Skript zur Vorlesung

Kommutative Algebra (2std.)

Sommersemester 2018

Prof. Dr. Martin Möller

Frankfurt am Main, 30. Mai 2018

Inhaltsverzeichnis

1 Einleitung

Dieses Skript wird parallel zur Vorlesung erstellt und fortlaufend verbessert und ergänzt.

Voraussetzungen sind Grundbegriffe der Algebra, wie sie in der Vorlesung 'Grundlagen der Algebra' behandelt werden. Kenntnisse der Vorlesung 'Algebra' sind sehr nützlich, auch wenn das Thema Galoistheorie hier nicht (direkt) verwendet wird.

Literatur

[AM69] Sir Michael Francis Atiyah, Ian Grant Macdonald, *Introduction to commutative algebra*, Adison-Wesley, 1969.

[AM69] Siegfried Bosch, *Algebra*, Springer, 1992.

[Bou89] Nicolas Bourbaki, *Éléments de mathématique. Algèbre commutative. Chapitre 1–7*, Hermann, Paris, 1961–1965; oder *Commutative algebra. Chapters 1–7*, Springer, 1989.

[Eis95] David Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts In Mathematics **150**, Springer, 1995.

[La02] Serge Lang, *Algebra*, revidierte dritte Auflage, Graduate Texts in Mathematics **211**, Springer, 2002.

[Lei14] Tom Leinster, *Basic Category Theory*, Cambridge Studies in Advanced Mathematics, **143**, Cambridge Univ. Press, 2014.

[Mat89] Hideyuki Matsumura, *Commutative Ring Theory*, übersetzt von Miles Reid, Cambridge University Press, 1989.

[Rot09] Joseph Rotman, *Introduction to homological algebra*, Springer Universitext, Second Edition, 2009.

2 Wiederholung: Grundbegriffe der Ringtheorie

Dieser Abschnitt fasst Begriffe aus der Ringtheorie zusammen, die aus der Vorlesung 'Grundlagen der Algebra' bekannt sein sollten.

Ringe sind in dieser Vorlesung grundsätzlich kommutativ und haben ein Einselement. Ein *Körper* ist ein solcher Ring, bei dem jedes von Null verschiedene Element invertierbar ist. Standardbeispiele sind der Ring der ganzen Zahlen $\mathbb{Z}$, Polynomringe $R[X]$ oder $R[X_1, X_2, \ldots, X_n]$ in einem oder mehreren Unbestimmten über einem Ring R, Matrixringe oder der Ring der Abbildungen in $\mathrm{Abb}(X, R)$ von einer Menge X in einen Ring R. Beispiele von Körpern sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ und deren Erweiterungen, wie in der Vorlesung Algebra konstruiert. Weitere Beispiele von Ringen sind der Ring der Potenzreihen oder der

Ringe der (stetigen, differentierbaren, holomorphien) Funktionen auf einer offenen Teilmenge von $\mathbb{R}^n$ oder $\mathbb{C}$.

Ein *Ringhomomorphismus* ist eine Abbildung $f : R \to S$ zwischen zwei Ringen, sodass $f(r_1{+}r_2) = f(r_1){+}f(r_2)$, sodass $f(r_1r_2) = f(r_1)f(r_2)$ und $f(1) = 1$ gilt. Die Menge aller Ringhomomorphismen notieren wir mit $\mathrm{Hom}_{\mathit{Ring}}(R, S)$.

Ein *Ideal* ist eine additive Untergruppe $\mathfrak{a} \subseteq R$, sodass für alle $r \in R$ und alle $a \in \mathfrak{a}$ auch $ra \in \mathfrak{a}$ gilt. Ideale sind genau die Kerne von Ringhomomorphismen. Bilder von Ringhomomorphismen sind im Allgemeinen nur Unterringe, keine Ideale. Ist $M \subset R$ eine Teilmenge, so schreiben wir

$$\langle M \rangle \;=\; \Big\{ \sum_{i=1}^{n} r_i m_i,\;\; m_1, \ldots, m_n \in M \Big\} \tag{2.1}$$

für das von M erzeugte Ideal. Ein Ideal heißt *Hauptideal*, wenn es von einem Element erzeugt werden. kann.

Eine *Einheit* ist ein Ringelement r mit einem multiplikativen Inversen, d.h. sodass es ein $s \in R$ gibt mit $rs = 1$. Die Menge aller Einheiten in R bildet eine Gruppe, die *Einheitengruppe* R^*. Zwei Elemente eines Rings, die sich nur durch Multiplikation mit einer Einheit unterscheiden, werden *assoziiert* genannt.

Ein *Nullteiler* ist ein Ringelement r, sodass es ein $s \in R \setminus \{0\}$ gibt mit $rs = 0$. Ein Ring, dessen Menge der Nullteiler nur aus dem Nullelement besteht, heißt *nullteilerfrei* oder *Integritätsbereich*. Beispiele für nullteilerfreie Ringe sind $\mathbb{Z}$, ein Körper K, Polynomringe $K[X]$, nicht aber $\mathbb{Z}/6\mathbb{Z}$ oder Produkte wie $\mathbb{Z} \times \mathbb{Z}$.

Ein Element $r \in R$ heißt *irreduzibel*, wenn r keine Einheit ist und aus einer multiplikativen Zerlegung $r = xy$ folgt, dass x oder y eine Einheit ist. Ein Element $r \in R$ heißt *prim*, falls aus $r|xy$ entweder $r|x$ oder $r|y$ (oder beides) folgt. In einem nullteilerfreien Ring ist jedes Primelement irreduzibel.

Ein Ring heißt *Hauptidealring*, wenn jedes Ideal ein Hauptideal ist. Beispiele von Hauptidealringen sind $\mathbb{Z}$ oder $K[X]$. Dies folgt daraus, dass jeder euklidsche Ring, d.h. jeder Ring mit einem euklidschen Algorithmus, ein Hauptidealring ist. In einem Hauptidealring sind die Begriffe prim und irreduzibel äquivalent. Hauptidealring sind *faktoriell*, d.h. jedes von Null verschiedene Element besitzt eine (bis auf Reihenfolge und Übergang zu assoziierten Elementen) eindeutige Zerlegung in irreduzible Elemente.

In jedem Integritätsring kann man den ggT und das kgV einer endlichen Menge von Ringelementen definieren. In Hauptidealringen existiert der ggT und das kgV für jede endliche Menge von Ringelementen $r_1, \ldots, r_n$ und es gilt

$$\langle \mathrm{ggT} \rangle \;=\; \langle r_1, \ldots, r_n \rangle, \quad \langle \mathrm{kgV} \rangle \;=\; \bigcap_{i=1}^{n} \langle r_i \rangle\,. \tag{2.2}$$

3 Moduln

Eine Motivation für Konzepte der Algebra ist das Lösen diophantischer Gleichungen. Bereits das Lösen linearer diophantischer Gleichungssysteme geht über den Rahmen der linearen Algebra hinaus. Dort wird, z.B. beim Gauß-Algorithmus an geeigneter Stelle dividiert, was nicht gestattet ist, wenn wir bei ganzzahligen Koeffizienten verbleiben wollen. Das erste Hauptziel dieses Abschnitts ist eine Analogon des Gauß-Algorithmus über den ganzen Zahlen.

Wir müssen dazu also Strukturen untersuchen, bei denen der Skalar-Körper nur noch ein Ring ist. Diese werden Moduln genannt. Man beachte, dass ein $\mathbb{Z}$-Modul nach untenstehender Definition nichts anderes ist als eine abelsche Gruppe. Struktursätze für (endliche) $\mathbb{Z}$-Moduln sind also Aussagen über (endliche) abelsche Gruppen. Wir werden viel präzisere Aussagen machen können als die Sylowsätze für (allgemeine, nicht notwendig abelsche) Gruppen.

Sei R ein Ring, wie immer in diesem Skript kommutativ und mit Einselement. Ein *R-Modul M* ist eine abelsche Gruppe $(M, +)$ und eine Skalarmultiplikation

$$\cdot : R \times M \longrightarrow M,$$

die den (vom Vektorraum-Fall bekannten) Axiomen

$$\begin{aligned} a \cdot (x+y) &= a \cdot x + a \cdot y \\ (a+b) \cdot x &= a \cdot x + b \cdot x \\ a \cdot (bx) &= (a \cdot b)x; \qquad 1 \cdot x = x \end{aligned}$$

für alle $a, b \in R$ und $x, y \in M$ genügt. Wörtlich wie lineare Abbildungen definiert man *R-Modulhomomorphismen*. Sind M und N zwei R-Moduln, so bezeichnen wir die Menge aller R-Modulhomomorphismen mit $\mathrm{Hom}_R(M, N)$. Wörtlich wie Untervektorräume definiert man *Untermoduln* sowie den *Schnitt* von Untermoduln. Dieser ist wiederum ein Untermodul.

Ebenso wie im Vektorraumfall definiert man den Begriff *Erzeugendensystem* eines R-Moduls und zu gegebenem R-Modul M und einer Teilmenge N definiert man $\langle N \rangle_R$, den von *N erzeugten* R-Modul als die Menge aller Linearkombinationen von Elementen aus N. Kann M von endlich vielen Elementen erzeugt werden, so wird M ein *endlich erzeugter R-Modul* genannt.

Beispiel 3.1 i) Für jedes $n \in \mathbb{N}$ ist das Produkt R^n mit komponentenweise Addition und diagonaler Skalarmultiplikation $r \cdot (a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$ ein R-Modul, genannt der *freie Modul* vom Rang n.

ii) Insbesondere ist für jeden Ring R ist R ein *freier R-Modul*. R-Untermoduln von R sind per Definition gerade die Ideale von R.

iii) Sei V ein K-Vektorraum und $\varphi \in \mathrm{End}_K(V)$ ein Endomorphismus. Vermöge der Skalarmultiplikation

$$K[X] \times V \longrightarrow V, \quad \left(\sum a_i X^i, v\right) \longmapsto \sum a_i \varphi^i(v)$$

wird V zu einem $K[X]$-Modul. Umgekehrt, falls V ein $K[X]$-Modul ist, so definiert

$$\varphi(v) = X \cdot v$$

einen Endomorphismus. Damit erhält man eine Bijektion zwischen $K[X]$-Moduln und Paaren $\big(V, \varphi \in \mathrm{End}_K(V)\big)$.

3.1 Summe, Produkt, Torsion

Die Konstruktionen in diesem Abschnitt sind immer noch vollkommen analog zum Fall von Vektorräumen. In der linearen Algebra werden oftmals nur endlich-dimensionale Vektorräume betrachtet. Dabei verschwimmt der Unterschied zwischen Summe und Produkt, den wir hier klarstellen.

Sei M_i für $i \in I$ eine Familie von R-Moduln. Ein *Produkt* in der Kategorie der Moduln (siehe Abschnitt ?? für diese Begriffsbildung) ist ein Modul M mit Abbildungen $\mathrm{pr}_j : M \to M_j$ für jedes $j \in I$, welcher universell in folgendem Sinne ist: Ist N ein weiterer R-Modul mit R-Modulhomomorphismen $p_j : N \to M_j$ für jedes $j \in I$, so gibt es genau einen R-Modulhomomorphismus $\varphi : N \to M$ mit $p_j = \mathrm{pr}_j \circ \varphi$.

Satz 3.2 *Für jede Familie M_i von R-Moduln gibt es ein Produkt, das wir mit $\prod_{i \in I} M_i$ bezeichnen.*

Beweis: Wir definieren

$$M \;=\; \{(m_i)_{i \in I},\; m_i \in M_i \quad \text{für alle } i \in I\} \tag{3.1}$$

und $\mathrm{pr}_j((m_i)_{i \in I}) = m_j$. Dann muss ein R-Modulhomomorphismus φ mit der geforderten Verträglichkeit mit p_j und pr_j durch $\varphi(n) = (p_j(n))_{j \in I}$ gegeben sein (Eindeutigkeit) und diese Formel als Definition von φ definiert in der Tat einen R-Modulhomomorphismus. □

Sei M_i für $i \in I$ eine Familie von R-Moduln. Eine *Summe* in der Kategorie der Moduln ist ein Modul M mit Abbildungen $i_j : M_j \to M$ für jedes $j \in I$, welcher universell in folgendem Sinne ist: Ist T ein weiterer R-Modul mit Abbildungen $\alpha_j : M_j \to T$ für jedes $j \in I$, so gibt es genau eine Abbildung $\psi : M \to T$ mit $\alpha_j = \psi \circ i_j$.

Satz 3.3 *Für jede Familie M_i von R-Moduln gibt es ein Produkt, das wir mit $\oplus_{i \in I} M_i$ bezeichnen.*

Beweis: Wir definieren

$$M \;=\; \{(m_i)_{i \in I},\; m_i \in M_i \text{ für alle } i \in I,\; m_i = 0 \text{ für fast alle } i \in I\} \tag{3.2}$$

und $i_j(m_j)$ sei das Tupel mit m_j an der j-ten Stelle und Null sonst. Insbesondere ist ein beliebiges Element $m \in M$ gegeben durch $m = \sum_{j \in J} i_j(m_j)$ für eine endliche Teilmenge $J \subset I$.

Damit muss ein R-Modulhomomorphismus ψ mit der geforderten Verträglichkeit mit α_j und i_j durch $\psi(m) = \sum_{j \in J} \alpha_j(m_j)$ gegeben sein (Eindeutigkeit) und diese Formel als Definition von ψ definiert in der Tat einen R-Modulhomomorphismus. $\square$

Ein Modul M, der isomorph zu dem Modul $\oplus_{i \in I} R$ für eine beliebige Indexmenge I ist, wird *freier Modul* vom *Rang* $|I|$ genannt. Dies verallgemeinert den Begriff aus dem Beispiel 3.1. (Siehe Abschnitt 4.3 für eine Methode, die Wohldefiniertheit das Rangbegriffs vom Vektorraumfall abzuleiten.) Bezeichnet $\varphi : \oplus_{i \in I} R \to M$ den Isomorphismus, so wird die Menge $b_i = \varphi(1_i)$ der Bilder der Einselemente der i-ten Komponente eine *Basis* von M genannt. Offenbar hat jedes Element eines freien Moduls eine eindeutige Darstellung als Linearkombination der Basiselemente.

Wie im Vektorraumfall sagt man für Untermoduln M_i eines gegeben Moduls M, dass dieser die *direkte Summe* von M_i ist, falls die M_i den Modul M erzeugen und falls $M_i \cap \langle \cup_{j \neq i} M_j \rangle = \{0\}$ ist. Die Notationen sind konsistent in dem Sinne, dass in diesem Fall $M \cong \oplus M_i$ eine Summe im Sinne der obigen Abbildungseigenschaft ist.

Der erste wesentliche Unterschied zum Vektorraumfall ist, dass nicht jeder R-Modul eine Basis besitzt: Für jedes Element x in dem $\mathbb{Z}$-Modul (d.h. der abelschen Gruppe) $\mathbb{Z}/p\mathbb{Z}$ gilt $p \cdot x = 0$, womit wir eine nichttriviale Linearkombination gefunden haben.

Ist R ein allgemeiner nullteilerfreier Ring und M ein R-Modul, so formulieren wir das eben gesehene Phänomen, indem wir alle Elemente $x \in M$, sodass es ein $a \in R \setminus \{0\}$ gibt mit $ax = 0$, *Torsionselemente* nennen. Die Menge aller Torsionselemente bilden einen Untermodul $M_{\text{tor}} \subseteq M$, genannt *Torsionsuntermodul*. Ist $M = M_{\text{tor}}$, so nennt man M einen *Torsionsmodul*. Beispielsweise ist im $\mathbb{Z}$-Modul $M = \mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z}$ der Torsionsuntermodul $M_{\text{tor}} = \mathbb{Z}/s\mathbb{Z}$.

Nichtsdestotrotz können wir den Begriff *linear unabhängig* für Moduln wie für Vektorräume definieren und verwenden. Wir definieren auch im Allgemeinen den *Rang* von M als das Supremum über die Anzahl linear unabhängiger Elemente in M. Man beachte lediglich, dass nicht mehr jeder Modul von einer bezüglich Inklusion maximalen linear unabhängigen Teilmenge erzeugt ist.

3.2 Kern, Kokern und Quotienten

Sei $f : M \to N$ ein R-Modulhomomorphismus. Dann ist der *Kern* von f der Untermodul $\operatorname{Ker}(f) = f^{-1}(0) \subseteq M$ und das *Bild* ist der Untermodul $\operatorname{Im}(f) = f(M) \subseteq N$. Der *Kokern* von ist der Quotient $\operatorname{coker}(f) = N/\operatorname{Im}(f)$. Wie im Fall von Gruppen gilt der Homomorphiesatz:

Satz 3.4 *Ist $f : M \to N$ ein R-Modulhomomorphismus, so wird durch die Vorschrift $\overline{f}(x + \operatorname{Ker}(f)) = f(x)$ ein R-Modulisomorphismus $\overline{f} : M/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ definiert.*

Beweis: Die Wohldefiniertheit von $\overline{f}$ folgt aus der Definition des Kerns. Die Abbildung $\overline{f}$ ist offenbar ein R-Modulhomomorphismus, surjektiv aufgrund der Einschränkung des Bildes. Ist $x + \mathrm{Ker}(f) \in \mathrm{Ker}(\overline{f})$, so ist $x \in \mathrm{Ker}(f)$, also $x + \mathrm{Ker}(f)$ das Nullelement des Quotientenmoduls und damit ist $\overline{f}$ injektiv. $\square$

Als Konsequenz erhalten wir zwei Isomorphiesätze.

Korollar 3.5 *Seien K, L Untermoduln des Moduls M. Dann induziert die Inklusion einen Isomorphismus*

$$K/(K \cap L) \longrightarrow (K + L)/L\,.$$

Ist zudem $K \subseteq L$, so erhalten wir aus der Identitätsabbildung einen Isomorphismus

$$(M/K)/(L/K) \longrightarrow M/L\,.$$

Beweis: Für die erste Aussage wenden wir den Homomorphiesatz auf die Verkettung $K \to M \to M/L$ an. Nach der definierenden Eigenschaft von Faktorräumen gibt die Identität eine Abbildung $M/K \to M/L$. Der Homomorphiesatz gibt nun die zweite Aussage. $\square$

Kern und Kokern können auch über eine universelle Abbildungseigenschaft definiert bzw. charakterisiert werden. Sei immer noch $f : M \to N$ ein R-Modulhomomorphismus. Dann wird ein Modul K mit einer Abbildung $i : K \to M$ der Kern von f genannt, wenn $f \circ i = 0$ ist und wenn für jeden R-Modulhomomorphismus $i' : K' \to M$ mit $f \circ i' = 0$ es einen R-Modulhomomorphismus $\varphi : K' \to K$ gibt, mit $\varphi \circ i = i'$. Man zeigt (Übung), dass der Kern wie eingangs definiert ein Kern von f in Sinne dieser Abbildungseigenschaft (und damit bis auf Isomorphie eindeutig) ist.

Ein Modul C mit einer Abbildung $q : N \to C$ der Cokern von f genannt, wenn $q \circ f = 0$ ist und wenn für jeden R-Modulhomomorphismus $q' : N \to C'$ mit $q' \circ f = 0$ es einen R-Modulhomomorphismus $\psi : C \to C'$ gibt, sodass $q \circ \psi = q'$ ist. Man zeigt wieder (Übung), dass der Cokern wie eingangs definiert ein Cokern von f in Sinne dieser Abbildungseigenschaft (und damit bis auf Isomorphie eindeutig) ist.

