

---

# 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
1.4	Noethersche und artinsche Moduln . . . . .	15
1.5	Unzerlegbare Moduln . . . . .	19



---

# 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  $\bar{f} : (M/\ker f) \rightarrow \text{im } f$  definiert durch  $\bar{f}(\bar{x}) = f(x)$  für alle  $x \in M$  ein  $R$ -Modulisomorphismus. Insbesondere ist  $M/\ker f \cong \text{im } f$

**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  $M/N \cong R/I$

*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  $M/N \cong R/I$  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

□

**Lemma 1.3.6.** Lemma von Schur.

Sei  $R$  ein Ring,  $M$  und  $N$  einfache  $R$ -Moduln und  $f : M \rightarrow N$  ein Homomorphismus. Dann ist  $f$  entweder die Nullabbildung oder ein Isomorphismus

*Beweis.* Ist  $f \neq 0$ , so ist  $\ker f \neq M$  und  $\operatorname{im} f \neq 0$ , also  $\ker f = 0$  und  $\operatorname{im} f = N$ . □

**Definition 1.3.7.** Ein Modul heißt *halbeinfach* (oder vollständig reduzibel), wenn er direkte Summe von einfachen Moduln ist.

**Lemma 1.3.8.** Jeder endlich erzeugte Modul  $\neq 0$  besitzt einen einfachen Quotienten.

*Beweis.* Sei  $M$  ein  $R$ -Modul und seinen  $x_1, \dots, x_n \in M$  mit  $0 \neq M = Rx_1 + \dots + Rx_n$ . Zu zeigen: Es gibt einen Untermodul  $N$  von  $M$  mit  $M/N$  einfach. Betrachte die durch Inklusion halbgeordnete Menge

$$X := \{P \mid P \text{ Untermodul von } M, P \subsetneq M\} = \{P \mid P \text{ Untermodul von } M, \{x_1, \dots, x_n\} \not\subseteq P\}$$

Jede Kette  $K \subseteq X$  besitzt eine obere Schranke in  $X$  (0 für  $K = \emptyset$ , da  $M \neq 0$  und  $\bigcup K$  für  $K \neq \emptyset$ , da  $\{x_1, \dots, x_n\}$  endlich)

Nach dem Lemma von Zorn gibt es daher ein maximales Element  $N$  in  $X$ . Gemäß 1.3.3(b) ist  $M/N$  einfach. □

**Definition 1.3.9.** Sei  $M$  ein Modul und  $N$  ein Untermodul von  $M$ . Dann heißt  $N$  ein *direkter Summand* von  $m$ , wenn es einen Untermodul  $P$  von  $M$  gibt mit  $M = N \oplus P$ .

**Satz 1.3.10.** Sei  $M$  ein Modul. Dann sind folgende Aussage äquivalent

(a)  $M$  ist halbeinfach

(b)  $M$  ist die Summe seiner einfacher Untermoduln

(c) Jeder Untermodul von  $M$  ist ein direkter Summand von  $M$ .

*Beweis.*

(a)  $\Rightarrow$  (b) ist klar

(b)  $\Rightarrow$  (c). Gelte (b) und sei  $N$  ein Untermodul von  $M$ .

$$X := \{P \mid P \text{ Untermodul von } M, N \cap P = 0\}$$

Jede Kette  $K \subseteq X$  besitzt eine obere Schranke in  $X$  (0 für  $K = \emptyset$ ,  $\bigcup K$  für  $K \neq \emptyset$ )

Nach dem Lemma von Zorn gibt es daher ein maximales Element  $P$  in  $X$ . Um  $M = N + P$  zu zeigen, reicht es wegen (b) zu zeigen, dass jeder einfache Untermodul  $L$  von  $M$  in

$N + P$  enthalten ist. Sei also  $L$  ein einfacher Untermodul von  $M$ . Dann ist entweder  $L \cap (N + P) = 0$  oder  $L \cap (N + P) = L$ . Im letzteren Fall sind wir fertig.

