so gilt $D = F$.

Beweis.

Für jedes $x \in D$ ist die Familie $(1, x, \dots, x^m)$ 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 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 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 $f(X) = X - a$ mit $a \in F$. Daher ist $x = a$ und $D = F$. □

Korollar 4.2.5.

Sei K ein algebraisch abgeschlossener Körper und R eine K -Algebra. Sei M ein einfacher R -Modul endlicher Dimension. Dann ist

$$\begin{aligned} K &\xrightarrow{\sim} \text{End}_R(M) \\ \lambda &\mapsto \lambda \text{id}_M \end{aligned}$$

ein Isomorphismus.

Beweis.

Da K ein Körper ist, wissen wir, dass die Abbildung injektiv ist. Andererseits ist $\text{End}_R(M)$ als Divisionsalgebra über dem algebraisch abgeschlossenen Körper K nach Lemma 4.2.4 isomorph zu K . Somit ist die K -lineare Abbildung auch surjektiv. □

Ein endlich erzeugter halbeinfacher Moduln M hat stets endliche Länge. Denn sei e_1, \dots, e_n ein endliches Erzeugendensystem von M . Jeder der endlich vielen Erzeuger hat nur in endlich vielen Summanden der Zerlegung $M \cong M_1 \oplus \dots \oplus M_r$ in einfache Moduln eine von Null verschiedene Komponente. Es können also nur endlich viele Komponenten getroffen werden.

Satz 4.2.6.

Sei M ein halbeinfacher R -Modul endlicher Länge. Dann ist $\text{End}_R(M)$ isomorph zu einem endlichen Produkt von Matrixringen über Divisionsringen.

Beweis.

Betrachte die Zerlegung $M \cong \bigoplus_{i=1}^k M_i^{n_i}$ in isotypische Komponenten mit $n_i \in \mathbb{N}$ und M_i paarweise nicht isomorphen einfachen R -Moduln. Dann gilt

$$\text{End}_R(M) = \bigoplus_{ij} \text{Hom}(M_i^{n_i}, M_j^{n_j}) \cong \bigoplus_i M(n_i \times n_i, \text{End}_R(M_i)) .$$

Nach Korollar 4.2.1 aus dem Schurschen Lemma ist aber $\text{End}_R(M_i)$ ein Divisionsring. \square

Satz 4.2.7.

Sei D ein Divisionsring und V endlich-dimensionaler D -Modul. Dann ist der Ring $\text{End}_D(V)$ halbeinfach und alle einfachen $\text{End}_D(V)$ -Moduln sind isomorph.

Beweis.

Wie in der linearen Algebra zeigt man, dass V eine D -Basis hat. Wähle eine D -Basis (e_1, \dots, e_n) von V und betrachte

$$\begin{aligned} R := \text{End}_D(V) &\rightarrow V \oplus \dots \oplus V \\ f &\mapsto (f(e_1), \dots, f(e_n)) , \end{aligned}$$

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 $\text{End}_D(V)$ -Modul einfach, also auch halbeinfach ist, ist der Ring $\text{End}_D(V)$ halbeinfach. Nach Satz 4.1.10 ist jeder einfache D -Modul isomorph zu einem Untermodul von D , also isomorph zu V . Jeder $\text{End}_D(V)$ -Modul ist somit direkte Summe einfacher $\text{End}_D(V)$ -Moduln, nämlich von Kopien von V . \square

Theorem 4.2.8 (Theorem von Wedderburn).

Jeder halbeinfache Ring R ist isomorph zu einem endlichen Produkt von Matrixringen über Divisionsringen. Ist R kommutativ, so ist jeder halbeinfache Ring R isomorph zu einem endlichen Produkt von Matrixringen über Körpern.

Beweis.

Da R halbeinfach ist, ist nach Satz 4.2.6

$$\text{End}_R(R) \cong \prod_i M(n_i \times n_i, D_i)$$

für gewisse $n_i \in \mathbb{N}$ und gewisse Divisionsringe D_i . Es gibt aber einen Isomorphismus

$$\begin{aligned} R^{\text{opp}} &\xrightarrow{\sim} \text{End}_R(R) \\ r &\mapsto (\varphi_r : x \mapsto xr) \end{aligned}$$

und daher

$$R \cong (R^{\text{opp}})^{\text{opp}} \cong \prod_i M(n_i \times n_i, D_i)^{\text{opp}} \cong \prod_i M(n_i \times n_i, D_i^{\text{opp}}) ,$$

wobei die letzte Isomorphie durch Transposition folgt. \square

Korollar 4.2.9.

Ein Ring ist genau dann rechts-halbeinfach, wenn er links-halbeinfach ist.

Bemerkungen 4.2.10.

1. Damit ist die Darstellungstheorie eines halbeinfachen Rings R bekannt: die Isomorphieklassen von einfachen Darstellungen 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.
2. Die Zerlegung eines halbeinfachen Rings R

$$R \cong \prod_i M(n_i \times n_i, D_i)$$

ist eindeutig bis auf Reihenfolge.

4.3 Fouriertransformation für Gruppen

Wir wollen nicht von vornherein voraussetzen, dass die Gruppenalgebra halbeinfach ist, und brauchen daher ein weiteres Hilfsmittel. Sei M ein R -Modul. Wir erinnern daran, dass dann M auch ein $\text{End}_R(M)$ -Modul ist und wir einen Ringhomomorphismus

$$\varphi_{\text{Jac}} : R \rightarrow \text{End}_{\text{End}_R(M)}(M)$$

haben.

Satz 4.3.1. (Jacobson'scher Dichtesatz)

Sei R ein Ring und M ein halbeinfacher R -Modul. Wir geben uns $f \in \text{End}_{\text{End}_R(M)}(M)$ und endlich viele Elemente $m_1, \dots, m_r \in M$ 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 $\varphi_{\text{Jac}}(R)$ in $\text{End}_{\text{End}_R(M)}(M)$ dicht sei: Wir können also die Wirkung jedes Morphismus $f \in \text{End}_{\text{End}_R(M)}(M)$ auf endlich vielen Elementen des Moduls wiedergeben durch die Multiplikation mit einem Skalar $x \in R$.

Beweis.

Wir betrachten zunächst den Fall $r = 1$. Da M halbeinfach ist, hat der Untermodul $Rm_1 \subset M$ ein Komplement D . Betrachte also eine Zerlegung

$$M = Rm_1 \oplus D .$$

Die idempotente Abbildung

$$\pi : M \rightarrow Rm_1 \hookrightarrow M,$$

die als Verkettung von kanonischer Surjektion und kanonischer Injektion definiert ist, liegt in $\text{End}_R(M)$. Da $f \in \text{End}_{\text{End}_R(M)}(M)$ liegen soll, gilt

$$f \circ \pi = \pi \circ f ,$$

also

$$f(m_1) = f \circ \pi(m_1) = \pi \circ f(m_1) .$$

Daraus folgt $f(m_1) \in Rm_1$. Es gibt also ein $x \in R$, so dass

$$f(m_1) = xm_1.$$

Für den allgemeinen Fall $r > 1$ betrachten wir die direkte Summe

$$(m_1, \dots, m_r) \in M \oplus \dots \oplus M$$

und die Abbildung

$$f \times f \times \dots \times f,$$

die in der Tat mit allen Elementen von

$$\text{End}_R(M \oplus \dots \oplus M) \cong M(r \times r, \text{End}_R M)$$

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 Matrixring,

$$A = M(n \times n, K).$$

Beweis.

Da K algebraisch abgeschlossen ist und K^n ein einfacher A -Modul sein soll, ist nach dem Schurschen Lemma 1.5.7 $\text{End}_A(K^n) \cong K$. Nach dem Dichtesatz 4.3.1 ist nun A dicht in $\text{End}_K(K^n)$. Da K^n von endlich vielen $m_i \in K^n$ erzeugt wird, folgt die Surjektivität von $\varphi_{\text{Jac}} : A \rightarrow \text{End}_K(K^n)$. □

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 $A \subset \text{End}_K(V)$ ein Teilring derart, dass V einfach ist als A -Modul, so gilt bereits $A = \text{End}_K(V)$. In dieser Sprache lässt sich die Notwendigkeit der Bedingung "algebraisch abgeschlossen" besonders gut einsehen: sind $K \subset L$ Körper und betrachten wir den Teilring $L \subset \text{End}_K(L)$, 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 $L \neq \text{End}_K(L)$.

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

$$K[G] \twoheadrightarrow \text{End}_K(V)$$

Beweis.

Wende den Satz von Wedderburn, Korollar 4.3.2, auf das Bild von $K[G]$ in $\text{End}_K(V)$ an. □

Satz 4.3.5 (Fouriertransformation).

Sei K ein algebraisch abgeschlossener Körper beliebiger Charakteristik und G eine endliche Gruppe. Seien L_1, \dots, L_r die bis auf Isomorphie verschiedenen irreduziblen Darstellungen von G

(i) Die Operation von G definiert eine Surjektion von Ringen

$$F : K[G] \twoheadrightarrow (\text{End}_K L_1) \times \cdots \times (\text{End}_K L_r). \quad (7)$$

(ii) Teilt die Charakteristik von K nicht die Gruppenordnung $|G|$, so ist dies sogar ein Isomorphismus von Ringen.

Beweis.

(i) Der $K[G]$ -Modul $L_1 \oplus \cdots \oplus L_r$, hat den Endomorphismenring

$$\text{End}_{K[G]}(L_1 \oplus \cdots \oplus L_r) = K \times K \times \cdots \times K.$$

Die Surjektivität folgt wieder aus dem Satz von Wedderburn 4.3.2, angewandt auf das Bild des Gruppenrings $K[G]$ unter der Projektion auf einen jeden Faktor.

(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 4.2.8. Alternativ betrachtet man $a \in K[G]$ im Kern der Surjektion. Dann ist auch die Linksmultiplikation mit a die Nullabbildung auf $K[G]$. 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 beachte, dass diese Information nicht ausreicht, um den Gruppenring zu kennen, wenn dieser nicht halbeinfach ist, also wenn $\text{char}(K)$ 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.

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, \dots, 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

$$Z(R) := \{z \in R \mid za = az \quad \forall a \in R\}.$$

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,

$$\dim_K Z(K[G]) = |\text{Isoklassen einfacher Darstellungen}| .$$

Andererseits gilt für ein beliebiges Element $z = \sum_h \lambda_h \delta_h$ im Zentrum $Z(K[G])$ des Gruppenrings:

$$\begin{aligned} z\delta_g &= \sum_{h \in G} \lambda_h \delta_h \cdot \delta_g = \sum_{h \in G} \lambda_{hg^{-1}} \delta_h \\ \delta_g z &= \sum_{h \in G} \lambda_{g^{-1}h} \delta_h . \end{aligned}$$

Also gilt $\lambda_{ghg^{-1}} = \lambda_h$ 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 Satzes. \square

Bemerkung 4.3.8.

Wir wollen noch die Beziehung zur Fouriertransformation erklären. Betrachten wir dafür die abelsche Gruppe aller komplexen Zahlen vom Betrage 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

$$\begin{aligned} L_n : S^1 &\rightarrow \text{GL}(1, \mathbb{C}) \cong \mathbb{C}^\times && \text{für } n \in \mathbb{Z} . \\ z &\mapsto z^n \end{aligned}$$

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. Die Funktion $f \in C^0(S^1)$ operiert auf einer stetigen endlich-dimensionalen Darstellung V durch

$$fv = \int_{S^1} f(z) \rho_V(z)(v) dz \quad \text{für } v \in V$$

insbesondere also auf der irreduziblen Darstellung L_n durch Multiplikation mit

$$\int_{S^1} f(z) z^n dz \in \mathbb{C} ,$$

was genau die Fourierkoeffizienten sind. Die Abbildung aus Satz 4.3.5

$$C^0(S^1) \xrightarrow{\sim} \prod_{n \in \mathbb{Z}} \text{End}_{\mathbb{C}} L_n$$

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 $\text{char } K$ die Gruppenordnung $|G|$ nicht teilt.

Definition 4.4.1

Sei L eine einfache Darstellung von G . Nach 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:

$$e_L : M \rightarrow M = \begin{cases} \text{id}_M & \text{falls } M \cong L \\ 0 & \text{falls } M \text{ einfach, } M \not\cong L \end{cases}$$

Dieses Element

$$e_L = F^{-1}(\text{id}_{\text{End}_K L}) \in K[G]$$

heißt Projektor zur einfachen Darstellung L .

Lemma 4.4.2.

Seien $(L_i)_{i=1 \dots r}$ die irreduziblen Darstellungen von G bis auf Isomorphismus und $e_i \in K[G]$ die zugehörigen Projektoren. Dann gilt

$$\begin{aligned} e_i \cdot e_j &= \delta_{ij} e_i \\ 1 &= e_1 + \dots + e_r \end{aligned}$$

und die e_i bilden eine Basis des Zentrums von $K[G]$.

Beweis.

folgt sofort aus Satz 4.3.5 über die Fouriertransformation. □

Definition 4.4.3

Für eine endlich-dimensionale Darstellung einer Gruppe G auf einem K -Vektorraum V definiert man ihren Charakter

$$\chi_V : G \rightarrow K$$

durch $\chi_V(g) = \text{Tr}_V g \equiv \text{Tr}_V \rho(g)$ 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:

$$\chi_V : K[G] \rightarrow K$$

Es gilt wegen der Linearität der Spur $\chi_V(h) = \text{Tr}_V h$ für jedes $h \in K[G]$.

Wir erinnern an den Isomorphismus von $K[G]$ -Moduln aus Lemma 4.1.5, die Frobenius-Abbildung:

$$\begin{aligned} \Phi : K[G]^* &\rightarrow K[G] \\ f &\mapsto \sum_{g \in G} f(\delta_g) \delta_{g^{-1}}. \end{aligned}$$

Theorem 4.4.4 (Charakter-Projektor-Formel).

Zwischen dem Charakter χ_L und dem Projektor e_L zu einer einfachen Darstellung L besteht die Beziehung

$$e_L = \frac{\dim_K L}{|G|} \Phi(\chi_L).$$

Beweis.

Für jeden $K[G]$ -Modul M haben wir einen Ringhomomorphismus $K[G] \rightarrow \text{End}_K(M)$ und somit eine Abbildung

$$\tau_M : K[G]^* \xrightarrow{\Phi} K[G] \rightarrow \text{End}_K(M)$$

betrachten. Insbesondere ist $K[G]$ wie jeder Ring ein Modul über sich selbst, der sogenannte reguläre Modul. Explizit ist diese Linkswirkung gegeben durch

$$\begin{aligned} \rho_g : K[G] &\rightarrow K[G] \\ \rho_g \left(\sum_{h \in G} \lambda_h \delta_h \right) &= \sum_{h \in G} \lambda_h \delta_{gh}. \end{aligned}$$

Für den regulären Modul gilt daher

$$\chi_{K[G]}(g) = \text{Tr}_{K[G]} \rho_g = \begin{cases} |G| & \text{für } g = e \\ 0 & \text{sonst.} \end{cases}$$

Für eine beliebige Funktion $f \in K[G]^*$ rechnen wir

$$\text{Tr}_{K[G]} (\rho_g \tau_{K[G]}(f)) = \sum_{h \in G} f(h) \text{Tr}_{K[G]} \rho_g \delta_{h^{-1}g} = |G| f(g).$$

Wir suchen diejenige Funktion $f_i \in K[G]^*$, deren Bild unter der Frobenius-Abbildung Φ der i -te Projektor ist, $\Phi(f_i) = e_i$. Für diese Funktion gilt für jeden $K[G]$ -Modul L $\tau_L(f_i) = \rho_L(e_i)$

Indem wir die Isomorphie aus Satz 4.3.5 anwenden, finden wir

$$\begin{aligned} f_i(g) &= \frac{1}{|G|} \text{Tr}_{K[G]} \rho_g \tau_{K[G]}(f_i) \\ &= \frac{1}{|G|} \sum_{j=1}^r \text{Tr}_{\text{End}_K(L_j)} (\rho_g)_* \circ \rho_{L_j}(e_i)_*. \end{aligned} \tag{8}$$

Hierbei haben wir den Isomorphismus F im zweiten Schritt benutzt. Die rechte Seite wertet man leicht mit Hilfe des folgenden Lemmas aus der linearen Algebra aus: \square

Lemma 4.4.5.

Ist L ein endlich-dimensionaler K -Vektorraum und $A : L \rightarrow L$ eine K -lineare Abbildung, so gilt für die Spur der induzierten Abbildung

$$\begin{aligned} A_* : \text{End}_K L &\rightarrow \text{End}_K L \\ \varphi &\mapsto A \circ \varphi \end{aligned}$$

die Beziehung

$$\text{Tr}_{\text{End}_K L} A_* = \dim_K L \cdot \text{Tr}_L A$$

Beweis.

