

§ 5. Moduln über Hauptidealringen

Wir kennen schon Gruppen, Ringe, Körper, Vektorräume. Moduln ergänzen und verallgemeinern diesen Zoo algebraischer Strukturen.

Erinnerung: K Körper, V ein K -Vektorraum, V ist eine abelsche Gruppe $(V, +)$ zusammen mit einer Abbildung (Skalarmultiplikation)

$$K \times V \rightarrow V$$

$$(\lambda, v) \mapsto \lambda v$$

so daß $\lambda(u+v) = \lambda u + \lambda v$

$$(\lambda + \mu)u = \lambda u + \mu u$$

$$\lambda(\mu u) = (\lambda\mu)u$$

$$1u = u$$

$$\forall u, v \in V, \lambda, \mu \in K$$

weiterhin:
↓ mit Eins

5.1 Definition: Sei R ein (nicht notwendig kommutativer) Ring.

Ein Linksmodul über R (oder: R -Linksmodul) M ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Abbildung

$$R \times M \rightarrow M$$

$$(a, m) \mapsto am$$

so daß $a(m+m') = am + am'$

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

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

$$1m = m$$

$$\forall m, m' \in M, a, b \in R$$

Natürlich gibt es auch Rechtsmoduln, mit einer Abbildung

$$? \times ? \rightarrow M$$

und Axiomen $?, ?, ?, ?$

(Achtung: der Modul, die Moduln -

das Modul und die Module finden Sie in Campus oder im Baumarkt)

Beispiele: • Der Ring R ist ein R -Linksmodul durch

$$R \times R \rightarrow R \quad (\text{Multiplikation im Ring})$$

$$(a, m) \mapsto am \quad \text{welche Ringaxiome implizieren die Modulaxiome?}$$

und ein R -Rechtsmodul durch $R \times R \rightarrow R$

$$\text{Wenn } R \text{ nicht kommutativ ist, } (m, a) \mapsto ma$$

z.B. der Ring $\text{Mat}(n \times n, K)$ der $n \times n$ -Matrizen über K , $n > 1$, dann sind die beiden Strukturen verschieden.

• Sei $R = \mathbb{Z}$. Eine abelsche Gruppe M ist ein \mathbb{Z} -Linksmodul durch

$$\begin{matrix} \mathbb{N} \\ \mathbb{N} \end{matrix} (n, m) \mapsto \underbrace{m + \dots + m}_n \quad \text{Axiome nachprüfen}$$

$$(-n, m) \mapsto -(\underbrace{m + \dots + m}_n)$$

$$\text{Und } (0, m) \mapsto 0$$

(und auf dieselbe Weise ein \mathbb{Z} -Rechtsmodul).

Umgekehrt ist ein \mathbb{Z} -Links- (oder Rechts-)modul eine abelsche Gruppe mit Addition $m + m := 2m$

$$\text{additiv Inverse } -m := (-1) \cdot m$$

Axiome abelsche Gruppe nachprüfen

$$\text{und neutralem Element } 0_M := 0_R \cdot m \quad (\text{für beliebiges } m \in M)$$

Das bedeutet: Abelsche Gruppen sind dasselbe wie \mathbb{Z} -Moduln.

• Sei $R = K$. K -Moduln (Links- oder Rechts-) sind dasselbe wie K -Vektorräume.

• Sei $R = \mathbb{Z}$ und S ein Ring. Dann ist $M = S$ ein \mathbb{Z} -Modul, weil jeder Ring eine abelsche Gruppe ist. z.B. als Linksmodul

$$\mathbb{Z} \times S \rightarrow S$$

$$(n, s) \mapsto ns = s + \dots + s$$

Das kann man auch so schreiben: $S \ni 1s, 1s+1s, 1s+\dots+1s, -1s$ usw. \Rightarrow

Es gibt genau einen Ringhomomorphismus $\mathbb{Z} \rightarrow S$, denn $1_{\mathbb{Z}} \mapsto 1_S$ (nach

Definition Ringhomomorphismus) $\Rightarrow n \mapsto \underbrace{1_S + \dots + 1_S}_n, -n \mapsto -(n \cdot 1_S)$

- Modulstrukturen hängen immer eng mit Ringhomomorphismen zusammen: Sei $(M, +)$ eine abelsche Gruppe und $\text{End}(M)$ die Menge aller Gruppenendomorphismen $f: M \rightarrow M$ mit

$$(f+g)(x) = f(x) + g(x)$$

$$\text{und } (fg)(x) = f(g(x))$$

Dann ist $\text{End}(M)$ ein Ring.