3.3 Ketten von Untermoduln

Wir benötigen den Begriff der Länge eines R-Moduls M und dazu den Begriff von Ketten. Eine *aufsteigende Kette* der Länge ℓ in M besteht aus R-Untermoduln

$$0 \subset M_1 \subset M_2 \subset \ldots \subset M_\ell = M.$$

Wir nennen die Kette *strikt (oder echt) aufsteigend*, wenn alle Inklusionen echt sind.

Das Supremum über die Längen aller Ketten von M wird die *Länge von M* genannt und mit $\ell_R(M)$ bezeichnet. Der Nullmodul hat die Länge Null und der $\mathbb{Z}$-Modul $\mathbb{Z}$ hat die Länge ∞, wie man an der Kette $\ldots p^{k+1} \cdot \mathbb{Z} \subsetneq p^k\mathbb{Z} \subsetneq \ldots$ leicht sieht. Dies ist insbesondere eine Kette von Idealen in $\mathbb{Z}$, die wir beginnend von einem gegebenen Ideal beliebig lang machen können.

Wir spezialisieren nun im Hinblick auf den folgenden Abschnitt auf den Fall, *dass R ein Hauptidealring ist*. Dann hat eine strikt aufsteigende Kette von Idealen in R, also eine Kette $0 \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \ldots$ endliche Länge. Um dies einzusehen, bemerken wir, dass $\bigcup_{i \geqslant 0} \langle a_i \rangle \subset R$ ist wieder ein Ideal ist, also erzeugt von einem Element x, da R Hauptidealring ist. Nun ist $x \in a_n$ für ein n und somit $\langle a_{n+k} \rangle = \langle a_n \rangle$ für alle $k \geqslant 0$. (Aufgrund dieser Eigenschaft werden wir in Abschnitt ?? sagen, dass Hauptidealringe noethersch sind.)

Der Längenbegriff hat folgende Eigenschaften.

Lemma 3.6 *a) Ist $M = M' \oplus M''$ eine direkte Summe von R-Moduln, so ist $\ell_R(M) = \ell_R(M') + \ell_R(M'')$.*

b) Ist $a = \varepsilon \cdot p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ die Primfaktorzerlegung von $a \in R$ mit $\varepsilon \in R^*$ und $\nu_i \in \mathbb{N}$, so ist $\ell_R(R/aR) = \sum_{i=1}^r \nu_i$.

Beweis: Zu Teil a): Sind $0 \subsetneq M_1' \subsetneq M_2' \subsetneq \ldots \subsetneq M_r' = M'$ und $0 \subsetneq M_1'' \subsetneq M_2'' \subsetneq \ldots \subsetneq M_s'' = M$ Ketten, so ist

$$0 \subsetneq M_1' \oplus 0 \subsetneq M_2' \oplus \ 0 \subsetneq \ldots \subsetneq M_r' \oplus 0 \subsetneq M_r' \oplus M_1'' \subsetneq \ldots \subsetneq M_r'' \oplus M_s'' = M$$

eine Kette der Länge $r+s$, also $\ell_R(M) \geqslant \ell_R(M') + \ell_R(M'')$. Für die umgekehrte Ungleichung betrachten wir die Projektion $\pi'' \colon M \longrightarrow M''$ mit dem Kern M'. Ist

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M$$

eine Kette von M, so bilden die $\pi''(M_i)$ eine (nicht unbedingt echt) aufsteigende) Kette von M'' und die $M_i \cap (M' \oplus 0)$ eine (nicht unbedingt echt) aufsteigende Kette von M'. Da $M_i \subsetneq M_{i+1}$ gilt $\pi''(M_i) \subsetneq \pi''(M_{i+1})$ oder $M_i \cap (M' \oplus 0) \subsetneq M_{i+1} \cap (M' \oplus 0)$. Daraus folgt die umgekehrte Ungleichung.

Zur Aussage b): Nach dem chinesischen Restesatz ist

$$R/aR \cong \oplus_{i=1}^r R/p_i^{\nu_i} R,$$

welches ein Isomorphismus von Ringen und damit auch von $\mathbb{Z}$-Moduln ist. Nach Teil a) müssen wir also nur noch den Fall $a = p^\nu$ betrachten. In diesem Fall konstruiert man eine Kette der geforderten Länge ν durch die Ideale $p_i^s R/p_i^{\nu_i} R$ für $s =, \ldots, \nu_i - 1$. Umgekehrt entsprechen Ideale in $R/p_i^{\nu_i} R$ bijektiv den Teilern von $p_i^{\nu_i}$ und diese sind bis auf Einheiten gerade die oben verwendeten p_i^s. $\square$

3.4 Der Elementarteilersatz für Hauptidealringe

Wir schränken uns in diesem Abschnitt auf den Fall, dass R ein Hauptidealring ist, ein. Dies beinhaltet die wichtigen Fälle $R = \mathbb{Z}$ und $R = K[X]$ und die Hauptaussagen dieses Abschnitts sind ohne diese Voraussetzung nicht richtig.

Der folgende Satz wird Elementarteilersatz genannt. Aus ihm werden alle wichtigen Sätze über R-Moduln (für R ein Hauptidealring) folgen.

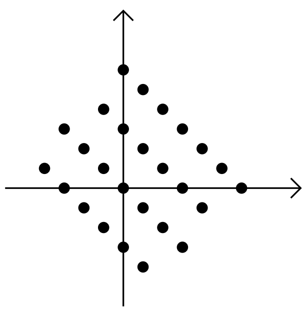
Satz 3.7 *Ist F ein freier R-Modul und M ein Untermodul von F von endlichem Rang n. Dann existieren $x_1, \ldots x_n \in F$, die Teil einer Basis von F sind, sowie $\alpha_1, \ldots, \alpha_n \in R \setminus \{0\}$, sodass*

i) $\{\alpha_1 x_1, \ldots, \alpha_n x_n\}$ *eine Basis von M ist und*

ii) $\alpha_i \mid \alpha_{i+1}$ *für $1 \leqslant i < n$.*

Die Elemente $\alpha_1, \ldots, \alpha_n$ sind bis auf Einheiten in R eindeutig bestimmt und werden Elementarteiler *von M genannt.*

Die Situation des Satzes tritt in der Natur z.B. beim Studium von Gittern auf, d.h. von freien $\mathbb{Z}$-Moduln vom Rang n, die diskret in $\mathbb{R}^n$ eingebettet sind. Gesucht sind dann die Elementarteiler wie z.B. im folgenden Bild für ein Untergitter des Standardgitters $\mathbb{Z}^2 \subseteq \mathbb{R}^2$.



Zum Beweis des Satzes benötigen wir den Begriff des *Inhalts* $\mathrm{cont}(x)$ für $x \in F$. Sei dazu $F^* = \mathrm{Hom}_R(F, R)$ der Dualraum von F. Die Menge

$$\{\varphi(x), \varphi \in F^*\} \subseteq R$$

ist ein Ideal von R, also erzeugt von einem Element $c \in R$, das bis auf Einheiten eindeutig bestimmt ist und mit $\mathrm{cont}(x)$ bezeichnet wird.

Lemma 3.8 *Ist F frei, so gelten folgende Aussagen.*

i) Ist $\{y_1, y_2, \ldots\}$ eine Basis von F und $x = \sum_{i=1}^{r} c_i y_i$ die Basisdarstellung von $x \in F$, so ist $\mathrm{cont}(x) = \mathrm{ggT}(c_1, \ldots, c_r)$.

ii) Für alle $x \in F$ gibt es $\varphi \in F^*$ mit $\varphi(x) = \operatorname{cont}(x)$.

iii) Für $x \in F$ und $\psi \in F^*$ gilt $\operatorname{cont}(x) \mid \psi(x)$.

iv) Ist $M \subseteq F$ ein Untermodul, so gibt es ein $x \in M$ mit $\operatorname{cont}(x) \mid \operatorname{cont}(y)$ für alle $y \in M$.

Beweis: ii) und iii) sind nach Definition klar. Zu i) sei $\varphi_1, \dots, \varphi_r$ die zu $y_1, \dots, y_r$ duale Basis und $\operatorname{ggT}(c_1, \dots, c_r) = \sum_{i=1}^r a_i c_i$ mit $a_i \in R$. Wir setzen $\varphi = \sum a_i \varphi_i$. Dann ist $\varphi(x) = \operatorname{ggT}(c_1, \dots, c_r)$, also $\operatorname{cont}(x) \mid \operatorname{ggT}(c_1, \dots, c_r)$. Andererseits sei ein beliebiges $F^* \ni \psi$ gegeben. Dann wird $\psi(x) = \sum \psi(y_i) c_i$ von $\operatorname{ggT}(c_1, \dots, c_r)$ geteilt und folglich $\operatorname{ggT}(c_1, \dots, c_r) \mid \operatorname{cont}(x)$.

Für iv) betrachten wir die Menge $\mathfrak{I}$ der Ideale in R der Form $\operatorname{cont}(y) \cdot R$ mit $y \in M$. In dieser Menge gibt es ein Element $\operatorname{cont}(x) \cdot R$, das in keinen Ideal der Form $\operatorname{cont}(y) \cdot R$ echt enthalten ist, denn sonst gäbe es eine unendliche strikt aufsteigende Kette von Idealen der Form $\operatorname{cont}(x_1) \cdot R \subsetneq \operatorname{cont}(x_2) \cdot R \subsetneq \cdots$, im Widerspruch dazu, dass R noethersch ist. Wir wollen zeigen, dass dieses x die gewünschte Eigenschaft hat.

Sei $\varphi \in F^*$ so, dass $\varphi(x) = \operatorname{cont}(x)$. Zunächst zeigen wir $\varphi(x) \mid \varphi(y)$ für alle $y \in M$. Wir schreiben

$$a\varphi(x) + b\varphi(y) = d := \operatorname{ggT}\big(\varphi(x), \varphi(y)\big).$$

Wegen $\varphi(ax + by) = d$ und iii) folgt $\operatorname{cont}(ax + by) \mid d \mid \varphi(x) = \operatorname{cont}(x)$. Da $\operatorname{cont}(x) \cdot R$ maximal in $\mathfrak{I}$ gewählt war, folgt hieraus $\operatorname{cont}(ax + by) = \operatorname{cont}(x) = d = \varphi(x) \mid \varphi(y)$.

Wir sind fertig, sobald wir für jedes $\psi \in F^*$ und jedes $y \in M$ die Beziehung $\varphi(x) \mid \psi(y)$ gezeigt haben. Es gilt $\varphi(x) \mid \psi(x)$ und $\varphi(x) \mid \varphi(y)$. Daher gilt $\varphi(x) \mid \psi(y)$ genau dann, wenn $\varphi(x) \mid \Big(\psi(y) - \frac{\varphi(y)}{\varphi(x)}\psi(x)\Big) = \psi\Big(y - \frac{\varphi(y)}{\varphi(x)} \cdot x\Big)$. Wir können also ohne Einschränkung y durch $y - \frac{\varphi(y)}{\varphi(x)} \cdot x$ ersetzen, anders gesagt, wir können unsere Betrachtung auf $y \in M$ mit $\varphi(y) = 0$ reduzieren. Mit dem gleichen Argument können wir ψ durch $\psi - \frac{\psi(x)}{\varphi(x)} \cdot \varphi$ ersetzen und damit $\psi(x) = 0$ annehmen. Sei nun

$$a\varphi(x) + b\psi(y) = d =: \operatorname{ggT}\big(\varphi(x), \psi(y)\big).$$

Dann ist

$$(\varphi + \psi)(ax + by) = a\varphi(x) + b\psi(y) = d,$$

also $\operatorname{cont}(ax + by) \mid d \mid \varphi(x) = \operatorname{cont}(x)$. Wieder besagt die Maximalität, dass diese Teilbarkeitsbeziehung alles Gleichheiten (bis auf Einheiten) sind und daher

$$\varphi(x) \mid d \mid \psi(y),$$

was zu zeigen war. $\square$

Beweis von Satz 3.7: Wir zeigen zunächst induktiv nach $n = \mathrm{Rang}(M)$ die im Satz implizit enthaltene Aussage, dass M frei ist. M ist sicher torsionsfrei, da F dies ist. Also ist für $n = 0$ nichts weiter zu zeigen. Wir wählen für den Induktionsschritt ein $x \in M$ wie in Lemma 3.8 iv) und $\varphi \in F^*$, sodass $\varphi(x) = \mathrm{cont}(x)$. Weiter gibt es ein $x_1 \in F$ mit $x = \varphi(x) \cdot x_1$, denn falls $x = \sum c_i y_i$ in einer Basis $y_1, \ldots, y_r$ von F, so leistet $\sum c_i/\varphi(x) \cdot y_i$ das Verlangte. Wir definieren $F' = \mathrm{Ker}(\varphi)$ und $M' = M \cap F'$. Wir behaupten, dass

$$F = Rx_1 \oplus F' \quad \text{und} \quad M = Rx \oplus M'$$

gilt. In der ersten Formel ist die Summe offenbar direkt und ist $y \in F$, so ist $y - \varphi(y) \cdot x_1 \in \mathrm{Ker}(\varphi)$. Die zweite Summe ist ebenso direkt, wir müssen zeigen, dass die beiden Summanden ganz M aufspannen. Unter Verwendung von Lemma 3.8 iv) ist

$$y = \frac{\varphi(y)}{\varphi(x)} \cdot x + \left(y - \frac{\varphi(y)}{\varphi(x)} x\right)$$

die gewünschte Darstellung für ein $y \in M$ beliebig. Wir können nun die Induktionsvoraussetzung auf M' anwenden und erhalten, dass M frei ist.

Wir können ebenso per Induktion nach $\mathrm{Rang}(M)$ annehmen, dass die Folgerungen des Satzes für M' bereits gelten, d.h. dass $x_2, \ldots, x_n$ Teil einer Basis von F' ist und es $\alpha_2, \ldots, \alpha_n$ gibt mit $\alpha_i \mid \alpha_{i+1}$ für $i \geqslant 2$, sodass $\alpha_2 x_2, \ldots, \alpha_n x_n$ eine Basis von M' ist. Mit x_1 wie oben und $\alpha_1 = \varphi(x)$ wir oben ist nur noch $\alpha_1 \mid \alpha_2$ zu zeigen. Sei dazu $\varphi_2 \in F^*$ mit $\varphi_2(x_2) = 1$. Dann gilt nach dem vorigen Lemma $\varphi(x) \mid \varphi_2(\alpha_2 x_2)$, also $\alpha_1 \mid \alpha_2$.

Die Eindeutigkeitsaussage folgt aus dem nächsten Lemma. □

Lemma 3.9 *Sei R ein Hauptidealring und $T \cong \bigoplus_{i=1}^n R/\alpha_i R$, wobei $\alpha_1, \ldots, \alpha_n \in R \setminus \{0\}$ Nichteinheiten mit $\alpha_i \mid \alpha_{i+1}$ sind. Dann sind $\alpha_1, \ldots, \alpha_n$ bis auf Einheiten in R eindeutig.*

Beweis: Der Beweis verwendet die Elemente größter Ordnung in T und daher ist es günstig, die Reihenfolge der Indizierung umzudrehen. Sei also $\widetilde{\alpha}_i = \alpha_{n-i+1}$ und folglich $\widetilde{\alpha}_{i+1} \mid \widetilde{\alpha}_i$. Wir nehmen an, dass es eine weitere Summenzerlegung

$$T \cong \bigoplus_{i=1}^{n} R/\widetilde{\alpha}_i R \cong \bigoplus_{j=1}^{m} R/\widetilde{\beta}_j R$$

ebenfalls mit $\beta_{j+1} \mid \beta_j$ gibt. Wir nehmen an, dass die Zerlegungen echt verschieden sind, sei k der kleinste Index mit $\widetilde{\alpha}_k R \neq \beta_k R$. Wir betrachten die Zerlegung des R-Moduls $\widetilde{\alpha}_k T$. Da für $\ell > k$ die $\widetilde{\alpha}_\ell$ alle Teiler von $\widetilde{\alpha}_k$ sind, erhalten wir

$$\widetilde{\alpha}_k T \cong \bigoplus_{i=1}^{k-1} \widetilde{\alpha}_k (R/\widetilde{\alpha}_i R) \cong \bigoplus_{i=1}^{k-1} \widetilde{\alpha}_k (R/\widetilde{\alpha}_i R) \oplus \widetilde{\alpha}_k \cdot (R/\widetilde{\beta}_k R) \oplus \ldots.$$

Da $\ell_R(\widetilde{\alpha}_k T) < \infty$ folgt aus dem Vergleich der Längen beider Seiten mit Hilfe von Lemma 3.6, dass $\widetilde{\alpha}_k \cdot (R/\widetilde{\beta}_k R) = 0$ ist, mit anderen Worten $\widetilde{\alpha}_k R \subset \widetilde{\beta}_k R$. Durch Vertauschen der Rollen von $\widetilde{\alpha}_k$ und $\widetilde{\beta}_k$ erhalten wir die umgekehrte Inklusion, insgesamt die Gleichheit im Widerspruch zur Wahl von k. Ist $\widetilde{\alpha}_j = \widetilde{\beta}_j$ für alle $j \leq \min\{m, n\}$, so folgt ebenfalls durch Berechnen von $\ell_R(T)$, dass $m = n$ ist. Insgesamt beweist dies das Lemma. $\square$

Beweis von Satz 3.7, Eindeutigkeit: Nach dem bereits Bewiesenen gibt es Elementarteiler $\alpha_1 \mid \alpha_2 \mid \ldots \mid \alpha_n$ von M und wir nehmen an, dass $\beta_1 \mid \beta_2 \mid \ldots \mid \beta_m$ ebenfalls Elementarteiler (bzgl. einer anderen Basis von F) sind. Wir definieren zu M die Menge:

$$M_{\mathsf{Sat}} = \{y \in F : \exists 0 \neq a \in R : a \cdot y \in M\}.$$

Man prüft sofort, dass M_{Sat} ein Untermodul von F ist, genannt die *Saturierung* von M in F. Wir behaupten, dass

$$M_{\mathsf{Sat}}/M \cong \bigoplus_{i=1}^{n} R/\alpha_i R \cong \bigoplus_{j=1}^{m} R/\beta_j R$$

ist. Sobald wir dies gezeigt haben, folgt die Eindeutigkeitsaussage aus dem vorangegangenen Lemma.

Zum Beweis der Behauptung verwenden wir die Basis $x_1, \ldots, x_n$ aus dem bereits bewiesenen Teil des Satzes. Es ist $\bigoplus_{i=1}^n R \cdot x_i \subseteq M_{\mathsf{Sat}}$ denn $\alpha_i(r_i \cdot x_i) = r_i(\alpha_i \cdot x_i) \in M$ für beliebiges r_i. Um zu zeigen, dass die Inklusion eine Gleichheit ist, nehmen wir $y \in M_{\mathsf{Sat}}$ beliebig her. Wir ergänzen $x_1, \ldots, x_n$ zu einer Basis $x_1, \ldots, x_t$ von F und schreiben $y = \sum_{i=1}^t c_i x_i$. Es ist $a \cdot y \in M$ für ein $0 \neq a \in R$ nach Definition der Saturierung. Also ist $\sum_{i=1}^t a c_i x_i \in M$. Daraus folgt, dass $a \cdot c_i = 0$ für $i = n+1, \ldots, t$. Da R nullteilerfrei ist, folgt $c_i = 0$, was zu zeigen war.

