Kapitel 7

Moduln

Wir hatten bereits gesehen, dass sich viele Überlegungen für Ringe und Körper ähneln, aber es auch gravierende Unterschiede gibt. In der Linearen Algebra hatten wir das Konzept eines Vektorraumes über einem Körper eingehend betrachtet. Was passiert, wenn wir in der Definition eines Vektorraums alles beibehalten und nur die Voraussetzung, dass der Grundkörper ein Körper ist abschwächen zu einem Ring oder zu einem Integritätsring oder zu einem Hauptidealring? Vieles gilt dann weiterhin, aber nicht nur Nullteiler werden uns dabei das Leben schwer machen, sondern das Fehlen von Inversen von Einträgen oder Koeffizienten wird darüberhinaus die naive Übertragung vieler Methoden für Vektorräume auf Moduln selbst über so 'gutmütigen' Ringen wie Hauptidealringen verhindern.

Moduln sind die Objekte, die dieselben Axiome erfüllen wie Vektorräume, jedoch über einem Ring gebildet werden. Wir werden daher zuerst einmal soviele Begriffe und Notationen aus der Linearen Algebra in die neue Situation hinüberretten und immer genau auf die neuen Phänome achten, die uns begegnen. In diesem Sinne ist das vorliegende Kapitel nochmal ein Schnelldurchlauf durch den roten Faden der Linearen Algebra.

Ehe wir in das Kapitel starten, möchte ich noch eine grammatikalische Warnung geben: Es heißt in der Algebra 'der Modul' und gemeint ist das Objekt, das in der ersten Definition eingeführt wird. Sagt man 'das Modul', so spricht man von einem Baustein eines Studienganges oder einer größeren technischen Apparatur.

7.1 Vom Vektorraum zum Modul

In diesem Abschnitt lohnt es sich, wenn man die Aufzeichnungen aus der Linearen Algebra daneben legt und vergleicht.

Definition 7.1.1 *Sei R ein kommutativer Ring (wie immer mit 1) und sei $M \neq \emptyset$ eine Menge. M heißt ein R-**Modul**, falls es eine innere Verknüpfung (Vektoraddition)*

$$\begin{aligned} + : M \times M &\longrightarrow M \\ (v, w) &\longmapsto v + w \end{aligned}$$

und eine äußere Verknüpfung (Skalarmultiplikation)

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ (\lambda, v) &\longmapsto \lambda \cdot v \end{aligned}$$

gibt, so dass:

(A) $(M, +)$ *abelsche Gruppe*

(S1) $\forall v \in M : \quad 1_R \cdot v = v$

(S2) $\forall \lambda, \mu \in R \ \ \forall v \in M : \quad \lambda(\mu \cdot v) = (\lambda\mu) \cdot v$

(S3) $\forall \lambda \in R \ \ \forall v, w \in M : \quad \lambda(v + w) = \lambda \cdot v + \lambda \cdot w$

(S4) $\forall \lambda, \mu \in R \ \ \forall v \in M : \quad (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$

Analog zum Vektorraumfall sprechen wir auch bei Moduln oft von **Vektoren** $v \in M$ und von **Skalaren** $\lambda \in R$.

Bemerkung 7.1.2 *Bei der Definition der Verknüpfungen wurde bereits implizit die Wohldefiniertheit der Abbildungen und die Abgeschlossenheit in M gefordert, ohne diese nochmals explizit als Bedingung aufzuführen. Die Definition eines Moduls entspricht bis auf die zum Übergang auf Ringe notwendigen Änderungen strukturell genau der Definition eines Vektorraums aus der Linearen Algebra (WS19/20).*

Lemma 7.1.3 *(Rechenregeln) Sei R ein kommutativer Ring und M ein R-Modul. Dann gilt:*

a) $\forall v \in M: \quad 0_R \cdot v = 0_M$

b) $\forall \lambda \in R: \quad \lambda \cdot 0_M = 0_M$

c) $\forall \lambda \in R \ \ \forall v \in M: \quad (-\lambda) \cdot v = -(\lambda \cdot v) = \lambda \cdot (-v)$

d) $\lambda \cdot v = 0 \Longrightarrow (v = 0 \ \textit{oder} \ \lambda \notin R^*)$

Sehen sie in Ihren Aufzeichnungen zur Linearen Algebra nach und vergleichen Sie mit den Rechenregeln für Vektorräume. Was wurde geändert und warum? Denken sie an Nullteiler.
Machen Sie sich klar, dass die Rechenregeln für Vektorräumen nichts anderes als Spezialfälle für die Rechenregeln für Moduln sind und auch im Modulfall die Beweise in exakt derselben Weise – mit der offensichtlichen Veränderung – geführt werden können.

