Daniel Plaumann
Technische Universität Dortmund
Sommersemester 2017

5. MODULN

Arbeitsblatt: Moduln vs. Vektorräume

Lesen Sie den Text sorgfältig und lösen Sie möglichst viele der Übungsaufgaben. Diskutieren Sie die Lösungen.

Der Unterschied zwischen Moduln und Vektorräumen kommt natürlich vom Unterschied zwischen Ringen und Körpern. Weil man in einem Ring R in der Regel nicht beliebig teilen kann, kann man die Elemente eines R-Moduls nicht beliebig reskalieren. Das macht einige ganz grundlegende Konzepte der linearen Algebra kaputt: Lineare Unabhängigkeit, Basen und Dimension.

Im folgenden ist wie immer R ein kommutativer Ring (mit Eins).

Definition. Es sei M ein R-Modul. Eine endliche Familie $x_1, \dots, x_n$ von Elementen in M heißt *R-linear unabhängig*, wenn sie die folgende Eigenschaft besitzt:

$$\forall a_1, \dots a_n \in R\Big(a_1x_1 + \cdots + a_nx_n = 0 \quad\Rightarrow\quad a_1 = \cdots = a_n = 0\Big).$$

Eine beliebige Familie ist linear unabhängig, wenn jede endliche Teilfamilie linear unabhängig ist. Eine **Basis** von M (über R) ist eine linear unabhängige Familie von Erzeugern. Ein R-Modul heißt **frei**, wenn er eine Basis besitzt.

Beispiel. Die Einheitsvektoren $e_1, \dots, e_n$ sind eine Basis von R^n. Allgemeiner hat jede direkte Summe

$$\bigoplus_{i \in I} R_i$$

mit $R_i = R$ für alle $i \in I$ eine Basis, deren Elemente die Tupel mit einer 1 an einer Stelle und 0 an allen anderen sind.

So weit ist das alles wie gewohnt. Es gelten zum Beispiel:

Übung 5.1. Sind $x_1, \dots, x_n$ linear unabhängig in einem R-Modul M, dann hat jedes Element im erzeugten Untermodul $\langle x_1, \dots, x_n \rangle$ eine eindeutige Darstellung als R-Linearkombination von $x_1, \dots, x_n$.

Übung 5.2. Seien M, N zwei R-Moduln.

(a) Ist $x_1, \dots, x_n$ eine Basis von M, dann gibt es zu jeder Wahl von $y_1, \dots, y_n \in N$ genau einen Homomorphismus $\varphi\colon M \to N$ mit $\varphi(x_i) = y_i$ für $i = 1, \dots, n$.

(b) Ist in (a) auch $y_1, \dots, y_n$ eine Basis von N, dann ist φ ein Isomorphismus.
(c) Zwei Moduln mit gleichlangen (endlichen) Basen sind isomorph.

(Die Beschränkung auf endliche Familien in diesen beiden Übungsaufgaben ist unwesentlich.)

Im allgemeinen braucht ein Modul allerdings keine Basis zu besitzen.

Übung 5.3. Für $R = \mathbb{Z}$ und $M = \mathbb{Z}/n$ gibt es überhaupt keine linear unabhängigen Familien.

Wir betrachten das Problem etwas abstrakter. Für einen Vektorraum V der Dimension n über einem Körper K entspricht die Wahl einer Basis der Wahl eines Isomorphismus mit K^n. So ist es auch bei freien Moduln.

Übung 5.4. Zur jeder Basis $x_1, \dots, x_n$ eines endlich-erzeugten freien R-Moduls M gehört ein Isomorphismus $M \xrightarrow{\sim} R^n$ und umgekehrt.

Anders gesagt, die Basis $x_1, \dots, x_n$ liefert eine Zerlegung von M in eine direkte Summe der Untermoduln $\langle x_i \rangle = R \cdot x_i$. Siehe dazu auch Aufgabe 22. Das führt zu der allgemeineren Frage, wann sich ein Modul überhaupt in Untermoduln zerlegen lässt.

Definition. Es sei M ein R-Modul und N ein Untermodul von M. Ein Untermodul N' von M heißt ein **Komplement** von N in M oder **komplementär zu** N, wenn

$$M = N + N' \quad \text{und} \quad N \cap N' = \{0\}$$

gelten.

In diesem Fall ist M isomorph zur direkten Summe $N \oplus N'$ und wir schreiben auch einfach $M = N \oplus N'$.

Aus Aufgabe 22 folgt: Genau dann gilt $M = N \oplus N'$, wenn jedes $x \in M$ eine eindeutige Darstellung

$$x = y + y' \quad \text{mit } y \in N, y' \in N'$$

besitzt. Aus der linearen Algebra ist bekannt:

Proposition 5.7. *Jeder Unterraum eines Vektorraums besitzt ein Komplement.*

Beweis. Ist K ein Körper, V ein K-Vektorraum und $U \subset V$ ein Unterraum, dann können wir eine Basis $\mathcal{B}_0$ von U wählen (Satz 3.2) und diese zu einer Basis $\mathcal{B} \supset \mathcal{B}_0$ von V verlängern (folgt ebenfalls aus Satz 3.2). Ist nun U' der von $\mathcal{B} \setminus \mathcal{B}_0$ aufgespannte Unterraum von V, dann ist U' ein Komplement von U in V. ∎

Übung 5.5. Überprüfen Sie die letzte Aussage im Beweis.

