2 Moduln

Der Begriff des *Moduls* verallgemeinert den Begriff des Vektorraumes, häufig werden Ringe durch Betrachtung von Moduln über ihnen studiert. Ringe sind weiterhin immer kommutativ mit Einselement.

2.1. Definition. Es sei R ein Ring. Ein *R-Modul* $M = (M,+,\cdot)$ oder *Modul über dem Ring R* ist eine Menge M mit Abbildungen $+ : M \times M \to M$, $(m_1,m_2) \mapsto m_1+m_2$, genannt *Addition*, und $\cdot : R\times M \to M$, $(a,m) \mapsto a\cdot m$, genannt *skalare Multiplikation*, so daß $(M,+)$ eine abelsche Gruppe ist und für alle $a,b \in R$, $m_1,m_2,m \in M$ gilt: Modul M

(i) $a(m_1+m_2) = am_1+am_2$

(ii) $(a+b)m = am+bm$

(iii) $(ab)m = a(bm)$

(iv) $1_R \cdot m = m$

2.2. Beispiel. (i) Ist R ein Ring, so ist R auch ein R-Modul mit den Operationen von R.

(ii) Ist $R = K$ ein Körper, so ist eine Menge M ein K-Modul genau dann, wenn M ein K-Vektorraum ist.

(iii) Eine Teilmenge M des Ringes R ist ein R-Modul genau dann, wenn M ein Ideal von R ist.

(iv) Es sei $G = (G,+)$ eine abelsche Gruppe. Definiert man für $g \in G$, $n \in \mathbb{Z}$:

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

so wird G zu einem $\mathbb{Z}$-Modul.

(v) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $R/\mathfrak{a}$ ein R-Modul vermöge der skalaren Multiplikation $r\cdot(a \bmod \mathfrak{a}) := (r\cdot a \bmod \mathfrak{a})$ für $r,a \in R$.

2.3. Definition. Es sei M ein R-Modul. Eine Teilmenge $M' \subseteq M$ heißt *Untermodul* von M, wenn M' eine Untergruppe von M ist, die abgeschlossen bezüglich skalarer Multiplikation von M ist, d.h. für $r \in R$, $m' \in M'$ gilt $r\cdot m' \in M'$. (Ein Untermodul ist wieder ein R-Modul.) Untermoduln

2.4. Lemma (Untermodulkriterium). *Es sei M ein R-Modul, dann ist eine Teilmenge M' von M ein Untermodul genau dann, wenn für alle $m_1,m_2 \in M', r \in R$ gilt:*

(i) $m_1 - m_2 \in M'$

(ii) $r\cdot m_1 \in M'$

Beweis. Analog zu Unterraumkriterium der linearen Algebra. □

2.5. Definition (& Lemma). Es sei M ein R-Modul, und es sei $M_\lambda, \lambda \in \Lambda$, eine Familie von Untermoduln von M.

Summe von Moduln $\sum_{\lambda\in\Lambda} M_\lambda$

(i) Die *Summe* $\sum_{\lambda\in\Lambda} M_\lambda$ ist die Menge aller *endlichen* Summen $\sum_{\lambda\in\Lambda'} m_\lambda$, wobei $\Lambda' \subseteq \Lambda$ endlich ist, und $m_\lambda \in M_\lambda$ für alle $\lambda \in \Lambda'$.

Die Summe ist der kleinste Untermodul von M, der alle M_λ enthält.

Durchschnitt von Moduln $\bigcap_{\lambda\in\Lambda} M_\lambda$

(ii) Der *Durchschnitt* $\bigcap_{\lambda\in\Lambda} M_\lambda$ ist ein Untermodul.

Beweis. Siehe Übung. □

Die Vereinigung zweier Untermoduln ist nicht notwendigerweise ein Untermodul. (Siehe Übung 9)

2.6. Definition. Es sei R ein Ring und M und N R-Moduln. Eine Abbildung $\varphi : M \to N$ heißt ein *R-Modul-Homomorphismus* oder *R-linear*, wenn für alle $m_1, m_2 \in M, r \in R$ gilt:

Modulhomomorphismus R-linear

(i) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$,

(ii) $\varphi(r \cdot m_1) = r \cdot \varphi(m_1)$.

