Einführung in die Modultheorie

Alexander von Felbert

01.05.2007

Inhaltsverzeichnis

1 Motivation und Überblick

Zu den wichtigsten algebraischen Konstrukten gehören, neben den Klassikern wie Gruppe, Ring, Körper und Vektorraum, auch und inbesondere die Moduln. Die Theorie der Moduln hat sich als Erweiterung der Ringtheorie aus der Darstellungstheorie von Gruppen, Ringen und Algebren entwickelt. In ihr finden die Methoden der Ringtheorie und der linearen Algebra Anwendung. An den vielen Beispielen werden wir sehen, dass der Begriff des Moduls über einem Ring viele der algebraischen Strukturen verallgemeinert.

Der Begriff Modul ist auch Grundlage der sog. Homologischen Algebra. Historisch steht der heutige Begriff am Ende einer langen Entwicklung, die damit begann, dass Gauß die Bezeichnung $a \equiv b \mod m$ – gelesen: a kongruent b modulo m – einführte für die Aussage, dass $a - b$ durch m teilbar ist ($a, b, m \in \mathbb{Z}$ mit $m > 0$). Als „Modul“ wurde zunächst die Zahl m, später die Menge aller ganzzhaligen Vielfachen von m, also die Teilmenge (bzw. das Ideal)

$$m \cdot \mathbb{Z} := \{mx | x \in \mathbb{Z}\}$$

von $\mathbb{Z}$ bezeichnet.

Einige Ergebnisse der linearen Algebra können leicht modifiziert für bestimmte Moduln angewendet werden. Es ist sicher hilfreich diese analogen Kenntnisse zunächst in der linearen Algebra zu studieren. Ferner sollte man Elementares über Gruppen und Ringe wissen, d.h. Worte wie Normalteiler, Ideal oder Ähnliches sollten keine Fremdwörter sein.

Dieses Dokument ist als ausführliche Einführung in die Theorie der Moduln zu verstehen. Viele Beweise oder Beispiele die in der Literatur oftmals nur kurz abgehandelt werden, sind in hier ausführlich festgehalten. Allerdings kratzen wir hier nur an der Oberfläche, denn weiterführende Themen werden, wenn überhaupt nur oberflächlich behandelt. Die vorkommenden Sätze, Lemmata und Beispiele habe ich jedoch so ausgewählt, dass wichtige weiterführende Themen, wie exakte Sequenzen, freie oder projektive Moduln, im Anschluss ohne Probleme studiert werden können.

2 Links-, Rechts- und Bimoduln

Bevor wir loslegen, definieren wir was wir unter einer inneren bzw. äußeren Verknüpfung verstehen.

Definition
Es seien M und N Mengen und $M \times M$ bzw. $M \times N$ ihr kartesisches Produkt. Unter einer **inneren Verknüpfung** auf M versteht man eine Abbildung $M \times M \to M$. Unter einer **äußeren Verknüpfung** auf M verstehen wir eine Abbildung $N \times M \to M$.

Die Forderung nach einer inneren Verknüpfung stellt also sicher, dass die Abbildung innerhalb der vorgegebenen Menge M operiert. Eine äußere Verknüpfung auf M schränkt das Bild einer speziellen Abbildung, die auf zwei im Allgemeinen verschiedenen Mengen

definiert ist, auf M ein.

2.1 Linksmoduln

Neben der nun folgenden Definition eines Linksmoduls existiert eine äquivalente Charakterisierung dieses algebraischen Konstrukts, die wir nach einigen Bemerkungen zur Definition anführen werden.

Definition (Linksmodul)
Es sei $R = (R, +, \cdot)$ ein Ring und $M = (M, \hat{+})$ eine ablesche Gruppe. M zusammen mit einer äußeren Verknüpfung (skalare Multiplikation)

$$\begin{aligned} * : R \times M &\to M \qquad \text{definiert durch} \\ (\alpha, x) &\mapsto \alpha * x \end{aligned}$$

heißt ein R-**Linksmodul** (oder **Linksmodul über** R) , wenn gilt:

(M_1) $(\alpha + \beta) * x = \alpha * x \ \hat{+} \ \beta * x$ (Distrubutivgesetze)

(M_2) $\alpha * (x \ \hat{+} \ y) = \alpha * x \ \hat{+} \ \alpha * y$

(M_3) $(\alpha \cdot \beta) * x = \alpha * (\beta * x)$ (Assoziativgesetz)

für alle $\alpha, \beta \in R$ und $x, y \in M$. Hat R ein Einselment 1, dann heißt der Modul unitär, wenn zusätzlich für alle $x \in M$ das *unitäres Gesetz* gilt :

$$1 * x = x. \qquad (M_4)$$

Die Distributivgesetze (M_1) und (M_2) fordern die „Verträglichkeit“ der Verknüpfung $*$ mit der Addition $+$ in R und der Addition $\hat{+}$ in M. Entsprechend stellt das Assoziativgesetz (M_3) die Verbindung der Multiplikation $\cdot$ in R mit der Skalarmultiplikation $*$ her.

Bemerkung 1
Beachten Sie, dass in vielen (äquivalenten) Definitionen eines Modul nicht zwischen der äußeren Verknüpfung $*$ und der Ringmultiplikation $\cdot$ unterschieden wird, und stattdessen dafür ein und dasselbe Symbol (meist $\cdot$) verwendet wird. Entpsrechendes gilt auch für die Ringaddition und die Addition von M. Weiter unten in diesem Dokument werden wir, soweit keine Verwechslungen zu befürchten sind, diese strenge Notation zu Gunsten einer einfacheren aufgeben. Das Produkt eines Paares $x, y \in R$ schreiben wir meist in der üblichen Kurzform ab anstatt $a \cdot b$.

Natürlich kann man, wie auch bei Gruppen oder Ringen, insbesondere die Axiome (M_1), (M_2) und (M_3) per Induktion erweitern: Bspw. gilt dann für $\alpha \in R$ und

$x, y, z \in M : \alpha * (x + y + z) = \alpha * (x + (y + z)) = \alpha * x \ \hat{+} \ \alpha * (x + y) = \alpha * x \ \hat{+} \ \alpha * x \ \hat{+} \ \alpha * y.$

Die Definition der Moduln *ähnelt* der Definition eines K-Vektorraums (K ein Körper) sehr: Die Axiome sind im Prinzip identisch, nur dass ein Vektorraum stets einen Körper K anstatt eines Ringes R fordert.

Definition
Es sei K ein Körper. Ein K-Modul V, nennt man K-**Vektorraum**.

Jeder K-Vektorraum V ist ein K-Modul V, d.h. jeder Vektorraum ist ein Modul über einem Körper. Die Umkehrung gilt im Allgemeinen jedoch nicht, d.h. es gibt R-Moduln die nicht die Vektorraum-Axiome erfüllen.

Im Vorgriff auf das erste Beispiel a) werden wir eine wichtige äußere Verknüpfung herleiten:
Es sei $(R, +, \cdot)$ ein Ring und weiter seien $\alpha \in R$ und $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Aufgrund der Definitionen der beiden Ringverknüpfungen $+$ und $\cdot$ können wir eine Skalarmultiplikation $*$ (und sogar noch mehr) zwischen der Menge der natürlichen Zahlen $\mathbb{N}$ und R wie folgt erklären:

- $0 * \alpha := 0$
- $n * \alpha := \underbrace{\alpha + \ldots + \alpha}_{n \text{ Mal}}$
- $\alpha^n := \underbrace{\alpha \cdot \ldots \cdot \alpha}_{n \text{ Mal}} = \underbrace{\alpha + \ldots + \alpha}_{\alpha^{n-1} \text{ Mal}}$
- $(-n) * \alpha := -(n * \alpha)$.

Natürlich kann man die ersten beiden Gleichungen auch via Induktion verifizieren: Der Induktionsanfang ist klar, da $0 * n := 0$ gemäß Definition gilt. Der Induktionsschritt ist aufgrund der Gleichung $n * \alpha = (n-1) * \alpha + \alpha$ ebenfalls klar. Entsprechend könnte man auch die Potenz via Induktion verifizieren.

Der letzte Punkt weitet die Definition der Skalarmultipliaktion auf $\mathbb{Z}$ und R aus; darauf kommen wir noch einmal zurück. Diese wohlbekannten, und in diesem Licht doch neuen, Rechenregeln werden sich für das erste Beispiel als nützlich erweisen.

2.2 Beispiele zu Moduln

In diesem Abschnitt werden wir wichtige Beispiele für Moduln kennenlernen und soweit nötig deren Eigenschaften auch explizit nachweisen.

Beispiel

a) Es sei $G = (G, \hat{+})$ eine abelsche Gruppe und $+$ die übliche Addition in $\mathbb{Z}$. Für $n, m \in \mathbb{N}_0$ und $x, y \in G$ ist $n * x$ bereits induktiv definiert worden. Für eine negative ganze Zahl $n \in \mathbb{Z}, n < 0$, setzt man $n*x := (-n)*(-x)$ in additiver Schreibweise.

Mit der oben erklärten skalaren Multiplikation $*$ ist G ein unitärer $\mathbb{Z}$-Linksmodul.

Beweis. Bedingung (M_4) der Definition folgt direkt aus der Definition von $*$, denn offensichtlich gilt dann $1*x = x$. Bedingung (M_1) ist ebenso einfach zu verifizieren, da für $n, m \in \mathbb{Z}$ offensichtlich gilt

$$\begin{aligned}(n+m) * x &= \underbrace{x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x}_{n+m \text{ Mal}} \\ &= \underbrace{x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x}_{n \text{ Mal}} \mathbin{\hat{+}} \underbrace{x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x}_{m \text{ Mal}} \\ &= n * x \mathbin{\hat{+}} m * x.\end{aligned}$$

Die Bedingung (M_2) kann ebenfalls durch Nachrechnen geprüft werden, dabei ist zu beachten, dass die folgenden Umformungen nur deshalb möglich sind, da die Gruppe als kommutativ (bzw. ablesch) vorausgesetzt wird.

$$\begin{aligned}(x \mathbin{\hat{+}} y) \cdot n &= \underbrace{(x \mathbin{\hat{+}} y) \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} (x \mathbin{\hat{+}} y)}_{n \text{ Mal}} \\ &= (\underbrace{x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x}_{n \text{ Mal}}) \mathbin{\hat{+}} (\underbrace{y \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} y}_{n \text{ Mal}}) \\ &= x * n \mathbin{\hat{+}} y * n.\end{aligned}$$

Schließlich bleibt noch (M_3) zu zeigen durch

$$\begin{aligned}(n \cdot m) * x &= \underbrace{(x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x)}_{n \cdot m \text{ Mal}} \\ &= \underbrace{\underbrace{(x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x)}_{m \text{ Mal}} \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} \underbrace{(x \mathbin{\hat{+}} \ldots \mathbin{\hat{+}} x)}_{m \text{ Mal}}}_{n \text{Mal}} \\ &= n * (m * x).\end{aligned}$$

Damit haben wir alle notwendigen Axiome der Definition nachgewiesen und es folgt, dass alle abelsche Gruppen G $\mathbb{Z}$-Linksmoduln sind. □

b) Es sei $R = (R, +, \cdot)$ ein Ring und seien $x, y \in R$. Betrachten wir die Ringmultiplikation als äußere Verknüpfung von Elementen aus R mit Skalaren aus R. Konkret soll die Skalarmultiplikation $* : R \times R \to R$ definiert sein durch $(x, y) \mapsto x * y := x \cdot y = xy$, es wird also die Ringmultiplikation als skalare Mulitplikation interpretiert. Entsprechend nimmt der Ring R eine Doppelrolle ein.

Da ein Ring gemäß Definition bzgl. der Multiplikation assoziativ und distributiv ist, sind (M_1) bis (M_3) natürlich erfüllt. Die Bedingung (M_4) ist genau dann erfüllt, wenn R selbst unitär ist, d.h. ein Einselement enthält.

c) Ist K ein Schiefkörper, dann zeigt ein Vergleich der Definitionen, dass die unitären K-Linksmoduln genau die Linksvektorräume über K sind.

d) Ist M eine abelsche Gruppe, R ein Ring und definiert man die skalare Multiplikation $(\alpha, x) \mapsto \alpha * x := 0$ für alle $\alpha \in R$ und $x \in M$, dann wird M ein R-Linksmodul. Moduln dieser Art heißen **trivial**.

e) Ist G eine abelsche Gruppe und $R = End(G)$, der Ring der Endomorphismen von G, dann ist G zusammen mit der natürlichen Operation

$$\begin{aligned} * : End(G) \times G &\to G \\ (\alpha, x) &\mapsto \alpha * x := \alpha(x) \end{aligned}$$

ein R-Linksmodul. Sämtliche Axiome (M_1) bis (M_3) bzw. (M_4) folgen aus der Definition eines Endomorphimus.

Die strenge Notation zwischen äußerer Verknüpfung und Ringmulitplikation lassen wir nun fallen!

Beispiel
Es seien K ein Körper und V ein Vektorraum über K. Weiter sei $f : V \to V$ eine K-lineare Abbildung von V in sich, also ein Vektorraum-Endomorphismus. Ist $p := \sum_{i=1}^{n} a_i X^i$ ein Polynom aus $K[X]$, dann ist auch die Abbildung

$$p(f) : K[x] \times End(V) \to End(V) \qquad \text{mit} \qquad (p, f) \mapsto p(f) = \sum a_i f^i$$

linear. Die Eigenschaften eines Endomorphismus bleiben durch die i-fache Komposition der Funktion f mit sich selbst, konkret $f^i = \underbrace{f \circ \ldots \circ f}_{i \text{ Mal}}$, erhalten. Definiert man eine äußere Verknüpfung wie folgt:

$$\begin{aligned} \cdot : \ K[X] \times V &\to V \qquad \text{definiert durch} \\ (p, v) &\mapsto p(f)(v) = \sum a_i f^i(v), \end{aligned}$$

für alle $p \in K[X]$ und $v \in V$, dann ist V zusammen mit der äußeren Verknüpfung ein unitärer $K[X]$-Modul. Wir konstatieren, dass die Abbildung $(p, v) \mapsto p(f)(v)$ auf den Vektor $v \in V$ angewendet werden kann, da $p(f) = \sum a_i f^i$ ein Vektorraum-Endomorphismus von V ist. Das Polynom f selbst kann nicht auf den Vektor v angewendet werden. Man beachte im Folgenden, dass $f^0 = id$ gerade die Identität ist.

Beweis. Es seien $p, q \in K[X]$ zwei Polynome und $v \in V$, dann folgt die Eigenschaft (M_1) folgt durch

$$\begin{aligned} (p+q) \cdot v &= \left(\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} b_j X^j \right) \cdot v \\ &= \left(\sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k \right) \cdot v, \end{aligned}$$

wobei die Koeffizienten a_i bzw. b_j mit $n < i \leq \max(m,n)$ bzw. $m < j \leq \max(m,n)$ gleich 0 gesetzt werden, je nachdem, ob m oder n das Maxium der beiden natürlichen Zahlen ist. Es sei $\max := \max(m,n)$, dann gilt

$$\begin{aligned}
(p+q)\cdot v &= \left(\sum_{k=0}^{\max}(a_k+b_k)X^k\right)\cdot v \\
&= \left(\sum_{k=0}^{\max}(a_k+b_k)f^k(v)\right) \\
&= (a_0+b_0)+(a_1+b_1)f(v)+\ldots+(a_{\max}+b_{\max})f^{\max}(v) \\
&= a_0+a_1f(v)+\ldots+a_{\max}f(v)^{\max}+b_0+b_1f(v)+\ldots+b_{\max}f^{\max}(v) \\
&= \left(\sum_{i=0}^{n}a_if^i(v)\right)+\left(\sum_{j=0}^{m}b_jf^j(v)\right) \\
&= p\cdot v+q\cdot v.
\end{aligned}$$

Bisher haben wir also nicht die spziellen Eigenschaften eines Ringendomorphismus benötigt, dies wird sich beim Nachweis der Bedingung (M_2) ändern. Es seien $v,w\in V$ und $p,q\in K[X]$:

$$\begin{aligned}
p\cdot(v+w) &= \sum_{i=0}^{n}a_iX^i\cdot(v+w) \\
&= \sum_{i=0}^{n}a_if^i(v+w) && (1)\\
&= a_0+a_1(f(v)+f(w))+\ldots+a_n(f^n(v)+f^n(w)) && (2)\\
&= a_0+a_1f(v)+\ldots+a_nf^n(v)+a_0+a_1f(w)+\ldots+a_nf^n(w) \\
&= p\cdot v+p\cdot w
\end{aligned}$$

Den Übergang von (1) zu (2) ist deshalb legitim, da f nach Voraussetzungen ein Endomorphismus ist und die Komposition von endomorphen Funktionen selbst wieder endomorph ist. Schließlich müssen wir noch (M_3) zeigen; seien dazu $p,q\in K[X]$ und $v\in V$:

$$\begin{aligned}
(pq)\cdot v &= \left(\sum_{i=0}^{n}a_iX^i\sum_{j=0}^{m}b_jX^j\right)\cdot v \\
&= \left(\sum_{k=0}^{n+m}\left(\sum_{k=i+j}a_ib_j\right)X^k\right)\cdot v \\
&= \sum_{k=0}^{n+m}\left(\sum_{k=i+j}a_ib_j\right)f^k(v)
\end{aligned}$$

Schreibt man die letzte Summe aus, so erhält man

$$= a_0b_0+(a_0b_1+a_1b_0)f(v)+(a_2b_0+a_0b_2+a_1b_1)f^2(v)\ldots+(a_nb_m)f^{m+n}(v).$$

Andererseits gilt für $p := \sum_{i=0}^{n} a_i X^i, q := \sum_{j=0}^{m} b_j X^j$ die Gleichungskette

$$\begin{aligned} p \cdot (q \cdot v) &= p \cdot \left(\sum_{j=0}^{m} b_j f^j(v) \right) \\ &= \sum_{i=0}^{n} a_i f^i \left(\sum_{j=0}^{m} b_j f^j(v) \right), \end{aligned} \tag{3}$$

und schreiben wir (3) aus, so ist diese Summe gerade

$$\begin{aligned} &= a_0 f^0 \left(\sum_{j=0}^{m} b_j f^j(v) \right) + \ldots + a_n f^n \left(\sum_{j=0}^{m} b_j f^j(v) \right) \\ &= a_0 b_0 + a_0 b_1 f(v) + \ldots + a_0 b_m f^m(v) \\ &\quad + a_1 f \left(\sum_{j=0}^{m} b_j f^j(v) \right) + \ldots a_n f^n \left(\sum_{j=0}^{m} b_j f^j(v) \right) \\ &= a_0 b_0 + a_0 b_1 f(v) + \ldots + a_0 b_m f^m(v) \\ &\quad + a_1 f(b_0 + b_1 f(v) + b_2 f^2(v) + \ldots + b_m f^m(v)) \\ &\quad + a_2 f^2(b_0 + b_1 f(v) + b_2 f^2(v) + \ldots + b_m f^m(v)) \\ &\quad + \vdots \\ &\quad + a_n f^n(b_0 + b_1 f(v) + b_2 f^2(v) + \ldots + b_m f^m(v)) \end{aligned}$$

$$\begin{aligned} &= a_0 b_0 + a_0 b_1 f(v) + \ldots + a_0 b_m f^m(v) \\ &\quad + a_1 f(b_0) + a_1 f(b_1 f(v)) + a_1 f(b_2 f^2(v)) + \ldots + a_1 f(b_m f^m(v)) \\ &\quad + a_2 f^2(b_0) + a_2 f^2(b_1 f(v)) + a_2 f^2(b_2 f^2(v)) + \ldots + a_2 f^2(b_m f^m(v)) \\ &\quad + \vdots \\ &\quad + a_n f^n(b_0) + a_n f^n(b_1 f(v)) + a_n f^n(b_2 f^2(v)) + \ldots + a_n f^n(b_m f^m(v)) \\ &= a_0 b_0 + a_0 b_1 f(v) + \ldots + a_0 b_m f^m(v) \\ &\quad + a_1 b_0 f(1) + a_1 b_1 f^2(v) + a_1 b_2 f^3(v) + \ldots + a_1 b_m f^{m+1}(v) \\ &\quad + a_2 b_0 f^2(1) + a_2 b_1 f^3(v) + a_2 b_2 f^4(v) + \ldots + a_2 b_m f^{m+2}(v) \\ &\quad + \vdots \\ &\quad + a_n b_0 f^n(1) + a_n b_1 f^{n+1}(v) + a_n b_2 f^{n+2}(v) + \ldots + a_n b_m f^{n+m}(v) \end{aligned}$$

Aus der letzten Gleichung kann man, die Diagonalen berücksichtigt, ablesen, dass die geforderte Identität tatsächlich besteht.

Es ist nur noch (M_4) nachzuweisen: Das neutrale Element des Polynomrings ist bezüglich der Multiplikation das Polynom $1X^0$ (und nicht etwa die konstante Einsfunktion!). Es gilt also $\forall v \in V : 1X^0 \cdot v = f^0(v) = id(v) = v$, damit ist (M_4) nachgewiesen. □

2.3 Charakterisierung von Moduln

Wie Sie wahrscheinlich bereits wissen hängt die Existenz einer Gruppenoperation unmittelbar mit der Existenz eines speziellen Homomorphismus zusammen. Auch die Existenz eines Moduls kann alternativ mit Hilfe eines speziellen Ring-Homomorphismuses charakterisiert werden:

Lemma 2.1: *Sei R ein Ring und M ein R-Modul. Dann kann man aus M stets einen Ring-Homomorphismus $\omega : R \to End(M)$ und umgekehrt induzieren.*

Letztes Lemma besagt also, dass man zu gegebenem R-Modul M stets einen Ring-Homomorphismus $\omega : R \to End(M)$ gewinnen kann. Andererseits induziert ein vorgegebenen Ring-Homomorphismus der Form von ω auch stets ein R-Modul. Deshalb sagt man auch, dass ein R-Modul M und ein Ring-Homomorphismus $\omega : R \to End(M)$ im wesentlichen dasselbe sind. Bevor wir diese Aussage beweisen noch eine wichtige Bemerkung vorab.

Bemerkung 2
Will man also aus einem Ring-Homomorphismus ω einen Modul ${}_RM$ generieren, so definiert man eine *äußere Verknüpfung* $R \times M \to M$ durch

$$(\alpha, x) \mapsto \alpha \cdot x := \omega(\alpha)(x), \qquad \forall x \in M$$

d.h. man wendet den Endomorphismus $\omega(\alpha) \in End(M)$ auf das Element $x \in M$ an.

Beweis.
Es sei $\omega : R \to End(M)$ ein Ring-Homomorphismus. Wir müssen zeigen, dass mit Hilfe von ω alle Punkte der Definition, also (M_1) bis (M_4), erfüllbar sind. Dazu definieren wir unsere äußere Verknüpfung, wie in Bemerkung 2 beschrieben.

Die Bedingung (M_2) folgt dann aufgrund der Eigenschaften des Ring-Homomorphismuses ω, denn es gilt

$$\begin{aligned} \alpha \cdot (x+y) &= \underbrace{\omega(\alpha)}_{\in End(M)} (x+y) \\ &= \omega(\alpha)(x) + \omega(\alpha)(y) = \alpha \cdot x + \alpha \cdot y. \end{aligned}$$

Die Bedingungen (M_1) und (M_3) bedeuten, dass $\omega : R \to End(M)$ mit der Addition bzw. Multiplikation verträglich ist. Wir konstatieren, dass ω selbst ein Ring-Homomorphismus ist und das Bild von Omega ein Endomorphismus von M, d.h. wir bilden in den Endomorphismenring $(End(M), +, \circ)$ ab, der als multiplikative Verknüp-

fung die Komposition besitzt. Deshalb gilt:

$$\begin{aligned}(\alpha+\beta)\cdot x &= \omega(\alpha+\beta)(x)\\ &= [\omega(\alpha)+\omega(\beta)](x)\\ &= \omega(\alpha)(x)+\omega(\beta)(x) = \alpha\cdot x+\beta\cdot x,\end{aligned}$$

$$\begin{aligned}(\alpha\beta)\cdot x &= \omega(\alpha\beta)(x)\\ &= [\omega(\alpha)\circ\omega(\beta)](x) = \alpha\cdot(\beta\cdot x).\end{aligned}$$

Die Bedingung (M_4) besagt, dass ω das Einselement von R in das Einselement von $End(M)$ abbildet, was ein Ring-Homomorphismus $R \to End(M)$ natürlich erfüllt. Es folgt, dass mit Hilfe von ω ein R-Modul erklärt ist.

Ist umgekehrt ein Modul gegeben, so ist es nun die Aufgabe daraus einen Ringhomomorphismus zu konstruieren. Dazu nutzen wir die äußere Verknüpfung des Moduls

$$\begin{aligned}R\times M &\to M\\ (\alpha, x) &\mapsto \alpha\cdot x\end{aligned}$$

die (M_1) bis (M_4) erfüllt, so kann man $\omega : R \to End(M)$ durch $\omega(\alpha)(x) =: \alpha\cdot x$ definieren. Man kann nun analog für die Rückrichtung argumentieren und stellt fest, dass ω ein Ring-Homomorphismus ist. □

Bevor wir weitere Beispiele zur äquivalenten Charakterisierung eines Moduls untersuchen, führen wir ein wichtiges Prinzip ein, dass auch in der klassischen Algebra (insbesondere in der Galois-Theorie) von großer Bedeutung ist:

Ziel ist es die Existenz, die Anzahl oder die Eindeutigkeit bspw. eines Homomorphismuses nachzuweisen. Um dies zu bewerkstelligen, geht man in diesem **Beweisverfahren** zunächst davon aus, dass es eine derartige Abbildung tatsächlich gibt. Dadurch folgert man (notwendig viele) grundlegende Eigenschaften des Homomorphismus, um im Anschluss die Existenzannahme fallen zu lassen. Mit Hilfe der gewonnen Charakterisierung des Homomorphismus versucht man sodann nachzuweisen, dass und in welcher Quantität dieser existieren kann.

