Inhaltsverzeichnis

1 Moduln

1.1 Definitionen und grundlegende Tatsachen

Definition 1.1.1. Ein *Modul* ist ein Tupel $(R, +_R, \cdot_R, M, +, \cdot)$, wobei $(R, +_R, \cdot_R)$ ein Ring (mit 1, nicht notwendigerweise kommutativ), $(M, +)$ eine abelsche Gruppe und $\cdot : R \times M \to M$ eine (meist gar nicht oder infix geschriebene) Abbildung mit folgenden Eigenschaften

$(\vec{D})$ $\forall a \in R : \forall x, y \in M : a(x + y) = ax + ay$ „distributiv"

(D') $\forall a, b \in R : \forall x \in M : (a + b)x = ax + bx$ „distributiv"

(N) $\forall x \in M : 1_R \cdot x = x$ „normiert"

(V) $\forall a, b \in R : \forall x \in M : (ab)x = a(bx)$ „verträglich"

Bemerkung 1.1.2. (a) Schlampiger Sprachgebrauch:

- „Sei M ein R-Modul" statt „Sei $(R, +_R, \cdot_R, M, +, \cdot)$ ein Modul"
- „Sei M ein Modul" statt „Es gebe einen Ring R so, dass M ein R-Modul ist"

(b) Statt „R-Modul" sagt man auch „Modul über R"

(c) Vektorräume sind Moduln über Körper. Viele Sprechweisen (wie „Skalar", „Linearkombination", nicht jedoch „Vektor") übertragen wir stillschweigend von Vektorräumen auf Moduln, ebenso Konventionen (wie „Punkt vor Strich").

(d) Abelsche Gruppen „sind" $\mathbb{Z}$-Moduln. Sei G eine abelsche Gruppe. Dann gibt es genau eine Skalarmultiplikation $\cdot : \mathbb{Z} \times G \to G$ vermöge derer G zu einem $\mathbb{Z}$-Modul wird, nämlich die natürliche, die durch

$$n \cdot a := \begin{cases} \underbrace{a + a + \cdots + a}_{n\text{-mal}} & \text{falls } n > 0 \\ 0 & \text{falls } n = 0 \\ \underbrace{-a - a - \cdots - a}_{(-n)\text{-mal}} & \text{falls } n < 0 \end{cases}$$

gegeben ist.

(e) $(\overrightarrow{D})$ besagt, dass für alle $a \in R$ die Abbildung $M \to M, x \mapsto ax$ ein Gruppenhomomorphismus ist. Insbesondere gilt $a \cdot 0 = 0$ und $a \cdot (-x) = -ax$ für alle $a \in R, x \in M$.

(D') besagt, dass für alle $x \in M$ die Abbildung $R \to M, a \mapsto ax$ ein Gruppenhomomorphismus ist. Insbesondere gilt $0 \cdot x = 0$ und $(-a) \cdot x = -ax$ für alle $a \in R, x \in M$.

Beispiele 1.1.3. (a) Nullmoduln $\{0\}$

(b) Sei A ein Unterring des Ringes B. Dann ist B ein A-Modul vermöge der Skalarmultiplikation $\cdot : A \times B \to B, (a, x) \mapsto ax$

Insbesondere ist jeder Ring ein Modul über sich selbst.

(c) Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$. Dann wird die abelsche Gruppe R^n zu einem $R^{n\times n}$-Modul vermöge der Skalarmultiplikation

$$\cdot : R^{n\times n} \times R^n \to R^n, (A, x) \mapsto Ax$$

Dies folgt aus den Rechenregeln für Matrixmultiplikation.

Definitionen, Propositionen, Sätze und Notationen 1.1.4. Sei R ein Ring. Die folgenden für die Theorie der R-Moduln grundlegenden Begriffe und Resultate sind eine direkte Verallgemeinerung der entsprechenden Tatsachen für Vektorräume (also für den Fall, dass R ein Körper) und für abelsche Gruppen (also $R = \mathbb{Z}$) aus der Linearen Algebra:

(a) Genauso wie bei Vektorräumen führt man *direkte Produkte* von R-Moduln ein.