Definition 7.1.4 *Sei R ein kommutativer Ring und seien M, N zwei R-Moduln. Eine Abbildung $\phi : M \longrightarrow N$ heißt* **R-linear** *(oder* **R-Modul-Homomorphismus***), falls*

$$\forall \lambda_1, \lambda_2 \in R \ \ \forall v_1, v_2 \in M : \phi(\lambda_1 \cdot_M v_1 +_M \lambda_2 \cdot_M v_2) = \lambda_1 \cdot_N \phi(v_1) +_N \lambda_2 \cdot_N \phi(v_2).$$

Eine R-lineare Abbildung ist also verträglich mit der R-Modulstruktur.

Beispiel 7.1.5 *Sei R ein kommutativer Ring und sei $A \in R^{m \times n}$ eine Matrix mit Einträgen aus R. Dann ist durch*

$$\begin{array}{rcl} F_A : R^{n \times 1} & \longrightarrow & R^{m \times 1} \\ x & \longmapsto & Ax \end{array}$$

ein R-Modul-Homomorphismus gegeben. Auch hier ist die Argumentation exakt analog zum Fall von Vektorräumen.

Lemma 7.1.6 *Sei R ein kommutativer Ring und sei $\phi : M \longrightarrow N$ ein R-Modul-Homomorphismus. Dann gilt:*

a) $\phi(0_M) = 0_N$

b) $\forall v \in M: \quad \phi(-v) = -\phi(v)$

Wieder läuft der Beweis exakt analog zu dem der Aussage in der Linearen Algebra und bleibt den Studierenden überlassen.

Bemerkung 7.1.7 *Die üblichen Begriffsbildungen für Homomorphismen existieren selbstverständlich auch für R-Modul-Homomorphismen. So ist zu einem gegebenen R-Modul-Homomorphismus $\phi : M \longrightarrow N$*

$$\begin{aligned} \ker(\phi) &:= \{v \in M \mid \phi(v) = 0_N\} \\ \mathrm{Im}(\phi) &:= \{y \in N \mid \exists v \in M \text{ mit } \phi(v) = y\}. \end{aligned}$$

Wie auch für andere Objekte und deren Morphismen üblich, sprechen wir bei einem injektiven R-Modul-Homomorphismus von einem R-Modul-Monomorphismus, bei Surjektivität von einem R-Modul-Epimorphismus und bei Bijektivität von einem R-Modul-Isomorphismus. Ein R-Modul-Homomorphismus mit $M = N$ heißt R-Modul-Endomorphismus; ist er zusätzlich bijektiv, so spricht man von einem R-Modul-Automorphismus.

Satz 7.1.8 *Sei R ein kommutativer Ring und sei $\phi : M \longrightarrow N$ ein R-Modul-Homomorphismus. Dann gilt:*

a) ϕ *Monomorphismus* $\Longleftrightarrow \ker(\phi) = \{0\}$

b) ϕ *Epimorphismus* $\Longleftrightarrow \mathrm{Im}(\phi) = N$

Auch hier hindert uns nichts daran, den Beweis aus der Linearen Algebra direkt zu übernehmen. Sehen Sie es sich einmal genau an.

Entsprechend des üblichen Vorgehens bei der Definition von Unterstrukturen einer gegebenen Struktur, können wir auch Untermoduln definieren.

Definition 7.1.9 *Sei R ein kommutativer Ring und sei M ein R-Modul. Eine Teilmenge $\emptyset \neq N \subseteq M$ heißt* **Untermodul**, *falls sie ein R-Modul bzgl. der Vektoraddition in M und der Skalarmultiplikation ist.*

Können Sie ein Untermodul-Kriterium formulieren? Sie dürfen beim Unterraum-Kriterium spicken.