Der erste Fall tritt aber nicht ein:

Ist  $L \cap (N + P) = 0$ , so  $(L + P) \cap N = 0$  (ist  $x \in L$  und  $y \in P$  mit  $x + y \in N$ , so  $x \in L \cap (N + P) = 0$  und daher  $y \in N \cap P = 0$ ), woraus wegen der Maximalität von  $P$  folgt  $P = L + P$ , also  $L \subseteq P$ .

(c) $\Rightarrow$ (a). Gelte (c).

Hilfsbehauptung: Jeder Untermodul eines Untermoduls  $N$  von  $M$  ist ein direkter Summand von  $N$ .

Begründung: Sei  $N$  ein Untermodul von  $M$  und  $P$  ein Untermodul von  $N$ . Wähle  $Q$  mit  $M = P \oplus Q$ . Setze  $R = Q \cap N$ . Wir zeigen  $N = P \oplus R$ . Es ist klar, dass  $P \cap R = 0$  (denn  $P \cap Q = 0$ ) und  $P + R \subseteq N$ . Zu zeigen ist also noch  $N \subseteq P + R$ .

Sei hierzu  $x \in N$ . Schreibe  $x = p + q$  mit  $p \in P$  und  $q \in Q$ , dann  $q = x - p \in N \cap Q = R$ . Betrachte nun die durch Inklusion halbgeordnete Menge

$$X := \left\{ Y \mid Y \text{ Menge von einfachen Untermoduln von } M \text{ mit } \sum_{N \in Y} N = \bigoplus_{N \in Y} N \right\}$$

Sei  $K$  eine Kette in  $X$ . Wir behaupten, dass dann  $Z := \bigcap K \in X$  gilt und  $Z$  eine obere Schranke von  $K$  in  $X$  ist.

Zu zeigen:  $\sum_{N \in Z} N = \bigoplus_{N \in Z} N$

Seien nun  $n \in \mathbb{N}$  und  $N_1, \dots, N_n \in Z$  paarweise verschieden und  $x_1 \in N_1, \dots, x_n \in N_n$  mit  $x_1 + \dots + x_n = 0$  [ $\rightarrow$  1.2.3(b)]. Da  $X$  eine Kette ist, gibt es  $Y \in K$  mit  $\{N_1, \dots, N_n\} \subseteq Y$ . Wegen  $\sum_{N \in Y} N = \bigoplus_{N \in Y} N$  folgt mit 1.2.3(b), dass  $x_1 = \dots = x_n = 0$ .

Da die Kette  $K \subseteq X$  beliebig war, gibt es nach dem Lemma von Zorn ein in  $X$  maximales Element  $Z$ . Setze  $P = \sum_{N \in Z} N = \bigoplus_{N \in Z} N$ . Wir zeigen  $M = P$ .

Angenommen  $M \setminus P \neq \emptyset$ . Wähle gemäß (c)  $Q$  mit  $M = P \oplus Q$ . Dann  $Q \neq 0$ . Wähle einen endlich erzeugten Untermodul  $Q' \neq 0$  von  $Q$ . Nach Lemma 1.3.8 gibt es einen Untermodul  $Q''$  von  $Q'$  mit  $Q'/Q''$  einfach.

Wähle gemäß Hilfsbehauptung  $R$  mit  $Q' = Q'' \oplus R$ . Dann ist  $R \subseteq Q' \subseteq Q$  und daher  $P \cap R = 0$ . Weiter ist  $R \cong Q'/Q''$  einfach. Es folgt  $\sum_{N \in Z \cup \{R\}} N = \bigoplus_{N \in Z \cup \{R\}} N$ . Daher ist  $Z \cup \{R\} \in X$ . Wegen der Maximalität von  $Z$  in  $X$  gilt  $R \in Z$  und daher  $R \subseteq P$ .  $\square$

**Korollar 1.3.11.** Direkte Summen, Untermoduln und Quotienten von halbeinfachen Moduln sind halbeinfach.

*Beweis.* direkte Summen: klar nach 1.3.7

Untermoduln: Sei  $N$  ein Untermodul des halbeinfachen Moduls  $M$ . Wir verwenden 1.3.10(c) um zu zeigen, dass  $N$  auch halbeinfach ist. Sei also  $L$  ein Untermodul von  $N$ . Da  $M$  halbeinfach ist, gibt es einen Untermodul  $P$  von  $M$  mit  $M = L \oplus P$ . Dann gilt  $N = L \oplus (P \cap N)$ , wie man sofort sieht.