Mit Hilfe des beschriebenen Beweisverfahrens zeigen wir, dass es zwischen dem Ring $(\mathbb{Z}, +, \cdot)$ und einem beliebigen Ring $(R, \hat{+}, \hat{\cdot})$ nur *einen* Homomorphismus g geben kann. Nehmen wir also zunächst an, dass ein Ring-Homomorphismus $g : \mathbb{Z} \to R$ existiert. Dann stimmt der Funktionswert $g(1) = 1_R \in R$ mit dem Einselement aus R überein, da ein Homomorphismen Einselemente auf Einselemente abbildet. Aus der Verträglichkeit des Homomorphismus g mit der Addition folgt weiter

$$\begin{aligned}g(n) = g(n\cdot 1) &= g(\underbrace{1+\ldots+1}_{n \text{ Mal}})\\ &= \underbrace{g(1)+\ldots+g(1)}_{n \text{ Mal}} = n \,\hat{\cdot}\, g(1) = n \,\hat{\cdot}\, 1_R\end{aligned}$$

für alle $n \in \mathbb{Z}$, wobei wir uns dabei auf die Definition der äußeren Verknüpfung (d.h. der multiplikativen Verknüpfung von R) $\hat{\cdot}$ aus Abschnitt 2.1 stützen (dazu fasst man R als Modul über $\mathbb{Z}$ auf). Weiter gilt für $m, n \in \mathbb{Z}$

$$\begin{aligned} g(mn) =& g(\underbrace{n + \ldots + n}_{m \text{ Mal}}) = \underbrace{g(n) + \ldots + g(n)}_{m \text{ Mal}} \\ =& \underbrace{n \hat{\cdot} 1_R + \ldots + n \hat{\cdot} 1_R}_{m \text{ Mal}} = (mn) \hat{\cdot} 1_R. \end{aligned}$$

Wenn es also einen Ringhomomorphismus $g : \mathbb{Z} \to R$ gibt, so ist es die Abbildung $n \mapsto n \hat{\cdot} 1_R$. Wir müssen dazu noch zeigen, dass $g : \mathbb{Z} \to R$ dann tatsächlich ein Homomorphismus ist. Dazu können wir ausnutzen, dass $(R, \hat{+}, \hat{\cdot})$ ein Modul über dem Ring $(\mathbb{Z}, +, \cdot)$ ist.

Die Additivität folgt durch $g(n+m) = (n+m) \hat{\cdot} 1_R = n \hat{\cdot} 1_R \ \hat{+} \ m \hat{\cdot} 1_R = g(n) \ \hat{+} \ g(m)$. Entsprechend folgt die Homogenität druch $g(mn) = (mn) \hat{\cdot} 1_R = m \hat{\cdot} (n \hat{\cdot} 1_R) = (m \hat{\cdot} 1_R) \hat{\cdot} (n \hat{\cdot} 1_R) = g(m) \hat{\cdot} g(n)$. Abschließend sei konstatiert, dass die Abbildung g gerade diejenige Abbildung ist, mit der man den sog. Primring konstruiiert.

Da man auf einem Bein schlecht steht, verwenden wir das Beweisprinzip noch ein weiteres Mal bei folgender Behauptung: Sei R ein kommutativer, S ein beliebiger Ring und $f : R \to S$ ein Homomorphismus. Unter einer **Erweiterung** oder **Fortsetzung** von f auf $R[X]$ verstehen wir einen Homomorphismus $\widetilde{f} : R[X] \to S$, so dass die „Einschränkung“ $f_{|R}$ mit f übereinstimmt.

Wir behaupten nun: Zu jedem $s \in S$, das mit $Bild(f)$ vertauschbar ist (d.h. $s[f(a)] = [f(a)]s$ für alle $a \in R$), gibt es genau eine Erweiterung $\widetilde{f}$, so dass $\widetilde{f}(x) = s$.

Existiert ein solches $\widetilde{f}$, so muss (aufgrund der Definition eines Ringhomomorphismuses) gelten

$$\begin{aligned} \widetilde{f}\left(\sum_{i=0}^{n} a_i X^i\right) &= \sum_{i=0}^{n} \widetilde{f}\left(a_i X^i\right) \\ &= \sum_{i=0}^{n} \widetilde{f}\left(a_i\right) \widetilde{f}\left(X\right)^i \\ &= \sum_{i=0}^{n} f\left(a_i\right) s^i. \end{aligned}$$

Also gibt es höchstens ein solches $\widetilde{f}$, da die Einschränkung auf R mit der Funktion f übereinstimmen muss. Umgekehrt verifiziert man, dass die Abbildung

$$\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} f(a_i) s^i$$

die gewünschten Eigenschaften besitzt. Die eben bewiesene Eindeutigkeit nutzen wir im zweiten der folgenden Beispiele.

Beispiel

1. Sei M eine abelsche Gruppe. Der einzige Ring-Homomorphismus $\mathbb{Z} \to End(M)$ macht M zu einem Modul über $\mathbb{Z}$. Abelsche Gruppen und Moduln über $\mathbb{Z}$ können daher als dasselbe betrachtet werden.

2. Sei V ein Vektorraum über einem Körper K und $f : V \to V$ eine lineare Abbildung. Zu der K-Modul-Struktur von V gehört ein Homomorphismus $\omega : K \to End(V)$. Für $\alpha \in K$ ist $\omega(\alpha) : V \to V$ die skalare Multiplikation mit dem Element α. Wir wollen ω zu einem Homomorphismus $\widetilde{\omega} : K[X] \to End(V)$ so erweitern, dass $\widetilde{\omega}(X) = f$. Nach dem eben Gezeigten (vor diesen Beispielen) ist das auf genau eine Weise möglich.

2.4 Rechtsmoduln und Bimoduln

Völlig analog zu Linksmoduln werden Rechtsmoduln, nun mit der verkürzten Notation, definiert:

Definition (Rechtsmodul)
Es sei R ein Ring und M eine ablesche Gruppe. M zusammen mit einer äußeren Verknüpfung $\cdot : M \times R \to M$ definiert durch $(x, \alpha) \mapsto x \cdot \alpha$ heißt ein R-**Rechtsmodul** (oder **Rechtsmodul über** R) , wenn gilt:

(M_1') $x \cdot (\alpha + \beta) = x \cdot \alpha + x \cdot \beta$ (Distrubutivgesetze)

(M_2') $(x + y) \cdot \alpha = x \cdot \alpha + y \cdot \alpha$

(M_3') $x \cdot (\alpha\beta) = (x \cdot \alpha) \cdot \beta$ (Assoziativgesetz)

für alle $\alpha, \beta \in R$ und $x, y \in M$.
Hat R ein Einselment 1, dann heißt der Modul **unitär**, wenn zusätzlich für alle $x \in M$ das *unitäres Gesetz* gilt:

$$x \cdot 1 = x. \qquad (M_4')$$

Bemerkung 3
Natürlich heißt ein R-Links-Modul deshalb so, da das Ringelement $\alpha \in R$ in der äußeren Verknüpfung auf der linken Seite steht. Zwischen Links- und Rechtsmodul ist nicht nur aus formalen Gründen zu unterscheiden, es besteht insbesondere ein inhaltlicher Unterschied, vorausgesetzt R ist nicht kommutativ.

Beweis. Wir zeigen durch Widerspruch: Es sei M ein Links-Modul über dem Ring R mit der äußeren Verknüpfung $\cdot : R \times M \to M$. Wir versuchen, das Produkt mit Elementen aus R von rechts zu schreiben. Zur Unterscheidung schreiben wir es mit $\circ$. Es sei also

$$\alpha \cdot x := x \circ \alpha, \qquad \forall \alpha \in R, x \in M$$

Der Linksmodul M ist mit dem so definierten äußeren Produkt $\circ : M \times R \to M$ im Allgemeinen kein Rechtsmodul: Gemäß Voraussetzungen ist M ein Linksmodul, d.h. es gilt insbesondere das Assoziativgesetzt für die skalare Multiplikation eines Ringelements von links. Wir nehmen nun zunächst an, dass M mit der Verknüpfung $\circ$ auch ein Rechtsmodul ist, doch anstelle des Assoziativgesetzes (M_3') gilt dann (alle weiteren Bedingungen kann man o.B.d.A. als gültig voraussetzen)

$$(\alpha\beta) \cdot x = x \circ (\alpha\beta) = (x \circ \alpha) \circ \beta = (\alpha \cdot x) \circ \beta = \beta \cdot (\alpha \cdot x) \lightning .$$

Ein Widerspruch zur Assoziativität des Linksmoduls. Ist R also nicht kommutativ, dann ist ein Linksmodul im Allgemeinen mit dem so definierten Produkt kein Rechtsmodul und umgekehrt, da in diesem Fall das Assoziativitätsgesetz nicht gilt. Die Distributivgesetze und das unitäre Gesetz gelten auch für nicht kommutatives R im Linksmodul M mit äußerer Verknüpfung $\circ$. □

Ist R aber kommutativ, dann erfüllt M zusammen mit der neu definierten äußeren Verknüpfung $\circ$ sämtliche Axiome der Definition eines R-Rechtsmodul, deshalb ist sodann nicht notwendig zwischen Links- und Rechtsmoduln zu unterscheiden. Ein Modul M über einem kommutativen Ring R nennen wir auch **zweiseitig**.

Neben R-Links- und R-Rechtsmoduln gibt es auch noch so genannte (R, S)-Bimoduln.

Definition
Es seien R, S zwei Ringe. Unter einem (R, S)-**Bimodul** verstehen wir ein R-Linksmodul, der gleichzeitig ein S-Rechtsmodul ist und für den gilt

$$(\alpha \cdot x)\beta = \alpha \cdot (x \cdot \beta) \qquad \forall x \in M;\ \alpha \in R,\ \beta \in S.$$

Sprechen wir von einem *Modul* bzw. von einem *R-Modul*, so meinen wir ein einseitiges R-Modul, d.h. entweder ein Links- oder Rechts-Modul, die Seite soll also nicht fixiert sein. Ist in dem Beweis bzw. in der Aussage eines Satzes oder eines Lemma die Seite der äußeren Ringverknüpfung von Bedeutung, so werden wir uns dabei auf die linke oder rechte Seite beschränken. Man beachte jedoch stets, dass alle Aussagen über Links-Moduln analog auch für Rechts-Moduln (Dualität) gelten. Wir werden ein R-Linksmodul M auch kurz mit ${}_RM$ und ein R-Rechtsmodul N mit N_R notieren.

2.5 Moduln und Algebren

In diesem Abschnitt werden wir erklären, was man unter einer Algebra zu verstehen hat, einige Beispiele dazu aufführen und die Zusammenhänge zu Moduln aufzeigen.

Es sei ein n-dimensionaler Vektorraum V über dem Körper K vorgegeben. Unser Ziel ist es aus V eine neue algebraische Struktur ähnlich einem Ring mit zusätzlichen Eigenschaften zu konstruieren.

Dazu sei e_i der i-te Einheitsvektor, d.h. $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)^T$ ist derjenige Vektor dessen i-te Koordinate 1 und dessen sämtliche übrigen Koordinaten 0 sind. Ein jeder Vektor $v = (k_1, \ldots, k_n) \in V$ auf genau eine Weise in der Form

$$v = k_1 e_1 + k_2 e_2 + \ldots + k_n e_n$$

darstellen. Es ist offensichtlich $\{e_i |\ i = 1, 2, \ldots, n\}$ eine Basis des K-Vektorraumes V. In V soll nun eine Vektor-Multiplikation erklärt werden, dazu definieren wir die Produktbildung zuerst für die Standardbasisvektoren

$$e_i e_j := \sum_{k=1}^{n} \lambda_{ijk} e_k \quad \text{für alle } i, j = 1, \ldots, n,$$

$$(ae_i)(be_j) := (ab)e_i e_j = (ab) \sum_{k=1}^{n} \lambda_{ijk} e_k = \sum_{k=1}^{n} (ab) \lambda_{ijk} e_k.$$

wobei die λ_{ijk} beliebige (aber zu fixierende) Elemente aus K sind. Mit Hilfe dieser Festlegung kann man nun das Produkt zweier beliebiger Vektoren erklären.

$$\left(\sum_{i=1}^{n} a_i e_i \right) \left(\sum_{i=j}^{n} b_j e_j \right) := \sum_{i=1}^{n} \sum_{j=1}^{n} (a_i b_j) e_i e_j = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_i b_j \lambda_{ijk} \right) e_k.$$

Da wir uns lediglich einen Vektorraum vorgegeben haben, ist insbesondere die Gültigkeit Assoziativitätsgesetzes der zusätzlichen Verknüpfung also der Multiplikation nachzuweisen. Soll die neue Struktur assoziativ sein, so muss notwendig

$$e_i(e_j e_k) = (e_i e_j) e_k$$

gelten. Rechnet man diese Produkte gemäß Definition nach, so erhält man

$$(e_i e_j) e_k = \left(\sum_{s=1}^{n} \lambda_{ijs} e_s \right) e_k = \sum_{s=1}^{n} \lambda_{ijs} (e_s e_k) = \sum_{s=1}^{n} \left(\lambda_{ijs} \sum_{t=1}^{n} \lambda_{skt} e_t \right) = \sum_{s=1}^{n} \left(\sum_{t=1}^{n} \lambda_{ijs} \lambda_{skt} \right) e_t$$

$$e_i (e_j e_k) = e_i \left(\sum_{s=1}^{n} \lambda_{jks} e_s \right) = \sum_{s=1}^{n} \lambda_{jks} (e_i e_s) = \sum_{s=1}^{n} \left(\lambda_{jks} \sum_{t=1}^{n} \lambda_{ist} e_t \right) = \sum_{s=1}^{n} \left(\sum_{t=1}^{n} \lambda_{jks} \lambda_{ist} \right) e_t$$

Soll also die Multiplikation assoziativ sein, so muss notwendig und hinreichend (aufgrund der Basiseigenschaft von den e_i) die Relation

$$\sum_{t=1}^{n} \lambda_{jks} \lambda_{ist} = \sum_{t=1}^{n} \lambda_{ijs} \lambda_{skt}$$

erfüllt sein. Bündelt man alle Ergebnisse so stellt man fest, dass durch die Festlegung der Multiplikation ein Ring A entstanden ist. Das algebraische Konstrukt A vereinigt dabei gleichzeitig die Vektorraum- und die Ringeigenschaften in sich, wir nennen deshalb A auch eine **Algebra** des Ranges oder der Dimension n über dem Körper K. Offensichtlich wird die Struktur und damit das Rechnen in der Algebra A wesentlich durch die Festlegung der so genannten **Multiplikations-Konstanten** λ_{ijk} bestimmt. So ist die Algebra A auch genau dann **kommutativ**, wenn $e_i e_j = e_j e_i$ und damit

$$\lambda_{ijk} = \lambda_{jik}$$

gilt.

Beispiel
Wir betrachten die Menge der komplexen Zahlen $(\mathbb{C}, +)$ als $\mathbb{R}$-Vektorraum. Unter diesen Umständen ist $\{1, i\}$ die Standardbasis und somit sind $e_1 := 1$ bzw. $e_2 := i$ die Standardbasisvektoren, d.h. man kann jedes Element $\alpha \in \mathbb{C}$ in der Form

$$\alpha = k_1 1 + k_2 i$$

mit $k_1, k_2 \in \mathbb{R}$ schreiben. Die Voraussetzungen sind nun gegeben, um daraus eine $\mathbb{R}$-Algebra zu konstruieren. Dazu müssen wir zunächst die Multiplikation definieren, d.h. die Produkte der Basiselemente bestimmen:

$$\begin{aligned} e_1 e_2 = e_2 e_1 &:= e_2, \\ e_1 e_1 &:= e_1, \\ e_2 e_2 &:= -e_1. \end{aligned}$$

Aus diesen drei Definitionen kann man nun sämtliche Multiplikations-Konstanten extrahieren, z.B. sind für $e_1 e_2 = \sum_{i=1}^{2} \lambda_{12i} e_i$ die Zahlen $\lambda_{121} = 0$ und $\lambda_{122} = 1$ die entsprechenden Größen. Sind also zwei beliebige Zahlen $\alpha, \beta \in \mathbb{C}$ mit $\alpha := a_0 + a_1 i$ und $\beta := b_0 + b_1 i$ gegeben, so ist deren Produkt definiert durch

$$\alpha \cdot \beta = (a_1 e_1 + a_2 e_2) \cdot (b_1 e_1 + b_2 e_2) := \sum_{i=1}^{2} \sum_{j=1}^{2} (a_i b_j) e_i e_j = a_1 b_1 + a_1 b_2 i + a_2 b_1 i - a_2 b_2.$$

Letztlich ergeben sich also daraus die für den Körper $\mathbb{C}$ üblichen Rechenregeln, womit auch bereits alle für die Algebra notwendigen Eigenschaften folgen.

Wir fassen die Erkenntnisse nun in einer Definition zusammen.

Definition
Unter einer **Algebra** A des Ranges n über einem Körper K versteht man einen Ring $(A, +, \cdot)$ mit folgenden Eigenschaften

i) A ist ein n-gliedriger K-Modul:

$$A = Kb_1 + \ldots + Kb_n$$

ii) Die Elemente aus K sind mit den Basiselementen $\{b_1, \ldots, b_n\}$ vertauschbar.

iii) Mit den Produkten von Elementen aus K und A wird nach dem assoziativen Gesetz und dem distributiven Gesetzen gerechnet.

Der Körper K heißt **Grundkörper** von K.

Will man sich kurz fassen, so sagt man zu einer Algebra A des Ranges n über K auch K-Algebra vom Rang n. Das beschriebene Konstrktionsverfahren könnte man auch für vorgegebene unendlich dimensionale K-Moduln durchführen. Weiter könnte man anstatt eines Körpers einen freien R-Modul vorgeben, da auch dieser eindeutige Darstellungen

als Linearkombinationen besitzt. In der noch folgenden alternativen Definition einer Algebra werden wir etwas allgemeiner mit einem festen R-Modul ansetzen.

Das folgende Beispiel wird nun einen Zusammenhang zwischen Modul und Algebra aufzeigen, dies ist für das Verständnis weiterführender Themenbereiche, wie z.B. die Darstellungstheorie (von Köchern), von Notwendigkeit.

Beispiel
Ein beliebiger Ring S lässt sich vermöge des Ringhomomorphismus $\phi : R \to S$ als R-Modul auffassen. Die äußere Verknüpfung $S \times R \to S$ (hier als Rechtsmodul) ergibt sich durch

$$(s, r) \mapsto s\phi(r),$$

also durch die Ringmultiplikation in S. Da ϕ ein Homomorphismus ist, ergeben sich die Modulaxiome von selbst.

Eine Algebra S über dem Ring R ist nun nichts anderes als ein Ringhomomorphismus $\phi : R \to S$, genauer:

Definition
Eine R-**Algebra** ist ein Ring A zusammen mit einem festen Ringhomomorphismus

$$\phi : R \to A,$$

wobei $Bild(\phi) \subseteq \text{Zentrum}(A)$ gilt. Es gilt also

$$\forall r \in R, a \in A : \qquad \phi(r)a = a\phi(r).$$

Man beachte, dass der Ring A nicht notwendig kommutativ sein muss. Mit vorangegangenem Beispiel sollte jedoch klar sein, dass vermöge der Abbildung

$$ra := \phi(r)a$$

eine jede R-Algebra A gleichzeitig ein R-Modul ist.

3 Untermoduln von Moduln

3.1 Grundlegendes zu Untermoduln

Bei Gruppen, Ringen, Körpern oder auch den Vektorräumen nehmen Unterräume eine bedeutende Position ein. Da ein Modul eine Verallgemeinerung vieler algebraischen Konstrukte darstellt, liegt eine aufgrund der Verwandtschaft zu anderen Strukturen entsprechende Definition eines „Untermoduls“ nahe.

Definition (Untermodul)
Es sei ${}_RM$ ein R-Links-Modul und $\cdot$ eine äußere Verknüpfung $R \times M \to M$. Eine nicht leere Menge $U \subseteq M$ heißt **Untermodul** von M, wenn gilt:

(U_1) U ist Untergruppe von M,

(U_2) $u \in U$ und $\alpha \in R \Rightarrow \alpha \cdot u \in U$

Für R-Rechtsmoduln verlangen wir anstatt (U_2) die Bedingung

$$u \in U \text{ und } \alpha \in R \Rightarrow u \cdot \alpha \in U.$$

Ansonsten stimmen die Definitionen wortlich überein.

Bemerkung 4
Die Bedingung (U_1) ist bekanntlich zum Untergruppenkriterium äquivalent, d.h. es gilt

$$(U_1) \Leftrightarrow (u, v \in U \Rightarrow u - v \in U),$$

wobei $U \neq \emptyset$ vorauszusetzen ist. Die Bedingung (U_2) schreibt man oft kürzer in der Form $R \cdot U \subseteq U$. Vergleichen Sie die Definition eines Untermodul mit der eines Ideals bzw. der eines Unter-Verktorraumes.

Beispiel

a) Ist $G = {}_{\mathbb{Z}}G$ eine abelsche Gruppe als $\mathbb{Z}$-Modul betrachtet, dann sind die Untermoduln hiervon genau die Untergruppen. Die Bedingung (U_1) ist offensichtlich erfüllt. (U_2) ist erfüllt, da die äußere Verknüpfung auch für jede Teilmenge von G als eine solche definiert ist und damit auch für jede Untergruppe gilt. Man sagt dann auch, dass die äußere Verknüpfung eine entsprechende für die Ungergruppe **induziert**, indem man den Definitionsbereich geeignet einschränkt.

b) Ist R ein Ring, dann sind die Untermoduln von ${}_RR$ (bzw. von R_R) genau die Linksideale (bzw. Rechtideale) von R. Ist R kommutativ dann sind Rechts- und Linksideale identisch, eine Unterscheidung also nicht mehr notwendig.

c) Ist K ein Körper und V ein unitärer K-Modul, also ein K-Vektorraum, dann sind die Untermoduln hiervon gerade die Untervektorräume von V. In diesem Fall kann man das Unterraum-Kriterium aus der linearen Algebra anwenden.

d) Ist M ein Modul über R, dann ist für jedes $m \in M$

$$Rm := \{\alpha \cdot m | \alpha \in R\}$$

ein Untermodul von ${}_RM$. Bedingung (U_1) folgt direkt aus den Eigenschaften der abelschen Gruppe M: Seien $s, r \in Rm$, d.h. es existieren $\alpha, \beta \in R$ mit $s = \alpha \cdot m$ bzw. $r = \beta \cdot m$. Wir müssen zeigen, dass $r - s \in Rm$ liegt, also dass $\alpha \cdot m - \beta \cdot m \in Rm$. Wendet man das Distributivgesetz an, so erhalten wir $(\alpha - \beta) \cdot m$ und da R ein Ring, muss $\alpha - \beta \in R$ und damit auch $r - s \in Rm$. Klar ist auch, dass mit $s = \alpha \cdot m$ auch $\beta \cdot s = \beta \cdot (\alpha \cdot m) = (\alpha\beta) \cdot m \in Rm$ liegt – man wende das Assoziativgesetz an. Das von $m \in M$ erzeugte Modul nennt man auch **zyklische Untermodul**.

e) Jeder Modul M enthält die Untermoduln $\{0\}$ und M. Diese Untermoduln nennen wir daher auch die **trivialen Untermoduln** von M.

Der Nullmodul $\{0\}$ wird häufig durch eine schlichte 0 notiert; abgesehen vom Abschnitt über exakte Sequenzen, werden wir jedoch stets das Nullmodul mit $\{0\}$ bezeichnen. Wie bei der äquivalenten Charakterisierung eines Moduls sind auch Ring-Homomorphismen bei der Profilfindung eines Untermoduls von entscheidender Bedeutung. Dies drücken wir in folgendem Lemma aus.

Lemma 3.1: *Es sei ${}_RM$ ein Modul über dem Ring R und U ein Untermodul von ${}_RM$, so dass*

$$\alpha \cdot x \in U \quad \text{für alle } \alpha \in R, x \in U.$$

Dann induziert die äußeren Verknüpfungen $R \times M \to M$ des R-Moduls ${}_RM$ eine entsprechende äußere Verknüpfung $R \times U \to U$, die U zu einem R-Untermodul macht.

Beweis. Man wende Lemma 2.1 auf die Restriktion der äußeren Verknüpfung auf U an und beachte, dass sich sämtliche Eigenschaften dieser Verknüpfung auf diese Einschränkung übertragen. □

3.2 Einfache, minimale und maximale Untermoduln

Dieser Teilabschnitt wird sich für all diejenigen als überaus nützlich erweisen, die sich mit weiterführender Modul- bzw. Ringtheorie beschäftigen werden. Insbesondere die Theorie über artinsche bzw. noethersche Ringe bzw. Moduln baut auf den nun folgenden Erkenntnissen auf.

Definition
Ein Modul ${}_RM =: M \neq 0$ heißt **einfach**, wenn für alle Untermoduln $U \leq M$ folgt, dass U entweder das Nullmodul 0 oder aber M selbst ist.

Ein Untermodul $U \leq M$, $U \neq 0$, heißt **minimaler** Untermodul von M, wenn für alle Untermoduln $U' \leq M$ von M mit $U' \subsetneq U$ folgt $U' = 0$.

Ein Untermodul $U \leq M$, $U \neq M$, heißt **maximaler** Untermodul von M, wenn für alle Untermoduln $U' \leq M$ von M mit $U \subsetneq U'$ folgt $U' = M$.

Ebenso spricht man von einfachen Ringen oder minimalen bzw. maximalen Idealen in Ringen. Ein einfacher Modul enthält nur die trivialen Untermoduln und es sei konstatiert, dass die *minimalen Untermoduln* genau die *einfachen Untermoduln* sind. Ist $U \leq M$ ein minimaler Untermodul von M, dann gibt es keinen echten Untermoduln von M „zwischen“ dem Nullmodul $\{0\}$ und U, es ist also U einfach. Entsprechend kann man ein einfaches Modul M auch als minimal auffassen.

Im Falle der Existenz sind die minimalen (= einfachen) bzw. die maximalen Untermoduln eines Moduls, offenbar minimale bzw. maximale Elemente in der *geordneten Menge* der nicht-trivialen Untermoduln mit der Inklusion als Ordnung. Diese recht einfache

Feststellung ist für Teile der Darstellungstheorie von großer Bedeutung und findet im folgenden Lemma Ausdruck.