Insgesamt ist also

$$M = \bigoplus_{i=1}^{n} R \cdot (\alpha_i x_i) \subseteq M_{\mathsf{Sat}} = \bigoplus_{i=1}^{n} R \cdot x_i$$

und daraus folgt die obige Behauptung über den Quotientenmodul. $\square$

Der oben genannte Beweis ist allerdings nicht in offensichtlicher Weise konstruktiv, d.h. nicht direkt in einen programmierbaren Algorithmus umzusetzen. Das Problem ist die Anwendung von Lemma 3.8 iv) zu Beginn des Beweises. Das gewünschte Element x dort wird als maximales Element einer Kette gewonnen und wir haben bisher uns keine Gedanken gemacht (wie wir größere Ideale in dieser Kette finden können und vor allem), wann diese Kette aufhört.

In der Praxis liegt die freie Modul F oft durch Angabe einer Basis $x_1, \ldots, x_r$ und M durch Erzeuger $z_1, \ldots, z_m$ vor, wobei $z_j = \sum_{i=1}^r a_{ij} x_i$. Wir fassen die

Koeffizienten in einer Matrix $A = (a_{ij})$ zusammen. Ziel ist es, die Elementarteiler anhand von A auszurechnen.

Sind $I \subseteq \{1, 2, \ldots, r\}$ und $J \subseteq \{1, 2, \ldots, m\}$ zwei Teilmengen mit t Elementen, so bezeichnen wir mit A_{IJ} die $t \times t$-Matrix, deren Eintrag an der Stelle (u, v) gerade $a_{i_u j_v}$ ist, wobei die Indexmengen als $I = \{i_1, \ldots, i_t\}$ mit $i_\ell < i_{\ell+1}$ und $J = \{j_1, \ldots, j_t\}$ mit $j_\ell < j_{\ell+1}$ für alle ℓ aufgezählt sind. Als *t-Minore* von A bezeichnet man die Determinante einer Matrix A_{IJ} mit I und J wie oben. Zum Beweis des folgenden Satzes ist es günstig, den Begriff des t-fachen äußeren Produkts $\Lambda^t F$ eines Moduls F zu verwenden. Wir definieren diesen hier ad hoc und nur für freie R-Moduln. (Siehe Abschnitt 4.2 für den Begriff im Allgemeinen). Sei also $x_1, \ldots, x_r$ eine Basis von F. Dann ist $\Lambda^t F$ der freie R-Modul erzeugt von Symbolen der Form $x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_t}$, wobei $1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant r$. Wir definieren für jede Indexmenge $j_1, j_2, \ldots, j_t$ ein Element $x_{j_1} \wedge x_{j_2} \wedge \ldots x_{j_t} \in \Lambda^t F$, indem wir dies als Null erklären, falls zwei Indizes gleich sind und andernfalls die Permutation $\pi \in S_t$ verwenden, sodass $j_\ell = i_\pi(\ell)$ mit $i_1 < i_2 < \ldots < i_t$. Dann definieren wir

$$x_{i_{\pi(1)}} \wedge x_{i_{\pi(2)}} \wedge \ldots \wedge x_{i_{\pi(t)}} = \operatorname{sgn}(\pi) x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_t}.$$

Schließlich definieren wir für ein beliebiges t-Tupel $z_1, \ldots, z_t$ von Elementen in F ein Element („t-faches äußeres Produkt“) $z_1 \wedge z_2 \wedge \ldots \wedge z_t \in \Lambda^t F$ durch sogenannte multilineare Fortsetzung. Damit ist gemeint, dass falls $z_i = \sum_{i=1}^r a_{ij} x_j$ die Basisdarstellung von z_i ist, wir das t-fache äußere Produkt der z_i definieren als

$$\begin{aligned} z_1 \wedge \ldots \wedge z_t &= \left(\sum_{j=1}^r a_{1j} x_j \right) \wedge \left(\sum_{j=1}^r a_{2j} x_j \right) \wedge \ldots \wedge \left(\sum_{j=1}^r a_{tj} x_j \right) \\ &= \sum_{j_1, \ldots, j_t = 1}^r a_{1j_1} \cdot a_{2j_2} \cdot \ldots \cdot a_{tj_t} \cdot (x_{j_1} \wedge x_{j_2} \wedge \ldots \wedge x_{j_t}) \\ &= \sum_{\substack{j_1, \ldots, j_t = 1 \\ \text{alle } j_k \text{ verschieden}}}^r a_{1j_1} \cdot a_{2j_2} \cdot \ldots \cdot a_{tj_t} \cdot (x_{j_i} \wedge x_{j_2} \wedge \ldots \wedge x_{j_t}) \\ &= \sum_{1 \leq i_1 < i_2 < \ldots < i_t \leq r} D(i_1, \ldots, i_t)(x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_t}) \end{aligned} \tag{3.3}$$

wobei

$$D(i_1, \ldots, i_t) \;=\; \sum_{\pi \in S_t} \operatorname{sgn}(\pi) a_{1 i_{\pi(1)}}, a_{2 i_{\pi(2)}} \ldots a_{t i_{\pi(t)}}\,.$$

(Diese Rechnung zeigt auch, dass die Definition von $\Lambda^t F$ nicht von der Wahl einer Basis abhängt, denn falls $z_1, \ldots, z_t$ eine andere Basis ist, so ist die Determinante der Basiswechselmatrix eine Einheit.)

Aus dieser Rechnung folgt auch, dass aus einer Inklusion $M \subseteq F$ von R-Moduln eine Inklusion $\Lambda^t M \subseteq \Lambda^t R$ der äußeren Produkte entsteht. Ist die

Basis $x_1, \ldots, x_t$ durch Ergänzen einer Basis von $x_1, \ldots, x_n$ wie im Elementarteilersatz entstanden, so bilden die $\alpha_1 x_1, \ldots, \alpha_n x_n$ eine Basis von M und somit die Elemente

$$\alpha_{i_1} x_{i_1} \wedge \alpha_{i_2} x_{i_2} \wedge \ldots \wedge \alpha_{i_t} x_{i_t} = (\alpha_{i_1} \alpha_{i_2} \cdot \ldots \cdot \alpha_{i_t}) x_{i_1} \wedge x_{i_2} \ldots \wedge x_{i_t} \tag{3.4}$$

eine Basis von $\Lambda^t M$. Diese sind (von Null verschiedene) Vielfache von Basiselementen von $\Lambda^t F$.

Satz 3.10 *Sei F ein endlich erzeugter freier R-Modul mit Basis $x_1, \ldots, x_r$. Sei $M \subseteq F$ ein Untermodul mit Erzeugern $z_1, \ldots, z_m$, wobei $z_i = \sum_{j=1}^r a_{ij} x_j$ und seien $\alpha_1, \ldots, \alpha_n$ die Elementarteiler von M. Sei μ_t der* ggT *aller t-Minoren der Koeffizientenmatrix $A = (a_{ij})$. Dann gilt*

$$\mu_t = \prod_{i=1}^t \alpha_i.$$

Beweis: Wir beginnen mit dem Fall $t = 1$. Es sei $\alpha_1 R$ das Ideal, welches von allen $\varphi(y)$ mit $(\varphi \in F^*)$ und $y \in M$ erzeugt wird. Ist $\psi_1, \ldots, \psi_r$ die Dualbasis zu $x_1, \ldots, x_r$, so lässt sich ein beliebiges φ als Linearkombination $\varphi = \sum_{\ell=1}^r b_\ell \psi_\ell$ schreiben. Weiter ist $y = \sum_{i=1}^m c_i z_i$ und insgesamt

$$\begin{aligned} \varphi(y) &= \sum_{\ell=1}^r b_\ell \psi_\ell \left(\sum_{i=1}^m c_i \cdot z_i \right) \\ &= \sum_{\ell=1}^r b_\ell \psi_\ell \left(\sum_{i=1}^m \sum_{j=1}^r c_i \cdot a_{ij} x_j \right) \\ &= \sum_{i=1}^m \sum_{j=1}^r c_i a_{ij} b_j \end{aligned}$$

Also ist das Ideal $\alpha_1 R$ gerade von den a_{ij} für $i = 1, \ldots, m$ und $j = 1, \ldots, r$ erzeugt, d.h. von den 1-Minoren von A.

Wir wenden diese Aussage auf die Inklusion von freien R-Moduln $\Lambda^t M \subset \Lambda^t F$ für beliebiges t an. Unter Verwendung der Basis aus Gleichung (3.4) sieht man, dass der erste Elementarteiler für diese Inklusion gleich $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_t$ ist, da $\alpha_i \mid \alpha_{i+1}$ und somit der ggT über alle Indextupel $\{i_1, \ldots, i_t\}$ angenommen wird. Mit dem Erzeugendensystem $z_1, \ldots, z_m$ von M wird $\Lambda^t M$ von den $z_{j_1} \wedge \ldots \wedge z_{j_t}$ aufgespannt, deren Basisdarstellung in den $x_{i_1} \wedge \ldots \wedge x_{i_t}$ wir in Gleichung (3.3) ausgerechnet haben, dort im Spezialfall $j_1 = 1, \ldots, j_t = t$. Dort war der Koeffizient die t-Minore $A_{\{1,\ldots,t\},\{i_1,\ldots,i_t\}}$. Für beliebiges $j_1, \ldots, j_t$ erhalten wir analog als Koeffizient eine beliebige t-Minore von A. Insgesamt besagt das erste Argument, dass der ggT aller t-Minoren gleich $\alpha_1 \cdot \ldots \cdot \alpha_t$ ist, was zu zeigen war. $\square$

Wir wollen noch aus diesem Satz eine Algorithmus zur Bestimmung der Elementarteiler eines Untermoduls ableiten. Äquivalenterweise suchen wir zu einer Matrix A (der Koeffizientenmatrix aus dem vorigen Satz) invertierbare

Matrizen S und T (die zu einem Basiswechsel in M bzw. F gehören), sodass $D = TAS$ die Einträge $D_{ii} = \alpha_i$ mit $\alpha_i \mid \alpha_{i+1}$ für $i = 1, \ldots, n$ und sonst nur Nullen als Einträge hat.

Angenommen wir haben bereits erreicht, dass der linke obere Eintrag a_{11} alle Einträge von A teilt. Dann ist insbesondere a_{i1} und a_{1j} für alle i, j durch a_{11} teilbar. Also ist die Addition des $-\frac{a_{1j}}{a_{11}}$-fachen der ersten Spalte zur j-ten Spalte eine durch ein Element in $\mathrm{GL}_2(R)$, also ein Basiswechsel in F beschrieben. Ebenso ist die Addition des $\left(-\frac{a_{i1}}{a_{11}}\right)$-fachen der ersten Zeile zur i-ten Zeile Resultat eines Basiswechsels in M. Am Ende dieser Schritte hat die Matrix in der ersten Zeile und Spalte mit Ausnahme von a_{11} nur Nullen und wir können induktiv den Algorithmus auf die Untermatrix ohne die erste Zeile und Spalte anwenden. Um die erste Annahme zu erreichen nehmen wir vereinfachend an, dass der Ring R euklidisch bzgl. der Gradfunktion δ ist. (Dies beinhaltet $R = K[x]$ und $\delta = \deg$ sowie $R = \mathbb{Z}$ und $\delta = |\cdot|$). Sei

$$d = \min_{i,j=1\ldots n} \bigl\{\delta(a_{ij})\bigr\}.$$

Einen der Matrixeinträge mit kleinstem $\mathrm{Grad} \neq 0$ können wir durch Zeilen- und Spaltenvertauschungen in der linken oberen Ecke annehmen. Wir zeigen, dass entweder a_{11} alle Einträge von A teilt oder wir d durch elementare Zeilen- und Spaltenumformungen (d.h. Basiswechsel in M bzw. F) verringern können.

Falls ein Eintrag der ersten Zeile, etwa a_{1j} nicht durch a_{11} teilbar ist, so schreiben wir $a_{ij} = q \cdot a_{11} + b$ mit $\delta(b) < d$ und durch $(-q)$-fache Addition der ersten Spalte auf die j-te Spalte erreichen wir, dass in der neuen Matrix $\widetilde{A}$ der Eintrag $\widetilde{a}_{1j} = b$ ist und $\delta(b) < d$ gilt. Analog gehen wir vor, wenn ein Eintrag der ersten Spalte nicht durch a_{11} teilbar ist. Da $d \in \mathbb{N}$ müssen wir dies nur endlich oft durchführen. Wie in der Anfangsbemerkung können wir nun durch Zeilen- und Spaltenoperationen erreichen, dass $a_{i1} = 0$ und $a_{1j} = 0$ für $i \geqslant 2$ und $j \geqslant 2$.

Angenommen in der „Restmatrix" gibt es noch einen Eintrag a_{ij} mit $i \geqslant 2$ und $j \geqslant 2$, der nicht durch a_{11} teilbar ist, also $a_{ij} = qa_{11} + b$ mit $0 < \delta(b) < d$. Dann addieren wir die erste Zeile zur i-ten, sodass nun $a_{i1} = a_{11}$, aber a_{ij} unverändert ist. Schließlich addieren wir $(-q)$ mal die erste Spalte auf die j-te Spalte, sodass nun $a_{ij} = b$ gilt. Auf diese Weise haben wir d verringert und beginnen mit dem Algorithmus von neuem. Da $d \in \mathbb{N}$ müssen wir dies nur endlich oft durchführen. Danach ist a_{11} in der Tat der erste Elementarteiler und wir können uns im gesamten Algorithmus auf die Restmatrix mit $i \geqslant 2$ und $j \geqslant 2$ beschränken.

3.5 Struktursätze für Moduln über Hauptidealringen

Wir halten einige wichtige Folgerungen aus dem Elementarteilersatz fest. In diesem Abschnitt ist immer noch R ein Hauptidealring.

Korollar 3.11 *Sei M ein endlich erzeugter R-Modul und $M_{tor} \subseteq M$ der Torsionsuntermodul. Dann ist M_{tor} endlich erzeugt und es gibt einen freien R-Modul M_F, sodass $M \cong M_{tor} \oplus M_F$. Insbesondere hat jeder endlich erzeugte torsionsfreie R-Modul eine Basis.*

Beweis: Seien $z_1, \ldots, z_r$ Erzeuger von M und $F \cong R^r$ ein freier R-Modul vom Rang r mit Basis $y_1, \ldots, y_r$. Sei $\varphi\colon F \longrightarrow M$ der Homomorphismus mit $\varphi(y_i) = z_i$. (Wie bei Vektorräumen ist auch bei freien Moduln ein Homomorphismus eindeutig durch die Bilder der Basis festgelegt und die Bilder der Basis können beliebig gewählt werden.) Wir wenden den Elementarteilersatz auf das Paar $\mathrm{Ker}(\varphi) \subseteq F$ an. Seien $x_1, \ldots, x_n$ die Elemente von $\ker(\varphi)$ aus diesem Satz, durch $x_{n+1}, \ldots, x_r$ zu einer Basis von F ergänzt und $\alpha_1, \ldots, \alpha_n$ die Elementarteiler, also

$$\mathrm{Ker}(\varphi) = \bigoplus_{i=1}^{n} R \cdot (\alpha_i x_i) \leqslant F = \bigoplus_{i=1}^{n} R \cdot x_i \oplus \bigoplus_{i=n+1}^{r} R \cdot x_i.$$

Also ist

$$M \cong F/\,\mathrm{Ker}(\varphi) \cong \bigoplus_{i=1}^{n} (R/\alpha_i R)\, x_i \oplus \bigoplus_{i=n+1}^{r} R \cdot x_i.$$

Der erste Summand ist offenbar ein Torsionsmodul, der zweite ist frei und wir haben die gewünschte Zerlegung gefunden. □

Wir zerlegen den Torsionsuntermodul weiter und definieren hierzu für ein Primelement p in R

$$M_p = \{x \in M : p^n x = 0 \quad \text{für ein} \quad n \in \mathbb{N}\},$$

genannt der *p-Torsionsanteil* von M.

Korollar 3.12 *Ist M ein endlich erzeugter Torsionsmodul, so ist*

$$M = \bigoplus_{p \in P} M_p,$$

wobei P die Menge der Primelemente (bis auf Assoziiertheit) von R bezeichnet. Dabei ist $M_p = 0$ für fast alle $p \in P$. Weiter gibt es für jedes p eine Folge natürlicher Zahlen $1 \leq \nu_{p,1} \leq \nu_{p,2} \leq \ldots \leq \nu_{p,r(p)}$, sodass

$$M_p \cong \bigoplus_{j=1}^{r(p)} R/p^{\nu_{p,j}} R$$

Mit dieser Eigenschaft sind die Zahlen $\nu_{p,j}$ eindeutig durch M bestimmt.

Dies ist auch der angekündigte Struktursatz über endlich erzeugte abelsche Gruppen (d.h. $\mathbb{Z}$-Moduln). Jede solche ist direkte Summe eines freien $\mathbb{Z}$-Moduls (also $\mathbb{Z}^r$) und eines Torsionsmoduls, für welche obige Zerlegung gilt.

Da $\mathbb{Z}/p^\nu\mathbb{Z}$ für alle $j \leq \nu$ eine Untergruppe der Ordnung p^j enthält, folgt aus dem Korollar oben, dass eine endliche abelsche Gruppe der Ordnung n für jeden Teilnehmer m von n eine Untergruppe der Ordnung m enthält.

Beweis von Korollar 3.12: Nach dem vorigen Korollar wissen wir bereits, dass $M = M_{\text{tor}} \cong \bigoplus_{i=1}^n R/\alpha_i R$ ist, wobei $\alpha_i \mid \alpha_{i+1}$ gilt. Sei $\alpha_i = \varepsilon_i \prod_{p\in P} p^{\nu_{p,i}}$ die Faktorisierung der α_i, wobei $\varepsilon_i \in R^*$. Nach dem chinesischen Restesatz gilt

$$R/\alpha_i R \cong \bigoplus_{p\in P} R/p^{\nu_{p,i}}R.$$

Durch Kombination dieser Zerlegung erhält man

$$M \cong \bigoplus_{p\in P} \bigoplus_{i=1}^{n} R/p^{\nu_{p,i}}R.$$

Dies ist offenbar bereits die gewünschte Zerlegung in p-Torsionsanteile. Um die $\nu_{p,i}$ wie gefordert zu erhalten, genügt es, diejenigen $\nu_{p,i}$ wegzulassen, die Null sind und zur Zerlegung sowieso nicht beitragen. Die Eindeutigkeitsaussage folgt leicht aus der Eindeutigkeitsaussage in Lemma 3.9. $\square$

4 Tensorprodukt und äußere Algebra

Das Tensorprodukt von Moduln ist eine Konstruktion, die zwei wesentlichen Konstruktionen aus der multilinearen Algebra, Bilinearformen und Determinantenformen verallgemeinert bzw. genauer gesagt als Untermoduln enthält. Es erlaubt zudem einen S-Modul M als R-Modul aufzufassen, falls es einen Ringhomomorphismus $f : R \to S$ gibt. Dieses Konzept wird als Basiswechsel in vielen Situation wiederauftreten.

4.1 Das Tensorprodukt

Das Tensorprodukt ist durch eine universelle Abbildungseigenschaft (UAE) definiert. Geben seien die R-Moduln $M_1, \dots, M_n$ sowie N. Eine Abbildung $f : M_1 \times \cdots M_n \to N$ wird *multilinear* genannt, wenn sie nach fixieren von $n-1$ beliebigen Argumenten R-linear im verbleibenden Argument ist. Für $n = 2$ spricht man auch von *bilinearen* Abbildungen.

Das *Tensorprodukt* von M_1 und M_2 ist ein R-Modul, den wir mit $M_1 \otimes_R M_2$ bezeichnen, mit einer R-bilinearen Abbildung $q : M_1 \times M_2 \to M_1 \otimes_R M_2$, mit folgender Eigenschaft: Zu jeder bilinearen Abbildung $f : M_1 \times M_2 \to N$ in einen R-Modul N gibt es genau eine Abbildung $F : M_1 \otimes_R M_2 \to N$, sodass $F \circ q = f$ ist.

