

---

# Inhaltsverzeichnis

---

<b>1</b>	<b>Moduln</b>	<b>1</b>
1.1	Definitionen und grundlegende Tatsachen . . . . .	1
1.2	Direkte Summen von Moduln und freie Moduln . . . . .	6
1.3	Halbeinfache Moduln . . . . .	11



---

# 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  $\cdot : R \times M \rightarrow M$  eine (meist gar nicht oder infix geschriebene) Abbildung mit folgenden Eigenschaften

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

$$(D') \quad \forall a, b \in R : \forall x \in M : (a + b)x = ax + bx \quad \text{„distributiv“}$$

$$(N) \quad \forall x \in M : 1_R \cdot x = x \quad \text{„normiert“}$$

$$(V) \quad \forall a, b \in R : \forall x \in M : (ab)x = a(bx) \quad \text{„verträglich“}$$

**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  $\cdot : \mathbb{Z} \times G \rightarrow G$  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)  $\vec{D}$  besagt, dass für alle  $a \in R$  die Abbildung  $M \rightarrow M, x \mapsto ax$  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  $R \rightarrow M, a \mapsto ax$  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  $\cdot : A \times B \rightarrow B, (a, x) \mapsto ax$

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

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

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 *Unterm modul* 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 Unterm modul 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) Unterm modul(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 Unterm odulen 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 Unterm modul von  $M$  und zwar der größte Unterm modul von  $M$ , der in allen  $N_i$  enthalten ist.

Weiter ist auch  $\sum_{i \in I} N_i := \{\sum_{i \in I} x_i | (x_i)_{i \in I} \in \prod_{i \in I} N_i, \{i \in I | x_i \neq 0\} \text{ endlich}\}$  Unterm modul von  $M$  und zwar der kleinste Unterm modul 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  $x_1, \dots, x_n \in M$  gibt mit

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

- (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  $i_1, \dots, i_n \in I$  und alle  $a_1, \dots, a_n \in R$  gilt

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

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

$$(1) \quad a_1 x_1 + \dots + a_n x_n = 0 \Rightarrow a_1 = \dots = a_n = 0$$

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  $x_1, \dots, x_n \in F$  und alle  $a_1, \dots, a_n \in R$  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  $x_1, \dots, x_n \in M$  bilden eine Basis von  $M$ , wenn  $(x_1, \dots, x_n) = (x_i)_{i \in \{1, \dots, n\}}$  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  $f : M \rightarrow N$  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  $f : M \rightarrow N$  heißt Einbettung/Monomorphismus (Epimorphismus, Isomorphismus), wenn  $f$  injektiv (surjektiv, bijektiv) ist.

Ein Modulhomomorphismus  $f : M \rightarrow M$  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  $M \rightarrow N$  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

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

und

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

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

$$\begin{aligned} \equiv & \xrightarrow{f} \bar{0} \\ \equiv_N & \xleftarrow{g} N \end{aligned}$$

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  $f : M \rightarrow N$  ein Modulhomomorphismus, so ist der *Kern*  $\ker f := \{x \in M \mid f(x) = 0\}$  von  $f$  ein Untermodul von  $M$  und das *Bild*  $\operatorname{im} f := \{f(x) \mid x \in M\}$  von  $f$  ist ein Untermodul von  $N$ .
- (j) *Homomorphiesatz*: Seien  $M$  und  $N$   $R$ -Moduln und  $L$  ein Untermodul von  $M$  und  $f : M \rightarrow N$  ein Modulhomomorphismus mit  $L \subseteq \ker f$ . Dann gibt es (genau) einen Modulhomomorphismus  $\bar{f} : (M/L) \rightarrow N$  mit  $\bar{f}(\bar{x}) = f(x)$  für alle  $x \in M$ .

