

M2: Wie viele Moduln gibt es?

Freie Moduln

1. Def: Sei M ein R -Rechtsmodul. Eine Familie von Elementen $\{m_i\}_{i \in I}$ heißt ...

linear unabhängig
Erzeugendensystem
Basis von M } [genau wie bei Vektorräumen]

M heißt endlich erzeugt, falls M ein endliches Erzeugendensystem besitzt.

M heißt frei, falls M eine Basis besitzt.

Sein Rang ist dann die Kardinalität einer Basis (meistens wohldefiniert, s.u.)

2. Bsp

(a) Ist $R = K$ ein Körper, so ist jeder Modul frei, und den Rang nennen wir „Dimension“.

Jeder endlich-erzeugte K -Modul ist isomorph

zu $K^{\oplus m} := \underbrace{K \times \dots \times K}_m$ mit Koordinatenweiser Add. & Skalarmultiplikation

für ein $m \in \mathbb{N}_0$.

(b) Analog ist für jeden Ring R $R^{\oplus m}$ ein freier R -Modul von Rang m . Genauer:

M endlich erzeugt frei $(\Leftrightarrow) M \cong R^{\oplus m}$
für ein $m \in \mathbb{N}_0$

(c) Ist $R = \mathbb{Z}$, so sind die freien R -Moduln gerade die freien abelschen Gruppen.

Diese sind nie divisibel,

$$\begin{array}{c} \uparrow \\ \forall m \in M, n \in \mathbb{N}: \exists m' \in M: m = n \cdot m' \\ \text{(scheitert, wenn } m \text{ ein Basiselement ist)} \end{array}$$

außerdem torsionsfrei $\leftarrow (\forall m \in M, n \in \mathbb{N}: n \cdot m = 0 \Rightarrow m = 0)$

$(\mathbb{S}^1, \cdot), (\mathbb{C}^\times, \cdot)$ nicht frei (divisibel, enthält Torsion)
nicht endlich erzeugt

$(\mathbb{Q}, +), (\mathbb{R}, +)$ nicht frei (divisibel),
nicht endlich erzeugt

\mathbb{Z}/n nicht frei (enthält Torsion)
endlich erzeugt

Die endlich erzeugten \mathbb{Z} -Moduln sind alle isomorph zu

$$\mathbb{Z}^{\oplus m} \oplus \mathbb{Z}/n_1 \oplus \dots \oplus \mathbb{Z}/n_k$$

für gewisse $m, k, n_1, \dots, n_k \in \mathbb{N}_0$ (siehe unten).

Diese sind genau dann frei, wenn sie torsionsfrei sind.

3. **Notiz:** \mathbb{R} -rechtslineare Abbildungen $\mathbb{R} \rightarrow \mathbb{R}$ entsprechen 1:1 Elementen von \mathbb{R}

$$\begin{aligned} \text{Hom}_{\mathbb{R}}(\mathbb{R}, \mathbb{R}) &\cong \mathbb{R} \\ \left(\begin{array}{l} r \mapsto a \cdot r \\ f \end{array} \right) &\leftarrow a \\ &\mapsto f(1) \end{aligned}$$

Allgemeiner:

4. **Satz:** Morphismen zwischen endlich-erzeugten freien \mathbb{R} -Rechtsmodulen entsprechen 1:1 Matrizen mit Einträgen in \mathbb{R} :

$$\begin{aligned} \text{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R}^m) &\cong \text{Mat}_{m \times n}(\mathbb{R}) \\ \left(\begin{array}{l} \left(\begin{array}{c} r_1 \\ \vdots \\ r_n \end{array} \right) \mapsto A \cdot \begin{array}{c} r_1 \\ \vdots \\ r_n \end{array} \end{array} \right) &\leftarrow A \end{aligned}$$

Das ist \mathbb{R} -Rechtslinear!

□

5. **Satz:** Sei \mathbb{R} ein Ring mit einem surjektiven Ringhomomorphismus $\mathbb{R} \rightarrow \mathbb{R}'$ zu einem kommutativen Ring \mathbb{R}' . Dann ist der Rang eines endlich-erzeugten freien \mathbb{R} -Moduls eindeutig bestimmt ($\mathbb{R}^n \cong \mathbb{R}^m \Rightarrow n = m$).