Satz 4.1 *Zu zwei beliebigen R-Moduln M_1 und M_2 existiert ein Tensorprodukt.*

Beweis: Sei zunächst $M = R^{M_1 \times M_2}$ der freie R-Modul mit Basiselementen (m_1, m_2) für $m_i \in M_i$. Aus diesem freien Modul wollen wir einen Untermodul herausdivieren (d.h. einen Quotientenmodul betrachten), indem alle Relationen stecken, die bei bilinearen Abbildungen gelten. Wir definieren also $U \subset M$ als den von Elementen

$$\begin{aligned} & r(m_1, m_2) - (rm_1, m_2), \quad r(m_1, m_2) - (m_1, rm_2), \\ & (m_1 + m_1', m_2) - (m_1, m_2) - (m_1', m_2) \\ \text{und} \quad & (m_1, m_2 + m_2') - (m_1, m_2) - (m_1, m_2') \end{aligned} \tag{4.1}$$

für alle $r \in R$ und $m_1, m_1' \in M_1$ sowie $m_2, m_2' \in M_2$ erzeugten Untermodul. Der Quotient ist also $M_1 \otimes_R M_2 := M/U$. Wir schreiben $m_1 \times m_2$ für die Restklassen von (m_1, m_2) und q für die Quotientabbildung.

Sei also nun $f : M_1 \times M_2 \to N$ gegeben. Dann ist $U \subset \mathrm{Ker}(f)$ nach Definition einer bilinearen Abbildung. Also steigt f zu F mit $F \circ q = f$ ab. Diese Abbildung ist auch eindeutig, denn M/U ist von allen sogenannten *Elementartensoren* $m_1 \times m_2$ erzeugt und hierauf ist der Wert von F als $f(m_1, m_2)$ vorgegeben. $\square$

Es gelten folgende elementare Eigenschaften.

i) Es gilt $R \otimes M = M$, denn die von $(r, m) \mapsto rm$ induzierte Abbildung $R \otimes M \to M$ hat als Inverses $m \mapsto 1 \otimes m$.

ii) Mit Hilfe der Argumentvertauschungsabbildung $(m_1, m_2) \mapsto (m_2, m_1)$ sieht man ein, dass $M_1 \otimes M_2 \cong M_2 \times M_1$ ist.

iii) Das Tensorprodukt ist assoziativ, d.h. (Übung, man verwende stets die universelle Eigenschaft)

$$(M_1 \otimes M_2) \otimes M_3 = M_1 \otimes (M_2 \otimes M_3)\,.$$

Beispiel 4.2 i) Bei freien Moduln $M_i = R^{X_i}$ für $i = 1, 2$ ist $M_1 \otimes M_2$ der freie Modul über der Produktmenge $X_1 \times X_2$. Dies ist ein Spezialfall der Aussage, dass das Tensorprodukt mit Summen vertauscht (Übung!), dass also gilt

$$M \otimes_R (\oplus_{i \in I} N_i) \;=\; \oplus_{i \in I}(M \otimes_R N_i) \tag{4.2}$$

und analog im ersten Argument.

ii) Bei Moduln, die nicht frei sind, kann das Tensorprodukt 'kleiner' als die Bestandteile werden. Zum Beispiel ist $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ der Nullmodul, denn

$$a \otimes b = a \cdot (1 \otimes b) = a \cdot (4 \otimes b) = a \cdot (1 \otimes 4b) = 0$$

für alle $a, b \in \mathbb{Z}$. Das gleiche Argument gibt auch $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\operatorname{ggT}(m,n)\mathbb{Z}$ (Übung).

Auch für Morphismen gibt es ein natürliches Tensorprodukt. Seien $f_1 : M_1 \to N_1$ und $f_2 : M_2 \to N_2$ zwei R-Modulhomomorphismen. Die Verkettung der Produktabbildung mit der Quotientabbildung in der Definition des Tensorprodukts $N_1 \otimes_R N_2$ induziert eine natürliche Abbildung zwischen den Tensorprodukten, die wir mit

$$f_1 \otimes f_2 : M_1 \otimes M_2 \to N_1 \otimes N_2$$

bezeichnen. Ist f_2 die Identität auf einem R-Modul T, so schreibt man oft auch $f_1 \otimes T$ (oder einfach f_1) für $f_1 \otimes \mathrm{id}_T$. Aus der Definition folgt unmittelbar, dass falls $g_i : N_i \to T_i$ weitere R-Modulhomomorphismen sind, so ist

$$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) \;=\; (g_1 \circ f_1) \otimes (g_2 \circ f_2)$$

Die Verträglichkeit zwischen Menge der R-Modulhomomorphismen mit dem Tensorprodukt beschreibt folgender Satz. ('Adjungiertheit der Funktoren Hom und Tensorieren')

Satz 4.3 *Sind M, N und T drei R-Moduln, so gibt es einen natürlichen Isomorphismus von R-Moduln*

$$\mathrm{Hom}_R(M \otimes_R N, T) \;=\; \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, T)) \;.$$

Beweis: Ist $\varphi : M \otimes_R N \to T$ ein Objekt der linken Seite, gibt nach Vorverkettung mit der Quotientabbildung eine R-bilineare Abbildung $\widetilde{\varphi} : M \times N \to T$, die durch Fixieren des ersten Arguments als Abbildung $\psi : M \to \mathrm{Hom}_R(N, T)$ auffassen kann. Die R-Linearität von $\widetilde{\varphi}$ im zweiten Argument rechtfertigt dabei, dass das Bild wirklich in $\mathrm{Hom}_R(N, T)$ liegt. Die R-Linearität von $\widetilde{\varphi}$ im ersten Argument besagt gerade, das ψ wieder R-linear ist.

Ist umgekehrt $\psi \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, T))$ gegeben, so fassen wir dies als Abbildung $M \times N \to T$ auf, die bilinear ist aufgrund der R-Linearitäten in der Definition von $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, T))$. Also erhalten wir nach Definition des Tensorprodukts eine Abbildung $\varphi : M \otimes_R N \to T$ und die beiden Konstruktionen sind offenbar zueinander invers. $\square$

Seien nun $f : M_1 \to M$ und $g : M \to M_2$ zwei R-Modulhomomorphismen. und T ein R-Modul. Es gilt:

Satz 4.4 *Ist g surjektiv, so ist auch $g \otimes_R T$ surjektiv. Gilt in diesem Fall zudem $\mathrm{Bild}(f) = \mathrm{Ker}(g)$, so ist auch $\mathrm{Bild}(f \otimes_R T) = \mathrm{Ker}(g \otimes_R T)$.*

In der Sprechweise von Abschnitt 6.5 ist das Tensorprodukt also ein rechtsexakter Funktor. Es ist nicht exakt, denn es gilt:

Beispiel 4.5 Ist $f : M_1 \to M$ injektiv, so ist $f_1 \otimes_R T$ im Allgemeinen nicht injektiv. Sei zum Beispiel $f : \mathbb{Z} \to 2\mathbb{Z}$ die Multiplikation mit zwei und $T = \mathbb{Z}/2\mathbb{Z}$. Dann ist $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$ und andererseits das Bild $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ der Nullmodul.

Beweis: Für die Surjektivität genügt es zu bemerken, dass das Tensorprodukt von Elementartensoren erzeugt wird. Die zweite Aussage ist ein Spezialfall der Aussage, das Tensorprodukt und Cokern vertauschen, dass also für $f : M_1 \to M$ die Isomorphie von

$$\mathrm{coker}(f \otimes_R T) \;=\; \mathrm{coker}(f) \otimes_R T$$

gilt. Wir zeigen dies, indem wir die Abbildungseigenschaft prüfen. Aus der Quotientabbildung $q : M \to \mathrm{coker}(f)$ erhalten wir eine Quotientabbildung $q \otimes T : M \otimes_R T \to \mathrm{coker}(f) \otimes_R T$. Die Verkettungsbedingung $(q \otimes T) \circ (f \otimes T) = (q \circ f) \otimes T = 0$ gilt offenbar. Ist ein Morphismus $q' : M \otimes_R T \to U$ gegeben, der auch der Verkettungsbedingung $q' \circ (f \otimes T) = 0$ genügt, so fassen wir diesen mit Hilfe von Satz 4.3 als $Q' : M \to \mathrm{Hom}_R(T, U)$ auf. Die Verkettungsbedingung besagt nun nach Konstruktion der Korrespondenz im Beweis von Satz 4.3, dass $Q' \circ f = 0$ ist. Also gibt es nach der universellen Eigenschaft des Kokerns, angewandt auf den R-Modul $\mathrm{Hom}_R(T, U)$ und Q' eine Abbildung $\Psi : \mathrm{coker}(f) \to \mathrm{Hom}_R(T, U)$ mit $\Psi \circ q = Q'$. Die umgekehrte Abbildung in Satz 4.3 liefert nun die gesuchte Abbildung $\psi : \mathrm{coker}(f) \otimes T \to U$ mit $\psi \circ (q \otimes T) = q'$. Die Eindeutigkeit von ψ folgt aus der Eindeutigkeit von Ψ. $\square$

4.2 Die Tensoralgebra, symmetrische Algebra, äußere Algebra

Sei M ein R-Modul. Die direkte Summe

$$T_R(M) \;=\; R \oplus M \oplus (M \otimes_R M) \oplus (M \otimes_R M \otimes_R M)$$

ist wiederum ein R-Modul, hat aber noch weitere Struktur: Auf $T_R(M)$ definiert man ein Produkt, das auf Elementartensoren mittels

$$(x_1 \otimes \cdots x_m) \cdot (y_1 \otimes \cdots y_n) \;=\; x_1 \otimes \cdots x_m \otimes y_1 \otimes \cdots y_n$$

definiert ist. Man prüft, dass dieses Produkt wohldefiniert ist, d.h. falls Elemente auf der linken Seite sich nur um eine Element in (4.1) unterscheidet, so gilt dies auch für das Ergebnis der Multiplikation.

Eine *R-Algebra T* ist ein Ring T zusammen mit einem Ringhomomorphismus $\varphi : R \to T$. Man prüft direkt nach, dass die Multiplikation auf $T_R(M)$ und die Inklusion $\varphi : R \to T_R(M)$ in die erste Komponente der direkten Summe die Eigenschaften einer Algebra hat, die *Tensoralgebra* zu M.

Die Tensoralgebra hat zwei Quotientenalgebren, die an vielen Stellen verwendet werden. Dies ist zum einen die *symmetrische Algebra* $\mathrm{Sym}_R(M)$ (oder kurz $\mathrm{Sym}(M)$), definiert als der Quotient von $T_R(M)$ nach dem von den Elementen $x \otimes y - y \otimes x$ für alle $x, y \in M$ erzeugten Ideal. Der andere wichtige Quotient ist die *äußere Algebra* $\Lambda_R M$, definiert als der Quotient von $T_R(M)$ nach dem von den Elementen $x \otimes x$ für alle $x, y \in M$ erzeugten Ideal. Wie in der linearen Algebra im Zusammenhang mit Determinanten bemerkt man, dass in der äusseren Algebra $(x+y)\otimes(x+y) = 0$ ist und damit $x\otimes y + y\otimes x = 0$ ist.

Wenn M graduiert ist, d.h. $M = \oplus_{i\in\mathbb{N}_0} M_i$, so erbt die Tensoralgebra eine Graduierung, denn es ist

$$T_R(M) = \oplus_{i\in\mathbb{N}_0} T_R(M)_i \quad \text{mit} \quad T_R(M)_i = \oplus_{j_1+\cdots j_r=i} M_{j_1}\otimes\cdots M_{j_r}$$

Sowohl bei der Definition der symmetrischen Algebra als auch bei der Definition der äußeren Algebra war das Ideal, bezüglich dem wir einen Quotienten gebildet haben, von homogenen Elementen erzeugt, egal welche Graduierung M hat. Deswegen erben $\mathrm{Sym}(M)$ und $\Lambda_R M$ die Graduierung von $T_R(M)$. Die homogenenen Anteile im Grad d bezeichnet man mit $(\mathrm{Sym}(M))_d$ bzw. $(\Lambda_R M)_d$. Am häufigsten wird der Fall $M = M_1$ verwendet und in diesem Fall schreibt man $\mathrm{Sym}^d(M)$ für $(\mathrm{Sym}(M))_d$ und $\Lambda^d M$ für $(\Lambda_R M)_d$.

Ist M frei von endlichem Rang r mit der trivialen Graduierung $M = M_i$, so ist $T_R(M)_d$ frei vom Rang r^d, es ist $\mathrm{Sym}^d(M)$ frei vom Rang $\binom{r+d-1}{r-1}$ und $\Lambda^d M$ frei vom Rang $\binom{r}{d}$, was konsistent mit der ad-hoc-Definition aus Abschnitt 3.4 ist.

4.3 Basiswechsel

Sei $f : R \to S$ ein Ringhomomorphismus. Dann gibt es zwei Konstruktionen, die bei einem Modul den zugrundeliegenden Ring ändern. Zum einen können wir bei einem vorgegebenen S-Modul N diesen nur noch, vermöge f als R-Modul auffassen. Wir bezeichnen diesen R-Modul als f_*N, die *Restriktion der Skalare* von S nach R.

Andererseits können wir zu einem gegebenen R-Modul M einen S-Modul basteln, nämlich $f^*M = M \otimes_R S$, die *Erweiterung der Skalare* von R nach S. Die S-Modulstruktur entsteht dabei durch die Multiplikation auf dem zweiten Faktor des Tensorprodukts, genauer gesagt wird $s \in S$ vermöge der Abbildung $\mathrm{id}\otimes[\cdot s]$. Man prüft mit Hilfe der Definition der Abbildung auf Tensorprodukten (und der dabei verwendeten UAE des Tensorprodukts), dass diese Definition allen Axiomen eines Moduls genügt.

Häufig verwendet man die Erweiterung der Skalare für den Fall, dass $\mathfrak{m}$ in R ein maximales Ideal ist, und $f : R \to R/\mathfrak{m} = k$ die Quotientabbildung auf den Restklassenkörper. Ebenso wichtig ist der Fall, dass R ein nullteilerfreier Ring und K der Quotientenkörper (siehe Abschnitt 7) und $f : R \to K$ (also beispielsweise $f : \mathbb{Z} \to \mathbb{Q}$) ist.

Ist $\varphi : M_1 \to M_2$ ein R-Modulhomomorphismus, so erhalten wir einen natürlichen S-Modulhomomorphismus $\varphi \otimes \mathrm{id} : f^*M_1 \to f^*M_2$. Die Beziehung zwischen Erweitern und Restriktion bezüglich Morphismen fasst folgendes Lemma zusammen.

Lemma 4.6 *Seien f, M und N wie oben. Dann gibt es einen natürlichen Isomorphismus von R-Moduln $f_* \operatorname{Hom}_S(f^*M, N) \cong \operatorname{Hom}_R(M, f_*N)$ gegeben durch $\varphi \mapsto (x \mapsto \varphi(x \otimes 1)$.*

Beweis: Um die Wohldefiniertheit der Abbildung einzusehen, kann man diese als $\varphi \mapsto \varphi \circ (\mathrm{id} \otimes f)$ schreiben. Die Umkehrabbildung ordnet $\psi \in \operatorname{Hom}_R(M, f_*N)$ die Abbildung $M \otimes_R S \to N$ gegeben auf Elementartensoren durch $m \otimes s \mapsto s\psi(m)$ zu. (Diese ist Vorschrift ist als Quotient der bilinearen Abbildung $(m, s) \mapsto s\psi(m)$ nach der UAE des Tensorprodukts wohldefiniert.) Offenbar sind die beiden Abbildungen zueinander invers. □

5 Grundbegriffe der Kategorientheorie

Kategorien umfassen Objekte und Morphismen dazwischen, in der puren Definition mit sehr wenig Bedingungen. Kategorientheorie ist im Wesentlichen eine sehr komfortable Sprechweise Dinge zu Formulieren, die in verschiedenen Kontexten (Mengen, Vektorräumen, Gruppen, Moduln, geordnete Mengen) auftreten. All diese Kontexte fallen unter den Begriff Kategorie, wie wir gleich sehen werden. Besonders nützlich wird es eine solche Sprechweise zu haben, wenn wir Objekte in einer Kategorie in Objekte einer anderen Kategorie transformieren wollen. Das Konzept eines Funktors formalisiert dies.

5.1 Kategorien

Eine *Kategorie* $\mathcal{A}$ besteht aus einer Familie[1] von Objekten $\operatorname{Ob}(\mathcal{A})$ und für $A, B \in \operatorname{Ob}(\mathcal{A})$ aus einer Familie von Morphismen $\operatorname{Mor}(A, B)$ und einer Zuordnung ('Verkettung')

$$\begin{aligned} \operatorname{Mor}(A, B) \times \operatorname{Mor}(B, C) \to & \quad \operatorname{Mor}(A, C) \\ f \times g \mapsto & \quad g \circ f \end{aligned} \tag{5.1}$$

sowie für jedes $A \in \operatorname{Ob}(\mathcal{A})$ aus einem ausgezeichneten Morphismus $\mathrm{id}_A \in \operatorname{Mor}(A, A)$, sodass die Assoziativität

$$h \circ (g \circ f) \;=\; (h \circ g) \circ f$$

für alle $f \in \operatorname{Mor}(A, B)$, $g \in \operatorname{Mor}(B, C)$ und $h \in \operatorname{Mor}(C, D)$, sowie und die Neutralität des Identitätsmorphismus

$$f \circ \mathrm{id}_A \;=\; f \;=\; \mathrm{id}_B \circ f$$

für alle $f \in \operatorname{Mor}(A, B)$ gelten.

Beispiele für Kategorien sind:

[1] Was ist eine Familie? Was ist der Unterschied zu einer Menge? Über die grundlegenden Konzepte der Mengentheorie geht dieses Skript hinweg, ebenso über die Stellen, an denen eine Kategorie als (lokal) klein vorausgesetzt werden sollte. Details hierzu z.B. in [Lei14]

- Die Kategorie der Mengen $\mathbf{Set}$, deren Morphismen Abbildungen (zwischen Mengen) sind.
- Die Kategorie der Gruppen $\mathbf{Grp}$, deren Morphismen Gruppenhomomorphismen sind.
- Die Kategorie der abelschen Gruppen $\mathbf{Ab}$, deren Morphismen ebenfalls Gruppenhomomorphismen sind.
- Die Kategorie der Gruppen $\mathbf{Rng}$, deren Morphismen Ringhomomorphismen sind.
- Zu jedem Ring R gibt es die Kategorie der R-Moduln $\mathbf{R}-\mathbf{Mod}$, deren Morphismen R-Modulhomomorphismen sind.
- Die Kategorie der topologischen Räume $\mathbf{Top}$, deren Morphismen stetige Abbildungen zwischen den topologischen Räumen sind.

Aufgrund der Existenz von id_A hat man in Kategorien naheliegenderweise die Begriffe von Rechtsinverser, Linksinverser und von einem Isomorphismus.