(b) Sind M und N R-Moduln, so heißt N ein *Untermodul* von M, wenn die N zugrunde liegende abelsche Gruppe eine Untergruppe der M zugrunde liegenden abelschen Gruppe ist und

$$\forall a \in R : \forall x \in M : a \cdot_N x = a \cdot_M x$$

Ein Untermodul eines Moduls ist offenbar durch seine Trägermenge (d.h. seine zugrunde liegende Menge) eindeutig bestimmt.

Ist M ein R-Modul und $N \subseteq M$, so ist N offenbar genau dann (Trägermenge) ein(e) Untermodul(s) von M, wenn $0 \in N, \forall x, y \in N : x + y \in N, \forall a \in R : \forall x \in N : ax \in N$

(c) Sei M ein Modul und $(N_i)_{i\in I}$ eine Familie von Untermoduln von M. Dann ist $\bigcap_{i\in I} N_i := \bigcap \{N_i | i \in I\}$ (mit $\bigcap_{i\in I} N_i = M$, falls $I = \emptyset$) wieder ein Untermodul von M und zwar der größte Untermodul von M, der in allen N_i enthalten ist.

Weiter ist auch $\sum_{i\in I} N_i := \left\{\sum_{i\in I} x_i | (x_i)_{i\in I} \in \prod_{i\in I} N_i, \{i \in I | x_i \neq 0\} \text{ endlich}\right\}$ Untermodul von M und zwar der kleinste Untermodul von M, der alle N_i enthält.

(d) Sei M ein R-Modul. Ist $x \in M$, so ist $Rx := \{ax | a \in R\}$ ein Untermodul von M und zwar der kleinste Untermodul, der x enthält.

Ist $(x_i)_{i \in I}$ eine Familie von Elementen von M, so ist $\sum_{i \in I} Rx_i$ der kleinste Untermodul von M, der alle x_i enthält.

Man nennt ihn den von den x_i $(i \in I)$ (oder $\{x_i | i \in I\}$) erzeugten Untermodul von M (oder lineare Hülle der Span von $\{x_i | i \in I\}$).

Man nennt M *zyklisch*, wenn M von einem Element erzeugt wird, d.h. es ein $x \in M$ gibt mit $M = Rx$. Man nennt M endlich erzeugt (e.e.), wenn M von endlich vielen Elementen erzeugt wird, d.h. es ein $n \in \mathbb{N}_0$ und $x_1, \ldots, x_n \in M$ gibt mit

$$M = Rx_1 + \cdots + Rx_n := \sum_{i=1}^{n} Rx_i := \sum_{i \in \{1,\ldots,n\}} Rx_i$$

(e) Sei M ein R-Modul. Eine Familie $(x_i)_{i \in I}$ in M heißt *linear unabhängig* (l.u.), wenn für alle $n \in \mathbb{N}_0$, alle paarweise verschiedenen $i_1, \ldots, i_n \in I$ und alle $a_1, \ldots, a_n \in I$ gilt

$$\sum_{j=1}^{n} a_j x_{i_j} = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Weiter nennt man $x_1, \ldots, x_n$ linear unabhängig, wenn $(x_1, \ldots, x_n) = (x_i)_{i \in \{1,\ldots,n\}}$ linear unabhängig ist, d.h. für alle $a_1, \ldots, a_n \in R$ gilt

$$(1) \qquad a_1 x_1 + \cdots a_n x_n = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Schließlich heißt eine Menge $F \subseteq M$ linear unabhängig, wenn $(x)_{x \in F}$ linear unabhängig ist, d.h. für alle $n \in \mathbb{N}_0$, alle paarweise verschiedenen $x_1, \ldots, x_n \in F$ und alle $a_1, \ldots, a_n \in R$ wieder 1 gilt.

(f) Sei M ein Modul. Eine Familie $(x_i)_{i \in I}$ in M heißt eine *Basis* von M, wenn sie M erzeugt und linear unabhängig ist. Weiter sagt man $x_1, \ldots, x_n \in M$ bilden eine Basis von M, wenn $(x_1, \ldots, x_n) = (x_i)_{i \in \{1,\ldots,n\}}$ eine Basis von M ist. Schließlich heißt $B \subseteq M$ eine Basis, wenn B den Modul M erzeugt und linear unabhängig ist.