$\mathrm{Hom}_R(M,N)$

Die Menge der R-linearen Abbildungen $M \to N$ wird mit $\mathrm{Hom}_R(M,N)$. Ein R-Modulisomorphismus ist ein bijektiver R-Modulhomomorphismus.

2.7. Bemerkung. (i) Ist $R = K$ ein Körper, so ist ein R-Modulhomomorphismus dasselbe wie eine K-lineare Abbildung von K-Vektorräumen.

(ii) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist der kanonische Epimorphismus $\pi : R \to R/\mathfrak{a}$ R-linear.

(iii) Sind M, N, P R-Moduln, und sind $\varphi : M \to N$, $\psi : N \to P$ R-Modulhomomorphismen, so ist auch $\psi \circ \varphi : M \to P$ ein R-Modulhomomorphismus.

(iv) Es seien M, N R-Moduln. Für $\varphi, \psi \in \mathrm{Hom}_R(M,N)$ und $r \in R, m \in M$ setzen wir $(\varphi + \psi)(m) := \varphi(m) + \psi(m)$ und $(r \cdot \varphi)(m) := r \cdot \varphi(m)$. Damit ist eine Addition und skalare Multiplikation auf der Menge $\mathrm{Hom}_R(M,N)$ erklärt, die $\mathrm{Hom}_R(M,N)$ zu einem R-Modul macht.

(v) Ist M ein R-Modul, so heißen die Elemente von $\mathrm{Hom}_R(M,M)$ *Endomorphismen* von M. Durch die Festlegung $\varphi \cdot \psi := \varphi \circ \psi$ für $\varphi, \psi \in \mathrm{Hom}_R(M,M)$ wird eine Multiplikation erklärt, die $\mathrm{Hom}_R(M,M)$ zu einem Ring macht. Er wird *Endomorphismenring* von M genannt. Er hat als Einselement die identische Abbildung $\mathrm{id}_M : m \mapsto m$, ist aber im Allgemeinen nicht kommutativ.

Endomorphismenring $\mathrm{Hom}_R(M,M)$

(vi) Jeder R-Modulhomomorphismus $\varphi : R \to M$ ist eindeutig bestimmt durch $\varphi(1_R)$, denn $\varphi(r) = \varphi(1_R \cdot r) = r \cdot \varphi(1_R)$. Dies liefert einen R-Modulhomomorphismus $M \xrightarrow{\sim} \mathrm{Hom}_R(R,M)$.

2.8. Lemma (& Definition). *Es sei $\varphi : M \to N$ ein R-Modulhomomorphismus. Dann heißt* $\mathrm{Kern}\,\varphi := \{m \in M \mid \varphi(m) = 0\}$ *der* Kern *von φ und* $\mathrm{Im}\,\varphi := \{\varphi(m) \mid m \in M\}$ *das* Bild *von φ.*

Kern $\mathrm{Kern}\,\varphi$

Bild $\mathrm{Im}\,\varphi$

Es ist $\mathrm{Kern}\,\varphi$ *ein Untermodul von M,* $\mathrm{Im}\,\varphi$ *ein Untermodul von N. φ ist injektiv genau dann, wenn* $\mathrm{Kern}\,\varphi = \{0\}$.

Beweis. Folgt aus den Definitionen wie in der linearen Algebra. □

2.9. Satz (& Definition). *Es sei M' ein Untermodul des R-Moduls M. Definiere für $m \in M$: $m+M' := m \bmod M' := \{n \in M \mid m-n \in M'\}$ die* Restklasse *von m modulo M',*

Restklasse
$m \bmod M' = m + M'$

$\overline{M} := \{m+M' \mid m \in M\}$ die Menge der Restklassen, $\pi : M \to \overline{M}$, $m \mapsto m+M'$. Dann wird für $m,n \in M$, $r \in R$ durch $(m+M')+(n+M') := (m+n)+M'$ und $r\cdot(m+M') := (r\cdot m)+M'$ auf $\overline{M}$ eine Addition und skalare Multiplikation erklärt, die $\overline{M}$ zu einem R-Modul und $\pi : M \to \overline{M}$ zu einem surjektiven R-Modulhomomorphismus machen mit $\operatorname{Kern}\pi = M'$.