Ohne Beschränkung der Allgemeinheit sei $L = K^n$. Dann ist $\text{End}_K(K^n) \cong M(n \times n, K)$. Die zu A gehörige Matrix muss von links mit einer beliebigen Matrix multipliziert werden. Dabei multipliziert man jeden Spaltenvektor dieser Matrix für sich mit A . Also operiert A_* auf jeder Spalte wie A auf K^n selbst. Daher ist die Matrix von A_* blockdiagonal mit n Blöcken der Gestalt A . \square

Weiter im **Beweis** von 4.4.4:

Aus Gleichung (8) folgt sofort

$$\begin{aligned} f_i(g) &= \sum_{j=1}^r \frac{\dim_K L_j}{|G|} \text{Tr}_{L_j} (\rho_g) \circ \rho_{e_i} \\ &= \frac{\dim_K L_i}{|G|} \chi_i(g) \end{aligned} \quad \square$$

Bemerkungen 4.4.6.

Aus den aus der linearen Algebra bekannten Eigenschaften der Spur folgt sofort:

(i) Der Charakter ist auch Konjugationsklassen konstant, also eine Klassenfunktion:

$$\chi_L(ghg^{-1}) = \chi_L(h) \quad \text{für alle } g, h \in G$$

Wir fassen 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 $V^* = \text{Hom}_K(V, K)$ 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

$$\chi_{V^*}(g) = \chi_V(g^{-1}).$$

Wir definieren auf $K[G]^*$ ein weiteres Produkt, indem wir die Frobenius-Abbildung zum Algebromorphismus erklären:

Definition 4.4.7

Für zwei Funktionen $f_1, f_2 \in K[G]^*$ definieren wir das Konvolutionsprodukt durch

$$\begin{aligned} f_1 \star f_2(h) &:= \Phi^{-1}(\Phi(f_1) \cdot \Phi(f_2))(h) \\ &= \Phi^{-1}(\sum_{h_1 h_2 = h} f_1(h_1) f_2(h_2) \delta_{h_1^{-1} h_2^{-1}})(h) = \sum_{h_1 \cdot h_2 = h} f_1(h_1) \cdot f_2(h_2). \end{aligned}$$

Lemma 4.4.8.

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

$$\chi_{L_i} \star \chi_{L_j} = \delta_{ij} \frac{|G|}{\dim_K L_i} \chi_{L_i}$$

Beweis.

Die Beziehung in $K[G]$

$$e_{L_i} \cdot e_{L_j} = \delta_{ij} e_{L_i}$$

für die Projektoren führt wegen $\chi_L = \frac{|G|}{\dim_K L} \Phi^{-1}(e_L)$ zu der behaupteten Beziehung

$$\begin{aligned}\chi_{L_i} \star \chi_{L_j} &= \frac{|G|^2}{\dim_K L_i \dim_K L_j} \Phi^{-1}(e_{L_i} \cdot e_{L_j}) = \frac{|G|^2}{\dim_K L_i \dim_K L_j} \delta_{ij} \Phi^{-1}(e_i) \\ &= \delta_{ij} \frac{|G|}{\dim_K L_i} \chi_{L_i} .\end{aligned}$$

□

Satz 4.4.9.

Habe K Charakteristik Null. So teilt die Dimension jeder einfachen G -Darstellung die Gruppenordnung $|G|$.

Beweis.

Sei L eine einfache Darstellung. Sei $n = |G|$ die Gruppenordnung. Dann gilt $g^n = 1$. Da der Charakterwert $\chi_L(g)$ als Spur die Summe der Eigenwerte von $\rho(g)$ ist, liegt $\chi_L(g)$ im Ring $\mathbb{Z}[\zeta]$, mit ζ einer primitiven n -ten Einheitswurzel.

Sei $I \subset \mathbb{Z}[\zeta]$ das von den Werten der Charaktere erzeugte Ideal. Aus Lemma 4.4.8 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

$$\frac{|G|}{\dim_K L} \in \mathbb{Z} ,$$

denn nur die Skalarisierung mit einer ganzen Zahl bildet ein Gitter wieder auf sich ab. □

Satz 4.4.10.

Betrachte auf $K[G]^$ die symmetrische Bilinearform*

$$(\varphi, \psi) := \frac{1}{|G|} \sum_{g \in G} \varphi(g) \psi(g^{-1})$$

Die Charaktere bilden eine Orthonormalbasis für den Raum der Klassenfunktionen bezüglich dieser Bilinearform.

Beweis.

Nach Definition des Konvolutionsprodukts gilt

$$(\varphi, \psi) = \frac{1}{|G|} (\varphi \star \psi)(e) \quad \text{mit } e \in G$$

dem neutralen Element. Sei (L_i) ein Repräsentantensystem für die Isomorphieklassen einfacher Darstellungen. Wertet man Lemma 4.4.8 auf dem neutralen Element e aus und beachtet

$$\chi_L(e) = \text{Tr } {}_L \rho_e = \dim_K L ,$$

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 liegt eine Basis für den gesamten Raum der Klassenfunktionen vor. \square

Korollar 4.4.11.

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.

Jede endlich-dimensionale Darstellung ist endliche direkte Summe einfacher Darstellungen. Wir können sogar die Vielfachheit, mit der eine vorgegebene irreduzible Darstellung L in einer Zerlegung der Darstellung V als direkte Summe irreduzibler Darstellungen auftritt, berechnen: gilt $V = \bigoplus_{i=1}^r n_i L_i$, so folgt $\chi_V = \sum_{i=1}^r n_i \chi_{L_i}$ und daher $(\chi_L, \chi_V) = n_L$.

Haben also zwei Darstellungen den gleichen Charakter, so treten die gleichen Multiplizitäten n_i auf, und beide Darstellungen sind zur direkten Summe $\bigoplus_{i=1}^r n_i L_i$ isomorph. \square

Es gibt auch eine umgekehrte Version der Orthogonalitätsbeziehungen, bei der über die r verschiedenen irreduziblen Charaktere von G summiert wird.

Korollar 4.4.12.

Sei $s \in G$ und sei $c(s)$ die Anzahl der Element in der Konjugationsklasse von c . 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.

Sei f_s die Klassenfunktion, die auf der Konjugationklasse von s gleich Eins ist und auf allen anderen Konjugationsklassen verschwindet. Da die Charaktere nach Satz 4.4.10 eine Orthonormalbasis für die Klassenfunktionen bilden, haben wir

$$f_s = \sum_{i=1}^h \lambda_i \chi_i \quad \text{mit} \quad \lambda_i = (f_s, \chi_i) = \frac{c(s)}{|G|} \chi_i(s^{-1}).$$

Daher folgt

$$f_s(t) = \frac{c(s)}{|G|} \sum_{i=1}^h \chi_i(s^{-1}) \chi_i(t) .$$

\square

Korollar 4.4.13.

Betrachtet man auf dem komplexen Gruppenring $\mathbb{C}[G]$ 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 $(V, +, \cdot)$ konstruieren wir dafür einen anderen komplexen Vektorraum $(\overline{V}, +, *)$: als abelsche Gruppe sind beide Vektorräume gleich, $(V, +) = (\overline{V}, +)$, aber die Skalarmultiplikation ist

$$\lambda * v := \overline{\lambda} \cdot v \quad \text{für alle } \lambda \in \mathbb{C}, v \in V.$$

Hierbei ist $\overline{\lambda}$ die zu λ konjugierte komplexe Zahl.

- Ist V eine G -Darstellung, so auch \overline{V} mit der gleichen linearen Abbildung eine G -Darstellung. Bezüglich einer fest gewählten Basis von V wird sie aber durch die komplex konjugierte Matrix dargestellt. Daher gilt

$$\chi_{\overline{V}}(g) = \overline{\chi_V(g)}.$$

- Andererseits wissen wir, dass für die kontragrediente Darstellung gilt

$$\chi_{V^*}(g) = \chi_V(g^{-1})$$

Es reicht also aus, einen Isomorphismus von G -Darstellungen

$$V^* \cong \overline{V}$$

zu konstruieren. Nach Lemma 4.1.14 gibt es ein G -invariantes hermitesches Skalarprodukt auf V . Wir definieren

$$\iota : V^* \rightarrow \overline{V}$$

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. ι ist sogar ein G -Morphismus, denn für alle $g \in G$, $v \in V$ und $\varphi \in V^*$ gilt:

$$\langle v, \iota(g\varphi) \rangle = g\varphi(v) = \varphi(g^{-1}v) = \langle g^{-1}v, \iota(\varphi) \rangle = \langle v, g\iota(\varphi) \rangle.$$

□

Bemerkung 4.4.14.

Wichtige Informationen über die komplexen Darstellungen einer endlichen Gruppe G werden oft 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 4.4.15.

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° 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 Ebenenspiegelung Spur Null hat, jede ebene Drehung um 120° jedoch Spur $-1 = \zeta_3 + \bar{\zeta}_3$ mit ζ_3 einer primitiven dritten Einheitswurzel. Die Orthogonalitätsrelationen aus den Korollaren 4.4.13 und 4.4.12 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

$$\chi_h(g^k) = \exp(2\pi i \frac{kh}{n}) ,$$

wobei wir $h \pmod n$ betrachten. Die Charaktere sind offenbar orthogonal:

$$\frac{1}{n} \sum_{k=1}^{n-1} e^{\frac{2\pi i k}{n}(h-h')} = \delta_{h,h'} \pmod{\mathbb{Z}} .$$

Für das Tensorprodukt dieser Darstellungen sehen wir sofort $\chi_h \chi_{h'} = \chi_{h+h' \pmod n}$. 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 $|C_n| = n$.

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

$$r^n = 1, \quad s^2 = 1 \quad \text{und} \quad rs = sr^{-1} .$$

Die Gruppenelemente sind von der Form r^k, sr^k mit $k \bmod n$. 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
ψ_1	1	1
ψ_2	1	-1
ψ_3	$(-1)^k$	$(-1)^k$
ψ_4	$(-1)^k$	$(-1)^{k+1}$

Um zwei-dimensionale Darstellungen zu finden, wählen wir eine primitive n -te Einheitswurzel $w := \exp(2\pi i/n)$ und setzen für $h \in \mathbb{Z}$:

$$\rho^{(h)}(r^k) = \begin{pmatrix} w^{hk} & 0 \\ 0 & w^{-hk} \end{pmatrix} \quad \rho^{(h)}(sr^k) = \begin{pmatrix} 0 & w^{-hk} \\ w^{hk} & 0 \end{pmatrix}$$

Man sieht sofort, dass wir h nur modulo n betrachten müssen. Ferner liefert das Vertauschen der Basisvektoren e_1 und e_2 der Standardbasis die Isomorphie $\rho^{(h)} \cong \rho^{(n-h)}$. Die Darstellungen $\rho^{(0)}$ und $\rho^{(n/2)}$ sind nicht unzerlegbar, denn die alle Matrizen haben die gemeinsamen Eigenvektoren $e_1 \pm e_2$. Daher gilt

$$\rho^{(0)} \cong \psi_1 \oplus \psi_2 \quad \rho^{(n/2)} \cong \psi_3 \oplus \psi_4 .$$

Für $0 < h < n/2$ sind die Darstellungen $\rho^{(h)}$ irreduzibel, da die Matrix $\rho^{(h)}(r)$ diagonalisierbar mit verschiedenen Eigenwerten ist, so dass diese Matrix und $\rho^{(h)}(s)$ nicht gleichzeitig diagonalisierbar sein können. Wir finden daher weitere Charaktere

$$\chi_h(r^k) = 2 \cos \frac{2\pi kh}{n} \quad \chi_h(sr^k) = 0 \quad \text{für } 1, \dots, n/2 - 1 .$$

Man rechnet nach, dass die Charaktere alle orthogonal im Sinne von Satz 4.4.10 sind, womit klar ist, dass die Darstellungen paarweise nicht isomorph sind. Insbesondere folgt aus der Quadratsumme der Dimensionen

$$|D_{2n}| = 2n = 4 \cdot 1^2 + (n/2 - 1) \cdot 2^2 ,$$

dass wir alle Isomorphieklassen von Darstellungen gefunden haben. Auch die Anzahl der Konjugationsklassen

$$\{e\}, \quad \{r^{n/2}\}, \quad \{r^k, r^{-k}\} \quad k = 1, \dots, \frac{n}{2} - 1$$

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
ψ_1	1	1
ψ_2	1	-1
χ_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 π 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

$$1 \rightarrow H \rightarrow A_4 \rightarrow K \rightarrow 1 .$$

Die Charaktere von drei eindimensionalen irreduziblen Darstellungen finden wir durch Zurückziehen der drei irreduziblen Charaktere von K . Den vierten Charakter finden wir mit Hilfe der Orthogonalitätsrelation.

	1	3	4	4
	1	x	t	t^2
χ_0	1	1	1	1
χ_1	1	1	w	w^2
χ_2	1	1	w^2	w
ψ	3	-1	0	0

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 4.4.16

(i) Die Quaternionen sind die reelle 4-dimensionale unitäre Algebra \mathbb{H} mit Basis 1, i, j, k, wobei die Multiplikation auf den Basiselementen durch die Relationen

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ ij &= k . \end{aligned}$$

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, denn jedes $a_0 + a_1i + a_2j + a_3k \in \mathbb{H} \setminus \{0\}$ hat ein Inverses, $\frac{1}{\sum_i a_i^2} (a_0 - a_1i - a_2j - a_3k)$. 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 Satz 4.2.7, aus dem hervorgeht, dass alle \mathbb{H} -Moduln isomorph zu direkten Summen eines einzigen irreduziblen \mathbb{H} -Moduls sind. Die Verbindung zu komplexen Vektorräumen stellt das folgende Lemma her:

Lemma 4.4.17.

Ein \mathbb{H} -Modul ist äquivalent zu einem komplexen Vektorraum V mit einer antilinearen Abbildung J , für deren Quadrat $J^2 = -\text{id}_V$ gilt.

Beweis.

Sei V ein \mathbb{H} -Modul. Die Wirkung mit $i \in \mathbb{H}$ ist dann die Skalarmultiplikation mit der imaginären Einheit von \mathbb{C} und versieht V mit der Struktur eines komplexen Vektorraums. Setze $J(v) = jv$. Die Eigenschaften von J folgen durch Nachrechnen.

Liegt umgekehrt ein komplexer Vektorraum V mit einer Abbildung J vor, so definiert man die Wirkung des Quaternionens i durch die Wirkung von $i \in \mathbb{C}$ und des Quaternionens j durch die Wirkung von J . □

Satz 4.4.18.

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.

$$V = \mathbb{C} \otimes_{\mathbb{R}} V_{\mathbb{R}} = \text{Ind}_{\mathbb{R}}^{\mathbb{C}}(V_{\mathbb{R}}) .$$

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.

$$V = \text{Res}_{\mathbb{R}}^{\mathbb{H}} V_{\mathbb{H}} .$$

Man sagt dann auch, V sei von quaternionalem Typ.

(c) V ist nicht isomorph zu \bar{V} . In diesem Fall sagt man auch, V sei von komplexem Typ.

Beweis.

Ist $V \cong \bar{V}$, so gilt nach dem Schurschen Lemma 1.5.5

$$\dim_{\mathbb{C}} \text{Hom}_G(V, \bar{V}) = 1 ;$$

sind die Moduln V und \bar{V} nicht isomorph, so gibt es keine nicht-verschwindenden G -Morphismen.

Für einen von Null verschiedenen Homomorphismus $J \in \text{Hom}_G(V, \bar{V})$ gilt

$$Jav = \bar{a}Jv \quad \text{für alle } a \in \mathbb{C}, v \in V$$

d.h. J ist antilinear. Wenden wir die reell-lineare Abbildung, die J unterliegt, zweimal an, so erhalten wir eine komplex lineare Abbildung, auf die wir das Schursche Lemma anwenden können. Daher ist

$$J^2 = \lambda \text{id}_V \quad \text{mit } \lambda \in \mathbb{C}^\times.$$

Wegen

$$\lambda Jv = J^3v = J(J^2v) = J\lambda v = \bar{\lambda}Jv$$

gilt $\lambda = \bar{\lambda}$, also ist λ reell, $\lambda \in \mathbb{R}$. Ersetzen wir J durch ein komplexes Vielfaches J' , also $J' = zJ$ mit $z \in \mathbb{C}^\times$, so ist

$$(J')^2 = zJzJ = |z|^2 J^2 = |z|^2 \lambda \text{id}_V.$$

Wir finden also einen antilinearen G -Isomorphismus J , für den entweder gilt

(a) $J^2 = \text{id}_V$ oder (b) $J^2 = -\text{id}_V$.