Ferner gilt, dass

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

(k) Isomorphiesatz: Seien  $M$  und  $N$   $R$ -Moduln und  $f : M \rightarrow N$  ein Modulhomomorphismus. Dann ist  $\bar{f} : (M/\ker f) \rightarrow \operatorname{im} f$  definiert durch  $\bar{f}(\bar{x}) = f(x)$  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  $R$  [ $\rightarrow$  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  $(a)_R = Ra \stackrel{R \text{ komm.}}{=} \{ab | b \in R\} = aR$ . 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  $2 \cdot \bar{1} = \bar{2} = 0$  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  $1 \cdot \bar{0} = \bar{0} = 0$  und  $2 \cdot \bar{1} = \bar{2} = 0$  in  $\mathbb{Z}/2\mathbb{Z}$ , womit die einzige linear unabhängige Teilmenge von  $\mathbb{Z}/2\mathbb{Z}$  die leere Menge ist, 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*  $\underline{e} =$

$$(e_1, \dots, e_n), \text{ wobei } e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ mit einer 1 an der } i\text{-ten Stelle.}$$

- (b)  $\mathbb{R}^2$  ist ein zyklischer  $\mathbb{R}^{2 \times 2}$  Modul [ $\rightarrow$  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

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

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

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

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  $f_i : M_i \rightarrow N$ . Dann gibt es genau einen Modulhomomorphismus  $f : \bigoplus_{i \in I} M_i \rightarrow N$  mit  $f|_{M_i} = f_i$  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  $x = \sum_{i \in \text{supp}(x)} \rho_i(x(i))$ . Um  $f \circ \rho_i = f_i$  für  $i \in I$  zu erfüllen, kann man daher nur

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

definieren. Man überprüft sofort, dass das so definierte  $f$  ein Homomorphismus ist.  $\square$

**Proposition und Definition 1.2.3.** Sei  $R$  ein Ring,  $M$  ein  $R$ -Modul und  $(N_i)_{i \in I}$  eine Familie von Untermoduln von  $M$ . 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

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

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  $R \rightarrow M, a \mapsto ax$  nennt man *Annihilator* von  $x$ , in Zeichen  $\text{ann}(x) = \{a \in R \mid ax = 0\}$ .

Es heißt  $x$  ein *Torsionselement* von  $M$  wenn  $\text{ann}(x) \neq \{0\}$ .

**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  $g : B \rightarrow N$  gibt es genau einen Homomorphismus  $f : M \rightarrow N$  mit  $f|_B = g$ .

*Beweis.*

(a)  $\Rightarrow$  (b) klar

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

- Eindeutigkeit: klar aus  $M = \sum_{x \in B} Rx$
- Existenz: Fixiere zunächst  $x \in B$ . Dann ist  $R \rightarrow Rx, a \mapsto ax$  ein Isomorphismus (mit Kern  $\text{ann}(x)$ ), dessen Umkehrfunktion ein Isomorphismus  $Rx \rightarrow R$  ist, der  $x$  auf 1 abbildet. Schaltet man den Homomorphismus  $R \rightarrow N, a \mapsto ag(x)$  dahinter, so erhält man einen Homomorphismus  $Rx \rightarrow N$ , der  $x$  auf  $g(x)$  abbildet. Da  $x \in B$  beliebig war, erhält man mit 1.2.2 einen Homomorphismus  $f : M = \bigoplus_{x \in B} Rx \rightarrow N$ , 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  $f : M \rightarrow R$  mit  $f(x_i) = 1$  und  $f(x_j) = 0$  für  $j \in \{1, \dots, n\} \setminus \{i\}$ . Dann

$$0 = f(0) = f\left(\sum_{j=1}^n a_j x_j\right) = \sum_{j=1}^n a_j f(x_j) = a_i f(x_i) = a_i$$

2.  $B$  erzeugt  $M$ : Nach (c) gibt es einen Homomorphismus  $M \rightarrow M$ , der auf  $B$  die Identität ist. Einerseits ist  $\text{id}_M$  ein solcher, andererseits auch  $\rho \circ f$ , wobei  $f : M \rightarrow N := \sum_{x \in B} Rx$  der nach (c) existierende Homomorphismus mit  $f|_B = \text{id}_B$  ist und  $\iota : N \hookrightarrow M, x \mapsto x$  die Inklusion. Also  $\text{id}_M = \iota \circ f$ , insbesondere  $M = \text{im}(\text{id}_M) = \text{im}(f) = N$

□

**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

$$R^n \rightarrow M, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^n a_i x_i$$

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  $x_1, \dots, x_n \in M$ . Annahme:  $B$  ist eine unendliche Basis von  $M$ . Dann gibt es für jedes  $i \in \{1, \dots, n\}$  ein endliches  $B_i \subseteq B$  mit  $x_i \in \sum_{y \in B_i} Ry$ . Dann ist  $B' := B_1 \cup \dots \cup B_n \subseteq B$  endlich mit  $M = \sum_{y \in B'} Ry$ . Da  $B$  unendlich 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  $B$  steht, außer wenn  $1 = 0$  in  $R$ , d.h.  $R = \{0\}$ . Im letzten Fall ist aber nach 1.2.8 nichts zu zeigen.  $\square$

