Moduln über einem kommutativen Ring

Die nachfolgende Definition verallgemeinert den Begriff des Vektorraumes. Anstelle eines Grundkörpers tritt ein – hier stets kommutativer – Ring R, den wir meist als *Grundring* ansprechen und für den gesamten Abschnitt fixieren.

Definition. 0/3/1

Ein *Modul* über dem Ring R (auch R-Modul) ist ein Tripel $(M,+,\cdot)$, bestehend aus einer Menge M sowie mit $+$ und $\cdot$ bezeichneten Abbildungen (*Operationen*)

$$\begin{array}{ll} M\times M\longrightarrow M\,, & R\times M\longrightarrow M, \\ (m,m')\mapsto m+m' & (a,m)\mapsto a\cdot m \end{array}$$

für die folgende Eigenschaften erfüllt sind:

(1) $(M,+)$ ist abelsche Gruppe.

(2) Für $m,m'\in M$, $a,b\in R$ gelten die beiden *Distributivgesetze*
$(a+b)\cdot m=a\cdot m+b\cdot m$, $a\cdot(m+m')=a\cdot m+a\cdot m'$, sowie
$(a\cdot b)\cdot m=a\cdot(b\cdot m)$, $1\cdot m=m$.

Vereinbarungen. 0/3/2

1. Das neutrale Element der abelschen Gruppe $(M,+)$ wird (wie üblich) mit 0 bezeichnet, das Inverse von $m\in M$ mit $-m$. Statt $m+(-m')$ wird auch $m-m'$ geschrieben sowie anstelle von $a\cdot m$ meist am $(m,m'\in M,\ a\in R)$.
2. *Punktrechnung geht vor Strichrechnung*, d.h. wir ersparen uns das Setzen einiger Klammern durch
$$a\cdot m+b\cdot m':=(a\cdot m)+(b\cdot m'),\quad a,b\in K,\quad m,m'\in M.$$
Erst damit erhalten in der Definition die ersten beiden unter (2) angegebenen Formeln einen Sinn.
3. M heißt die *zugrundeliegende Menge des Moduls.*
Anstelle von $(M,+,\cdot)$ schreiben wir (etwas nachlässig) auch M, wenn kein Zweifel darüber besteht, welche Operationen gemeint sind; wir sprechen dann kurz von dem Modul M.

Diese (wie üblich großzügige) Notation ist natürlich sorgfältig zu interpretieren.

4. In Anlehnung an vertraute Notationen setzen wir
$$U+U':=\{m+m'\,|\,m\in U,m'\in U'\}\,,$$
$$RU:=R\cdot U:=\{a\cdot m\mid a\in R,m\in U\}$$
für beliebige Teilmengen $U,U'\subseteq M$.

Bemerkung. Ist M ein R-Modul, $m,m'\in M$ und $a\in R$, so gilt 0/3/3

(1) $0\cdot m=0$, $a\cdot 0=0\,,$

(2) $-(a\cdot m)=(-a)\cdot m=a\cdot(-m)\,.$

. . . leicht z.z., vgl. z.B. [RW] 3/1/3 .

Auf der linken Seite von (2) steht dabei das Nullelement des Ringes R, während auf der rechten Seite das Nullelement des R-Moduls M steht.

Die Definition der Multiplikation lässt in (2) keine andere Interpretation zu!

Beispiele.

0. Jede einelementige Menge bildet mit den einzig möglichen Operationen einen R-Modul, der gewöhnlich mit $\mathbf{0}$ bezeichnet wird (*Nullmodul*).

Ist R der Nullring, so existieren wegen $0 = 1$ nach der Bemerkung keine weiteren Moduln; es wird daher meist stillschweigend vorausgesetzt, dass R wenigstens zwei Elemente besitzt.

1. Der Grundring R bildet mit seiner Addition und Multiplikation einen R-Modul.
2. Eine abelsche Gruppe ist stets auch $\mathbb{Z}$-Modul mit der üblichen n-fachen Addition eines Gruppenelements m oder seines Inversen (wir erhalten $n \cdot m$ bzw. $(-n) \cdot m$ für $n \in \mathbb{N} \setminus \{0\}$). Es gibt daher keinen Anlass, zwischen $\mathbb{Z}$-Moduln und abelschen Gruppen zu unterscheiden.
3. K sei ein Körper. K-Vektorräume sind Moduln über K.
4. X sei eine Menge, $R^X = \mathrm{Abb}(X, R)$ die Menge der Abbildungen von X in den Ring R. Für $a \in R$ und $f, g \in M$ werden Abbildungen $f+g$ und $a \cdot f$ aus R^X durch
$$(f+g)(x) := f(x) + g(x), \quad x \in X$$
$$(a \cdot f)(x) := a \cdot f(x), \quad x \in X$$
definiert. Durch die Operationen $(f, g) \mapsto f+g$ und $(a, f) \mapsto a \cdot f$ wird R^X zum R-Modul.

Das Beispiel 4 kann leicht verallgemeinert werden:

5. I sei eine nichtleere Indexmenge, $(M_i)_{i \in I}$ eine Familie von R-Moduln. Dann bildet die Produktmenge $\bigtimes_{i \in I} M_i$ einen R-Modul mit den Operationen
$$(m_i)_{i \in I} + (m'_i)_{i \in I} := (m_i + m'_i)_{i \in I}\,, \quad a \cdot (m_i)_{i \in I} := (a \cdot m_i)_{i \in I}$$
$(a \in R$ und $(m_i)_{i \in I}, (m'_i)_{i \in I} \in \bigtimes_{i \in I} M_i$).
Der so konstruierte Modul heißt *direktes Produkt* der Moduln M_i.
Das *Produkt einer leeren Familie* von Moduln wird als der Nullmodul $\mathbf{0}$ definiert.
Für das direkte Produkt wird gelegentlich auch das Symbol $\prod_{i \in I} M_i$ verwendet. Als Spezialfall des Produkts erhalten wir den Modul $R^n = \underbrace{R \times \ldots \times R}_{n \text{ Faktoren}}$.
6. Beschränkung des Skalarbereichs: Ist M ein R-Modul und R eine R-Algebra, so wird durch den Strukturhomomorphismus $R' \to R$ eine Multiplikation der Elemente aus R' mit denen Elementen der Menge M vermittelt. Wir erhalten daher einen R'-Modul mit der selben zugrundeliegenden Mengen M.