Im Falle (a) betrachten wir den reellen Untervektorraum der J -Fixpunkte $V^J \subset V$. Weil die Endomorphismen ρ_g mit J vertauschen, trägt dieser eine reelle G -Darstellung: es gilt

$$J\rho_g v = \rho_g Jv = \rho_g v$$

und somit ist für jedes $g \in G$ auch $\rho_g v \in V^J$. Die Abbildung

$$\begin{aligned} V^J \otimes_{\mathbb{R}} \mathbb{C} &\rightarrow V \\ v \otimes_{\mathbb{R}} (\lambda_1 + i\lambda_2) &\mapsto \lambda_1 v + \lambda_2 i v \end{aligned}$$

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 4.4.17 auf V die Struktur eines \mathbb{H} -Vektorraums. \square

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 $N_1 \subseteq N_2 \subseteq \dots \subseteq N_k \subseteq N_{k+1} \subseteq \dots$ 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) \Rightarrow (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) \Rightarrow (iii) Sei $N \subseteq M$ Untermodul. Wir betrachten die Menge

$$X := \{N' \mid N' \subseteq N \text{ Untermodul von } M, N' \text{ endlich erzeugt}\}$$

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 $x \in N \setminus N_0$, 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) \Rightarrow (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, als Ring 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 $x \in N_k$.

□

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. □

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 $M = \langle a_1, \dots, a_r \rangle$ und sei $F := R^r$. Betrachte die Surjektion

$$\begin{aligned} F = R^r &\twoheadrightarrow M \\ (\alpha_1, \alpha_2, \dots, \alpha_r) &\mapsto \sum_{i=1}^r \alpha_i a_i \end{aligned}$$

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. □

Korollar 5.1.7.

1. *Endlich erzeugte Moduln über Hauptidealringen sind noethersch.*
2. *Die endlich erzeugten abelschen 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 (i).
3. Folgt aus Satz 5.1.1, da eine Untergruppe einer abelschen Gruppe auch ein \mathbb{Z} -Untermodul ist.

□

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 :

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \dots$$

Für diese aufsteigende Idealkette im noetherschen Ring R gibt es ein j , so dass gilt

$$\mathfrak{a}_j = \mathfrak{a}_{j+1} = \dots$$

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. \square

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 rechtsartinsch 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 $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \dots$ 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 noetherschen, da er Hauptidealring ist.)

Wie für noethersche Ringe zeigt man:

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 $\bigoplus_{i=1}^r M_i$ 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 endlich koerzeugt, wenn es zu jeder Familie $(M_i)_{i \in I}$ von Untermoduln mit $\bigcap_{i \in I} M_i = 0$ eine endliche Teilmenge $J \subset I$ mit $\bigcap_{j \in J} M_j = 0$ 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 $\bigcap_{i \in I} M_i = N$ eine endliche Teilmenge $J \subset I$ mit $\bigcap_{j \in J} M_j = N$ 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 $N = \bigcap_{i \in I} M_i$. Setze $X = \{\bigcap_{j \in J} M_j \mid J \subset I \text{ endlich}\}$. 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 $N = \bigcap_{i \in I} M_i$ 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 $M_0 \supset M_1 \supset M_2 \supset \dots$ von Untermoduln von M setze man $N := \bigcap_{i \in \mathbb{N}} M_i$. Weil M/N endlich koerzeugt ist, gibt es eine endliche Teilmenge $J \subset \mathbb{N}$ mit $N = \bigcap_{j \in J} M_j$. 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 einfach, 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 4.2.8.

(5) \Rightarrow (4) Betrachte für den treuen Modul M und für alle n alle R -Modulmorphisamen

$$R \rightarrow M^n .$$

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

$$\begin{aligned} R &\rightarrow M^n \oplus M \\ r &\mapsto (f(r), r.m) \end{aligned}$$

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 $\text{Ann}(M)$ ein beidseitiges Ideal. Da R einfach ist und $1 \notin \text{Ann}(M)$, 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 $\text{End}_K(M) = \text{Kid}_M$ gilt. (Das ist zum Beispiel immer der Fall, wenn K algebraisch abgeschlossen ist.) Dann ist die Strukturabbildung

$$R \rightarrow \text{End}_K(M)$$

surjektiv.

Beweis.

Wir faktorisieren die Strukturabbildung

$$\begin{array}{ccc} R & \longrightarrow & \text{End}_K(M) \\ \downarrow & \nearrow & \\ R/\text{Ann}(M) & & \end{array}$$

Dann ist M ein treuer $R/\text{Ann}(M)$ -Modul, so dass die Abbildung $R/\text{Ann}(M) \rightarrow \text{End}_K(M)$ injektiv ist. Somit ist $R/\text{Ann}(M)$ als K -Algebra endlich-dimensional und insbesondere artinsch. Damit ist $R/\text{Ann}(M)$ ein artinscher Ring, der einfach ist, da M einfacher Modul ist. Nach dem Struktursatz Theorem 5.2.7.2 gilt $R/\text{Ann}(M) \cong \text{End}_K(M)$. \square

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:

$$R \otimes_K R^{\text{opp}} \cong M(n \times n, K) .$$

Beweis.

R ist als R - R -Bimodul ein $R \otimes_K R^{\text{opp}}$ -Modul. Da die beidseitigen Ideale gerade die $R \otimes_K R^{\text{opp}}$ -Untermoduln sind, der Ring R aber einfach ist, ist R als $R \otimes_K R^{\text{opp}}$ -Modul einfach.

Nun gilt

$$\begin{array}{ccc} \text{End}_{R \otimes_K R^{\text{opp}}} R & \rightarrow & Z(R) \\ f & \mapsto & f(1) , \end{array}$$

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

$$\text{End}_{R \otimes_K R^{\text{opp}}} R \cong Z(R) \cong K .$$

Nach dem vorangegangenen Korollar ist dann

$$R \otimes_K R^{\text{opp}} \rightarrow \text{End}_K(R) \cong M(n \times n, K)$$

surjektiv. Bild und Urbild sind K -Vektorräume der gleichen Dimension n^2 , daher ist die Abbildung sogar ein Isomorphismus. \square

6 Auflösungen und abgeleitete Funktoren

Der Funktor $\text{Hom}(U, -)$ ist genau dann exakt, wenn U ein projektives Objekt einer abelschen Kategorie ist; ähnlich ist $\text{Hom}(-, U)$ 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 $P \rightarrow M \rightarrow 0$ aus einem projektiven Objekt P gibt.
2. Sie hat genug injektive Objekte, falls es für jedes Objekt M einen Monomorphismus $0 \rightarrow M \rightarrow I$ in ein injektives Objekt I gibt.

Beispiele 6.1.2.

1. Für jeden Ring R hat die Kategorie $R\text{-Mod}$ 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 der endlichen abelschen Gruppen hat überhaupt keine projektiven und injektiven Objekte, insbesondere nicht genug.

Dazu überlegen wir uns zunächst dass die kurze exakte Sequenz

$$0 \rightarrow \mathbb{Z}_n \rightarrow \mathbb{Z}_{n^2} \rightarrow \mathbb{Z}_n \rightarrow 0$$

nicht spaltet. Daher ist die zyklische Gruppe \mathbb{Z}_n weder projektiv noch injektiv. Jede endliche abelsche Gruppe A lässt sich schreiben als $A = \bigoplus \mathbb{Z}_{n_i} \cong \prod \mathbb{Z}_{n_i}$, 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.

3. Die Kategorie der endlich erzeugten abelschen Gruppen hat zwar genug Projektive (die freie abelsche Gruppe auf einem endlichen Erzeugersystem 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 in der Form $\bigoplus \mathbb{Z}_{n_i} \oplus \mathbb{Z}^n$ schreiben. Wäre sie injektiv, so würde nach Korollar 1.4.15 insbesondere ihre Teilbarkeit folgen. Die explizite Beschreibung zeigt aber, dass endlich-erzeugte abelsche Gruppen nie teilbar sind.

Definition 6.1.3

Sei M ein Objekt in einer abelschen Kategorie \mathcal{C} .

1. Eine projektive Auflösung von M ist eine exakte Sequenz

$$\cdots \rightarrow P_i \rightarrow P_{i-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$$

in der alle Objekte (außer natürlich M) projektiv sind. Der Morphismus

2. Eine injektive Auflösung ist eine exakte Sequenz

$$0 \rightarrow M \rightarrow Q_0 \rightarrow Q_1 \rightarrow \cdots ,$$

in der alle Objekte Q_i injektiv sind.

Freie Auflösungen sind Spezialfälle. Wir haben schon in Betrachtung 3.1.3 gesehen, dass Moduln über Hauptidealringen freie Auflösungen der Länge 1 besitzen,

$$0 \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0 .$$

Lemma 6.1.4.

Hat die Kategorie \mathcal{C} genug Projektive, so hat jedes Objekt 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}^{opp} . Zunächst existiert ein Epimorphismus $P_0 \rightarrow M \rightarrow 0$, da \mathcal{C} genug Projektive hat. Sei $K_0 := \ker(P_0 \rightarrow M)$. Das Objekt K_0 ist im Allgemeinen nicht projektiv, aber wir können einen Epimorphismus $P_1 \rightarrow K_0$ von einem projektiven Objekt P_1 finden. Damit ist die resultierende Sequenz

$$\begin{array}{ccccccc}
 P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & \searrow & & \nearrow & & & \\
 & & K_0 & & & & \\
 & \nearrow & & \searrow & & & \\
 0 & & & & 0 & &
 \end{array}$$

exakt. Iteriert man dieses Verfahren, erhält man offensichtlich eine projektive Auflösung. \square

Bemerkung 6.1.5.

Wir wollen kurz eine Fragestellung vorstellen, in der Auflösungen auftreten. Sei R ein kommutativer Ring und sei $A \in M(p \times q, R)$. Wir wollen das homogene lineare Gleichungssystem $AX = 0$ untersuchen. Konkret könnte man z.B. den Polynomring $R = K[X_1, \dots, X_s]$ in mehreren Variablen über einem Körper betrachten. Das homogene lineare Gleichungssystem ist dann ein Gleichungssystem, das polynomial von s Parametern abhängt.

Wir fassen die Matrix A als Morphismus von freien R -Modul auf:

$$F_1 = R^q \xrightarrow{A} F_0 = R^p$$

und suchen eine Beschreibung von $\ker A$. Lösungen können dann durch einen Morphismus von freien Moduln

$$F_2 \xrightarrow{X} F_1 = R^q$$

mit $A \circ X = 0$ beschrieben werden: jedes Bild eines Elements in F_2 unter X ist eine Lösung. Ist das Bild von X gleich dem Kern von A , so haben wir eine vollständige Parametrisierung der Lösungen gefunden. Im Falle eines noetherschen Rings R , also zum Beispiel für $R = K[X_1, \dots, X_s]$, ist $\ker A$ als Untermodul eines endlich erzeugten Moduls noethersch, und der freie Modul F_2 kann sogar endlich erzeugt gewählt werden. Es gibt also r Erzeugende von Lösungen.

Mit anderen Worten: wir haben den Anfang einer freien Auflösung

$$F_2 \xrightarrow{X} F_1 = R^q \xrightarrow{A} F_0 = R^p \rightarrow R^p/AR^q \rightarrow 0$$

konstruiert. Nun gibt es aber über Ringen, im Gegensatz zu Körpern, wieder Abhängigkeiten der Lösungen in F_2 . Im allgemeinen geht die freie Auflösung weiter:

$$\dots F_3 \rightarrow F_2 = R^r \xrightarrow{X} F_1 = R^q \xrightarrow{A} F_0 = R^p \rightarrow R^p/AR^q \rightarrow 0 .$$

Die Elemente des Moduls F_3 beschreiben also Abhängigkeiten zwischen Lösungen; 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. Man kann auch den Quotientenmodul R^p/AR^q als eine "koordinatenfreie" Version des homogenen linearen Gleichungssystems ansehen.

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

$$\begin{array}{ccccccc} \cdots & \xrightarrow{d_{n+1}} & C_{n+1} & \xrightarrow{d_n} & C_n & \xrightarrow{d_{n-1}} & \cdots \\ & & \downarrow f_{n+1} & & \downarrow f_n & & \\ \cdots & \xrightarrow{d_{n+1}} & D_{n+1} & \xrightarrow{d_n} & D_n & \xrightarrow{d_{n-1}} & \cdots \end{array}$$

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 beschränkten Kettenkomplexe, für die nur endlich viele Objekte C_i nicht das Nullobjekt in \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 $Z_i(C_{\bullet}, d_{\bullet}) := \ker(d_{i-1})$.
2. Die i -Ränder $B_i(C_{\bullet}, d_{\bullet})$ sind definiert als das Bild von d_i .
3. Wegen der Kettenkomplexbedingung $d^2 = 0$ sind die Ränder ein Unterobjekt der Zykel, d.h. der Monomorphismus $B_i \rightarrow C_i$ faktorisiert durch einen Monomorphismus $B_i \rightarrow Z_i$:

$$\begin{array}{ccc} B_i & \longrightarrow & C_i \\ & \searrow & \uparrow \\ & & Z_i \end{array}$$

Die i -te Homologie des Komplexes C_{\bullet} ist definiert als der Quotient

$$H_i(C_{\bullet}, d_{\bullet}) := Z_i/B_i = \ker(d_{i-1})/\text{Im}(d_i) .$$

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 $H_n : Ch_{\mathcal{C}} \rightarrow \mathcal{C}$ 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_* statt $H_*(f)$ geschrieben.

2. Sei $P_\bullet \rightarrow M$ eine projektive Auflösung eines Objekts $M \in \mathcal{C}$. Dann ist der Komplex $P_\bullet \rightarrow 0$ azyklisch. Seine nullte Homologie ist $P_0/(\text{Im}(P_1 \rightarrow P_0)) = P_0/\ker(P_0 \rightarrow M) \cong M$.
3. Sei C_\bullet ein Kettenkomplex, der in nicht-negativen Graden konzentriert ist, der also endet mit $\dots \rightarrow C_1 \rightarrow C_0 \rightarrow 0$. Dann gilt $H_0(C_\bullet) = C_0/\text{Im}(C_1 \rightarrow C_0)$ und wir haben durch die kanonische Surjektion auf den Quotienten einen surjektiven Morphismus $C_0 \rightarrow H_0(C_\bullet)$. Offenbar ist dann

$$\dots \rightarrow C_n \rightarrow C_{n-1} \rightarrow \dots \rightarrow C_0 \rightarrow H_0(C_\bullet) \rightarrow 0$$

ein Komplex. Dieser 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 skalaren Multiplikation mit x einen Kettenkomplex

$$0 \rightarrow R \xrightarrow{x} R \rightarrow 0$$

konstruieren. Dann ist $H_0(C_\bullet) = R/x.R$ und $H_1(C_\bullet) = \{r \in R \mid x.r = 0\} = \text{Ann}_r(x)$.

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 und $H_1(C_\bullet) = \{(r_1, r_2) \in R^2 \mid r_1 a + r_2 b = 0\} / \{(-\lambda b, \lambda a)\}$ 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 $\mathcal{C} = \text{Ab}$:

$$\begin{array}{ccccccc} \dots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 0 & \longrightarrow & \dots \end{array}$$

Grad 2 1 0 -1

ist $h_0(c_0) \in \text{Hom}(g(c_0), f(c_0))$. Ausserdem folgt für einen Morphismus $c_1 \in \text{Hom}(c'_0, c_0)$ 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 $\mathcal{C}(D_\bullet)$

$$\begin{array}{ccc} g(c'_0) & \xrightarrow{g(c_1)} & g(c_0) \\ h_0(c'_0) \downarrow & & \downarrow h_0(c_0) \\ f(c'_0) & \xrightarrow{f(c_1)} & f(c_0) \end{array}$$

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 $\hat{h}|_{\ker d} \subseteq \text{Im } d$, und somit $\hat{h}_* = 0$ in Homologie. \square

Das Beispiel 6.2.3 8. für einen Homologieisomorphismus ist allerdings nicht von dieser Form: alle Kettenabbildungen von dem unteren Komplex in den oberen sind null, also kann es keine Kettenhomotopieäquivalenz geben.

6.3 Das Fundamentallemma der homologischen Algebra

Die folgende Aussage ist zentral für die gesamte homologische Algebra:

Satz 6.3.1.

Sei $f : M \rightarrow N$ ein Morphismus in einer abelschen Kategorie, $P_\bullet \rightarrow M \rightarrow 0$ ein Kettenkomplex aus projektiven Objekten und $N_\bullet \rightarrow N \rightarrow 0$ eine beliebige exakte Sequenz.