(g) Seien M und N R-Moduln. Dann heißt f ein *(R-)(Modul-)Homomorphismus* oder eine $(R-)$ lineare Abbildung von M nach N, wenn $f : M \to N$ ein Gruppenhomomorphismus der M und N zugrundeliegenden abelschen Gruppen ist und

$$\forall a \in R : \forall x \in M : f(ax) = af(x)$$

Ein Modulhomomorphismus $f : M \to N$ heißt Einbettung/Monomorphismus (Epimorphismus, Isomorphismus), wenn f injektiv (surjektiv, bijektiv) ist.

Ein Modulhomomorphismus $f : M \to M$ heißt *(Modul-)Endomorphismus* von M. Ein Endomorphismus, der ein Isomorphismus ist, heißt *Automorphismus*. Es heißen

M und N *isomorph*, in Zeichen $M \cong N$, wenn es einen Isomorphismus $M \to N$ gibt.

Hintereinanderschaltungen von Modulhomomorphismen sind wieder Modulhomomorphismen. Umkehrabbildungen von Modulisomorphismen sind wieder Modulisomorphismen.

(h) Sei M ein R-Modul. Eine *Kongruenzrelation* auf M ist eine Äquivalenzrelation $\equiv$ der M zugrundeliegenden Menge, für die gilt

$$\forall x, y, x', y' \in M : (x \equiv x' \wedge y \equiv y') \Rightarrow x + y \equiv x' + y'$$

und

$$\forall x, x' \in M : \forall a \in R : x \equiv x' \Rightarrow ax \equiv ax'$$

Diese Definition wurde gerade so gemacht, dass

$$+ : (M/\equiv) \times (M/\equiv) \to (M/\equiv), (\overline{x}, \overline{y}) \mapsto \overline{x+y}$$

und

$$\cdot : R \times (M/\equiv) \to (M/\equiv), (a, \overline{x}) \mapsto \overline{ax}$$

wohldefiniert sind.

Ist M ein R-Modul und $\equiv$ eine Kongruenzrelation auf M, so wird die Quotientenmenge $M/\equiv$ vermöge der Addition $+$ und der Skalarmultiplikation $\cdot$ ein R-Modul, wie man durch direktes Nachrechnen sieht. Die Zuordnungen

$$\equiv \overset{f}{\mapsto} \overline{0}$$
$$\equiv_N \overset{g}{\mapsfrom} N$$

vermitteln eine Bijektion zwischen der Menge der Kongruenzrelationen auf M und der Menge der Untermoduln von M, wobei $\equiv_N$ gegeben ist durch

$$a \equiv_N b :\Leftrightarrow a - b \in N$$

für $a, b \in M$.

Ist N ein Untermodul von M, so nennt man $M/N := M/\equiv_N$ auch den *Quotientenmodul* von M nach N.

(i) Sind M und N R-Moduln und $f : M \to N$ ein Modulhomomorphismus, so ist der *Kern* $\ker f := \{x \in M | f(x) = 0\}$ von f ein Untermodul von M und das *Bild* $\operatorname{im} f := \{f(x) | x \in M\}$ von f ist ein Untermodul von N.

(j) Homomorphiesatz: Seien M und N R-Moduln und L ein Untermodul von M und $f : M \to N$ ein Modulhomomorphismus mit $L \subseteq \ker f$. Dann gibt es (genau) einen Modulhomomorphismus $\overline{f} : (M/L) \to N$ mit $\overline{f}(\overline{x}) = f(x)$ für alle $x \in M$.