Wenn M ein R -Linksmodul ist, dann ist $\ell_a: M \rightarrow M$

(Links-multiplikation mit festem $a \in R$) $x \mapsto ax$

ein Gruppenendomorphismus *warum?* $\Rightarrow \ell_a \in \text{End}(M)$.

Und $R \rightarrow \text{End}(M)$ ist ein Ringhomomorphismus *nachprüfen*

$$a \mapsto \ell_a$$

Sei umgekehrt $\psi: R \rightarrow \text{End}(M)$ ein Ringhomomorphismus. Dann

ist M ein R -Linksmodul mit der gegebenen Addition und der

Abbildung $R \times M \rightarrow M$

$$(a, x) \mapsto \underbrace{\psi(a)}_{\in \text{End}(M)}(x) \quad \text{Axiome nachprüfen}$$

- Sei R ein Ring. Der entgegengesetzte Ring R^{op} (op für "opposite") ist als Menge gleich R , hat dieselbe Addition, aber die entgegengesetzte Multiplikation: $a \cdot_{\text{op}} b := b \cdot a$. R^{op} ist auch ein Ring, mit derselben 1. Die R -Linksmoduln sind genau die R^{op} -Rechtsmoduln.

↳ nachprüfen

- In der Darstellungstheorie betrachtet man Darstellungen (von Ringen oder Gruppen oder...). Darstellungen und Moduln sind das gleiche, aber nicht dasselbe. (Gebildet ausgedrückt: es handelt sich um zwei äquivalente Kategorien.)

- Ein Links- (Rechts-) Ideal in R ist ein R -Links- (Rechts-) Modul.

- Sei K ein Körper, $K[x]$ und $K[y]$ Polynomringe über K .

Sei $R = K[x]$ und $M = K[y]$ und $R \times M \rightarrow M$ definiert durch

$$(d, f(y)) \mapsto d \cdot f(y), \quad (x, f(y)) \mapsto \frac{d}{dy} f(y), \quad (x^2, f(y)) \mapsto \frac{d}{dy} \left(\frac{d}{dy} f(y) \right)$$

welche Modulaxiome sind erfüllt? "Ableitung" usw

• Sei K ein Körper und M ein K -Vektorraum sowie

$\Psi: M \rightarrow M$ eine K -lineare Abbildung, d.h. $\Psi \in \text{End}_K(M)$

Dann wird M ein R -Modul durch

$$R \times M \longrightarrow M \quad \leftarrow \text{z.B. Linksmodul}$$

$$(f(x), m) \longmapsto a_n \Psi^n(m) + a_{n-1} \Psi^{n-1}(m) + \dots + a_1 \Psi(m) + a_0 m$$

$$\underbrace{a_n x^n + \dots + a_1 x + a_0}_u \quad \text{hier muß man die Axiome genauer nachprüfen}$$

Umgekehrt sei N ein $K[x]$ -Modul, d.h. $K[x] \times N \rightarrow N$ erfüllt die Axiome. Dann erfüllt auch die Einschränkung $K \times N \rightarrow N$ die Axiome (ist das eine allgemeine Regel?) $\Rightarrow N$ ist ein K -Vektorraum.

Die Abbildung $\Psi: N \rightarrow N$ ist K -linear warum?

$$n_0 \mapsto x \cdot n_0 \quad (\text{und wohldefiniert})$$

und für $f(x) = a_n x^n + \dots + a_1 x + a_0$ ist $f(x) \cdot n_0 = a_n \Psi^n(n_0) + \dots + a_1 \Psi(n_0) + a_0 n_0$
auf N

Die $K[x]$ -Modulstruktur liefert also eine Vektorraumstruktur auf N plus $\Psi \in \text{End}_K(N)$.