1. Dann gibt es eine Fortsetzung $f_\bullet : P_\bullet \rightarrow N_\bullet$ 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

$$\begin{array}{ccc} P_0 & \xrightarrow{d} & M \\ \downarrow & & \downarrow f \\ N_0 & \longrightarrow & N \longrightarrow 0 \end{array}$$

Da P_0 projektiv ist, gibt es eine Fortsetzung von $f \circ d$ zu $P_0 \rightarrow N_0$, so dass das entstehende Diagramm kommutiert. Diese Fortsetzung ist natürlich nicht unbedingt 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 $P_0 \rightarrow N_0$ auf M' ein. Sei $x \in \ker d = M'$, dann gilt $df(x) = f(dx) = f(0) = 0$, also erhalten wir durch Restriktion eine Abbildung $f' : M' \rightarrow N'$. Wir haben also ein neues Diagramm

$$\begin{array}{ccc} P_1 & \longrightarrow & M' \\ \downarrow & & \downarrow f' \\ N_1 & \longrightarrow & N' \longrightarrow 0 \end{array}$$

in dem die untere Zeile wiederum exakt ist. Da auch P_1 projektiv ist, kann man in der gleichen Weise wie vorhin fortfahren und erhält einen Morphismus $P_1 \rightarrow N_1$. Insgesamt finden wir eine Fortsetzung über die gesamte Auflösung.

- 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:

$$\begin{array}{ccccccc} & & & & P_0 & \xrightarrow{d} & M \\ & & & & \downarrow f_0 & & \downarrow 0 \\ N_1 & \xrightarrow{d} & N_0 & \xrightarrow{d} & N & \longrightarrow & 0 \end{array}$$

Da $d \circ f_0 = 0 \circ d = 0$ gilt, können wir f_0 als einen Morphismus $P_0 \rightarrow \ker(N_0 \rightarrow N)$ auffassen. Wegen der Exaktheit von N_\bullet ist der Morphismus $N_1 \rightarrow \ker(N_0 \rightarrow N)$ surjektiv. Im Diagramm

$$\begin{array}{ccc} & & P_0 \\ & \swarrow h_0 & \downarrow \\ N_1 & \longrightarrow & \ker(N_0 \rightarrow N) \longrightarrow 0 \end{array}$$

erhalten wir wegen der Projektivität von P_0 eine Hochhebung $h_0 : P_0 \rightarrow N_1$ über $N_1 \rightarrow \ker(N_0 \rightarrow N) \rightarrow 0$, so dass $d \circ h_0 = f_0$. Ähnlich wie vorher lässt sich das Argument jetzt für $f_1 - h_0 \circ d$ wiederholen:

$$\begin{array}{ccccccc} & & & & P_1 & \xrightarrow{d} & P_0 \\ & & & & \downarrow f_1 & \swarrow h_0 & \downarrow f_0 \\ N_2 & \xrightarrow{d} & N_1 & \xrightarrow{d} & \ker d & \longrightarrow & 0 \end{array}$$

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 $f : P_\bullet \rightarrow P'_\bullet$ und $f' : P'_\bullet \rightarrow P_\bullet$. Dann ist aber auch $f \circ f'$ eine Fortsetzung der Identität id_M zu einem Endomorphismus des Kettenkomplexes P'_\bullet . Eine andere Fortsetzung der Identität id_M ist natürlich auch 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, $F : \mathcal{C} \rightarrow \mathcal{D}$. 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 $F : \mathcal{C} \rightarrow \mathcal{D}$ ein additiver Funktor.

1. Hat \mathcal{C} genug Projektive, so sind die linksabgeleiteten Funktoren $L_n F : \mathcal{C} \rightarrow \mathcal{D}$ von F auf Objekten gegeben durch die Homologie des Komplexes $F(P_\bullet)$:

$$L_n F(X) := H_n(F(P_\bullet)) ,$$

wobei $P_\bullet \rightarrow X$ eine beliebige projektive Auflösung von X ist.

2. Hat \mathcal{C} genug Injektive, so sind die (rechts-)abgeleiteten Funktoren $R^n F : \mathcal{C} \rightarrow \mathcal{D}$ analog auf Objekten definiert:

$$R^n F(X) := H^n(F(I_\bullet)) ,$$

wobei $X \rightarrow I_\bullet$ eine injektive Auflösung ist.

Bemerkungen 6.3.4.

- Die abgeleiteten Funktoren verschwinden offenbar, wenn der Funktor F exakt ist.
- Wegen des Fundamentallemmas 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 folgt auch, dass die abgeleiteten Funktoren wirklich Funktoren sind, also auch auf Morphismen definiert sind. Denn ist $f : X \rightarrow Y$ ein Morphismus, so kann man f bis auf Homotopie in eindeutiger Weise zu einem Morphismus

$f_\bullet : P_\bullet \rightarrow Q_\bullet$ der projektiven Auflösungen P_\bullet und Q_\bullet hochheben. Damit erhält man einen Morphismus $F(f_\bullet) : F(P_\bullet) \rightarrow F(Q_\bullet)$ 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 $P_\bullet \rightarrow X$ eine projektive Auflösung, so impliziert die Rechtsexaktheit von F , dass die Sequenz

$$F(P_1) \rightarrow F(P_0) \rightarrow F(X) \rightarrow 0$$

exakt ist. Also gilt mit Hilfe des Homomorphiesatzes

$$F(X) \cong F(P_0)/(\ker(F(P_0) \rightarrow F(X))) \cong F(P_0)/\text{Im}(F(P_1)) = H_0(F(P_\bullet)) .$$

□

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 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:

$$\begin{array}{ccccccc} M' & \xrightarrow{\iota} & M & \longrightarrow & M'' & \longrightarrow & 0 \\ f' \downarrow & & f \downarrow & & f'' \downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{\iota} & N & \longrightarrow & N'' \end{array}$$

Dann gibt es eine exakte Sequenz

$$\ker f' \rightarrow \ker f \rightarrow \ker f'' \xrightarrow{\partial} \text{coker } f' \rightarrow \text{coker } f \rightarrow \text{coker } f''$$

mit einem Morphismus ∂ , der im Beweis beschrieben wird. Der Name ‘‘Schlangenlemma’’ erklärt sich, wenn man oben die Zeile $\ker f' \rightarrow \ker f \rightarrow \ker f''$ und unten die Zeile $\text{coker } f' \rightarrow \text{coker } f \rightarrow$

coker f'' hinzunimmt:

$$\begin{array}{ccccccc}
 \ker f' & \longrightarrow & \ker f & \longrightarrow & \ker f'' & \dashrightarrow & 0 \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 M' & \xrightarrow{\iota} & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & N' & \xrightarrow{\iota} & N & \longrightarrow & N'' \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & & \text{coker } f' & \longrightarrow & \text{coker } f & \longrightarrow & \text{coker } f''
 \end{array}$$

\dashrightarrow (dashed arrows) connect $\ker f' \rightarrow \ker f''$ to $\text{coker } f' \rightarrow \text{coker } f''$ and $M' \rightarrow M''$ to $N' \rightarrow N''$.

Ist $M' \rightarrow M$ ein Monomorphismus, so auch $\ker f' \rightarrow \ker f$. Ist $N \rightarrow N''$ Epimorphismus, so auch $\text{coker } f \rightarrow \text{coker } f''$.

Beweis.

Durch Diagrammjagd, wobei wir nach dem vollen Einbettungssatz voraussetzen dürfen, dass \mathcal{C} eine 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 ∂ . Sei $m'' \in \ker f''$. Da $M \rightarrow M''$ 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 $f(m_0)$ unter $N \rightarrow N''$ nach 0 abgebildet wird, 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 statt mit m_0 mit $m := m_0 + \iota(m')$ mit $m' \in M'$ gearbeitet, so wäre wegen $n'_0 + f'(m') \mapsto f(m)$ das Element $n'_0 + f'(m')$ ein Urbild von m . Somit ist die Klasse $[n'_0] =: \partial(m'')$ wohldefiniert bis auf ein Bild unter f' , also in $\text{coker } f'$. Nach Konstruktion ist ∂ 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 $\ker f' \rightarrow \ker f$ ist offensichtlich, und die Exaktheit bei $\text{coker } f'$ und $\text{coker } f$ und die Zusatzaussage über die Surjektivität folgen dann durch Übergang zu der opponierten Kategorie \mathcal{C}^{opp} .
- Exaktheit bei $\ker f$. Aus der Exaktheit der oberen Zeile folgt sofort, dass der Kern von $\ker f \rightarrow \ker f''$ im Bild von $\ker f' \rightarrow \ker f$ 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 $N' \rightarrow N$ 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 $\ker f \rightarrow \ker f'' \xrightarrow{\partial} \text{coker } f'$ null ist. Ist m'' das Bild eines Elements $m \in \ker f$ unter $M \rightarrow M''$, so ist $f(m) = 0$ und es gilt nach Konstruktion von ∂ , 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 $f(m)$ 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 . 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 $f(m)$ ist. Also ist δ das gesuchte Urbild von m'' in $\ker f$.

□

Bemerkung 6.4.2 (Natürlichkeit).

Aus der Konstruktion folgt, dass der Schlangenmorphismus ∂ natürlich ist, d.h., wenn wir einen Morphismus von Diagrammen $D_1 \rightarrow D_2$ der obigen Form haben, so kommutiert das Diagramm

$$\begin{array}{ccc} \ker(f''_{D_1} : M''_{D_1} \rightarrow N''_{D_1}) & \xrightarrow{\partial} & \operatorname{coker}(f'_{D_1} : M'_{D_1} \rightarrow N'_{D_1}) \\ \downarrow & & \downarrow \\ \ker(f''_{D_2} : M''_{D_2} \rightarrow N''_{D_2}) & \xrightarrow{\partial} & \operatorname{coker}(f'_{D_2} : M'_{D_2} \rightarrow N'_{D_2}) \end{array}$$

Die Kategorie der Kettenkomplexe $Ch_{\mathcal{C}}$ einer abelschen Kategorie ist wieder eine abelsche Kategorie. Daher ist klar, was eine kurze exakte Sequenz

$$0 \rightarrow M'_{\bullet} \rightarrow M_{\bullet} \rightarrow M''_{\bullet} \rightarrow 0$$

von Kettenkomplexen ist. Insbesondere gilt dann, dass für jedes n die Sequenz $0 \rightarrow M'_n \rightarrow M_n \rightarrow M''_n \rightarrow 0$ exakt ist.

Satz 6.4.3.

Ist $0 \rightarrow M'_{\bullet} \rightarrow M_{\bullet} \rightarrow M''_{\bullet} \rightarrow 0$ eine kurze exakte Sequenz von Kettenkomplexen in \mathcal{C} , so gibt es eine lange exakte Sequenz

$$\dots \rightarrow H_i(M'_{\bullet}) \rightarrow H_i(M_{\bullet}) \rightarrow H_i(M''_{\bullet}) \xrightarrow{\partial} H_{i-1}(M'_{\bullet}) \rightarrow \dots$$

in Homologie.

Beweis.

Wir nehmen wieder an, dass \mathcal{C} eine Unterkategorie der Kategorie der R -Moduln über einem Ring R ist. Das kommutierende Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'_n & \longrightarrow & M_n & \longrightarrow & M''_n \longrightarrow 0 \\ & & d \downarrow & & d \downarrow & & d \downarrow \\ 0 & \longrightarrow & M'_{n-1} & \longrightarrow & M_{n-1} & \longrightarrow & M''_{n-1} \longrightarrow 0 \end{array}$$

zusammen mit dem Schlangenlemma 6.4.1 liefert, weil der Kern des Differential d gerade die Zykel und das Bild die Ränder sind, eine lange exakte Sequenz

$$0 \rightarrow Z_n M' \rightarrow Z_n M \rightarrow Z_n M'' \rightarrow \frac{M'_{n-1}}{B_{n-1} M'} \rightarrow \frac{M_{n-1}}{B_{n-1} M} \rightarrow \frac{M''_{n-1}}{B_{n-1} M''} \rightarrow 0$$

Daher sind die Zeilen exakt in dem kommutierenden Diagramm

$$\begin{array}{ccccccc}
 M'_n/B_n M' & \longrightarrow & M_n/B_n M & \longrightarrow & M''_n/B_n M'' & \longrightarrow & 0 \\
 \downarrow d & & \downarrow d & & \downarrow d & & \\
 0 & \longrightarrow & Z_{n-1} M' & \longrightarrow & Z_{n-1} M & \longrightarrow & Z_{n-1} M''
 \end{array}$$

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. \square

Satz 6.4.4.

1. Sei \mathcal{C} eine abelsche Kategorie mit genug Injektiven, \mathcal{D} eine beliebige abelsche Kategorie und $F : \mathcal{C} \rightarrow \mathcal{D}$ ein linksexakter additiver Funktor. Sei

$$0 \rightarrow M' \xrightarrow{\iota} M \xrightarrow{p} M'' \rightarrow 0$$

eine kurze exakte Sequenz in \mathcal{C} . Dann gibt es eine lange exakte Sequenz in \mathcal{D}

$$0 \rightarrow R^0 F(M') \rightarrow \dots \rightarrow R^i F(M') \xrightarrow{\iota_*} R^i F(M) \xrightarrow{p_*} R^i F(M'') \xrightarrow{\partial} R^{i+1} F(M') \rightarrow \dots$$

2. Hat \mathcal{C} genug Projektive und ist der Funktor F rechtsexakt, dann gibt es eine lange exakte Sequenz in \mathcal{D}

$$\dots \rightarrow L_i F(M') \xrightarrow{\iota_*} L_i F(M) \xrightarrow{p_*} L_i F(M'') \xrightarrow{\partial} L_{i-1} F(M') \xrightarrow{\iota_*} \dots \rightarrow L_0 F(M'') \rightarrow 0$$

Der Homomorphismus ∂ heißt Verbindungshomomorphismus.

Beweis.

Um abgeleitete Funktoren zu berechnen, müssen wir projektive Auflösungen von $P' \rightarrow M', P_\bullet \rightarrow M$ und $P''_\bullet \rightarrow M''$ betrachten. Um Satz 6.4.3 anwenden zu können, sollen aber diese Auflösungen eine kurze exakte Sequenz $0 \rightarrow P'_\bullet \rightarrow P_\bullet \rightarrow P''_\bullet \rightarrow 0$ von Kettenkomplexen bilden, d.h. es soll das Diagramm

$$\begin{array}{ccccccc}
 P'_n & \longrightarrow & P_n & \longrightarrow & P''_n & & \\
 \downarrow & & \downarrow & & \downarrow & & \\
 \vdots & & \vdots & & \vdots & & \\
 \downarrow & & \downarrow & & \downarrow & & \\
 P'_0 & \longrightarrow & P_0 & \longrightarrow & P''_0 & & \\
 \epsilon' \downarrow & & \epsilon \downarrow & & \epsilon'' \downarrow & & \\
 0 & \longrightarrow & M' & \xrightarrow{\iota} & M & \longrightarrow & M'' \longrightarrow 0
 \end{array}$$

kommutieren. Hierbei sind ϵ' und ϵ'' 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 $P'_\bullet \rightarrow M'$ und $P''_\bullet \rightarrow M''$ und setzen $P_i := P'_i \oplus P''_i$ und nehmen als Differential die direkte Summe der Differentiale. Dann ist P_\bullet sicher ein exakter Komplex von projektiven Objekten. Die horizontalen Pfeile sind die kanonischen Injektionen $P'_i \rightarrow P'_i \oplus P''_i$ und die kanonischen Surjektionen $P'_i \oplus P''_i \rightarrow P''_i$.

Es bleibt, $\epsilon : P'_0 \oplus P''_0 \rightarrow M$ zu definieren; dies machen wir komponentenweise: die erste Komponente ist $\iota \circ \epsilon' : P'_0 \rightarrow M$. Für die zweite Komponente beachten wir, dass $M \rightarrow M''$ surjektiv ist, und benutzen die Projektivität von P''_0 , um ϵ'' zu einem Morphismus $P''_0 \rightarrow M$ zu heben. \square

Bemerkungen 6.4.5.

1. Die rechtsabgeleiteten Funktoren eines linksexakten Funktors verschwinden offenbar 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

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'_\bullet & \longrightarrow & M_\bullet & \longrightarrow & M''_\bullet \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N'_\bullet & \longrightarrow & N_\bullet & \longrightarrow & N''_\bullet \longrightarrow 0 \end{array}$$

ein kommutierendes Diagramm von exakten Sequenzen von Kettenkomplexen ist, so erhalten wir einen Morphismus zwischen den zugehörigen langen exakten Sequenzen aus Satz 6.4.3, also eine kommutierende Leiter

$$\begin{array}{ccccccc} \cdots & H_i(M'_\bullet) & \longrightarrow & H_i(M_\bullet) & \longrightarrow & H_i(M''_\bullet) & \xrightarrow{\partial} H_{i-1}(M'_\bullet) \longrightarrow \cdots \\ & \downarrow & & \downarrow & & \downarrow & \downarrow \\ \cdots & H_i(N'_\bullet) & \longrightarrow & H_i(N_\bullet) & \longrightarrow & H_i(N''_\bullet) & \xrightarrow{\partial} H_{i-1}(N'_\bullet) \longrightarrow \cdots \end{array}$$

Wenn

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' \longrightarrow 0 \end{array}$$

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

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & L_i F(M') & \xrightarrow{\iota_*} & L_i F(M) & \xrightarrow{p_*} & L_i F(M'') & \xrightarrow{\partial} & L_{i-1} F(M') & \xrightarrow{\iota_*} & \cdots \longrightarrow L_0 F(M'') \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & L_i F(N') & \xrightarrow{\iota_*} & L_i F(N) & \xrightarrow{p_*} & L_i F(N'') & \xrightarrow{\partial} & L_{i-1} F(N') & \xrightarrow{\iota_*} & \cdots \longrightarrow L_0 F(N'') \rightarrow 0 \end{array}$$

6.5 Tor und Ext

Die wichtigsten abgeleiteten Funktoren sind die von Tensorprodukt und Hom-Funktor.