Definition 7.1.10 *Sei R ein kommutativer Ring, sei M ein R-Modul und sei $V = (v_i)_{i \in I}$ eine nicht-leere Familie von Elementen aus M mit Indexmenge I. Dann heißt jede Summe*

$$\sum_{i \in I} \lambda_i v_i,$$

*für die $\lambda_i \in R$ für alle $i \in I$ und $\lambda_i = 0$ für alle bis auf endlich viele $i \in I$ gilt, eine R-***Linearkombination** *von V.*
Der **von V aufgespannte Untermodul** *ist die Menge*

$$\langle V \rangle_R := span_R(V) = \{w \in M \mid w \text{ } R\text{-Linearkombination von } V\}.$$

Eine R-Linearkombination heißt **trivial**, *falls $\lambda_i = 0$ für alle $i \in I$.*
Ist $M = \langle V \rangle_R$, so heißt V **Erzeugendensystem** *von M.*

Definition 7.1.11 *Sei R ein kommutativer Ring und sei M ein R-Modul. M heißt* **endlich erzeugt**, *falls es ein $n \in \mathbb{N}_0$ und eine Familie $V = (v_1, \ldots, v_n)$ mit $v_i \in M$ für alle $1 \leq i \leq n$ gibt, so dass $M = \langle V \rangle_R$.*
Für ein $x_1 \in M$, heißt $\langle x_1 \rangle_R$ der von x_1 erzeugte **zyklische Untermodul** *von M.*

Bis hierhin ist uns nichts wirklich Unerwartetes in der Theorie der Moduln begegnet. Wir konnten den Definitionen für Vektorräume direkt folgen und sahen auch jeweils die erwarteten ersten Folgerungen daraus. Bei der nun folgenden Linearen Unabhängigkeit wird die Situation etwas unbersichtlicher.

Definition 7.1.12 *Sei R ein kommutativer Ring und M ein R-Modul. Eine Familie V von Elementen aus M heißt* **linear unabhängig über** *R, falls einzig die triviale R-Linearkombination der Elemente der Familie 0_M liefert. Ansonsten ist V* **linear abhängig**.

Beispiel 7.1.13 *Sei $R = K[x, y]/\langle xy \rangle$. Dann sind die Vektoren $(x, 0)^T$ und $(0, y)^T$ in $M = R^2$ linear abhängig, denn*

$$y \cdot \begin{pmatrix} x \\ 0 \end{pmatrix} + x \cdot \begin{pmatrix} 0 \\ y \end{pmatrix} = 0_M.$$

Nehmen Sie sich die Zeit, dieses Beispiel genau zu betrachten und zu überlegen, was genau hier anders ist als im Fall eines Vektorraums über einem Körper.

Definition 7.1.14 *Sei R ein kommutativer Ring und sei M ein R-Modul. Eine nicht-leere Familie V von Elementen aus M heißt eine Basis von M über R, falls gilt:*

a) $M = span_R(V)$

b) V ist linear unabhängig über R.

Besitzt ein R-Modul M eine Basis über R, so heißt er **freier** *Modul.*

Beispiel 7.1.15 *$\mathbb{Z}/\langle 2\rangle$ ist ein freier $\mathbb{Z}/\langle 2\rangle$-Modul mit Basis $[1]_2$.*
$\mathbb{Z}/\langle 2\rangle$ ist als $\mathbb{Z}$-Modul nicht frei, da $2 \cdot [1]_2 = [0]_2$.
Überlegen Sie auch hier genau, was der Unterschied ist bzw. was genau schiefgeht. Nur so erkennen Sie die subtilen Probleme, die wir durch das Zulassen von beliebigen kommutativen Ringen statt Körpern neu antreffen.

