Algebra 2

Sommersemester 2018

Universität Heidelberg

Dr. Denis Vogel

Letzte Aktualisierung: 16. April 2018

Mitschrieb von Jonas Wildberger und Celine Fietz

Dies ist eine inoffizielle Version. Es können daher Fehler vorkommen.

Inhaltsverzeichnis

1 Moduln

In dieser Vorlesung steht die Bezeichnung "Ring" stets für einen (nicht notwendig kommutativen) Ring mit 1. In diesem Kapitel sei R ein Ring.

1.1 Grundlagen über Moduln

Definition 1.1.1. *Ein "R-Linksmodul" ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung $R \times M \to M$, $(a,x) \mapsto ax$ (skalare Multiplikation), sodass für alle $a,b \in R$, $x,y \in M$ gilt:*

a) $a(x+y) = ax + ay$

b) $(a+b)x = ax + bx$

c) $a(bx) = (ab)x$

d) $1x = x$

Ein "R-Rechtsmodul" ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung $M \times R \to M$, $(x,a) \mapsto xa$, sodass für alle $a,b \in R$, $x,y \in M$ gilt:

a′) $(x+y)a = xa + yb$

b′) $x(a+b) = xa + xb$

c′) $x(ab) = (xa)b$

d′) $x1 = x$

Anmerkung: Es bezeichne R^{op} den zu R entgegengesetzten Ring, d.h. eine Menge R mit derselbern Addition, sowie der Multiplikation $a \cdot_{\text{op}} b := b \cdot a$. Ist M ein $R-$Rechtsmodul, dann wird M durch $ax := xa$ zu einem R^{op}-Linksmodul, denn es gilt

$$a(bx) = (bx)a = (xb)a = x(ba) = (ba)x = (a \cdot_{\text{op}} b)x \quad \text{für alle } a,b \in R,\ x,a \in M$$

Analog anders herum. Im Folgenden betrachten wir in der Regel nur R-Linksmoduln, und unter einem R-Modul verstehen wir einen R-Linksmodul

- Forderung a) impliziert, dass für alle $a \in R$ die Abbildung

  $$l_a : M \to M, \quad x \mapsto ax$$

  zum Ring $\text{End}(M)$ aller Gruppenhomomorphismen $M \to M$ gehört.

  $$(\text{mit } (f+g)(x) := f(x) + g(x),\ (f \cdot g) := (f \circ g)(x) = f(g(x))$$

für $f, g \in \operatorname{End}(M)$, $x \in M$). Nach $b) - d)$ ist die Abbildung $\varphi : R \to \operatorname{End}(M)$, $a \mapsto l_a$ ein Ringhomomorphismus. Umgekehrt macht jeder Ringhomomorphismus $\varphi : R \to \operatorname{End}(M)$ eine abelsche Gruppe $(M, +)$ zu einem R-Modul via $ax := \varphi(a)(x)$

- Für alle $x \in M$ ist $0x = 0$, $(-1)x = -x$, und für alle $a \in R$ ist $a0 = 0$

Beispiel 1.1.2: a) Ist K ein Körper, dann sind K-Moduln die K-Vektorräume.

b) Jede abelsche Gruppe G ist ein $\mathbb{Z}$-Modul via

$$\mathbb{Z} \times G \to G, \quad (n, x) \mapsto nx := \begin{cases} \underbrace{x + \ldots x}_{\text{n-mal}} & n > 0 \\ 0 & n = 0 \\ -(\underbrace{x + \ldots + x}_{\text{(-n)-mal}}) & n < 0 \end{cases}$$

Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$ (analog zur Algebra 1), insbesondere gibt es für jede abelsche Gruppe G genau einen Ringhomomorphismus $\mathbb{Z} \to \operatorname{End}(G)$, d.h. genau eine Struktur als $\mathbb{Z}-$Modul, sodass die Moduladdition mit der gegebenen Addition auf G überein einstimmt (nämlich obige).

Definition 1.1.3. *Seien M, M' R-Moduln, $\varphi : M \to M'$. Dann heißt φ "R-Modulhomomorphismus"(R-linear), wenn für alle $x, y \in M$, $a, b \in R$ gilt:*

a) $\varphi(x + y) = \varphi(x) + \varphi(y)$

b) $\varphi(ax) = a\varphi(x)$

$Hom_R(M, M')$ bezeichne die Menge der R-Modulhomomorphismen von M nach M'.

Anmerkung: $\operatorname{Hom}_R(M, M')$ ist eine abelsche Gruppe bezüglich $(f + g)(x) := f(X) + g(x)$ für $f, g \in \operatorname{Hom}_R(M, M')$, $x \in M$

Beispiel 1.1.4: Sei M ein R-Modul, $\varphi \in \operatorname{Hom}_R(M, M) =: \operatorname{End}_R(M) \subseteq \operatorname{End}_{\mathbb{Z}}(M) = \operatorname{End}(M)$. Den Polynomring $R[X]$ kann man wie über kommutativen Ringen definieren, allerdings ist die Einsetzungsabbildung

$$R[X] \to R, \quad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i b^i, \quad \text{für ein } b \in R$$

im Allgemeinen kein Ringhomomorphismus ("X vertauscht mit Elementen aus R, b im Allgemeinen nicht"). Die Abbildung

$$\Psi : R[X] \to \mathrm{End}(M), \quad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i \varphi^i$$

ist ein Ringhomomorphismus, da φ R-linear ist. Somit wird M zum $R[X]$-Modul.