Ferner gilt, dass

- $\overline{f}$ ist injektiv $\Leftrightarrow L = \ker f$ und
- $\overline{f}$ ist surjektiv $\Leftrightarrow f$ ist surjektiv

(k) Isomorphiesatz: Seien M und N R-Moduln und $f : M \to N$ ein Modulhomomorphismus. Dann ist $\overline{f} : (M/\ker f) \to \operatorname{im} f$ definiert durch $\overline{f}(\overline{x}) = f(x)$ für alle $x \in M$ ein R-Modulisomorphismus. Insbesondere ist $M/\ker f \cong \operatorname{im} f$

Bemerkung 1.1.5. Sei R ein kommutativer Ring. Dann sind die Untermoduln des R-Modul R [$\to$1.1.3(b)] (oder kurz gesagt die R-Untermoduln von R) genau die Ideale des Ringes R. Insbesondere sind zum Beispiel das von einem $a \in R$ erzeugte Ideal und der davon erzeugte Untermodul als Menge dasselbe $(a)_R = Ra \overset{R \text{ komm.}}{=} \{ab | b \in R\} = aR$. Trotzdem macht es vom Sinn her einen Unterschied. ob man (a) oder Ra schreibt. Zum Beispiel meint man mit $R/(a)$ den Ring und mit R/aR den R-Modul (deren zugrundeliegenden abelschen Gruppen dieselben sind)

Warnung 1.1.6. Für den mit Vektorräumen, aber nicht mit Moduln vertrauten Hörern ist Vorsicht geboten:

(a) In einem R-Modul M kann $ax = 0$ für ein $a \in R$ und ein $x \in M$ gelten, ohne dass $a = 0$ oder $x = 0$ gilt (zum Beispiel $2 \cdot \overline{1} = \overline{2} = 0$ im $\mathbb{Z}$-Modul $\mathbb{Z}/2\mathbb{Z}$)

(b) Nicht jeder Modul hat eine Basis: zum Beispiel ist jedes Element des $\mathbb{Z}$-Moduls $\mathbb{Z}/2\mathbb{Z}$ linear abhängig, denn $1 \cdot \overline{0} = \overline{0} = 0$ und $2 \cdot \overline{1} = \overline{2} = 0$ in $\mathbb{Z}/2\mathbb{Z}$, womit die einzige linear unabhängige Teilmenge von $\mathbb{Z}/2\mathbb{Z}$ die leere Menge is, welche aber $\mathbb{Z}/2\mathbb{Z}$ nicht erzeugt.

Beispiele 1.1.7. (a) Für jeden Ring R ist R^n ein R-Modul mit der *Standardbasis* $\underline{e} = (e_1, \dots, e_n)$, wobei $e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ mit einer 1 an der i-ten Stelle.

(b) $\mathbb{R}^2$ ist ein zyklischer $\mathbb{R}^{2\times 2}$ Modul [$\to$1.1.3(c)], welcher von jedem $x \in \mathbb{R}^{2\times 2} \setminus \{0\}$ erzeugt ist. Da aber jedes $x \in \mathbb{R}^{2\times 2}$ linear abhängig ist, hat dieser Modul keine Basis.

1.2 Direkte Summen von Moduln und freie Moduln

Definition 1.2.1. Sei R ein Ring und $(M_i)_{i\in I}$ eine Familie von R-Moduln. Dann nennt man den R-Untermodul

$$\bigoplus_{i\in I} M_i := \left\{ x \in \prod_{i\in I} M_i | \operatorname{supp}(x) \text{ endlich} \right\}$$

von $\prod_{i\in I} M_i$ *die (äußere) direkte Summe* der M_i $(i \in I)$. Man fasst M_j $(j \in I$ häufig) als Untermodul von $\bigoplus_{i\in I} M_i$ auf vermöge der Einbettung

$$\rho_j : M_j \to \prod_{i\in I} M_i, x \mapsto \left(i \mapsto \begin{cases} x & \text{falls } i = j \\ 0 & \text{sonst} \end{cases} \right)$$

Ist $M_i = M$ für alle $i \in I$, so schreibt man

$$M^{(I)} := \bigoplus_{i\in I} M \subseteq \prod_{i\in I} M = M^I$$

Proposition 1.2.2. Sei R ein Ring, $(M_i)_{i\in I}$ eine Familie von Modulhomomorphismen $f_i : M_i \to N$. Dann gibt es genau einen Modulhomomorphismus $f : \bigoplus_{i\in I} M_i \to N$ mit $f\big|_{M_i} = f_i$ für alle $i \in I$ $(f \circ \rho_i = f_i$ für $i \in I)$.