Hier bezeichnen natürlich $m_i + m'_i$ und $a \cdot m_i$ die Summe bzw. das Produkt in dem R-Modul M_i.

Homomorphismen 0/3/4

Definition. M, N bezeichnen R-Moduln. Eine Abbildung $f : M \to N$ der zugrundeliegenden Mengen heißt *Homomorphismus von R-Moduln* (auch *R-Homomorphismus* oder *R-lineare Abbildung*), falls für alle $r \in R$ und $m, m' \in M$
$$f(m + m') = f(m) + f(m'),$$
$$f(r \cdot m) = r \cdot f(m).$$
Der Grundring R wird nur in Zweifelsfällen in die Bezeichnungen aufgenommen; sonst wird z.B. anstelle von *R-linear* kurz *linear* geschrieben.

Sind Verwechslungen möglich, so sollte das Wort „linear“ nicht ohne Bezug auf R verwendet werden.

Die Definition lässt sich auch folgendermaßen ausdrücken:

Aus $r_1, \ldots, r_n \in R$ und $m_1, \ldots, m_n \in M$ folgt stets

$$f(r_1 m_1 + \ldots + r_n m_n) = r_1 f(m_1) + \ldots + r_n f(m_n).$$

Natürlich ist insbesondere $f(0) = 0$ und $f(-m) = -f(m)$.

Eine leichte Rechnung zeigt: Sind $f : M \to N$ und $g : N \to P$ linear, dann gilt dies auch für die Produktabbildung $g \cdot f : M \to P$.

Definition. (*Kategorie der R-Moduln*) 0/3/5

Die *Kategorie* $(\mathbf{mod}_R)$ *der R-Moduln* wird durch die Klasse der R-Moduln (Objekte) und deren R-lineare Abbildungen (Morphismen) gegeben, wobei die letzteren als Tripel aus Quellobjekt, Zielobjekt und der betreffenden Abbildung verstanden werden. Das Kompositionsgesetz ist durch das Produkt von Abbildungen definiert.

Die Verifikation der Eigenschaften einer Kategorie ist hier trivial. Die allgemein definierten Begriffe des *Isomorphismus*, *Endomorphismus*, *Automorphismus* usw. sind nun auch für diesen Spezialfall verfügbar.
Mit $\mathrm{Hom}_R(M, N)$ wird die Menge der Homomorphismen $M \to N$ bezeichnet, mit $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ die Menge der Endomorphismen und mit $\mathrm{GL}_R(M)$ die Gruppe der Automorphismen von M.

Bemerkung. 0/3/6

1. Die identischen Abbildungen eines Moduls in sich bilden die Identitäten der Kategorie $(\mathbf{mod}_R)$.
3. Ein R-Homomorphismus $f : M \to N$ ist genau dann Isomorphismus, wenn er bijektiv ist. In diesem Fall ist die inverse Abbildung f^{-1} ebenfalls R-linear, und $g := f^{-1}$ ist der eindeutig bestimmte Homomorphismus mit $f \cdot g = \mathrm{id}_N$ und $g \cdot f = \mathrm{id}_M$.
4. Existiert ein Isomorphismus $f : M \to N$ von R-Moduln, so nennen wir diese isomorph und schreiben dafür $M \underset{R}{\cong} N$ (kurz $M \cong N$).

   Durch Isomorphie ist auf jeder Menge von R-Moduln eine Äquivalenzrelation definiert.
5. I sei eine nichtleere Indexmenge, $(M_i)_{i \in I}$ eine Familie von R-Moduln. Das bereits zuvor definierte direkte Produkt $\prod_{i \in I} M_i$ ist gleichzeitig das kategoriale direkte Produkt der Moduln M_i in $(\mathbf{mod}_R)$, wenn als Projektionen die Homomorphismen

   $$\pi_j : \prod_{i \in I} M_i \to M_j \text{ mit } (m_i)_{i \in I} \mapsto m_j$$

   verwendet werden.

Vgl. 0/3/3, Beispiel 5.

Beispiele.

(1) Die *Nullabbildung* $0 : M \to N$, die jedes Element von M auf das Nullelement in N abbildet, ist eine R-lineare Abbildung.

(2) Sind $n, m \in \mathbb{N} \setminus \{0\}$, so gehört zu jeder R-linearen Abbildung $f : R^n \to R^m$ genau eine Matrix $A \in \mathrm{M}(m, n)$ mit

$${}^{\mathrm{t}}f(x_1, \ldots, x_n) = A \cdot {}^{\mathrm{t}}(x_1, \ldots, x_n) \text{ für alle } x_1, \ldots x_n \in R.$$

Leider ist dies für R-Moduln eine sehr spezielle Situation.

(3) Für $M, N \in (\mathbf{mod}_R)$ ist $\mathrm{Hom}_R(M, N)$ ein R-Modul mit den Operationen

$$(f + g)(m) := f(m) + g(m) \text{ und } (r \cdot f)(m) := r \cdot f(m)$$

für $r \in R$, $m \in M$ und $f, g \in \mathrm{Hom}_R(M, N)$.

Untermoduln 0/3/7

Definition. Ist $(M,+,\cdot)$ ein R-Modul und $U \subseteq M$ eine Teilmenge, dann heißt U *Untermodul,* falls die Operationen $+$ und $\cdot$ Einschränkungen auf U besitzen und U mit diesen einen R-Modul bildet.

U ist Untergruppe von M bezüglich $+$ und gegenüber Multiplikation mit Elementen aus R abgeschlossen.