Und die beiden Zuordnungen sind invers zueinander: warum?

$$\text{Also: } \begin{array}{ccc} (M, \Psi) & \xleftrightarrow{1:1} & M \text{ } K[x]\text{-Modul} \\ \uparrow & \swarrow & \leftarrow \in \text{End}_K(M) \\ K\text{-Vektorraum} & & \end{array}$$

Ein $K[x]$ -Modul ist das gleiche wie ein Paar bestehend aus einem K -Modul und einem Endomorphismus.

Als Beispiele von Modulen haben wir also insbesondere:

K -Vektorräume $\rightsquigarrow K$ -Moduln

abelsche Gruppen $\rightsquigarrow \mathbb{Z}$ -Moduln

Endomorphismen von K -Vektorräumen $\rightsquigarrow K[x]$ -Moduln

K , \mathbb{Z} und $K[x]$ sind Hauptidealringe, deshalb betrachten wir in diesem Kapitel Moduln über Hauptidealringen. Durch diese Einschränkung erhalten wir eine Chance auf zugängliche und relativ allgemeine Ergebnisse.

Über den Hauptidealring K (Körper) werden wir nichts Neues lernen, aber er legt eine weitere Einschränkung nahe: In linearen Algebren lernen wir viel über endlich-dimensionale Vektorräume, aber nicht über unendlich-dimensionale - ohne Mengenlehre zu diskutieren, können wir nicht einmal die Existenz von Basen klären.

Von Vektorräumen können wir auch lernen, welche Begriffe wir auf Moduln übertragen sollten: es gibt Untervektorräume, Quotientenvektorräume, lineare Abbildungen zwischen verschiedenen Vektorräumen (nicht nur Endomorphismen) usw. Vieles, aber nicht alles lässt sich direkt verallgemeinern.

5.2 Definition: Sei M ein R -Linksmodul, $N \subset M$ eine Teilmenge. N heißt R -Teilmodul (oder Untermodul) von M : $\Leftrightarrow N$ ist eine Untergruppe der abelschen Gruppe M und die Abbildung $R \times M \rightarrow M$ schränkt ein auf $R \times N \rightarrow N$, wodurch N selbst zu einem R -Modul wird.

Wie beim Untervektorraum-Kriterium kann man auch nachprüfen (für $N \subset M$), daß $0 \in N$, $x+y \in N \forall x,y \in N$ und $ax \in N \forall x \in N, a \in R$.

Dazu muß man nachprüfen, daß $-x = (-1)x$ ist $\forall x \in N$.

\uparrow \nwarrow
 in der abelschen Gruppe Skalarmultiplikation

Zwar
Teilmenge

Etwas allgemeiner kann man (wie bei Untergruppen) auch definieren: Seien N und M R -Moduln. Dann sagen wir: N ist ein Untermodul von M (genauer: isomorph zu einem Untermodul), genau dann wenn es einen injektiven Modulhomomorphismus $\varphi: N \rightarrow M$ gibt.

Das verwendet die folgende Verallgemeinerung von K -linearen Abbildungen:

5.3 Definition: Sei R ein Ring, X und Y R -Moduln. Eine Abbildung $\varphi: X \rightarrow Y$ ist ein Homomorphismus von R -Moduln (ein R -Modulhomomorphismus, R -linear): $\Leftrightarrow \varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2) \quad \forall x_1, x_2 \in X$ und $\varphi(ax) = a\varphi(x) \quad \forall x \in X, a \in R$.
Wenn φ zusätzlich bijektiv ist, heißt es ein R -Modulisomorphismus.
Dann heißen X und Y isomorph als R -Moduln.

Ein Modulhomomorphismus ist insbesondere ein Homomorphismus von abelschen Gruppen.

