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 $K^{\oplus m} := \underbrace{K \times \dots \times K}_{m \text{ Faktoren}}$ 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:

$$M \text{ endlich erzeugt frei} \iff M \cong R^{\oplus m} \text{ für ein } m \in \mathbb{N}_0$$

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

$\forall m \in M, n \in \mathbb{N}: \exists m' \in M: \; m = n \cdot m'$
(scheitert, wenn m ein Basiselement ist)

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

$(S^1, \cdot), (\mathbb{C}^*, \cdot)$ 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

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

für gewisse $m, k, n_1, \ldots, n_k \in \mathbb{N}_0$ (siehe unten).
Diese sind genau dann frei, wenn sie torsionsfrei sind.

3. Notiz: R-rechtslineare Abbildungen $R \longrightarrow R$ entsprechen 1:1 Elementen von R

$$\begin{aligned} \mathrm{Hom}_R(R,R) &\cong R \\ (r \mapsto a\cdot r) &\leftarrow\!\shortmid a \\ f &\mapsto f(1) \end{aligned}$$

Allgemeiner:

4. Satz: Morphismen zwischen endlich-erzeugten freien R-Rechtsmoduln entsprechen 1:1 Matrizen mit Einträgen in R:

$$\mathrm{Hom}_R(R^n, R^m) \cong \mathrm{Mat}_{m\times n}(R)$$

$$\underbrace{\left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \mapsto A \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right)}_{\text{Das ist } R\text{-Rechtslinear!}} \leftarrow\!\shortmid A$$

$\square$

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

Insbesondere gilt das also für

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

Beweis:

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

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

$$R/\mathfrak{m} \cong k \qquad \text{(Ringisomorphismus).}$$

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

$$R^{\oplus n} / R^{\oplus n} \cdot \mathfrak{m} \cong (R/\mathfrak{m})^{\oplus n} \cong k^{\oplus n}$$

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

$$\begin{tikzcd}
M_1 \arrow[r, "f"] \arrow[d, two heads] \arrow[rd, bend left=60, "0"] & M_2 \arrow[d, two heads] \\
M_1 / M_1 \cdot \mathfrak{m} \arrow[r, dashed, "\exists! \bar{f}"] & M_2 / M_2 \cdot \mathfrak{m}
\end{tikzcd}$$

(Universelle Eigenschaft des Quotienten)

Wir erhalten so einen Funktor

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

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

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

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

spaltet: $\quad \exists\, N \xleftarrow{s} R^{\oplus n}$ mit $g \circ s = \mathrm{id}$.

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

$M \times R^{\oplus n}$ mit koordinaten-weiser Add. & Skalarmultiplikation

⚠ i.A. falsch, z.B. spaltet

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

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:

$m \mapsto \binom{m}{0}$; $\binom{m}{x} \mapsto x$

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\mathrm{id}"', "\cong"] & M \oplus R^{\oplus n} \arrow[r] \arrow[d, "(f\ s)"] & R^{\oplus n} \arrow[r] \arrow[d, "\mathrm{id}"', "\cong"] & 0 \\
0 \arrow[r] & M \arrow[r, "f"'] & N \arrow[r, "g"'] & R^{\oplus n} \arrow[r] & 0
\end{tikzcd}$$

exakt

$$(f\ s)\binom{m}{x} := f(m) + s(x)$$

Zu zeigen: das kommutiert!

$$\begin{tikzcd}
m \arrow[r, mapsto] \arrow[d, mapsto] \arrow[dr, phantom, "\checkmark"] & \binom{m}{0} \arrow[d, mapsto] \\
m \arrow[r, mapsto] & f(m)
\end{tikzcd}
\qquad
\begin{tikzcd}
\binom{m}{x} \arrow[r, mapsto] \arrow[d, mapsto] \arrow[dr, phantom, "\checkmark"] & x \arrow[d, mapsto] \\
f(m)+s(x) \arrow[r, mapsto] & \underbrace{g(f(m))}_{0} + \underbrace{g(s(x))}_{x}
\end{tikzcd}$$