0/3/8

Ebenso wie für Vektorräume lässt sich ein einfaches Kriterium für diese Bedingung angeben: *M sei ein R-Modul. Die nichtleere Teilmenge $U \subseteq M$ ist genau dann ein Untermodul von M, wenn für $a, a' \in R$ und $m, m' \in U$ stets $am + a'm' \in U$ gilt.*

… ein beliebter Fehler: Die Bedingung $U \neq \emptyset$ wird übersehen.

Der Beweis ist völlig analog zum vertrauten Fall. Auch die folgenden Eigenschaften von Untermoduln und Erzeugendensystemen können fast wörtlich aus der linearen Algebra übertragen werden ([RW], 3/1/12 – 3/1/23).

Betrachten Sie diesen Abschnitt vorwiegend als Wiederholung.

Beispiele.

… ständig verwendete Untermoduln.

(1) Jeder Modul M besitzt die *trivialen Untermoduln* $\{0\}$ und M.

(2) $I \neq \emptyset$ bezeichnet eine Indexmenge. Dann ist

$$R^{(I)} := \{(r_i)_{i\in I} \in R^I \mid r_i = 0 \text{ für fast alle } i\}$$

ein Untermodul von R^I; er stimmt im Fall einer endlichen Menge I mit $R^{(I)}$ überein.

(3) Ist $\boldsymbol{a}$ ein Ideal in R und M ein R-Modul, so wird durch

$$\boldsymbol{a}M := \boldsymbol{a} \cdot M := \left\{ \sum_{n\in M} a_i m_i \;\middle|\; n \in \mathbb{N},\, a_i \in \boldsymbol{a},\, m_i \in M \right\}$$

ein Untermodul von M definiert.

Definition. (*Kern eines Homomorphismus*) 0/3/9

Ist $f : M \to N$ eine R-lineare Abbildung, so heißt $\ker(f) := f^{-1}(0)$ der *Kern von f.*

Diese Menge ist nichts anderes als der Kern des durch f gegebenen Homomorphismus der additiven Gruppe $(M,+)$ in die additive Gruppe $(N,+)$.

Bemerkung. (*Eigenschaften von Kern und Bild*) 0/3/10

$f : M \to N$ sei ein Homomorphismus in $(\mathbf{mod}_R)$.

(1) $\ker(f)$ ist ein Untermodul von M.

(2) $\mathrm{im}(f)$ ist ein Untermodul von N.

(3) f ist Monomorphismus $\iff$ $\ker(f) = \mathbf{0}$.

Bemerkung. (*Durchschnitt von Untermoduln*) 0/3/11

$(U_i)_{i\in I}$ sei eine (nicht leere) Familie von Untermoduln des R-Moduls M. Dann ist auch ihr Durchschnitt $\bigcap_{i\in I} U_i$ ein Untermodul von V.

Die Vereinigung von Untermoduln ist im Allgemeinen kein Untermodul. Leicht zu sehen ist aber

Bemerkung – Definition. (*Summe zweier Untermoduln*) 0/3/12

Sind U_1, U_2 Untermoduln des R-Moduls M, dann ist auch

$$U_1 + U_2 = \{\boldsymbol{u}_1 + \boldsymbol{u}_2 \mid \boldsymbol{u}_1 \in U_1,\ \boldsymbol{u}_2 \in U_2\}$$

ein Untermodul von M, er heißt *Summe* dieser Untermoduln.

Lemma. *U_1, U_2, U_3 seien Untermoduln des R-Moduls M.* 0/3/13

(1) $U_1 + U_1 = U_1$.

Diese Rechenregeln sind wohl eine nützliche Illustration, sollten aber nicht als „Stoff zum auswendig Lernen“ angesehen werden.

(2) $U_1 + U_2 = U_2 + U_1$.

(3) $(U_1 + U_2) + U_3 = U_1 + (U_2 + U_3)$,
hier ist es daher nicht nötig, Klammern zu setzen.

(4) $(U_1 \cap U_2) + (U_1 \cap U_3) \subseteq U_1 \cap (U_2 + U_3)$.

(5) $U_1 + (U_2 \cap U_3) \subseteq (U_1 + U_2) \cap (U_1 + U_3)$ *und insbesondere*
$U_1 + (U_2 \cap U_3) = (U_1 + U_2) \cap U_3$, *falls* $U_1 \subseteq U_3$ (*modulares Gesetz*).

Tatsächlich lassen sich auch Summen von beliebig (nicht notwendig endlich) vielen Untermoduln definieren. Wir bilden zunächst deren Vereinigung. Da der Durchschnitt von Untermoduln stets Untermodul ist, existiert ein kleinster Untermodul, der diese Vereinigung enthält.
Entsprechend können wir für jede Teilmenge von M vorgehen. Wir beginnen mit einer alternativen Beschreibung dieses Durchschnitts.

Definition. (*Linearkombination*) 0/3/14

S sei Teilmenge des R-Moduls M. Eine *Linearkombination* (auch *Vielfachensumme*) von Elementen aus S ist eine Summe $\sum_{s\in S} a_s \cdot s$ mit $a_s \in R$, wobei fast alle Koeffizienten a_s gleich 0 sind.
Wir lassen ausdrücklich den Fall einer leeren Menge S zu und erinnern daran, dass die Summe über eine leere Indexmenge definitionsgemäß 0 ist.

Die angegebene Definition erfasst zunächst den Fall endlicher Mengen. Damit die Summe auch für unendliche Mengen S einen Sinn erhält, bezeichnen wir für Familien $(m_i)_{i\in I}$ von Elementen aus M, in denen fast alle m_i verschwinden, mit $\sum_{i\in I} m_i$ die (endliche!) Summe über alle diejenigen m_i, für die $m_i \neq 0$ ist. Solche Summen erfüllen die vertrauten Rechenregeln; beispielsweise folgt

$$\sum_{i\in I} m_i + \sum_{i\in I} n_i = \sum_{i\in I} (m_i + n_i).$$

Alternativ bilden wir die von vornherein endlichen Summen $\sum_{i=1}^{n} a_i s_i$ mit $n \in \mathbb{N}$, $a_i \in R$ und $s_i \in S$.