Lemma 3.2: *Es sei* ${}_RM =: M \neq 0$ *ein R-Modul. Dann gilt die Äquivalenz*

$$M \text{ ist einfach} \quad \Leftrightarrow \quad \forall m \in M \setminus \{0\} : mR = M$$

Beweis. „⇒“: Da $m \neq 0$ ist $Rm \neq 0$. Es ist $1 \in R$, dann muss auch $m \cdot 1 = m \in Rm$, d.h. $M \subseteq Rm$, also $Rm = M$.
„⇐“: Sei $U \leq M$ ein Untermodul ungleich dem Nullmodul 0 und $u \in U$ mit $u \neq 0$. Dann ist $Ru = M$. Andererseits muss auch $Ru \leq U \leq M$ gelten, also $U = M$. □

Beispiel

a) $\mathbb{Z}$ als Ring (bzw. $\mathbb{Z}$ als $\mathbb{Z}$-Modul) enthält keine minimalen (=einfachen) Ideale (bzw. Untermoduln), denn ist $n\mathbb{Z} \neq \{0\}$, dann ist z.B. $2n\mathbb{Z}$ ein darin echt enthaltenes Ideal ungleich dem Nullideal $\{0\}$. Die maximalen Ideale von $\mathbb{Z}$ sind genau die Primideale $p\mathbb{Z}$, p eine Primzahl. Ein Beweis ergibt sich aus dem aus der (linearen) Algebra bekannten Zusammenhang

$$\forall m, n \in \mathbb{Z} :$$
$$m\mathbb{Z} \leq n\mathbb{Z} \quad \Leftrightarrow \quad n|m.$$

Hierbei notiert $n|m$ die ganzzahlige Division der Zahl m durch die Zahl n ohne Rest. Eine Primzahl p besitzt nur sich selbst und die Einheit 1 als Teiler, d.h. lediglich für $1|p$ erhalten wir einen echten Obermodul $1\mathbb{Z} = \mathbb{Z}$.

b) Das $\mathbb{Z}$-Modul ${}_{\mathbb{Z}}\mathbb{Q}$ besitzt weder minimale noch maximale Untermoduln. Das ${}_{\mathbb{Z}}\mathbb{Q}$ kein minimales Untermodul kann man analog zu a) nachweisen. Angenommen $U \leq M$ sei ein minimales Untermodul, dann können wir ein $u \in U$ mit $u \neq 0$ wählen. Sodann gilt folgende Inklusionskette

$$0 \subsetneq 2u\mathbb{Z} \subsetneq u\mathbb{Z} \subseteq U \subseteq Q.$$

Entscheindend ist nun, dass $2u\mathbb{Z}$ echt in $u\mathbb{Z}$ enthalten ist und das ergibt einen Widerspruch zur Minimalität von U! D.h. U kann kein minimaler Untermoduln sein.

Der Nachweis, dass $\mathbb{Q}_{\mathbb{Z}}$ keine maximalen Untermoduln besitzt skizzieren wir nur: Ist X ein beliebiges Erzeugendensystem, so können wir endlich viele Elemente weggelassen und die Restmenge ist wieder ein Erzeugendensystem von $\mathbb{Q}_{\mathbb{Z}}$. Daraus folgert man, dass X unendliche viele Elemente besitzen muss, denn ansonsten wäre $\emptyset$ ein Erzeugendensystem von $\mathbb{Q}_{\mathbb{Z}}$ und damit würde $\mathbb{Q}_{\mathbb{Z}} = \{0\}$ folgen ↯. Angenommen M wäre ein maximaler Modul und $q \in \mathbb{Q}, q \notin M$, dann ist

$$q\mathbb{Z} + M := \{qz + m |\ z \in \mathbb{Z}, m \in M\}.$$

Auch diese Menge ist ein Untermodul von $\mathbb{Q}_{\mathbb{Z}}$, da dieser M echt enthält folgt

$$q\mathbb{Z} + M = \mathbb{Q}.$$

Also wäre $M \cup \{q\}$ ein Erzeugendensystem von $\mathbb{Q}_{\mathbb{Z}}$ und dann auch M allein, waraus $M = \mathbb{Q}$ folgen würde $\lightning$.

c) In einem K-Vektorraum V sind genau die 1-dimensionalen Unterräume die minimalen (=einfachen) Unterräume. Diese können mit Elementen $v \in V \setminus \{0\}$ in der Form vK geschrieben werden. Ist V ein n-dimensionaler Vektorraum, dann sind genau die $(n-1)$-dimensionalen Unterräume die maximalen Unterräume.

d) Ist K ein Schiefkörper, dann ist sowohl ${}_KK$ einfach als auch K als Ring betrachtet. Ein Schiefkörper besitzt zu jedem Element ungleich 0 ein inverses. D.h. wir können zu $a \in K \setminus \{0\}$ ein $a' \in K$ finden, so dass $aa' = a'a = 1$. Deshalb muss dann $Ka = aK = K$ gelten, d.h. ein Schiefkörper besitzt lediglich die trivialen Ideale. D.h. in ${}_KK$ ist ${}_KK$ selbst minimales Untermodul und $\{0\}$ ist maximaler Untermodul.

e) Wir betrachten nun $M_{n,n}(K)$, den Ring der quadratischen $(n \times n)$-Matrizen mit Koeffizienten aus einem Schiefkörper K. Es ist $M_{n,n}(K)$ als Ring einfach, nicht jedoch als $M_{n,n}(K)$-Modul.

Die nun noch folgenden Lemmata sind sehr nützlich bei der Beweisführung vieler Sätze aus der Modul- und Ringtheorie.

Lemma 3.3: *Es sei $U \lneq M$ ein echter Untermodul. Dann sind äquivalent:*

$$U \text{ ist maximaler Untermodul von } M \quad \Leftrightarrow \quad \forall x \in M, x \notin U \text{ gilt:} \quad xR + U = M.$$

Beweis. „$\Rightarrow$“: Da $x \notin U$ ist $xR+U$ ein echter Obermodul von U. Gemäß Voraussetzung ist U ein maximaler Untermodul von M, deshalb muss $xR + U = M$ folgen.

„$\Leftarrow$“: Sei $U \lneq U' \leq M$ und sei $x \in U', x \notin U$. Also ist $M = (xR + U) \leq (U' + U) \leq U' \leq M$, also muss $U' = M$ sein. □

3.3 Zyklizität, Erzeugendensysteme und Durchschnitt von Moduln

Das letzte Beispiel legt nahe, ebenso wie bei Gruppen, die Eigenschaft der Zyklizität auch für Moduln einzuführen.

Definition
Es sei ${}_RM$ ein Mdoul über dem Ring R. Ein Untermodul U von M heißt **zyklisch** oder **monogen**, wenn es ein $m \in M$ gibt mit $U = Rm$.

Betrachten wir einen Ring ohne Einselement, so muss m nicht notwendig in Rm liegen.

Es sei M ein beliebiger Modul. Für die folgenden Betrachtungen ist es zweckmäßig, Systeme von Untermoduln von M mit Hilfe von Indexmengen zu beschreiben: Es sei I stets eine nicht-leere (endliche oder unendliche) Menge, die wir **Indexmenge** nennen werden. Jedem „Index“ $i \in I$ sei eindeutig ein Untermodul U_i von M zugeordnet. Das aus Untermoduln bestehende System $\{U_i | i \in I\}$ bezeichnen wir als **Familie von Untermoduln**. Analog könnte man auch Familien von Vektorräumen, Ringen oder Gruppen definieren.

Lemma 3.4: *Ist* ${}_RM =: M$ *ein Modul über dem Ring* R *und* $\{U_i | i \in I\}$ *eine Familie von Untermoduln von* M*, dann ist auch der Durchschnitt* $\bigcap_{i\in I} U_i$ *ein Untermodul von* M*.*

Beweis. Seien $x, y \in \bigcap_{i\in I} U_i$, d.h. $x, y \in U_i$ für alle $i \in I$. Dann liegt auch $x - y \in U_i$ für alle $i \in I$ in jedem Untermoduln U_i (vgl. Bemerkung 4). Damit liegt auch $x-y \in \bigcap_{i\in I} U_i$. Der zweite Teil des Beweises verläuft analog: Es seien $\alpha \in R$ und $x \in \bigcap_{i\in I} U_i$. Gemäß Definition des Durchschnitts ist damit $x \in U_i$ für alle $i \in I$ gültig. Da die $U_i, i \in I$ allesamt Untermoduln sind, folgt $\alpha \cdot x \in U_i$ für alle $i \in I$ und damit $\alpha \cdot x \in \bigcap_{i\in I} U_i$. □

Ab nun betrachten wir *Erzeugendesysteme* eines Modul ${}_RM =: M$. Es sei $A \subseteq M$ eine beliebige Teilmenge. Um Aussagen über eine gegebene Teilmenge $A \subseteq M$ zu treffen, die durch Moduleigenschaften bedingt ist, so ist es sicher sinnvoll, den Elementen keine Aufmerksamkeit zu schenken die mit A oder den Moduleigenschaften nichts zu tun haben. Wir suchen also das *kleinste* Untermodul von M, welches A enthält; die Existenz eines derartigen Untermodul, folgt aus dem eben bewiesenen Lemma 3.4.

Definition
Es sei ${}_RM =: M$ ein Modul über dem Ring R und $A \subseteq M$. Der Untermodul

$$ {}_R\langle A\rangle := \bigcap \{U | U \text{ ist Untermodul von } M \textit{ mit } A \subseteq U\} $$

heißt der **von** A **erzeugte Untermodul** zu M. Ist ${}_R\langle A\rangle = M$, dann heißt M von ${}_R\langle A\rangle$ erzeugt und A ein **Erzeugendensystem** von M.

Der Modul M heißt **endlich erzeugt**, wenn es ein endliches Erzeugendensystem $\{a_1, \ldots, a_n\} \subseteq M$ gibt. In diesem Fall schreiben wir $M = {}_R\langle a_1, \ldots, a_n\rangle$. Abkürzend werden wir anstatt ${}_R\langle . \rangle$ nur kurz $\langle . \rangle$ schreiben.

Es sind $\langle \emptyset \rangle = \{0\}$ und $\langle M \rangle = M$; jeder endliche Modul ist natürlich endlich erzeugt. Folgende Eigenschaften ersieht man sofort aus der Definition von $\langle A \rangle$:

(E_1) $A \subseteq \langle A \rangle$,

(E_2) $\langle A \rangle \subseteq U$ für jeden Untermodul U mit $A \subseteq U$.

(E_1) gilt, da alle Untermoduln U über die der Druchschnitt gebildet wird die Menge A enthalten müssen. Der Druchschnitt von Untermoduln ist selbst ein Untermodul, deshalb können die Untermoduln U über die der Durchschnitt gebildet wird nur Obermoduln

sein, d.h. es gilt (E_2).

Im Sinne (E_1) und (E_2) sagen wir, dass $\langle A\rangle$ der **kleinste Untermodul** von M ist, der A enthält. Ist A bereits ein Untermodul, dann gilt (E_2) auch für $U = A$, d.h. $U = \langle U\rangle$.

Für die praktische Bestimmung von $\langle A\rangle$ ist die Definition ungeeignet, da es für gewöhnlich große Mühe bereitet sämtliche Untermoduln von M aufzuspüren. Mit einigen weiteren Überlegungen werden wir jedoch ein handliches Kriterium zu diesem Zwecke entwickeln:

Jeder Untermodul U der die Menge A enthält, muss auch $A+A$ und $A^- := \{-x|x \in A\}$ und damit alle endlichen Summen enthalten, die man mit den Elemente aus $A \cup A^-$ bilden kann. Ferner muss der Untermodul U der A enthält, bezüglich der äußeren Verknüpfung abgeschlossen sein, d.h. für alle $\alpha \in R$ und $x \in A \cup A^-$ muss auch $\alpha \cdot x$ in U enthalten sein. Betrachten wir daher die Menge

$$\widetilde{A} := \{\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \ldots + \alpha_n \cdot x_n | x_i \in A \cup A^-, n \in \mathbb{N}, \alpha_i \in R\}. \qquad \text{(Erz)}$$

$\widetilde{A}$ besteht also aus allen endlichen Linearkombinationen $\sum \alpha_i x_i$ mit $\alpha_i \in R$ und $x_i \in A$. Nach dem eben Gesagten gilt $A \subseteq \widetilde{A} \subseteq \langle A\rangle$, denn schließlich ist mit $x, y \in A$ auch $x - y$ bzw. $y - x \in \widetilde{A}$ sowie $\alpha \cdot x \in \widetilde{A}$ enthalten. Damit ist $\widetilde{A}$ ein *Untermodul*, der A enthält.

Da $\langle A\rangle$ aber – gemäß Definition – der kleinste Untermodul ist, der die Menge A enthält, gilt auch $\langle A\rangle \subseteq \widetilde{A}$ und mit (E_{ii}) von oben ergibt sich damit die Identität $\langle A\rangle = \widetilde{A}$.

Manche Autoren definieren $\widetilde{A}$ als der durch A *erzeugte Untermodul* von M und zeigen im Anschluss, dass dieser zugleich der kleinste Modul von M ist, der A enthält.

Aus (Erz) folgt direkt, dass eine Teilmenge $X \subseteq M$ eines R-Moduls M genau dann ein Erzeugendensystem ist, wenn es zu jedem $m \in M$ eine endliche Teilmenge $X_0 \subseteq X$ mit $|X_0| = n \in \mathbb{N}$ gibt, so dass

$$m = \sum_{i=1}^{n} r_i x_i$$

gilt. Dabei hängt $n \in \mathbb{N}$ im Allgemeinen von dem Modulelement m ab und ist mitnichten fest. Ebenso ist die Summendarstellung im Allgemeinen nicht eindeutig, d.h. die Koeffizienten $x_j \in X_0$ und $r_j \in R$ eines Summanden $x_j r_j$ sind nicht eindeutig bestimmbar. Im endlichen Fall, d.h. $X = \{x_1, \ldots, x_t\}$ kann man zwar jedes Element $m \in M$ durch

$$m = \sum_{i=1}^{t} r_i x_i$$

mit festem $t \in \mathbb{N}$ schreiben, da fehlende Summanden $x_j r_j$ einfach durch $x_j 0$ aufgefüllt werden können, doch die Summendarstellung ist auch in diesem speziellen Fall nicht eindeutig. Die Eindeutigkeit ist erst dann erfüllt, wenn die Menge zusätzlich linear unabhängig ist, doch dazu später mehr.

Lemma 3.5: *Es sei ${}_RM =: M$ ein Modul über dem Ring R und $\{U_i | i \in I\}$ eine Familie von Untermoduln von M. Dann gelten:*

i) Der Durchschnitt $\bigcap_{\substack{i\in I \\ A\subset U_i}} U_i$ bezüglich der Ordnung „$\subseteq$“ der kleinste Untermodul von M, welcher die Teilmenge $A \subseteq M$ enthält.

ii) Der Durchschnitt $\bigcap_{i\in I} U_i$ ist der bezüglich der Ordnung $\subseteq$ größte Untermodul von M, der in allen U_i, $i \in I$, enthalten ist.

Beweis. Ad i): Den Beweis haben wir bereits weiter oben erbracht.

Ad ii): Es sei U_{max} der größte Untermodul von M, der in allen U_i, $i \in I$, enthalten ist. Dann muss $U_{max} \supseteq \bigcap_{i\in I} U_i$ gelten, da auch der Durchschnitt ein Untermodul von M (vgl. Lemma 3.3) und U_{max} das größte deratige Untermodul ist. Andererseits ist, gemäß Definition, U_{max} in allen U_i enthalten, deshalb muss $U_{max} \subseteq \bigcap_{i\in I} U_i$ gelten. Insgesamt folgt $U_{max} = \bigcap_{i\in I} U_i$. □

3.4 Summe und Vereinigung von Untermoduln

Nachdem wir zu Beginn des letzten Abschnitts bereits festgestellt haben, dass der Durchschnitt einer Familie von Untermoduln stets wieder ein Untermodul ist, werden wir nun die Vereinigung und die Summe von Untermoduln näher untersuchen. Aus der linearen Algebra wissen wir, dass die Vereinigung von Untervektorräumen im Allgemeinen nicht wieder ein Unterraum ist:

Beispiel

Wir untersuchen die Vereinigung der Untervektorräume $U_1 := \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} | x \in \mathbb{R} \right\}$ und $U_2 := \left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} | y \in \mathbb{R} \right\}$ des Vektorraums $\mathbb{R}^2$. U_1 entspricht der Abzisse und U_2 der Ordinate und die Vereinigung $X := U_1 \cup U_2 = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \end{pmatrix} | x, y \in \mathbb{R} \right\}$ ist nicht abgeschlossen gegenüber der Vektoraddition. Sind bpsw. $(1,0)^T, (0,1)^T \in X$, dann ist $(1,0)^T + (0,1)^T = (1,1)^T$ nicht in X enthalten.

Da K-Vektorräume gerade K-Moduln sind, ist auch die Vereinigung von Moduln im Allgemeinen nicht wieder ein Modul. Jedoch wird von dieser Vereinigungsmenge ein Untermodul aufgespannt, den man auch die **Summe** der Untermoduln des Systems $\{U_i | \ i \in I\}$ nennt und durch $\sum_{i\in I} U_i$ notiert.

Lemma 3.6: *Es seien $M_R =: M$ ein R-Rechtsmodul und $\Lambda := \{U_i | \ i \in I\}$ eine Familie von Untermoduln $U_i \leq M$. Dann gilt*

$$\left\langle \bigcup_{i\in I} U_i \right\rangle = \begin{cases} \{\sum_{i\in I} u_i | \ u_i \in U_i \text{ und } I_0 \subseteq I \text{ endlich,}\} & \text{falls } \Lambda \neq \emptyset \\ 0, \text{ falls } \Lambda = \emptyset \end{cases}$$

d.h. im Falle $\Lambda \neq \emptyset$ ist $\left\langle \bigcup_{i\in I} U_i \right\rangle$ die Menge aller endlichen Summen $\sum u_i$ mit $u_i \in U_i$.

Beweis. Wie wir bereits festgestellt haben, kann man das von einer nicht leeren Menge X erzeugte Untermodul $\langle X \rangle$ durch die Menge aller endlichen Linearkombinationen charakterisieren (vgl. (Erz)). Deshalb ist $\left\langle \bigcup_{i\in I} U_i \right\rangle$ im Falle $I \neq \emptyset$ gleich der Menge aller endlichen Summen

$$\sum_{j=1}^{n} u_j r_j \qquad \text{mit } u_j \in \left\langle \bigcup_{i\in I} U_i \right\rangle, r_i \in R.$$

Die Bilder des äußere Produktes $M \times R \to M$ liegen sämtlich in M, d.h. wir können die Summanden $u_j r_j$, die in einem festen $U_i, i \in I$ liegen, durch ein Modulelement ausdrücken:

$$\sum_{j=1}^{n} u_j r_j = \sum_{i\in I'} u_i',$$

also gilt $\left\langle \bigcup_{i\in I} U_i \right\rangle \subseteq \left\{ \sum_{i\in I'} u_i' |\ a_i' \in A_i,\ I' \subseteq I \text{ endlich} \right\}$. Die umgekehrte Inklusion ist aufgrund der Definition von $\langle . \rangle$ klar. □

Der hier entwickelte Begriff der Summe von Untermoduln ist für alles Weitere in der Modultheorie von großer Bedeutung.

Definition
Seien M_R ein R-Rechtsmodul und $\Lambda = \{U_i |\ i \in I\}$ eine Familie von Untermoduln mit $U_i \leq M$. Dann heißt

$$\sum_{i\in I} U_i := \left\langle \bigcup_{i\in I} U_i \right\rangle,$$

die **Summe der Untermoduln** $\{U_i |\ i \in I\}$.

Jedes Element aus $\sum_{j\in J} U_j$ kann in der Form

$$\sum_{j=1}^{n} u_j \qquad \text{mit } u_j \in U_j,\ n \in \mathbb{N}$$

geschrieben werden, da die Summe von Untermoduln aus allen *endlichen* Summen besteht und eventuell fehlende Summanden u_j gleich Null gesetzt werden können. Die Darstellung $\sum_{j\in J} u_j$ muss jedoch nicht eindeutig sein, da die Untermoduln auch gemeinsame Elemente besitzen können. In Abschnitt 5 werden wir den Spezialfall der Summe von Untermoduln kennen, in welchem die Darstellung eindeutig ist.

3.5 Endlich erzeugte und endlich koerzeugte Moduln

Auch dieser Abschnitt dient insbesondere als Vorbereitung für die so genannten noetherschen bzw. artinschen Moduln. Ein Modul ist nämlich genau dann endlich erzeugt, wenn

er noethersch ist und ein Faktormodul ist genau dann endlich koerzeugt, wenn er artinsch ist. Noethersche und artinsche Moduln sind für die weiterführende Theorie der Moduln und der Darstellungstheorie von großer Bedeutung. In diesem Abschnitt beschränken wir uns jedoch auf den Zusammenhang zwischen endlich erzeugten bzw. endlich koerzeugten Moduln und der Summe bzw. dem Durchschnitt von Moduln.

Wie wir bereits wissen heißt ein R-Modul M endlich erzeugt, wenn es ein endliches Erzeugendensystem $\{m_1, \ldots, m_n\} \subseteq M$ gibt. Sei also $\{m_1, \ldots, m_n\}$ ein Erzeugendensystem eines R-Linksmoduls M, dann gilt $\langle m_1, \ldots, m_n \rangle = M$. Das bedeutet, dass jedes Modulelement $m \in M$ als endliche Linearkombination $\sum_{i=1}^{n} r_i m_i$ mit $r_i \in R$ geschrieben werden kann. Hieraus folgt direkt die Identität

$$M = Rm_1 + \ldots + Rm_n.$$

Diese einfachen Erkenntnisse werden wir in diesem Abschnitt für einen Beweis benötigen. Zunächst wenden wir uns jedoch der Charakterisierung maximaler Untermoduln zu.

Lemma 3.7: *Seien M ein R-Modul und $U \lneq M$ ein Untermodul. Dann gilt:*
Maximaler Untermodul U von M $\quad\Leftrightarrow\quad$ $m \notin U \;\Rightarrow\; M = mR + U$.

Beweis. „$\Rightarrow$“: Seien $U \leq M$ ein maximaler Untermodul und $m \notin U$, dann ist U ein echter Untermodul zu $mR + U$. Da U maximal ist, muss $mR + U = M$ gelten.

„$\Leftarrow$“: Nun seien $U \lneq U' \leq M$ und $m \in U'$ jedoch $m \notin U$. Nach Voraussetzungen gilt dann $M = mR + U$ und damit $mR + A \leq U + U' \leq U' \leq M$, d.h. es muss $U' = M$ gelten. Damit ist U ein maximaler Untermodul von M. □

Lemma 3.8: *Ist der R-Modul M endlich erzeugt, dann ist jeder echte Untermodul $U \lneq M$ in einem maximalen Untermodul von M enthalten.*

Beweis. Es seien $\{x_1, \ldots, x_n\}$ ein Erzeugendensystem von M und $U \lneq M$ ein echter Untermodul. Dann ist die Menge

$$\mathcal{M} := \{U' |\; U \leq U' \lneq M\}$$

wegen $U \in \mathcal{M}$ nicht leer und durch „$\subseteq$“ geordnet. Um das Zornsche Lemma anwenden zu können, muss zunächst gezeigt werden, dass jede total geordnete Teilmenge $\Lambda \subseteq \mathcal{M}$ eine obere Schranke in $\mathcal{M}$ besitzt. Dazu sei

$$A := \bigcup_{U' \in \Lambda} U'$$

die Vereinigungsmenge der Moduln aus Λ. Da Λ total geordnet ist gilt $U \subseteq A$. Angenommen es würde $A = M$ gelten, dann würde $\{x_1, \ldots, x_n\} \subseteq A$ folgen. Deshalb müsste es ein $U' \in \Lambda$ geben mit $\{x_1, \ldots, x_n\} \subseteq U'$, d.h. $U' = M$ ↯. Es muss also $A \in \mathcal{M}$ gelten. Nun können wir das Lemma von Zorn anwenden, womit die Existenz eines maximalen Elements $U_{max} \in \mathcal{M}$ folgt. Ferner ist U im maximalen Untermodul U_{max} enthalten. □

Jeder Modul M besitzt $U := \{0\}$ als echten Untermodul und nach dem Lemma muss dieser dann in einem maximalen Untermodul enthalten sein. Damit haben wir gezeigt:

Folgerung 3.9: *Jeder endlich erzeugte R-Modul $M \neq \{0\}$ besitzt einen maximalen Untermodul.*

Beispiel
Die abelsche Gruppe $\mathbb{Z}$ betrachtet als $\mathbb{Z}$-Modul wird durch die Einheit 1 erzeugt. Alle Untermoduln besitzen die Form $n\mathbb{Z}$ mit $n \in \mathbb{Z}$ und es gilt der schon benutze Zusammenhang

$$\forall m, n \in \mathbb{Z}:$$
$$m\mathbb{Z} \leq n\mathbb{Z} \;\Leftrightarrow\; n|m.$$

Untersuchen wir also konkret $30\mathbb{Z}$ als Untermodul von $\mathbb{Z}$, so ist dieser Untermodul in einem maximalen Untermodul von $\mathbb{Z}$ enthalten. In $\mathbb{Z}$ ist ein Ideal (bzw. Untermodul) genau dann maximal, wenn es von der Form $p\mathbb{Z}$ mit p Primzahl ist. Bilden wir, wie im konstruktiven Beweis, die Menge $\mathcal{M} := \{U|\ 30\mathbb{Z} \leq U \lneq \mathbb{Z}\}$, so besteht diese Menge gerade aus allen $m\mathbb{Z}$, wobei m die Zahl 30 teilt. Da jede ganze Zahl eine kanonische Primfaktorzerlegung besitzt, sind auf jeden Fall maximale Untermoduln in $\mathcal{M}$ enthalten. Die Ordnungen aller anderen nicht maximalen Untermoduln sind Potenzen der Primzahlteiler von 30, d.h. jeder Untermodul aus $\mathcal{M}$ ist tatsächlich in einem maximalen Untermodul enthalten. So ist $30\mathbb{Z}$ z.B. in $2\mathbb{Z}$ oder $5\mathbb{Z}$ enthalten.

SATZ 3.10: *Sei ${}_RM =: M$ ein Modul. Dann gilt:*
M ist endlich erzeugt $\Leftrightarrow$ $\forall$ Menge $\{U_i \leq M|\ i \in I\}$ mit $\sum_{i\in I} U_i = M$ existiert eine endliche Teilmenge $I_0 \subseteq I$, so dass

$$\sum_{i\in I_0} U_i = M$$

gilt.