Definition 6.5.1

Sei R ein Ring.

1. Definiere zu einem R -Rechtsmodul X einen Funktor $F_X : R\text{-Mod} \rightarrow \text{Ab}$ durch $F_X(Y) := X \otimes_R Y$. Dieser Funktor ist rechtsexakt (vgl. Beispiele 2.3.11.3) Seine linksabgeleiteten Funktoren bezeichnen wir mit

$$\text{Tor}_n^R(X, Y) := L_n F_X(Y) .$$

2. Definiere zu einem R -Modul X einen Funktor $G_X : (R\text{-Mod})^{\text{opp}} \rightarrow \text{Ab}$ durch $G_X(Y) := \text{Hom}_R(Y, X)$. G_X ist linksexakt (vgl. Beispiele 2.3.11.5). Seine rechtsabgeleiteten Funktoren bezeichnen wir mit

$$\text{Ext}_R^n(Y, X) := R^n G_X(Y) .$$

In der Definition von Ext wird eine injektive Auflösung in $(R\text{-Mod})^{\text{opp}}$ verwendet. Dies ist aber tatsächlich das gleiche wie eine projektive Auflösung in $R\text{-Mod}$.

Folgende Beobachtungen folgen sofort aus den Definitionen:

- $\text{Tor}_n^R(X, Y) = 0$ für alle Y und $n > 0$ genau dann, wenn der Rechtsmodul X flach ist.
- $\text{Ext}_R^n(Y, X) = 0$ für alle Y und $n > 0$ 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 \mathbb{Z}_n ist gegeben durch

$$0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow \mathbb{Z}_n \rightarrow 0 .$$

Wir berechnen nun $\text{Tor}_k^{\mathbb{Z}}(X, Y)$ für den \mathbb{Z} -Modul $X = \mathbb{Z}_m$. Wegen $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}_m$ ist dies die Homologie des Komplexes

$$0 \rightarrow \mathbb{Z}_m \xrightarrow{n} \mathbb{Z}_m \rightarrow 0$$

Daraus folgt

$$\text{Tor}_k^{\mathbb{Z}}(X, Y) \cong \begin{cases} \mathbb{Z}_{\text{ggT}(m,n)}; & \text{falls } k = 0, 1 \\ 0; & \text{sonst.} \end{cases}$$

Man beachte, dass in der Tat $\text{Tor}_0(X, Y) = X \otimes_{\mathbb{Z}} Y$ gilt, vgl. Lemma 6.3.5.

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 $\text{Tor}_k^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n)$ als Kohomologie des Komplexes

$$0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow 0$$

und finden

$$\text{Tor}_0^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n) \cong \mathbb{Z}_n \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_n \quad \text{und} \quad \text{Tor}_1^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n) = 0 .$$

Der Funktor Tor_1 verschwindet auf endlich erzeugten abelschen Gruppen nur dann nicht, wenn sie einen Torsionsanteil haben, daher sein Name.

2. Eine sehr ähnliche Rechnung zeigt, dass

$$\text{Ext}_{\mathbb{Z}}^k(\mathbb{Z}_m, \mathbb{Z}_n) \cong \begin{cases} \mathbb{Z}_{\text{ggT}(m,n)}; & \text{falls } k = 0, 1 \\ 0; & \text{sonst.} \end{cases}$$

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 (wiederum sogar freie) Auflösung gegeben ist durch:

$$\dots \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{\epsilon} \mathbb{Z}$$

wobei ϵ definiert ist durch $\epsilon(t) = 1$ und $N := 1 + t + \dots + t^{n-1}$. Man rechnet nämlich leicht nach, dass $(1-t)N = 1 - t^n$ gilt, also ein Kettenkomplex vorliegt. Umgekehrt verschwindet die Klasse eines Polynoms $f \in \mathbb{Z}[t]$ in R 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, und umgekehrt. Der Komplex ist also exakt.

Nach Tensorieren der projektiven Auflösung über R mit \mathbb{Z} 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

$$\dots \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \rightarrow 0.$$

Somit gilt

$$\mathrm{Tor}_k^R(\mathbb{Z}, \mathbb{Z}) \cong \begin{cases} \mathbb{Z}; & \text{falls } k = 0 \text{ (vgl. Lemma 6.3.5)} \\ \mathbb{Z}_n; & \text{falls } n \text{ ungerade} \\ 0 & \text{falls } k > 0 \text{ gerade.} \end{cases}$$

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 $\mathrm{Ext}_{\mathbb{Z}}^1(A, \mathbb{Z}) = 0$ 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 Tor' von Tor zu definieren, indem man die erste Variable projektiv auflöst.

Wir zeigen die Isomorphie von Tor und Tor' , indem wir zeigen, dass Tor zu einem dritten Funktor $\underline{\mathrm{Tor}}$ isomorph ist, der offensichtlich symmetrisch in seinen beiden Variablen ist. 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} von \mathcal{C} und Morphismen $d_h : X_{ij} \rightarrow X_{i-1,j}$ und $d_v : X_{ij} \rightarrow X_{i,j-1}$ 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 von X_{ij} .

2. Die Morphismen von Doppelkomplexen sind gegeben durch Familien von Morphismen $f_{ij} : X_{ij} \rightarrow Y_{ij}$, die mit den Differentialen d_h und d_v kommutieren.
3. Assoziiert zu einem Doppelkomplex sind zwei einfache Komplexe

$$|X_{\bullet\bullet}|_n := \coprod_{i+j=n} X_{ij} \quad (\mathrm{Tot} X_{\bullet\bullet})_n := \prod_{i+j=n} X_{ij}$$

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

$$\begin{array}{ccc} X_{i,j} & \xrightarrow{d_h} & X_{i-1,j} \\ \downarrow d_v & & \downarrow d_v \\ X_{i,j-1} & \xrightarrow{d_h} & X_{i-1,j-1} \end{array}$$

kommutiert also nicht. Die Schiefkommutativität der Differentiale, $d_h d_v = -d_v d_h$, stellt vielmehr sicher, dass die Totalkomplexe $|X|$ und $TotX$ wieder Kettenkomplexe sind: Ist $x \in X_{ij}$, so gilt

$$d(dx) = d(d_h x + d_v x) = d_h d_h x + d_h d_v x + d_v d_h x + d_v d_v x = 0.$$

Definition 6.6.3

1. Sei R ein Ring. Seien (P_\bullet, d) ein R^{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 Grad 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 Koszulregel:

Immer, wenn ein Element vom Grad i an einem Element vom Grad j vorbeigeschoben wird, wird ein Vorzeichen $(-1)^{ij}$ eingeführt.

2. Sei (P_\bullet, d) ein R -Kettenkomplex, so definiere den \mathbb{Z} -Doppelkomplex $\text{Hom}_R(P, Q)_{\bullet, \bullet}$ durch

$$\text{Hom}_R(P, Q)_{i,j} := \text{Hom}_R(P_i, Q_j).$$

Hierbei sind die Differentiale des Dopplekomplexes natürlich durch Vorschalten und Nachschalten der Differentiale von P_\bullet und Q_\bullet gegeben.

3. Sei $P_\bullet \rightarrow X$ eine projektive Auflösung von R^{opp} -Moduln, $Q_\bullet \rightarrow Y$ eine projektive Auflösung von R -Moduln. Dann setzen wir

$$\widetilde{\text{Tor}}_n^R(X, Y) := H_n(|P \otimes_R Q|).$$

Wir benötigen noch einen Hilfssatz, um den Komplex zu untersuchen:

Lemma 6.6.4.

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. $|X|$ exakt, falls für ein $N \in \mathbb{Z}$ gilt: $X_{ij} = 0$ für alle Zeilen $j < N$;

2. $TotX$ exakt, falls für ein $N \in \mathbb{Z}$ gilt: $X_{ij} = 0$ für $i < N$.

Die Bedingungen (1) und (2) sind natürlich immer erfüllt, falls X nichtnegativ graduiert ist. Es 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 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

$$|X|_0 = \bigoplus_{n \in \mathbb{Z}} X_{-n,n} = \bigoplus_{n \geq 0} X_{-n,n}.$$

Sei $x = (x_{n_0}, x_{n_0-1}, \dots, x_0) \in |X|_0$ ein beliebiges Element, mit $x_n \in X_{-n,n}$, und sei $d(x) = 0$. Wegen $d_h x_n \in X_{-n-1,n}$ und $d_v x_n \in X_{-n,n-1}$ bedeutet dies ausgeschrieben:

$$\begin{aligned} d_h(x_{n_0}) &= 0 \\ d_v(x_i) + d_h(x_{i-1}) &= 0 \text{ in } X_{-i,i-1} \text{ für } 0 < i \leq n_0 \\ d_v(x_0) &= 0. \end{aligned}$$

Da die Zeilen exakt sind, gibt es Elemente $y_n \in X_{-n+1,n}$, so dass gilt

$$\begin{aligned} d_h(y_{n_0}) &= x_{n_0} \\ d_h(y_i) &= x_i - d_v(y_{i+1}) \text{ für } 0 \leq i < n_0 \end{aligned}$$

denn

$$d_h(x_i - d_v(y_{i+1})) = d_h(x_i) + d_v d_h(y_{i+1}) = d_h x_i + d_v x_{i+1} - d_v d_v(y_{i+2}) = 0.$$

Damit ist mit $y = (y_{n_0}, \dots, y_0) \in |X|_1$ ein Element mit $d(y) = x$ gefunden. Der Totalkomplex $|X|$ ist somit exakt.

- Beim Beweis von (2) nehmen wir $N = 0$ an und betrachten $(\dots, x_{-2}, x_{-1}, x_0) \in (TotX)_0$, wobei die Folge durchaus unendlich viele nicht-verschwindende Einträge 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 $TotX$ erlaubt ist.

□

Satz 6.6.5.

Für einen R -Rechtsmodul X und einen R -Linksmodul Y gilt

$$\mathrm{Tor}_n^R(X, Y) = \widetilde{\mathrm{Tor}}_n^R(X, Y).$$

Beweis.

Seien $P_\bullet \rightarrow X$ und $Q_\bullet \rightarrow Y$ projektive Auflösungen. Wir bezeichnen mit \tilde{P}_\bullet den augmentierten Komplex mit $\tilde{P}_n := P_n$ für $n \geq 0$ und $P_{-1} = X$. Dann ist \tilde{P}_\bullet exakt, und da Q_i projektiv für jedes i ist, ist nach Satz 1.4.9 auch der Doppelkomplex $\tilde{P} \otimes_R Q$ zeilenweise exakt. Nach Lemma 6.6.4 ist damit der Totalkomplex $|\tilde{P} \otimes Q|$ ebenfalls exakt.

Trivialerweise ist

$$0 \rightarrow X[-1] \rightarrow \tilde{P}_\bullet \rightarrow P_\bullet \rightarrow 0$$

eine kurze exakte Sequenz von Komplexen, wobei $X[-1]$ den Komplex bezeichnet, der in Grad -1 den Modul X enthält und 0 überall sonst. Da Q_i projektiv ist, liefert Tensorieren mit Q_\bullet eine exakte Sequenz von Doppelkomplexen. Da der Funktor $|\cdot|$, der Doppelkomplexe auf Komplexe abbildet, exakt ist, erhalten wir eine kurze exakte Sequenz von Totalkomplexen

$$0 \rightarrow |X[-1] \otimes Q| \rightarrow |\tilde{P} \otimes Q| \rightarrow |P \otimes Q| \rightarrow 0$$

Da der Komplex $\tilde{P} \otimes_R Q$ exakt ist, zerfällt die dazu gehörige lange exakte Sequenz für $n \geq 0$ in Stücke, die vom Verbindungshomomorphismus geliefert werden:

$$0 \rightarrow H_n |P \otimes Q| \rightarrow H_{n+1} |X[-1] \otimes Q| \rightarrow 0 ,$$

also in Isomorphismen. Nach Definition gilt für die erste abelsche Gruppe

$$H_n |P \otimes Q| = \widetilde{\text{Tor}}_n^R(X, Y) ;$$

für die zweite Gruppe finden wir

$$H_{n+1} |X[-1] \otimes Q| = H_n(X \otimes Q) \equiv \text{Tor}_n^R(X, Y) .$$

Damit ist die Isomorphie 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 $P_\bullet \rightarrow X$ und $Q_\bullet \rightarrow X$ projektive Auflösungen. Dann liefert die Vertauschung der Faktoren eine Isomorphie $P \otimes Q \rightarrow Q \otimes P$ von Doppelkomplexen. Wir finden somit

$$\begin{aligned} \text{Tor}_*^R(X, Y) &\cong \widetilde{\text{Tor}}_*^R(X, Y) = H_*(|P \otimes_R Q|) \\ &\cong H_*(|Q \otimes_R P|) = \widetilde{\text{Tor}}_*^R(X, Y) = \text{Tor}_*^R(Y, X) \end{aligned}$$

Also ist im Falle eines kommutativen Rings R auch der abgeleitete Funktor Tor_*^R kommutativ in den beiden Argumenten.

Satz 6.6.6.

Seien $X, Y \in R\text{-Mod}$ und $Y \rightarrow I_\bullet$ eine injektive Auflösung und $P_\bullet \rightarrow X$ eine projektive Auflösung. Setze:

$$\text{Ext}_R^n(X, Y) := H^n(\text{Hom}_R(X, I_\bullet)) \text{ und } \widetilde{\text{Ext}}_R^n(X, Y) := H_n(\text{TotHom}_R(P, I)) .$$

Dann gilt

$$\text{Ext}_R^n(X, Y) \cong \widetilde{\text{Ext}}_R^n(X, Y) \cong \text{Ext}_R^n(X, Y)$$

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

$$\text{Ex}^n(M, N) = \{0 \rightarrow N \rightarrow X_{n-1} \rightarrow X_{n-2} \rightarrow \cdots \rightarrow X_0 \rightarrow M \rightarrow 0\} / \sim,$$

wobei \sim die Äquivalenzrelation ist, die erzeugt wird von $E \sim E'$, wenn es eine Leiterabbildung $E \rightarrow E'$ 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.)

Wir wollen nun Ex^n zu einem Funktor $\mathcal{C}^{\text{opp}} \times \mathcal{C} \rightarrow \text{Set}$ machen. Gegeben seien eine Erweiterung

$$E = (0 \rightarrow N \rightarrow X_{\bullet} \rightarrow M \rightarrow 0) \in \text{Ex}^*(M, N)$$

und Morphismen

$$f : M' \rightarrow M \quad \text{und} \quad g : N \rightarrow N'.$$

Betrachte für f das Pullback-Diagramm

$$\begin{array}{ccc} X_1 & \xrightarrow{0} & M' \\ \downarrow d & \searrow & \downarrow f \\ X_0 \times_M M' & \longrightarrow & M' \\ \downarrow & & \downarrow \\ X_0 & \xrightarrow{d} & M \end{array}$$

wobei der Morphismus $X_1 \rightarrow X_0 \rightarrow M$ aus der exakten Sequenz kommt und daher gleich Null ist. Betrachte

$$f^*E : 0 \rightarrow N \rightarrow X_{n-1} \rightarrow \cdots \rightarrow X_1 \rightarrow X_0 \times_M M' \rightarrow M' \rightarrow 0$$

Dual definieren wir durch einen Pushout unter N , vgl. Abschnitt 2.5

$$g_*E : 0 \rightarrow N' \rightarrow X_{n-1} \sqcup_N N' \rightarrow X_{n-2} \rightarrow \cdots \rightarrow X_0 \rightarrow M \rightarrow 0.$$

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 $\mathcal{C}^{\text{opp}} \times \mathcal{C} \rightarrow \text{Set}$.

Beweis.

1. Für die Wohldefiniertheit muss gezeigt werden, dass f^* nicht vom Repräsentanten E der Äquivalenzklasse abhängt. Sei also

$$\begin{array}{ccccccc} E : & 0 & \longrightarrow & N & \longrightarrow & X_{\bullet} & \longrightarrow & M & \longrightarrow & 0 \\ & & & \parallel & & \downarrow & & \parallel & & \\ E' : & 0 & \longrightarrow & N & \longrightarrow & X'_{\bullet} & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

eine elementare Äquivalenz von exakten Sequenzen und $f : M' \rightarrow M$ ein Morphismus. Dann erhalten wir auf Grund der Funktorialität 2.5.2 (4) des Pullbacks eine Abbildung

$$X_0 \times_M M' \rightarrow X'_0 \times_M M' ,$$

die zusammen mit den anderen Morphismen $X_i \rightarrow X'_i$ 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 die eben konstruierte Erweiterung f^*E ebenfalls exakt ist.