Beweis. Für jedes $x \in \bigoplus_{i\in I} M_i$ gilt $x = \sum_{i\in \operatorname{supp}(x)} \rho_i(x(i))$. Um $f \circ \rho_i = f_i$ für $i \in I$ zu erfüllen, kann man daher nur

$$f : \bigoplus_{i\in I} M_i \to N, x \mapsto \sum_{i\in I} f_i(x(i))$$

definieren. Man überprüft sofort, dass das so definierte f ein Homomorphismus ist. □

Proposition und Definition 1.2.3. Sei R ein Ring, M ein R-Modul und $(N_i)_{i\in I}$ eine Familie von Untermoduln on M. Dann sind die folgenden Bedingungen äquivalent

(a) Die Abbildung von der äußeren direkten Summe $\bigoplus_{i\in I} N_i$ nach M, die auf N_i die Identität ist, ist ein Isomorphismus

(b) $M = \sum_{i\in I} N_i$ und für alle $n \in \mathbb{N}$, paarweise verschiedenen $i_1, \dots, i_n \in I$ und alle $x_1 \in N_{i_1}, \dots, x_n \in N_{i_n}$ gilt

$$(x_1 + \cdots + x_n = 0) \Rightarrow (x_1 = \cdots = x_n = 0)$$

Gelten diese Bedingungen, so nennt man M die *(innere) direkte Summe* der N_i $(i \in I)$ und schreibt (angesichts der Isomorphismus aus (a)) wieder $M = \bigoplus_{i\in I} N_i$

Definition 1.2.4. Sei R ein Ring, M ein R-Modul und $x \in M$. Der Kern des R-Modulhomomorphismus $R \to M, a \mapsto ax$ nennt man *Annihilator* von x, in Zeichen $\operatorname{ann}(x) = \{a \in R | ax = 0\}$.
Es heißt x ein *Torsionselement* von M wenn $\operatorname{ann}(x) \neq \{0\}$.

Satz 1.2.5. Sei R ein Ring, M ein R-Modul und $B \subseteq M$. Dann sind äquivalent

(a) B ist eine Basis von M

(b) $M = \bigoplus_{x \in B} Rx$ und B enthält kein Torsionselement

(c) Für jeden R-Modul N und jede Abbildung $g : B \to N$ gibt e genau einen Homomorphismus $f : M \to N$ mit $f\big|_b = g$.

Beweis.

$(a) \Rightarrow (b)$ klar

$(b) \Rightarrow (c)$ Gelte (b). Sei N ein R-Modul und $g : B \to N$ eine Abbildung. Zu zeigen sind Existenz und Eindeutigkeit eines Homomorphismus $f : M \to N$ mit $f\big|_B = g$

- Eindeutigkeit: klar aus $M = \sum_{x \in B} Rx$
- Existenz: Fixiere zunächst $x \in B$. Dann ist $R \to Rx, a \mapsto ax$ ein Isomorphismus (mit Kern $\operatorname{ann}(x)$), dessen Umkehrfunktion ein Isomorphismus $Rx \to R$ ist, der x auf 1 abbildet. Schaltet man den Homomorphismus $R \to N, a \mapsto ag(x)$ dahinter, so erhält man einen Homomorphismus $Rx \to N$, der x auf $g(x)$ abbildet. Da $x \in B$ beliebig war, erhält man mit 1.2.2 einen Homomorphismus $f : M = \bigoplus_{x \in B} Rx \to N$, der jedes $x \in B$ auf $g(x)$ abbildet.

$(c) \Rightarrow (a)$ Gelte (c). Zu zeigen ist, dass B linear unabhängig ist und M erzeugt.