φ Modulisomorphismus $\Rightarrow \varphi^{-1}$ Modulisomorphismus

$\varphi: X \rightarrow Y$ R -Modulhomomorphismus

$\Rightarrow \text{Kern}(\varphi) = \{x_1 \in X : \varphi(x_1) = 0\}$ ist ein Untermodul von X

und $\text{Im}(\varphi) = \{\varphi(x_1) : x_1 \in X\}$ ist ein Untermodul von Y

Dann ist φ Isomorphismus $\Leftrightarrow \text{Kern}(\varphi) = \{0\}$ und $\text{Im}(\varphi) = Y$.

Isomorphie von Moduln ist eine Äquivalenzrelation.

Beispiele: • Homomorphismen zwischen K -Vektorräumen sind genau Homomorphismen zwischen K -Moduln. $\stackrel{K-}{\Rightarrow} K$ -lineare Abbildungen

• Homomorphismen zwischen \mathbb{Z} -Moduln sind genau Homomorphismen zwischen abelschen Gruppen.

• Was sind Homomorphismen zwischen $K[x]$ -Moduln, wenn wir diese als Paare (M, φ) mit M K -Vektorraum und $\varphi \in \text{End}_K(M)$ betrachten?

M $K[x]$ -Modul $\rightsquigarrow \varphi: M \rightarrow M$ ist der Endomorphismus
 $m \mapsto xm$

N auch $K[x]$ -Modul, $\psi: N \rightarrow N$
 $n \mapsto xn$

$\alpha: M \rightarrow N$ $K[x]$ -Modulhomomorphismus \Rightarrow

$\alpha(\lambda m) = \lambda \alpha(m), \alpha(m_1 + m_2) = \alpha(m_1) + \alpha(m_2) \Rightarrow \alpha$ ist K -linear

$\alpha(xm) = x\alpha(m), \alpha(x^2m) = x^2\alpha(m)$ usw

(*)

das folgt aus (*): $\alpha(x^2m) = x\alpha(xm) = x^2\alpha(m)$

α $K[x]$ -Homomorphismus bedeutet also zwei Bedingungen:

α ist K -linear und

$$(*) \alpha(xm) = x\alpha(m) \quad \forall m, \text{ oder ohne } m: \alpha(x \cdot -) = x \cdot \alpha(-)$$

Vorsicht: x steht hier für zwei (vielleicht sehr verschiedene)

Endomorphismen: Auf M ist x der Vektorraum endomorphismus $\varphi: M \rightarrow M$
und auf N ist x die K -lineare Abbildung $\psi: N \rightarrow N$

$$\leadsto (*) \text{ bedeutet eigentlich: } \alpha \circ \varphi = \psi \circ \alpha$$

Wenn α nun sogar ein Isomorphismus ist, ist es auch ein Vektorraum-Isomorphismus und α^{-1} auch. Dann wird (*) zu

$$(*) \varphi = \alpha^{-1} \circ \psi \circ \alpha \quad (\text{oder } \psi = \alpha \circ \varphi \circ \alpha^{-1})$$

und das bedeutet: Die beiden linearen Abbildungen φ und ψ sind zueinander ähnlich im Sinne der linearen Algebra.

Spezialfall: $M=N$ sind ähnlich endlich-dimensional und eine Basis für $M=N$ wird gewählt. Die darstellenden Matrizen bezüglich dieser Basis sind A und $B: \varphi(v) = Av, \psi(v) = Bv$ für $v \in M=N$.

α Isomorphismus bedeutet: die darstellende Matrix T ist invertierbar (eine Basis transformation) und (*) wird zu

$$(*) A = T^{-1} B T$$

Das ist genau die Bedingung für Ähnlichkeit von Matrizen.

Was haben wir jetzt gezeigt?

(Vektorraum, linearer Endomorphismus) $\xrightarrow{1:1} K[x]$ -Modul

speziell: Ähnlichkeit von zwei Endomorphismen desselben Vektorraums $\xrightarrow{1:1} K[x]$ -Modul-Isomorphismus

speziell: Ähnlichkeit von zwei Matrizen $\xrightarrow{1:1} K[x]$ -Isomorphismus zwischen endlich-dimensionalen Modulen

Frage: rationale / Jordan-Normalform $\xrightarrow{1:1} ???$

Wie sollen wir jetzt weiter vorgehen? Vektorräume (endlicher Dimension) klassifizieren ist einfach. Ein endlich-dimensionaler K -Vektorraum hat Dimension $n \in \mathbb{N}_0$ und (für $n \geq 1$) eine Basis b_1, \dots, b_n . Einen Isomorphismus $V \rightarrow K^n$ können wir definieren durch $\varphi: b_j \mapsto e_j$ (e_1, \dots, e_n : Standardbasis). Damit kennen wir V .