**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  $R$ .

Um dies zu zeigen, wähle zueinander inverse  $R$ -Modulisomorphismen  $f : R^n \rightarrow R^m, g : R^m \rightarrow R^n$ . Bezeichne mit  $\underline{x} = (x_1, \dots, x_n)$  und  $\underline{y} = (y_1, \dots, y_m)$  die Standardbasen des  $R^n$  und  $R^m$ . Wähle  $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in R^{m \times n}$  mit  $f(x_j) = \sum_{i=1}^m a_{ij} y_i$  für  $j \in \{1, \dots, n\}$

und  $B = (b_{ji})_{1 \leq j \leq n, 1 \leq i \leq m} \in R^{n \times m}$  mit  $f(y_i) = \sum_{j=1}^n b_{ji} x_j$  für  $i \in \{1, \dots, m\}$ . Dann gilt für  $k \in \{1, \dots, m\}$

$$\begin{aligned} y_k &= (f \circ g)(y_k) = f(g(y_k)) \\ &= f\left(\sum_{j=1}^n b_{jk} x_j\right) \\ &= \sum_{j=1}^n b_{jk} f(x_j) \\ &= \sum_{j=1}^n b_{jk} \sum_{i=1}^m a_{ij} y_i \\ &= \sum_{i=1}^m \left(\sum_{j=1}^n b_{jk} a_{ij}\right) y_i \stackrel{R \text{ komm.}}{=} \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} b_{jk}\right) y_i \end{aligned}$$

und daher

$$\sum_{j=1}^n a_{ij} b_{jk} = \begin{cases} 1 & \text{falls } k = i \\ 0 & \text{sonst} \end{cases}$$

für alle  $i, k \in \{1, \dots, m\}$ , d.h.  $AB = I_m$ .

Wegen  $n < m$  können wir  $A' := (A \quad \underbrace{0}_{(m-n)\text{-Spalten}}) \in R^{m \times m}$  und  $B' := \begin{pmatrix} B \\ 0 \end{pmatrix} \in R^{m \times m}$

(mit  $m - n$  0-Zeilen) setzen, so dass  $A'B' = AB = I_m$ .

Mit dem Determinantenproduktsatz folgt

$$0 = 0 \cdot 0 = (\det A')(\det B') = \det(A'B') = 1$$

□

**Bemerkung 1.2.12.** Statt den Determinantenproduktsatz über kommutativen Ringen zu verwenden, kann man den Beweis des letzten Satzes auch mit der Theorie kommutativer Ringe auf die Dimensionstheorie von Vektorräumen zurückspielen.

Sei  $R$  ein kommutativer Ring mit  $1 \neq 0$ ,  $m, n \in \mathbb{N}_0$  mit  $R^m \cong R^n$ . Wir zeigen  $m = n$ .

*Beweis.* Wähle ein maximales Ideal  $\mathfrak{m}$  von  $R$ . Wähle einen  $R$ -Modulisomorphismus  $f : R^m \rightarrow R^n$ . Betrachte die  $R$ -Untermoduln

$$\mathfrak{m}R^m := \left\{ \sum_{i=1}^n a_i x_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{m}, x_i \in R^m \right\} = \mathfrak{m}^m$$

von  $R^m$  und

$$f(\mathfrak{m}R^m) = \left\{ \sum_{i=1}^n a_i y_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{m}, y_i \in R^n \right\} = \mathfrak{m}^n$$

von  $R^n$

Mit dem Isomorphiesatz erhalten wir einen Modulisomorphismus  $R^m/\mathfrak{m}^m \rightarrow R^n/\mathfrak{m}^n$  und offensichtlich gilt  $R^m/\mathfrak{m}^m \cong (R/\mathfrak{m})^m$  (betrachte z.B.  $R^m \rightarrow (R/\mathfrak{m})^m$ ). Da nun  $(R/\mathfrak{m})^m$  und  $(R/\mathfrak{m})^n$  als  $R$ -Moduln isomorph sind, sind sie auch als  $(R/\mathfrak{m})$ -Moduln isomorph. Für den Körper  $K := R/\mathfrak{m}$  gilt also

$$m = \dim_K K^m = \dim_K K^n = n$$

□

**Definition 1.2.13.** Sei  $R$  ein kommutativer Ring mit  $1 \neq 0$  und  $M$  ein freier  $R$ -Modul mit Basis  $B$ . Dann heißt  $\text{rk } M := |B| \in \mathbb{N}_0 \cup \{\infty\}$  der *Rang* von  $M$  [hängt nach 1.2.11 nicht von der Wahl der Basis  $B$  ab]