- Die Abbildung $X \times_M M' \rightarrow M'$ ist surjektiv, denn zu $m' \in M'$ finde $x \in X_0$ mit $f(m') = dx$, da $d : X_0 \rightarrow M$ surjektiv ist.
- Der Morphismus $X_1 \rightarrow X_0 \times_M M'$ ist $x \mapsto (dx, 0)$, was wegen $d(dx) = 0 = f(0)$ wirklich in $X_0 \times_M M'$ liegt. Daher ist

$$\ker(X_1 \rightarrow X_0 \times_M M') = \ker(X_1 \rightarrow X_0) = \text{Im}(X_2 \rightarrow X_1) .$$

- Schließlich enthält $\ker(X_0 \times_M M' \rightarrow M')$ 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 $x \in \text{Im}(X_1 \rightarrow X_0)$ und somit $(x, 0) \in \text{Im}(X_1 \rightarrow X_0 \times_M M')$.

Das Argument für die Exaktheit von g_* ist wieder dual.

3. Nun zur 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 $f : M' \rightarrow M$ und $g : N \rightarrow N'$. 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

$$\begin{array}{ccccc} & & N & & \\ & g \swarrow & \downarrow d & \searrow 0 & \\ N' & & X & & M' \\ & \searrow 0 & \downarrow d & \swarrow f & \\ & & M & & \end{array}$$

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.

□

Wir wollen nun noch die Mengen Ex^n mit der Struktur von abelschen Gruppen versehen. Seien $E, E' \in \text{Ex}^n(M, N)$. Für $n \geq 2$ betrachten wir das Pullback-Diagramm

$$\begin{array}{ccccc}
 X_1 \oplus X'_1 & & & & \\
 \downarrow & \searrow^{d \circ pr_2} & & & \\
 X_0 \times_M X'_0 & \longrightarrow & X'_0 & & \\
 \downarrow & & \downarrow d & & \\
 X_0 & \xrightarrow{d} & M & &
 \end{array}$$

und das duale Pushout-Diagramm. Wir definieren

$$E + E' : 0 \rightarrow N \rightarrow X_{n-1} \sqcup_N X'_{n-1} \rightarrow X_{n-2} \oplus X'_{n-2} \rightarrow \cdots \rightarrow X_1 \oplus X'_1 \rightarrow X_0 \times_M X'_0 \rightarrow M \rightarrow 0 .$$

Im Fall $n = 1$ müssen wir den mittleren Term von $E + E'$ definieren als

$$\{(x, x') \in X \oplus X' \mid d(x) = d(x')\} / (d(n), 0) \sim (0, d(n)) (n \in N).$$

Lemma 6.7.2.

Die Mengen $\text{Ex}^n(M, N)$ 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 $dx_0 = m$, 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 $\ker(X_0 \rightarrow M) \times_M \ker(X'_0 \rightarrow M) = \text{Im}(X_1 \oplus X'_1 \rightarrow X_0 \times_M X'_0)$.
 - Die Exaktheit bei N und bei $X_{n-1} \sqcup_N X'_{n-1}$ folgt dual.
- Um die abelsche Gruppenstruktur zu definieren, brauchen wir zunächst ein neutrales Element; dieses ist für $n \geq 2$ gegeben durch

$$0 \rightarrow N \xrightarrow{\text{id}} N \rightarrow 0 \rightarrow \cdots \rightarrow M \xrightarrow{\text{id}} M \rightarrow 0$$

bzw. für $n = 1$ durch die zerfallende kurze exakte Sequenz. Die Assoziativität und Kommutativität der Multiplikation ist aus der Definition sofort ersichtlich.

- Den Beweis für die Existenz von Inversen lassen wir aus.

□

Satz 6.7.3.

Hat die Kategorie \mathcal{C} genug Projektive, so gibt es einen natürlichen Isomorphismus von Funktoren $\text{Ex}^n \cong \text{Ext}^n$.

Beweis.

Sei $P_\bullet \rightarrow M$ eine projektive Auflösung von M . Sei $E \in \text{Ex}^n(M, N)$. Dann hat nach dem Fundamentallemma 6.3.1 das Hochhebungsproblem für die Identität id_M

$$\begin{array}{ccccccccccccccc}
 \cdots & \longrightarrow & P_{n+1} & \xrightarrow{d} & P_n & \longrightarrow & P_{n-1} & \longrightarrow & P_{n-2} & \longrightarrow & \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \vdots & & \downarrow f_n & & \downarrow f_{n-1} & & \downarrow f_{n-2} & & & & \downarrow f_0 & & \parallel & & \\
 E : & & 0 & \longrightarrow & N & \longrightarrow & X_{n-1} & \longrightarrow & X_{n-2} & \longrightarrow & \cdots & \longrightarrow & X_0 & \longrightarrow & M & \longrightarrow & 0
 \end{array}$$

eine Lösung. Wegen der Kommutativität des linken Quadrats gilt $f_n \circ d = 0$, also liegt

$$f_n \in \ker(\text{Hom}(P_n, N) \rightarrow \text{Hom}(P_{n+1}, N)) .$$

Wir können die Klasse

$$\Phi(E) := [f_n] \in \text{Ext}^n(M, N)$$

betrachten. Wir zeigen zunächst, dass $\Phi(E) \in \text{Ext}^n(M, N)$ wohldefiniert ist: es hängt weder von der Wahl der Hochhebung f_\bullet der Identität id_M noch von der Wahl der Erweiterung E innerhalb einer Äquivalenzklasse ab. Dann zeigen wir, dass $\Phi : \text{Ex}^n(M, N) \rightarrow \text{Ext}^n(M, N)$ ein Isomorphismus von abelschen Gruppen ist.

Das Fundamentallemma 6.3.1 garantiert eine Hochhebung $f_n : P_n \rightarrow N$, die eindeutig bis auf Homotopie ist. Das heißt, jede weitere Lösung ist von der Form $f_n + H \circ d$, wobei $H : P_{n-1} \rightarrow N$ Teil einer Kettenhomotopie ist. Da dies keinen Unterschied in Homologie macht, ist die erste Wohldefiniertheit gezeigt.

Also ist die Klasse von f_n in $H^n(\text{Hom}(P_\bullet, N)) = \text{Ext}^n(M, N)$ wohldefiniert, wenn wir zeigen können, dass sie invariant unter der Äquivalenzrelation in Ex ist. Ist aber $E \rightarrow E'$ eine elementare Äquivalenz, so können wir deren Hochhebung $P_\bullet \rightarrow E'$ speziell so wählen, dass es die Hochhebung $P_\bullet \rightarrow E$ von id_M ist, gefolgt von der Äquivalenzabbildung $E \rightarrow E'$. Da diese per Definition die Identität auf N ist, erhalten wir das gleiche Element in Ext^n .

Ist umgekehrt $f : P_n \rightarrow N$ ein Repräsentant eines Elementes von $\text{Ext}^n(M, N)$, so können wir das Pushout-Diagramm

$$\begin{array}{ccc}
 P_n & \xrightarrow{d} & P_{n-1} \\
 f \downarrow & & \downarrow \\
 N & \longrightarrow & N \sqcup_{P_n} P_{n-1} \\
 & \searrow 0 & \downarrow \text{dashed} \\
 & & P_{n-2}
 \end{array}$$

betrachten und daraus eine exakte Sequenz

$$0 \rightarrow N \rightarrow N \sqcup_{P_n} P_{n-1} \rightarrow P_{n-2} \rightarrow P_{n-3} \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0$$

konstruieren. Es ist klar, dass die Komposition $\text{Ext} \rightarrow \text{Ex} \rightarrow \text{Ext}$ die Identität ist; die andere Richtung ist gegeben durch das folgende Diagramm, das eine Äquivalenz in Ex angibt:

$$\begin{array}{ccccccccccccccc}
 0 & \longrightarrow & N & \longrightarrow & N \sqcup_{P_n} P_{n-1} & \longrightarrow & P_{n-2} & \longrightarrow & \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \parallel & & \downarrow (d, f_{n-1}) & & \downarrow f_{n-2} & & & & \downarrow f_0 & & \parallel & & \\
 0 & \longrightarrow & N & \xrightarrow{d} & X_{n-1} & \xrightarrow{d} & X_{n-2} & \longrightarrow & \cdots & \longrightarrow & X_0 & \longrightarrow & M & \longrightarrow & 0
 \end{array}$$

Es ist klar, dass die Null in Ex^n auf die Null in Ext^n abgebildet wird, denn wir können als Hochhebung auf P_n den Nullmorphismus wählen.

Wir müssen nun noch zeigen, dass die Bijektion zwischen Ext^n und Ex^n die Addition respektiert. Dazu beobachten wir zunächst, dass wir die Addition in Ext^n wie folgt charakterisieren können: Ist $\Delta : M \rightarrow M \oplus M$ die Diagonalenabbildung und $\Sigma : N \oplus N \rightarrow N$ die Summenabbildung, so ist

$$f + g : \text{Ext}(M, N) \oplus \text{Ext}(M, N) \xrightarrow{\sim} \text{Ext}(M \oplus M, N \oplus N) \xrightarrow{\Sigma_* \Delta^*} \text{Ext}(M, N) .$$

Ebenso gilt in 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

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_n \oplus P_n & \longrightarrow & \cdots & \longrightarrow & P_0 \oplus P_0 & \longrightarrow & M \oplus M & \longrightarrow & 0 \\ & & \downarrow (f, f') & & & & \downarrow (f, f') & & \parallel & & \\ E \oplus E' : & & N \oplus N & \longrightarrow & \cdots & \longrightarrow & X_0 \oplus X'_0 & \longrightarrow & M \oplus M & \longrightarrow & 0 \end{array}$$

die Hochhebung als die direkte Summe der Hochhebungen f, f' definieren, die zu E bzw. E' gehören; damit ist die Additivität gezeigt. \square

Beispiel 6.7.4.

Sei p eine Primzahl; dann gilt nach Beispiel 6.5.2 in der Kategorie der abelschen Gruppen $\text{Ext}_{\text{Ab}}^1(\mathbb{Z}_p, \mathbb{Z}_p) = \mathbb{Z}_p$. Wir wissen also, dass es p Äquivalenzklassen von Erweiterungen

$$0 \rightarrow \mathbb{Z}_p \rightarrow G \rightarrow \mathbb{Z}_p \rightarrow 0$$

geben muss. Für die nicht-trivialen Gruppenelemente von $\text{Ext}_{\text{Ab}}^1(\mathbb{Z}_p, \mathbb{Z}_p)$ 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 Gruppen $\text{Ext}^*(M, N)$ aufzuprägen. Ist $E \in \text{Ex}^n(M, N), E' \in \text{Ex}^m(Q, M)$ mit $m > 0$ und $n > 0$, so liefert die Komposition $X_0 \rightarrow M \rightarrow X'_{m-1}$ einen Morphismus. Aus $X_1 \rightarrow X_0 \rightarrow M = 0$ und $M \rightarrow X'_m \rightarrow X'_{m-1} = 0$, folgt, dass

$$0 \rightarrow N \rightarrow X_{n-1} \rightarrow \cdots \rightarrow X_0 \rightarrow X'_{m-1} \rightarrow \cdots \rightarrow X'_0 \rightarrow Q ,$$

wieder eine Erweiterung ist.

Wir definieren $\text{Ex}^0(M, N)$ als $\text{Hom}(M, N)$; die Multiplikation $\text{Ex}^0 \times \text{Ex}^0 \rightarrow \text{Ex}^0$ ist dann einfach Komposition von Morphismen. Ferner setzen wir

$$\begin{array}{ccc} \text{Ex}^0 \times \text{Ex}^n & \rightarrow & \text{Ex}^n \\ (f, E) & \mapsto & f^* E \end{array}$$

bzw.

$$\begin{array}{ccc} \text{Ex}^n \times \text{Ex}^0 & \rightarrow & \text{Ex}^n \\ (E, g) & \mapsto & g_* E \end{array}$$

Satz 6.7.5 (Yoneda-Produkt).

Ist $E \in \text{Ex}^n(M, N)$, $E' \in \text{Ex}^m(Q, M)$, so definiere das Yoneda-Produkt $EE' \in \text{Ex}^{n+m}(Q, N)$ durch die Erweiterung

$$0 \rightarrow N \rightarrow X_{n-1} \rightarrow \cdots \rightarrow X_0 \rightarrow X'_{m-1} \rightarrow \cdots \rightarrow X'_0 \rightarrow Q ,$$

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 Ex^n aus Lemma 6.7.2. \square

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 $G \rightarrow \text{Aut}_{\mathbb{Z}}(M)$ durch Morphismen abelscher Gruppen. Ist A eine abelsche Gruppe, so verstehen wir A auch als G -Modul mit der trivialen Operation.

Wir definieren zunächst:

Definition 7.1.1

Die Invarianten M^G eines G -Moduls M sind die Fixpunkte der G -Operation:

$$M^G = \{m \in M \mid g.m = m \text{ für alle } g \in G\} .$$

Die Koinvarianten M_G sind definiert als Quotient

$$M_G = M / (gm - m \mid g \in G, m \in M) .$$

Invarianten und Koinvarianten fassen wir als additive Funktoren

$$(-)^G, (-)_G : \mathbb{Z}[G]\text{-Mod} \rightarrow \text{Ab}$$

auf, denn ist $f : M \rightarrow N$ ein $\mathbb{Z}[G]$ -Modulmorphismus (also eine G -äquivalente Abbildung), so folgt aus $g.m = m$ für alle $g \in G$ auch $g.f(m) = f(g.m) = f(m)$ für alle $g \in G$, so dass die Einschränkung von f auf die Invarianten ein Homomorphismus $f^G : M^G \rightarrow N^G$ abelscher Gruppen ist. Weil $f(gm - m) = gf(m) - f(m)$ gilt, induziert der Homomorphismus f auch einen Homomorphismus abelscher Gruppen $f_G : M_G \rightarrow N_G$ auf den Koinvarianten.

Lemma 7.1.2.

Es gibt natürliche Isomorphismen $M^G \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ und $M_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$, wobei \mathbb{Z} mit der trivialen Rechtsmodulstruktur versehen wird. Insbesondere ist nach Beispiel 2.3.11.4 der Funktor $(-)^G$ linksexakt und der Funktor $(-)_G$ rechtsexakt nach Beispiel 2.3.11.3.

Beweis.

Für den ersten Isomorphismus beachte, dass ein Element aus $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ durch das Bild der Eins $1 \in \mathbb{Z}$ eindeutig festgelegt ist. Für dieses muss für alle $g \in G$ gelten $g.f(1) = f(g.1) = f(1)$, also $f(1) \in M^G$. Umgekehrt definiert jedes solche $x \in M^G$ eine Morphismus in $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Für den zweiten Isomorphismus beachte, dass in $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M$ gilt

$$1 \otimes (gm - m) = (1.g) \otimes m - 1 \otimes m = 0 ,$$

so 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. \square

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 linksableitete Funktor der Koinvarianten:

$$H_n(G; M) := (L_n(-)_G)(M) = \text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M) .$$

2. Die Kohomologie der Gruppe G mit Koeffizienten im $\mathbb{Z}[G]$ -Modul M ist definiert als

$$H^n(G; M) := (R^n(-)^G)(M) = \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, M) .$$

Für den trivialen G -Modul \mathbb{Z} schreiben wir auch kürzer $H_n(G)$ und $H^n(G)$.

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 . Dann ist $\mathbb{Z}[G] \cong \mathbb{Z}[t]/(t^n - 1)$, und die Kohomologie 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 den trivialen $\mathbb{Z}[G]$ -Modul \mathbb{Z}_n . Nach Tensorieren der Auflösung

$$\dots \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{\epsilon} \mathbb{Z}$$

mit $N := 1 + t + \dots + t^{n-1}$ aus Beispiel 6.5.2.3 mit \mathbb{Z}_n ergibt sich der Komplex

$$\dots \xrightarrow{0} \mathbb{Z}_n \xrightarrow{0} \mathbb{Z}_n \rightarrow 0$$

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: Sei M ein C_n -Modul. Die Multiplikation mit $N = 1 + t + \dots + t^{n-1}$ ist wegen $gN = N$ für alle $g \in C_n$ eine Abbildung $M \rightarrow M^G$. Da außerdem $Ngm = Nm$ für alle $g \in C_n$ gilt, folgt, dass die Multiplikation mit N eine Normabbildung $\bar{N} : M_G \rightarrow M^G$ auf dem Quotienten M_G induziert.