Definition. (*lineare Hülle, Erzeugendensystem*) 0/3/15

Die Menge $\mathrm{L}_R(S)$ aller Linearkombinationen der Teilmenge S des R-Moduls M heißt *lineare Hülle* von S. Wir verwenden gelegentlich die recht anschauliche Schreibweise

$$\mathrm{L}_R(S) =: \sum_{s\in S} R\cdot s =: \sum_{s\in S} Rs.$$

Ist $\mathrm{L}_R(S) = M$, so heißt S ein *Erzeugendensystem für* M*;* wir sagen auch M *ist von der Menge* S *erzeugt.*

Bemerkung. (*Eigenschaften der linearen Hülle*) 0/3/16

$S \subseteq M$ sei Teilmenge des Moduls M.

(1) $S \subseteq \mathrm{L}_R(S)$.

(2) $\mathrm{L}_R(S)$ ist stets ein Untermodul. Für einen beliebigen Untermodul U von M, der die Menge S enthält, gilt $\mathrm{L}_R(S) \subseteq U$.

(3) $\mathrm{L}_R\big(\mathrm{L}_R(S)\big) = \mathrm{L}_R(S)$.

(4) $\mathrm{L}_R(\emptyset) = \mathbf{0}$, $\mathrm{L}_R(M) = M$.

(5) $(U_i)_{i\in I}$ sei eine Familie von Untermoduln von M. Dann ist

$$\mathrm{L}_K\Big(\bigcup_{i\in I} U_i\Big) = \Big\{ \sum_{i\in I} m_i \;\Big|\; m_i \in U_i,\ \text{fast alle } m_i = 0 \Big\}.$$

(6) Ist $f : M \to N$ eine R-lineare Abbildung und $S \subseteq M$ eine Teilmenge, so gilt

$$f\big(\mathrm{L}_R(S)\big) = \mathrm{L}_R\big(f(S)\big).$$

Teil (2) der Bemerkung besagt, dass $\mathrm{L}_R(S)$ der kleinste Untermodul ist, der die Menge S enthält. $\mathrm{L}_R(S)$ ist daher Durchschnitt aller Untermoduln von M, die S umfassen.
Nach (6) bildet eine R-lineare Abbildung $f : M \to N$ insbesondere jedes Erzeugendensystem von M auf ein Erzeugendensystem von $\operatorname{im} f$ ab.

Eigenschaft (5) rechtfertigt folgende

Definition. (*Summe einer Familie von Untermoduln*) 0/3/17

$(U_i)_{i\in I}$ sei eine Familie von Untermoduln des R-Moduls M. Dann heißt der Untermodul

$$\sum_{i\in I} U_i := \left\{ \sum_{i\in I} m_i \,\middle|\, m_i \in U_i,\ \text{fast alle } m_i = 0 \right\}$$

die *Summe der Untermoduln* U_i.

Insbesondere:
$U_1 + \ldots + U_n = \{x_1 + \ldots + x_n \mid x_i \in U_i\}$.

Für eine endliche Indexmenge $I\ (\neq \emptyset)$ entspricht dies der in 0/3/12 gegebenen Definition der Summe von Untermoduln.

Ist $S = \{m_1, \ldots, m_s\}$ eine endliche Teilmenge von M, so verwenden wir die Bezeichnung $\mathrm{L}_K(m_1, \ldots, m_s)$ für die lineare Hülle von S, und es ist

$$\mathrm{L}_K(m_1, \ldots, m_s) = \{t_1 m_1 + \ldots + t_s m_s \mid t_1, \ldots, t_s \in R\}.$$

Direkte Summen und lineare Fortsetzung 0/3/18

Vektorräume sind direkte Summen eindimensionaler Unterräume, besitzen daher eine sehr spezielle Struktur. Für Moduln über beliebigen Ringen existieren im Allgemeinen keine vergleichbar einfachen Zerlegungen in direkte Summanden.

Definition. (*direkte Summe*)

$(U_i)_{i\in I}$ sei eine Familie von Untermoduln des R-Moduls M. Dann heißt M *direkte Summe* der Untermoduln U_i, falls für alle $m \in M$ eindeutig bestimmte $m_i \in U_i$ existieren mit $m = \sum_{i\in I} m_i$ und $m_i = 0$ für fast alle $i \in I$. Dabei heißt m_i die *Komponente von* m *in* U_i.
Wir beschreiben diesen Sachverhalt durch das Symbol $M = \bigoplus_{i\in I} U_i$ bzw. im Fall einer endlichen Familie $(U_1, \ldots, U_n)$ durch

$$M = U_1 \oplus \ldots \oplus U_n$$

und sprechen von einer *direkten Zerlegung des Moduls* M *in die angegebenen Summanden* U_i.
Sind U_1, U_2 Untermoduln mit $U_1 \oplus U_2 = M$, so heißen U_1, U_2 *komplementär* zueinander.
Aus formalen Gründen wird der Nulluntermodul als direkte Summe über die leere Familie von Untermoduln angesehen.

Die Bedingung „$\boldsymbol{u}_i = \mathbf{0}$ für fast alle $i \in I$“ können wir für endliche Familien $(U_i)_{i\in I}$ natürlich weglassen.

Bemerkung. Sind U_1 und U_2 Unterräume von M, so gilt genau dann $M = U_1 \oplus U_2$, wenn die folgenden beiden Bedingungen erfüllt sind: 0/3/19

(1) $U_1 + U_2 = M$,

(2) $U_1 \cap U_2 = \mathbf{0}$.

Vorsicht, für eine Familie aus mehr als zwei Untermoduln sieht die entsprechende Bedingung komplizierter aus!

Beweis. ($\Rightarrow$): (1) ist offensichtlich. Ist $0 \neq m \in U_1 \cap U_2$, so steht die Beziehung $0 = 0 + 0 = m + (-m)$ im Widerspruch zur Eindeutigkeit der Summenzerlegung, womit auch (2) folgt.
($\Leftarrow$): Es ist nur zu zeigen, dass für $m_1, m_1' \in U_1$ und $m_2, m_2' \in U_2$ aus $m_1 + m_2 = m_1' + m_2'$ stets $m_1 = m_1'$ und $m_2 = m_2'$ folgt. Die Voraussetzung ergibt $m_1 - m_1' = m_2' - m_2 \in U_1 \cap U_2 = \mathbf{0}$ und damit die Behauptung. ❑

Beispiele.