$\overline{M}$ heißt der Restklassenmodul *von M modulo M' oder* Faktormodul *von M nach M'. Schreibweise ist dann $M/M' := \overline{M}$. Die Abbildung π heißt* Restklassenhomomorphismus *oder* kanonischer Epimorphismus *von M auf M/M'.*

Restklassenmodul
Restklassen-
homomorphismus π

Beweis. (1) Auf M wird durch $m \sim n :\Leftrightarrow m-n \in M'$ eine Äquivalenzrelation erklärt. Die Äquivalenzklasse, die m enthält ist gerade $m+M'$. Deshalb ist die Abbildung π wohldefiniert.

(2) Die festgelegte Addition und skalare Multiplikation sind wohldefiniert und machen $\overline{M}$ zu einem R-Modul; das Inverse von $m+M'$ bezüglich der Addition ist $(-m)+M'$, das Nullelement ist $0_M + M' = M'$.

Dies ist die einzige R-Modulstruktur von $\overline{M}$, die π zu einem R-Modulhomomorphismus macht.

(3) Für $m \in M$ ist $\pi(m) = 0_{\overline{M}} = 0_M + M' = M'$ genau dann, wenn $m+M' = 0_M + M'$, d.h. $m \in M'$. Folglich ist $\operatorname{Kern}\pi = M'$.

□

2.10. Bemerkung. Untermoduln von M sind genau die Kerne von R-Modulhomomorphismen $M \to N$.

2.11. Lemma (& Definition). *Es sei $\varphi : M \to N$ ein R-Modulhomomorphismus, und es sei M' ein Untermodul von M mit $M' \subseteq \operatorname{Kern}\varphi$. Dann wird durch $\overline{m} := m+M' \mapsto \varphi(m)$ ein R-Modulhomomorphismus $\overline{\varphi} : M/M' \to N$ definiert. Dieser heißt* durch φ induziert. *Es gilt* $\operatorname{Kern}\overline{\varphi} = \operatorname{Kern}\varphi/M'$.

induzierter Modulhomomorphismus

Beweis. $\overline{\varphi}$ ist wohldefiniert, denn aus $\overline{n} = \overline{m}$ folgt $m-n =: x \in M'$, also $\varphi(m) = \varphi(n+x) = \varphi(n) + \varphi(x) = \varphi(n)$, denn $x \in \operatorname{Kern}\varphi$.

$\overline{\varphi}$ ist offenbar ein R-Modulhomomorphismus und $\overline{\varphi}(\overline{m}) = 0$ genau dann, wenn $\varphi(m) = 0$, also $\operatorname{Kern}\overline{\varphi} = \operatorname{Kern}\varphi/M'$. □

2.12. Satz (Homomorphiesatz). *Es seien $\varphi : M \to N$ ein R-Modulhomomorphismus, M' ein Untermodul von M und $\pi : M \to M/M'$ der kanonische Epimorphismus. Dann gilt:*

(a) *φ faktorisiert durch π, d.h., es gibt einen R-Modulhomomorphismus $\psi : M/M' \to N$ mit $\varphi = \psi \circ \pi$.*

$$\begin{tikzcd} M \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & N \\ & M/M' \arrow[ur, "\psi"'] & \end{tikzcd}$$

genau dann, wenn $M' \subseteq$ $\operatorname{Kern}\varphi$. *In diesem Fall ist ψ durch φ induziert und insbesondere eindeutig bestimmt.*

(b) $\operatorname{Im}\varphi \cong M/\operatorname{Kern}\varphi$.