Können wir Basen für beliebige Module definieren? (Abgesehen von mengentheoretischen Schwierigkeiten: schon bei ∞ -dimensionalen Vektorräumen braucht man das Auswahlaxiom für die Existenz von Basen.) Basis: Erzeugendensystem und linear unabhängig. Das ist ein Problem. Beispiele:

• Sei $R = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$ (abelsche Gruppe) für $n \in \mathbb{N}$.

$\Rightarrow \forall m \in M: \underbrace{n \cdot m}_{= \underbrace{m + \dots + m}_{n\text{-mal}}} = 0$ (Restklasse). Aus $\lambda \cdot m = 0_M$ folgt für $\lambda \neq 0$ nicht: $m = 0$

• Sei K ein Körper, $K[x]$ der Polynomring als K -Vektorraum gesehen und $R := \text{End}_K(K[x])$ der Ring der K -linearen Endomorphismen von $K[x]$. Wie sehen "Basen" von R aus? $1_R \in R$ erzeugt $R = R \cdot 1_R$ (jedes Element von R ist ein Vielfaches von 1_R). Und 1_R ist "linear unabhängig": $\lambda \cdot 1_R = 0 \Rightarrow \lambda = 0$. Also verdient es $\{1_R\}$, eine Basis genannt zu werden. Und R scheint R -Dimension 1 zu haben.

Jetzt suchen wir nach einer anderen Basis von R (als R -Modul):

$K[x]$ hat die K -Vektorraum-Basis $1, x, x^2, \dots$. Also können wir ein $f \in \text{End}_K(K[x])$ definieren, indem wir f -Bilder der Basisvektoren festlegen. Sei $f_1: K[x] \rightarrow K[x]$ definiert durch

d.h. $x^i \mapsto 0$ für i ungerade $1 \mapsto 1$
 $x \mapsto 0$
 $x^2 \mapsto x$
 $x^3 \mapsto 0$
 $x^i \mapsto x^{i/2}$ für i gerade.

Analog $f_2: 1 \mapsto 0$, d.h. $x^i \mapsto x^{(i-1)/2}$, ungerade $x^4 \mapsto x^2$
!
 $x \mapsto 1$ $x^i \mapsto 0$, gerade
 $x^2 \mapsto 0$
 $x^3 \mapsto x$
 $x^4 \mapsto 0$
...

$$\Rightarrow f_1 + f_2: X^i \mapsto \begin{cases} X^{i/2}, & i \text{ gerade} \\ X^{(i-1)/2}, & i \text{ ungerade} \end{cases}, \text{ d.h. } \begin{matrix} 1 \mapsto 1 \\ X \mapsto X \\ X^2 \mapsto X \\ X^3 \mapsto X \\ X^4 \mapsto X^2 \\ \dots \end{matrix}$$

Nun seien $g_1, g_2 \in R$.

$g_1 f_1$ bedeutet Komposition

$$\Rightarrow (g_1 f_1 + g_2 f_2) / (X^i) = \begin{cases} g_1 (X^{i/2}), & i \text{ gerade} \\ g_2 (X^{(i-1)/2}), & i \text{ ungerade} \end{cases}$$

Elemente im Links-
modul ${}_R R$

Falls $g_1 f_1 + g_2 f_2 = 0$, folgt $g_1 = 0$ und $g_2 = 0$ warum?

↑
"Struktur"
im Ring R

$\Rightarrow f_1$ und f_2 sind linear unabhängig!

f_1 und f_2 bilden auch ein Erzeugendensystem:

Sei $g \in R$. Dann ist $g = g_1 f_1 + g_2 f_2$, wenn wir g_1 und g_2

definieren durch $g_1 (X^i) := g (X^{2i})$ und $g_2 (X^i) := ?$

$\Rightarrow R$ hat auch eine Basis, die aus 2 Elementen besteht.