Quotienten: Sei  $N$  ein Untermodul des halbeinfachen Moduls  $M$ . Zu zeigen:  $M/N$  ist halbeinfach.

Wähle einen Untermodul  $P$  von  $M$  mit  $M = N \oplus P$ . Dann ist  $M/N \cong P$  halbeinfach

nach dem gerade Gezeigten (betrachte den Homomorphismus  $M = N \oplus P \rightarrow P, x+y \mapsto y$  und wende den Homomorphiesatz an).  $\square$



## 1.4 Noethersche und artinsche Moduln

**Definition 1.4.1.** Ein Modul  $M$  heißt *noethersch* bzw. *artinsch*, wenn jede aufsteigende bzw. absteigende Kette von Untermoduln  $M_1 \subseteq M_2 \subseteq \dots$  bzw.  $M_1 \supseteq M_2 \supseteq \dots$  von  $M$  stationär wird (d.h.  $\exists k \in \mathbb{N} : \forall n \geq k : M_n = M_k$ ).

Ein Ring  $R$  heißt noethersch bzw. artinsch, wenn er als  $R$ -Modul noethersch bzw. artinsch ist.

**Bemerkung 1.4.2.** Sei  $R$  ein kommutativer Ring

- (a)  $R$  ist genau dann noethersch, wenn jede aufsteigende Kette von Idealen in  $R$  stationär wird [→1.1.5]
- (b) Ist  $S = R[a_1, \dots, a_n]$  ein kommutativer Ring mit  $n \in \mathbb{N}_0, a_1, \dots, a_n \in S$ , so besagt der *Hilbertsche Basissatz*:  $R$  noethersch  $\Rightarrow S$  noethersch.

**Satz 1.4.3.** Ein Modul ist noethersch genau dann, wenn alle seine Untermoduln endlich erzeugt sind [→1.1.4(d)].

**Lemma 1.4.4.** Seien  $L, L'$  und  $N$  Untermoduln des Moduls  $M$  mit  $L \subseteq L', L \cap N = L' \cap N$  und  $L + N = L' + N$ . Dann gilt  $L = L'$

*Beweis.* Sei  $x \in L'$ . Zu zeigen ist  $x \in L$ . Schreibe  $x = l + n$  mit  $l \in L$  und  $n \in N$ . Dann ist  $x - l = n \in L' \cap N = L \cap N$  und daher  $x = (x - l) + l \in L$ .  $\square$

**Satz 1.4.5.** Sei  $N$  ein Untermodul des Moduls  $M$ . Dann ist  $M$  noethersch bzw. artinsch genau dann, wenn sowohl  $N$  als auch  $M/N$  noethersch bzw. artinsch ist.

*Beweis.* klar mit 1.3.3(a) und 1.4.4  $\square$

**Korollar 1.4.6.** Endlich Summen noetherscher bzw. artinscher Moduln sind auch noethersch bzw. artinsch.

*Beweis.* Sind  $N_1, \dots, N_n$  noethersche bzw. artinsche Untermoduln des Moduls  $M$  mit  $M = \sum_{i=1}^n N_i$ , so gibt es nach 1.2.2 einen Epimorphismus

$$\bigoplus_{i=1}^n N_i \rightarrow \sum_{i=1}^n N_i$$

weshalb  $M = \sum_{i=1}^n N_i \cong (\bigoplus_{i=1}^n N_i) / L$  für einen Untermodul  $L$  von  $\bigoplus_{i=1}^n N_i$  gilt.

Mit 1.4.5 reicht es daher, die Behauptung für direkte Summen zu zeigen.