Insbesondere gilt das also für

- kommutative Ringe \mathbb{R} (Wähle $\mathbb{R}' = \mathbb{R}$).
- $\mathbb{R} = \mathbb{Z}[G]$ ($\exists \mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}$)

Beweis:

Wähle maximales Ideal \mathfrak{m} in R , $k := R/\mathfrak{m}$ Körper

Definiere $\mathfrak{m} := \ker(R \rightarrow R' \rightarrow k)$, sodass also

gilt: $R/\mathfrak{m} \cong k$ (Ringisomorphismus).

beidseitiges Ideal

Für jeden R -Rechtsmodul M haben wir einen
Rechtsuntermodul $M \cdot \mathfrak{m}$ (Linearkombination in M mit
Koeffizienten in \mathfrak{m}),

und Quotientenmodul $M/M \cdot \mathfrak{m}$ ist ein k -Modul,
also ein k -VR. Zum Beispiel ist

$$R^{\oplus n} / R^{\oplus n} \mathfrak{m} \cong \left(\frac{R}{\mathfrak{m}} \right)^{\oplus n} \cong k^{\oplus n}$$

Für jeden Morphismus $M_1 \xrightarrow{f} M_2$ in Mod_R haben
wir einen induzierten Morphismus \bar{f} , und dieser ist
 k -linear.

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ \downarrow & & \downarrow \\ M_1 / M_1 \mathfrak{m} & \xrightarrow{\exists! \bar{f}} & M_2 / M_2 \mathfrak{m} \end{array}$$

(Universelle
Eigenschaft des
Quotienten)

Wir erhalten so einen Funktor

$$\text{"mod } \mathfrak{m}\text{"}: \text{Mod}_R \rightarrow \text{Vec}_k.$$

Falls $R^{\oplus n} \cong R^{\oplus m}$, liefert Funktor $k^{\oplus n} \cong k^{\oplus m}$, also $n = m$.

□

6. Satz: Jede kurze exakte Sequenz in ModR von der Form

$$0 \rightarrow M \xrightarrow{f} N \xrightarrow{g} R^{\oplus n} \rightarrow 0 \quad (n \in \mathbb{N})$$

spaltet: $\exists N \leftarrow_s R^{\oplus n}$ mit $g \circ s = \text{id}$.

Insbesondere ist $N \cong M \oplus R^{\oplus n}$.

$M \times R^{\oplus n}$ mit Koordinatenweiser Add. & Skalarmultiplikation



i.A. falsch, z.B. spaltet

$$0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \rightarrow \mathbb{Z}/2 \rightarrow 0 \text{ nicht.}$$

Beweis:

Da $R^{\oplus n}$ frei, reicht es, s auf Elementen einer Basis zu definieren. Wähle dazu zu jedem Basiselement ein beliebiges Urbild unter g .

Für Isomorphismus $N \cong M \oplus R^{\oplus n}$ wende Fünferlemma an auf:

$$m \mapsto \begin{pmatrix} m \\ 0 \end{pmatrix}; \begin{pmatrix} m \\ x \end{pmatrix} \mapsto x$$

$$\begin{array}{ccccccc} 0 & \rightarrow & M & \rightarrow & M \oplus R^{\oplus n} & \rightarrow & R^{\oplus n} \rightarrow 0 \\ & & \text{id} \downarrow \cong & & \downarrow (f \ s) & & \text{id} \downarrow \cong \\ 0 & \rightarrow & M & \xrightarrow{f} & N & \xrightarrow{g} & R^{\oplus n} \rightarrow 0 \end{array} \quad \text{exakt}$$

$$(f \ s) \begin{pmatrix} m \\ x \end{pmatrix} := f(m) + s(x)$$

Zu zeigen: das kommutiert!

$$\begin{array}{ccc} m \mapsto \begin{pmatrix} m \\ 0 \end{pmatrix} & \begin{pmatrix} m \\ x \end{pmatrix} \mapsto x & \\ \downarrow & \checkmark & \downarrow \\ m \mapsto f(m) & f(m) + s(x) \mapsto \underbrace{g(f(m))}_0 + \underbrace{g(s(x))}_x & \end{array}$$

wegen Exaktheit \square

Moduln über Hauptidealringen

7. Def.: Ein Hauptidealring (HIR) ist ein (kommutativer) Integritätsring, in dem jedes Ideal von einem einzigen Element erzeugt wird.

Ein Integritätsring ist ein Ring $R \neq 0$, in dem es keine echten Nullteiler (also keine Nullteiler außer Null) gibt.

8. Bsp.:

(a) \mathbb{Z}	\mathbb{Z}/n	\mathbb{Z}/p	\mathbb{Q}	\mathbb{R}	$\mathbb{Z}[G]$
	(n nicht prim, $n \neq 1$)	(p prim)			
<u>HIR</u>	X	<u>alle Körper sind HIR</u>			X (u. A nicht kommutativ)

(b) Für jeden Körper K ist der Polynomring $K[X]$ ein HIR.

Hingegen ist $\mathbb{Z}[X]$ kein HIR (\mathbb{Z}, X)

Auch $K[X, Y]$ ist kein HIR. (X, Y)

(c) Der Nullring ist kein HIR, denn Nullring ist per Def. kein Integritätsring.