Beweis. „$\Rightarrow$“: Es sei $\{m_1, \ldots, m_n\}$ ein Erzeugendensystem des R-Moduls M, d.h. es gilt $M = m_1R + \ldots + m_nR$. Weiter seien eine Indexmenge I und eine Menge von Untermoduln $\{U_i \leq M|\ i \in I\}$ gegeben, so dass die Identität $\sum_{i\in I} U_i = M$ erfüllt ist. Ein jedes Modulelement $m \in M$ kann in einem endlich erzeugten Modul durch eine endliche Linearkombination dargestellt werden, insbesondere kann man auch die erzeugenden Elemente $m_j \in \{m_1, \ldots, m_n\}$ als endliche Linearkombination schreiben. Folglich existiert eine Teilmenge $I_0 \subseteq I$, so dass

$$m_1, \ldots, m_n \in \sum_{i\in I_0} U_i.$$

Und damit

$$M = m_1R + \ldots + m_nR \leq \sum_{i\in I_0} U_i \leq M,$$

es muss also $\sum_{i\in I_0} U_i = M$ gelten.

„$\Leftarrow$“: Es sei $\{Rm|\ m \in M\}$ die Menge aller zyklischen Untermoduln und da $1 \in R$ gilt, folgt $\sum_{m\in M} Rm = M$. D.h. es existiert eine endliche Teilmenge $M_0 = \{m_1, \ldots, m_n\} \subseteq M$, so dass $\sum_{m\in M_0} Rm = M$ gilt. □

Nun definieren wir den zu „endlich erzeugt“ dualen Begriff.

Definition
Der Modul M über dem Ring R heißt **endlich koerzeugt** genau dann, wenn es zu jeder Menge $\{U_i \leq M|\ i \in I\}$ mit $\bigcap_{i\in I} U_i = \{0\}$ eine endliche Teilmenge $I_0 \subseteq I$ gibt mit $\bigcap_{i\in I_0} U_i = \{0\}$.

Die Ähnlichkeit der Definition zu obigem Satz ist unverkennbar. Beispiele werden den neuen Begriff veranschaulichen.

Beispiel

a) Es sei $\mathbb{P}$ die unendlich abzählbare Menge aller Primzahlen. Der Modul $\mathbb{Z}_\mathbb{Z}$ ist nicht endlich koerzeugt, da

$$\bigcap_{p\in\mathbb{P}} p\mathbb{Z} = \{0\}$$

aber für nur endlich viele Primzahlen $p_1, \ldots, p_n$

$$\bigcap_{i=1}^{n} p_i\mathbb{Z} = kgV(p_1, \ldots, p_n)\mathbb{Z} = (p_1 \ldots p_n)\mathbb{Z} \neq \{0\}$$

gilt.

b) Ein Vektorraum V über dem Körper K ist dann und nur dann endlich koerzeugt, wenn er endliche Dimension hat. Weiter ist ein Vektorraum endlicher Dimension ist gleichzeitig auch endlich erzeugbar.

3.6 Faktor-Moduln von M nach U

In analoger Art und Weise, wie wir dies bei Gruppen und Ringen gehalten haben, untersuchen wir nun sog. Faktormoduln. Dabei ähnelt die Definition von Faktormodulen insbesondere der von Faktorräumen. Auch bei diesem Konstrukt werden wir die Bedeutung der Existenz bestimmter Ringhomomorphismen versuchen zu unterstreichen.

Definition (Faktor-Moduln)
Es sei U ein Untermodul von ${}_RM$, dann wird auf der uns bekannten Faktorgruppe M/U eine skalare Multiplikation $R \times M/U \to M/U$ durch

$$\alpha(x + U) := (\alpha \cdot x) + U$$

definiert. Wegen $\alpha U \subseteq U$ ist dies wohldefiniert, und somit ist M/U ebenfalls ein R-Linksmodul, der **Faktormodul von** M **nach** U (oder *Restklassenmodul* bzw. *Modulquotient von* M). In M/U haben wir also die Moduloperationen

$$(x+U)+(y+U) := (x+y)+U$$
$$\alpha(x+U) := (\alpha \cdot x)+U.$$

Beispiel

a) Wie wir wissen ist $(\mathbb{Z},+,\cdot)$ ein Ring, d.h. insbesondere, dass $(\mathbb{Z},+)$ eine abelsche Gruppe ist. D.h. wir können $\mathbb{Z}$ als Modul über sich selbst auffassen. Den Untermoduln entsprechen dann den Untergruppen von $\mathbb{Z}$, die bekanntlich von der Form $n\mathbb{Z} = \{nz | z \in \mathbb{Z}, n \geq 0\}$ sind. Nun betrachten wir die Faktorgruppe $\mathbb{Z}/n\mathbb{Z} = \{x+n\mathbb{Z} | x \in \mathbb{Z}\}$, also die Menge aller Restklassen $\overline{x} := r+\mathbb{Z} = \{r+nz | 0 \leq r < n, z \in \mathbb{Z}\}$. Als äußere Verknüpfung setzen wir für beliebige $x, y \in \mathbb{Z}$

$$\underbrace{x}_{\text{Ringelement}} \cdot \underbrace{(y+n\mathbb{Z})}_{\text{Modulelement}} := (xy)+n\mathbb{Z},$$

d.h. in diesem Fall entspricht die äußere Verknüpfung $\cdot$ gerade der Multiplikation in Restklassen-Faktorringen und die äußere Verknüpfung ist eigentlich eine innere. Die Addition der Nebenklassen ist auch klar,

$$x+(y+n\mathbb{Z}) := (x+y)+n\mathbb{Z}.$$

b) Es ist die Menge $G := (\mathbb{C}^* = \mathbb{C} \setminus \{0\}, \cdot)$ eine abelsche Gruppe und $U := \{\varepsilon_n \in \mathbb{C} \mid \varepsilon_n := \exp(\frac{2\pi k}{n}), k = 0, 1, \ldots, n-1\}$ zusammen mit der Multiplikation von komplexen Zahlen eine abelsche Untergruppe von G. Diese Untergruppe von G nennt man auch die Gruppe der komplexen Einheitswurzeln [1]. Wie im Abschnitt 2.2 gezeigt wurde ist G ein Links-Modul über dem Endomorphismenring R. Es ist U ein Untermoduln von G, da für $z \in U$ die Gleichung $z^n = 1$ gilt und damit für $\phi \in End(G)$ entsprechend $\phi(z^n) = \phi(1) = \phi(z)^n = 1$ gilt.

Es sei $R := End(G)$ der Endomorphismen-Ring von G. Die Menge aller Endomorphismen einer abelschen Gruppe bildet zusammen mit den inneren Ringverknüpfungen $f+g$ und $f \circ g$, definiert durch

$$(f+g)(x) := f(x)+g(x)\ \forall x \in \mathbb{C}$$
$$(f \circ g)(x) := f(g(x))\ \forall x \in \mathbb{C},$$

einen algebraischen Ring. Die Faktorgruppe G/U besitzt bekanntlich die (multiplikative) Gestalt

$$G/U = \{zU \mid z \in \mathbb{C}^*\},$$

[1] Das neutrale Element dieser Gruppe ist $1 = \exp(\frac{2 \cdot 0 \cdot \pi \cdot i}{n})$. Wie wir wissen sind die komplexen n-ten Einheitswurzeln gerade komplexe Lösungen der Gleichung $z^n = 1$. Sind u, v Lösungen, so auch $u^{-1} = \frac{1}{u}$ und $u \cdot v$. Ersteres begründet sich durch die Gleichung $(u^{-1})^n = \frac{1^n}{u^n} = \frac{1}{u^n} = 1$ und letzteres da $(uv)^n = u^n v^n = 1 \cdot 1 = 1$ gilt. Damit sind die Gruppen-Axiome erfüllt und da die Gruppe M zyklisch ist, ist M abelsch.

wobei $zU := \{z \cdot u \quad | \quad u \in U\}$ die Nebenklassen repräsentieren. Die Faktorgruppe G/U erweitern wir nun zu einem Faktormodul durch die äußere Verknüpfung $End(\mathbb{C}^*) \times G/U \to G/U$ definiert durch

$$\phi \bullet (z \cdot U) := \underbrace{\phi(z)}_{\in \mathbb{C}^*} U \qquad \forall \phi \in End(\mathbb{C}^*), z \in \mathbb{C}^*.$$

In G/U haben wir also die Moduloperationen

$$\begin{aligned}(z_1 U) + (z_2 U) &:= (z_1 + z_2)U \qquad \forall z_1, z_2 \in \mathbb{C}^*, \\ \phi \bullet (z \cdot U) &:= \phi(z)U \qquad \forall \phi \in End(G), z \in \mathbb{C}^*.\end{aligned}$$

Aufgrund der Eigenschaften der Abbildungen $\phi : \mathbb{C}^* \to \mathbb{C}^* \in End(\mathbb{C}^*)$ sind diese Verknüpfungen wohldefiniert.

Wie wir in den Beispielen gesehen haben, kann man, aus einer Faktorgruppe zusammen mit der äußeren Verknüpfung des zu Grunde gelegten Moduls, in natürlicher Weise ein Faktor-Modul erzeugen. Dies drückt auch folgendes Lemma aus.

Lemma 3.11: *Sei U ein Untermodul des R-Moduls M. Die Faktorgruppe M/U hat als Elemente bekanntlich die Restklassen*

$$x + U = \{x + u | u \in U\}, \qquad x \in M.$$

Die äußere Verknüpfung $R \times M \to M$ des R-Moduls M induziert eine entsprechende Verknüpfung

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

die M/U zu einem R-Faktormodul macht.

Beweis. Wir verwenden die surjektive und aus der klassischen Algebra wohlbekannte projektive Abbildung

$$\begin{aligned} \pi : M &\to M/U \\ x &\mapsto x + U. \end{aligned}$$

Zu zeigen ist, dass die Zuordnung

$$(\alpha, \pi(x)) \mapsto \pi(\alpha * x)$$

eine äußere Verknüpfung $R \times M/U$ definiert, die M/U zu einem Modul macht.

Damit die Zuordnung überhaupt eindeutig definiert ist, muss man sich zunächst davon überzeugen, dass $\pi(\alpha * x)$ nicht von (einem Repräsentanten) x, sondern nur von $\pi(x)$ (der Nebenklasse) abhängt. Sei also $\pi(x) = \pi(y)$, dann ist bekanntlich $x - y \in U$, da $\pi(x) = \pi(y) \Leftrightarrow x \equiv y(U) \Leftrightarrow x - y \equiv 0(U)$. Es folgt $\alpha * x - \alpha * y = \alpha * (x - y) \in U$, weil U ein Untermodul ist, also $\pi(\alpha * x) = \pi(\alpha * y)$ wie gewünscht. Wir haben also damit

nachgewiesen, dass diese Zuordnung wohldefiniert ist (Wohldefiniertheit).

Um zu zeigen, dass M/U mit dieser äußeren Verknüpfung ein Modul ist, bestätigen wir die Eigenschaften (M_1) bis (M_4). Wir beginnen bei (M_1):

$$\begin{aligned}
\alpha * (\pi(x) + \pi(y)) &= \alpha * [\pi(x+y)] && \text{(nach Def. der Addition in } M/U) \\
&= \pi(\alpha * (x+y)) && \text{(nach Def. der äuß. Verk. in } M/U) \\
&= \pi(\alpha * x + \alpha * y)) && \text{(wg. } (M_1) \text{ in } M) \\
&= \pi(\alpha * x) + \pi(\alpha * y)) && \text{(da } \pi \text{ Homomorphismus)} \\
&= \alpha * \pi(x) + \alpha * \pi(y) && \text{(da } \pi \text{ Homomorphismus)}
\end{aligned}$$

Ausgehend von der Gleichung (M_1) in M wird auf beiden Seiten π angewendet, und die Definition der Verknüpfungen werden eingesetzt. Ebenso verfährt man bei (M_2) bis (M_4). □

3.7 Untermoduln mit Idealen konstruieren

Ist $\mathfrak{a}$ ein Untermodul von ${}_RR$, also ein Linksideal von R, dann kann man das Faktor-Modul $R/\mathfrak{a}$ zwar noch nicht wieder (kanonisch) zu einem Ring machen, denn dazu müsste $\mathfrak{a}$ ein Ideal sein (es mangelt an der Kommutativität); nach der vorhergehenden Konstruktion des Faktor-Moduls wird $R/\mathfrak{a}$ jedoch vermöge $\alpha \bullet (\beta + \mathfrak{a}) = (\alpha\beta) + \mathfrak{a}$ zu einem R-Links-Modul.

Definition
Es sei $\mathfrak{a}$ ein Linksideal von R und $M := {}_RM$ ein R-Links-Modul, dann definieren wir das Produkt $\mathfrak{a}M$ durch

$$\mathfrak{a}M := \langle \{\alpha x |\ \alpha \in \mathfrak{a}, x \in M\} \rangle .$$

Die Menge $\mathfrak{a}M$ ist ein Untermoduln von M. Es gelten die Rechenregeln

$$\begin{aligned}
\mathfrak{a}(\mathfrak{b}M) &= (\mathfrak{a}\mathfrak{b})M \\
(\mathfrak{a}\mathfrak{b})M &= \mathfrak{a}M + \mathfrak{b}M \\
\mathfrak{a}(U + U') &= \mathfrak{a}U + \mathfrak{a}U'
\end{aligned}$$

für Linksideale $\mathfrak{a}, \mathfrak{b}$ von R und Untermoduln U, U' von M.

Beweis. $\mathfrak{a}(\mathfrak{b}M)$ wird erzeugt von den Elementen der Form

$$a \sum b_i x_i \quad \text{mit } a \in \mathfrak{a}, b_i \in \mathfrak{b}, x_i \in M,$$

also von den Elementen der Form abx, $a \in \mathfrak{a}, b \in \mathfrak{b}, x \in M$. Der Untermodul $(\mathfrak{a}\mathfrak{b})M$ wird erzeugt von den Elemeneten $(\sum a_i b_i)x$, also auch von abx mit $a \in \mathfrak{a}, b \in \mathfrak{b}, x \in M$. Also ist

$$\mathfrak{a}(\mathfrak{b}M) = \langle \{abx |\quad a \in \mathfrak{a}, b \in \mathfrak{b}, x \in M, \} \rangle = (\mathfrak{a}\mathfrak{b})M.$$

Ähnlich gilt

$$\begin{aligned}(\mathfrak{a}+\mathfrak{b})M &= \langle\{(a+b)x| \quad a\in\mathfrak{a}, b\in\mathfrak{b}, x\in M,\}\rangle\\ &= \langle\{ax| \quad a\in\mathfrak{a}, x\in M,\}\rangle \cup \langle\{by| \quad b\in\mathfrak{b}, y\in M,\}\rangle\\ &= \mathfrak{a}M+\mathfrak{b}M,\\ \mathfrak{a}(U+U') &= \langle\{a(x+y)| \quad a\in\mathfrak{a}, x\in U, y\in U',\}\rangle\\ &= \langle\{ax| \quad a\in\mathfrak{a}, x\in U\}\rangle \cup \langle\{ay| \quad a\in\mathfrak{a}, y\in U'\}\rangle\\ &= \mathfrak{a}U+\mathfrak{a}U'.\end{aligned}$$

□

Es ist $\mathfrak{a}M$ der Untermodul von M, der aus allen (endlichen) Summen der Form $\sum \alpha_i x_i$ mit $\alpha_i \in \mathfrak{a}$ und $x_i \in M$ besteht. Für diesen Untermodul wird die Faktorgruppe $M/(\mathfrak{a}M)$ in natürlicher Weise sogar zu einem $R/\mathfrak{a}$-Modul durch die Festlegung der äußeren Verknüpfung $\bullet$ durch

$$\underbrace{(\alpha+\mathfrak{a})}_{\text{Nebenklasse von } R} \bullet \underbrace{(m+\mathfrak{a}M)}_{\in M/(\mathfrak{a}M)} := \alpha\cdot m+\mathfrak{a}M.$$

Führen wir diese Konstruktion mit einem maximalen Ideal des kommutativen Ringes R mit 1 durch, dann wird $M/\mathfrak{a}M$ demnach zu einem Vektorraum über dem Körper $K = R/\mathfrak{a}$.

Bemerkung 5
Es seien M ein R-Modul und $\mathfrak{a}$ ein *zweiseitiges* Ideal von R. Dann ist $M/\mathfrak{a}M$ in natürlicher Weise ein $R/\mathfrak{a}$-Modul.

3.8 Annullator und Torsionselemente

Definition
Es sei M ein R-Modul und $m \in M$. Die Menge an Ringelementen

$$Ann(m) := \{\alpha \in R|\ \alpha\cdot m = 0\}$$

nennen wir den **Annullator** von m.

Es sei U ein Untermodul von M. Die Menge an Ringelementen

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

nennen wir den **Annulator** des Untermoduls $U \leq M$.

Je nach betrachteter algebraischer Struktr kann der Annulator auch different definiert sein. Der Annullator $Ann(m)$ eines Modulelements $m \in M$ ist wegen $(\alpha, \beta \in R)$

$$\begin{aligned}\alpha\cdot m = 0,\ \beta\cdot m = 0 &\Rightarrow (\alpha+\beta)\cdot x = 0,\\ \alpha\cdot m = 0,\ \beta\in R &\Rightarrow (\beta\alpha)\cdot x = 0\end{aligned}$$

ein *Linksideal* von R. In analoger Weise zeigt man, dass $Ann(U)$ ein Linksideal ist. Wegen

$$\alpha \cdot n = 0,\ \beta \in R \Rightarrow\ (\alpha\beta) \cdot n = \alpha \cdot (\beta \cdot n) = 0$$

ist $Ann(U)$ aber auch ein *Rechtsideal*. Also ist $Ann(U)$ ein *zweiseitiges Ideal*. Es ist $Ann(U)U = \{0\}$, also ist U nach obiger Bemerkung in kanonischer Weise ein $R/Ann(U)$-Modul. Mit Hilfe der Identität $Ann(U) = \bigcap_{u \in U} Ann(u)$ kann man alternativ zeigen, dass $Ann(U)$ ein Untermodul in ${}_RR$ ist, d.h. ein Ideal in R.

Definition
Es sei ${}_RM =: M$ ein R-Linksmodul. Ein Element $a \in M$ heißt **Torsionselement** (oder Element endlicher Ordnung), wenn $Ann(a) \neq \{0\}$ gilt. Ein Modul ohne Torsionselemente ungleich $0 \in M$ heißt **torsionsfrei**. Der Modul M nennen wir **treu**, wenn $Ann(M) = \{0\}$ gilt.

Ein torsionsfreier Modul enthält also, bis auf das Nullelement 0, kein Element endlicher Ordnung, d.h. $T(A) = \{0\}$ also ist nur das Nullelement 0 ist ein Torsionselement. Ist ein Modul M torsionsfrei, dann folgt mit $\alpha \in R$ und $m \in M, m \neq 0$ aus der Gleichung $\alpha \cdot m = 0$ stets $\alpha = 0$, d.h. $Ann(m) = \{0\}$. Mit $\alpha, \beta \in R, \alpha \neq 0$ und $m \in M$ folgt somit aus $(\alpha\beta) \cdot m = \alpha \cdot (\underbrace{\beta \cdot m}_{=:m' \in M}) = 0$, dass $\beta \cdot m = 0$ gelten muss, also $\beta = 0$. Der Ring R ist damit *nullteilerfrei* bzw. R ein *Integritätsring*.

Beispiel a) Eine abelsche Gruppe G kann man als $\mathbb{Z}$-Modul interpretieren. Dann ist jedes Element mit endlicher Ordnung in der Gruppe G ein Torsionselement im $\mathbb{Z}$-Modul ${}_{\mathbb{Z}}G$. Insbesondere ist bei endlicher Gruppe G jedes Element Torsionselement: Betrachten wir ein beliebiges Gruppenelement $g \in G$ und bilden die von g erzeugte Untergruppe $H := \langle g \rangle$ von G. Nach Lagrange muss die Ordnung von H (die der Ordnung von g entspricht) ein Teiler von $|G|$ sein.

b) Es sei V ein Vektorraum über dem Körper K mit $dim_K(V) = n$ und $f : V \to V$ linear. Es sei ${}_{K[X]}V$ der bezüglich f gebildete $K[X]$-Modul. Vergleichen Sie mit dem letzten Beispiel in Abschnitt 2.2. Zu jedem $v \in V$ sind die $n+1$ Vektoren $v, f(v), \ldots, f^n(v)$ im n-dimensionalen Vektorraum V linear abhängig. Folglich gibt es eine nicht triviale Linearkombination $\sum_{i=0}^{n} \alpha_i f^i(v) = 0$ und für $p = \sum_{i=0}^{n} \alpha_i X^i \in K[X]$ gilt $p \neq 0$ und $p \cdot v = \sum_{i=0}^{n} \alpha_i f^i(v) = 0$. Also ist jedes Element $v \in {}_{K[X]}V$ ein Torsionselement, da stets ein Ringelement $p \in K[X] \setminus \{0\}$ gefunden werden kann, so dass $Ann(v) \neq \{0\}$ ist.

c) Das Modulelement 0 ist stets Torsionselement, da für alle $\alpha \in R$ die Gleichung $\alpha \cdot 0 = 0$ gilt: Subtrahiert man von $\alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0 + \alpha \cdot 0$ den Summand $\alpha \cdot 0$ so erhält man gerade $\alpha \cdot 0 = 0$.

d) Ist R ein Ring so sind die Torsionselemente von ${}_RR$ genau die Nullteiler von R und das Ringelement 0. Setzen wir $R := K \times K$ mit einem Körper K, dann ist die Menge der Nullteiler von R offensichtlich $\{(K \times \{0\}) \cup (\{0\} \times K)\}$. Damit kann

die Menge aller Torsionselemente in ${}_RR$ kein Untermodul sein. Für $r \in R$ sind z.B. $(r,0),(0,r)$ Torsionelemente aber $(r,0)+(0,r)=(r,r)$ ist kein Torsionselement.

Analog zu abelschen Torsionsgruppen kann man nun die Menge aller Torsionselemente zu einer Gruppe zusammenfassen.

Definition
Es sei ${}_RM =: M$ ein R-Linksmodul. Die Menge aller Torsionselemente $m \in M$

$$Tor(M) = \{m \in M |\ Ann(m) \neq \{0\}\} = \{m \in M |\ \exists \alpha \in R, \alpha \neq 0 \text{ mit } \alpha \cdot m = 0\}$$

nennen wir **Torsionsmodul** von M (von lat. „torquere“ ver-/drehen).

Nun können wir die zentralen Ergebnissen dieses Abschnitts formulieren und beweisen.

SATZ 3.12: *Es sei ${}_RM =: M$ ein R-Linksmodul über einem Integritätsring R. Dann gilt.*

(i) $Tor(M)$ *ist ein Untermodul von* M.

(ii) $M/Tor(M)$ *ist torsionsfrei.*

Beweis. Ad (i): Mit $m \in Tor(M)$ und $\alpha \in Ann(m), \alpha \neq 0$ und $\beta \in R$ gilt $\alpha \cdot (\beta \cdot m) = (\alpha\beta) \cdot m = \beta \cdot (\alpha \cdot m) = 0$, d.h. $\beta \cdot m \in Tor(M)$. Damit haben wir nachgewiesen, dass $Tor(M)$ invariant gegenüber der äußeren Verknüpfung ist. Nun müssen wir noch zeigen, dass $Tor(M)$ eine Untergruppe ist. Dazu sei m' ein weiteres Element aus $Tor(M)$ und $\alpha' \neq 0$ sei aus $Ann(m')$. Dann gilt $\alpha\alpha' \cdot (m+m') = \alpha(\cdot\alpha' m) + \alpha(\cdot\alpha' m') = 0$. Da R ein Integritätsring ist gilt $\alpha\alpha' \neq 0$ und damit ist $m + m' \in Tor(M)$. Natürlich ist mit $m \in Tor(M)$ auch $-m \in Tor(M)$, da in diesem Fall ein $\alpha \in Ann(m), \alpha \neq 0$ existiert und damit $\alpha \cdot (-m) = (\alpha(-1)) \cdot m = -\alpha \cdot m$ gilt. Da $\alpha \neq 0$ ist auch $-\alpha \neq 0$, d.h. $-m \in Tor(M)$.
Ad(ii): Es sei nun $m + Tor(M)$ ein Torsionselement im Fakormodul $M/Tor(M)$, es muss also gemäß Voraussetzungen gelten:

$$\alpha \cdot (m + Tor(M)) = \alpha \cdot m + Tor(M) = Tor(M) \tag{4}$$

für $\alpha \neq 0, \alpha \in R$. Beachten Sie, dass $Tor(M) = 0 + Tor(M)$ das neutrale Element des Faktormodul $M/Tor(M)$ und $Tor(M)$ gegenüber äußerer Multipliation von Ringelementen (als Untermodul) abgeschlossen ist. d.h. $\alpha \cdot Tor(M) = Tor(M)$. Schließlich muss also noch $\alpha \cdot m \in Tor(M)$ wegen (4) gelten. Es gibt also ein $\beta \neq 0$ mit $0 = \beta \cdot (\alpha \cdot m) = (\beta\alpha) \cdot m$. Wieder wegen $\beta\alpha \neq 0$ folgt $m \in Tor(M)$ und das Torsionselement $m + Tor(M) = 0 + Tor(M)$ ist trivial. □

Bemerkung 6
Wie wir wissen heißt ein R-Modul M zyklisch oder monogen, wenn er von einem Element x erzeugt wird, d.h. wenn $M = Rx = \langle x \rangle$ gilt. Betrachten wir nun den Homomorphismus $L : R \to M$ mit $\alpha \mapsto \alpha \cdot x$ für alle $x \in M$, so stellt man aufgrund der Identität $1 \cdot x = x$ fest, dass L surjektiv ist. Ferner hat L gerade den Annulator $Ann(x)$ als Kern. Es liegt nun nahe den Homomorphiesatz anzuwenden, dann erhalten wir einen *Isomorphismus* zwischen $R/Ann(x)$ und M, d.h. $R/Ann(x) \cong M$.

4 Modul-Homomorphismen

Gruppen-Homomorphismen erhalten die Struktur von Gruppen, Ring-Homomorphismen erhalten die Struktur von Ringen und schließlich erhalten Modul-Homomorphismen die Struktur von Mouln. Die Struktur einer Gruppe, eines Ringes oder auch eines Moduls wird dadurch insbesondere durch dessen Verknüpfungen bestimmt.

4.1 Grundlegendes über Homomorphismen

Definition
Es sei R ein Ring und ${}_RM := (M, +)$, ${}_RN := (N, \hat{+})$ zwei Moduln über R mit den äußeren Verknüpfungen $\cdot$ von ${}_RM$ bzw. $\bullet$ von ${}_RN$. Eine Abbildung $f : {}_RM \to {}_RN$ heißt ein **R-Modul-Homomorphismus** (oder auch **R-linear**), wenn für alle $x, y \in M$ und alle $r \in R$ gilt

$$f(x + y) = f(x) \;\hat{+}\; f(y) \qquad \text{(Additivität)}$$
$$f(r \cdot x) = r \bullet f(x) \qquad \text{(Homogenität)}$$

Alle lineare Abbildungen $f : V \to W$ zwischen zwei Vektorräumen V, W über dem Körper K sind K-Modul-Homomorphismen. Eine sehr bedeutende R-lineare Abbildung, die wir bereits verwendet haben, ist die sog. kanonische Projektion.