Beweis. (a) "$\Rightarrow$" Angenommen, $\psi : M/M' \to N$ existiert. Dann gilt für $\overline{m} = m + M' \in M/M'$: $\varphi(m) = \psi(\pi(m)) = \psi(\overline{m})$, d.h. ψ ist durch φ induziert. Weiterhin gilt $\psi(\overline{m}) = 0 \Leftrightarrow \varphi(m) = 0$. Für $m \in M'$ gilt aber $\varphi(m) = \psi(\pi(m)) = \psi(0) = 0$, also $M' \subseteq \operatorname{Kern}\varphi$.

"$\Leftarrow$" Ist $M' \subseteq \operatorname{Kern}\varphi$, so folgt die Existenz von ψ aus (2.11).

(b) Im Fall $M' = \operatorname{Kern}\varphi$, $N = \operatorname{Im}\varphi$ folgt die Existenz von $\psi : M/\operatorname{Kern}\varphi \to \operatorname{Im}\varphi$. Offenbar ist ψ surjektiv und $\operatorname{Kern}\psi \overset{(2.11)}{=} \operatorname{Kern}\varphi/\operatorname{Kern}\varphi = \{\overline{0}\}$, d.h. ψ ist ein Isomorphismus.

$\square$

2.13. Folgerung. Sind $P \subseteq N$ Untermoduln von M, so induziert der kanonische Epimorphismus $\pi : M \to M/N$ einen Isomorphismus $(M/P)/(N/P) \cong M/N$.

Beweis. Wegen $P \subseteq N = \operatorname{Kern}\pi$ haben wir nach dem Homomorphiesatz ein kommutatives Diagramm

$$\begin{tikzcd} M \arrow[rr, "\pi"] \arrow[dr] & & M/N \\ & M/P \arrow[ur, "\psi"] & \end{tikzcd}$$

mit $\operatorname{Kern}\psi = \operatorname{Kern}\pi/P = N/P$. Mit π ist auch ψ surjektiv. Also folgt nach dem Homomorphiesatz $M/N = \operatorname{Im}\psi \cong (M/P)/\operatorname{Kern}\psi = (M/P)/(N/P)$. $\square$

2.14. Satz (Isomorphiesatz). *Sind M_1, M_2 Untermoduln von M, so gilt*

$$(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2).$$

Beweis. Es sei φ die Komposition von $M_1 \overset{\varepsilon}{\hookrightarrow} M_1 + M_2 \overset{\pi}{\twoheadrightarrow} (M_1 + M_2)/M_2$, d.h. $\varphi : M_1 \longrightarrow M_1 + M_2/M_2, m_1 \longmapsto m_1 + M_2$.

φ ist surjektiv, denn die Elemente von $(M_1 + M_2)/M_2$ sind der Form $m_1 + m_2 + M_2 = m_1 + M_2$, $m_1 \in M_1$, $m_2 \in M_2$.

Es ist $\varphi(m_1) = 0$ genau dann, wenn $m_1 \in M_2$, also folgt $\operatorname{Kern}\varphi = M_1 \cap M_2$. Somit ergibt sich die Behauptung aus dem Homomorphisatz. $\square$

2.15. Beispiel. (i) Es seien $f, g \in R = K[X]$ teilerfremd. Dann gilt $(f)/(f) \cap (g) \cong R/g$, denn $(f) + (g) = (\operatorname{ggT}(f,g)) = (1) = R$.

(ii) In $\mathbb{Z}$ gilt z.B. $(3)/(15) \cong \mathbb{Z}/5\mathbb{Z}$.

$(m) = R \cdot m$

2.16. Definition. Es sei M ein R-Modul. Ist $m \in M$, so ist $(m) := R \cdot m = \{rm \mid r \in R\}$ ein Untermodul von M. Ist $(m_\lambda)_{\lambda \in \Lambda}$ eine Familie von Elementen $m_\lambda \in M$ mit $M = \sum_{\lambda \in \Lambda} R \cdot m_\lambda$, so heißt $(m_\lambda)_{\lambda \in \Lambda}$ ein *Erzeugendensystem* von M. Ist Λ endlich, dann heißt M *endlich erzeugt*. Man schreibt dann $(m_1, \ldots, m_s) := \sum_{i=1}^{s} R \cdot m_i$.