Satz 7.1.16 *Sei R kommutativer Ring und M ein R-Modul. Dann ist eine nicht-leere Familie $V = (v_i)_{i\in I}$ von Elementen $v_i \in M$ genau dann eine Basis von M, wenn für jedes $a \in M$ eine eindeutige Darstellung als R-Linearkombination existiert.*

Beweis: Da V den R-Modul M genau dann erzeugt, wenn jedes $a \in M$ sich als R-Linearkombination von Elementen von V darstellen läßt, bleibt zum Beweis der Aussage nur zu zeigen, dass die R-lineare Unabhängigkeit genau dann gegeben ist, wenn die Darstellung für jedes $a \in M$ eindeutig ist. Ist die Darstellung jedes Elements aus M eindeutig, so ist insbesondere die Darstellung von 0_M eindeutig, was R-lineare Unabhängigkeit impliziert. Besitzt umgekehrt ein $a \in M$ zwei unterschiedliche Darstellungen als R-Linearkombination, so bildet deren Differenz eine nicht-triviale Darstellung von 0_M als R-Linearkombination aus (endlich vielen) Elementen aus V, weswegen V nicht R-linear unabhängig sein kann.

□

Bemerkung 7.1.17 *Wegen der eindeutigen Darstellung jedes Elements eines freien R-Modul bzgl. einer gegebenen Basis ist ein R-Modul-Homomorphismus zwischen zwei freien Moduln bereits durch Angabe der Bilder der Basiselemente eindeutig festgelegt. Dies gilt genau analog zum Fall von Vektorräumen.*

Warnung 7.1.18 *Über Körpern läßt sich aus jedem endlichen Erzeugendensystem eines K-Vektorraums V eine Basis auswählen (Basisauswahlsatz). Über Ringen ist das offensichtlich nicht möglich, da z.B. im zweiten Teil von Beispiel 7.1.15 keine $\mathbb{Z}$-Basis von $\mathbb{Z}/\langle 2\rangle$ existiert. Der einzige von Null verschiedene Vektor des Moduls liefert keine linear unabhängige Familie.*
Weiterhin kann über Körpern jede Familie linear unabhängiger Vektoren eines K-Vektorraums V zu einer Basis ergänzt werden (Basisergänzungssatz).

Über Ringen gilt das nicht mehr, denn (2) *ist eine $\mathbb{Z}$-linear unabhängige Familie in $M = \mathbb{Z}^1$, jedoch erzeugt sie $\mathbb{Z}^1$ nicht als $\mathbb{Z}$-Modul, obwohl es keinen weiteren Vektor aus $\mathbb{Z}^1$ gibt, mit dem 2 eine linear unabhängige Familie bildet. Beachten Sie, dass $2 \cdot a - a \cdot 2 = 0$, wobei jeweils der erste Faktor als Element aus $R = \mathbb{Z}$ und der zweite als Element aus $M = \mathbb{Z}^1$ aufzufassen ist. Jeder K-Vektorraum besitzt eine Basis und ist somit ein freier K-Modul. Dies gilt offensichtlich nicht für Moduln über einem Ring.*

Besitzt ein R-Modul M eine Basis, d.h. ist M frei, so kann er mit dem Modul R^m identifiziert werden:

Satz 7.1.19 *Sei R ein kommutativer Ring und M ein R-Modul mit Basis $V = (b_1, \ldots, b_m)$, so ist die Abbildung*[1]

$$\begin{array}{rcl} I_V : M & \longrightarrow & R^{m\times 1} \\ b_i & \longmapsto & e_i \text{ für } 1 \leq i \leq m \end{array}$$

ein R-Modulisomorphismus mit Inversem

$$\begin{array}{rcl} \Phi_V : R^{m\times 1} & \longrightarrow & M \\ e_i & \longmapsto & b_i \text{ für } 1 \leq i \leq m. \end{array}$$

Der Beweis folgt auch hier (wie im Vekotrraumfall) direkt aus der Überprüfung der Homomorphismuseigenschaft sowie dem Nachrechnen von $I_V \circ \Phi_V = Id_{R^{m\times 1}}$ und $\Phi_V \circ I_V = Id_M$.

Betrachten wir nun eine etwas speziellere Klasse von kommutativen Ringen: Integritätsringe. Wir setzen also zusätzlich Nullteilerfreiheit voraus. Diese Annahme ermöglicht es uns die Beweise in recht einfacher Art zu führen. Auch schon für Moduln über kommutativen Ringen haben zwei Basen desselben Moduls über demselben Ring stets die selbe Länge, aber dies erfordert mehr einen aufwendigeren Beweis (siehe z.B. Hungerford, Algebra, Kapitel VI.2).