9. Satz: Ein kommutativer Ring $R \neq 0$ ist genau dann ein HIR, wenn jeder Untermodul U eines endl. erzeugten freien R -Moduls F wieder frei ist mit $\text{Rang}(U) \leq \text{Rang}(F)$.



$\text{Rang}(U) = \text{Rang}(F)$ ist auch für echte Untermoduln ($U \subsetneq F$) möglich, z. B.
 $n \cdot \mathbb{Z} \subsetneq \mathbb{Z}$



Für beliebige Ringe sieht die Welt anders aus, z. B.:

$$R = \mathbb{Z}[x]$$

Der freie R -Modul von Rang 1, R , besitzt Untermodul $(\mathbb{Z}, x) \subseteq R$, der nicht frei ist.

$$R = \mathbb{Z}[x_1, x_2, x_3, \dots]$$

Der freie R -Modul von Rang 1, R , besitzt freien Untermodul von unendlichem Rang:

$$U = (x_1, x_2, x_3, \dots)$$

Beweis:

($\uparrow\uparrow$) Ist $I \subseteq R$ Ideal, so ist I nach Annahme frei von $\text{Rang} I \leq 1$. Also wird I von nur einem Element erzeugt.

Ferner ist R Integritätsring:

Für jedes $0 \neq a \in R$ haben wir einen R -linearen Iso

Sei ferner $0 \neq b \in R$.

$$\begin{array}{ccccc}
 f(1) \cdot a & a \cdot R & \xleftarrow[\cong]{f} & R & \xrightarrow{1} \\
 \downarrow \cdot b & \downarrow \cdot b & & \downarrow \cdot b & \downarrow \\
 f(1) \cdot a \cdot b & a \cdot R & \xleftarrow[\cong]{f} & R & \\
 \uparrow \neq 0 & & \text{(R-linear)} & & \uparrow b \neq 0 \\
 \text{da } f \text{ Iso} & & & &
 \end{array}$$

Also ist $a \cdot b \neq 0$

(\Downarrow) Sei $U \subseteq R^{\oplus n}$. Induktion über n .

IA: $n=0$ ✓

IS: Sei $U \subseteq R^{\oplus n} \oplus R$. Betrachte kurze exakte Seq.:

$$0 \rightarrow U \cap (0 \oplus R) \rightarrow U \xrightarrow{\pi} \frac{U}{U \cap (0 \oplus R)} \rightarrow 0$$

• $U \cap (0 \oplus R)$ ist Untermodul von $0 \oplus R \cong R$, also nach Def. von HIR frei von Rang ≤ 1 .

• $\frac{U}{U \cap (0 \oplus R)} \cong \frac{R^{\oplus n} \oplus R}{0 \oplus R} \cong R^{\oplus n}$, ist also

nach IV frei von Rang $\leq n$.

Also hat die exakte Sequenz die Form:

$$0 \rightarrow R^a \rightarrow U \rightarrow R^b \rightarrow 0$$

mit $a \leq 1$, $b \leq n$. Aus Satz 6 folgt nun:

$$U \cong R^a \oplus R^b = R^{a+b}$$

mit $a+b \leq n+1$. □

10. Schwacher Struktursatz für Moduln / HIR

Jeder endlich-erzeugte Modul über einem HIR R ist isomorph zu

$$R^{\oplus n} \oplus \frac{R}{R \cdot d_1} \oplus \dots \oplus \frac{R}{R \cdot d_k}$$

für gewisse $n, k \in \mathbb{N}_0$, $d_1, \dots, d_k \in R$.

Beweisskizze:

Sei M so ein Modul. Da M endlich erzeugt ist,

\exists Epimorphismus $R^{\oplus N} \rightarrow M$ ($N \in \mathbb{N}_0$)

Der Kern ist frei von Rang $k \in N$ (da R HIR),

also haben wir k.e.S.:

$$0 \rightarrow R^{\oplus k} \xrightarrow{f} R^{\oplus N} \rightarrow M \rightarrow 0$$

Diagonalisiere die Matrix, die f beschreibt.

$$\begin{array}{c} \begin{array}{|c|} \hline \left(\begin{array}{ccc} 0 & & \\ \vdots & & \\ 0 & & \\ d_1 & \dots & \\ \vdots & & \\ & & d_k \end{array} \right) \\ \hline \end{array} \\ \begin{array}{l} \uparrow N \\ \downarrow N \end{array} \end{array} \quad \begin{array}{l} \leftarrow k \\ \rightarrow k \end{array} \quad \begin{array}{l} \uparrow n = N - k \\ \downarrow k \end{array}$$

Dann ist also $M \cong \frac{R^{\oplus N}}{\left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ d_1 \dots \\ \vdots \\ d_k \end{array} \right) \cdot R^{\oplus k}} = \dots \checkmark$

□