Durch Induktion nach  $n \in \mathbb{N}_0$  zeigen wir daher, dass für alle noetherschen bzw. artinschen  $R$ -Moduln  $N_1, \dots, N_n$  auch  $\bigoplus_{i=1}^n N_i$  noethersch bzw. artinsch ist.

Induktionsanfang für  $n = 0$ : klar

Induktionsschritt  $n - 1 \rightarrow n, (n \in \mathbb{N})$ : Seien  $N_1, \dots, N_n$  noethersche bzw. artinsche  $R$ -Moduln. Dann ist  $\bigoplus_{i=1}^{n-1} N_i$  noethersch bzw. artinsch nach Induktionsvoraussetzung. Wegen

$$\left( \bigoplus_{i=1}^n N_i \right) / \left( \bigoplus_{i=1}^{n-1} N_i \right) \cong N_n$$

folgt mit 1.4.5, dass  $\bigoplus_{i=1}^n N_i$  auch noethersch bzw. artinsch ist.  $\square$

**Korollar 1.4.7.** Jeder endlich erzeugte Modul über einem noetherschen bzw. artinschen Ring ist noethersch bzw. artinsch.

*Beweis.* Sei  $R$  ein noetherscher bzw. artinscher Ring und  $M$  ein endlich erzeugter  $R$ -Modul. Nach 1.4.6 ist ohne Einschränkung  $M$  zyklisch. Dann ist  $M \cong R/N$  für einen  $R$ -Untermodul  $N$  von  $R$ . Mit  $R$  ist nach 1.4.5 auch  $R/N$  noethersch bzw. artinsch.  $\square$

**Definition 1.4.8.** Sei  $M$  ein Modul. Dann heißt

$$\ell(M) := \sup \{n \in \mathbb{N}_0 \mid \text{es gibt Untermoduln } M_0, \dots, M_n \text{ von } M \text{ mit } M_0 \supsetneq \dots \supsetneq M_n\} \in \mathbb{N}_0 \cup \{\infty\}$$

die *Länge* von  $M$ .

Es heißt  $M$  von endlicher Länge, wenn  $\ell(M) < \infty$ .

**Beispiele 1.4.9.** Sei  $M$  ein Modul. Dann

- $\ell(M) = 0 \Leftrightarrow M = 0$
- $\ell(M) = 1 \Leftrightarrow M$  ist einfach

**Satz 1.4.10.** Sei  $N$  ein Untermodul des Moduls  $M$ . Dann gilt

$$\ell(M) < \infty \Leftrightarrow (\ell(M/N) < \infty \wedge \ell(N) < \infty)$$

und falls  $\ell(M) < \infty$

$$\ell(M) = \ell(M/N) + \ell(N)$$

*Beweis.* Man sieht sofort  $\ell(M) = \sup \hat{M}, \ell(M/N) \stackrel{1.3.3(a)}{=} \sup \hat{K}$  und  $\ell(N) = \sup \hat{N}$  mit

$$\hat{M} := \{m \in \mathbb{N}_0 \mid \exists \text{ Untermoduln } M_0, \dots, M_m \text{ von } M : M = M_0 \supsetneq \dots \supsetneq M_m = 0\}$$

$$\hat{K} := \{k \in \mathbb{N}_0 \mid \exists \text{ Untermoduln } L_0, \dots, L_k \text{ von } M : M = L_0 \supsetneq \dots \supsetneq L_k = N\}$$

$$\hat{N} := \{n \in \mathbb{N}_0 \mid \exists \text{ Untermoduln } N_0, \dots, N_n \text{ von } M : N = N_0 \supsetneq \dots \supsetneq N_n = 0\}$$

Offensichtlich gilt  $\forall k \in \hat{K} : \forall n \in \hat{N} : k + n \in \hat{M}$ , was „ $\Rightarrow$ “ und „ $\geq$ “ beweist.