Beispiel

a) Es sei ${}_RM =: M$ ein R-Links-Modul und U ein Untermodul von M. Dann nennen wir die Abbildung

$$\begin{aligned} \pi : M &\to U \\ x &\mapsto x + U \qquad \text{für } x \in M \end{aligned}$$

die **kanonische Projektion**. Zunächst weisen wir die Additivität nach, dazu seien $x, y \in M$, $r \in R$ dann gilt $\pi(r(x + y)) = r(x + y) + U$. Nun muss man lediglich wissen, wie die Verknüpfungen innerhalb eines Faktormoduls definiert sind, denn damit folgt sofort $r(x+y)+U = (rx+U)+(ry+U) = r\pi(x)+r\pi(y)$ die Additivität und die Homogenität.

b) Die **Nullabbilung** $a \mapsto 0$ zwischen zwei beliebigen Moduln sowie die identische Abbildung sind stets Modul-Homomorphismen. Sie werden auch **triviale Homomorphismen** genannt.

c) Die **kanonische Inklusion** $\iota : U \to M$, $u \mapsto u$ eines Untermoduls U von M, auch identische Injektion genannt, ist ein Modul-Homomorphismus. Die identische Abbilung $id_M : M \to M$ ist ein Spezialfall der Inklusion und wie wir bereits wissen ebenfalls ein Modul-Homomorphismus.

d) Sei ${}_RM$ ein R-Linksmodul, so ist $L_r : M \to M$, $m \mapsto rm$ die Linksmultiplikation mit einem festgewählten $r \in R$ ein Endomorphismus der abelschen Gruppe M: Es seien $m, m' \in M$, dann gilt $L_r(m + m') = r(m + m') = rm + rm' = L_r(m) +$

$L_r(m')$. Da $End(M)$ ein Ring ist, wird durch $L : R \to End(M)$ mit $r \mapsto L_r$ ein Ringhomomorphismus definiert. Umgekehrt induziert jeder Ringhomomorphismus $L : R \to End(M)$ eine äußere Verknüpfung $R \times M \to M$ definiert durch $(r, m) \mapsto (L(r))(m)$ und damit eine R-Modulstruktur auf M.

In den folgenden Bemerkungen fassen wir grundlegende Eigenschaften von Modul-Homomorphismen kompakt zusammen.

Bemerkung 7

a) Ist $\phi : M \to M'$ ein Modul-Homomorphismus von Moduln M und M', 0 das neutrale Element von M und $0'$ das neutrale Element von M', so gilt

   i) $\phi(0) = 0'$,

   ii) $\phi(-a) = -\phi(a) \quad \forall a \in M$.

   Beweis. Ad i): Aus $\phi(0) = \phi(0+0) = \phi(0)+\phi(0)$ folgt durch Addition von $-\phi(0)$ gerade $0' = \phi(0)$.
   Ad ii): Es ist $0' = f(0) = f(a - a) = f(a) + f(-a)$ und da das Inverse stets eindeutig ist, muss $f(-a) = -f(a)$ gelten. □

b) Sind $\phi : M \to N$ und $\varphi : N \to P$ beide R-Modul-Homomorphismen, dann auch das Kompositum $\varphi \circ \phi := \varphi(\phi)$.

   Beweis. Seien $x, y \in M$ dann gilt $\varphi \circ \phi(x + y) = \varphi(\phi(x + y)) = \varphi(\phi(x) + \phi(y)) = \varphi(\phi(x)) + \varphi(\phi(y)) = \varphi \circ \phi(x) + \varphi \circ \phi(y)$. Entsprechend zeigt man auch die Multiplikativität für $r \in R$: $\varphi \circ \phi(r \cdot x) = \varphi(\phi(r \cdot x)) = \varphi(r \cdot \phi(x)) = r \bullet \varphi(\phi(x))$. □

c) Ist $\phi : M \to M'$ ein R-Modul-Isomorphismus, also ein bijektiver R- Modul - Homomorphismus, so ist die Umkehrabbildung $\phi^{-1} : M' \to M$ ebenfalls ein R-Modul- Homomorphismus, also auch ein R-Modul-Isomorphismus. Es sei $\cdot$ die äußere Verknüpfung von M und $\bullet$ die äußere Verknüpfung von M'.

   Beweis. Die Abbildung $\phi : V \to W$ ist bijektiv, denn ϕ ist die zu ϕ^{-1} inverse Abbildung. Wir müssen also nur zeigen, dass f^{-1} linear ist, d.h. wir müssen die Additivität und die Multiplikativität von ϕ^{-1} zeigen.
   Dazu seien $x', y' \in M'$ und da ϕ bijektiv ist, gibt es $x, y \in M$, so dass $\phi(x) = x'$ bzw. $\phi(y) = y'$. Dann gilt $\phi^{-1}(x') = x$ und $\phi^{-1}(y') = y$ und es folgt

$$\begin{aligned} \phi^{-1}(x' + y') &= \phi^{-1}(\phi(x) + \phi(y)) \\ &= \phi^{-1}(\phi(x + y)) && \text{(da } \phi \text{ homomorph)} \\ &= x + y \\ &= \phi^{-1}(x') + \phi^{-1}(y') \end{aligned}$$

Es sei $r \in R$ und $x' \in M'$, dann gilt $x' = \phi(x) \Rightarrow \phi^{-1}(x') = x$ und deshalb

$$\begin{aligned}\phi^{-1}(r \bullet x') &= \phi^{-1}(r \bullet \phi(x)) \\ &= \phi^{-1}(\phi(r \cdot x)) \\ &= r \cdot x \\ &= r \cdot \phi^{-1}(x').\end{aligned}$$

Damit haben wir alles gezeigt. □

d) Offenbar ist die identische Abbildung $id_M : M \to M$ eines Moduls M stets ein Automorphismus von M.

Wird eine Abbildung f angewendet auf x, so werden wir dies entweder durch $f(x)$ oder kurz durch fx notieren.

Definition

Es seien M, N zwei R-Rechtsmoduln. Wir bezeichnen

$$Hom(M,N) = Hom_R(M,N) := \{f : M \to N |\ f \text{ ist } R-\text{linear }\}$$

als die **Homomorphismengruppe** der Moduln M und N. Es ist $Hom(M,N)$ bezüglich der Addition

$$(f+g)(x) := f(x) + g(x)$$

eine abelsche Gruppe.

Beweis. Natürlich ist die Menge an Abbildungen $Hom(M,N)$ gegenüber der definierten inneren Verknüpfung abgeschlossen. Dem neutralen Element entspricht die Nullfunktion $\widehat{0}$, welche stets homomorph ist. Zu vorgegebenem Element $f \in Hom(M,N)$ ist $-f$ das Inverse, so dass $f(x) + (-f(x)) = (-f(x)) + f(x) = \widehat{0}$ gilt. Die Kommutativität ergibt sich aus der Kommutativität des Moduls N. □

Sind V, W Vektorräume, dann ist die Menge aller linearen Abbildungen $Hom(V,W)$ zusammen mit den üblichen Verknüpfungen selbst wieder ein Vektorraum. Im Gegensatz dazu ist $Hom(M,N)$ im Allgemeinen kein R-Modul mehr. Es sei darauf verwiesen, dass für bestimmte Spezialfälle (z.B. das Dualmodul) $Hom(M,N)$ doch noch eine Modulstruktur aufweist.

Eine Homomorphismengruppe umfasst alle strukturerhaltenden Abbildungen zwischen zwei Moduln; es liegt daher nahe zu versuchen *alle* Modul-Homomorphismen zu bestimmen.

Beispiel

Es sei $n \in \mathbb{N}, n \geq 2$. Ziel ist es sätmliche $\mathbb{Z}$-Modul-Homomorphismen $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}$ zu bestimmen. Generell ist die Nullabbildung von Moduln ein Modul-Homomorphismus.

Es sei ϕ ein geforderter Modul-Homomorphismus und $\gamma := \phi(x + n\mathbb{Z})$ das Bild von ϕ, d.h. $\gamma \in \mathbb{Q}$. Dann gilt

$$\begin{aligned} \gamma &= \phi(x + n\mathbb{Z}) = \phi(\overline{x}) \\ \Rightarrow n \cdot \gamma &= n \cdot \phi(x + n\mathbb{Z}) = \underbrace{\phi(x + n\mathbb{Z}) + \ldots + \phi(x + n\mathbb{Z})}_{n \text{ Mal}} \\ &= \phi(nx + n\mathbb{Z}) = \phi(0 + n\mathbb{Z}) = \phi(\overline{0}) = 0. \end{aligned}$$

Also muss $\gamma = 0$ sein, d.h. ϕ kann nur die Nullfunktion sein und deshalb ist die Null-Abbildung der einzige $\mathbb{Z}$-Modul-Homomorphismus $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}$.

Die nächsten elementaren Definitionen sind Ihnen aller Voraussicht nach bereits aus anderen Zweigen der Mathematik bekannt.

Definition
Es sei $\phi : M \to N$ ein R-Modul-Homomorphismus. Dann bezeichnen wir den Definitionsbereich M von ϕ als die **Quelle von** ϕ und notieren diese Beziehung kurz durch $Qu(\phi) = M$. Durch $Zi(\phi) = N$ notieren wir das **Ziel von** ϕ, dass dem Wertebereich N von ϕ entspricht.

Aus der (linearen) Algebra kennen Sie sicherlich bereits die Begriffe Kern und Bild eines Homomorphismus. Analoges gibt es auch für Modul-Homomorphismen.

Definition
Es seien M und N R-Moduln und $\phi : M \to N$ ein R-Modul-Homomorphismus. Dann bezeichnen wir mit

$$Kern(\phi) := \{m \in M |\ \phi(m) = 0\},$$

den **Kern des Homomorphismus** ϕ und

$$Bild(\phi) := \{\phi(m) \in N |\ m \in M\} = \{n \in N |\ \exists m \in M, \text{ so dass } \phi(m) = n\},$$

als **Bild des Homomorphismus** ϕ.

Da Moduln letztlich abelsche Gruppen $(M, +)$ mit einer zusätzlichen äußeren Verknüpfung sind, entspricht der Kern eines Homomorphismuses ϕ allen Elementen aus $Qu(\phi)$, die durch ϕ auf die Null abgebildet werden.

Die Begriffe Surjektion, Injektion und Bijektion sollen, wie üblich in der klassischen Algebra, definiert sein. Einen surjektiven Modul-Homomorphismus nennen wir **Epimorphismus**, ein injektiver Modul-Homomorphismus heißt **Monomorphismus**. Ist ein Modul-Homomorphismus surjektiv und injektiv, also bijektiv, dann nennen wir ihn auch **Isomorphismus**. Ein Modul-Homomorphismus $\phi : M \to M$ wird **Endomorphismus** genannt. Einen bijektiven Endomorphismus $\phi : M \to M$ nennen wir **Automorphismus** von M.

Ist $\phi : M \to N$ ein Modul-Homomorphismus von R und U ein Untermodul von M. Dann bezeichnen wir durch $\phi(U) := \{\phi(u) |\ u \in U\}$ die Bilder von ϕ über U. Es sei $U' \leq N$ ein Untermodul von N, dann notieren wir $\phi^{-1}(U') := \{x \in M |\ \phi(x) \in U'\}$ als das Urbild von ϕ über U'.

Lemma 4.1: *Sei $\phi : M \to N$ ein R-Modul-Homomorphismus zwischen zwei R-Moduln M und N. Weiter seien $U \leq M$ und $U' \leq N$ Untermoduln. Dann gilt:*

i) $\phi(U)$ ist Untermodul von N.

ii) $\phi^{-1}(U')$ ist Untermodul von M.

Beweis. Ad i): Es seien $u'_1, u'_2 \in \phi(U)$, dann existieren $u_1, u_2 \in U$, so dass $\phi(u_1) = u'_1$ bzw. $\phi(u_2) = u'_2$ gilt. Wir zeigen zunächst, dass $\phi(U)$ eine abelsche Gruppe ist: Da U ein Untermodul ist, liegt auch die Differenz $u_1 - u_2$ in U und deshalb gilt $\phi(u_1 - u_2) = \phi(u_1) - \phi(u_2) = u'_1 - u'_2 \in \phi(U)$. Mit dem Untergruppen-Kriterium folgt, dass $\phi(U)$ eine Untergruppe von N ist. Sei nun $r \in R$, dann ist mit $u \in U$ auch $ru \in U$, da U abgeschlossen gegenüber der äußeren Verknüpfung. Es folgt $\phi(ru) = r\phi(u) \in \phi(U)$.

Ad ii): Es seien $u_1, u_2 \in \phi^{-1}(U')$, dann existieren $u'_1, u'_2 \in U'$, so dass $u'_1 = \phi(u_1)$ bzw. $u'_2 = \phi(u_2)$ gilt. Da U' ein Untermodul ist, liegt auch die Differenz $u'_1 - u'_2$ in U', d.h. es muss auch ein Urbild für die Differenz in der Menge $\phi^{-1}(U')$ geben. Es gilt also $\phi(u_1 - u_2) = \phi(u_1) - \phi(u_2) = u'_1 - u'_2 \in U'$. Sei nun $r \in R$ und $u \in \phi^{-1}(U') \Rightarrow \exists u' \in U'$, so dass $u' = \phi(u)$ gilt. Mit $u' \in U'$ liegt auch $ru' \in U'$ und damit gilt $\phi(ru) = r\phi(u) = ru' \in U'$, d.h. zu ru existiert ein Element $r\phi(u) = ru'$.

□

Die Komposition bildet auf der Menge der Funktionen eine multiplikative Verknüpfung. Eine naheliegende Frage ist nun, ob die Surjektivität bzw. die Injektivität bei der Hintereinanderschaltung zweier Epi- bzw. Monomorphismen erhalten bleibt. Kann man einen Homomorphismus in zwei Epimorphismen bzw. Monomorphismen zerlegen, so liegt auch die Frage nahe, welche der Faktoren dann ebenfalls epi- bzw. monomorph sind.

Lemma 4.2: *Seien A, B, C jeweils R-Moduln und $\alpha : A \to B$ bzw. $\beta : B \to C$ Modul-Homomorphismen. Dann gelten:*

i) *Monomorphismen α, β $\Rightarrow$ Monomorphismus $\beta\alpha$,*

ii) *Epimorphismen α, β $\Rightarrow$ Epimorphismus $\beta\alpha$,*

iiii) *Monomorphismus $\beta\alpha$ $\Rightarrow$ Monomorphismus α,*

iv) *Epimorphismus $\beta\alpha$ $\Rightarrow$ Monomorphismus β.*

Beweis. Ad i): Sind $\gamma_1, \gamma_2 : M \to A$ jeweils R-Modul-Homomorphismen, dann gilt folgende Implikationskette:

$$\beta\alpha\gamma_1 = \beta\alpha\gamma_2 \ \Rightarrow\ \alpha\gamma_1 = \alpha\gamma_2 \ \Rightarrow\ \gamma_1 = \gamma_2$$

Beide Implikationsschritte gelten, da α bzw. β injektiv sind.

Ad ii): Zu zeigen ist, dass $\forall c \in C$ ein $a \in A$ existiert, so dass $\beta\alpha(a) = c$ gilt. Dazu benutze man, analog zu i), dass α bzw. β surjektiv sind. Es folgt, dass $\beta\alpha$ epimorph sind. Anstatt eines $a \in A$ könnte man auch, wie in i) allg. einen Modulhomomorphismus $\gamma : M \to A$ verwenden.

Ad iii): Es seien wieder $\gamma_1, \gamma_2 : M \to A$ zwei R-Modul-Homomorphismen, dann gilt folgende Implikationskette:

$$\alpha\gamma_1 = \alpha\gamma_2 \;\Rightarrow\; \beta\alpha\gamma_1 = \beta\alpha\gamma_2 \;\Rightarrow\; \gamma_1 = \gamma_2.$$

Es ist also α ein Monomorphismus.

Ad iv): Nach Voraussetzung ist $\beta\alpha$ surjektiv, d.h. für alle $c \in C$ existiert ein $\gamma : M \to A$, so dass $\beta\alpha\gamma = c$ gilt. Also gibt es auch für alle $c \in C$ ein $\alpha\gamma$, so dass $\beta(\alpha\gamma) = c$ gilt. □

Die Erkenntnisse des nächsten Lemma werden wir im Abschnitt über die Zerlegung eines Homomorphismus benötigen. Es wird insbesondere formuliert, dass sich das Urbild des Bildes eines Homomorphismus $\alpha : A \to B$ aus $Qu(\alpha)$ und dem $Kern(\alpha)$ zusammensetzt.

Lemma 4.3: *Seien A, B zwei R-Moduln und $\alpha : A \to B$ ein Modul-Homomorphismus. Dann gelten:*

i) $U \leq A \quad \Rightarrow \quad \alpha^{-1}(\alpha(U)) = U + Kern(\alpha).$

ii) $U' \leq B \quad \Rightarrow \quad \alpha(\alpha^{-1}(U')) = U' \cap Bild(\alpha).$

Es sei nun auch $\beta : B \to C$ ein Homomorphismus. Dann gelten weiter:

iii) $Kern(\beta\alpha) = \alpha^{-1}(Kern(\beta)),$

iv) $Bild(\beta\alpha) = \beta(Bild(\alpha)).$

Beweis. Ad i): Wir zeigen zunächst, dass $\alpha^{-1}(\alpha(U))$ eine Teilmenge von $U + Kern(\alpha)$ ist. Dazu wählen wir ein beliebiges Element $a \in \alpha^{-1}(\alpha(U))$, dann gilt $\alpha(a) \in \alpha(U)$. Da $\alpha(a)$ also in $\alpha(U)$ liegt, muss es ein $u \in U$ geben, so dass $\alpha(a) = \alpha(u)$ gilt. Daraus ergibt sich sofort $\alpha(a - u) = 0 \;\Rightarrow\; a - u \in Kern(\alpha) \;\Rightarrow\; a \in U + Kern(\alpha)$.
Nun zeigen wir die umgekehrte Inklusion $U + Kern(\alpha) \subseteq \alpha^{-1}(\alpha(U))$. Seien dazu $u \in U, k \in Kern(\alpha)$, dann folgt $\alpha(u + k) = \alpha(u) + \alpha(k) = \alpha(u) + 0 = \alpha(u) \in \alpha(U) \;\Rightarrow\; u + k \in \alpha^{-1}(\alpha(U))$.

Ad ii): Es sei $b \in \alpha(\alpha^{-1}(U')) \subseteq U' \cap Bild(\alpha)$. Dann liegt das Urbild $\alpha^{-1}(b) \in \alpha^{-1}(U')$. Sei $a := \alpha^{-1}(b) \in A$, dann gilt $\alpha(a) \in U'$ gleichzeitig aber offensichtlich auch in $Bild(\alpha)$, womit die erste Inklusion folgt.
Sei nun $x \in U' \cap Bild(\alpha)$, dann muss es ein $a \in A$ geben, so dass $\alpha(a) = x$ gilt. Da gleichzeitig x auch in in U' liegt, muss das Urbild a von x gerade in $\alpha^{-1}(U')$ liegen.

Deshalb muss x tatsächlich in $U' \cap Bild(\alpha)$ enthalten sein.

Ad iii): Es ist $a \in Kern(\beta\alpha)$ genau dann, wenn $\beta\alpha(a) = \beta(\alpha(a)) = 0$ gilt. Das wiederrum ist genau dann der Fall, wenn $\alpha(a) \in Kern(\beta)$ und damit $a \in \alpha^{-1}(Kern(\beta))$ liegt.

Ad iv): $Bild(\beta\alpha) = \beta\alpha(A) = \beta(\alpha(A)) = \beta(Bild(\alpha))$. □

Ist also eine Modulhomomorphismus $\alpha : A \to B$ gegeben, so können wir mit Hilfe des eben bewiesene Lemma sämtliche Untermoduln von A und B durch Untermoduln aus dem jeweils anderen Modul beschreiben. Dazu seien $U \leq A$ und $U' \leq B$ Untermoduln.

Folgerung 4.4:

i) *Ist $\alpha : A \to B$ ein* Monomorphismus*, dann erhält man jeden Untermodul U von A in der Form $\alpha^{-1}(U')$.*

ii) *Ist $\alpha : A \to B$ ein* Epimorphismus*, dann erhält man jeden Untermodul U' von B in der Form $\alpha(U)$.*

Beweis. Ad i): Man setze $U' := \alpha(U)$ und beachte, dass für einen Monomorphismus $\alpha^{-1}(\alpha(U)) = U$ gilt. Nun folgt alles mit Lemma 4.1 und 4.3.

Ad ii): Man setze $U := \alpha^{-1}(U')$ und beachte, dass für einen Epimorphismus $\alpha(\alpha^{-1}(U')) = U'$ gilt. Nun folgt alles mit Lemma 4.1 und 4.3. □

4.2 Der Homomorphie- und die Isomorphiesätze

Die entscheidende Eigenschaften des Kerns bzw. des Bildes eines Homomorphismuses, welche grundlegend für den Homomorphiesatz sind, werden in dem nächsten Lemma formuliert.

Lemma 4.5: *Sei $\phi : M \to N$ ein R-Modul-Homomorphismus zwischen zwei R-Moduln M und N. Dann sind $Kern(\phi) \subseteq M$ ein Untermodul von M und $Bild(\phi) \subseteq N$ ein Untermodul von N.*

Beweis. Es seien $x, y \in Kern(\phi)$, dann ist auch $x - y \in Kern(\phi)$. Dann ist $\phi(x - y) = \phi(x) - \phi(y) = 0 - 0 = 0$, also liegt gemäß Definition auch $x - y \in Kern(\phi)$. Wir müssen nur noch zeigen, dass der Kern auch die skalare Struktur respektiert. Dazu sei zusätzlich $\alpha \in R$, dann liegt auch $\alpha \cdot x$ im Kern von ϕ, da $\phi(\alpha \cdot x) = \alpha \bullet \phi(x) = \alpha \bullet 0 = 0$. Das $\alpha \bullet 0 = 0$ gilt folgt durch die Gleichung $\alpha \bullet 0 = \alpha \bullet (0+0) = \alpha \bullet 0 + \alpha \bullet 0$ und Addition von $-(\alpha \bullet 0)$.

Nun zum Bild von ϕ. Es seien $x', y' \in Bild(\phi)$, dann liegt auch $x' - y' \in Bild(\phi)$, da $x' - y' = \phi(x) - \phi(y) = \phi(x - y)$, wobei $x, y \in M$ gerade die Urbilder von x', y' sind. Wir haben also für $x' - y'$ das Urbild $x - y$ gefunden und damit liegt auch $x' - y'$ im Bild von ϕ. Nun noch die Homogenität: es gilt $\alpha \bullet x' = \alpha \bullet \phi(x) = \phi(\alpha \cdot x)$, d.h. $\alpha \cdot x$ ist Urbild von $\alpha \bullet x'$ unter ϕ. □

Das Bild und den Kern eines Homomorphismus haben wir bereits weiter oben definiert, und dank dem eben bewiesenen Lemma wissen wir nun, dass beide Mengen jeweils Untermoduln sind, so dass die folgenden Definitionen Sinn ergeben:

Definition
Es sei $\phi : M \to N$ ein R-Modulhomomorphismus. Dann heißt $Koke(\phi) := Zi(\phi)/Bild(\phi) = N/\phi(M)$ der **Kokern** von ϕ und $Kobi(\phi) := Qu(\phi)/Kern(\phi) = M/\phi^{-1}(0)$ das **Kobild** von ϕ.

Wie Sie vielleicht bemerkt haben, kann man die Beweisfüuhrung aus der (linearen) Algebra fast wörtlich übernehmen. Entsprechend beinhaltet auch das Folgenende nicht viel Neues.

Lemma 4.6: *Es seien ${}_RM$ und ${}_RN$ R-Links-Moduln und $\phi : {}_RM \to {}_RN$ ein R-Modul-Homomorphismus. Dann gilt folgende Äquivalenz*

$$\phi \text{ ist injektiv } \Leftrightarrow Kern(\phi) = \{0\}.$$

Beweis. „⇒“ Es sei ϕ injektiv; gilt dann $\phi(a) = \phi(b)$ für $a, b \in {}_RM$ so folgt $a = b$. Das Nullelement 0 liegt stets in $Kern(\phi)$. Sei nun weiter $k \in Kern(\phi)$, d.h. es ist $\phi(k) = 0 = \phi(0)$, dann muss $k = 0$ sein, da ϕ injektiv. Also $Kern(\phi) = \{0\}$.

„⇐“ Es sei nun $Kern(\phi) = \{0\}$, wir müssen zeigen, dass ϕ injektiv ist. Deshalb gelte für $a, b \in {}_RM$ die Gleichung $\phi(a) = \phi(b) \Rightarrow \phi(a - b) = 0$, d.h. $a - b \in Kern(\phi)$. Da aber nur 0 im Kern liegt, muss $a - b = 0 \Rightarrow a = b$ gelten. Damit muss ϕ injektiv sein. □

Nun der bekannte und bedeutende Homomorphisatz und im Anschluss die beiden Isomorphiesätze formuliert für Moduln. Seien also M, N R-Moduln und $\phi : M \to N$ ein Modul-Homomorphismus. Durch den Untermodul $Kern(\phi)$ ist eine Partition in Nebenklassen und damit eine Äquivalenzrelation $\sim$ auf M gegeben. Dabei gilt für $x, y \in M$:

$$\begin{aligned} x \sim y &\Leftrightarrow x + Kern(\phi) = y + Kern(\phi) \\ &\Leftrightarrow x - y \in Kern(\phi) \Leftrightarrow \phi(x - y) = 0 \Leftrightarrow \phi(x) = \phi(y). \end{aligned}$$

Zwei Modulelemente liegen also genau dann in derselben Äquivalenzklasse, wenn sich diese dasselbe Bild teilen. Entsprechend liegt es daher nahe jeder Nebenklasse $x + Kern(\phi)$ das Bild $\phi(x)$ zuzuordnen.