Erzeugendensystem
endlich erzeugt

unverkürzbar Erzeugendensystem

Ein *unverkürzbares Erzeugendensystem* ist ein Erzeugendensystem derart, daß keine echte Teilmenge ein Erzeugendensystem ist.

Basis, linear unabhängig

Ein Erzeugendensystem B heißt *Basis* von M, wenn es *linear unabhängig* über R ist, d.h. für je endlich viele paarweise verschiedene Elemente $m_1, \ldots, m_s \in B$ gilt: Ist $0 = \sum_{i=1}^{s} r_i m_i$ mit $r_1, \ldots, r_s \in R$, so folgt $r_1 = \ldots = r_s = 0$.

2.17. Bemerkung. (i) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $R/\mathfrak{a}$ ein R-Modul mit unverkürzbarem Erzeugendensystem $\{1 \bmod \mathfrak{a}\}$.

(ii) Ist $R = K$ ein Körper, so ist jedes unverkürzbare Erzeugendensystem eine Basis. Ist R kein Körper, so sind minimale Erzeugendensysteme i.a. *keine* Basis.

Beispiel: $R = K[X]$, $\mathfrak{a} = (X^3)$, dann ist $X^3 \neq 0$ in R, aber $X^3(1 \bmod \mathfrak{a}) = 0$ in $R/\mathfrak{a}$. $R/\mathfrak{a}$ hat keine Basis als R-Modul, denn für alle $m \in R/\mathfrak{a}$ ist $X^3 \cdot m = 0$.

Als $R/\mathfrak{a}$-Modul hat $R/\mathfrak{a}$ die Basis $\{1_R \bmod \mathfrak{a}\}$, denn aus $(r \bmod \mathfrak{a}) \cdot (1 \bmod \mathfrak{a}) = 0$ in $R/\mathfrak{a}$ für $r \in R$ folgt $r \in \mathfrak{a}$, d.h. $r \bmod \mathfrak{a} = 0$ in A.

Allgemein: Jeder Ring A hat als A-Modul die Basis $\{1_A\}$.

(iii) Die Elementanzahl eines unverkürzbarer Erzeugendensysteme ist im allgemeinen nicht eindeutig bestimmt.

2.18. Definition. Es sei $(M_\lambda)_{\lambda\in\Lambda}$ eine Familie von R-Moduln. Dann ist

direkte Summe $\bigoplus_{\lambda\in\Lambda} M_\lambda$

$$\bigoplus_{\lambda\in\Lambda} M_\lambda := \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda \text{ für alle } \lambda \in \Lambda \text{ und } m_\lambda = 0 \text{ für fast alle } \lambda\}$$

mit der durch

$$(m_\lambda)_{\lambda\in\Lambda} + (n_\lambda)_{\lambda\in\Lambda} := (m_\lambda + n_\lambda)_{\lambda\in\Lambda}$$

definierten Addition und der durch

$$r(m_\lambda)_{\lambda\in\Lambda} := (r \cdot m_\lambda)_{\lambda\in\Lambda}$$

definierten Skalarmultiplikation ein R-Modul, der die *direkte Summe* von $(M_\lambda)_{\lambda\in\Lambda}$ genannt wird.

Ist $M_\lambda = R$ für alle $\lambda \in \Lambda$, so schreibt man $R^{(\Lambda)} := \bigoplus_{\lambda\in\Lambda} M_\lambda$. Hat Λ $n < \infty$ viele Elemente, so schreibt man R^n statt $R^{(\Lambda)}$. Man setzt $R^0 := \{0_R\}$. $R^{(\Lambda)}$, R^n

Ein R-Modul heißt *frei*, wenn er isomorph zu einem R-Modul der Form $R^{(\Lambda)}$ ist. freie Moduln

2.19. Bemerkung. (i) Die Elemente von R^n sind n-Tupel $(r_1, \dots, r_n)$ mit $r_i \in R$.

(ii) Jeder freie R-Modul $R^{(\Lambda)}$ besitzt die *kanonische Basis* $(e_\lambda)_{\lambda\in\Lambda}$ mit $e_\lambda = (\delta_{\mu\lambda})_{\mu\in\Lambda}$.