Um „ $\Leftarrow$ “ und „ $\leq$ “ zu beweisen, reicht es

$$\forall m \in \hat{M} : \exists k \in \hat{K} : \exists n \in \hat{N} : m \leq k + n$$

zu zeigen. Sei hierzu  $m \in \hat{M}$ . Wähle Untermoduln  $M_0, \dots, M_m$  von  $M$  mit  $M = M_0 \supsetneq \dots \supsetneq M_m = 0$ . Setze  $L_i := M_i + N$  und  $N_i := M_i \cap N$  für  $i \in \{0, \dots, m\}$ . Nach Lemma 1.4.4 ist dann jeweils mindestens eine der beiden Inklusionen  $L_i \supsetneq L_{i+1}$  und  $N_i \supsetneq N_{i+1}$  echt. (für  $i \in \{0, \dots, m-1\}$ ). Setzt man

$$k := |\{i \in \{0, \dots, m-1\} \mid L_i \supsetneq L_{i+1}\}| \in \hat{K}$$

und

$$n := |\{i \in \{0, \dots, m-1\} \mid N_i \supsetneq N_{i+1}\}| \in \hat{N}$$

so folgt  $m \leq k + n$   $\square$

**Definition 1.4.11.** Sei  $M$  ein Modul. Es heißt  $(M_0, \dots, M_n)$  eine *Kompositionsreihe* von (der Länge  $n$ ) von  $M$ , wenn  $M_0, \dots, M_n$  Untermoduln von  $M$  sind mit

$$M = M_0 \supsetneq \dots \supsetneq M_n = 0$$

derart, dass die sogenannten Faktoren  $M_i/M_{i+1}$  ( $i \in \{0, \dots, n-1\}$ ) alle einfach sind.

**Bemerkung 1.4.12.** Jeder endliche Modul besitzt natürlich eine Kompositionsreihe. Folgender Satz verallgemeinert dies.

**Satz 1.4.13.** Sei  $M$  ein Modul. Es sind folgende Aussagen äquivalent

- (a)  $\ell(M) < \infty$
- (b)  $M$  ist noethersch und artinsch
- (c)  $M$  besitzt eine Kompositionsreihe.

In diesem Fall ist die Länge einer jeden Kompositionsreihe von  $M$  gleich der Länge von  $M$ .

*Beweis.*

(a)  $\Rightarrow$  (b) trivial

(b)  $\Rightarrow$  (c) Sei  $M$  noethersch und artinsch. Da  $M$  noethersch ist, gibt es zu jedem Untermodul  $N \neq 0$  von  $M$  einen Untermodul  $N'$  von  $N$  mit  $N/N'$  einfach (sonst könnte man eine aufsteigende Kette  $0 \subsetneq N_1 \subsetneq \dots \subsetneq \dots$  von echten Untermoduln von  $M$  konstruieren).

Setze nun  $M_0 = N$  und wähle für  $i = 0, 1, \dots$  solange  $M_i \neq 0$  einen Untermodul  $M_{i+1}$  von  $M_i$  mit  $M_i/M_{i+1}$  einfach.

Dieses Verfahren bricht ab, da  $M$  artinsch ist.

(c)  $\Rightarrow$  (a) und Zusatz: Sei  $(M_0, \dots, M_n)$  eine Kompositionsreihe von  $M$ . Dann  $\ell(M) \stackrel{1.4.10}{=} \ell(M_0/M_1) + \dots + \ell(M_{n-1}/M_n) \stackrel{1.4.9}{=} n$

□

**Satz 1.4.14.** Satz von Jordan-Hölder

Sei  $M$  ein Modul endlicher Länge  $n$  und seien  $M = M_0 \supsetneq \dots \supsetneq M_n = 0$  und  $M = N_0 \supsetneq \dots \supsetneq N_n = 0$  zwei Kompositionsreihen von  $M$ . Dann gibt es  $\sigma \in S_n$  mit  $M_{i-1}/M_i \cong N_{\sigma(i)-1}/N_{\sigma(i)}$  für  $i \in \{1, \dots, n\}$