SATZ 4.7 (Homomorphiesatz)**:** *Für einen R-Modul-Homomorphismus $\phi : {}_RM \to {}_RN$ gilt*

$$\begin{aligned} \Phi : M/Kern(\phi) &\to Bild(\phi) \\ x + Kern(\phi) &\mapsto \phi(x) \end{aligned}$$

ist ein R-Modul-Isomorphimus, d.h. es gilt $\phi(M) \cong M/Kern(\phi)$.

Beweis. Wir zeigen zunächst, dass Φ ein Modul-Homomorphismus ist. Dazu seinn $x + Kern(\phi)$, $x' + Kern(\phi)$ Elemente aus $M/Kern(\phi)$. Sodann gilt

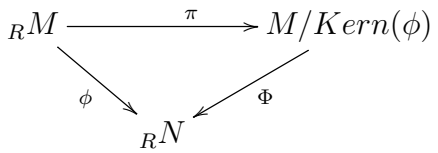
$$\begin{aligned}\Phi([x + Kern(\phi)] + [x' + Kern(\phi)]) &= \Phi((x + x') + Kern(\phi)) \\ &= \phi(x + x') = \phi(x) + \phi(x') \\ &= \Phi(x + Kern(\phi)) + \Phi(x' + Kern(\phi)).\end{aligned}$$

Entsprechend für die skalare Multiplikation:

$$\begin{aligned}\Phi(\alpha \bullet [x + Kern(\phi)]) &= \Phi((\alpha \cdot x) + Kern(\phi)) \\ &= \phi(\alpha \cdot x) = \alpha \cdot \phi(x) \\ &= \alpha \bullet \Phi(x + Kern(\phi)).\end{aligned}$$

Es bleibt zu zeigen, dass Φ injektiv und surjektiv ist. Dazu sei zunächst $(x + Kern(\phi))$ aus $Kern(\Phi)$, es muss also notwendig $\phi(x) = 0$ gelten. D.h. es liegt x im Kern von ϕ und damit gilt $\{x + Kern(\phi) | x \in Kern(\phi)\} = Kern(\Phi)$. Da wir uns über einer Faktorgruppe bewegen die aus Nebenklassen besteht und $Kern(\phi)$ als neutrales Element besitzt, folgt damit die Injektivität von Φ. Sei n nun ein Element aus $Bild(\Phi) = Bild(\phi)$, dann gibt es ein m aus ${}_RM$ mit $\phi(m) = n$. Es folgt damit $\Phi(m + Kern(\phi)) = \phi(m) = n$, also ist Φ surjektiv. □

Der Homomorphiesatz kann durch ein kommutatives Diagramm veranschaulicht werden. Dazu sei $\phi : M \to N$ R-linear. Dann existiert nach dem Homomorphiesatz ein eindeutig bestimmter R-Modul-Homomorphismus $\Phi : M/Kern(\phi) \to N$ mit $\Phi \circ \pi = \phi$, so dass das folgende Diagramm kommutiert:



Auch die beiden Isomorphiesätze für Moduln werden analog zu den bereits bekannten Sätzen aus der (linearen) Algebra bewiesen, deshalb werden wir hier keinen Beweis notieren.

SATZ 4.8 (Erster Isomorphiesatz)**:** *Sind U, U' Untermoduln von M über R, so existiert ein kanonischer Isomorphismus*

$$(U + U')/U \cong U'/(U \cap U').$$

Eine bedeutende Folgerung aus dem ersten Isomorphiesatz ist die Folgende.

Folgerung 4.9: *Es seien M ein R-Modul und $U_1, U_2 \leq M$ Untermoduln von M. Ist $M = U_1 \oplus U_2$ eine Zerlegung von M, dann gilt $M/U_2 \cong U_1$.*

Beweis. $M/U_2 = (U_1 + U_2)/U_2 \cong U_2/(U_1 \cap U_2) = U_2/\{0\} \cong U_2$. □

Beispiel
Seien $n, m \in \mathbb{Z}$, $d := ggT(n,m)$ und $v := kgV(n,m)$. Dann gilt bekanntlich $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ bzw. $m\mathbb{Z} \cap n\mathbb{Z} = v\mathbb{Z}$. Mit dem ersten Isomorphiesatz folgt damit

$$\begin{aligned}(m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} &\cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}),\\ \Rightarrow d\mathbb{Z}/n\mathbb{Z} &\cong m\mathbb{Z}/v\mathbb{Z},\\ \Rightarrow \mathbb{Z}/\frac{n}{d}\mathbb{Z} &\cong \mathbb{Z}/\frac{v}{m}\mathbb{Z}.\end{aligned}$$

Wie wir aus der elementaren Zahlentheorie wissen, gilt für alle $n, m \in \mathbb{N}$ die Formel für das kleinste gemeinsame Vielfache $kgV(n,m) = \frac{nm}{ggT(n,m)}$, welche aus obiger Isomorphie gewonnen werden kann.

SATZ 4.10 (Zweiter Isomorphiesatz)**:** *Sind U, U' Untermoduln von ${}_RM$ mit $U' \subseteq U$, so besteht ein kanonischer Isomorphismus*

$$M/U \cong (M/U')/(U/U').$$

Beispiel
Seien $n, m \in \mathbb{Z}$ und $n\mathbb{Z}, m\mathbb{Z} \leq \mathbb{Z}$ Untermoduln von $\mathbb{Z}$ über $\mathbb{Z}$. Wie wir bereits wissen gilt $n\mathbb{Z} \subseteq m\mathbb{Z}$ genau dann, wenn m ein Teiler von n ist. So gilt die Inklusion $25\mathbb{Z} \subsetneq 5\mathbb{Z}$, da 5 die Zahl 25 echt teilt und mit dem zweiten Isomorphiesatz folgt:

$$\mathbb{Z}/5\mathbb{Z} \cong (\mathbb{Z}/25\mathbb{Z})/(5\mathbb{Z}/25\mathbb{Z}) \cong (\mathbb{Z}/25\mathbb{Z})/(\mathbb{Z}/5\mathbb{Z}).$$

Zunächst mag die Isomorphie $\mathbb{Z}/5\mathbb{Z} \cong (\mathbb{Z}/25\mathbb{Z})/(\mathbb{Z}/5\mathbb{Z})$ erstaunen, betrachtet man jedoch bspw. die Restklasse $\overline{0} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$ aus $\mathbb{Z}/5\mathbb{Z}$ so erkennt man, dass darin die Restklassen $\overline{0} = \{\ldots, -30, -15, 0, 15, 30, \ldots\}$, $\overline{5} = \{\ldots, -25, -10, 5, 20, 35, \ldots\}$ und $\overline{10} = \{\ldots, -35, -20, -5, 10, 25, 40, \ldots\}$ aus $\mathbb{Z}/15\mathbb{Z}$ quasi enthalten sind.

4.3 Produktzerlegung von Homomorphismen

Die Zerlegung eines Problems in einfachere Teilprobleme ist ein erfolgreiches Paradigma um selbiges zu lösen. Daher werden wir in diesem Abschnitt versuchen einen gegebenen Homomorphismus in ein Produkt von zwei Homomorphismen zu zerlegen, wobei zumindest einer der Faktoren angenehme Eigenschaften aufweisen sollte, um dadurch eine Problemreduktion zu bewirken.

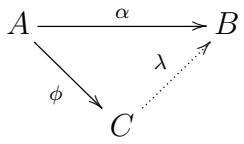
Eine sehr einfache und doch wichtige Zerlegung eines beliebigen Homomorphismus drücken wir in folgendem Lemma aus.

Lemma 4.11: *Ein jeder Homomorphismus $f : M \to N$ kann in der Form $f = \iota\pi$ dargestellt werden, wobei $\pi : M \to Bild(f)$ mit $\pi(m) := f(m)$ für alle $m \in M$ die kanonische Projektion auf das Bild von f und $\iota : Bild(f) \to N$ die kanonische Inklusion bzw. Injektion des Bildes von f auf das Ziel von f ist.*

Ein Beweis lohnt sich nicht, da bei Beachtung der Definitionen die Behauptung direkt folgt. Ohne sich dessen vielleicht Bewusst gewesen zu sein, kennen wir bereits eine weitere Methode Homomorphismen in eine Produkt zu zerlegen: den Homomorphiesatz. Ein

erstes Ziel dieses Abschnittes ist es nun den Homomorphiesatz zu verallgemeinern, um dadurch eine noch größere Anzahl an Homomorphismen zu erfassen.

Der erste Schritt hin zur Verallgemeinerung ist, den Faktormodul gegen einen beliebigen Modul C auszutauschen und zusätzlich einen surjektiven Homomorphismus von A nach C zu fordern. Damit also eine geeignete Zerlegung existieren kann, muss folgendes Diagramm notwendig kommutieren:



Dass obiges Diagramm kommutativ ist, wird in folgendem Satz durch i) formuliert.

SATZ 4.12 (Verallg. des Homomorphiesatzes)**:** *Seien A, B, C Moduln über dem Ring R und $\alpha : A \to B$ ein Homomorphismus bzw. $\phi : A \to C$ ein Epimorphismus mit $Kern(\phi) \subseteq Kern(\alpha)$. Sodann existiert ein Homomorphismus $\lambda : C \to B$ mit folgenden drei Eigenschaften:*

i) $\alpha = \lambda\phi$

ii) $Bild(\lambda) = Bild(\alpha)$

iii) λ *ist ein Monomorphismus* $\quad\Leftrightarrow\quad Kern(\phi) = Kern(\alpha)$.

Beweis. Gemäß Voraussetzungen ist ϕ ein Epimorphismus also surjektiv, d.h. zu jedem Element $c \in C$ existiert ein Urbild $a_c \in A$, so dass $\phi(a_c) = c$ gilt. Sei nun $c \in C$ fest zu $a_c \in A$ gewählt, dann wird durch die Zuordnung

$$c \mapsto \alpha(a_c)$$

eine Abbildung $\lambda : C \to B$ mit $\lambda(c) := \alpha(a_c)$ definiert: Es muss nachgewiesen werden, dass λ wohldefiniert ist, d.h. unabhängig von der Wahl der a_c. Es sei $c := \phi(a) = \phi(a_c)$ mit $a, a_c \in A$, dann gilt $\phi(a - a_c) = 0$ und damit $a - a_c \in Kern(\phi) \leq Kern(\alpha)$ nach Voraussetzungen, d.h. $a - a_c$ liegt auch im Kern von α. Gemäß Definition von λ gilt weiter die Identität $\phi(a) = \phi(a_c) = \lambda(c)$.

Nun zeigen wir schließlich noch, dass λ ein Homomorphismus ist: Seien $c_1 = \phi(a_1), c_2 = \phi(a_2)$ mit $a_1, a_2 \in A$ und $r_1, r_2 \in R$. Dann gilt

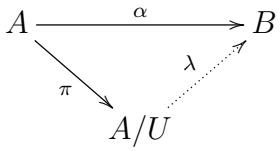
$$\begin{aligned}\phi(r_1a_1 + r_2a_2) &= r_1\phi(a_1) + r_2\phi(a_2) = r_1c_1 + r_2c_2\\ &= \lambda(r_1c_1 + r_2c_2) = \alpha(r_1a_1 + r_2a_2) = r_1\alpha(a_1) + r_2\alpha(a_2)\\ &= r_1\lambda(c_1) + r_2\lambda(c_2).\end{aligned}$$

Die Eigenschaften i) und ii) sind offensichtlich aufgrund der Definition von λ erfüllt. Es bleibt also noch iii) zu zeigen. „$\Rightarrow$“: Sei λ ein Monomorphismus und nach Voraussetzungen gilt $Kern(\phi) \subseteq Kern(\alpha)$, d.h. wir müssen noch die andere Inklusion $Kern(\alpha) \subseteq Kern(\phi)$ nachweisen. Dazu sei $a \in Kern(\alpha)$ und damit $0 = \alpha(a) = \lambda(\phi(a))$, was nur für

$\phi(a) = 0$ möglich ist, d.h. $a \in Kern(\phi) \Rightarrow Kern(\alpha) \subseteq Kern(\phi) \Rightarrow Kern(\alpha) = Kern(\phi)$.
„$\Leftarrow$“: Sei nun $Kern(\alpha) = Kern(\phi)$. Aus $\lambda(c) = 0$ und $c = \phi(a)$ folgt, dass $\alpha(a) = 0$ und damit $a \in Kern(\alpha) = Kern(\phi)$ gilt. Es gilt also $c = \phi(a) = 0$. □

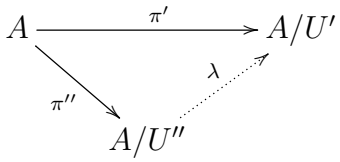
Folgerung 4.13: *Es gelten die Voraussetzungen des verallg. Homomorphiesatzes, d.h. es seien A, B, C Moduln über R und $\alpha : A \to B$ sei ein Modul-Homomorphismus bzw. $\phi : A \to C$ ein Epimorphismus mit $Kern(\phi) \subseteq Kern(\alpha)$. Sodann folgen die daraus resultierenden Spezialfälle:*

1. *Es sei $U \leq Kern(\alpha)$ ein Untermodul von A sowie $C := A/U$ und entsprechend $\phi := \pi : A \to A/U$ der kanonische Epimorphismus. Dann ist das Diagramm*



   kommutativ. Die Abbildung $\lambda : A/U \to B$ ist dabei definiert durch $a + U \mapsto \lambda(a + U) = \alpha(a)$. Im Falle $U = Kern(\alpha)$ entspricht dies gerade dem Homomorphiesatz 4.4.

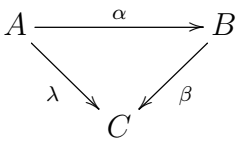
2. *Es seien nun $U'' \leq U' \leq A$ und $\alpha := \pi' : A \to A/U'$ sowie $C := A/U''$ und damit $\phi := \pi'' : A \to A/U''$. In diesem Fall ist das Diagramm*



   kommutativ und $\lambda : A/U'' \to A + U'$ soll durch $a + U'' \mapsto a + U'$ definiert sein.

Ab jetzt setzen wir die Existenz der Produktzerlegung eines Homomorphismus voraus, dazu müssen wir natürlich die Ausgangssituation verändern:

Seien A, B, C Moduln über dem Ring R und $\alpha : A \to B$, $\beta : B \to C$ und $\lambda : A \to C$ drei R-Modul-Homomorphismen, so dass folgendes Diagramm kommutiert:



Es gilt also $\lambda = \beta\alpha$. Nun studieren wir den Zusammenhang zwischen den Eigenschaften des Homomorphismus $\lambda : A \to C$ und der „Zerlegbarkeit“ von dem Modul B. Wie der unbestimmte Begriff „Zerlegbarkeit“ zu interpretieren ist klären wir in der nächsten

Definition
Seien A, B, C Moduln über dem Ring R und $\alpha : A \to B$, $\beta : B \to C$ und $\lambda : A \to C$ drei R-Modul-Homomorphismen, so dass $\lambda = \beta\alpha$ gilt.

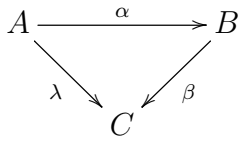
Ein **Monomorphismus** $\alpha : A \to B$ heißt **zerfallend** genau dann, wenn $Bild(\alpha) \leq B$ ein direkter Summand in B ist.
Ein **Epimorphismus** $\beta : B \to C$ heißt **zerfallend** genau dann, wenn $Kern(\beta) \leq B$ ein direkter Summand in B ist.

Beispiel
Es seien $(\mathbb{Z}/n\mathbb{Z}, +)$ ein $\mathbb{Z}$-Modul und $n = \sum_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzelegung von n. Natürlich sind die $p_i,\ i \in \{1, \ldots, r\}$ allesamt Primzahlen und die Potenzen $\alpha_i,\ i \in \{1, \ldots, r\}$ natürliche Zahlen. Nach dem Hauptsatz über endliche abelsche Gruppen gilt $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. Weiter wissen wir, dass sämtliche Untermoduln von den Restklassen der Teiler von n erzeugt werden, d.h. die $\overline{p_i^{\alpha_j}}$ mit $j \in \{1, \ldots, i\}$ sind Generatoren für $\mathbb{Z}$-Untermoduln von $\mathbb{Z}/n\mathbb{Z}$.

Wir setzen nun $n := 15$, d.h. wir untersuchen $\mathbb{Z}/15\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Mögliche Untermoduln sind neben den trivialen $\{0\}$ und $\mathbb{Z}/15\mathbb{Z}$ noch $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$ bzw. $\langle\overline{5}\rangle = \{\overline{0}, \overline{5}, \overline{10}\}$. Man kann nun mit Hilfe eines Isomorphismus $\langle\overline{p_i}\rangle \to \mathbb{Z}/\frac{n}{p_i}\mathbb{Z}$ zeigen, dass die Untermoduln jeweils isomorph zu einer endlichen abelschen Gruppe sind. Es sei $\overline{a} \in \langle\overline{p_i}\rangle$, da $\langle\overline{p_i}\rangle$ zyklisch ist, existiert ein $x \in \mathbb{Z}$, so dass $a = xp_i$ gilt. Die Abbildung $\overline{a} \mapsto \overline{x}$ ist ein Isomorphismus der gewünschen Form.

Betrachten wir den surjektiven Epimorphismus $\pi : \mathbb{Z}/15\mathbb{Z} \to (\mathbb{Z}/15\mathbb{Z})/(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})$ definiert durch $\overline{a} \mapsto \overline{a} + \mathbb{Z}/5\mathbb{Z}$. Dabei sind der Kern und Bild von π jeweils isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Der Epimorphismus ist also zerfallend, da $Kern(\pi) \leq (\mathbb{Z}/15\mathbb{Z})$ ein direkter Summand ist.

Lemma 4.14: *Das Diagramm*



sei kommutativ, d.h. $\lambda = \beta\alpha$. Dann gelten:

i) $Bild(\alpha) + Kern(\beta) = \beta^{-1}(Bild(\lambda))$,

ii) $Bild(\alpha) \cap Kern(\beta) = \alpha(Kern(\lambda))$.

Beweis. Die Beweise sind mit Hilfe des Lemma 4.3 schnell erbracht. Ad i): Da $\lambda = \beta\alpha$ gilt, folgt damit direkt $Bild(\lambda) = Bild(\beta\alpha) = \beta(Bild(\alpha))$. Es gilt also $Bild(\lambda) = \beta(Bild(\alpha)) \Rightarrow \beta^{-1}(Bild(\lambda)) = \beta^{-1}\beta(Bild(\alpha)) = Bild(\alpha) + Kern(\beta)$, wobei die letzte Gleichung durch Anwendung von Lemma 4.3 folgt.

Ad ii): Es gilt $Kern(\lambda) = Kern(\beta\alpha) = \alpha^{-1}(Kern(\beta))$ und mit Lemma 4.3 folgt damit $\alpha(Kern(\lambda)) = \alpha(\alpha^{-1}(Kern(\beta))) = Bild(\alpha) \cap Kern(\beta)$. □

Folgerung 4.15: *Seien die Voraussetzungen aus letztem Lemma gegeben. Dann gelten:*

i) *Epimorphismus* $\lambda \quad \Rightarrow \quad Bild(\alpha) + Kern(\beta) = \beta^{-1}(C) = B.$

ii) *Monomorphismus* $\lambda \quad \Rightarrow \quad Bild(\alpha) \cap Kern(\beta) = \alpha(0) = \{0\}.$

iii) *Isomorphismus* $\lambda \quad \Rightarrow \quad Bild(\alpha) \oplus Kern(\beta) = B.$

Beweis. Dies folgt unmittelbar aus den Definitionen bzw. dem vorangegangenen Lemma. □

Besonders im Hinblick auf so genannte exakte Sequenzen ist die nächste Folgerung von großer Wichtigkeit.

Folgerung 4.16: *Seien die Voraussetzungen aus letztem Lemma gegeben. Dann gelten:*

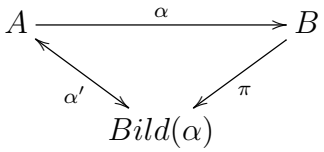
1. *Für $\alpha : A \to B$ sind äquivalent:*
   α ist ein zerfallender Monomorphismus $\Leftrightarrow$ $\exists$ Homomorphismus $\beta : B \to A$ mit $\beta\alpha = id_A$.

2. *Für $\beta : B \to C$ sind äquivalent:*
   β ist ein zerfallender Epimorphismus $\Leftrightarrow$ $\exists$ Homomorphismus $\gamma : C \to B$ mit $\beta\gamma = id_C$.

Beweis. Ad 1.: „⇒“: Es sei $B = Bild(\alpha) \oplus B_1$ und $\pi : B \to Bild(\alpha)$ die durch

$$\pi(\alpha(a) + b_1) := \alpha(a), \quad \alpha(a) \in Bild(\alpha),\ b_1 \in B_1,$$

definierte Projektion von B auf $Bild(\alpha)$. Weiter sei $\alpha' : A \to Bild(\alpha)$ mit $a \mapsto \alpha(a)$ die Einschränkung des Ziels von B auf $Bild(\alpha)$. Da α gemäß Voraussetzung injektiv ist und α' sich auf das Bild von α beschränkt, ist α' ein Isomorphismus.

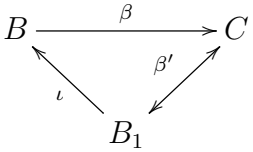


Es sei nun $\beta := \alpha'^{-1}\pi$, dann gilt

$$\beta\alpha(a) = \alpha'^{-1}\pi\alpha(a) = \alpha'^{-1}\alpha(a) = a, \quad a \in A, \tag{5}$$

also $\beta\alpha = id_A$.
„⇐“: Aufgrund der Voraussetzung $\beta\alpha = id_A$ ist α ein Monomorphismus, da id stets bejektiv ist. Nach Folgerung 4.14, iii) zerfällt damit α.

Ad 2.: „⇒“: Sei nun $B = Kern(\beta) \oplus B_1$ und sei $\iota : B_1 \to B$ die Injektion von B_1 in B. Da β gemäß Voraussetzung surjektiv und $Kern(\beta) \cap B_1 = \{0\}$ ist, können wir $\beta' : B \to B_1$ durch $b \mapsto b$ für alle $b \in B_1$ definieren. Dies entspricht einer Einschränkung der Quelle von B auf B_1.



Es ist nun offensichtlich, dass wir $\gamma := \iota\beta'^{-1}$ setzen müssen, denn dann gilt

$$\beta\gamma(c) = \beta\iota\beta'^{-1}(c) = \beta(beta'^{-1}(c))0c, \quad c \in C,$$

also $\beta\gamma = id_C$.

„$\Leftarrow$“: Da $\beta\gamma = 1_C$ gilt, ist β ein Epimorphismus und zerfällt damit nach Folgerung 4.14, iii). □

4.4 Summe und Durchschnitt unter Homomorphismen

In diesem Abschnitt setzen wir unsere Ausführungen über endlich erzeugte und endlich koerzeugte Moduln fort. Dort haben wir bereits den engen Zusammenhang zwischen endlich erzeugt und der Summe von Untermoduln sowie zwischen endlich koerzeugt und dem Durchschnitt von Untermoduln festgestellt. Nun wenden wir uns der Frage zu, wie sich die Summe und der Durchschnitt von Untermoduln unter Homomorphismen und Inversenbildung verhalten.

Lemma 4.17: *Seien $\phi : A \to B$ ein Homomorphismus und $\{A_i \leq A |\ i \in I\}$ bzw. $\{B_j \leq B |\ j \in J\}$ Mengen von Untermoduln der Quelle und des Ziels von α. Dann gelten:*

i) $\alpha(\sum_{i\in I} A_i) = \sum_{i\in I} \alpha(A_i)$,

ii) $\alpha^{-1}(\bigcap_{j\in J} B_j) = \bigcap_{j\in J} \alpha^{-1}(B_j)$,

iii) $\alpha^{-1}(\sum_{j\in J} B_j) \geq \sum_{j\in J} \alpha^{-1}(B_j)$,

iv) $\alpha(\bigcap_{i\in I} A_i) \leq \bigcap_{i\in I} \alpha(A_i)$.

Seien nun $B_j \leq Bild(\alpha)$ für alle $j \in J$ und $Kern(\alpha) \leq A_i$ für alle $i \in I$, dann gelten:

v)

$$\alpha^{-1}(\sum_{j\in J} B_j) = \sum_{j\in J} \alpha^{-1}(B_j),$$
$$\alpha(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} \alpha(A_i).$$

Bevor wir dieses Lemma beweisen vergegenwertigen wir uns zunächst was es aussagt: Das Summenzeichen kann aus dem Homomorphismus α und das Durchschnittszeichen aus der Umkehrabbildung α^{-1} gezogen werden, ohne dass sich dabei das Bild von α ändern würde. Zieht man hingegen das Summenzeichen aus α^{-1} bzw. das Durchschnittszeichen aus α, so entstehen dadurch Unterräume und unter gewissen Umstände sind diese sogar gleich.

Beweis. Ad i) bis iv): Man wende Lemma 4.1 und die Definitionen der Summe des Durchschnitts und eines Homomorphismus an.

Ad v): Durch Anwendung von i) und Lemma 4.3 ergibt sich

$$\begin{aligned}\alpha^{-1}(\sum_{j\in J} B_j) &= \alpha^{-1}(\sum_{j\in J} B_j \cap Bild(\alpha)) = \alpha^{-1}(\sum_{j\in J} \alpha\alpha^{-1}(B_j)) \\ &= \alpha^{-1}\alpha(\sum_{j\in J} \alpha^{-1}(B_j)) = (\sum_{j\in J} \alpha^{-1}(B_j)) + Kern(\alpha) \\ &= \sum_{j\in J} \alpha^{-1}(B_j).\end{aligned}$$

Analog folgt

$$\begin{aligned}\alpha(\bigcap_{i\in I} A_i) &= \alpha(\bigcap_{i\in I} A_i + Kern(\alpha)) = \alpha(\bigcap_{i\in I} (\alpha^{-1}\alpha(A_i))) \\ &= \alpha\alpha^{-1}(\bigcap_{i\in I} (\alpha(A_i))) = (\bigcap_{i\in I} (\alpha(A_i))) \cap Bild(\alpha) \\ &= \bigcap_{i\in I} \alpha(A_i).\end{aligned}$$

□

Das entscheidende Ergebnis dieses Abschnitts ist die nächste Folgerung über den Zusammenhang zwischen endlich koerzeugten Faktormoduln und dem Durchschnitt von Untermoduln.

Folgerung 4.18: *Seien M ein R-Modul und $U \leq M$ ein Untermodul. Dann gilt folgende Äquivalenz:*

M/U ist endlich koerzeugt $\Leftrightarrow$ $\forall$ Menge $\{U_i \leq M |\ i \in I\}$ mit $\bigcap_{i\in I} U_i = U$ gibt es eine endliche Teilmenge $I_0 \subseteq I$, so dass

$$\bigcap_{i\in I_0} U_i = U$$

gilt.