$\Rightarrow R \cong R \oplus R = \{ (a, b) : a, b \in R \}$ *nachprüfen: das ist auch ein R -Linksmodul*

durch $f_1 \mapsto (1, 0)$

$f_2 \mapsto (0, 1)$

$g_1 f_1 + g_2 f_2 \mapsto (g_1, g_2)$

*nachprüfen: das ist ein Isomorphismus
von R -Linksmodulen*

$\Rightarrow R \cong R \oplus R = (R \oplus R) \oplus R = \dots = R^n$ für jedes $n \in \mathbb{N}$.
" $R \oplus \dots \oplus R$

Hier kann man also die Dimension des R -Linksmoduls R nicht sinnvoll definieren. Auch deshalb müssen wir die Klasse der betrachteten Ringe einschränken. Aber das erste Beispiel zeigt, daß wir selbst für \mathbb{Z} -Modul im Allgemeinen keine Basis finden.

Unser Ziel ist jetzt, wenigstens bei kommutativen Ringen Moduln zu finden, die eine Basis eindeutiger Größe, also auch eine Dimension haben. Dafür definieren wir ganz allgemein, was Basen überhaupt sind, ohne auch nur Endlichkeit vor auszusetzen.

Auf Links- oder Rechtsmodul wird es nie ankommen, deshalb steht " R -Modul" immer für beides.

5.8 Definition: Sei R ein Ring und $\{M_i: i \in I\}$ eine ^{nichtleere} Menge von R -Modulen.

Das direkte Produkt der M_i ist als Menge das Kartesische Produkt

$$\prod_{i \in I} M_i = \{ (m_i)_{i \in I} : m_i \in M_i \text{ für } i \in I \}$$

mit der Addition $(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)_{i \in I}$

und der R -Modulstruktur $\lambda (m_i)_{i \in I} := (\lambda m_i)_{i \in I}$ für $\lambda \in R$.

Die direkte Summe der M_i ist die Teilmenge von $\prod M_i$, deren Elemente nur an endlich vielen Einträgen ungleich 0 sind:

$$\bigoplus_{i \in I} M_i = \{ (m_i)_{i \in I} : \exists I' \subset I, |I'| < \infty, m_i = 0 \text{ für } i \notin I' \}$$

↑ abhängig von (m_i)

Beweisen Sie die Definition: $\prod M_i$ und $\bigoplus M_i$ sind R -Module.

$\bigoplus M_i$ ist ein Teilmodul von $\prod M_i$.

(Links-)

Sei M ein R -Modul und $x \in M$. Dann ist $f_x: R \rightarrow M$ ein Homomorphismus von R -Linksmodulen. *nachprüfen* $a \mapsto ax$

Der Kern von f_x ist $\text{ann}_R(x) := \{a \in R : ax = 0\}$, ein Linksideal in R , also auch ein Untermodul von ${}_R R$. "ann" steht für "Annulator."

Das Bild von f_x ist ein Untermodul von ${}_R M$, Bezeichnung:

$$Rx = \{ax \mid a \in R\}$$

Dann gilt (wie bei Vektorräumen) ${}_R R / \text{ann}_R(x) \cong_R Rx$ (Modul isomorphismus)

(nachprüfen)

Statt x können wir auch eine Teilmenge von M wählen, dann ist

$$RX := \sum_{x \in X} Rx = \langle X \rangle \subset M$$

↑ der von X erzeugte Linksmodul in M

i.A. keine direkte Summe

RX ist das Bild der R -linearen Abbildung $\bigoplus R \rightarrow M$

($\bigoplus R$ enthält nach Definition Elemente

$$(a_x)_{x \in X} \mapsto \sum_{x \in X} a_x x$$

$(a_x)_{x \in X}$ mit nur endlich vielen Einträgen $\neq 0$)

ℤ(ℤ)

Beispiel: $\mathbb{Z} \xrightarrow{\bar{v}}$ ℤ(ℤ) Projektion ist f_1 , Kern = $n\mathbb{Z} = 0 \text{ in } \mathbb{Z} \ (\bar{1})$

Wenn $R = K$ ein Körper ist und M ein K -Modul, d.h. ein K -Vektorraum, können wir $x_1, \dots, x_n \in M$ wählen und $K^n \xrightarrow{\varphi} \underbrace{Kx_1 + Kx_2 + \dots + Kx_n}_{K\text{-Erzeugnis}} \subset M$ definieren. φ ist genau dann injektiv, wenn x_1, \dots, x_n in M linear unabhängig sind.