1. B linear unabhängig: Seien $x_1, \dots, x_n \in B$ paarweise verschieden und $a_1, \dots, a_n \in R$ mit $a_1x_1 + \dots + a_nx_n = 0$. Sei $i \in \{1, \dots, n\}$. Zu zeigen ist $a_i = 0$. Gemäß(c) gibt es einen Homomorphismus $f : M \to R$ mit $f(x_i) = 1$ und $f(x_j) = 0$ für $j \in \{1, \dots, n\} \setminus \{i\}$. Dann
$$0 = f(0) = f\left(\sum_{j=1}^{n} a_j x_j\right) = \sum_{j=1} a_j f(x_j) = a_i f(x_i) = a_i$$
2. B erzeugt M: Nach (c) gibt es einen Homomorphismus $M \to M$, der auf B die Identität ist. Einerseits ist id_M ein solcher, andererseits auch $\rho \circ f$, wobei $f : M \to N := \sum_{x \in B} Rx$ der nach (c) existierende Homomorphismus mit $f\big|_B = \mathrm{id}_B$ ist und $\iota : N \hookrightarrow M, x \mapsto x$ die Inklusion. Also $\mathrm{id}_M = \iota \circ f$, insbesondere $M = \operatorname{im}(\mathrm{id}_M) = \operatorname{im}(f) = N$

$\square$

Definition 1.2.6. Ein Modul heißt *frei*, wenn er eine Basis besitzt.

Bemerkung 1.2.7. Sei R ein Ring, M ein R-Modul, $n \in \mathbb{N}_0$ und $x_1, \dots, x_n \in M$. Dann bilden $x_1, \dots, x_n$ genau dann eine Basis von M, wenn der Homomorphismus
$$R^n \to M, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^{n} a_i x_i$$
ein Isomorphismus ist.

Bemerkung 1.2.8. Ist M ein $\{0\}$-Modul, so ist $M = \{0\}$, denn ist $x \in M$, so ist $x = 1 \cdot x = 0 \cdot x = 0$

Lemma 1.2.9. Ein endlich erzeugter Modul hat niemals eine unendliche Basis.

Beweis. Sei M ein endlich erzeugter R-Modul, etwa $M = \sum_{i=1}^{n} Rx_i$ mit $x_1, \ldots, x_n \in M$. Annahme: B ist eine unendliche Basis von M. Dann gibt es für jedes $i \in \{1, \ldots, n\}$ ein endliches $B_i \subseteq B$ mit $x_i \in \sum_{y \in B_i} Ry$. Dann ist $B' := B_1 \cup \cdots \cup B_n \subseteq B$ endlich mit $M = \sum_{y \in B'} Ry$. Da B unendlich h ist, gibt es ein $z \in B \setminus B'$

Nun gilt $z \in \sum_{y \in B'} Ry$, was im Widerspruch zur linearen Unabhängigkeit von B steh, außer wenn $1 = 0$ in R, d.h. $R = \{0\}$. Im letzten Fall ist aber nach 1.2.8 nichts zu zeigen. □

Bemerkung 1.2.10. (a) Jeder Modul über dem Nullring hat genau zwei Basen, nämlich $\emptyset$ und $\{0\}$. In der Tat: Nach 1.2.8 handelt es sich um den Nullmodul und in einem $\{0\}$-Modul ist 0 linear unabhängig.

(b) In den Übungen geben wir einen Ring $R \neq 0$, der als R-Modul zu R^2 isomorph ist. Durch Induktion schließt man, dass $R \cong R^n$ für alle $n \in \mathbb{N}$. Damit besitzt R als R-Modul für jedes $n \in \mathbb{N}$ eine n-elementige Basis, aber nach 1.2.9 keine unendliche Basis.

Satz 1.2.11. Sei R ein kommutativer Ring mit $1 \neq 0$. Dann sind je zwei Basen eines R-Moduls entweder beide unendlich oder beide endlich mit der selben Anzahl von Elementen

Beweis. Sei M ein R-Modul mit Basen B und C. Im Fall von $|B| = \infty = |C|$ sind wir fertig, sonst ist M endlich erzeugt und daher $m = |B|, n = |C| \in \mathbb{N}_0$ nach Lemma 1.2.9. Nach 1.2.7 gilt $R^n \cong M \cong R^m$, somit reicht es zu zeigen: Sei R ein kommutativer Ring und $m, n \in \mathbb{N}_0, m > n$ mit $R^m \cong R^n$ als R-Modul, dann gilt $1 = 0$ in R. □

Index