Auch kompliziertere Definition von Kategorien, deren Objekte nicht notwendigerweise 'Mengen mit Zusatzstruktur' sind, werden häufig gebraucht. Beispielweise sind Bilden die Tripel (R, S, π) mit $R, S \in \mathrm{Ob}(\mathbf{Rng})$ und $\pi \in \mathrm{Mor}_{\mathbf{Rng}}(R, S)$ die Objekte einer Kategorie, der Morphismen Paare von Ringhomomorphismen sind, die mit dem gegebenen Morphismus kommutieren, also $(f, g) \in \mathrm{Mor}((R, S, \pi), (R_2, S_2, \pi_2))$, falls $f \in \mathrm{Mor}_{\mathbf{Rng}}(R, R_2)$, $g \in \mathrm{Mor}_{\mathbf{Rng}}(S, S_2)$ und falls $\pi_2 \circ f = g \circ \pi$.

Das Interessante an eine Kategorie müssen nicht unbedingt die Objekte sein. Zum Beispiel definiert jede Gruppe G eine Kategorie (die wir auch mit G bezeichnen), die nur ein Objekt hat und einen Morphismus für jedes Gruppenelement. Das Axiom des neutralen Elements zeigt, dass die in der Tat eine Kategorie ist. (Auch ein Monoid definiert daher eine Kategorie). Das Axiom des inversen Elements ist äquivalent dazu, zu verlangen, dass jeder Morphismus in der Kategorie G ein Isomorphismus ist.

Zu jeder Kategorie $\mathcal{A}$ gibt es die duale Kategorie $\mathcal{A}^\vee$, mit $\mathrm{Ob}(\mathcal{A}) = \mathrm{Ob}(cA^\vee)$, aber deren Morphismen in die andere Richtung weisen, d.h. zu jedem $f \in \mathrm{Mor}_{\mathcal{A}}(A, B)$ gibt es einen eindeutigen Morphismus $f^\vee \in \mathrm{Mor}_{\mathcal{A}}(B, A)$.

5.2 Funktoren

Die Definition eines Funktors codiert die minimalen Kompatibilitätsbedingungen, die eine Transformation von Objekten einer Kategorie in eine andere Kategorie in allen relevanten Fällen genügt.

Seien $\mathcal{A}$ und $\mathcal{B}$ Kategorien. Ein *Funktor* $F : \mathcal{A} \to \mathcal{B}$ besteht aus einer Abbildung $\mathrm{Ob}(\mathcal{A}) \to \mathrm{Ob}(\mathcal{B})$, die wir zumeist $A \to F(A)$ notieren, und einer

Abbildung auf Morphismen $\mathrm{Mor}_{\mathcal{A}}(A, A') \to \mathrm{Mor}_{\mathcal{B}}(F(A), F(A'))$, die wir mit $f \mapsto F(f)$ notieren, sodass

$$F(\mathrm{id}_A) \;=\; \mathrm{id}_{F(A)}$$

und, wenn immer definiert,

$$F(g \circ f) \;=\; F(g) \circ F(f)$$

gelten.

Beispiel 5.1 i) Die einfachsten Funktoren sind die *Vergissfunktoren*, die einen Teil der Struktur einer Kategorie vergessen. Zum Beispiel gibt es den Vergissfunktor $V : \mathbf{Grp} \to \mathbf{Set}$, der die Gruppenstruktur vergisst, den Vergissfunktor $V : \mathbf{Rng} \to \mathbf{Grp}$, oder auch den Vergissfunktor $V : \mathbb{Z} - \mathbf{Mod} \to \mathbf{Ab}$, die wir alle mit dem selben Symbol bezeichnen, da die Definitions- und Bildbereiche Uneindeutigkeiten auflösen.

Auch die Inklusion $\mathbf{Ab} \to \mathbf{Grp}$ definiert einen Funktor. Wir hatten bereits im Abschnitt 3 jeder abelschen Gruppe einen $\mathbb{Z}$-Modul zugeordnet. Jeder Homomorphismus abelscher Gruppen ist auch ein Homomorphismus von $\mathbb{Z}$-Moduln. Damit haben wir einen Funktor $\mathbf{Ab} \to \mathbb{Z} - \mathbf{Mod}$ definiert, der invers zum Vergissfunktor ist.

ii) Historisch taucht der Funktorbegriff zuerst in der algebraischen Topologie auf. Sei $\mathbf{Top}_\bullet$ die Kategorie der punktierten topologischen Räume, deren Objekte Paare (X, x) aus einem topologischen Raum X und einem Punkt $x \in X$ sind. Morphismen sind stetige Abbildungen, die die ausgezeichneten Punkte aufeinander abbilden. Hierauf gibt es den Funktor

$$\pi_1 : \mathbf{Top}_\bullet \to \mathbf{Grp}, \quad (X, x) \mapsto \pi_1(X, x)\,,$$

der jedem punktieren topologischen Raum seine Fundamentalgruppe zuordnet.

iii) Zwei der in diesem Skript prominentesten Funktoren arbeiten auf Kategorien von Moduln. Sei dazu R ein Ring und T ein R-Modul. Dann wird $\mathrm{Hom}_R(\cdot, T) : M \to \mathrm{Hom}_R(M, T)$ zu einem Funktor $\mathbf{R{-}Mod}^\vee \to \mathbf{R{-}Mod}$, indem man $f \in \mathrm{Mor}_{\mathbf{R\text{–}Mod}^\vee}(M_1, M_2)$ die Abbildung

$$\mathrm{Hom}(f) : g \mapsto g \circ f \in \mathrm{Mor}_{\mathbf{R\text{–}Mod}}(\mathrm{Hom}_R(M_1, T)\,, \mathrm{Hom}_R(M_2, T)) \tag{5.2}$$

zuordnet. Dieser wird auch der *Hom-Funktor* genannt. Ein solcher Funktor, der 'die Pfeilrichtung umdreht', also vom dual einer Kategorie in eine andere Kategorie, abbildet, wird *kontravariant* genannt.

Ist wiederum T ein R-Modul, dann ist

$$\otimes_R T : M \mapsto M \otimes_R T, \quad f \mapsto f \otimes_R T \tag{5.3}$$

ein Funktor $\otimes_R T : \mathbf{R}{-}\mathbf{Mod} \to \mathbf{R}{-}\mathbf{Mod}$, wie wir in Abschnitt 4.1 nachgerechnet haben. Dieser dreht die Pfeilrichtung von Morphismen nicht um. Solche Funktoren werden *kovariant* genannt.

iv) Ein Funktor von der Kategorie G zu einer Gruppe in die Kategorie $\mathbf{Set}$ ist nichts anderes als eine Menge mit einer G-Operation (Übung).

v) Jedem topologischen Raum die Menge seiner offenen Teilmengen zuzuordnen ist ein kontravarianter Funktor $\mathcal{O} : \mathbf{Top}^\vee \to \mathbf{Set}$.

5.3 Natürliche Transformationen

Funktoren transformieren Objekte einer Kategorie in eine andere. Diese Abstraktion kann man noch eine Stufe weiterführen und die Transformationen von einem Funktor in einen anderen betrachten.

Seien $\mathcal{A}$ und $\mathcal{B}$ zwei Kategorien und F und G Funktoren von $\mathcal{A}$ nach $\mathcal{B}$. Eine *natürliche Transformation* $\alpha : F \to G$ ist eine Kollektion von Morphismen $\alpha_A : F(A) \to G(A)$ in $\mathcal{B}$, sodass für jede Abbildung $f : A \to A' \in \mathrm{Mor}_{\mathcal{A}}(A, A')$ die Verkettungen $\alpha_{A'} \circ F(f) = G(f) \circ \alpha_A$ übereinstimmen.

Die natürlichen Transformationen von Funktoren zwischen den Kategorien $\mathcal{A}$ und $\mathcal{B}$ bilden wiederum eine Kategorie $[\mathcal{A}, \mathcal{B}]$. Ein *natürlicher Isomorphismus* ist eine natürliche Transformation, welche ein Isomorphismus in der Kategorie $[\mathcal{A}, \mathcal{B}]$ ist.

Ist beispielsweise G eine Gruppe und $F, G : G \to \mathbf{Set}$ Funktoren, so ist eine natürliche Transformation $\alpha : F \to G$ nichts anderes als eine G-äquivariante Abbildung der F bzw. G zugrundeliegenden Mengen mit G-Operation (Übung).

Sei $\mathbf{Vekt}_k$ die Kategorie der k-Vektorräume und $\mathbf{Vekt}_k^{end}$ die Unterkategorie der endlichdimensionalen k-Vektorräume. Dann ist Dualisieren ein Funktor $(\cdot)^\vee : \mathbf{Vekt}_k \to \mathbf{Vekt}_k^\vee$, die zweifache Verkettung also ein Funktor $(\cdot)^{\vee\vee} : \mathbf{Vekt}_k \to \mathbf{Vekt}_k$, ebenso wie die Identität $\mathrm{id} : \mathbf{Vekt}_k \to \mathbf{Vekt}_k$. Für endlichdimensionale Vektorräume sind V und $V^{\vee\vee}$ kanonisch zueinander isomorph und dieser Isomorphismus definiert einen natürlichen Isomorphismus $\mathrm{id} \cong (\cdot)^{\vee\vee}$ von Funktoren von der Kategorie $\mathbf{Vekt}_k^{end}$ in sich selbst.

5.4 Darstellbarkeit

Zu einem gegebenen Objekt A in einer Kategorie $\mathcal{A}$ bilden die Morphismen ausgehend von A einen $\mathbf{Set}$-wertigen Funktor und die Morphismen mit Ziel gleich A einen $\mathbf{Set}$-wertigen Funktor. Darstellbarkeit untersucht die Frage, welche $\mathbf{Set}$-wertige Funktoren von dieser Bauart sind.

Genauer gesagt, sei $\mathrm{Mor}_{\mathcal{A}}(A, \cdot) : \mathcal{A} \to \mathbf{Set}$ der Funktor, der ein Objekt $A' \in \mathcal{A}$ auf die Menge $\mathrm{Mor}_{\mathcal{A}}(A, A')$ abbildet und $f \in \mathrm{Mor}_{\mathcal{A}}(B, C)$ auf die Abbildung

$$\mathrm{Mor}(A, f) : \quad \mathrm{Mor}_{\mathcal{A}}(A, B) \to \mathrm{Mor}_{\mathcal{A}}(A, C), \quad g \mapsto f \circ g\,.$$

Dual dazu sei $\mathrm{Mor}_{\mathcal{A}}(\cdot, A) : \mathcal{A}^{\vee} \to \mathbf{Set}$ der Funktor, der ein Objekt $A' \in \mathcal{A}$ auf die Menge $\mathrm{Mor}_{\mathcal{A}}(A', A)$ abbildet und $f \in \mathrm{Mor}_{\mathcal{A}}(C, B) = \mathrm{Mor}_{\mathcal{A}^{\vee}}(B, C)$ auf die Abbildung

$$\mathrm{Mor}(f, A) : \mathrm{Mor}_{\mathcal{A}}(B, A) \to \mathrm{Mor}_{\mathcal{A}}(C, A), \quad g \mapsto g \circ f\,.$$

Ein Funktor $F : \mathcal{A} \to \mathbf{Set}$ ist *darstellbar*, falls es ein Objekt $X \in \mathcal{A}$ gibt, sodass $F \cong \mathrm{Mor}(X, \cdot)$ ist. Ein Funktor $F : \mathcal{A}^{\vee} \to \mathbf{Set}$ ist *darstellbar*, falls es ein Objekt $X \in \mathcal{A}$ gibt, sodass $F \cong \mathrm{Mor}(\cdot, X)$ ist. In beiden Fällen wird X das *darstellende Objekt* genannt.

Beispiel 5.2 i) Sei I eine einelementige Menge. Dann ist $\mathrm{Mor}(I, M) \cong M$ für jede Menge M. Also ist der Funktor $\mathrm{id}_{\mathbf{Set}}$ darstellbar

ii) Seien $U, V \in \mathrm{Ob}(\mathbf{Vekt}_k)$ fixiert und $\mathrm{Bilin}(U, V, \cdot)$ der Funktor $\mathbf{Vekt}_k \to \mathbf{Set}$, der jedem $W \in \mathrm{Ob}(\mathbf{Vekt}_k)$ die Menge der Bilinearformen $U \times V \to W$ zuordnet. Dann besagt Satz 4.1 (bzw. die Definition des Tensorprodukts) gerade, dass das Tensorprodukt $U \otimes V \in \mathrm{Ob}(\mathbf{Vekt}_k)$ den Funktor $\mathrm{Bilin}(U, V, \cdot)$ darstellt.

iii) Der Funktor $\mathcal{P} : \mathbf{Set}^{\vee} \to \mathbf{Set}$, der jeder Menge ihre Potenzmenge zuordnet und der $f : A \to B$ die Abbildung $\mathcal{P}(f) : \mathcal{P}(B) \to \mathcal{P}(A)$ gegeben durch $\mathcal{P}(B) \ni U \mapsto f^{-1}(U) \in \mathcal{P}(A)$ zuordnet, wird durch eine zweielementige Menge $X = \{1, 2\}$ dargestellt, denn Abbildungen $f : M \to X$ stehen in natürlicher Bijektion zu Teilmengen von M.

iv) Der Funktor $\mathcal{O} : \mathbf{Top}^{\vee} \to \mathbf{Set}$ wird durch den zweipunktigen topologischen Raum, bei dem genau eine einpunktige Menge offen ist, dargestellt (Sierpinski-Raum).

6 Homologische Algebra

Ein *Komplex* $M^{\bullet}$ (hier ausschliesslich von R-Moduln) ist eine durch $i \in \mathbb{Z}$ indizierte Kollektion M^i mit Abbildungen $d_i : M^i \to M^{i+1}$, die man auch Differentiale nennt, und die der Bedingung $d_{i+1} \circ d_i = 0$ für alle i genügen. Diese Bedingung ist zu $\mathrm{Bild}(d_i) \subseteq \mathrm{Ker}(d_{i+1})$ äquivalent. Homologische Algebra 'misst' wie weit ein Komplex davon entfernt ist *exakt* zu sein. Exaktheit bedeutet, dass $\mathrm{Bild}(d_i) = \mathrm{Ker}(d_{i+1})$ für alle i ist. Homologische Algebra 'misst' des weiteren, wie weit ein exakter Komplex sich von Exaktheit entfernt hat, nachdem ein Funktor auf den Komplex angewendet wurde.

6.1 Komplexe und exakte Sequenzen

Wir führen etwas Terminolgie zu Komplexen ein. Falls $M^i = 0$ für $b \geq b_0$ für ein $b_0 \in \mathbb{Z}$, so wird der Komplex $M^{\bullet}$ als *nach oben beschränkt* bezeichnet und falls $M^i = 0$ für $b \leq b_0$, so ist er *nach unten beschränkt*. In diesem Fall lässt man die Nullmoduln im Komplex in der Regel weg. Wichtige Spezialfälle hiervon ist eine *kurze exakte Sequenz*

$$0 \to M^{-1} \to M^0 \to M^1 \to 0.$$

Dies ist äquivalent dazu, dass d_{-1} injektiv, dass d_1 surjektiv ist und dass $\mathrm{Bild}(d_{-1}) = \mathrm{Ker}(d_0)$ ist. Exaktheit von $0 \to M^0 \to M^1 \to 0$ bedeutet gerade, dass d^0 ein Isomorphismus ist.

Komplexe von R-Moduln bilden eine Kategorie, die wir mit $\mathbf{Kom}(\mathbf{R}-\mathbf{Mod})$ oder kurz mit $\mathbf{Kom}$ bezeichnen. Ein Morphismus $f \in \mathrm{Mor}_{\mathbf{Kom}}(M^\bullet, N^\bullet)$ ist eine Kollektion von Abbildungen $f_i : M^i \to N^i$, die mit den Differentialen (die wir in der Regeln in allen Komplexen mit d_i bezeichnen) kommutieren, d.h. sodass $d_i \circ f_i = f_{i+1} \circ d_i$ ist. Ein solcher Morphismus von Komplexen ist also ein kommutierendes 'Leiterdiagramm'.

Im Umgang mit exakten Sequenzen tauchen folgende zwei Lemmata immer wieder auf.

Lemma 6.1 *Gegeben sei folgendes kommutierendes Diagramm*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f_1"] \arrow[d, "\alpha"] & M \arrow[r, "g_1"] \arrow[d, "\beta"] & M'' \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "f_2"] & N \arrow[r, "g_2"] & M'' \arrow[r] & 0\,, \end{tikzcd} \tag{6.1}$$

dessen Zeilen kurze exakte Sequenzen sind. Sind α und γ Isomorphismen, so ist auch β ein Isomorphismus.

Die Beweistechnik ist unter dem Namen Diagrammjagd bekannt. Es gibt in jedem Beweisschritt quasi nur eine Möglichkeit eine Voraussetzung zu verwenden und damit im Argument weiterzukommen.

Beweis: Wir zeigen, dass β injektiv ist. Dazu sei x mit $\beta(x) = 0$ vorgegeben. Also ist $g_2(\beta(x)) = \gamma(g_1(x)) = 0$. Da γ ein Isomorphismus ist, muss $g_1(x) = 0$ sein. Damit ist $x = f_1(y) \in \mathrm{Bild}(f_1)$ aufgrund der Exaktheit der ersten Zeile. Dann ist $f_2(\alpha(y)) = \beta(f_1(y)) = 0$ und aufgrund der Injektivität von α und f_2 folgt $y = 0$ und somit $x = 0$.

Wir zeigen, dass β surjektiv ist. Sei dazu $z \in N$ vorgegeben. Dann ist $\gamma^{-1}(g_2(z)) = g_1(x)$ aufgrund der Exaktheit der ersten Zeile. Nun behauptet niemand, dass bereits $\beta(x) = z$ ist, aber $g_2(\beta(x) - z) = 0$ nach Definition. Also ist $z - \beta(x) = f_2(u)$ für ein $u \in N'$. Sei $x' = x + f_1(\alpha^{-1}(u))$. Dann ist $\beta(x') = \beta(x) + f_2(u) = z$, wie gewünscht. □

Lemma 6.2 *Gegeben sei folgendes kommutierendes Diagramm*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f_1"] \arrow[d, "\alpha"] & M \arrow[r, "g_1"] \arrow[d, "\beta"] & M'' \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "f_2"] & N \arrow[r, "g_2"] & M'' \arrow[r] & 0\,, \end{tikzcd} \tag{6.2}$$

dessen Zeilen kurze exakte Sequenzen sind. Dann gibt es einen R-Modulhomomorphismus $\delta : \mathrm{Ker}(\gamma) \to \mathrm{Coker}(\alpha)$*, genannt Verbindungshomomorphismus, sodass der Komplex*

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ker}(\alpha) \arrow[r] & \mathrm{Ker}(\beta) \arrow[r] & \mathrm{Ker}(\gamma) \arrow[dll, rounded corners] & \\ & \mathrm{Coker}(\alpha) \arrow[r] & \mathrm{Coker}(\beta) \arrow[r] & \mathrm{Coker}(\gamma) \arrow[r] & 0\,, \end{tikzcd} \tag{6.3}$$

induziert von den Abbildungen f_i *und* g_i *exakt ist.*

Beweis: Der erste Schritt ist die Konstruktion von δ, die man unter dem Slogan 'Beliebiges g_1-Urbild nehmen und mit β abbilden, dann ist das Ergebnis im Bild von f_2. Nimm das (eindeutige) Urbild!' zusammenfassen kann. Sei also $y = g_1(x) \in \mathrm{Ker}(\gamma)$ gegeben. Dann ist $g_2(\beta(x)) = \gamma(y) = 0$ wegen der Kommutativität des Diagramms, also $\beta(x)$ im $\mathrm{Bild}(f_2)$ wegen der Exaktheit der unteren Zeile, wie behauptet. Wir müssen die Unabhängigkeit von der Wahl des Urbildes x zeigen. Sei also x' ein weiteres g_1-Urbild von y. Dann ist $x - x' = f_1(z)$ wegen der Exaktheit der oberen Zeile. Also unterscheiden sich die β-Bilder von x und x' um $\alpha(z)$. Das Bild von δ ist also (nicht als Element von N', wohl aber) als Element von $\mathrm{Coker}(\alpha)$ wohldefiniert.