2.20. Satz. *Es sei M ein R-Modul. Dann gilt*

(a) M ist endlich erzeugt genau dann, wenn M isomorph zu einem Faktormodul eines endlich erzeugten freien Moduls ist.

(b) M ist frei genau dann, wenn M eine Basis hat. frei $\leftrightarrow$ Basis

Beweis. (a) "$\Rightarrow$" Es sei $M = (m_1, \dots, m_s)$. Dann ist die Abbildung $\varphi : R^s \to M, (r_1, \dots, r_s) \mapsto r_1 m_1 + \ldots + r_s m_s$ ein surjektiver Homomorphismus, also $M = \operatorname{Im}\varphi \cong R^s / \operatorname{Kern}\varphi$ nach Homomorphiesatz.

"$\Leftarrow$" Nach Voraussetzung haben wir R-Modulhomomorphismen $R^s \xrightarrow{\pi} R^s/N \xrightarrow[\sim]{\psi} M$, wobei ψ ein Isomorphismus ist. Da π surjektiv ist, ist auch $\varphi := \psi \circ \pi$ surjektiv. Ist $\{e_1, \dots, e_s\}$ eine Basis von R^s, so ist $\{\varphi(e_1), \dots, \varphi(e_s)\}$ ein Erzeugendensystem von M. (Denn $m = \varphi(\sum r_i e_i) = \sum r_i \varphi(e_i)$).

(b) Die Abbildung φ im ersten Teil des Beweises von (a) ist injektiv (also ein Isomorphismus) genau dann, wenn $\{m_1, \dots, m_s\}$ linear unabhängig ist.

□

2.21. Beispiel. Es sei $R = K[x,y,z]$. Dann ist $M = ((x,y),(y,z)) \subseteq R^2$ ein Untermodul des R^2. Folglich ist R^2/M ein R-Modul, der durch die Restklassen $\overline{e}_1, \overline{e}_2$ von $(1,0)$ bzw. $(0,1)$ erzeugt wird.

Die Elemente von R^2/M sind von der Form

$$(r_1,r_2) + M = r_1(1,0) + r_2(0,1) + M = r_1[(1,0)+M] + r_2[(0,1)+M] = r_1\overline{e}_1 + r_2\overline{e}_2.$$

2.22. Definition. Es sei F ein endlich erzeugter freier R-Modul. Dann heißt die Anzahl der Elemente einer (jeder) Basis von F der *Rang* von F. Er ist wohldefiniert nach Übung 15.

Rang

[Tip: Zurückführen auf Situation bei Vektorräumen.]

Ist $R = K$ ein Körper, so ist der Rang von F gerade die Vektorraumdimension.

2.23. Definition. Sei M ein R-Modul.

$\mathfrak{a} \cdot M$

(i) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist das Produkt
$$\mathfrak{a} \cdot M := \left\{ \sum_{i=1}^{s} a_i m_i \,\middle|\, s \in \mathbb{N}, a_i \in \mathfrak{a}, m_i \in M \right\}$$
ein Untermodul von M.

(ii) Ist N ein Untermodul von M, so ist
$$N : M := N :_R M := \{ r \in R \mid r \cdot M \subseteq N \}$$
ein Ideal von R, genannt *Quotientenideal*.

Quotientenideal $N : M$

Annulator $\mathrm{Ann}_R M$

(iii) Das Ideal $0 :_R M = \{ r \in R \mid r \cdot M = 0 \}$ heißt der *Annulator* von M. Bezeichnung $\mathrm{Ann}_R M$.

2.24. Beispiel. (i) $\mathrm{Ann}_R(R) = (0_R)$, denn $r1_R = 0_R$ genau dann, wenn $r = 0_R$. Ist F ein freier R-Modul, so ist $\mathrm{Ann}_R(F) = (0_R)$.

(ii) $\mathrm{Ann}_R(R/\mathfrak{a}) = \mathfrak{a}$.