Wenn φ zusätzlich surjektiv ist, also ein Isomorphismus $K^n \cong M$, dann sind x_1, \dots, x_n eine Basis von M .

Diese Definition/Charakterisierung funktioniert allgemein:

5.5 Definition: Sei $\{x_i\}_{i \in I}$ eine Menge von Elementen in M , einem R -

K -links-Modul und $\varphi: R^{(I)} \rightarrow M$

$$\bigoplus_{i \in I} R \xrightarrow{\varphi} \sum_{i \in I} R x_i$$

nachprüfen: das existiert und ist R -linear, und es gibt nur eine solche Abbildung

Wenn φ surjektiv ist, heißt $\{x_i\}_{i \in I}$ ein Erzeugendensystem von M (über R).

Wenn φ injektiv ist, heißt $\{x_i\}_{i \in I}$ linear unabhängig (über R).

Wenn φ bijektiv ist, heißt $\{x_i\}_{i \in I}$ eine Basis von M (über R).

Der R -Modul M heißt frei (über R), wenn M eine Basis (über R) besitzt.

$\{x_i\}_{i \in I}$ linear unabhängig heißt also: $\text{Kern } \varphi = 0$, d.h. $\sum_{\text{endlich}} a_i x_i = 0 \Rightarrow$ alle $a_i = 0$.

$\{x_i\}_{i \in I}$ Erzeugendensystem bedeutet: jedes $m \in M$ ist von der Form

$$m = \sum_{\text{endlich}} a_i x_i.$$

$\{x_i\}_{i \in I}$ Basis bedeutet: Erzeugendensystem und linear unabhängig.

$\mathbb{Z}/n\mathbb{Z}$ hat Erzeugendensystem $\bar{1}$ (oder \bar{e} mit $\text{ggT}(e, n) = 1$), aber $\bar{1}$ ist nicht linear unabhängig. $\mathbb{Z}/n\mathbb{Z}$ ist kein freier \mathbb{Z} -Modul.

Für $R = \mathbb{Z}/n\mathbb{Z}$ ist $M = \mathbb{Z}/n\mathbb{Z}$ ein freier Modul. Der R -Modul ${}_R R$ ist frei für jeden Ring R .

Wir haben schon gesehen, daß die Dimension eines freien Moduls im Allgemeinen nicht wohldefiniert ist: $\mathbb{R} = \mathbb{R}^n$ bzw. $M \subseteq M_K$ kann passieren. Aber für kommutative Ringe kann man die Dimension eines freien Moduls definieren:

5.6 Theorem: Sei R ein kommutativer Ring und M ein R -Modul mit Basen v_1, \dots, v_n und w_1, \dots, w_ℓ . Dann gilt $n = \ell$. Diese Zahl wird der Rang des freien Moduls M genannt.

Beweis: Idee: Wenn $R = K$ ein Körper ist, wissen wir schon, daß das stimmt, der Rang ist einfach die Dimension von M , und in linearer Algebra wurde gezeigt, daß die Dimension wohldefiniert ist.

Wie können wir zu dieser Situation übergehen. Aus Algebra wissen wir, daß R (mindestens) ein maximales Ideal I besitzt und R/I ein Körper ist.

Wie machen wir aus R -Moduln K -Vektorräume?

K wie wird hier R kommutativ verwendet?