Beweis. „⇒“: Seien $\pi : M \to M/U$ der kanonische Epimorphismus und $\{U_i \leq M |\ i \in I\}$ eine Familie von Untermoduln, so dass $\bigcap_{i\in I} U_i = U$ gilt. Für ein $i \in I$ ist der Kern $U = Kern(\pi) \leq U_i$ ein Untermodul, da $\bigcap_{i\in I} U_i = U = Kern(\pi)$ gilt. Es sind die Voraussetzungen von v) des letzten Lemmas erfüllt, deshalb folgt

$$\bigcap_{i\in I} \pi(U_i) = \pi(\bigcap_{i\in I} U_i) = \pi(U) = 0 + U = \overline{0}.$$

Da M/U endlich koerzeugt ist existiert zur Menge $\{\pi(U_i) \leq M/U |\ i \in I\}$ mit $\bigcap_{i\in I} \pi(U_i) = \overline{0}$ eine endliche Indexmenge $I_0 \subseteq I$, so dass $\bigcap_{i\in I_0} \pi(U_i) = \overline{0}$ gilt. Mit ii) des letzten Lemmas folgt damit

$$\begin{aligned}\pi^{-1}(\overline{0}) = U = \pi^{-1}(\bigcap_{i\in I_0} \pi(U_i)) \\ = \bigcap_{i\in I_0} \pi^{-1}\pi(U_i) = \bigcap_{i\in I_0} U_i + U = \bigcap_{i\in I_0} U_i.\end{aligned}$$

„$\Leftarrow$“: Sei nun $\{\overline{U_i} \leq M/U |\ i \in I\}$ eine Menge von Untermoduln des Faktormoduls mit $\bigcap_{i\in I} \overline{U_i} = \overline{0}$. Mit i) aus dem letzten Lemma folgt damit

$$\pi^{-1}(\overline{0}) = U = \pi^{-1}(\bigcap_{i\in I} \overline{U_i}) = \bigcap_{i\in I} \pi^{-1}(\overline{U_i}).$$

Gemäß den Voraussetzungen existiert eine endliche Indexmenge $I_0 \subseteq I$ mit

$$\bigcap_{i\in I_0} \pi^{-1}(\overline{U_i}) = U.$$

Aufgrund von v) des letzten Lemmas und $U = Kern(\pi) \leq \pi^{-1}(U_i)$ folgt dann schließlich

$$\begin{aligned}\pi(\bigcap_{i\in I_0} \pi^{-1}(\overline{U_i})) = \bigcap_{i\in I_0} \pi\pi^{-1}(\overline{U_i}) \\ = \bigcap_{i\in I_0} \overline{U_i} \cap Bild(\pi) = \bigcap_{i\in I_0} \overline{U_i} = \pi(U) = \overline{0}.\end{aligned}$$

□

5 Direktes Produkt und direkte Summe von Moduln

Die direkte Summe bzw. das direkte Produkt ist ein fundamentales Prinzip das in fast allen Disziplinen der Mathematik Anwendung findet, deshalb werden Sie vielleicht schon das Wichtigste zu diesem Thema wissen. Ist dies der Fall, so können Sie diesen Abschnitt auch überspringen. Wir werden zunächst die innere (direkte) Summe studieren, welche wir im Anschluss zur äußeren (direkten) Summe verallgemeinern.

5.1 Definitionen und Beispiele

Die dirkete Summe ist ein Spezialfall der Summe von Untermoduln, welche wir im Abschnitt 3.3 bereits kennengelernt und definiert haben:

Seien $\{U_i |\ i = 1, \ldots, n\}$ Untermoduln eines R-Modul M, dann ist die **Summe der Untermoduln** die Menge aller endlichen Linearkombinationen, genauer:

$$U_1 + \ldots + U_n = \sum_{i=1}^{n} U_i = \left\{ \sum_{i=1}^{n} u_i |\ u_i \in U_i \text{ für } i = 1, \ldots, n \right\}.$$

Bei der Summe von Untermoduln wird keine Forderung an die Untermoduln U_i gestellt, insbesondere kann U_i das Nullmodul sein bzw. kann gelten $U_i = U_j$ für $i \neq j$ und $i, j \in \{i = 1, \ldots, n\}$.

Definition
Es sei M ein beliebger R-Modul und $\{U_i |\ i \in I\}$ eine Familie von Untermoduln von M mit $U_i \neq \{0\}$. Dann heißt M die (innere) **direkte Summe** dieser Untermoduln, wenn folgende Bedingungen erfüllt sind:

(D_1) M ist die Summe der Unterräume U_i, d.h. $M = \sum_{i \in I} U_i$,

(D_2) Für jeden Index $j \in I$ gilt $U_j \cap \sum_{\substack{i \in I \\ i \neq j}} U_i = \{0\}$.

Wenn M die direkte Summe der Untermoduln U_i ist, wird dieser Sachverhalt durch $M = \bigoplus_{i \in I} U_i$ oder bei endlicher Indexmenge I mit $|I| = n$ durch $M = U_1 \oplus \ldots \oplus U_n$ notiert.

Aus der Bedingung (D_2) folgt, dass die Untermoduln paarweise verschieden sein müssen.

Definition i) Ein Untermodul $U \leq M$ heißt **direkter Summand** von M genau dann, wenn ein Untermodul U' existiert, so dass $M = U \oplus U'$ gilt.

ii) Ein Modul $M \neq 0$ heißt **direkt unzerlegbar** genau dann, wenn $\{0\}$ und M die einzigen direkten Suammanden von M sind.

Kann man also einen Modul M in zwei Untermoduln zerlegen, d.h. es gilt $M = U \oplus U'$, dann nennt man auch manchmal U' das **direkte Komplement** von U.
Ist $U \leq M$ ein nicht triviales Untermodul von M, dann ist U im Allgemeinen kein direkter Summand von M. Im Gegensatz dazu kann man für einen Untervektorraum U eines Vektorraums V stets ein Komplement U' finden, so dass $V = U \oplus U'$ gilt. Ein Beweis mit Hilfe des Basisergänzungssatzes ist recht einfach: Man ergänze die Basis des Unterraums zu einer des gesamten Vektorraums.

Beispiel

a) Sei V ein K-Vektorraum und sei $\{b_i |\ i \in I\}$ eine Basis von V, dann gilt offenbar

$$V = \bigoplus_{i \in I} b_i K.$$

Wie bereits bemerkt ist jeder Unterraum von V ein direkter Summand.

b) In ${}_{\mathbb{Z}}\mathbb{Z}$ ist das Ideal $n\mathbb{Z}$ mit $n \in \mathbb{N}, n \notin \{0, 1, -1\}$ kein direkter Summand. Angenommen $\mathbb{Z} = n\mathbb{Z} \oplus m\mathbb{Z} \Rightarrow nm \in n\mathbb{Z} \cap m\mathbb{Z} = \{0\}$, d.h. es müsste $m = 0$ und damit $\mathbb{Z} = n\mathbb{Z}$ also $n = \pm 1$ – Widerspruch. Es folgt also, dass ${}_{\mathbb{Z}}\mathbb{Z}$ direkt unzerlegbar ist.

c) Jeder einfache Modul M ist direkt unzerlegbar, da er nur die trivialen Untermoduln besitzt.

d) Jeder Modul M, der einen größten Untermodul $\neq M$ oder einen kleinsten Untermodul $\neq \{0\}$ besitzt, ist direkt unzerlegbar.

e) Die Kleinsche Vierergruppe $V_4 = \{(0,0);(0,1);(1,0);(1,1)\}$ ist inneres direktes Produkt bzw. direkte Summe der Normalteiler $\{(0,0);(1,0)\}$ und $\{(0,0);(0,1)\}$, da $(1,1) = (1,0) + (0,1)$ und der Durchschnitt beider Normalteiler $\{(0,0)\}$ ist. Allerdings existiert zur Untergruppe $\{(0,0);(1,1)\}$ kein direktes Komplement.

Die nun folgende Charakterisierung wird häufig in Beweisen benötigt.

Lemma 5.1: *Sei $\{U_i|\ i \in I\}$ eine Familie von Untermoduln $U_i \leq M$ und gelte $M = \sum_{i\in I} U_i$. Dann sind äquivalent:*

Es existiert eine Indexmenge $J \subseteq I$, so dass $M = \bigoplus_{i\in J} U_i$ gilt $\quad\Leftrightarrow$

$\forall x \in M$ ist die Darstellung $x = \sum_{i\in J} u_i$ mit $u_i \in U_i$ und $J \subseteq I$ endlich, in folgendem Sinne eindeutig: Gilt

$$x = \sum_{i\in J} u_i = \sum_{i\in J} u_i' \qquad \text{mit } u_i, u_i' \in U_i,$$

so folgt $\forall i \in J$, dass $u_i = u_i'$ gilt.

Beweis. „$\Rightarrow$“: Es sei $M = \bigoplus_{i\in J} U_i$ die Zerlegung in eine direkte Summe, insbesondere gelten also (gemäß Definition) die Bedingungen (D_1) und (D_2). Sei nun $x = \sum_{i\in J} u_i = \sum_{i\in J} u_i'$, dann folgt

$$\underbrace{u_j - u_j'}_{\in U_j} = \sum_{\substack{i\in J\\ j\neq i}} u_i - u_i' \qquad \in \left(U_j \cap \sum_{\substack{i\in J\\ j\neq i}} U_i \right).$$

Wegen (D_2) gilt $U_j \cap \sum_{\substack{i\in J\\ j\neq i}} U_i \leq U_j \cap \sum_{\substack{i\in I\\ j\neq i}} U_i = \{0\}$ und deshalb folgt $u_j = u_j'$ für alle $j \in J$.

„$\Leftarrow$“: Sei $u \in \left(U_j \cap \sum_{\substack{i\in J\\ j\neq i}} U_i\right)$, dann gilt $u = u_k \in U_k$ und es gibt eine endliche Teilmenge $J \subseteq I$ mit $k \notin J$, so dass

$$u = u_k = \sum_{i\in J} u_i, \qquad u_i \in U_i.$$

Füllt man die linke Seite mit Summanden $0 \in U_i, i \in J$ und die rechte Seite mit dem Summanden $0 \in U_k$ auf, so kommt auf beiden Seiten die gleiche endliche Indexmenge $J \cup \{k\}$ vor und wegen der Eindeutigkeit folgt $u = u_k = 0$, d.h. es gilt (D_2). □

Man kann eine direkte Summe auch für beliebige Moduln definieren. Dabei können beliebige Moduln $M \neq \{0\}$, also nicht nur Untermoduln eines vorgegebenen Moduls, in Beziehung zueinander treten. Deshalb bezeichnen wir diese direkte Summe bzw. dieses direkte Produkt auch als äußeres Produkt bzw. äußere Summe.

Definition
Es sei $\{M_i|\ i \in I,\ M_i \neq 0\}$ eine Familie von Moduln über dem Ring R. Es sei

$$X := \{\sigma : I \to \bigcup_{i \in I} M_i\}$$

die Menge aller Abbildungen von der Indexmenge I in die Vereinigungsmenge der Moduln.

i) Für jeden Index $i \in I$ ist $\sigma(i)$ ein Element aus M_i.

ii) Es gilt $\sigma(i) \neq 0$ für höchstens endlich viele Indizes.

Erfüllt die Menge X nun die Eigenschaften i) und ii) und sind σ_1, σ_2 und σ Abbildungen aus X, so ist bei festem Index i sowohl $\sigma_1(i) + \sigma_2(i)$ als auch $r\sigma(i)$ wieder ein Modulelement aus M_i. Die durch

$$\begin{aligned} (\sigma_1 + \sigma_2)(i) &:= \sigma_1(i) + \sigma_2(i) \qquad \text{und} \\ (r\sigma)(i) &:= r\sigma(i) \end{aligned}$$

definierten Abbildungen besitzen daher wieder die Eigenschaft i) und ii).

Der R-Modul X mit den Eigenschaften i) und ii) heißt (äußere) **direkte Summe** der Modulfamilie $\{M_i|\ i \in I,\ M_i \neq 0\}$ und wird mit $\bigoplus_{i \in I} M_i$ bzw. bei endlicher Indexmenge $M_1 \oplus \ldots \oplus M_n$ bezeichnet.

Erfüllt die Menge X lediglich die Eigenschaft i), so heißt der dadurch entstandene R-Modul X das (äußere) **direkte Produkt** der Modulfamilie $\{M_i|\ i \in I,\ M_i \neq 0\}$ und wird durch $\prod_{i \in I} M_i$ bzw. bei endlicher Indexmenge durch $X_1 \times \ldots \times X_n$ notiert.

Es ist $X = \bigoplus_{i \in I} M_i$ ein Untermoduln von $\prod i \in I M_i$ und sogar ein echter Untermodul für eine *unendliche* Indexmenge I. Ist I jedoch endlich, dann sind direkte Summe und direktes Produkt identisch. Die äußere direkte Summe bzw. das äußere direkte Produkt kann für eine endliche Indexmenge I auch intuitiver charakterisiert werden:

Zunächst ist ein Modulelment α aus $\prod i \in I M_i$ eine Abbildung der Indexmenge. Ihr entspricht im Fall $|I| = n \in \mathbb{N}$ jedoch umkehrbar eindeutig ein n-Tupel $(m_1, \ldots, m_n)$ des Bildes $m_1 := \alpha(1), \ldots, m_n := \alpha(n)$. Gilt nämlich $m_1 \in M_1, \ldots, m_n \in M_n$, so bestimmt das n-Tupel $(m_1, \ldots, m_n)$ auch eindeutig die durch $\alpha(i) = m_i$ $(i = 1, \ldots, n)$ definierte Abbilung. In diesem Sinn kann man also $M_1 \oplus \ldots \oplus M_n$ auch als Menge aller n-Tupel $(m_1, \ldots, m_n)$ auffassen, bei denen $m_i \in M_i$ für $i = 1, \ldots, n$ gilt.

5.2 Universelle Abbildungseigenschaften

Die beiden folgenden Definitionen sind unscheinbar, doch von größter Wichtigkeit. Es sei im Folgenden stets I eine Indexmenge und $J \subseteq I$.

Definition
Ist $M := \prod_{i\in I} M_i$ das direkte Produkt der R-Moduln M_i, so sind in natürlicher Weise Modulhomomorphismen $\pi_i : M \to M_i$ mit $i \in I$ definiert durch $\sigma \mapsto \pi_i(\sigma) := \sigma(i)$. Die Abbildung π_i heißt die **Projektion** auf die i-te Komponente.

Zur Projektion dual definiert man R-Homomorphismen $\alpha_i : M_i \to \bigoplus_{i\in I} M_i$ durch $\alpha_i(m_i) = (n_j)_{j\in J}$, wobei $n_j = 0$ für $i \neq j$ und $n_i = m_i$ gesetzt sind. Die Abbildung α_i nennt man **Injektion**. Oftmals notieren wir die Injektion auch durch ι.

Für $I = \{1, 2, \ldots, n\}$ sind entspricht der Projektion gerade $\pi_i(m_1, \ldots, m_i, \ldots, m_n) := m_i$ und der Injektion $\alpha_i(m_i) := (0, \ldots, 0, m_i, 0, \ldots, 0)$ mit m_i als i-ten Eintrag.

SATZ 5.2: *Ist π eine Permutation der Indexmenge I einer Familie $\{M_i |\ i \in I,\ M_i \neq 0\}$ von R-Moduln. Weiter sei $I = \bigcup_{j\in J} I_j$ eine Zerlegung von I in disjunkte Teilmengen. Dann gilt:*

1) $\prod_{i\in I} M_i \cong \prod_{i\in I} M_{\pi(i)}$ *bzw.* $\bigoplus_{i\in I} M_i \cong \bigoplus_{i\in I} M_{\pi(i)}$

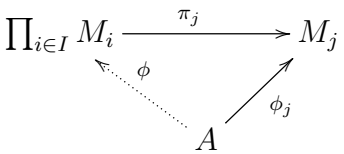
2) $\prod_{i\in I} M_i \cong \prod_{j\in J} \prod_{i\in I_j} M_i$ *bzw.* $\bigoplus_{i\in I} M_i \cong \bigoplus_{j\in J} \left(\bigoplus_{i\in I_j} M_i\right)$

Beweis. Ad 1): Es sei $\sigma \in \{\phi : I \to \bigcup_{i\in I} M_i |\ \forall i \in I : \phi(i) \in M_i\}$ ein beliebiges Element aus dem direkten Produkt $\prod_{i\in I} M_i$. Man betrachte dann die Abbildung $\Delta : I \xrightarrow{\pi} I \xrightarrow{\sigma} \prod_{i\in I} M_{\pi(i)}$ definiert durch $\sigma \mapsto \sigma \circ \pi$. Die Abbildung Δ ist ein Modulisomorphismus. Damit folgt auch die Behauptung für die direkte Summe.

Ad 2): Nun betrachte man den Modulisomorphismus Δ definiert durch $\sigma \mapsto \bigcup_{j\in J} \sigma_j$, wobei $\sigma_j \in \prod_{i\in I_j} M_i$ die Restriktion von σ auf I_j bezeichnet und $\bigcup_{j\in J} \sigma_j$ durch $\left(\bigcup_{j\in J} \sigma_j\right)(k) = \sigma_k$. □

Projektionen sind insbesondere im Kontext von direkten Produkten von Interesse; dagegen interessiert man sich im Kontext der direkten Summen insbesondere für Injektionen. Dies wir auch an den beiden folgenden Sätzen zum Ausdruck gebracht.

SATZ 5.3: *Seien A ein R-Modul und $\{M_i |\ i \in I\}$ eine Familie von Moduln über R. Sei weiter $\{\phi_i : A \to M_i |\ \phi$ homomorph $, i \in I\}$ eine Familie von Modul-Homomorphismen, dann gibt es genau einen Modul-Homomorphismus $\phi : A \to \prod_{i\in I} M_i$, so dass für jedes $i \in I$ das folgende Diagramm*

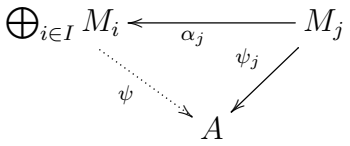


kommutiert, d.h. $\phi_j = \pi_j \circ \phi$ gilt.

Beweis. Angenommen es existiert ein derartiges $\phi : A \to \prod_{i\in I} M_i$, dann muss wegen $\pi_j \circ \phi = \phi_j$ die j-te Komponente von $\phi(a) \in \prod_{i\in I} M_i$ gleich $\phi_j(a)$ sein. Es ist also

notwendig für das gesuchte ϕ, dass für alle $i \in I$ die Gleichung $\phi(a)(i) = \phi_i(a)$ erfüllt ist. Sei nun $\phi(a)(i) := \phi_i(a)$, dann ist andererseits das dadurch definierte ϕ selbst ein Modul-Homomorphismus und es gilt $\phi_j = \pi_j \circ \phi$. □

SATZ 5.4: *Seien A ein R-Modul und $\{M_i |\ i \in I\}$ eine Familie von Moduln über R. Sei weiter $\{\psi_i : M_i \to A |\ \psi \text{ homomorph }, i \in I\}$ eine Familie von Modul-Homomorphismen, dann gibt es genau einen Modul-Homomorphismus $\psi : \bigoplus_{i\in I} M_i \to A$, so dass für jedes $i \in I$ das folgende Diagramm*



kommutiert, d.h. $\psi_j = \psi \circ \alpha_j$ gilt.

Beweis. Für ein jedes $m = (m_i |\ i \in I) \in \bigoplus_{i\in I} M_i$ gilt $m = \sum_{i\in I} \alpha_i(m_i)$. Besitzt die Indexmenge I unendlich viele Elemente, so ist diese Summe formal unendlich. Dennoch kann man auch in diesem Fall $\sum_{i\in I} \alpha_i(m_i)$ als endliche Summe behandeln, da nur endlich vielen Summanden ungleich Null sind. Angenommen es gibt das gesuchte ψ mit $\psi \circ \alpha_j = \psi_j$, dann muss gelten:

$$\psi(m) = \psi(m_i |\ i \in I) = \psi\left(\sum_{i\in I} \alpha_i(m_i)\right) = \sum_{i\in I} \psi\alpha_i(m_i) = \sum_{i\in I} \psi_i(m_i).$$

Für ein (festes) $j \in I$ wird durch die Injektionen α_j die Komposition $\psi \circ \alpha_i$ für den Eintrage m_j auf das Bild von $\psi_j(m_j)$ zurückgeführt. Dadurch wird die Funktion ψ eindeutig festgelegt. Natürlich besitzt $\psi : (m_i |\ i \in I) \mapsto \sum_{i\in I} \psi_j(m_j)$ die geforderten Eigenschaften, da alle ψ_i selbst homomorph sind. □

6 Freie Moduln und Basen von Moduln

Wie wir bereits weiter oben konstatiert haben, sind die Axiome für Moduln und Vektorräume sehr ähnlich. Trotz der formalen Ähnlichkeit zwischen den Definitionen eines R-Modul und eines K-Vektorraum kann man vergleichsweise wenig aus der Theorie der Vektorräume in die Theorie der Moduln übertragen. Dies liegt insbesondere daran, dass der Begriff des Ringes und damit des Moduls zu allgemein gehalten ist, um eine derart strenge Struktur (wie die eines Vektorraumes) zu erhalten. Deshalb ist die Modultheorie wesentlich komplizierter und aufwendiger, als die über Vektorräume. Dennoch liegt der Versuch, das Methodenarsenal der Vektorräume derart zu modifizieren, nahe, um einige Ergebnisse über Vektorräume auch für Moduln nutzbar zu machen.

6.1 Grundbegriffe und Beispiele

Ein großer Unterschied zwischen Vektorräumen und Moduln ist, dass Moduln im Allgemeinen **keine Basis** besitzen. Bestimmte abelsche Gruppen G, betrachtet als $\mathbb{Z}$-Modul,

besitzen z.B. keine Basis. Wollen wir also Erkenntnisse aus der linearen Algebra „retten“, so werden wir nicht umhinkommen, den im Abschnitt 2 allgemein definierten Begriff Modul einzuschränken. In diesem Abschnitt betrachten wir ausschließlich *unitäre Moduln*, d.h. es gilt stets $1 \cdot x = x$.

Definition

Es seien R ein Ring, M ein R-Linksmodul und $B \subseteq M$ eine Teilmenge von M.

(1) Jede endliche Summe $\sum_{i=1}^{n} r_i \cdot b_i$ mit $r_i \in R,\ b_i \in B, n \in \mathbb{N}$, wird als **Linearkombination** von Elementen aus B bezeichnet.

(2) Die Teilmenge B von M heißt **linear unabhängig**, falls für jede endliche Teilmenge $\{b_1, \ldots, b_m\} \subseteq B$ ($m \in \mathbb{N}$, $b_i \neq b_j$ für $i \neq j$ und $i, j = \{1, \ldots, m\}$) aus

$$\sum_{i=1}^{m} r_i \cdot b_i = 0 \qquad \text{mit } r_i \in R,$$

folgt, dass $r_i = 0$ für alle $i \in \{1, \ldots, m\}$. Erfüllt die Teilmenge B von M diese Bedingung nicht nennen wir sie **linear abhängig**.

(3) Eine Teilmenge B eines Modul M heißt **Basis** von M, wenn B ein Erzeugendensystem von M, d.h. $\langle B \rangle = M$ gilt, und B linear unabhängig ist.

Beachten Sie, dass eine linear unabhängige Teilmenge in der Literatur auch oftmals als **frei** bezeichnet wird. Da dies jedoch zu ungewollten Verwechslungen mit freien Moduln führen könnte, werden wir im Folgenden stets den Begriff „linear unabhängig“ bevorzugen.

Ist $B \neq \emptyset$ ein Erzeugendensystem von M, so lässt sich jedes Element m aus M als endliche Linearkombination $m = \sum_{i=1}^{n} r_i \cdot b_i$ mit $r_i \in R, b_i \in B$ schreiben.

Beispiel

a) Durch entsprechende Interpretation ist die leere Menge $\emptyset$ linear unabhängig. Grundsätzlich erfüllt die leere Menge, aufgrund von Mangel an Elementen, jede Allaussage: „Gib mir ein Element der leeren Menge und ich zeige Dir, dass dieses Element die geforderte Aussage erfüllt“. Ansonsten könnte man auch einfach per Definition die leere Menge als linear unabhängig erklären. Weiter ist die leere Menge gemäß Definition Basis des Nullmoduls 0.

b) Jede Teilmenge, die die 0 enthält ist nicht linear unabhängig (also linear abhängig), denn $\sum 0 \cdot b_i + r \cdot 0 = 0$ gilt auch für $r \neq 0$. Allgemeiner formuliert ist jede Teilmenge mit einem Torsionselement (Element von endlicher Ordnung) linear abhängig.

c) Jeder (unitäre) Modul M besitzt sich selbst als Erzeugendensystem, denn jedes $m \in M$ ist als (endliche) Linearkombination der Form $m = 1 \cdot m$ darstellbar.

d) Ist R ein (unitärer) Ring, so ist $\{1\}$ eine Basis von R als R-Links- oder Rechts-Modul betrachtet.

e) Sei R ein Ring mit 1, dann ist $\{(1,0);(0,1)\}$ eine Basis für das R-Modul R^2. Vergleichen Sie mit d).

f) Ist $I \neq \emptyset$ eine (endliche oder unendliche) Indexmenge, dann ist die direkte Summe $\bigoplus_{i\in I} R_i$ mit $R_i := R$ für alle $i \in I$ linear unabhängig und ein Erzeugendensystem. Es sei δ_{ij} das Kroneckerdelta (auch Kroneckersymbol), d.h. $\delta_{ij} := \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$. Die Basis

$$B_\epsilon := \{\epsilon_i : I \to R |\ \epsilon_i(j) = \delta_{ij} \text{ mit } i,j \in I\},$$

besteht aus den Kronecker-Delta-Funktionen. Im endlichen Fall $I = \{1,2,\ldots,n\}$ kann man eine bijektive Abbildung zwischen B_ϵ und der Menge der Standardbasisvektoren $e_i := (0,\ldots,0,\underbrace{1}_{i\text{-ter Eintrag}},0,\ldots,0)$ des R^n angeben. Dabei wird jeder Standardbasisvektor e_i auf δ_{ij} abgebildet.