## 1.3 Halbeinfache Moduln

**Notation 1.3.1.**  $0 := \{0\}$  Nullmodul

**Definition 1.3.2.** Ein Modul  $M$  heißt *einfach* (oder irreduzibel), falls  $M \neq 0$  und  $0$  und  $M$  die einzigen Untermoduln von  $M$  sind.

**Bemerkung 1.3.3.** Sei  $N$  ein Untermoduln von  $M$ .

- (a) Bezeichne  $\varphi : M \rightarrow M/N$  den kanonischen Epimorphismus. Dann vermitteln die Zuordnungen

$$\begin{aligned} L &\mapsto L/N = \varphi(L) \\ \varphi^{-1}(P) &\leftarrow P \end{aligned}$$

Eine Bijektion zwischen der Menge der Untermoduln  $L$  von  $M$  mit  $N \subseteq L$  und der Menge der Untermoduln von  $M/N$

- (b) Es folgt, dass  $M/N$  einfach ist genau dann, wenn  $N$  ein maximaler echter Untermodul ist.

**Beispiele 1.3.4.** (a) Sei  $R$  ein kommutativer Ring und  $I$  ein  $R$ -Untermodul von  $R$ , d.h. ein Ideal von  $R$  [→1.1.5]. Dann ist  $R/I$  ein einfacher  $R$ -Modul  $\Leftrightarrow I$  ist ein maximales Ideal von  $R \Leftrightarrow R/I$  ist ein Körper.

- (b) Sei  $R$  ein Hauptidealring und  $p \in R \setminus \{0\}$ . Dann ist  $R/pR$  ein einfacher Modul genau dann, wenn  $p$  irreduzibel in  $R$  ist.

*Beweis.*  $\Rightarrow$  Ist  $(p)$  ein maximales Ideal von  $R$ , so auch ein Primideal, d.h.  $p$  ist prim in  $R$  und daher auch irreduzibel in  $R$  (wegen  $p \neq 0$ )

$\Leftarrow$  Ist  $p$  irreduzibel in  $R$ , so ist  $R/(p)$  ein Körper und daher ist  $(p)$  ein maximales Ideal in  $R$ .

□

**Lemma 1.3.5.** Sei  $R$  ein Ring und  $M$  ein  $R$ -Modul. Es sind äquivalent:

- (i)  $M$  ist einfach
- (ii)  $M \neq 0$  und jedes Element von  $M \setminus \{0\}$  erzeugt  $M$
- (iii) Es gibt einen maximalen echten  $R$ -Untermodul  $N$  von  $M$  mit  $M/N \cong M$

*Beweis.*

- (a)  $\Rightarrow$  (c) Gelte (a) Wähle  $x \in M \setminus \{0\}$ . Dann ist der Homomorphismus  $\varphi : R \rightarrow M, a \mapsto ax$  surjektiv und daher  $M/N \cong M$  mit  $N := \ker \varphi$ . Mit  $M$  ist auch  $M/N$  einfach, weswegen nach 1.3.3(b)  $N$  ein maximaler echter Untermodul von  $M$  ist.

- (c)  $\Rightarrow$  (b) trivial

- (b)  $\Rightarrow$  (a) trivial

□



---

# Index

---

## Modul, 1

Äußere Direkte Summe, 6

Annihilator, 7

Automorphismus, 3

Basis, 3

Direktes Produkt, 2

Einfache Moduln, 11

Freie Moduln, 8

Homomorphismus, 3

Bild, 4

Endomorphismus, 3

Kern, 4

Innere Direkte Summe, 6

Kongruenzrelation, 4

Linear unabhängig (l.u.), 3

Quotientenmodul, 4

Rang, 10

Standardbasis, 5

Torsionselement, 7

Unterm modul, 2

Zyklische Moduln, 3