Wir zeigen die Exaktheit bei $\mathrm{Ker}(\gamma)$. Sei $y \in \mathrm{Ker}(\delta)$. Nach der Konstruktion von δ und mit den Notationen von dort ist also das f_2-Urbild von $\beta(x)$ gleich $\alpha(z)$ für ein z. Also ist $x - f_1(\alpha)$ ein weiteres Urbild von y mit der Eigenschaft, dass $\beta(x - f_1(\alpha)) = 0$. Also ist $x - f_1(\alpha)$ das gesuchte Element im Kern von β. Sie nun umgekehrt $y = g_1(x) \in \mathrm{Ker}(\gamma)$ mit $x \in \mathrm{Ker}(\beta)$ gegeben. Dann ist x ein Urbild, das wir in der Definition von δ verwenden können und für dieses ist $\beta(x) = 0$ und somit $\delta(x) = 0$.

Die Exaktheit an den anderen Stellen zeigt man mit ähnlichen Argumenten (Übung). □

Bemerkung 6.3 Ohne die Injektivität von f_1 und die Surjektivität von g_2 erhält man immer noch die exakte Sequenz (6.3), allerdings ohne die Nullen am Anfang und am Ende.

6.2 Kohomologie von Komplexen

Ist $M^\bullet$ ein Komplex so ist die *i-te Kohomologiemodul* der R-Modul $\mathrm{Ker}(d_i)/\,\mathrm{Bild}(d_{i-1})$. Ein Komplex ist also genau dann exakt, wenn alle seine Kohomologiegruppen verschwinden. In diesem Abschnitt stellen wir Methoden zusammen Kohomologiegruppen zu 'berechnen', indem wir die Kohomologie verschiedener Komplexe miteinander vergleichen.

Kohomologie nehmen, d.h. das Anwenden von $H^i(\cdot)$ ist ein Funktor $\mathbf{Kom}(\mathbf{R}-\mathbf{Mod}) \to \mathbf{R}-\mathbf{Mod}$. Auf Objekten ist die gerade obige Definition, auf Morphismen müssen wir dies nun erläutern. Sei also $f \in \mathrm{Mor}_{\mathbf{Kom}}(M^\bullet, N^\bullet)$ gegeben, also eine Abbildungen $f_i : M^i \to N^i$ die mit den Differentialen kompatibel sind. Wir definieren $H^i(f)$ indem wir $x \in H^i(M^\bullet)$ auf $f_i(x)$ abbilden. Da $d_i(f_i(x)) = f_{i+1}(d_i(x)) = f_{i+1}(0) = 0$ ist, landet die Abbildung in der Tat in $H^1(N^\bullet)$. Unterscheiden sich x und x' um ein Element $d_{i-1}(y)$, so unterscheiden sich die Bilder um $f_i(d_{i-1}(y)) = d_{i-1}(f_{i-1}(y)) \in \mathrm{Bild}(d_{i-1})$. Dies zeigt die Wohldefiniertheit. Das Identitätsaxiom und das Verkettungsaxiom in der Definition eines Funktors sind mit dieser Definition offenbar erfüllt.

Den Begriff der kurzen exakten Sequenz kann von $\mathbf{R}-\mathbf{Mod}$ auf $\mathbf{Kom}(\mathbf{R}-\mathbf{Mod})$ ausdehnen, indem man definiert, dass

$$0 \to M_1^\bullet \to M^\bullet \to M_2^\bullet \to 0$$

exakt ist, falls für jedes $i \in \mathbb{Z}$ die Sequenz

$$0 \to M_1^i \to M^i \to M_2^i \to 0$$

exakt ist. Damit können wir nun die wichtigste Komohomogieberechnungsmethode formulieren.

Satz 6.4 *Gegeben sei eine kurze exakte Sequenz*

$$0 \longrightarrow M_1^\bullet \xrightarrow{f} M^\bullet \xrightarrow{g} M_2^\bullet \longrightarrow 0$$

von R-Moduln. Dann gibt es Homomorphismen $\delta_i : H^i(M_2^\bullet) \to H^{i+1}(M_1^\bullet)$, sodass durch

$$\begin{array}{c} H^{i-1}(M_1^\bullet) \xrightarrow{H^{i-1}(f)} H^{i-1}(M^\bullet) \xrightarrow{H^{i-1}(f)} H^{i-1}(M_2^\bullet) \longrightarrow \\ \hookrightarrow H^i(M_1^\bullet) \xrightarrow{H^i(f)} H^i(M^\bullet) \xrightarrow{H^i(f)} H^i(M_2^\bullet) \longrightarrow \\ \hookrightarrow H^{i+1}(M_1^\bullet) \xrightarrow{H^{i+1}(f)} H^{i+1}(M^\bullet) \xrightarrow{H^{i+1}(f)} H^{i+1}(M_2^\bullet) \end{array} \tag{6.4}$$

ein exakter Komplex von R-Moduln gegeben ist.

Die δ_i werden naheliegenderweise auch Verbindungshomomorphismen genannt. Die Situation erinnert nicht nur graphisch an das Schlangenlemma, der Beweis folgt auch ziemlich direkt aus diesem.
Beweis: Wir betrachten das Teilstück

$$\begin{tikzcd} & M_1^i/\operatorname{Bild}(d_{i-1}) \arrow[r, "f^i"] \arrow[d, "d_i"] & M^i/\operatorname{Bild}(d_{i-1}) \arrow[r, "g^i"] \arrow[d, "d_i"] & M_2^i/\operatorname{Bild}(d_{i-1}) \arrow[r] \arrow[d, "d_i"] & 0 \\ 0 \arrow[r] & \operatorname{Ker}(d_i) \arrow[r, "f^{i+1}"] & \operatorname{Ker}(d_i) \arrow[r, "g^{i+1}"] & \operatorname{Ker}(d_i)\,, & \end{tikzcd} \tag{6.5}$$

das auf die kurze Version des Schlangenlemmas (siehe Bemerkung 6.3) passt. Jetzt beobachtet man, dass

$$H^i(M^\bullet) \;=\; \operatorname{Ker}(d_i : M^i/\operatorname{Bild}(d_{i-1}) \to M^{i+1})$$

aufgrund der Definition von Komplexen und des Homomorphiesatzes ist. Weiterhin ist

$$H^{i+1}(M^\bullet) \;=\; \operatorname{Coker}(d_i : M^i/\operatorname{Bild}(d_{i-1}) \to M^{i+1})$$

und beides analog für $M_1^\bullet$ und $M_2^\bullet$. Also ergibt das Schlangenlemma das Teilstück von $H^i(M_1^\bullet)$ bis $H^{i+1}(M_2^\bullet)$ in (6.4). Zusammensetzen der Teilstücke (die Abbildung in den Teilstücken ist ja die Gleiche, egal ob wir das überlappende Teilstück auf der 'Kern'- oder 'Cokern'-Seite des Schlangenlemmas wiederfinden) liefert die Behauptung. □

6.3 Homotopien von Komplexen

Seien $f, g : M^\bullet \to N^\bullet$ zwei Abbildungen von Komplexen. Eine *Homotopie* ist eine Kollektion von Abbildungen $h_n : M^n \to N^{n-1}$, sodass

$$f_n - g_n \;=\; d_{n-1} \circ h_n + h_{n+1} \circ d_n \tag{6.6}$$

gilt.

Satz 6.5 *Homotope Abbildungen induzieren die gleichen Abbildungen auf der Kohomologie, d.h. $H^n(f) = H^n(g)$ für alle $n \in \mathbb{Z}$.*

Beweis: Übung! □

6.4 Homologie von Komplexen

In manchen Situation sind die Differentiale eines Komplexes absteigend im Index. Dies macht man notationell durch einen unteren Index kenntlich. Ein Komplex $M_\bullet$ besteht also aus R-Moduln M_i und Abbildungen $d_i : M_i \to M_{i-1}$

mit $d_i \circ d_{i-1} = 0$. Analog zu oben definiert man die n-the *Homologie* $H_n(M_\bullet)$ von $M_\bullet$ als $H_n(M_\bullet) = \mathrm{Ker}(d_n)/\,\mathrm{Bild}(d_{n-1})$. Analog zu Satz 6.4 gibt eine kurze exakte Sequenz von Komplexen wieder eine lange exakte Sequenz der Homologiegruppen, mit dem Unterschied, dass der Verbindungshomomorphismus nun abwärts im Index (statt bisher von i nach $i+1$ geht).

Der Begriff der Homotopie überträgt sich auch, nur dass die Indexverschiebung nun $+1$ statt -1 ist, also eine Homotopie ist eine Abbildung $h_n : M_n \to N_{n+1}$ mit $f_n - g_n = d_{n+1} \circ h_n + h_{n-1} \circ d_n$. Mit diesem Begriff gilt Satz 6.5 auch für die Homologien von Komplexen.

6.5 Rechts- und Linksexakte Funktoren

Für Konstruktionen der homologischen Algebra sind folgende zwei Arten von Funktoren besonders relevant. Ein kovarianter Funktor $F : \mathbf{R}-\mathbf{Mod} \to \mathbf{R}-\mathbf{Mod}$, der eine kurze exakte Sequenz $0 \to M_1 \to M \to M_2 \to 0$ in eine 'ganz kurze' exakte Sequenz $F(M_1) \to F(M) \to F(M_2) \to 0$ überführt, wird *rechtsexakt* genannt. Ein kovarianter Funktor $F : \mathbf{R}-\mathbf{Mod} \to \mathbf{R}-\mathbf{Mod}$, der eine kurze exakte Sequenz $0 \to M_1 \to M \to M_2 \to 0$ in eine 'ganz kurze' exakte Sequenz $0 \to F(M_1) \to F(M) \to F(M_2)$ überführt, wird *linksexakt* genannt. Gleichermassen definiert man die Begriffe für kontravariante Funktoren. Ein Funktor, der rechts- und linksexakt ist, wird *exakt* genannt.

Wir wiederholen in diesem Kontext nochmal Satz 4.4

Satz 6.6 *Für jeden R-Modul N ist $\cdot \otimes_R N$ ein rechtsexakter Funktor.*

Für Hom-Funktoren gilt eine ähnliche Aussage.

Satz 6.7 *Die Funktoren* $\mathrm{Hom}_R(\cdot, N)$ *und* $\mathrm{Hom}_R(N, \cdot)$ *sind für jeden R-Modul N linksexakt.*

Beweis: Die Exaktheit von $0 \to M_1 \to M \to M_2$ ist äquivalent dazu, dass M_1 der Kern $f : M_1 \to M$ der Abbildung $g : M \to M_2$ ist. Nach der universellen Eigenschaft des Kerns gibt es also für jede Abbildung $f' : N \to M$ mit $g \circ f = 0$ ein Abbildung $\varphi : N \to M_1$ mit $f \circ \varphi = f'$. Die ist die Inklusion $\mathrm{Ker} \subseteq \mathrm{Bild}$ der Sequenz,

$$0 \to \mathrm{Hom}_R(N, M_1) \to \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M_2)$$

deren Exaktheit wir zeigen sollen. Die Injektivität der ersten Abbildung folgt unmittelbar aus der Injektivität von f und die umgekehrte Inklusion $\mathrm{Bild} \subseteq \mathrm{Ker}$ folgt aus der Exaktheit in der Mitte der Ausgangssequenz.

Die Exaktheit von $M_1 \to M \to M_2 \to 0$ ist äquivalent dazu, dass M_2 der Cokern $g : M \to M_2$ der Abbildung $f : M_1 \to M$. Die gesuchte Exaktheit von

$$0 \to \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M_1, N)$$

folgt dual zum ersten Beweis aus der universellen Eigenschaft des Cokerns. □

7 Lokalisierung

Lokalisierung bzgl. S bedeutet Bruchrechnen, wobei S als Nennermenge zugelassen werden kann. Der Begriff stammt aus der Anschauung der (komplexen oder algebraischen) Geometrie: Lokalisierung bei den Potenzen eines Elements f bedeutet die Teilmenge $\{f = 0\}$ auszublenden und 'lokal, auf dem Komplement von $\{f = 0\}$' die Rechnungen weiterzuführen. Wir geben eine knappe Zusammenfassung der Konstruktion, hauptsächlich um den Begriff Quotientenkörper zur Verfügung zu haben.

Sei R ein Ring. Eine *multiplikativ abgeschlossene Teilmenge* $S \subseteq R$ ist eine Menge mit $1 \in S$ und $S \cdot S \subseteq S$. Beispiele hierfür sind $S = \{1\}$, $S = \{f^n, n \in \mathbb{N}_0\}$ für ein $f \in R$ sowie $S = R \backslash \mathfrak{p}$ für $\mathfrak{p}$ ein Primideal in R. In einem nullteilerfreien Ring ist das Nullideal ein Primideal und in diesem Fall ist $S = R \setminus \{S\}$ ein wichtiges Beispiel einer multiplikativ abgeschlossene Teilmenge.

Zu einer solchen multiplikativ abgeschlossene Teilmenge definieren wir den Ring der Brüche mit Nenner in S als die Faktormenge $S^{-1}R = (R \times S)/\sim$ nach der Äquivalenzrelation $(r_1, s_1) \sim (r_2, s_2)$, falls es ein $a \in S$ gibt mit $a(r_1 s_2 - r_2 s_1) = 0$. Reflexivität und Symmetrie sind offensichtlich und die Transitivität sieht man wie folgt ein: Seien $a, b \in S$ mit $a(r_1 s_2 - r_2 s_1) = 0$ und $b(r_2 s_3 - r_3 s_2) = 0$ gegeben. Dann ist

$$abs_2(r_1 s_3 - r_3 s_1) \;=\; bs_3(ar_2 s_1) - s_1 a(br_2 s_3) \;=\; 0\,.$$

Die Elemente von $S^{-1}R$ schreiben wir daher wie Brüche ab sofort $\frac{r}{s}$. Aus $S^{-1}R$ wird mit komponentenweiser Multiplikation und der von Brüchen üblichen Addition ein Ring mit Einselement $\frac{1}{1}$.

Dieser Ring ist auch Lösung einer universellen Abbildungseigenschaft.

Satz 7.1 *Der Ring $S^{-1}R$ ist eine R-Algebra $\varphi : R \to S^{-1}R$, sodass die Bilder von S Einheiten in $S^{-1}R$ sind und universell mit dieser Eigenschaft: Ist A eine weitere R-Algebra mit Strukturmorphismus $\psi : R \to A$ sodass $\psi(S) \subset A^\times$, dann gibt es genau einen Ringhomorphismus $\widehat{\psi} : S^{-1}R \to A$, sodass $\widehat{\psi} \circ \phi = \psi$.*

Beweis: Mit $r \mapsto \frac{r}{1}$ definieren wird ϕ. Dann ist $\frac{1}{s}$ das Inverse von $\phi(s)$ für $s \in S$.

Da $\widehat{\psi}$ die Abbildung ψ fortsetzen muss und ein Ringhomomorphismus ist, ist $\widehat{\psi}(\frac{r}{s}) = \psi(r)\psi(s)^{-1}$ die einzig mögliche Abbildung, wenn dies wohldefiniert und ein Ringhomomorphismus ist.

Ist $(r_1, s_1) \sim (r_2, s_2)$, also gibt es $a \in S$ mit $a(r_1 s_2 - r_2 s_1) = 0$, dann ist

$$\begin{aligned} \widehat{\psi}(\tfrac{r_1}{s_1}) - \widehat{\psi}(\tfrac{r_1}{s_2}) \;&=\; \psi(r_1)\psi(s_1)^{-1} - \psi(r_2)\psi(s_2)^{-1} \\ &=\; \psi(as_2 r_1)\psi(as_1 s_2)^{-1} - \psi(as_1 r_2)\psi(as_1 s_2)^{-1} \;=\; 0\,. \end{aligned}$$

Die Multiplikativität von $\widehat{\psi}$ ist offensichtlich. Für die Verträglichkeit mit der Addition rechnet man nach, dass für zwei beliebige Punkte in $S^{-1}R$

$$\begin{aligned}\widehat{\psi}(\tfrac{r_1}{s_1}+\tfrac{r_1}{s_2}) &= \psi(r_1s_2+r_2s_1)\psi(s_1s_2)^{-1}\\ &= \psi(r_1s_2)\psi(s_1s_2)^{-1}+\psi(r_2s_1)\psi(s_1s_2)^{-1}\\ &= \psi(r_1)\psi(s_1)^{-1}+\psi(r_2)\psi(s_2)^{-1}=\widehat{\psi}(\tfrac{r_1}{s_1})+\widehat{\psi}(\tfrac{r_1}{s_2})\end{aligned}$$

gilt. □

Wir heben zwei wichtige Spezialfälle hervor. Ist R nullteilerfrei, so ist $S = R\setminus\{0\}$ multiplikativ abgeschlossen und in $S^{-1}R$ jedes von Null verschiedene Element invertierbar. Also ist $S^{-1}R$ in diesem Fall ein Körper, der *Quotientenkörper* $\mathrm{Quot}(R)$.

Der Fall $0 \in S$ ist per Definition nicht ausgeschlossen. Nach Definition der Äquivalenzrelation ist aber in diesem Fall $S^{-1}R = 0$ der Nullring.

Die Konstruktion der Lokalisierung funktioniert nicht nur für Ringe sondern auch für Moduln. Sei M ein R-Modul und $S \subset R$ multiplikativ abgeschlossen. Dann definieren wir $S^{-1}M = (M \times S)/\sim$ und die Äquivalenzrelation analog wie oben durch $(m_1, s_1) \sim (m_2, s_2)$, falls es ein $a \in S$ gibt mit $a(m_1s_2 - m_2s_1) = 0$.

Auch der Modul $S^{-1}M$ erfüllt eine universelle Abbildungseigenschaft analog zu Satz 7.1, indem man 'Algebren' durch 'Moduln' ersetzt und die Eigenschaft 'invertierbar' durch 'die Operation von s durch Multiplikation ist bijektiv'.

Satz 7.2 *Die Moduln $S^{-1}M$ und $M \otimes_R S^{-1}R$ sind zueinander isomorph.*

Beweis: Die Abbildungen $\frac{m}{s} \mapsto m \otimes \frac{1}{s}$ und umgekehrt $m \otimes \frac{a}{s} \mapsto \frac{am}{s}$ sind wohldefiniert und zueinander invers. □

8 Projektive, injektive und flache Moduln

Im letzten Abschnitt haben wir festgestellt, dass der Hom-Funktor und der Tensorfunktor im Allgemeinen (nicht exakt, sonder nur) rechts- bzw. linksexakt sind. Dennoch sind für manche R-Moduln diese Funktoren exakt. Hier wollen wir solche R-Moduln charakterisieren.

8.1 Projektive Moduln

Ein R-Modul P wird *projektiver Modul* genannt, wenn der Funktor $\mathrm{Hom}_R(P, \cdot)$ ein exakter Funktor ist. Konkreter gesagt ist ein R-Modul P projektiv genau dann für jede Surjektion $g : M \to M_2$ und jeden Morphismus $q : P \to M_2$ es einen Morphismus ('Liftung') $\widehat{q} : P \to M$ mit $g \circ \widehat{q} = q$ gibt ('Liftungskriterium'). Wir fassen die wesentlichen Eigenschaften projektiver Moduln zusammen.