Eine andere Möglichkeit besteht darin, ein Skalarprodukt auf V zu definieren und das *orthogonale Komplement* von U in V zu bilden.

Übung 5.6. Welche komplementären Unterräume besitzt der Unterraum $U = \mathrm{Span}(e_1)$ in K^2?

Bei Moduln ist das nicht so:

Übung 5.7. Sei $R = \mathbb{Z}$, $M = \mathbb{Z}$ und $N = 2\mathbb{Z} = \{2m \mid m \in \mathbb{Z}\}$. Zeigen Sie, dass N kein Komplement in M besitzt.

Ein recht allgemeines Kriterium für die Existenz eines Komplements steckt in folgendem Lemma.

Lemma 5.8. *Für eine kurze exakte Sequenz*

$$0 \to N \xrightarrow{\varphi} M \xrightarrow{\psi} P \to 0$$

von R-Moduln sind äquivalent:
(1) Es gibt einen Homomorphismus $\sigma\colon M \to N$ mit $\sigma \circ \varphi = \mathrm{id}_N$.
(2) Es gibt einen Homomorphismus $\tau\colon P \to M$ mit $\psi \circ \tau = \mathrm{id}_P$.
In diesem Fall folgen $M = \varphi(N) + \tau(P)$ und $\varphi(N) \cap \tau(P) = \{0\}$, insbesondere $M \cong N \oplus P$.

Man sagt in diesem Fall, dass die kurze exakte Sequenz **spaltet**.

Beweis. (1)⇒(2): Sei $y \in P$ und wähle $x \in M$ mit $\psi(x) = y$. Setze

$$\tau(y) = x - \varphi(\sigma(x)).$$

Dann gilt $\psi(\tau(y)) = \psi(x - \varphi(\sigma(x))) = \psi(x) - 0 = \psi(x) = y$ wie gewünscht. Außerdem ist τ wohldefiniert: Denn ist $x' \in M$ mit $\psi(x') = y$, dann folgt $\psi(x - x') = 0$, also $x - x' \in \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$. Es gibt also $z \in N$ mit $\varphi(z) = x - x'$. Es folgt

$$\begin{aligned} x - \varphi(\sigma(x)) - (x' - \varphi(\sigma(x'))) &= x - x' - (\varphi(\sigma(x)) - \varphi(\sigma(x'))) = \varphi(z) - \varphi(\sigma(x - x')) \\ &= \varphi(z) - \varphi(\sigma(\varphi(z))) = \varphi(z) - \varphi(z) = 0. \end{aligned}$$

Weil φ und σ Homomorphismen sind, ist außerdem auch τ ein Homomorphismus.

(2)⇒(1): Für $x \in M$ gilt $\psi(x - \tau(\psi(x))) = 0$. Es gibt also eindeutig $y \in N$ mit $\varphi(y) = x - \tau(\psi(x))$. Setze $\sigma(x) = y$. Weil τ und ψ Homomorphismen sind, ist auch σ einer. Für $y \in N$ gilt außerdem $\tau(\psi(\varphi(y))) = \tau(0) = 0$ und deshalb $\sigma(\varphi(y)) = y$.

Wenn (2) erfüllt ist, dann können wir jedes $x \in M$ als

$$x = \big(x - \tau(\psi(x))\big) + \tau(\psi(x)) \tag{$*$}$$

schreiben. Dabei gilt $\psi(x - \tau(\psi(x))) = \psi(x) - \psi(x) = 0$. Der erste Summand in $(*)$ liegt also in $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi) = \varphi(\mathrm{N})$. Der zweite Summand liegt in $\tau(P)$. Ist $x \in \varphi(N) \cap \tau(P)$, etwa $x = \varphi(y) = \tau(z)$, so folgt $\psi(x) = \psi(\varphi(y)) = 0$ und damit $z = \psi(\tau(z)) = \psi(x) = 0$, also $x = \tau(0) = 0$.

Man beachte, dass φ und τ injektiv sind (warum?) und $\varphi(N)$ und $\tau(P)$ damit isomorph zu N bzw. P. Es folgt also $M \cong N \oplus P$. ∎

Korollar 5.9. *Es sei M ein R-Modul, $N \subset M$ ein Untermodul. Genau dann besitzt N ein Komplement in M, wenn die kurze exakte Sequenz*

$$0 \to N \to M \to M/N \to 0$$

(mit der Inklusion $N \subset M$ bzw. der Restklassenabbildung $M \to M/N$) spaltet.

Beweis. Wenn N ein Komplement N' besitzt, dann ist also $\alpha\colon N \oplus N' \to M$, $(y, y') \mapsto y + y'$ ein Isomorphismus. Ist $\pi\colon N \oplus N' \to N$, $(y, y') \mapsto y$ die Projektion auf den ersten Faktor, dann ist $\sigma = \pi \circ \alpha^{-1}\colon M \to N$ ein Homomorphismus mit $\sigma \circ \varphi = \mathrm{id}_N$, so dass die Sequenz spaltet.

Wenn die Sequenz umgekehrt spaltet, dann ist $\tau(M/N)$, mit τ wie im Lemma, ein Komplement von N. ∎

Übung 5.8. Jede exakte Sequenz

$$0 \to U \xrightarrow{\varphi} V \xrightarrow{\psi} W \to 0$$

von Vektorräumen über einem Körper K spaltet. (*Hinweis:* Wähle ein Komplement von $\varphi(U)$.)