0. Ein R-Modul M besitzt stets die *triviale Zerlegung* $M \oplus \mathbf{0} = M$.
1. Ist R ein Körper, U ein Untermodul des R-Moduls M, so existiert stets ein Untermodul U' von M, der zu U komplementär ist. Dieser Satz sollte aus der linearen Algebra wohlbekannt sein ([RW], 3/2/2). ... eine keineswegs triviale Aussage!
2. Der Untermodul $U := \mathbb{Z} \cdot \overline{2}$ des $\mathbb{Z}$-Moduls $M := \mathbb{Z}/(4)$ besitzt keinen komplementären Untermodul. Warum?

Definition – Bemerkung. 0/3/20 $p : M \to M$ sei eine R-lineare Abbildung mit $p^2 = p$, dann heißt p *Projektion von* M *auf* $\mathrm{im}(p)$ *längs* $\ker(p)$ und es gilt

$$M = \ker(p) \oplus \mathrm{im}(p).$$

Beweis. Für $m \in M$ gilt $p\big(m - p(m)\big) = p(m) - p^2(m) = p(m) - p(m) = 0$, also ist in jeder Summe $m = \big(m - p(m)\big) + p(m)$ der erste Summand aus $\ker(p)$, d.h. $M = \ker(p) + \mathrm{im}(p)$. Weiter ist $\ker(p) \cap \mathrm{im}(p) = 0$, denn für alle Elemente m aus dem Durchschnitt gilt $m = p(m')$, wenn $m' \in M$ geeignet gewählt wird, sowie $\mathbf{0} = p(m) = p^2(m') = p(m') = m$. Die Behauptung ergibt sich nun aus der vorhergehenden Bemerkung. ❑

Dass tatsächlich jede direkte Zerlegung eines Moduls auf diese Weise entsteht, zeigt folgender

Satz. 0/3/21 *Ist* $M = U_1 \oplus U_2$, *dann existiert genau eine lineare Abbildung* $p : M \to M$ *mit* $p^2 = p$, *für die* $U_1 = \ker(p)$ *und* $U_2 = \mathrm{im}(p)$ *ist.*

Beweis. Falls eine solche Abbildung p existiert, muss für $m_1 \in U_1$ und $m_2 \in U_2$ gelten $p(m_1 + m_2) = p(m_1) + p(m_2) = 0 + m_2 = m_2$, denn für $m_2 \in U_2 = \mathrm{im}(p)$ ist wegen $p^2 = p$ stets $p(m_2) = m_2$.
Da für jeden Vektor $m \in M$ eindeutig bestimmte $m_1 \in U_1$ und $m_2 \in U_2$ mit $m = m_1 + m_2$ existieren, ist p durch die Bedingung $p(m_1 + m_2) = m_2$ vollständig beschrieben. Umgekehrt ist leicht zu sehen, dass auf diese Weise eine lineare Abbildung mit den geforderten Eigenschaften definiert wird, woraus die Existenz von p folgt. ❑

Diese Konstruktion begegnet uns bald noch allgemeiner als *Prinzip der linearen Fortsetzung.*

Lineare Fortsetzung 0/3/22

Eine R-lineare Abbildung lässt sich von den direkten Summanden eines Moduls auf diesen fortsetzen; das wird nun als allgemeines Prinzip formuliert.

Satz – Definition. *$(U_i)_{i\in I}$ sei eine Familie von Untermoduln des R-Moduls M und $M = \bigoplus_{i\in I} U_i$. Ist $(f_i)_{i\in I}$ eine Familie R-linearer Abbildungen $f_i : U_i \to M'$, dann existiert genau ein Homomorphismus $f : M \to M'$, dessen Einschränkungen auf die Untermoduln U_i die Abbildungen f_i sind.*
f heißt *lineare Fortsetzung* der Homomorphismen f_i auf M.

... wörtlich wie für Vektorräume, nur ist die Voraussetzung $M = \bigoplus_{i\in I} U_i$ hier selten erfüllt.

Beweis. Für $m \in M$ existieren eindeutig bestimmte $m_i \in U_i$, die fast alle 0 sind und für die $m = \sum_{i\in I} m_i$ ist. Falls eine lineare Abbildung $f : M \to M'$ mit der geforderten Eigenschaft existiert, muss $f(m_i) = f_i(m_i)$ sein, also gilt

$$(*) \qquad f(m) = \sum_{i\in I} f_i(m_i).$$

Umgekehrt ist leicht zu sehen, dass $(*)$ tatsächlich eine lineare Abbildung definiert. ❏

Lemma. *Ist $f : M = \bigoplus_{i\in I} U_i \to M'$ lineare Fortsetzung der Homomorphismen $f_i : U_i \to M'$, so gilt* 0/3/23

(1) $\mathrm{im}(f) = \sum_{i\in I} \mathrm{im}(f_i)$.

(2) *f ist genau dann injektiv, wenn alle Abbildungen f_i injektiv sind und $\mathrm{im}(f) = \bigoplus_{i\in I} \mathrm{im}(f_i)$ ist.*

(3) *f ist genau dann ein Isomorphismus, wenn alle f_i injektiv sind und $M' = \bigoplus_{i\in I} \mathrm{im}(f_i)$ ist.*

Beweis. (1) ist offensichtlich, wir zeigen (2). ($\Rightarrow$): Injektivität von f ist gleichbedeutend mit $\ker(f) = \mathbf{0}$. Aus $\ker(f_i) \subseteq \ker(f)$ folgt $\ker(f_i) = \mathbf{0}$, d.h. die Abbildungen f_i sind injektiv. Nun sei $m' = \sum_{i\in I} m'_i$ und $m'_i = f_i(m_i) \in \mathrm{im}(f_i)$, so ist $m' = f(\sum_{i\in I} m_i)$. Da f injektiv ist, wird durch m' das Urbild $\sum_{i\in I} m_i$ eindeutig bestimmt. m'_i ist Bild der i-ten Komponente m_i in $\oplus_{i\in I} U_i$ und daher durch m' eindeutig bestimmt. ($\Leftarrow$): Leicht kann $\ker(f) = \mathbf{0}$ verifiziert werden, womit sich Injektivität von f ergibt.
Die letzte Behauptung folgt aus (1) und (2). ❏

($\Leftarrow$) in (2) verbleibt als einfache Übungsaufgabe.