Satz 7.1.20 *Sei R ein Integritätsring und M ein R-Modul mit endlicher Basis der Länge m. Dann erfüllt jede Familie $(x_1, \ldots, x_n)$ von R-linear unabhängigen Elementen aus M die Ungleichung $n \leq m$.*

[1] Wegen Bemerkung 7.1.17 reicht es, nur die Bilder der Basis anzugeben und die Bilder aller weiteren Elemente durch lineare Fortsetzung zu erhalten.

Beweis: Nach Satz 7.1.19 reicht es zu zeigen, dass $m+1$ Elemente in R^m stets linear abhängig sind. Dies zeigen wir durch Induktion nach m.
Als Induktionsanfang für $m = 1$ seien $(a), (b) \in R^1$. Dann ist $b \cdot (a) - a \cdot (b) = 0_{R^1}$, weshalb die beiden Vektoren linear abhängig sind.
Unter der Induktionsvoraussetzung, dass die Behauptung für m gilt, seien für den Induktionsschritt

$$v_1 = \begin{pmatrix} v_{1,1} \\ \vdots \\ v_{1,m} \end{pmatrix}, \ldots, v_{m+1} = \begin{pmatrix} v_{m+1,1} \\ \vdots \\ v_{m+1,m} \end{pmatrix}$$

$m+1$ Vektoren in R^m. Sind $v_{i,m} = 0$ für alle $1 \leq i \leq m+1$, so liegen alle $v_1, \ldots, v_{m+1}$ im Bild der kanonischen Inklusion des R^{m-1} in den R^m und sind daher bereits nach Induktionsvoraussetzung linear abhängig. Daher können wir nach Umsortieren oBdA annehmen, dass $v_{m+1,m} \neq 0$. Für $1 \leq i \leq m$ gilt nun:

$$w_i := v_{m+1,m} \cdot v_i - v_{i,m} \cdot v_{m+1} = \begin{pmatrix} v_{m+1,m}v_{i,1} - v_{i,m}v_{m+1,1} \\ \vdots \\ v_{m+1,m}v_{i,m-1} - v_{i,m}v_{m+1,m-1} \\ 0 \end{pmatrix}.$$

Diese m Vektoren $w_1, \ldots, w_m$ liegen wiederum alle im Bild der kanonischen Inklusion des R^{m-1} in den R^m und sind daher nach Induktionsvoraussetzung linear abhängig. Es gibt also $\lambda_1, \ldots, \lambda_m \in R$, von denen mindestens eines von Null verschieden ist, mit $\sum_{i=1}^{m} \lambda_i w_i = 0$. Damit gilt:

$$\left(\sum_{i=1}^{m} \lambda_i v_{m+1,m} \cdot v_i \right) - \left(\sum_{i=1}^{m} \lambda_i v_{i,m} \right) v_{m+1} = 0,$$

was eine nicht-triviale Linearkombination der Null ist. Die Vektoren $v_1, \ldots, v_{m+1}$ sind also linear abhängig, was zu zeigen war.

□

Haben Sie bemerkt, dass dies genau dasselbe Argument ist wie bei Vektorräumen mit dem einzigen Unterschied, dass wir hier das Teilen durch Elemente von R vermeiden mussten.

Korollar 7.1.21 *Sei R ein Integritätsring und sei M ein R-Modul, der eine endliche Basis besitzt. Dann haben je zwei Basen von M (als R-Modul) die gleiche Länge.*

Beweis: Beide Basen sind linear unabhängig. Damit kann nach dem vorigen Satz keine der beiden größere Länge haben als die jeweils andere.

□

Definition 7.1.22 *Sei R ein Integritätsring und sei M ein R-Modul, der eine endliche Basis besitzt. Dann heißt die Länge einer Basis von M der* **Rang** *von M, kurz* $\operatorname{rang}(M)$.