Es gilt im Falle einer zyklischen Gruppe mit Erzeuger t für die Invarianten bzw. Koinvarianten

$$\ker(1 - t) = M^G \quad \text{bzw.} \quad M/\text{Im}(1 - t) = M_G$$

und daher

$$\ker N/\text{Im}(1 - t) = \ker \bar{N} \quad \text{bzw.} \quad \ker(1 - t)/\text{Im} N = M^G/\text{Im} \bar{N} = \text{coker} \bar{N} .$$

Nach Tensorieren der Auflösung aus Beispiel 6.5.2.3 mit M erhalten wir den Komplex

$$\dots M \xrightarrow{1-t} M \xrightarrow{N} M \xrightarrow{1-t} M \rightarrow 0$$

und somit

$$H_k(\mathbb{Z}_n; M) \cong \begin{cases} M/\text{Im}(1 - t) = M_G, & \text{falls } k = 0 \text{ (vgl. Lemma 6.3.5);} \\ \ker(1 - t)/\text{Im} N = \text{coker} \bar{N}, & \text{falls } k \text{ ungerade;} \\ \ker N/\text{Im}(1 - t) = \ker \bar{N}, & \text{falls } k > 0 \text{ gerade.} \end{cases}$$

4. Ebenso können wir die Kohomologie ausrechnen. Indem wir $\text{Hom}_R(-, M)$ auf die Auflösung aus Beispiel 6.5.2.3 anwenden, erhalten wir den Komplex

$$0 \rightarrow M \xrightarrow{1-t} M \xrightarrow{N} M \xrightarrow{1-t} M \xrightarrow{N} \dots$$

und somit

$$H^k(\mathbb{Z}_n; M) \cong \begin{cases} \ker(1 - t) = M^G & \text{falls } k = 0 \text{ (vgl. Lemma 6.3.5);} \\ \ker N/\text{Im}(1 - t) = \ker \bar{N}, & \text{falls } k \text{ ungerade;} \\ \ker(1 - t)/\text{Im} N = \text{coker} \bar{N}, & \text{falls } k > 0 \text{ gerade.} \end{cases}$$

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 $a_m t^m + \dots + a_n t^n$ mit $m \leq n \in \mathbb{Z}$ und $a_n \in \mathbb{Z}$. Eine freie Auflösung des trivialen Moduls $M = \mathbb{Z}$ über $\mathbb{Z}[G]$ ist gegeben durch

$$0 \rightarrow \mathbb{Z}[t, t^{-1}] \xrightarrow{1-t} \mathbb{Z}[t, t^{-1}] \xrightarrow{t-1} \mathbb{Z} \rightarrow 0 .$$

Tensorieren mit M über $\mathbb{Z}[G]$ gibt den Komplex

$$0 \rightarrow M \xrightarrow{1-t} M \rightarrow 0$$

aus dem folgt

$$H_0(G; M) = M/\text{Im}(1 - t) = M_G \quad \text{und} \quad H_1(G; M) = \ker(1 - t) = M^G .$$

Die Anwendung von $\text{Hom}_{\mathbb{Z}}(-, M)$ liefert den gleichen Komplex mit anderer Gradierung und daher

$$H_0(G; M) = H^1(G; M) = M_G \quad \text{und} \quad H_1(G; M) = H^0(G; M) = M^G .$$

Alle höhere Homologie und Kohomologie ist null, weil die Auflösung des trivialen Moduls M Länge 2 hat.

Bemerkung 7.1.7 (Satz von Maschke).

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 hieraus insbesondere der Satz von Maschke 4.1.13 folgt.

Denn sei

$$0 \rightarrow V' \rightarrow V \rightarrow V'' \rightarrow 0$$

eine beliebige kurze exakte Sequenz von $K[G]$ -Moduln. Wir wollen zeigen, dass dann die induzierte Sequenz

$$0 \rightarrow \text{Hom}_G(V'', V') \rightarrow \text{Hom}_G(V, V') \rightarrow \text{Hom}_G(V', V') \rightarrow 0$$

exakt ist. Denn dann liefert das Urbild der Identität $\text{id}_{V'}$ eine Retraktion $V \rightarrow V'$, so dass die exakte Sequenz $0 \rightarrow V' \rightarrow V \rightarrow V'' \rightarrow 0$ spaltet, vgl. Satz 1.4.3. Dazu betrachten wir die entsprechende kurze exakte Sequenz von K -Vektorräumen,

$$0 \rightarrow \text{Hom}_K(V'', V') \rightarrow \text{Hom}_K(V, V') \rightarrow \text{Hom}_K(V', V') \rightarrow 0,$$

die wir als exakte Sequenz von $K[G]$ -Moduln ansehen. Die Wirkung ist hierbei gegeben durch

$$\begin{aligned} K[G] \times \text{Hom}_K(V, W) &\rightarrow \text{Hom}_K(V, W) \\ (\delta_g, \varphi) &\mapsto \delta_g \cdot \varphi(-) + \varphi(\delta_{g^{-1}}-) . \end{aligned}$$

Da die Elemente von $\text{Hom}_G(V, W)$ genau die G -Invarianten im $K[G]$ -Modul $\text{Hom}_K(V, W)$ sind, müssen wir zeigen, dass die Sequenz der Invarianten

$$0 \rightarrow H^0(G, \text{Hom}_K(V', V')) \rightarrow H^0(G, \text{Hom}_K(V, V')) \rightarrow H^0(G, \text{Hom}_K(V'', V')) \rightarrow 0$$

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 $W = \text{Hom}_K(V', V')$.

7.2 Funktorialität

Homologie und Kohomologie sind Funktoren, allerdings muss man bei der Definition sorgfältig sein. Betrachte die Kategorie $GrpMod$, deren Objekte Paare sind, bestehend aus einer Gruppe G und einem G -Modul M , und deren Morphismen definiert sind durch

$$\begin{aligned} &\text{Hom}_{GrpMod}((G, M), (G', M')) \\ &:= \{ \alpha : G \rightarrow G', f : M \rightarrow M' \mid f(g.m) = \alpha(g)f(m) \text{ und } \alpha \text{ Gruppenhomomorphismus} \} . \end{aligned}$$

Ein Morphismus $(\alpha, f) : (G, M) \rightarrow (G', M')$ ist also ein Morphismus $f : M \rightarrow \alpha^*N$ von $K[G]$ -Moduln, wobei α^*N der $K[G]$ -Modul ist, der durch Pullback, also Restriktion der Skalare, aus N entsteht.

Dies schließt zwei wichtige Fälle ein: Für festes G kann die Kategorie $\text{Mod}_{\mathbb{Z}[G]}$ als Unterkategorie von $GrpMod$ aufgefasst werden. Homologie ist ein Funktor auf dieser Unterkategorie; das wussten wir aber schon wegen der Funktorialität von Tor im zweiten Argument.

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 . Damit erhält man für jeden Gruppenmorphismus $\alpha : G \rightarrow H$ eine induzierte Abbildung $\alpha_* : H_i(G) \rightarrow H_i(H)$ auf der Gruppenhomologie.

Satz 7.2.1.

Gruppenhomologie ist ein Funktor $GrpMod \rightarrow Ab$.

Beweis.

Sei $(\alpha, f) : (G, M) \rightarrow (H, N)$ ein Morphismus $GrpMod$. Wähle projektive Auflösungen $P_\bullet \rightarrow M$ über $\mathbb{Z}[G]$ und $Q_\bullet \rightarrow N$ über $\mathbb{Z}[H]$. Wir können alle H -Moduln Q_n in Q_\bullet mit α zu G -Moduln zurückziehen und so Q_\bullet als $\mathbb{Z}[G]$ -Komplex auffassen mit der gleichen Abbildung als Differential. Dieser Komplex ist dann zwar nicht mehr projektiv; da aber das Differential unverändert ist, ist der Komplex immer noch azyklisch. Wegen des Fundamentallemmas 6.3.1 gibt es eine bis auf Homotopie eindeutige Hochhebung $f_\bullet : P_\bullet \rightarrow \alpha^*(Q)_\bullet$ des Morphismus $f : M \rightarrow \alpha^*(N)$ von G -Moduln. Diese induziert einen Morphismus von Komplexen abelscher Gruppen

$$\text{id} \otimes f_\bullet : \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_\bullet \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} \alpha^*(Q)_\bullet .$$

Da die Homologie der rechten Seite $H_i(H; N)$ ist, erhalten wir somit eine wohldefinierte Abbildung $(\alpha, f)_* : H_i(G; M) \rightarrow H_i(H; N)$. Die Funktorialität folgt aus der Eindeutigkeit der Hochhebung bis auf Homotopie. \square

Beispiel 7.2.2.

Wir zeigen, dass die vom surjektiven Gruppenhomomorphismus $\alpha : \mathbb{Z} \rightarrow \mathbb{Z}_n$ induzierte Abbildung auf $H_1(-; \mathbb{Z})$ 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} :

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}[t, t^{-1}] & \xrightarrow{1-t} & \mathbb{Z}[t, t^{-1}] & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow t \rightarrow t & & \downarrow t \rightarrow t & & \parallel \\ \dots & \xrightarrow{N} & \mathbb{Z}[t]/(t^n - 1) & \xrightarrow{1-t} & \mathbb{Z}[t]/(t^n - 1) & \longrightarrow & \mathbb{Z} \longrightarrow 0 \end{array}$$

Durch Übergang zu den Koinvarianten auf den Auflösungen erhalten wir:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \longrightarrow & 0 \\ & & \parallel & & \parallel & & \\ \dots & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

also ist die Abbildung auf $H_1(-, \mathbb{Z})$ die Standardreduktion $\mathbb{Z} \rightarrow \mathbb{Z}_n$ von abelschen Gruppen.

Satz 7.2.3.

Sei G eine Gruppe und M ein G -Modul. Sei $g_0 \in G$ und betrachte den Automorphismus (α, f) in $GrpMod$, der gegeben ist durch $\alpha(g) := g_0 g g_0^{-1}$ und $f(m) := g_0.m$. Dann ist $(\alpha, f)_* = \text{id}_{H_*(G; M)}$.

Beweis.

Sei $P_\bullet \rightarrow M$ 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 τ ein Automorphismus von Kettenkomplexen, der $f : M \rightarrow M$ fortsetzt, also kann $(\alpha, f)_*$ berechnet werden als die von τ induzierte Abbildung in Homologie. Aber nach Tensorieren mit dem trivialen Modul \mathbb{Z} , auf dem insbesondere g_0 trivial wirkt, ist

$$\text{id}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \tau : \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_n \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_n$$

die Identität. \square

Bemerkung 7.2.4.

Ist G eine Gruppe, so nennt man die Automorphismen, die sich durch Konjugation darstellen lassen, die inneren Automorphismen; diese bilden einen Normalteiler $\text{Inn}(G) \subset \text{Aut}(G)$. Die Quotientengruppe $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$ heißt die Gruppe der äußeren Automorphismen. Der vorige Satz zeigt, dass $H_*(G)$ eine Operation der Quotientengruppe $\text{Out}(G)$ 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 explizite für 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 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

$$r \cdot (r_0 | \cdots | r_n | m) := r r_0 | r_1 | \cdots | r_n | m.$$

Schließlich führen wir noch Strukturabbildungen $d : B_n(R, M) \rightarrow B_{n-1}(R, M)$ ein durch

$$d := \sum_{i=0}^n (-1)^i d_i \quad \text{mit} \quad d_i(r_0 | \cdots | r_{n+1}) := r_0 | \cdots | r_i r_{i+1} | \cdots | r_{n+1},$$

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

$$d_i \circ d_j = d_j \circ d_{i+1} \quad \text{falls} \quad i \geq j$$

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

$$\begin{aligned} d \circ d &= \sum_{i=0}^{n-1} \sum_{j=0}^n (-1)^{i+j} d_i \circ d_j \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^i (-1)^{i+j} d_i \circ d_j + \sum_{i=0}^{n-1} \sum_{j=i+1}^n (-1)^{i+j} d_i \circ d_j \\ &= \sum_{i=1}^n \sum_{j=0}^{i-1} (-1)^{i+j-1} d_j \circ d_i + \sum_{i=0}^{n-1} \sum_{j=i+1}^n (-1)^{i+j} d_i \circ d_j \\ &= \sum_{j=0}^{n-1} \sum_{i=j+1}^n (-1)^{i+j-1} d_j \circ d_i + \sum_{i=0}^{n-1} \sum_{j=i+1}^n (-1)^{i+j} d_i \circ d_j = 0. \end{aligned}$$

Hierbei wurde die Summe zuerst aufgespalten, dann die obige Relation 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, $h : B_n(R; M) \rightarrow B_{n+1}(R; M)$, so dass $h \circ d + d \circ h = \text{id}$ 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 $h \circ d_i = d_{i+1} \circ h$ und damit

$$d \circ h + h \circ d = \sum_{i=0}^{n+1} (-1)^i d_i \circ h + \sum_{i=0}^n (-1)^i h \circ d_i = d_0 \circ h = \text{id} .$$

□

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 R und 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. Man mache sich klar, dass Gruppenringe immer frei als abelsche Gruppen sind, wenn der Grundring 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.

Beispiel 7.3.4 (Erste Homologiegruppe).

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.

Es gilt immer $H_1(G; \mathbb{Z}) \cong G_{ab}$. Um dies zu sehen, betrachten wir den Anfang der Bar-Auflösung des trivialen Moduls \mathbb{Z} über $\mathbb{Z}[G]$:

$$\mathbb{Z}[G] \otimes \mathbb{Z}[G] \otimes \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] \otimes \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]$$

$$g_0 | g_1 | g_2 \longmapsto g_0 g_1 | g_2 - g_0 | g_1 g_2 + g_0 | g_1$$

$$g_0 | g_1 \longmapsto g_0 g_1 - g_0$$

Da \mathbb{Z} ein freier \mathbb{Z} -Modul ist, haben wir eine freie Auflösung gefunden. Um die Homologie zu finden, tensorieren wir diese Sequenz von links mit dem trivialen $\mathbb{Z}[G]$ -Modul \mathbb{Z} über $\mathbb{Z}[G]$ und erhalten

$$\mathbb{Z}[G] \otimes \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z}$$

$$g_1 | g_2 \longmapsto g_2 - g_1 g_2 + g_1$$

$$g \longmapsto 0$$

Also ist

$$H_1(G; \mathbb{Z}) = \mathbb{Z}[G]/(g_1 + g_2 - g_1g_2 | g_1, g_2 \in G) .$$

Also ist die offensichtliche Abbildung $G \rightarrow H_1(G; \mathbb{Z})$ ein Epimorphismus von Gruppen. Denn im Quotienten ist die Klasse von $n\delta_g$ gleich der Klasse von δ_{g^n} . Es genügt nun, zu zeigen, dass jeder Morphismus $f : G \rightarrow A$ 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 $\mathbb{Z}[G] \rightarrow A$ fortsetzen, nämlich durch $\sum_g a_g [g] \mapsto \sum_g a_g f(g)$. Unter dieser Abbildung geht ein Element der Form $g_1 + g_2 - g_1g_2$ offensichtlich nach null. 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 $G' \triangleleft G$ ein Normalteiler in einer Gruppe G mit Quotientengruppe G'' . Wir erlauben uns, dies in Form einer exakten Sequenz $1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$ 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:

$$\begin{array}{ccccc}
 & & G_1 & & \\
 & \nearrow & \downarrow f & \searrow & \\
 1 & \longrightarrow & G' & & G'' \longrightarrow 1 \\
 & \searrow & \downarrow & \nearrow & \\
 & & G_2 & &
 \end{array}$$

In diesem Fall ist f automatisch ein Isomorphismus. Zunächst folgt aus Kommutativität des rechten Dreieckes $\ker f \subset \ker(G_1 \rightarrow G'')$. Ist $x \in \ker f \subset \ker(G_1 \rightarrow G'') = \text{Im}(G' \rightarrow G_1)$, 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; die Surjektivität von f folgt analog.

2. Ist eine Erweiterung $1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$ 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 $g_0 \in G'$

$$g'' \cdot g_0 := g g_0 g^{-1} .$$

Da G' ein Normalteiler ist, liegt $g'' \cdot g_0$ wieder in G' . Die Wahl des Urbilds g ist unerheblich, denn zwei solche Wahlen unterscheiden sich durch ein Element von G' , und Konjugation mit Elementen von G' ist die Identität auf G' , weil G' als abelsch angenommen war.