Definition. (*direkte Summe von Homomorphismen*) 0/3/24

$M = \bigoplus_{i\in I} U_i$ und $M' = \bigoplus_{i\in I} U'_i$ seien Moduln und $f_i : U_i \to U'_i$ R-lineare Abbildungen. Wir betrachten die Abbildungen f_i nach Hintereinanderausführung mit den Inklusionen $U'_i \subseteq M'$ als Homomorphismen $U_i \to M'$.
Der durch lineare Fortsetzung der Abbildungen f_i definierte Homomorphismus $f : M \to M'$ heißt *direkte Summe der Homomorphismen* f_i, er wird mit $\bigoplus_{i\in I} f_i$ bezeichnet. Im Fall einer endlichen Familie $(f_1, \ldots, f_m)$ verwenden wir vorzugsweise das Symbol $f_1 \oplus \ldots \oplus f_m$.

Aus Lemma 0/3/23 ergibt sich unmittelbar der folgende

Satz. (*Eigenschaften der linearen Fortsetzung*) 0/3/25

Ist $M = \bigoplus_{i\in I} U_i$, $M' = \bigoplus_{i\in I} U'_i$ und sind $f_i : U_i \to U'_i$ lineare Abbildungen mit der direkten Summe $f = \bigoplus_{i\in I} f_i : M \to M'$, so gilt:

(1) *f ist genau dann surjektiv, wenn alle f_i surjektiv sind.*

(2) *f ist genau dann injektiv, wenn alle f_i injektiv sind.*

(3) *f ist genau dann ein Isomorphismus, wenn alle f_i Isomorphismen sind.*

Wir konstruieren nun aus beliebigen Moduln einen neuen, der die gegebenen als direkte Summanden enthält. 0/3/26

Definition. (*äußere direkte Summe*)

$(M_i)_{i\in I}$ sei eine Familie von R-Moduln. Wir betrachten im direkten Produkt der Familie den Untermodul

$$\bigoplus_{i\in I} M_i := \left\{(\boldsymbol{v}_i)_{i\in I} \in \bigtimes_{i\in I} M_i \,\middle|\, \boldsymbol{v}_i = \mathbf{0} \ \text{ für fast alle } \ i \in I\right\};$$

er heißt *äußere direkte Summe* der R-Moduln M_i und wird für eine endliche Familie $(M_1, \ldots, M_m)$ auch mit $M_1 \oplus \ldots \oplus M_m$ bezeichnet.
Den Nullmodul betrachten wir als direkte Summe über die leere Familie.

Verwechseln Sie nicht die zuvor definierte „innere" mit der äußeren direkten Summe!

Das Prinzip der linearen Fortsetzung kann nun neu formuliert werden.

Satz. *Es gibt natürliche injektive Homomorphismen* $q_j : M_j \to \bigoplus_{i\in I} M_i$, *definiert durch* $q_j(\boldsymbol{v}) := (\boldsymbol{v}_i)_{i\in I}$ *mit* $\boldsymbol{v}_i := \boldsymbol{v}$ *für* $i = j$ *und* $\boldsymbol{v}_i = \mathbf{0}$ *für* $i \neq j$. *Durch die Familie* $(p_i)_{i\in I}$ *dieser Homomorphismen wird* $\bigoplus_{i\in I} M_i$ *zum Koprodukt in der Kategorie* $(\mathbf{mod}_R)$.

Wir identifizieren M_j und den Untermodul $\operatorname{im}(q_j)$ von $\bigoplus_{i\in I} M_i$, schreiben also künftig $M_j = \operatorname{im}(q_j)$. Dadurch wird auch die Bezeichnung gerechtfertigt:
Die äußere direkte Summe $\bigoplus_{i\in I} M_i$ *ist (im bisherigen Sinn) direkte Summe der Untermoduln* $\operatorname{im}(q_i)$, $i \in I$.

Bemerkung. 0/3/27

(1) M sei direkte Summe der Untermoduln U_i mit $i \in I$, so ist der durch lineare Fortsetzung der Identitäten $U_i \to U_i$ gegebene Homomorphismus $\bigoplus_{i\in I} U_i \to M$ der äußeren direkten Summe der U_i in den Modul M ein Isomorphismus.

(2) Für endliche Indexmengen stimmen äußere direkte Summe und direktes Produkt überein,

$$M_1 \oplus \ldots \oplus M_n = M_1 \times \ldots \times M_n .$$

(3) Ist $M_i = M$ für alle $i \in I$, so verwenden wir für die äußere direkte Summe anstelle von $\bigoplus_{i\in I} M_i$ auch das Symbol $M^{(I)}$.

Dies stimmt mit der in 0/3/18 verwendeten Bezeichnung überein.