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) $\mathbb{Z}$ — HIR

$\mathbb{Z}/_n$ (n nicht prim, $n \neq 1$) — ×

$\mathbb{Z}/_p$ (p prim), $\mathbb{Q}$, $\mathbb{R}$ — alle Körper sind HIR

$\mathbb{Z}[G]$ — × (u. A. nicht kommutativ)

(b) Für jeden Körper K ist der Polynomring $K[X]$ ein HIR.
Hingegen ist $\mathbb{Z}[X]$ kein HIR $\quad (2, X)$
Auch $K[X,Y]$ ist kein HIR. $\quad (X, Y)$

(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 $\operatorname{Rang}(U) \leq \operatorname{Rang}(F)$.

⚠ $\operatorname{Rang}(U) = \operatorname{Rang}(F)$ 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 vom Rang 1, R, besitzt Untermodul $(2, X) \subseteq R$, der nicht frei ist.

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

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

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

Beweis:

($\Uparrow$) Ist $I \subseteq R$ Ideal, so ist I nach Annahme frei von $\operatorname{Rang} I \leq 1$. 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 $0 \neq b \in R$.

$$\begin{tikzcd}
f(1)\cdot a \arrow[d, mapsto] & a\cdot R \arrow[d, "\cdot b"'] & R \arrow[l, "f"', "\cong"] \arrow[d, "\cdot b"] & 1 \arrow[d, mapsto] \arrow[lll, mapsto, bend right] \\
f(1)\cdot a\cdot b & a\cdot R & R \arrow[l, "f"', "\cong"] & b \neq 0 \arrow[lll, mapsto, bend left, "(R\text{-linear})"]
\end{tikzcd}$$

$f(1)\cdot a\cdot b \neq 0$, da f Iso

Also ist $a \cdot b \neq 0$

(⇓) Sei $U \leq R^{\oplus n}$. Induktion über n.

<u>IA:</u> $n = 0$ ✓

<u>IS:</u> Sei $U \leq R^{\oplus n} \oplus R$. Betrachte kurze exakte Seq.:

$$0 \to U \cap (0 \oplus R) \to U \to U / U \cap (0 \oplus R) \to 0$$

- $U \cap (0 \oplus R)$ ist Untermodul von $0 \oplus R \cong R$, also nach Def. von HIR frei von Rang ≤ 1.
- $U / U \cap (0 \oplus R) \leq \dfrac{R^{\oplus n} \oplus R}{0 \oplus R} \cong R^{\oplus n}$, ist also nach IV frei von Rang $\leq n$.

Also hat die exakte Sequenz die Form:

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

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

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

mit $a + b \leq n+1$. $\square$

10. Schwacher Struktursatz für Moduln / HIR

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

$$R^{\oplus n} \oplus R/R\cdot d_1 \oplus \ldots \oplus R/R\cdot d_k$$

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

Beweisskizze:

Sei M so ein Modul. Da M endlich erzeugt ist,
$\exists$ Epimorphismus $\quad R^{\oplus N} \twoheadrightarrow M \quad (N \in \mathbb{N}_0)$

Der Kern ist frei von Rang $k \leq N$ (da R HIR), also haben wir k. e. S.:

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

Diagonalisiere die Matrix, die f beschreibt.

$$\begin{array}{ccc}
 & \overset{k}{\longleftrightarrow} & \\
N \updownarrow & \begin{pmatrix} 0 & & \\ \vdots & & \\ 0 & & \\ d_1 & & \\ & \ddots & \\ & & d_k \end{pmatrix} & \begin{matrix} \updownarrow n = N-k \\ \\ \\ \updownarrow k \end{matrix}
\end{array}$$

Dann ist also $M \cong \dfrac{R^{\oplus N}}{\begin{pmatrix} 0 & & \\ \vdots & & \\ 0 & & \\ d_1 & & \\ & \ddots & \\ & & d_k \end{pmatrix} \cdot R^{\oplus k}} = \ldots$ ✓

$\square$