Satz 8.1 *Ist F ein freier R-Modul, so ist F projektiv.*

Ist $P = \oplus_{i \in I} P_i$ eine direkte Summe von R-Moduln, so ist P projektiv genau dann wenn alle P_i projektiv sind.

Zu jedem projektiven R-Modul P gibt es einen freien R-Modul F mit einer Surjektion $F \to P$.

Ist P projektiv, so ist P direkter Summand eines freien Moduls.

Beweis: Sei $g : M \to M_2$ eine Surjektion, $F = R^X$ der freie Modul mit Basis X und $q : P \to M_2$ ein R-Modulhomomorphismus. Indem man zu jedem $x \in X$ ein Urbild y_x von $q(x)$ wählt, definiert $x \mapsto y_x$ einen R-Modulhomomorphismus $\widehat{q} : F \to M$ und dieser hat offenbar die geforderte Eigenschaft $q = g \circ \widehat{q}$, wie man mit Hilfe der Basisdarstellung nachrechnet.

Für $P = \oplus_{i \in I} P_i$ ist $\mathrm{Hom}_R(P, N) = \oplus_{i \in I} \mathrm{Hom}_R(P_i, N)$ nach der universellen Eigenschaft der Summe. Also ist die Abbildung $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M_2)$ surjektiv, genau dann wenn all die Abbildungen $\mathrm{Hom}_R(P_i, M) \to \mathrm{Hom}_R(P_i, M_2)$ für $i \in I$ surjektiv sind.

Für die dritte Aussage nehmen wir den freien R-Modul $F = R^P$ mit der ('riesigen') Basis P selbst und die Abbildung $F \to P$ gegeben aus Basiselementen durch $[p] \mapsto p$. Dies ist offenbar eine Surjektion.

Eine Inklusion der vierten Aussage folgt unmittelbar aus den ersten zwei Aussagen. Für die umgekehrte Inklusion sei P projektiv und $p : F \to P$ eine Surjektion wie in der dritten Aussage. Wir wenden die definierende Eigenschaft von projektiv auf $\mathrm{id}_P : P \to P$ an und erhalten eine Abbildung ('Spaltung') $s : P \to F$ mit $p \circ s = \mathrm{id}_P$. Es ist noch zu zeigen, dass $F = \mathrm{Bild}(s) \oplus \mathrm{Ker}(p)$ ist. Dazu wenden wir Lemma 6.1 auf $0 \to \mathrm{Ker}(p) \to P \oplus \mathrm{Ker}(p) \to P \to 0$ in der ersten Zeile und $0 \to \mathrm{Ker}(p) \to F \to P \to 0$ und $\beta = (\mathrm{id}_{\mathrm{Ker}(p)}, s)$ an. $\square$

Ein banales Beispiel für einen projektiven, aber nicht freien R-Modul ist durch einen Produktring $R = R_1 \oplus R_2$ und $P = R_1$ gegeben, wobei R_i beides Ring mit Eins sind. Dann ist $P \subset R$ direkter Summand eines freien Moduls, aber selbst nicht frei (da Multiplikation mit $(1,0) \in R$ und $(1,1) \in R$ den gleichen Effekt auf P hat, im Widerspruch zur eindeutigen Basisdarstellung.)

Ein interessanteres Beispiel für einen projektiven, aber nicht freien R-Modul in einem nullteilerfreien Ring R ist durch einen Zahlring gegeben, der kein Hauptidealring ist. Dies leistet zum Beispiel $R = \mathbb{Z}[\sqrt{-5}]$. Dort ist das Ideal $P = \langle 2, 1 + \sqrt{-5} \rangle$ kein Hauptideal. Das liegt an der nicht-eindeutigen Faktorisierung

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}), \tag{8.1}$$

welche aber zunächst nur zeigt, dass R kein Hauptidealring ist. Um zu zeigen, dass P kein Hauptideal ist, nimmt man an, dass $P = \langle x+y\sqrt{-5}\rangle$ ist und erhält sofort einen Widerspruch, nachdem man die Darstellungen der Erzeuger von P mit dem Galois-Konjugierten multipliziert, d.h. aus $2 = (a+b\sqrt{-5})(x+y\sqrt{-5})$ und $1+\sqrt{-5} = (a+b\sqrt{-5})(x+y\sqrt{-5})$ folgt

$$x^2+5y^2 \,|\, 4 \quad \text{und} \quad x^2+5y^2 \,|\, 6$$

also teilt es auch den ggT und daraus folgt $x = \pm 1$ und $y = 0$, der gesuchte Widerspruch.

Damit haben wir gesehen, dass P nicht frei vom Rang Eins ist. Andererseits kann P auch nicht frei vom Rang zwei sein, denn ausgehend von der Basisdarstellung der Erzeuger erhalten wir durch Multiplikation mit 3 bzw. mit $(1-\sqrt{-5})$ sofort mit (8.1) einen Widerspruch zur Eindeutigkeit der Basisdarstellung.

Es bleibt zu zeigen, dass P projektiv ist. Dazu zeigen wir, dass die Projektion $p : R^2 \to P$, $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto 2x + (1+\sqrt{-5})y$ eine Spaltung $s : P \to R^2$ besitzt und realisieren damit P als direkten Summanden eines freien Moduls. Sei dazu $\widetilde{s} : R^2 \to R^2$ die Multiplikation mit

$$A = \begin{pmatrix} -2 & -1-\sqrt{-5} \\ 1-\sqrt{-5} & 3 \end{pmatrix} \tag{8.2}$$

Dann rechnet man direkt nach, dass der Kern von p im Kern von $\widetilde{s}$ enthalten ist und somit die Abbildung zu $s : P = R^2/\operatorname{Ker}(p) \to R^2$ absteigt. Die Spaltungseigenschaft $p \circ s = \mathrm{id}_P$ rechnet man auch direkt nach.

8.2 Injektive Moduln

Die Definition des vorigen Unterkapitels lässt sich dualisieren. Ein R-Modul I wird *injektiver Modul* genannt, wenn der Funktor $\operatorname{Hom}_R(\cdot, I)$ ein exakter Funktor ist. Konkreter gesagt ist ein R-Modul I injektiv genau dann für jede Injektion $f : M_1 \to M$ und jeden Morphismus $p : M_1 \to I$ es eine Fortsetzung $\widehat{p} : M \to I$ mit $\widehat{p} \circ f = p$ gibt.

Analog zu oben zeigt man, dass falls ein Projekt von Moduln injektiv ist, so auch jeder Summand und wenn in einer Summe von Moduln jeder Summand injektiv ist, so ist auch die Summe injektiv.

Allerdings sind Beispiele für injektive Moduln nicht so offensichtlich (ausser dem Nullmodul), denn freie Moduln sind i.A. nicht injektiv, wie man $R = \mathbb{Z}$, $p = \mathrm{id} : M_1 = \mathbb{Z} \to I = \mathbb{Z}$ und $f : \mathbb{Z} \to \mathbb{Q}$ der natürlichen Inklusion sieht. Das Konzept injektiver Moduln geht auf R. Baer (1956-1967 in Frankfurt) zurück. Wir verwenden sein Kriterium.

Satz 8.2 *Für den Nachweis der Injektivität eines Moduls genügt es die Definition jede Injektion $f : \mathfrak{a} \to R$ von einem Ideal $\mathfrak{a}$ (statt für beliebige Injektionen $f : M_1 \to M$) zu testen.*

Beweis: Der Modul I habe die Fortsetzungseigenschaft für Idealinklusionen und es sei $f : M_1 \to M$ eine beliebige Injektion und $g : M_1 \to I$ vorgegeben. Der Beweis wendet Zorns Lemma auf alle Paare (M', g') mit $M_1 \subseteq M' \subseteq M$ und Fortsetzungen g' von g an. Diese Menge ist durch Inklusion der Moduln von Fortsetzungseigenschaft der Abbildungen geordnet. Jede Kette hat eine obere Schranke, die Vereinigung der Kettenglieder. Sei also (M_0, g_0) ein maximales Element Wenn $M_0 = M$ ist sind wir fertig. Andernfalls gibt es ein $b \in M \setminus M_0$. Sei $\mathfrak{a} = \{r \in R : rb \in M_0\}$. und definiere $h : \mathfrak{a} \to I$ durch $h(r) = g_0(rb)$.

Nach Voraussetzung gibt es also eine Abbildung $\widehat{h} : R \to I$, die h fortsetzt. Wir definieren $M_0^+ = \langle M_0, b\rangle$ und $g^+ : M_0^+ \to I$ durch

$$g^+(m_0 + rb) \;=\; g_0(m_0) + \widehat{h}(1)\,.$$

Sobald wir geprüft haben, dass das wohldefiniert ist, haben wir den gewünschten Widerspruch zur Maximalität von M_0, da g^+ offenbar auch g fortsetzt.

Zum Nachweis der Wohldefiniertheit sei $m_0+rb = n_0+sb$. Dann ist $(r-s)b = m_0 - n_0 \in M_0$ und damit $r - s \in \mathfrak{a}$. Dann ist also

$$g_0(m_0 - n_0) = g_0((r-s)b) = h(r-s) = \widehat{h}(r-s) = (r-s)\widehat{h}(1)$$

was wir zur gewünschten Unabhängigkeit von der Darstellung umsortieren können. □

Der wesentliche Schritt zum Existenzbeweis vieler injektiver Moduln ist folgendes Lemma. Sei R ein nullteilerfreier Ring. Ein R-Modul M ist *divisibel*, falls jedes $m \in M$ durch jedes $r \in R \setminus \{0\}$ teilbar ist, d.h. es ein $m' \in M$ gibt mit $m = rm'$. (Die Definition kann man auf nicht-nullteilerfreie Ringe fortsetzen, indem man Annihilatoren betrachtet.) Beispiele für divisible Moduln sind der Quotientenkörper $\mathrm{Quot}(R)$ oder allgemeiner $\mathrm{Quot}(R)$-Vektorräume.

Lemma 8.3 *Ist R nullteilerfrei und I injektiv, so ist I divisibel.*

Beweis: Um die Teilbarkeit durch $r \in R \setminus \{0\}$ nachzuweisen, wenden wir die Definition von Injektiv (Fortsetzungskriterium) auf die Inklusion $R \cdot r \to R$ an. Das Bild von Eins ist das gesuchte $1/r$-fache. □

Satz 8.4 *Jeder endlichdimensionale $\mathrm{Quot}(R)$-Vektorraum V ist ein injektiver R-Modul.*

Der Satz gilt auch ohne die Voraussetzung endlichdimensional. Wir geben nur den Beweis für $\mathrm{Quot}(R)$ selbst, der die schwächere Version impliziert.

Beweis: Wir können $V = \mathrm{Quot}(R)$ annehmen. Nach Satz 8.2 genügt es $p : \mathfrak{a} \to V$ über die Injektion $f : \to R$ auszudehnen. Wir beobachten, dass für alle

$a \in \mathfrak{a}\backslash\{0\}$ der Quotient $f(a)/a$ den gleichen Wert c hat, denn $a'f(a) = f(aa') = af(a')$. (Hierbei verwenden wir wirklich, dass $\mathfrak{a}$ ein Ideal und nicht nur ein R-Modul ist.) Wir definieren $\widehat{p}$, indem wir $1 \mapsto c$ abbilden. Dies setzt offenbar p fort. □

Ist R ein Hauptidealring so können wir Lemma 8.3 verschärfen.

Satz 8.5 *Ist R ein Hauptidealring, so ist I injektiv genau dann wenn I divisibel ist. Insbesondere sind Quotienten injektiver Moduln wieder injektiv.*

Beweis: Sei I divisibel, $i : \mathfrak{a} \to R$ eine Injektion eines Ideals $\mathfrak{a} = R \cdot a$ und $p : \mathfrak{a} \to I$ gegeben. Wir können $a \neq 0$ annehmen. Aufgrund der Divisibilität von I gibt es ein $c \in I$ mit $ac = p(a)$. Dann ist $\widehat{p} : 1 \mapsto c$ die gesuchte Fortsetzung. □

Korollar 8.6 *Jeder Modul lässt sich in einen injektiven Modul einbetten.*

Beweis: Wir zeigen die Aussage zunächst für $R = \mathbb{Z}$. Wir schreiben den $\mathbb{Z}$-Modul M als Quotient $M = F/K$ eines freien Moduls $F = \mathbb{Z}^X$ über der Menge X. Dann ist $M \subset \mathbb{Q}^X/K$ und damit nach dem vorigen Satz in einen injektiven Modul eingebettet.

Der zweite Schritt ist die Behauptung, dass zu einer injektiven abelschen Gruppe I der Modul $M = \mathrm{Hom}_{\mathbb{Z}}(R, I)$ ein injektiver R-Modul ist. Um dies zu zeigen, zeigen wir, dass $\mathrm{Hom}_R(\cdot, M)$ exakt ist oder äquivalent, dass $\mathrm{Hom}_R(R \otimes_R \cdot, I)$ exakt ist. Dieser Funktor ist aber die Verkettung von Tensorieren mit R, also der Identität, und dem Funktor $\mathrm{Hom}_{\mathbb{Z}}(\cdot, I)$, welcher aufgrund der Injektivität von I exakt ist.

Einen Modul für einen allgemeinen Ring R betrachten wir zunächst als $\mathbb{Z}$-Modul, also als abelsche Gruppe und verwenden die Abbildung

$$\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, M)\,, \quad m \mapsto \varphi_m = (r \mapsto rm)\,.$$

Diese ist offenbar $\mathbb{Z}$-linear und injektiv, da φ_m durch das Bild von 1, also durch m festgelegt. Wir verwenden nun den ersten Teil und betten M, immer noch als $\mathbb{Z}$-Modul, via $i : M \to I$ in einen injektiven $\mathbb{Z}$-Modul ein. Die Verkettung von φ it $i_* : \mathrm{Hom}_{\mathbb{Z}}(R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R, I)$ ist also eine Einbettung in einen injektiven R-Modul. Jetzt muss man noch die Definition der R-Modulstrukturen ansehen um festzustellen, dass diese Abbildung in der Tat ein R-Modulhomomorphismus ist. □

8.3 Flache Moduln

Ein R-Modul N ist flach, falls der Funktor $\cdot \otimes_R N$ exakt ist. Flache Moduln spielen in der komplexen und algebraischen Geometrie eine wichtige Rolle, da

Tensorieren den Basiswechsel von einer Deformation einer komplexen Mannigfaltigkeit über einer 'großen Basis' zu einer einzelnen Mannigfaltigkeit (eine 'Deformation über einem einzelnen Punkt) beschreibt. Dies übersteigt den Rahmen dieser Vorlesung, weswegen wir knapp die wichtigsten Eigenschaften zusammenfassen.

Satz 8.7 *Eine direkte Summe $N = \oplus N_i$ ist flach genau dann wenn alle Summanden dies sind.*

Ein projektiver R-Modul ist flach.

Beweis: Für die erste Aussage notieren wir, dass Tensorieren mit direkten Summen vertauscht (Beispiel 4.2) und dass eine direkte Summe von Abbildungen genau dann injektiv ist, wenn alle Summandenabbildungen dies sind.

Offenbar ist R ein flacher R-Modul und damit ist jeder freie R-Modul flach. Nach der ersten Aussage und Satz 8.1 ist damit auch jeder projektive Modul flach. $\square$

9 Abgeleitete Funktoren

9.1 Konstruktion via projektiver und injektiver Auflösungen

Eine *projektive Auflösung* des R-Moduls M ist ein ('homologischer') exakter Komplex

$$\cdots \to P_3 \to P_2 \to P_1 \to P_0 \to N \to 0 \to 0 \to \cdots \tag{9.1}$$

bei dem die Moduln P_i allesamt projektiv sind. Wir schreiben dafür auch kurz $P_\bullet \to M$, wobei $P_\bullet$ nun ein durch $\mathbb{N}$ indizierter exakter Komplex ist. Den Morphismus $P_0 \to M$ benennen wir üblicherweise mit ε. Lässt man die Voraussetzung der Exaktheit fallen, so nennen wir $P_\bullet \to M$ einen projektiven Komplex mit Ziel M. Den Komplex $P_\bullet$ nennen wir auch den abgeschnittenen ('truncated') Komplex. Ganz analog definiert man auch die Begriffe freie Auflösung und flache Auflösung, indem man die entsprechenden Eigenschaften für die P_i fordert. Aus Satz 8.1 folgt direkt:

Lemma 9.1 *Jeder R-Modul hat eine freie (und damit eine flache und eine projektive) Auflösung.*

Für einen vernünftigen Funktor F (die korrekten Adjektive sind: kovariant, additiv, bewahrt Multiplikation....) definieren wir den *linksabgeleiteten Funktor* $L_nF(M) = H_n(F(P_\bullet))$, wobei $P_\bullet \to M$ eine projektive Auflösung von M ist. Das für uns wichtigste Beispiel ist die Linksableitung des Tensorfunktors

$$\mathrm{Tor}_n^R(\cdot, N) = L_n(\cdot \otimes_R N) \tag{9.2}$$

zu einem festen R-Modul N. Um die Funktoreigenschaften der Linksableitung zu rechtfertigen, müssen wir noch die Wirkung auf einem Morphismus $f : M \to M'$ rechtfertigen und ausserdem ist noch die Unabhängigkeit von der verwendeten projektiven Auflösung zu zeigen. Wir starten die Rechtfertigung mit folgendem Vergleichssatz.

Satz 9.2 *Gegeben eine Abbildung und $f : M \to M'$, ein projektiver Komplex $P_\bullet \to N$ und eine projektive Auflösung $P'_\bullet \to M'$. Dann gibt es eine Homomorphismus $f_\bullet : (P_\bullet \to M) \to (P'_\bullet \to M')$ von komplexen von R-Moduln und je zwei solcher Homomorphismen sind homotop.*

Beweis: Wir konstruieren die Abbildungen f_i induktiv, startend mit $i = 0$. Dazu wenden wir die Eigenschaft, dass P_0 projektiv ist, auf die Surjektion ε' und die Abbildung $f \circ \varepsilon : P_0 \to M'$ an, um eine Abbildung $f_0 : P_0 \to P'_0$ zu konstruieren. Im Induktionsschritt sei $f_n : P_n \to P'_n$ bereits konstruiert. Wir betrachten die Abbildung $g = f_n \circ d_{n+1}$ und wollen zeigen, dass $\mathrm{Bild}(g) \subseteq \mathrm{Bild}(d'_{n+1})$. Wegen der Exaktheit von $(P'_\bullet \to M')$ ist $\mathrm{Bild}(d'_{n+1}) = \mathrm{Ker}(d'_n)$, also ist $d'_n \circ g = 0$ zu zeigen. Dies folgt aus $d'_n \circ g = d'_n \circ f_n \circ d_{n+1} = f_{n-1} \circ d_n \circ d_{n+1} = 0$. Nun können wir die Eigenschaft projektiv auf $g : P_{n+1} \to \mathrm{Bild}(d'_{n+1})$ und die Surjektion von d'_{n+1} auf sein Bild anwenden.