Homomorphiesatz und Isomorphiesätze

Wir beschreiben nun R-lineare Abbildungen mit Hilfe des Homomorphieprinzips. Zunächst wird daran erinnert, dass die Faktorgruppe einer abelschen Gruppe $(M,+)$ nach einer Untergruppe U durch die Menge $M/U = \{\overline{m} \mid m \in M\}$ aller Klassen $\overline{m} = m + U$ beschrieben wird, wobei die für Gruppenoperation $\overline{m} + \overline{m'} = \overline{m + m'}$ gilt. Da Moduln definitionsgemäß eine Gruppenstruktur besitzen, ist der nun folgende Satz fast offensichtlich. 0/3/28

Satz – Definition. (*Faktorraum und kanonischer Homomorphismus*)

Für jeden Untermodul U *des* R*-Moduls* M *ist die kanonische surjektive Abbildung*

$$p : M \to M/U,\ m \mapsto m + U$$

linear, wenn mittels der Multiplikation

$$R \times M/U \longrightarrow M/U$$
$$(a, m + U) \mapsto a \cdot (m + U) := am + U$$

auf der Faktorgruppe M/U *die Struktur eines* R*-Moduls definiert wird.*
M/U heißt dann *Faktorraum* (auch *Quotientenraum*) von M nach U.
Der *kanonische Homomorphismus* p ist surjektiv und es gilt $\ker(p) = U$.

Der Faktormodul wird analog zur Faktorgruppe konstruiert.

Rechtfertigung. Wir haben zu zeigen, dass die Definition der Multiplikation von der Wahl der Repräsentanten unabhängig ist, denn es ist nicht von vornherein klar, ob $am+U$ unverändert bleibt, wenn m in der Klasse $m+U$ variiert.

Das ist ein ähnliches Problem wie bei der Konstruktion der Faktorgruppe.

Wir wählen dazu $m_1, m_2 \in M$, die zur selben Klasse in M/U gehören, d.h. $m_1 - m_2 \in U$. Multiplikation mit $a \in K$ ergibt $am_1 - am_2 = a(m_1 - m_2) \in U$, denn U ist Untermodul. Also liegen am_1 und am_2 ebenfalls in derselben Klasse bezüglich U. Die Verifikation der Modulaxiome für M/U bereitet nun keine Schwierigkeiten, und die Linearität des surjektiven Gruppenhomomorphismus p folgt aus der Definition der Multiplikation mit Skalaren. ❏

Noch allgemeiner zeigt sich, dass die nichtleeren Fasern beliebiger linearer Abbildungen Elemente eines Faktorraumes sind. Dazu können wir auf das entsprechende Prinzip für Gruppen zurückgreifen.

Satz. (*Homomorphiesatz*) 0/3/29

Ist $f : M \to M'$ eine R-lineare Abbildung, so existiert eine eindeutig bestimmte injektive R-lineare Abbildung $j : M/\ker(f) \to M'$ mit $f = j \cdot p$, wobei p den kanonischen Homomorphismus von M auf den Faktorraum $M/\ker(f)$ bezeichnet:

... zentraler Satz zur Klassifikation linearer Abbildungen; die später betrachteten „endlichdimensionalen“ Räume erlauben einfache Varianten.

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "p"'] & & M' \\ & M/\ker(f) \arrow[ur, "j"'] & \end{tikzcd}$$

Insbesondere gilt $\operatorname{im}(f) \cong M/\ker(f)$.

Beweis. j sei der eindeutig bestimmte Gruppenhomomorphismus mit $f = j \cdot p$ (vgl. [RW] 1/1/26). Für $m \in M$ muss dann $f(m) = (jp)(m) = j(m+U)$ sein, d.h. es bleibt zu zeigen, dass j mit der Multiplikation von Elementen aus R verträglich ist:

$$j\big(a \cdot (m+U)\big) = j(am+U) = f(am) = af(m) = a \cdot j(m+U)$$

für $a \in K$, $m \in M$. ❏

Korollar. (1. *Isomorphiesatz*) 0/3/30

Sind U_1, U_2 Untermoduln eines Moduls, so vermittelt die durch den kanonischen Homomorphismus p induzierte Abbildung

$$U_1 \xrightarrow{\subseteq} U_1 + U_2 \xrightarrow{p} (U_1+U_2)/U_2$$

einen Isomorphismus

$$U_1/(U_1 \cap U_2) \cong (U_1+U_2)/U_2.$$

Beweis. $f : U_1 \to (U_1+U_2)/U_2$ sei der obige Homomorphismus, entstanden durch Komposition der Inklusionsabbildung mit dem kanonischen Homomorphismus p. Dann ist $f(m_1) = m_1 + U_2$ für $m_1 \in U_1$ und daher f surjektiv. Wenden wir den Homomorphiesatz auf f an, so ergibt sich ein Isomorphismus

Offensichtlich ist hier $\ker(f) = U_1 \cap U_2$, denn aus $f(m) = 0$ folgt $m \in U_2$, daher $\ker(f) = U_1 \cap U_2$.

$$U_1/(U_1 \cap U_2) = U_1/\ker(f) \to \operatorname{im}(f) = (U_1+U_2)/U_2,$$

der die Klasse von $m_1 \in U_1$ auf $p(m_1)$ abbildet. ❏

Als Übungsaufgabe eignet sich die folgende „Kürzungsregel“.

Korollar. (2. *Isomorphiesatz*) 0/3/31

Sind U_1 und U_2 Untermoduln von U_3 und $U_1 \subseteq U_2$, so ist U_2/U_1 Kern der surjektiven linearen Abbildung

$$U_3/U_1 \to U_3/U_2, \quad m + U_1 \mapsto m + U_2,$$

die daher einen Isomorphismus $(U_3/U_1)/(U_2/U_1) \cong U_3/U_2$ induziert.

Wenden Sie den Homomorphiesatz auf $U_3/U_1 \to U_3/U_2$ an.

Das Korollar verallgemeinert in folgender Weise den Homomorphiesatz.

Bemerkung. (*Faktorisierung über Untermoduln des Kerns*) 0/3/32

Ist $f : M \to M'$ eine R-lineare Abbildung und $U \subseteq \ker(f)$ ein Untermodul, so faktorisiert f über den kanonischen Homomorphismus $M \to M/U$.

$$\begin{tikzcd}
 & M \arrow[rr, "f"] \arrow[d, dotted] \arrow[dr] & & M' \\
\ker(f)/U \arrow[r] & M/U \arrow[r] \arrow[urr, dotted] & M/\ker(f) \arrow[ur] &
\end{tikzcd}$$

Beweis. Wir wählen im vorigen Korollar $U_1 := U$, $U_2 := \ker(f)$, $U_3 := M$ und erhalten den Homomorphismus $M/U \to M/\ker(f)$, für den das Diagramm kommutiert. ❏

Leicht modifiziert lässt sich die Bemerkung auch so formulieren: f *faktorisiert genau dann über den kanonischen Homomorphismus $M \to M/U$, wenn* $U \subseteq \ker(f)$.