*Beweis.* Induktion nach  $n \in \mathbb{N}_0$

$n = 0$ : trivial

$n - 1 \rightarrow n$  ( $n \in \mathbb{N}$ ): Setze  $L := N_1$  und betrachte

- (2)  $M = L + M_0 \supsetneq \dots \supsetneq L + M_n = L$
- (3)  $L = L \cap M_0 \supsetneq \dots \supsetneq L \cap M_n = 0$

Hilfsbehauptung: Für alle  $i \in \{1, \dots, n\}$  gilt

**entweder**  $(L + M_{i+1})/(L + M_i) = 0$  und  $(L \cap M_{i+1})/(L \cap M_i) \cong M_{i-1}/M_i$   
**oder**  $(L + M_{i+1})/(L + M_i) \cong M_{i-1}/M_i$  und  $(L \cap M_{i+1})/(L \cap M_i) = 0$

Begründung: Sei  $i \in \{1, \dots, n\}$ . Ist  $(L \cap M_{i-1})/(L \cap M_i) \neq 0$ , so ist  $(L \cap M_{i-1})/(L \cap M_i) \hookrightarrow M_{i-1}/M_i$  ein Isomorphismus, da  $M_{i-1}/M_i$  einfach.

Ist  $(L + M_{i-1})/(L + M_i) \neq 0$ , so ist  $M_{i-1}/M_i \twoheadrightarrow (L + M_{i-1})/(L + M_i)$  ein Isomorphismus, da  $M_{i-1}/M_i$  einfach. Daher reicht es zu zeigen, dass genau einer der Moduln  $(L \cap M_{i-1})/(L \cap M_i)$  und  $(L + M_{i-1})/(L + M_i)$  ein Nullmodul ist.

Wegen Lemma 1.4.4 können nicht beide 0 sein. Es reicht daher zu zeigen, dass genau  $n$  der  $2n$  Inklusionen (2) und (3) echt sind. Dies folgt aus (1.4.13), indem man aus 2 und 3 eine Kompositionsreihe gewinnt.

Da  $M/L$  einfach ist, ist genau eine der  $n$  Inklusionen in (2) echt, etwa  $L + M_{k-1} \supsetneq L + M_k$ . Nach der Hilfsbehauptung erhält man aus (3) eine Kompositionsreihe von  $L$  der Länge  $n - 1$  (beachte  $L \cap M_{k-1} = L \cap M_k$ ). Da  $L = N_1 \supsetneq \dots \supsetneq N_n = 0$  ebenfalls eine solche ist, gibt es nach Induktionsvoraussetzung eine Bijektion  $\tau : \{2, \dots, n\} \rightarrow \{1, \dots, n\} \setminus \{k\}$  mit  $N_{i-1}/N_i \cong (L \cap M_{\tau(i)-1})/(L \cap M_{\tau(i)}) \cong M_{\tau(i)-1}/M_{\tau(i)}$  für  $i \in \{1, \dots, n\} \setminus \{k\}$ . Zusammen mit  $N_0/N_1 \cong M/L = (L + M_{k-1})/(L + M_k) \cong M_{k-1}/M_k$  liefert dies die gewünschte Bijektion.  $\square$

**Definition 1.4.15.** [ $\rightarrow$  1.2.4]

Sei  $R$  ein Ring,  $M$  ein  $R$ -Modul und  $E \subseteq M$ . Dann nennt man den  $R$ -Modul  $\text{ann}(E) := \{a \in R \mid \forall x \in E : ax = 0\}$  von  $R$  den Annihilator von  $E$ .

**Bemerkung 1.4.16.** Sei  $R$  ein kommutativer Ring,  $M$  ein  $R$ -Modul und  $E \subseteq M$ . Dann ist  $\text{ann}(E) = \text{ann}(\sum_{x \in E} Rx)$ . Insbesondere gilt für  $M = R/aR$  mit  $a \in R$ , dass

$$\text{ann}(R/aR) = \text{ann}(\{\bar{1}\}) = \text{ann}(\bar{1}) = aR$$

**Beispiele 1.4.17.** (a) Ist  $V$  ein  $K$ -Vektorraum, so  $\ell(V) = \dim(V)$

(b) Sei  $R$  ein Hauptidealring,  $n \in \mathbb{N}_0$ ,  $p_1, \dots, p_n \in R$  irreduzibel und  $m := p_1 \cdot \dots \cdot p_n$ .