(iii) Der Modul R^2/M aus Beispiel (2.21) ist nicht frei, denn:
$$(xz - y^2)(1,0) = z(x,y) + (-y)(y,z) \in M$$
und
$$(xz - y^2)(0,1) = (-y)(x,y) + x(y,z) \in M,$$
also $0 \neq xz - y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \in \mathrm{Ann}_R(R^2/M)$.

2.25. Lemma. *Es sei M ein R-Modul, und es sei $\mathfrak{a} \subseteq \mathrm{Ann}_R(M)$ ein Ideal. Dann besitzt M auch eine $(R/\mathfrak{a})$-Modulstruktur.*

Beweis. Wir übernehmen die Addition von M als R-Modul, aber wir definieren eine neue skalare Multiplikation durch
$$\overline{r} \cdot m := (r + \mathfrak{a}) \cdot m := rm \qquad \text{für } r \in R,\ m \in M.$$
Dies ist unabhängig von der Auswahl des Repräsentanten r der Restklasse $r + \mathfrak{a}$, da $a \cdot M = 0$, also wohldefiniert und leistet das Gewünschte. □

2.26. Beispiel. (i) Ist $\mathfrak{a}$ ein Ideal von R, so ist $R/\mathfrak{a}$ auch ein $R/\mathfrak{b}$-Modul für jedes Ideal $\mathfrak{b}$ mit $\mathfrak{b} \subseteq \mathrm{Ann}_R(R/\mathfrak{a}) = \mathfrak{a}$.

(ii) Ist M ein R-Modul und ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $M/\mathfrak{a}M$ ein $R/\mathfrak{a}$-Modul, denn $\mathfrak{a} \subseteq \mathrm{Ann}_R(M/\mathfrak{a}M)$.

$\mu_R(M)$

2.27. Definition. Es sei M ein endlich erzeugter R-Modul. Dann bezeichnen wir mit $\mu(M) := \mu_R(M)$ die minimale Anzahl der Elemente eines Erzeugendensystems von M als R-Modul.

minimale Erzeugendensysteme

Ein Erzeugendensystem mit $\mu(M)$ Elementen heißt ein *minimales Erzeugendensystem*.

Ist $R = K$ ein Körper, also M ein endlich erzeugter K-Vektorraum, so ist ein Erzeugendensystem von M unverkürzbar genau dann, wenn es minimal ist, genau dann, wenn es eine Basis ist. Dann ist $\mu(M) = \dim_K(M)$.

Ist R kein Körper, so müssen unverkürzbare Erzeugendensysteme, nicht minimal sein. Betrachte $(1-x,x) = (1) = K[x]$.

Wir wollen nun sehen, daß die Situation über lokalen Ringen besser ist.

2.28. Definition. Ist R ein Ring, so nennt man den Durchschnitt $\mathrm{Rad}(R)$ aller maximalen Ideale von R das *Jacobson-Radikal* von R. $\mathrm{Rad}(R)$ ist ein Ideal von R.

Jacobson-Radikal
$\mathrm{Rad}(R)$

2.29. Beispiel. (i) $\mathrm{Rad}(K[x_1,\dots,x_n]) = (0)$.

(ii) Ist $(R,\mathfrak{m})$ ein lokaler Ring mit dem (einzigen) maximalen Ideal $\mathfrak{m}$, so ist $\mathrm{Rad}(R) = \mathfrak{m}$.

2.30. Lemma. *Für ein Element a eines Ringes R sind äquivalent:*

(a) $a \in \mathrm{Rad}(R)$,

(b) $1-ab \in R^\times$ *für alle* $b \in R$.

Beweis. (a)⇒(b): Ist $1-ab \notin R^\times$, also $(1-ab)R \neq R$, so gibt es ein maximales Ideal $\mathfrak{m}$ vom R mit $1-ab \in \mathfrak{m}$. Wegen $a \in \mathrm{Rad}(R) \subseteq \mathfrak{m}$ ist auch $ab \in \mathfrak{m}$, folglich $1 = (1-ab)+(ab) \in \mathfrak{m} \neq R$, Widerspruch. (b)⇒(a): Antithese: Es sei $\mathfrak{m}$ ein maximales Ideal von R mit $a \notin \mathfrak{m}$. Dann ist $aR+\mathfrak{m} = R$, also $ab+r = 1$ für geeignete $b \in R$, $r \in \mathfrak{m}$. Daher ist $1-ab = r \in \mathfrak{m}$ keine Einheit, Widerspruch. □

2.31. Bemerkung. Ist $(R,\mathfrak{m})$ ein lokaler Ring, so ist $R^\times = R\backslash\mathfrak{m}$.

Beweis. Es ist klar, daß $\mathfrak{m} \not\subseteq R^\times$, also $R^\times \subseteq R\backslash\mathfrak{m}$.