Das für jede Linearkombination $\sum_{i=1}^n r_i\delta_{ji} = 0$ automatisch $r_i = 0$ für alle $i \in \{1,\ldots,n\}$ folgt direkt aus der Definition der δ_{ij}. Da 1 den Ring R erzeugt und man die direkte Summe auch als Menge aller Abbildungen $I \to \bigcup_{i\in I} R_i$ betrachten kann, folgt auch, dass B_ϵ ein Erzeugendensystem ist.

g) In dem Modul $M := (\mathbb{Z},+)$ über dem Ring $\mathbb{Z}$ ist nur $\{1\}$ oder $\{-1\}$ eine Basis von M. So ist z.B. $\{2,5\}$ zwar ein minimales Erzeugendensystem, da man jedes $x \in \mathbb{Z}$ durch $x\cdot(5-2\cdot 2) = x$ erhält, jedoch ist $\{2,5\}$ nicht linear unabhängig. Aus der Gleichung $z_1\cdot 2 + z_2\cdot 5 = 0$ folgt also nicht notwendig $z_1, z_2 = 0$. Man könnte bspw. $z_1 := -5$ und $z_2 := 2$ setzen. Es ist also eine einzige ganze Zahl, z.B. $\{5\}$, maximal linear unabhängig, da $\mathbb{Z}$ ein Integritätsring ist.

6.2 Freie Moduln

Definition

Es sei M ein R-Modul. Der R-Modul M heißt **frei**, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) M besitzt eine Basis.

(ii) Es gibt eine Teilmenge B von M, so dass sich jedes $m \in M$ eindeutig in der Form $m = \sum_{b\in B} r_b \cdot b$ mit $r_b \in R$, $r_b = 0$ für fast alle $b \in B$, schreiben lässt.

(iii) M ist isomorph zu $R^{(I)} := \bigoplus_{i\in I} R$ als R-Linksmodul für eine geeignete Indexmenge I.

Wir beweisen die Äquivalenz dieser drei Aussagen.

Beweis. (i) $\Rightarrow$ (ii): Ist B eine Basis von M, so schreibt sich jedes $m \in M$ als $m = \sum_{b\in B} r_b \cdot b$ mit $r_b \in R$, fast alle $r_b = 0$. Diese Darstellung ist eindeutig, da aus $m = \sum_{b\in B} r_b \cdot b = \sum_{b\in B} s_b \cdot b$ folgt $\sum_{b\in B} (r_b - s_b) \cdot b = 0$, also $r_b = s_b$ und B ist linear unabhängig.

(ii) $\Rightarrow$ (iii): Aus der Voraussetzung folgt die Existenz einer Teilmenge B von M, so dass sich jedes Modulelement eindeutig als Linearkombination schreiben lässt. Eine Linearkombination ist eine endliche Summe mit einzelnen Summanden $r_b \cdot b \in M$ mit $b \in B$, d.h. jeder Summand liegt auf jeden Fall im Untermodul Rb. Deshalb lässt sich M auch wie folgt als direkte Summe von Untermoduln darstellen:

$$M \cong \bigoplus_{b\in B} Rb.$$

Für $b \in B$ gilt $Ann(b) = \{0\}$ und nach Bemerkung 6 ist dann $R/\{0\} \cong Rb \Leftrightarrow R \cong Rb$ als R-Linksmodul. Damit folgt schließlich

$$M \cong \bigoplus_{b\in B} R.$$

(iii) $\Rightarrow$ (i): Eine Basis von $\bigoplus_{b\in B} R$ ist $\{\delta_{ij} |\ i \in I\}$. Vergleich Sie bitte mit dem Beispiel f) aus diesem Teilabschnitt. □

Neben all den oben genannten Beispielen sind natürlich sämtliche Vektorräume (als Spezialfälle von Moduln) zugleich auch freie Moduln.

Folgerung 6.1: *Ist M ein endlich erzeugter R-Modul und sei M linear unabhängig, dann gibt es ein $n \in \mathbb{N}$ mit $M \cong R^n = R \oplus R \oplus \ldots \oplus R$.*

Beweis. Sei $M = \langle x_1, \ldots, x_r \rangle$ und B eine Basis. Die x_i sind eindeutig darstellbar als $x_i = \sum_{b\in B} r_b \cdot b$, da nach Voraussetzungen B eine Basis ist. Das bedeutet insbesondere, dass die Darstellung $x_i = \sum_{b\in B} r_b \cdot b$ eine Linearkombination, also endlich ist. Die x_i erzeugen den Modul M, deshalb können wir ein beliebiges Modulelement $m \in M$ durch $m = \sum_{i=1}^{r} s_i \cdot x_i = \sum_{\substack{i=1 \\ b\in B}}^{r} s_i \cdot r_b \cdot b$, wobei nur endlich viele verschiedene b an der Summenbildung beteiligt sind, d.h. B ist endlich. □

Bemerkung 8
Für einen freien R-Modul $M \neq \{0\}$ ist $Ann(M) = \{0\} \subset R$.

Beweis. Angenommen es gäbe ein $r \in Ann(M), r \neq 0$. Weiter sei $b \in B$ ein Basiselement, dann folgt aufgrund der Linearkombination $r \cdot b = 0$ und der linearen Unabhängigkeit, dass das Ringlement r doch gleich 0 sein muss – Widerspruch. □

Ein zentrales Ergebnis der linearen Algebra besagt: Ist V ein Vektorraum und B, B' Basen von V, dann enthält B und B' gleich viele Basisvektoren. Dies muss für Moduln im Allgemeinen nicht mehr gelten, wie folgendes Beispiel (vgl. Meyberg, *Algebra*, Band 1, 5.3) zeigt.

Beispiel
Es sei ein Vektorraum V über dem Körper K mit abzählbar unendlicher Basis $B_V := \{x_1, x_2, \ldots\}$ gegeben. Die direkte Summe $W := V \oplus V$ ist selbst auch ein K-Vektorraum mit abzählbarer Basis B_W. Da die Vektorräume V und W gleichmächtig sind, d.h. es gilt $|B_V| = |B_W|$ existiert eine bijektive Abbildung $f : B_V \to B_W$, die zu einer K-linearen Abbildung $f : V \to W$ durch

$$f(\sum_{i=0}^{\infty} r_i x_i) := \sum_{i=0}^{\infty} r_i f(x_i)$$

erweitert werden kann; es ist f also ein Vektorraum-Homomorphismus. Im Folgenden notieren wir die Komposition zweier Funktionen f und g oft in der Kurzform $fg := f \circ g$. Wir setzen $End := End_K(V)$ und betrachten die Abbildung $\widetilde{f} : End \oplus End \to End$ definiert durch

$$\widetilde{f}(\phi \oplus \psi)(x) := \phi(f_1(x)) + \psi(f_2(x)),$$

wobei die Funktionen f_1 bzw. f_2 durch die Gleichung $f(x) = f_1(x) \oplus f_2(x)$ erklärt sein sollen – dies ist aufgrund der Definition des Vektorraums $W = V \oplus V$ legitim. Jeder Vektor $x \in W$ kann gemäß Definition als direkte Summe (=direktes Produkt) $x = u \oplus v = u \times v =: (u, v)$ geschrieben werden; die Funktionen f_1 bzw. f_2 sind also jeweils für einen Unterraum von W zuständig. Wir können also z.B. $f(u, v) := f_1(u, 0) + f_2(0, v)$ setzen.

Wir zeigen nun, dass $\widetilde{f}$ ein Isomorphismus der freien Moduln $End \oplus End$ und End ist. Es ist f ein Gruppen-Homomorphismus der zu Grunde liegenden Gruppen $(V, +)$ bzw. $(W, +)$ und als direkte Folgerung der Definition ist damit auch $\widetilde{f}$ ein Homomorphismus. Sei $\pi \in End$, dann gilt aber auch

$$\begin{aligned}\widetilde{f}(\pi \cdot (\phi \oplus \psi))(x) &= \pi(\phi f_1(x)) + \pi(\psi f_2(x)) \\ &= \pi \widetilde{f}(\phi \oplus \psi)(x).\end{aligned}$$

Bisher haben wir gezeigt, dass $\widetilde{f}$ ein Modul-Homomorphismus ist. Es bleibt noch die Bijektivität zu zeigen. Sei dazu $\phi \oplus \psi = (\phi, \psi) \in Kern(\widetilde{f}) \subseteq (End \oplus End)$. Es muss also für alle $x = (u, v) \in W$ für das Paar (ϕ, ψ)

$$\phi(f_1(u, 0)) + \psi(f_2(0, v)) = 0$$

gelten. Insbesondere muss also für $(u, 0) \in W$ die Gleichung $\phi(f_1(u, 0)) + \psi(f_2(0, 0)) = 0$ für alle $u, v \in V$ erfüllt sein. Doch $\phi(f_1(u, 0)) = 0$ kann nur für $\phi = \widehat{0}$ gelten, da f bijektiv. Analog kann man $\psi = \widehat{0}$ folgern, womit schließlich $(\phi, \psi) = (\widehat{0}, \widehat{0})$ folgt. Es ist also $Kern(\widetilde{f}) = \{(\widehat{0}, \widehat{0})\}$ und damit $\widetilde{f}$ *injektiv*.

Dass $\widetilde{f}$ auch *surjektiv* ist kann man folgendermaßen einsehen: Es sei $\pi \in End$, dann setzen wir $g := \pi f^{-1} : V \oplus V \xrightarrow{f^{-1}} V \xrightarrow{\pi} V$ und $g_1 := g_{|V \oplus 0}$ und $g_2 := g_{|0 \oplus V}$, d.h. es ist

$g = g_1 \oplus g_2$. Nun wenden wir die Funktionen g auf $\widetilde{f}$ an:

$$\begin{aligned}\widetilde{f}(g_1 \oplus g_2)(x) &= \widetilde{f}(g_1 \oplus g_2)(u,v)\\ &= g_1 f_1(u,0) + g_2 f_2(0,v)\\ &= \pi f^{-1}(f_1(u,0) \oplus 0) + \pi f^{-1}(0 \oplus f_2(0,v))\\ &= \pi(f^{-1}(f_1(u,0) \oplus 0) + f^{-1}(0 \oplus f_2(0,v)))\\ &= \pi(x).\end{aligned}$$

Damit haben wir nachgewiesen, dass $\widetilde{f}$ ein Isomorphismus der freien Moduln $End \oplus End$ und End ist, d.h. $End \cong End \oplus End$ als End-Moduln. Aus $End \cong End \oplus End$ kann man induktiv $End^n \cong End^m$ für alle $m, n \in \mathbb{N}$ folgern. Natürlich besitzt eine mögiche Basis von End^n und End^m für $m \neq n$ jeweils eine differente Mächtigkeit der Basen.

Der folgende Satz gibt nun Voraussetzungen an, in der die im letzten Beispiel aufgezeigte Situation nicht mehr auftreten kann. Für *kommutative* Ringe mit 1 verhalten sich freie R-Moduln wie Vektorräume bzw. in diesem Fall sind es sogar Vektorräume.

SATZ 6.2: *Ist R ein kommutativer Ring mit 1 und M ein freier R-Modul, dann haben je zwei Basen von M dieselbe Mächtigkeit.*

Für den Beweis benötigen wir den

SATZ 6.3: *Ist R ein Ring mit 1 und $\mathfrak{a} \neq R$ ein Ideal von R, dann gibt es in R mindestens ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$.*

Den Satz 6.3 werden wir an dieser Stelle nicht beweisen; allerdings werden wir einen ganz ähnlichen Beweis bzw. ein Beweisprinzip im Satz 4.5 aufzeigen, welches das Zornsche Lemma verwendet und in der Modul- und Ringtheorie von großer Bedeutung ist. Mit Hilfe dieses Beweisprinzips ist es dann nicht mehr schwer den Nachweis des letzten Satzes selbst durchzuführen. Alternativ kann man natürlich auch in der Literatur nachschlagen, z.B. MEYBERG, LANG oder VAN DER WAERDEN. Nun aber die Beweisführung von Satz 6.2:

Beweis. (*von Satz 6.2*)
Nach Satz 6.3 enthält R ein maximales Ideal $\mathfrak{m}$. Wie aus der Algebra bekannt gilt: $R/\mathfrak{m}$ ist Körper genau dann, wenn $\mathfrak{m}$ ein maximales Ideal von R ist, also ist $R/\mathfrak{m}$ ein Körper. Wie in Abschnitt 3.6 erläutert wird $M/\mathfrak{m}M$ zu einem Vektorraum über dem Körper $K := R/\mathfrak{m}$. Da M ein freier Modul ist, gilt $M = \bigoplus_{b \in B} Rb$ mit einer Basis B. Daraus folgt mit Hilfe der Basis B $\mathfrak{m}M = \bigoplus_{b \in B} \mathfrak{m}b$ und damit die Isomorphie

$$M/\mathfrak{m}M = \left(\bigoplus_{b \in B} Rb\right) / \left(\bigoplus_{b \in B} \mathfrak{m}b\right) \cong \bigoplus_{b \in B} Rb/\mathfrak{m}b \cong \bigoplus_{b \in B} R/\mathfrak{m}.$$

Somit hat $M/\mathfrak{m}M$ als K-Vektorraum eine Basis der Mächtigkeit von B. Aus der Invarianz der Mächtigkeit von Vektorraumbasen folgt die Behauptung. □

Lemma 6.4 (Zornsche Lemma)**:** *Sei A eine geordnete Menge. Besitzt jede total geordnete Teilmenge von A eine obere Schranke in A, dann besitzt A ein maximales Element.*

Wir erinnern uns, dass das Zornsche Lemma zum Auswahlaxiom und dem Wohlordnungssatz äquivalent ist. Nun der bereits angekündigte Satz, in dessen Beweis ein wichtiges *Beweisprinzip* zu finden ist.

SATZ 6.5: *Jeder Vektorraum V über einem Schiefkörper K besitzt eine Basis.*

Beweis. Sei K ein Schiefkörper und V ein Vektorraum über K. Bezeichne $\mathcal{L}$ die Menge aller linear unabhängigen Teilmengen von V. Da die leere Menge linear unabhängig ist, ist $\mathcal{L}$ nicht leer. Mit der Inklusion von Teilmengen als Ordnungsrelation ist $\mathcal{L}$ eine geordnete Menge. Um das Zornsche Lemma anwenden zu können, muss gezeigt werden, dass jede total geordnete Teilmenge Λ von $\mathcal{L}$ eine obere Schranke in $\mathcal{L}$ besitzt. Ist $\Lambda = \emptyset$, dann ist jedes Element aus $\mathcal{L}$ obere Schranke von Λ. Sei nun $\Lambda = \{X_j |\ j \in J\} \neq \emptyset$, dann zeigen wir, dass

$$X := \bigcup_{j \in J} X_j$$

linear unabhängig ist und daher eine obere Schranke von Λ in $\mathcal{L}$ darstellt. Seien $x_1, \ldots, x_n$ verschiedene Elemente aus Λ. Da Λ total geordnet ist, gibt es ein $X_j \in \Lambda$ mit $x_1, \ldots, x_n \in X_j$. Da X_j linear unabhängig ist, ist $\{x_1, \ldots, x_n\}$ linear unabhängig und folglich ist X linear unabhängig. Nach dem Zornschen Lemma existiert dann in $\mathcal{L}$ ein maximales Element Y. Wir zeigen, dass Y eine Basis von V über K ist. Da Y linear unabhängig ist, braucht nur $\langle Y \rangle$ gezeigt zu werden. Ist $V = 0$, dann folgt $Y = \emptyset$ und nach Definition von $\langle y \rangle$ folgt $\langle Y \rangle = V$. Ist $V \neq 0$, dann folgt $Y \neq \emptyset$. Sei nun $v \in V$ mit $v \notin Y$, dann kann $Y \cup \{v\}$ wegen der Maximalität von Y nicht linear unabhängig sein. Also existieren verschiedene $y_1, \ldots, y_n \in Y$ sowie $k, k_1, \ldots, k_n \in K$ mit

$$vk + \sum_{j=1}^{n} y_j k_j = 0,$$

wobei nicht alle $k, k_1, \ldots, k_n$ gleich 0 sind. $k = 0$ ist nicht möglich, da dann $k_j = 0$ für $j \in \{1, \ldots, n\}$ folgen würde, weil Y linear unabhängig ist. Wegen $k \neq 0$ folgt

$$v = vkk^{-1} = \sum_{j=1}^{n} y_j(-k_j k^{-1}) \in \langle Y \rangle\,,$$

also $V = \langle Y \rangle$. □

Wie wir bereits in Abschnitt 2.2 festgestellt haben ist jeder Ring R über sich selbst ein R-Modul. Die Ringmultiplikation ist eigentlich eine innere Verknüpfung, das hindert jedoch nicht daran $(a, b) \mapsto ab$ auch als äußere Verknüpfung aufzufassen. Auch für den nun folgenden Satz ist es von entscheidender Bedeutung, dass R ein kommutativer Ring mit Einselement ist.

SATZ 6.6: *Seien R ein kommutativer Ring mit Einselement 1_R, M ein R-Modul und $x \in M$ ein Modulelement. Dann gibt es genau einen Modul-Homomorphismus $f : R \to M$ mit $f(1_R) = x$.*

Beweis. Zunächst sei bemerkt, dass der Modulhomomorphismus $f : R \to M$ als Definitionsmenge einen kommutativen Ring R besitzt und deshalb ein zweiseitiges Modul ist. Wir müssen also den Ring R als ein Modul über sich selbst auffassen. Angenommen der Homomorphismus f würde existieren, dann muss für jedes $r \in R$ aufgrund der Homogenität

$$f(r) = f(r1_R) = rf(1_R) = r \cdot x = x \cdot r$$

gelten, da gemäß Voraussetzungen $f(1_R) = x$ angenommen wird und R kommutativ ist. Es sei nun $f : R \to M$ definiert durch $r \mapsto rx = xr$, dann ist f in der Tat ein Homomorphismus (die sog. Rechts- bzw. Linksmultiplikation) und es gilt $1_R \mapsto 1_R x = x$:

Seien $r, s \in R$ und $x \in M$, dann gilt $f(r+s) = (r+s)x = rx + sx = f(r) + f(s)$ und damit die Additivität. Die Homogenität folgt durch $f(rs) = (rs)x = r(sx) = rf(s)$. □

Wir haben also gerade nachgewiesen, dass es zu jedem Modulelement $x \in M$ genau einen Modul-Homomorphismus $f : R \to M$ gibt, so dass das Einselement von R auf das fixierte $x \in M$ abgebildet wird. Da der Ring R als kommutativ vorausgesetzt wird sind R und M beide als R-Modul jeweils zweiseitig, deshalb entsprechen sich Links- und Rechtsmultiplikation.

Sei nun $\{x_j \in M |\ j \in J\}$ eine Familie von Elementen. Nach Satz 6.6 gibt es zu jedem $j \in J$ genau einen Modul-Homomorphismus $f_j : R \to M$ mit $f_j(1_R) = x_j$. Die Familie von Elementen $\{x_j |\ j \in J\}$ induziert damit eine Familie von Modul-Homomorphismen $\{f_j : R \to M |\ f_j \text{ homomorph}, \ f_j(1_R) = x_j, \ j \in J\}$. Gemäß Satz 5.4 existiert ein Modul-Homomorphismus

$$f : \bigoplus_{j \in J} R \to M, \tag{6}$$

für den $f \circ r_j = f_j$ für alle $j \in J$ gilt, wobei r_j die Injektion auf den j-ten Eintrag ist. Wendet man $(r_j |\ j \in J) \in \bigoplus_{j \in J} R$ auf f an, so kann man jedes Bild

$$f(r_j |\ j \in J) = \sum_{j \in J} r_j x_j$$

als Linearkombination dargestellt werden. Ist die Indexmenge J endlich (bspw. $|J| = n$), dann entspricht dies gerade

$$f(r_1, \ldots, r_n) = f(1_R r_1, \ldots, 1_R r_n) = \sum_{j \in J} f_j(1_R r_j) = \sum_{j \in J} r_j f_j(1_R) = \sum_{j \in J} r_j x_j.$$

Lemma 6.7: *Unter den vorgenannten Voraussetzungen gilt:*

(i) f *ist injektiv* $\Leftrightarrow$ $\{x_j |\ j \in J\}$ *ist linear unabhängig.*

(ii) f *ist surjektiv* $\Leftrightarrow$ $\{x_j |\ j \in J\}$ *ist ein Erzeugendensystem.*

(iii) f *ist bijektiv* $\Leftrightarrow$ $\{x_j |\ j \in J\}$ *ist eine Basis von* M.

Beweis. Ad (i): f injektiv $\Leftrightarrow$ Kern der Abbildung $f : \bigoplus_{j\in J} R \to M$ definiert durch $(r_j|\ j \in J) \mapsto \sum_{j\in J} r_j x_j$ besteht nur aus $\{0\} \Leftrightarrow \sum_{j\in J} r_j x_j = 0 \Rightarrow r_j = 0$ für alle $j \in J$ $:\Leftrightarrow f$ injektiv.

Ad (ii): f surjektiv $:\Leftrightarrow \forall m \in M\ \exists J_0 \subseteq J$ mit $|J_0| = n \in \mathbb{N}$, so dass $m = \sum_{j=1}^{n} r_j x_j$ gilt. D.h. jedes Element kann als (endliche) Linearkombination aus Elementen von $X := \{x_j|\ j \in J\}$ dargestellt werden. Aufgrund der Identität $f(r_1, \ldots, r_n) = \sum_{j=1}^{n} r_j f_j(1_R) = \sum_{j=1}^{n} r_j x_j = m$ ist klar, dass damit gerade die Surjektivität der Funktion f gemeint ist.

Ad (iii): Folgt direkt aus (i) und (ii). □

In den folgenden Beispielen werden wir sehen, dass das letzte Lemma eine sehr nützliche Charakterisierung darstellt.

Beispiel

a) Schon zu Beginn dieses Abschnitts, haben wir darauf hingewiesen, dass Moduln im Allgemeinen keine Basis besitzen. Seien $m \geq 2$ eine natürliche Zahl und $(\mathbb{Z}/m\mathbb{Z}, +)$ betrachtet als $\mathbb{Z}$-Modul. Das Modul ist endlich und besitzt genau m Elemente. Es seien nun $x_j \in \mathbb{Z}/m\mathbb{Z}$ für alle $j \in J$. Sodann können wir den nach (5) zugehörigen Modul-Homomorphismus

$$f : \bigoplus_{j} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

bilden. Ist $J \neq \emptyset$, so kann f nicht injektiv sein, da eine unendliche in eine endliche Menge abgebildet wird. Eine direkte Summe über einer Indexmenge $J = \emptyset$ ist allerdings als 0 zu interpretieren, d.h. in diesem Fall kann f nicht surjektiv sein. Mit dem Lemma 6.7 folgt also, dass $\mathbb{Z}/m\mathbb{Z}$ keine Basis besitzen kann.

Natürlich kann man auch direkt mit Hilfe der Definition nachweisen, dass $\mathbb{Z}/m\mathbb{Z}$ keine Basis besitzen kann. Sei $\overline{a}$ ein Element des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$, dann gilt: $\overline{a}$ ist eine Einheit $\Leftrightarrow ggT(a, m) = 1 \Leftrightarrow \overline{a}$ ist kein Nullteiler. In diesem speziellen Ring ist also ein Element entweder eine Einheit oder aber ein Nullteiler. Angenommen uns liegt eine Menge von Einheiten vor, dann müssen wir nur jedes Element mit dem Ringelement $m \neq 0$ multiplizieren und erhalten dadurch eine nicht triviale Linearkombination der Null. Eine vorgegebene Menge $\neq \emptyset$ kann also nicht linear unabhängig sein. Dagegen kann man ein erzeugendes Element (oft auch primitives Element) in $\mathbb{Z}/m\mathbb{Z}$ finden. Das Auffinden einer primitiven Restklasse ist im Allgemeinen jedoch keine einfache Aufgabe, jedenfalls kann eine primitive Restklasse bzw. dessen Vertreter niemals eine Quadratzahl sein und der Vertreter muss teilerfremd zu m sein. Es ist bspw. $\{\overline{3}\}$ ein minimales Erzeugendensystem (primitives Element) von $\mathbb{Z}/8\mathbb{Z}$.

b) Nun untersuchen wir den $\mathbb{Z}$-Modul $(\mathbb{Q}, +)$, die Menge der rationalen Zahlen zusammen mit der üblichen Addition. Jede Menge mit mindestens zwei Elementen $\gamma, \delta \in \mathbb{Q}$ ist linear abhängig. Ist $\gamma, \delta = 0$, so ist die Behauptung trivial. Seien

also $\gamma, \delta \neq 0$ und $\gamma = a/b$ bzw. $\delta = c/d$ die reduzierten Bruchdarstellungen. Wir müssen nun zeigen, dass es ganze Zahlen $z_1, z_2 \in \mathbb{Z}$ gibt, so dass die Linearkombination $z_1\gamma + z_2\delta = 0$ auch Lösungen ungleich $z_1, z_2 = 0$ besitzt. Weiter sei $m := kgV(b, d) \in \mathbb{N} \setminus \{0\}$ der Hauptnenner beider Brüche, dann sind $m\gamma$ und $m\delta$ ganze Zahlen. Es folgt, dass

$$(m\gamma)\delta + (-m\delta)\gamma = 0$$

eine nicht triviale Linearkombination der Null ist.

Ferner hat $\mathbb{Q}$ kein endliches Erzeugendensystem über $\mathbb{Z}$. Angenommen es existiert ein endliches Erzeugendensystem $\{\gamma_1, \ldots, \gamma_n\}$ mit Elementen aus $\mathbb{Q}$. Bildet man nun den Hauptnenner, d.h. berechnet man das kleinste gemeinsame Vielfache von allen Nennern m der Zahlen $\gamma_i,\ i \in \{1, \ldots, n\}$, so ist jede Linearkombination auch als Bruchdarstellung mit Nenner m möglich. Es werden also offensichtlich nicht alle rationale Zahlen durch das Erzeugendensystem erfasst $\lightning$.

Literatur

[1] Algebra, Teil 1, K. Meyberg, 1980, Hanser Verlag.

[2] Algebra, Teil 2, K. Meyberg, 1980, Hanser Verlag.

[3] Algebra – Erster Teil, L. Rédei, 1959, Akademische Verlagsgesellschaft Geest & PortigK.-G.

[4] Repetitorium der Algebra, Michael Holz, 2005, 2. Auflage, Binomi Verlag.

[5] Algebra I, Winfried Scharlau, 2004, FernUniversität in Hagen.

[6] Einführung in die Mengenlehre, Oliver Deister, 2004, Springer Verlag.