Definition 1.1.5. *Seien M, M' R-Moduln, $\varphi : M \to M'$ R-linear. φ heißt*

"Monomorphismus" $\overset{Def}{\Leftrightarrow}$ φ ist injektiv (Notation: $M \hookrightarrow M'$)

"Epimorphismus" $\overset{Def}{\Leftrightarrow}$ φ ist surjektiv (Notation: $M \twoheadrightarrow M'$)

"Isomorphismus" $\overset{Def}{\Leftrightarrow}$ φ ist bijektiv (Notation: $M \overset{\sim}{\to} M'$)

Existiert ein Isomorphismus zwischen M, M', so heißen M, M' "isomorph" (Notation: $M \cong M'$)

Anmerkung: Ist φ ein Isomorphismus, dann ist φ^{-1} ein Isomorphismus.

Bemerkung 1.1.6. *Seien M, M' R-Moduln. Dann gilt:*

a) R kommutativ $\Rightarrow$ $Hom_R(M, M')$ ist ein R-Modul via $(a\varphi)(x) := a\varphi(x)$ für $a \in R$, $\varphi \in Hom_R(M, M')$, $x \in M$.

b) $End_R(M) = Hom_R(M, M)$ ist ein Unterring von $End(M) = End_{\mathbb{Z}}(M)$.

c) Die Abbildung $\Phi : Hom_R(R, M) \to M$, $\varphi \mapsto \varphi(1)$ ist ein Isomorphismus von abelschen Gruppen (hierbei ist R auf natürliche Weise ein R-Linksmodul). Ist R kommutativ, so ist Φ ein Isomorphismus von R-Moduln.

d) $End_R(R) \cong R^{op}$

Beweis. a) Beachte: Für $a \in R$, $\varphi \in \mathrm{Hom}_R(M, M')$ ist $a\varphi$ wieder $R-$linear, denn für $a, b \in R$, $x \in M$ ist $(a\varphi)(bx) = a\varphi(bx) = ab\varphi(x) = ba\varphi(x) = b(a\varphi)(x)$

b) Nachrechnen.

c) Eine Umkehrabbildung zu Φ ist gegeben durch

$$\Psi : M \to \mathrm{Hom}_R(R, M), \quad m \mapsto (\varphi : R \to M,\ a \mapsto am)$$

d) Nach Aussage *c*) haben wir sofort einen Isomorphismus: $\Phi : \mathrm{End}_R(R) \to R$, $\varphi \mapsto \varphi(1)$ von abelschen Gruppen. Es ist

$$\begin{aligned}\Phi(\varphi\psi) &= (\varphi\psi)(1) = \varphi(\psi(1)) = \varphi(\psi(1)\cdot 1) = \psi(1)\varphi(1)\\ &= \varphi(1)\cdot_{\mathrm{op}}\psi(1) = \Phi(\varphi)\cdot_{\mathrm{op}}\Phi(\psi)\end{aligned}$$

□

Definition 1.1.7. *Sei M ein R-Modul, $N \subseteq M$. N heißt R-Untermodul von M, wenn gilt:*

a) $0 \in N$

b) $x + y \in N$ *für alle* $x, y \in N$

c) $ax \in N$ *für alle* $a \in R, x \in N$

Beispiel 1.1.8: a) Betrachte R als R-Linksmodul. Dann sind die Untermodul von R genau die Linksideale in R (analog: Rechtsideale für R als R-Rechtsmodul).

b) Ist M ein R-Modul, dann sind $\{0\}$ (meist als 0 geschrieben) und $M \subseteq M$ die trivialen Untermoduln. Ist $(M_i)_{i\in I}$ eine Familie von Untermoduln von M, dann ist $\bigcap_{i\in I} M_I \subseteq M$ ein Untermodul, sowie $\sum_{i\in I} M_i = \{\sum_{i\in I} x_i |\, x_i \in M_i,\, x_i = 0$ für fast alle $i \in I\}$

c) Sind M, M' R-Moduln, $\varphi \in \mathrm{Hom}_R(M, M')$, $N \subseteq M$ ein Untermodul, $N' \subseteq M'$ ein Untermodul, dann sind $\varphi(N) \subseteq M'$ und $\varphi^{-1}(N') \subseteq M$ Untermoduln.

$\mathrm{im}\,\varphi := \varphi(M)$ heißt das "Bild" von φ

$\ker\varphi := \varphi^{-1}(\{0\})$ heißt der "Kern" von φ

Es gilt: φ ist injektiv $\Leftrightarrow \ker\varphi = 0$ und φ surjektiv $\Leftrightarrow \mathrm{im}\,\varphi = M'$

Bemerkung + Definition 1.1.9. *Sei M ein R-Modul, $N \subseteq M$ ein Untermodul. Dann ist die Faktorgruppe ${}^{M}\!/\!_{N}$ via $a(x+N) = ax + N$, $a \in R$, $x \in M$ ein R-Modul,der "Faktormodul" von M nach N. Die kanonische Abbildung $\pi : M \to {}^{M}\!/\!_{N}$, $m \mapsto m + N$ ist ein Modulepimorphismus mit* $\ker\pi = N$.

Beispiel 1.1.10: Sei $I \subseteq R$ ein Linksideal, M ein R-Modul. Dann ist

$$IM := \left\{\sum_{i=1}^{n} a_i x_i |\, n \in \mathbb{N},\, a_i \in I,\, x_i \in M\right\} \subseteq M$$

ein Untermodul von M. Ist I ein zweisetiges Ideal, dann ist ${}^{R}\!/_{I}$ ein Ring (beachte: Die Zweiseitigkeit von I geht ein bei der Wohldefiniertheit der Multiplikation

$$ {}^{R}\!/_{I} \times {}^{R}\!/_{I} \longrightarrow {}^{R}\!/_{I}, \quad (a+I, b+I) \mapsto ab + I $$

${}^{M}\!/_{IM}$ ist ein ${}^{R}\!/_{I}$−Modul vermöge

$$ (a+I)(x+M) := ax + IM, \quad a \in R,\, x \in M $$