Ist umgekehrt $a \in R\backslash\mathfrak{m}$, aber $a \notin R^\times$, also $aR \neq R$, so muß a im einzigen maximalen Ideal enthalten sein, also $a \in \mathfrak{m}$, Widerspruch. □

2.32. Lemma (Lemma von Nakayama (1912-1964)). *Ist M ein endlich erzeugter R-Modul und* $\mathfrak{a} \subseteq R$ *ein Ideal mit* $\mathfrak{a} \subseteq \mathrm{Rad}(R)$, *so folgt aus* $\mathfrak{a}M = M$ *schon* $M = 0$.

Beweis. Nach Voraussetzung besitzt M ein minimales Erzeugendensystem $\{m_1,\dots,m_s\}$. Antithese: $s > 0$. Wegen $\mathfrak{a}M = M$ gibt es dann eine Gleichung $m_s = \sum_{i=1}^{s} a_i m_i$ mit $a_i \in \mathfrak{a}$, also $(1-a_s)m_s = \sum_{i=1}^{s-1} a_i m_i$. Wegen $a_s \in \mathfrak{a} \subseteq \mathrm{Rad}(R)$ ist $1-a_s$ eine Einheit (nach 2.30), also $m_s \in Rm_1+\ldots+Rm_{s-1}$ im Widerspruch zur vorausgesetzten Minimalität von $\{m_1,\dots,m_s\}$. □

2.33. Folgerung. Ist $(R,\mathfrak{m})$ ein lokaler Ring, $K := R/\mathfrak{m}$ und M ein endlich erzeugter R-Modul, so sind für Elemente $m_1,\dots,m_s$ äquivalent:

(a) $M = Rm_1+\ldots+Rm_s$,

(b) die Restklassen $\overline{m}_1,\dots,\overline{m}_s \in M/\mathfrak{m}M$ der $m_i \in M$ bilden ein Erzeugendensystem des K-Vektorraumes $M/\mathfrak{m}$.

Beweis. (a)⇒(b) klar.

(b)⇒(a) Aus $M/\mathfrak{m}M = Km_1+\ldots+Km_s$ folgt für $N := Rm_1+\ldots+Rm_s$ aber $M = N+\mathfrak{m}M$, also $M/N = \mathfrak{m}\cdot(M/N)$. [da $(M/N)/\mathfrak{m}(M/N) = (M/N)/((N+\mathfrak{m}M)/N) \cong M/(N+\mathfrak{m}M) = 0$] Aus dem Nakayama-Lemma folgt nun $M/N = 0$, also $M = N$. □

2.34. Folgerung. Unter den Voraussetzungen von (2.33) gelten:

(a) $\mu(M) = \dim_K(M/\mathfrak{m}M)$,

(b) $\{m_1,\dots,m_s\} \subseteq M$ ist ein minimales Erzeugendensystem von M genau dann, wenn $\{\overline{m}_1,\dots,\overline{m}_s\}$ eine K-Basis von $M/\mathfrak{m}M$ ist.

(c) (Auswahlsatz) Jedes Erzeugendensystem von M enthält ein minimales Erzeugendensystem. Jedes unverkürzbare Erzeugendensystem ist minimal.

(d) (Ergänzungssatz) Elemente $m_1,\dots,m_s \in M$ lassen sich zu einem minimalen Erzeugendensystem ergänzen genau dann, wenn ihre Restklassen $\overline{m}_1,\dots,\overline{m}_s \in M/\mathfrak{m}M$ linear unabhängig über K sind.