Definition. (*exakte Folge*) 0/3/33

Ein Diagramm

$$\cdots \longrightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \longrightarrow \cdots$$

in $(\mathbf{mod}_R)$ heißt *exakte* Folge, wenn für jedes dort auftretende Paar (f_i, f_{i+1}) aufeinander folgender Homomorphismen $\operatorname{im}(f_i) = \ker(f_{i+1})$ gilt.

Der Begriff wird in der homologischen Algebra verwendet.

Derartige Folgen eignen sich gut zur Beschreibung vertrauter Eigenschaften.

Bemerkung. 0/3/34

(1) Die Folge

$$\mathbf{0} \longrightarrow M \xrightarrow{f} M'$$

ist genau dann exakt, wenn f injektiv ist.

(2) Die Folge

$$M \xrightarrow{g} M' \longrightarrow \mathbf{0}$$

ist genau dann exakt, wenn g surjektiv ist.

(3) U sei ein Untermodul von M und $p : M \to M/U$ der kanonische Homomorphismus. Dann ist

$$\mathbf{0} \longrightarrow U \xrightarrow{\subseteq} M \xrightarrow{p} M/U \longrightarrow \mathbf{0}$$

eine exakte Folge.

Diese Sequenz heißt auch *exakte Folge zum Untermodul U*.

Beweis. (1) ist eine nur geringfügig modifizierte Form von 0/3/10 (3), denn das Bild der einzig möglichen Abbildung $\mathbf{0} \to M$ (Nullabbildung) ist der Nullunterraum. Unter (2) ist M' Kern der Abbildung $M' \to \mathbf{0}$, d.h. Exaktheit der Folge bedeutet $\mathrm{im}(p) = M'$. Zum Beweis der Eigenschaft (3) bleibt nur noch zu überlegen, warum $U = \ker(p)$ ist – dies folgt aus 0/3/28. ❑

Definition (*Kokern*) 0/3/35

Ist $f : M \to M'$ ein Homomorphismus, dann heißt $\mathrm{coker}(f) := M'/\mathrm{im}(f)$ der *Kokern* von f.

Folgende Eigenschaften zeigen, dass *Kern* und *Kokern* in $(\mathbf{mod}_R)$ zueinander duale Begriffe sind; sie werden durch die folgenden Universaleigenschaften beschrieben.

Satz. (*Universalität von Kern und Kokern*) 0/3/36

$f : M \to M'$ sei ein Homomorphismus.

(1) *Ist $j : U \to M$ die Inklusionsabbildung von $U := \ker(f)$ nach M, so gilt $f \cdot j = \mathbf{0}$, und für jeden Homomorphismus $j' : U' \to M$ mit $f \cdot j' = \mathbf{0}$ existiert genau ein Homomorphismus $s : U' \to U$ mit $j \cdot s = j'$.*
Durch diese Eigenschaften ist U bis auf Isomorphie eindeutig bestimmt.

... Übungsaufgabe. Diese Aussagen lassen sich auch auf allgemeinere Strukturen übertragen.

(2) *Ist $p : M' \to W := \mathrm{coker}(f)$ der kanonische Homomorphismus auf den Faktorraum nach $\mathrm{im}(f)$, so gilt $p \cdot f = \mathbf{0}$, und für jeden Homomorphismus $p' : M' \to W'$ mit $p' \cdot f = \mathbf{0}$ existiert genau ein Homomorphismus $t : W \to W'$ mit $t \cdot p = p'$.*
Durch diese Eigenschaften ist W bis auf Isomorphie eindeutig bestimmt.

Wir werden den Satz nicht verwenden und deuten den Beweis nur durch ein Diagramm an.

$$\begin{tikzcd}
U \arrow[r, "j"] & M \arrow[r, "f"] & M' \arrow[r, "p"] \arrow[dr, "p'"] & W \arrow[d, dotted, "t"] \\
U' \arrow[u, dotted, "s"] \arrow[ur, "j'"] & & & W'
\end{tikzcd}$$

Für jede lineare Abbildung erhalten wir durch ihren Kern und ihren Kokern auf natürliche Weise eine Folge von Homomorphismen. 0/3/37

Bemerkung. (*exakte Folge eines Homomorphismus*)

Ist $f : M \to W$ eine R-lineare Abbildung, so gibt es eine exakte Folge

$$\mathbf{0} \longrightarrow \ker(f) \xrightarrow{\subseteq} M \xrightarrow{f} W \xrightarrow{p} \mathrm{coker}(f) \longrightarrow \mathbf{0}.$$

Dabei bezeichnet $\subseteq$ die Inklusionsabbildung und p den kanonischen Homomorphismus.

Beweis. Wir können uns die obige Folge so vorstellen, dass zwei exakte Folgen zusammengefügt werden, die sich nach 3/2/18 (1), (2) ergeben: Aus

$$\mathbf{0} \longrightarrow \ker(f) \xrightarrow{\subseteq} M \xrightarrow{m \mapsto f(m)} \operatorname{im}(f)$$

und

$$\operatorname{im}(f) \xrightarrow{\subseteq} W \xrightarrow{p} \operatorname{coker}(f) \longrightarrow \mathbf{0}$$

bilden wir

$$\begin{tikzcd}
 & & & \operatorname{im}(f) \arrow[dr, dotted, "\subseteq"] & & & \\
\mathbf{0} \arrow[r] & \ker(f) \arrow[r, "\subseteq"] & M \arrow[ur, dotted] \arrow[rr, "f"] & & W \arrow[r, "p"] & \operatorname{coker}(f) \arrow[r] & \mathbf{0}.
\end{tikzcd}$$

❑