Satz 7.1.23 *Sei R ein Hauptidealring und sei M ein freier R-Modul vom Rang $m < \infty$. Dann ist auch jeder Untermodul von M frei vom Rang $\leq m$.*

Beweis: Der Beweis erfolgt durch Induktion nach dem Rang m von M.
Sei zum Induktionsanfang $m = 1$. Dann ist $M \cong R$ und wegen der Hauptidealringeigenschaft von R ist jeder Untermodul von M, d.h. jedes Ideal in R, von einem Element erzeugt (das wegen der Nullteilerfreiheit von R linear unabhängig über R ist, sofern es nicht Null ist) und hat damit eine Basis aus höchstens einem Element.
Unter der Induktionsvoraussetzung, dass die Behauptung für Untermoduln von Moduln vom Rang $m-1$ gilt, zeigen wir nun im Induktionsschritt die Behauptung für einen Untermodul N eines R-Modul M vom Rang m. Betrachte dazu eine Basis $(v_1, \ldots, v_m)$ von M und den R-Modul-Homomorphismus

$$\begin{array}{rcl} \pi_m : M & \longrightarrow & \langle v_m \rangle_R \cong R \\ a = \sum_{i=1}^{m} a_i v_i & \longmapsto & a_m v_m. \end{array}$$

Dann ist $\operatorname{Im}(\pi_m)$ der von v_m erzeugte freie Modul vom Rang 1 und der Untermodul $\ker(\pi_m) \subseteq M$ der Untermodul $L = \langle v_1, \ldots, v_{m-1} \rangle_R \subseteq M$, der selbst frei vom Rang $m-1$ ist.
Betrachten wir nun

$$\begin{array}{rcl} \pi_m \mid_N : N & \longrightarrow & \langle v_m \rangle_R \\ w & \longmapsto & \pi_m(w) \end{array}$$

Dann ist $\mathrm{Im}(\pi_m \mid_N) = \pi_m(N)$ ein Untermodul des freien Moduls $\langle v_m \rangle_R \cong R$ vom Rang 1 und damit nach Induktionsanfang selbst frei vom Rang höchstens 1. Ist der Rang Null, so liegt N im Kern von π_m und ist nach Induktionsvoraussetzung frei vom Rang $\leq m-1$. Ist der Rang 1, so besitzt $\pi_m(N)$ eine einelementige Basis, sagen wir (w_m).
Betrachten wir nun $\ker(\pi_m \mid_N) = \{\sum_{i=1}^{m} b_i v_i \in N \mid b_m = 0\} = N \cap L$. Dieser Modul ist als Untermodul des freien Moduls L selbst frei, sagen wir mit Basis $(w_1, \ldots, w_s)$ mit $s \leq m-1$.
Nach dem Homomorphiesatz gilt nun

$$N/(L \cap N) \cong \pi_m(N).$$

Wählen wir ein Repräsentantensystem $\mathcal{O}$ für $N/(L \cap N)$, ist dieses nach Konstruktion bijektiv zu $\pi_m(N) = \langle w_m \rangle_R$ und so besitzt demnach jedes Element $w \in N$ eine Darstellung als $w = r + s$ für geeignete $r \in \mathcal{O}$ und $s \in L \cap N$.
Da wegen der linearen Unabhängigkeit von $v_1, \ldots, v_m$ insbesondere $L \cap \langle v_m \rangle_R = \{0\}$, sind auch $(w_1, \ldots, w_s, r_m)$ R-linear unabhängig, wobei r_m das zu w_m korrespondierende Element von $\mathcal{O}$ ist. Damit ist eine Basis von N aus höchstens m Elementen gefunden und die Behauptung bewiesen.

□

Bemerkung 7.1.24 *Die Konstruktion eines Faktormoduls und des zugehörigen Restklassenhomomorphismus ist genau analog zur Konstruktion, die wir in Abschnitt 4.4 für Faktorräume von Vektorräumen kennengelernt haben. Auch die Isomorphiesätze (Abschnitt 4.5) lassen sich direkt vom Vektorraumfall auf den Modulfall übertragen. Wir haben bereits Faktorstrukturen von 3 verschiedenen Objekten – Gruppen, Ringe, Vektorräume – in der Vorlesung kennengelernt. Versuchen Sie, selbst die korrekte Definition des Faktormoduls inklusive der induzierten Verknüpfungen zu formulieren und überprüfen Sie, dass im Modulfall im Beweis des Homomorphiesatzes keine (im Vergleich zum Vektorraumfall neuen) Probleme auftreten.*