3. Umgekehrt lässt sich aus jeder Operation $\alpha : G'' \rightarrow \text{Aut}(G')$ von G'' auf einer beliebigen Gruppe G' durch Gruppenautomorphismen eine Erweiterung $G = G' \rtimes_{\alpha} G''$, das semi-direkte Produkt, bilden. Die zu Grunde liegende Menge von G ist $G' \times G''$, und die Multiplikation ist definiert durch

$$(g'_1, g''_1) \cdot (g'_2, g''_2) := (g'_1(g''_1 \cdot g'_2), g''_1 g''_2)$$

(Merkregel für die Richtung des Zeichens \rtimes : Die Spitze des Dreiecks zeigt in Richtung des Normalteilers). Die Erweiterung $1 \rightarrow G' \rightarrow G' \rtimes G'' \rightarrow G'' \rightarrow 1$ zerfällt stets, denn der

Gruppenhomomorphismus $s_0 : G'' \xrightarrow{g'' \mapsto (1, g'')} G' \rtimes G''$ ist ein Schnitt. Sind s_1, s_2 Schnitte, so heißen sie 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 alle $g'' \in G''$ gilt.

4. Folgende natürliche Fragen stellen sich:

- Zerfallen alle Erweiterungen? 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?

5. Gruppenkohomologie beantwortet beide Fragen, zumindest für abelsche Normalteiler G' . Wir betrachten zunächst den zweiten Punkt. Ein Schnitt $s = (\delta, \text{id}) : G'' \rightarrow G' \rtimes G''$ muss die Identität auf der zweiten Koordinate sein. Auf der ersten Komponente, wobei wir die Gruppenstruktur auf der abelschen Gruppe G' additiv schreiben, muss gelten

$$(\delta g_1'', g_1'') \cdot (\delta g_2'', g_2'') = (\delta g_1'' + g_1'' \cdot \delta g_2'', g_1'' g_2'') \stackrel{!}{=} (\delta(g_1'' g_2''), g_1'' g_2'') ,$$

also die Gleichung

$$\delta(g_1'' g_2'') = \delta(g_1'') + g_1'' \cdot \delta(g_2'') . \quad (9)$$

erfüllt sein.

Wenn zwei Funktionen $\delta_1, \delta_2 : G'' \rightarrow G'$ beide diese Gleichung erfüllen, dann auch $\delta_1 + \delta_2$; dies definiert also eine abelsche Gruppenstruktur auf der Menge aller Schnitte. Ein Schnitt δ ist genau dann äquivalent zum Nullschnitt s_0 , wenn es ein $g' \in G'$ gibt, so dass

$$\delta(g'') = g' - g'' \cdot (g') .$$

Satz 7.4.2.

Sei G' eine abelsche Gruppe; sei G'' eine Gruppe, die durch Gruppenautomorphismen auf G' operiere. Die Gruppe der Schnitte $G'' \rightarrow G' \rtimes G''$ ist dann isomorph zu $H^1(G'', G')$, wobei die abelsche Gruppe G' über die G'' -Operation als G'' -Modul gesehen wird.

Beweis.

Wir betrachten die Bar-Auflösung des trivialen G'' -Moduls \mathbb{Z} und studieren den Komplex abelscher Gruppen mit

$$C^n := \text{Hom}_{\mathbb{Z}[G'']}(\mathbb{Z}[G'']^{\otimes n+1}, G') .$$

Dann gilt $H^n(G'', G') = H^n(C^\bullet)$. Ein Element in C^1 ist ein $\mathbb{Z}[G'']$ -linearer Morphismus

$$f : \mathbb{Z}[G''] \otimes_{\mathbb{Z}} \mathbb{Z}[G''] \rightarrow G' .$$

Wegen des Isomorphismus

$$\begin{aligned} \text{Hom}_{\mathbb{Z}[G']}(\mathbb{Z}[G''] \otimes_{\mathbb{Z}} \mathbb{Z}[G''], G') &\rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G''], G') \\ f &\mapsto s(-) = f(1, -) \end{aligned}$$

ist diese Funktion äquivalent zu einem \mathbb{Z} -linearen Morphismus $s : \mathbb{Z}[G''] \rightarrow G'$. Die Umkehrabbildung ist $f(g_1'' | g_2'') = g_1'' \cdot s(g_2'')$. Die Funktion s ist wiederum äquivalent zu einer Funktion $\delta : G'' \rightarrow G'$. Die Funktion f ist 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 $g_0'' = 1$ gilt $0 = g_1''\delta(g_2'') - \delta(g_1''g_2'') + \delta(g_1'')$. Also falls δ die Gleichung (9) erfüllt. Umgekehrt ist f genau dann ein Korand, wenn es einen $\mathbb{Z}[G]$ -linearen Morphismus $\tilde{f} : \mathbb{Z}[G] \rightarrow G'$ 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

$$\delta(g_1'') = g' - g_1''(g') .$$

□

Wir beschreiben als Vorbereitung auch noch die Elemente von $H^2(G'', G')$ als Äquivalenzklassen von Funktionen $f : G'' \times G'' \rightarrow G'$ mit

$$(df)(g_1'', g_2'', g_3'') = g_1''f(g_2'', g_3'') - f(g_1''g_2'', g_3'') + f(g_1'', g_2''g_3'') - f(g_1'', g_2'') = 0 , \quad (10)$$

modulo der Identifikation von Funktionen, die sich um einen Ausdruck der Form

$$da := a(g_1'') - a(g_1''g_2'') + g_1'' \cdot a(g_2'')$$

mit einer Funktion $a : G'' \rightarrow G'$ unterscheiden.

Satz 7.4.3.

Sei G'' eine Gruppe mit einer Operation auf der abelschen Gruppe G' durch Gruppenautomorphismen. Dann gibt es eine Bijektion von der Menge der Erweiterungen von G'' durch G' modulo Äquivalenz nach $H^2(G'', G')$, wobei die abelsche Gruppe G' durch die G'' -Operation zum G'' -Modul wird.

Beweis.

Sei $E : 1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$ eine solche Erweiterung. Im Allgemeinen gibt es keinen Schnitt, der ein Gruppenhomomorphismus ist. Wir wählen daher einen Schnitt $s : G'' \rightarrow G$ von Mengen. Dann ist $s(g_1'')s(g_2'')s(g_1''g_2'')^{-1}$ in $\ker(G \rightarrow G'') = \text{Im}(G' \rightarrow G)$. Wir definieren daher die Funktion

$$\begin{aligned} f_{E,s} : G'' \times G'' &\rightarrow G' \\ (g_1'', g_2'') &\mapsto s(g_1'')s(g_2'')s(g_1''g_2'')^{-1} . \end{aligned}$$

Man rechnet nach, dass Gleichung (10) erfüllt ist; daher definiert $f_{E,s}$ eine Klasse in $H^2(G'', G')$.

Ist $s' : G'' \rightarrow G$ ein anderer Schnitt, so ist $a := s's^{-1} : G'' \rightarrow G' \rtimes G$. Damit ist

$$\begin{aligned} (f_{E,s'} - f_{E,s})(g_1'', g_2'') &= a(g_1'')s(g_1'')a(g_2'')s(g_2'')s(g_1''g_2'')^{-1}a(g_1''g_2'')^{-1}s(g_1''g_2'')s(g_2'')^{-1}s(g_1'')^{-1} \\ &= a(g_1'')s(g_1'')a(g_2'')s(g_1'')^{-1}a(g_1''g_2'')^{-1} \\ &= a(g_1'') - a(g_1''g_2'') + g_1'' \cdot a(g_2'') = (da)(g_1'', g_2'') . \end{aligned}$$

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 Erweiterung dieselbe Funktion f ergeben.

Umgekehrt sei eine beliebige Funktion $f : G'' \times G'' \rightarrow G'$ gegeben. Wir versuchen, eine Gruppenstruktur G_f auf $G' \rtimes G''$ durch

$$(g_1', g_1'')(g_2', g_2'') := (g_1' + g_1'' \cdot g_2' + f(g_1'', g_2''), g_1''g_2'')$$

zu definieren. Die Projektion $G_f \rightarrow G''$ ergibt eine kurze exakte Sequenz $E_f : 1 \rightarrow G' \rightarrow G_f \rightarrow G'' \rightarrow 1$. Man rechnet leicht nach, dass es stets Inverse in G_f gibt. Die Assoziativität der Multiplikation ist dagegen nicht automatisch:

$$\begin{aligned} [(g'_1, g''_1)(g'_2, g''_2)](g'_3, g''_3) &= (g'_1 + g''_1 \cdot g'_2 + f(g''_1, g''_2), g''_1 g''_2) \cdot (g'_3, g''_3) \\ &= (g'_1 + g''_1 \cdot g'_2 + f(g''_1, g''_2) + (g''_1 g''_2) \cdot g'_3 + f(g''_1 g''_2, g''_3), g''_1 g''_2 g''_3) . \\ (g'_1, g''_1)[(g'_2, g''_2)(g'_3, g''_3)] &= (g'_1, g''_1)(g'_2 + g''_2 \cdot g'_3 + f(g''_2, g''_3), g''_2 g''_3) \\ &= (g'_1 + g''_1 \cdot (g'_2 + g''_2 \cdot g'_3 + f(g''_2, g''_3)) + f(g''_1, g''_2 g''_3), g''_1 g''_2 g''_3) \end{aligned}$$

Die Differenz ist in G' :

$$g''_1 f(g''_2, g''_3) - f(g''_1 g''_2, g''_3) + f(g''_1, g''_2 g''_3) - f(g''_1, g''_2) = (df)(g''_1, g''_2, g''_3) .$$

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

$$\left\{ \begin{array}{l} \text{Erweiterungen von } G'' \text{ durch } G' \\ \text{modulo Äquivalenz} \end{array} \right\} \cong \left\{ \begin{array}{l} \text{Funktionen } f : G'' \times G'' \rightarrow G' \text{ mit } df = 0 \\ \text{modulo Funktionen } da \text{ für } a : G'' \rightarrow G' \end{array} \right\} .$$

Die rechte Seite ist nach der vorangegangenen Betrachtung mit der Bar-Auflösung genau $H^2(G'', G')$. □

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:

$$\begin{aligned} x &\leq x && \text{Reflexivität} \\ x \leq y \wedge y \leq z &\Rightarrow x \leq z && \text{Transitivität} \\ x \leq y \wedge y \leq x &\Rightarrow x = y && \text{Antisymmetrie.} \end{aligned}$$

- (ii) Eine Totalordnung auf S ist eine partielle Ordnung, für die je zwei Elemente vergleichbar sind:

$$x, y \in S \Rightarrow x \leq y \text{ oder } y \leq x .$$

- (iii) Sei S partiell geordnet, $T \subset S$ Teilmenge.

Ein Element $b \in S$ heißt obere Schranke von T , falls

$$x \leq b \text{ für alle } x \in T .$$

- (iv) Sei S partiell geordnet. Ein Element $m \in S$ heißt maximales Element, falls

$$m \leq x \Rightarrow m = x .$$

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

- Äquivalenzen von Kategorien, 44, 50
- Überkategorie, 64
- äußere Automorphismen, 137

- abelsche Kategorie, 57
- additiv, 55
- additive Kategorie, 55
- additiver Funktor, 55, 59
- adjungierte Funktoren, 48
- Algebra über einem Ring, 4
- amalgamierte Summen, 66
- Annulator, 13
- Antihomomorphismus, 4
- artinscher Modul, 105
- artinscher Ring, 105
- Auswahlaxiom, 60
- Auswertehomomorphismus, 7
- azyklischer Kettenkomplex, 111

- Bar-Komplex, 137
- Basis eines Moduls, 22
- Begleitmatrix, 76
- Bild eines Morphismus, 58
- Bimodul, 3

- Charakter, 91
- Charaktertafel, 97

- darstellbarer Funktor, 51
- darstellendes Objekt, 51
- Darstellung, 9
- Darstellungsabbildung eines Moduls, 6
- Differenzial, 26
- Differenzkern, 64
- direkte Summe von Darstellungen, 16
- direkte Summe von Moduln, 14
- Doppelkomplex, 123

- einfache Darstellung, 33
- einfacher Modul, 33
- einfacher Ring, 106
- Einsetzungshomomorphismus, 7
- Elementarteilersatz, 70
- endlich erzeugter Modul, 12, 106
- endlich koerzeugter Modul, 106
- Endomorphismenring, 5
- Epimorphismus, 57
- erblicher Ring, 69

- Erzeugendensystem, 12
- exakte Sequenz, 25
- exakter Funktor, 59

- Faktormodul, 11
- Faltung, 9
- Faserprodukt, 64
- flacher Modul, 30
- freie Familie, 22
- freier Modul, 22, 61
- Frobenius-Abbildung, 78
- Frobeniussche Normalform, 76
- Funktor, 42
- Funktorkategorie, 44

- Gruppenerweiterung, 139
- Gruppenring, 8
- Gruppoid, 41

- halbeinfache Kategorie, 60
- halbeinfacher Modul, 78
- halbeinfacher Ring, 78
- halbexakter Funktor, 59
- Hilbertscher Basissatz, 104
- Homologie, 111, 133
- Homologie der Gruppe \mathbb{Z} , 134
- Homologie einer zyklischen Gruppe, 133
- Homotopie, 113

- Induktion, 49
- induktiv geordnete Menge, 142
- initialer Ring, 2
- initialer universeller Morphismus, 53
- initiales Objekt, 56
- injektive Auflösung, 109
- injektiver Modul, 32
- injektives Objekt, 60
- innere direkte Summe, 16
- innerer Automorphismus, 137
- Invarianten, 132
- Invariantenteiler, 76
- irreduzible Darstellung, 33
- isomorphe Kategorien, 43
- isotypische Komponente, 81

- Jacobsonscher Dichtesatz, 87
- Jordansche Normalform, 76

- Kern, 56

Kettenhomotopie, 113
 Kettenkomplex, 25
 kleine Kategorie, 41
 Kobild, 58
 kofreier Modul, 61
 Kohomologie, 133
 Koinduktion, 49
 Koinvarianten, 132
 Kokern, 57
 kommutativer Ring, 1
 Kompositionsfaktoren, 36
 Kompositionsreihe, 36
 kontragrediente Darstellung, 93
 kontravarianter Funktor, 42
 Konvolution, 9
 Koprodukt, 45
 koregulärer Modul, 61
 Koszulregel, 124
 kurze exakte Sequenz, 26

 Länge eines Moduls, 36
 linksabgeleiteter Funktor, 116
 linksadjungierter Funktor, 47
 linksexakter Funktor, 59
 Linksmodul, 2

 maximales Element, 142
 Modulhomomorphismus, 2
 Monomorphismus, 57
 Morphismus von Darstellungen, 11

 natürliche Transformation, 43
 noetherscher Modul, 102
 noetherscher Ring, 102

 obere Schranke, 142
 opponierter Ring, 4

 partielle Ordnung, 142
 Polynom, 6
 Polynomring, 6
 Produkt von Moduln, 14
 Produkt von Objekten, 46
 projektive Auflösung, 109
 projektiver Modul, 28
 projektives Objekt, 60
 Pullback, 12, 64
 Pullbackfunktor, 65
 punktierte Kategorien, 56
 Pushout, 66

 Quasi-Isomorphismus, 113

 Quaternionen, 99
 quaternionischer Vektorraum, 100
 Quotientenmodul, 11

 Ränder in einem Komplex, 111
 Rang einer abelschen Gruppe, 75
 Rang eines Moduls, 23
 rechtsabgeleiteter Funktor, 116
 rechtsadjungierter Funktor, 48
 rechtsexakter Funktor, 59
 Rechtsmodul, 2
 regulärer Modul, 61
 Restriktion der Skalare, 12
 Retraktion, 26
 Ring, 1
 Ringhomomorphismus, 1

 Satz von Jordan-Hölder, 37
 Satz von Maschke, 82, 135
 Satz von Wedderburn, 88
 Schlangenlemma, 117
 Schnitt, 26
 Schursches Lemma, 35
 semi-direktes Produkt, 139
 Sequenz, 25
 Skalarenerweiterung, 49
 Skalarerweiterung, 100
 Sockel eines Moduls, 81
 Strukturabbildung eines Moduls, 6
 Subquotienten, 36
 Syzygien, 110

 teilbarer Modul, 31
 Tensorprodukt, 16
 terminaler Ring, 2
 terminaler universeller Morphismus, 54
 terminales Objekt, 56
 Theorem von Wedderburn, 86
 Torsionselement, 14
 torsionsfreier Modul, 14
 Totalgrad, 123
 Totalkomplex, 123
 Totalordnung, 142
 treue Darstellung, 13
 treuer Modul, 13

 unitärer Ring, 1
 Unitaritätstrick, 83
 Universelle Eigenschaft, 6
 universelle Eigenschaft, 53
 Unterdarstellung, 11

Untermodul, 11
unzerlegbare Darstellung, 33
unzerlegbarer Modul, 33

Verbindungshomomorphismus, 120
Vergissfunktork, 42
volltreuer Funktork, 44

wesentlich surjektiver Funktork, 45

Yoneda-Lemma, 51

Zentrum eines Ringes, 89
Zornsches Lemma, 142
Zykel in einem Komplex, 111
zyklischer Modul, 13