Wenn $g_\bullet$ eine weitere Abbildung ist, die sich mit f (und die Nullabbildungen in negativen Graden) zu einem Homomorphismus von Komplexen $(P_\bullet \to M) \to (P'_\bullet \to M')$ ergänzt, so wollen wir Abbildungen $h_n : P_n \to P'_{n+1}$ mit $f_n - g_n = d'_{n+1} \circ h_n + h_{n-1} \circ d_n$ konstruieren, wobei es notationell günstig ist $P_{-1} = M$ und $P'_{-1} = M'$ zu setzen. Die Abbildung h_{-1} leistet dann den Induktionsanfang, da $f_{-1} = g_{-1} = f$ per Definition. Für den Induktionsschritt überlegt man sich, dass $\mathrm{Bild}(f_{n+1} - g_{n+1} - h_n \circ d_{n+1}) \subset \mathrm{Bild}(d'_{n+2})$ wegen der Exaktheit der unteren Zeile und verwendet wieder die Projektivität von P'_{n+1}.
□

Der Satz liefert unmittelbar die Funktorialität der Linksableitungen, indem man die gegebene Abbildung zu einer Abbildung der projektiven Auflösungen ergänzt, dies als Abbildung zwischen den Abgeschnittenen Komplexen betrachtet, den Funktor anwendet und die induzierte Abbildungen auf den Homologien der Komplexe verwendet. Eine andere Wahl der Abbildung zwischen den Komplexen ist homotop. Nach Anwendung des Funktors auf das ganze 'Leiterdiagramm' sind die Abbildungen immer noch homotop und damit hängt die induzierte Abbildungen auf den Homologien nach (der Homologie-Version von) Satz 6.5 nicht von den Wahlen ab.

Der Satz liefert auch die Unabhängigkeit von der Wahl der projektiven Auflösung, indem man ihn auf $f = id_N$ und zwei Auflösungen $P_\bullet$ und $P'_\bullet$ anwendet. Nach anwenden des Funktors erhält man zunächst Abbildungen zwischen den Homologiegruppen definiert via der beiden Auflösungen, und zwar in beide Richtungen. Um zu zeigen, dass diese Abbildungen zueinander invers sind, wendet man den Satz noch einmal $f = id_N$ und die gleichen (!) Auflösungen an. Da sowohl die Identität als auch die Verkettung der beiden gerade definierten Abbildungen Morphismen dieses Komplexes sind, sind sie nach dem Satz homotop. Nach Anwenden des Funktors sind die induzierten Abbildungen auf den Homologiegruppen also gleich. Dies zeigt, dass die Abbildungen in der Tat zueinander invers sind.

Wir notieren eine direkte Konsequenz der Definition.

Korollar 9.3 *Ist $P_\bullet \to M$ eine projektive Auflösung von N und $K_n = \mathrm{Ker}(d_n)$ sowie $K_0 = \mathrm{Ker}(\varepsilon)$, so ist*

$$L_{n+1}F(N) \;=\; L_nF(K_0) \;=\; \cdots \;=\; L_1F(K_{n-1})\,.$$

Wir wollen auch die Linksableitungen in kurzen exakten Sequenzen vergleichen können. Bevor wir (die Homologie-Version von) Theorem 6.4 anwenden können, müssen wir projektive Auflösungen in einer exakten Sequenz ergänzen. Das leistet das folgende Hufeisenlemma.

Lemma 9.4 *Ist $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln, und seien projektive Auflösungen $P'_\bullet \to M'$ und $P''_\bullet \to M''$ gegeben. Dann gibt es eine projektive Auflösung $P_\bullet \to M$ und Morphismen, sodass das Diagramm*

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & P_2 \arrow[r] \arrow[d] & P_2 \arrow[r] \arrow[d] & P_2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_1 \arrow[r] \arrow[d] & P_1 \arrow[r] \arrow[d] & P_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_0 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

kommutiert und die Zeilen exakt sind.

Bisher habe wir nirgends verwendet, dass unser Standardbeispiel ein rechtsexakter Funktor ist. Dies tritt erst beim folgenden Lemma, das direkt aus der Definition folgt.

Lemma 9.5 *Ist F rechtsexakt, so ist $L_0F(M) = F(M)$.*

Zusammengenommen haben wir nun ein Hauptresultat zur Berechnung der Tor-Funktoren.

Korollar 9.6 *Ist* $0 \to M' \to M \to M'' \to 0$ *eine kurze exakte Sequenz von R-Moduln, so induzieren die Morphismen zusammen mit dem Verbindungshomomorphismus eine lange exakte Sequenz*

$$\begin{aligned} \cdots &\to \mathrm{Tor}_2(M', N) \to \mathrm{Tor}_2(M, N) \to \mathrm{Tor}_2(M'', N) \\ &\to \mathrm{Tor}_1(M', N) \to \mathrm{Tor}_1(M, N) \to \mathrm{Tor}_1(M'', N) \\ &\to M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0 \end{aligned} \tag{9.3}$$

Wir betrachten nun den dualen Standpunkt für linksexakte kovariante Funktoren. Eine *injektive Auflösung* des R-Moduls M ist ein ('kohomologischer') exakter Komplex

$$0 \to M \to I^0 \to I^1 \to I^2 \to I^3 \to N \cdots \tag{9.4}$$

bei dem die Moduln I_j allesamt injektiv sind. Wir schreiben dafür auch kurz $M \to I^\bullet$. Durch sukzessive Anwendung von Korollar 8.6 erhalten wir:

Lemma 9.7 *Jeder R-Modul hat eine injektive Auflösung.*

Sei nun ein F ein 'vernünftiger' linksexakter Funktor. Der rechtsabgeleiteten Funktoren sind nun dual zu oben definiert als $R^nF(M) = H^n(F(I^\bullet))$ wobei $M \to I^\bullet$ eine injektive Auflösung von M ist. Das wichtigste Beispiel ist die Rechtsableitung des Hom-Funktors

$$\mathrm{Ext}^n(N, \cdot) \;=\; R^n \,\mathrm{Hom}(N, \cdot) \tag{9.5}$$

Die Wohldefiniertheit von Rechtsableitungen, also die Unabhängigkeit von der Wahl einer injektiven Auflösung, und die Funktorialität zeigt man mit der dualen Version von Satz 9.2. Die duale Version des Hufeisenlemmas gilt auch (mit dem gleichen Beweis). Als Folge erhält man folgende Aussage für rechtsabgeleitete Funktoren, die wir für den Spezialfall Ext angeben. Wiederum wird die Linksexaktheit erst für die Identifikation $\mathrm{Ext}^0(N, M') = \mathrm{Hom}(N, M')$ benötigt.

Korollar 9.8 *Ist* $0 \to M' \to M \to M'' \to 0$ *eine kurze exakte Sequenz von R-Moduln, so induzieren die Morphismen zusammen mit dem Verbindungshomomorphismus eine lange exakte Sequenz*

$$\begin{aligned} 0 &\to \mathrm{Hom}(N, M') \to \mathrm{Hom}(N, M) \to \mathrm{Hom}(N, M'') \\ &\to \mathrm{Ext}^1(N, M') \to \mathrm{Ext}^1(N, M) \to \mathrm{Ext}^1(N, M'') \\ &\to \mathrm{Ext}^2(N, M') \to \mathrm{Ext}^2(N, M) \to \mathrm{Ext}^2(N, M'') \to \cdots \end{aligned} \tag{9.6}$$

In den beiden oben diskutierten Fällen waren die Funktoren kovariant. Um den linksexakten kontravarianten Funktor $\mathrm{Hom}(\cdot, N)$ abzuleiten, benötigt man wieder zu gegebenem Modul M eine projektive Auflösung $P_\bullet \to M$. Wir bezeichnen die Rechtsableitungen zur Unterscheidung mit kleinem e, also

$$\mathrm{ext}^n(\cdot, N) \;=\; R^n \operatorname{Hom}(\cdot, N) \tag{9.7}$$

und die Verwendung von projektive Auflösungen in dieser Situation, also für F einen linksexakten und kontravarianten Funktoren, wird wiederum durch $R^0F(M) = F(M)$ gerechtfertigt.

Satz 9.9 *Es gibt einen Isomorphismus* $\mathrm{ext}^n(M, N) \cong \mathrm{Ext}^n(M, N)$.

Aufgrund des Satzes schreiben wir in der Folge oft einfach Ext und verwenden die Definition via Rechts- oder Linksableitung, die gerade günstig ist. Der Beweis steht z.B. in [Rot09].

9.2 Einige Eigenschaften von Tor

Der nächste Satz erläutert den Grund für die Bezeichnung des Tor-Funktors. Zu einem gegebenen nullteilerfreien Ring R definieren wir den Quotientenmodul $K = \mathrm{Quot}(R)/R$, also $K = \mathbb{Q}/\mathbb{Z}$ im Fall $R = \mathbb{Z}$.

Satz 9.10 *Sei R nullteilerfrei ist M ein Torsionsmodul, so ist* $\mathrm{Tor}_1(K, M) = M$. *Allgemein, also für jeden R-Modul M, ist* $\mathrm{Tor}_n(K, M) = 0$ *für $n \geq 2$. Ist andererseits M torsionsfrei, so ist* $\mathrm{Tor}_1(K, M) = 0$.

Mit anderen Worten, der Funktor $\mathrm{Tor}_1(K, \cdot)$ ist isomorph zum Torsionsfunktor, der jedem Modul seinen Torsionsuntermodul zuordnet.
Beweis: Aus der Definition von K entsteht die exakte Sequenz

$$\mathrm{Tor}_1(\mathrm{Quot}(R), M) \to \mathrm{Tor}_1(K, M) \to R \otimes_R M \to \mathrm{Quot}(R) \otimes_R M\,.$$

Der letzte Term hiervon ist Null nach Voraussetzung und $R \otimes_R M \cong M$. Es genügt also einzusehen, dass $\mathrm{Quot}(R)$ ein flacher R-Modul ist, da für einen solchen alle höheren Tor-Moduln verschwinden. Dazu interpretiert man $\mathrm{Quot}(R)$ als direkten Limes (siehe z.B. [Rot09]) der freien R-Moduln $\frac{1}{r}R$, welche alle flach sind und zeigt, dass Flachheit unter direkten Limes erhalten bleibt.

Für $n \geq 2$ ist $\mathrm{Tor}_n(K, M)$ zwischen $\mathrm{Tor}_n(\mathrm{Quot}(R), M)$ und $\mathrm{Tor}_{n-1}(R, M)$ eingeklemmt, welche beide aufgrund der Flachheit verschwinden.

Wir verwenden eine exakte Sequenz $0 \to M \to V \to T$, wobei V ein $\mathrm{Quot}(R)$-Vektorraum ist und T ein Torsionsmodul. Aus der Sequenz folgt die Behauptung, da V als Summe von Moduln isomorph zu $\mathrm{Quot}(R)$ flach ist und damit $\mathrm{Tor}_1(K, V) = 0$ ist und andererseits $\mathrm{Tor}_2(K, M)$ nach der vorigen Behauptung verschwindet.

Um diese Sequenz zu konstruieren nimmt man für V die injektive Einhüllende (siehe z.B. [Rot09], im Falle eines Hauptidealrings ist $V = M \otimes_R \mathrm{Quot}(R)$). Diese ist zugleich (das ist ein nicht offensichtlicher Satz) sogenannte maximale essentielle Erweiterung, d.h. zu jedem $v \in V$ gibt es ein $r \in R$ mit $rv \in M$ aber $rv \neq 0$. Da nach Voraussetzung M torsionsfrei ist, muss V auch torsionsfrei sind. Da V zudem injektiv, also divisibel ist, ist V ein $\mathrm{Quot}(R)$-Vektorraum. Die Existenz von r mit $tv \in M \setminus \{0\}$ zeigt auch, dass $T = V/M$ wie gewünscht ein Torsionsmodul ist. □

9.3 Einige Eigenschaften von Ext

Gegeben seien zwei R-Moduln M_1 und M_2. Dann wird M eine *Extension* von M_1 durch M_2 genannt, wenn es Morphismen $f : M_1 \to M$ und $g : M \to M_2$ gibt, die eine kurze exakte Sequenz $0 \to M_1 \to M \to M_2 \to 0$ bilden. Wir schreiben $\xi = (M, f, g)$ für alle Daten einer kurzen exakten Sequenz. Die kurze exakte Sequenz ist *spaltend*, wenn es einen Schnitt $s : M_2 \to M$ gibt, d.h. der Morphimus s erfüllt $g \circ s = \mathrm{id}_{M_2}$. Zwei kurze exakte Sequenzen sind äquivalent, wenn es einen Morphismus φ gibt, sodass das Diagramm

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "f_1"] \arrow[d, "\mathrm{id}_{M_1}"] & M \arrow[r, "g_1"] \arrow[d, "\varphi"] & M_2 \arrow[r] \arrow[d, "\mathrm{id}_{M_2}"] & 0 \\ 0 \arrow[r] & M_1 \arrow[r, "f_2"] & \widetilde{M} \arrow[r, "g_2"] & M_2 \arrow[r] & 0\,, \end{tikzcd} \tag{9.8}$$

kommutiert. Das Lemma (6.1) impliziert, dass in diesem Fall φ ein Isomorphismus ist. Damit ist Äquivalenz von Extensionen symmetrisch und somit offensichtlich eine Äquivalenzrelation. Die Menge der Äquivalenzklassen von Extensionen bezeichnen wir mit $e(M_2, M_1)$, die Elemente typischerweise mit $[\xi]$

Als Beispiel betrachten wir $R = \mathbb{Z}$ und $M_1 = M_2 = \mathbb{Z}/p\mathbb{Z}$ für eine ungerade Primzahl p. Die spaltenden Sequenz, also mit $M = M_1 \oplus M_2$ ist offensichtlich (Elementordnungen!) nicht zur Sequenz mit $\xi = (M, f, g)$ mit $M = \mathbb{Z}/p^2\mathbb{Z}$ und Abbildungen definiert durch $f(1) = p$ sowie $g : 1 \mapsto 1$ äquivalent. Es gibt aber auch inequivalente Extensionen mit dem gleichen Modul M in der Mitte. Wir nehmen dazu $\xi_2 = (M, f_2, g)$ mit $f_2(1) = 2p$ her, was auch eine injektive Abbildung ist. Angenommen es gibt einen Automorphismus $\varphi : M \to M$, der das Diagramm (9.11) kommutativ macht. Dann muss $\varphi(p) = 2p$ sein. Man rechnet nach, dass der einzige Automorphismus mit dieser Eigenschaft durch $\varphi(1) = 2$ definiert ist. Damit aber kommutiert das hintere Quadrat nicht.

Satz 9.11 *Es gibt eine Bijektion $\psi : e(M_2, M_1) \to \mathrm{Ext}^1(M_2, M_1)$ zwischen Äquivalenzklassen von Extensionen und dem ersten Ext-Modul. Diese Bijektion bildet die spaltende Extension auf das Nullelement ab.*

Insbesondere spaltet jede Extension von M_1 durch M_2 genau dann wenn $\mathrm{Ext}^1(M_2, M_1) = 0$ ist.

Beweis: Wir starten mit der Definition von ψ und mit einer Extension $\xi = (M, f, g)$. Wir nehmen eine projektive Auflösung von M_2 und konstruieren wie im Beweis von Satz (9.2) Abbildungen φ_i, sodass das Diagramm

$$\begin{tikzcd}
P_3 \arrow[r, "d_3"] \arrow[d] & P_2 \arrow[r, "d_2"] \arrow[d] & P_1 \arrow[r, "d_1"] \arrow[d, "\varphi_1"] & P_0 \arrow[r, "d_0"] \arrow[d, "\varphi_0"] & M_2 \arrow[r] \arrow[d, "\mathrm{id}_{M_2}"] & 0 \\
0 \arrow[r] & 0 \arrow[r] & M_1 \arrow[r, "f"] & M \arrow[r, "g"] & M_2 \arrow[r] & 0\,,
\end{tikzcd} \tag{9.9}$$

kommutiert (bzw. wir wenden diesen Satz auf ξ nach links fortgesetzt mit Nullen an). Dann definiert $[\varphi] \in \mathrm{Ext}^1(M_2, M_1)$, denn $\varphi \in \mathrm{Ker}(d_2^*)$ und wir setzen $\psi([\xi]) = [\varphi]$.

Dabei sind nun mehrere Wohldefiniertheiten zu prüfen. Zuerst ist zu zeigen, dass $[\varphi]$ nicht von der Wahl der Abbildungen, die wir in (9.10) gewählt haben, abhängt. Seien φ_i' eine andere Wahl und h_i die Bausteine der Homotopie, die nach Satz (9.2) existiert. Da h_1 als Bild den Nullmodul hat, ist also nach Definition einer Homotopie $\varphi_1 - \varphi_1' = h_0 \circ d_1$ und das ist genau was Gleichheit von Klassen in $H_1(\mathrm{Hom}\,(P_\bullet, M_1))$ bedeutet. Weiterhin ist zu zeigen, dass äquivalente Extensionen das gleiche Bild haben. Dies folgt sofort aus der Definition von ψ, da wir φ_1 beim Vergleich von Extensionen wie in (9.11) einfach nur mit id_{M_1} verketten.

Für die zweite Aussage über eine Extension mit einer Spaltung s genügt es $\varphi_0 = s \circ d_0$ und $\varphi_1 = 0$ zu nehmen.

Zur Konstruktion einer Umkehrabbildung nehmen wir wieder die projektive Auflösung $P_\bullet \to M_2$ und ein Element in $\mathrm{Ext}^1(M_2, M_1) = H_1(\mathrm{Hom}\,(P_\bullet, M_1))$ her, also eine Abbildung $\varphi_1 : P_1 \to M_1$ mit $\varphi \circ d_2 = 0$. Damit haben wir eine exakte Sequenz $0 \to P_1/\,\mathrm{Bild}(d_2) \to P_0 \to M_2 \to 0$. Um daraus eine Extension von M_1 durch M_2 zu machen, wenden wir das untenstehende Lemma 9.12 an und definieren damit die Abbildung $\theta : \mathrm{Ext}^1(M_2, M_1) \to e(M_2, m_1)$.

Zur Wohldefiniertheit der Abbildung ist zu zeigen, dass die Äquivalenzklasse der Extension nicht von der Wahl von φ_1 modulo Ränder abhängt. Eine andere Wahl φ_1' unterscheidet sich von der ursprünglichen um das d_1-Bild einer Abbildung $h : P_0 \to M_1$, also $\varphi_1' - \varphi_1 = h \circ d_1$. Dann aber kommutiert das Diagramm

$$\begin{tikzcd}
P_3 \arrow[r, "d_3"] \arrow[d] & P_2 \arrow[r, "d_2"] \arrow[d] & P_1 \arrow[r, "d_1"] \arrow[d, "\varphi_1'"] & P_0 \arrow[r, "d_0"] \arrow[d, "\varphi_0 + h"] & M_2 \arrow[r] \arrow[d, "\mathrm{id}_{M_2}"] & 0 \\
0 \arrow[r] & 0 \arrow[r] & M_1 \arrow[r, "f"] & M \arrow[r, "g"] & M_2 \arrow[r] & 0\,,
\end{tikzcd} \tag{9.10}$$

mit der gleichen unteren Reihe wie zuvor.

Es bleibt zu zeigen, dass die Verkettungen $\theta \circ \psi$ und $\psi \circ \theta$ jeweils die Identität auf den Definitionsbereichen ist. (Übung) □

Lemma 9.12 *Gegeben ein Morphismen wie im Diagramm*

$$\begin{tikzcd} 0 \arrow[r] & X_1 \arrow[r, "f_1"] \arrow[d, "\varphi_1"] & X \arrow[r, "g_1"] & M_2 \arrow[r] \arrow[d, "id_{M_2}"] & 0 \\ & M_1 & & M_2 & , \end{tikzcd} \tag{9.11}$$

sodass die erste Zeile exakt ist. Dann gibt es eine Ergänzung der zweiten Zeile zu einer Extension von M_1 durch M_2. Je zwei solche Ergänzungen sind äquivalente Extensionen.

Beweis: Übung. □

Stichwortverzeichnis