Dann gilt  $\ell(R/mR) = n$  und

$$R/mR \supsetneq p_1 R/mR \supsetneq \dots \supsetneq p_1 \cdot \dots \cdot p_n R/mR$$

mit Faktoren  $(p_1 \cdot \dots \cdot p_{i-1} R/mR)/(p_1 \cdot \dots \cdot p_i R/mR) \cong (p_1 \cdot \dots \cdot p_{i-1} R)/(p_1 \cdot \dots \cdot p_i R) \cong R/p_i R$  für  $i \in \{1, \dots, n\}$ .

Nach dem Satz von Jordan-Hölder gibt es für alle Kompositionsreihen  $R/mR = M_0 \supsetneq \dots \supsetneq M_n = 0$  ein  $\sigma \in S_n$  mit  $M_{i-1}/M_i \cong p_{\sigma(i)} R$  und daher  $\text{ann}(M_{i-1}/M_i) = \text{ann}(R/p_{\sigma(i)} R) \stackrel{1.4.16}{=} p_{\sigma(i)} R$

Die Faktoren einer jeden Kompositionsreihe von  $R/mR$  liefern also bis auf Reihenfolge und Assoziiertheit genau die Faktoren von  $m = p_1 \cdot \dots \cdot p_n$ .

## 1.5 Unzerlegbare Moduln

**Definition 1.5.1.** Ein Modul  $M$  heißt *unzerlegbar*, falls  $M \neq 0$  und für alle Untermoduln  $L$  und  $N$  von  $M$  gilt

$$M = L \oplus N \Rightarrow (L = 0 \vee N = 0)$$

**Bemerkung 1.5.2.** Jeder einfache Modul  $[\rightarrow 1.3.2]$  ist unzerlegbar, aber die Umkehrung stimmt nicht, wie 1.3.4(b) in Verbindung mit Satz ?? unten zeigt.

**Lemma 1.5.3.** Sei  $M$  ein zyklischer Modul

- (a) Jeder direkte Summand von  $M$   $[\rightarrow 1.3.9]$  ist wieder zyklisch
- (b)  $M \cong R/N$  für einen  $R$ -Untermodul  $N$  von  $R$ .

*Beweis.* (a) Seien  $L$  und  $N$  Untermoduln von  $M$  mit  $M = L \oplus N$ . Schreibe  $M = Rx$  mit  $x \in M$  und  $x = y + z$  mit  $y \in L, z \in N$ . Wir zeigen  $L = Ry$ . Sei hierzu  $w \in L$ . Zu zeigen ist, dass  $w \in Ry$ . Schreibe  $az = ax - ay = w - ay \in L \cap N = 0$ . Also  $w = ax = ay \in Ry$ .

- (b) Schreibe  $M = Rx$  mit  $x \in M$ . Wähle für  $N$  den Kern des  $R$ -Modulhomomorphismus  $R \rightarrow M, a \mapsto ax$ .

□



---

# Index

---

## Modul, 1

- Äußere Direkte Summe, 6
- Annihilator, 7
- Artinsche Moduln, 15
- Automorphismus, 3
- Basis, 3
- Direkter Summand, 12
- Direktes Produkt, 2
- Einfache Moduln, 11
- Freie Moduln, 8
- Halbeinfache Moduln, 12
- Hilbertscher Basissatz, 15
- Homomorphismus, 3
  - Bild, 4
  - Endomorphismus, 3

## Kern, 4

- Innere Direkte Summe, 6
- Kompositionsreihe, 17
- Kongruenzrelation, 4
- Länge, 16
- Linear unabhängig (l.u.), 3
- Noethersche Moduln, 15
- Quotientenmodul, 4
- Rang, 10
- Standardbasis, 5
- Torsionselement, 7
- Unterm modul, 2
- Unzerlegbare Moduln, 19
- Zyklische Moduln, 3