Sei M irgendein Modul. Und sei $I_M := \{ \sum_{i=1}^n a_i x_i \mid a_i \in R, x_i \in M \}$. Das ist ein Teilmodul von M (nachprüfen)

R kommutativ $\Rightarrow M/I_M$ ist ein R/I -Modul durch

$$(a+I)(x+I_M) := ax + I_M \quad \text{wie wird } R \text{ kommutativ verwendet?}$$

Zurück zum gegebenen M : $v_1 + I_M, v_2 + I_M, \dots, v_n + I_M$ ist eine K -Basis von M/I_M .

Deun: $\mathbb{R}^n \xrightarrow{\bar{u}} M \xrightarrow{\bar{u}} M/I_M \Rightarrow \bar{v}_1, \dots, \bar{v}_n \in M/I_M$ bilden ein Erzeugendensystem.
 $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i v_i \mapsto \sum_{i=1}^n a_i v_i + I_M$

$$\text{Kern}(\bar{u}) = I_M = \text{Kern}(R^n \rightarrow M/I_M) \Rightarrow K^n \xrightarrow{\sim} M/I_M$$

$$I \cdot R^n = I^n \xrightarrow{U} 0 \quad \text{Details nachprüfen} \Rightarrow \bar{v}_1, \dots, \bar{v}_n \text{ Basis von } M/I_M.$$

Ebenso: $\bar{w}_1, \dots, \bar{w}_\ell$ Basis der K -Vektorraums $M/I_M \Rightarrow \ell = n. \square$

Wir brauchen auch Endlichkeitsbedingungen. Bei Hauptidealringen kennen wir eine (Algebra, 1.17 und 1.18): Sei R ein Hauptidealring. Dann ist R noethersch, d.h. es erfüllt die folgenden drei, zueinander äquivalenten Bedingungen:

- Jede aufsteigende Kette $I_1 \subset I_2 \subset I_3 \subset \dots$ von Idealen in R wird stationär.
- In jeder nichtleeren Menge von Idealen in R gibt es ein bezüglich Inklusion maximales Element.
- Jedes Ideal I in R ist endlich erzeugbar, d.h. von der Form $\langle a_1, \dots, a_n \rangle = Ra_1 + \dots + Ra_n$ mit $a_1, \dots, a_n \in R$.

Die dritte Eigenschaft ist bei einem Hauptidealring klar: I ist, wie jeder Ideal, ein Hauptideal, d.h. $I = Ra$ für ein $a \in R$.

Auch die erste Eigenschaft ist leicht zu verifizieren — betrachte $\bigcup I_i$.

(Da wir Ringe wie $K[x]$ betrachten wollen, also ∞ -dimensionale Vektorräume, wäre ~~ein~~ endlich-dimensionale zu viel verlangt; noethersch ist der beste Ersatz dafür.)

Analoge Definition für Moduln:

5.7 Definition: Ein R -Modul M ist noethersch \Leftrightarrow jeder Untermodul von M ist endlich erzeugt, d.h. es gibt ein endliches Erzeugendensystem.

$$\text{endlich erzeugt} \quad (\Leftrightarrow) \quad \exists n \in \mathbb{N}: \exists R^n \rightarrow M \text{ surjektiv}$$

Das ist äquivalent zu den Analoga der anderen beiden Bedingungen:

- Jede aufsteigende Kette $M_1 \subset M_2 \subset M_3 \subset \dots$ von Untermoduln von M wird stationär. (Diese Bedingung heißt auch: aufsteigende Kettenbedingung.)
- In jeder nichtleeren Menge von Teilmoduln von M gibt es ein bezüglich Inklusion maximales Element.

Beispiele nicht noetherscher Ringe und Moduln:

- $K[x_1, x_2, \dots]$, Polynomring in unendlich vielen Variablen. Das Ideal $\langle x_1, x_2, \dots \rangle$ ist nicht endlich erzeugt. Die aufsteigende Kette $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \dots$ wird nicht stationär. Details?

• $\mathbb{Z}[\frac{1}{2}]$ (d.h. \mathbb{Z} adjungiert $\frac{1}{2}$, als Ring), enthält $\mathbb{Z}, \frac{1}{2}, \frac{1}{4}, \dots, \frac{1}{2^n} \in \mathbb{Z}$ ist eine abelsche Gruppe, also ein \mathbb{Z} -Modul, aber über \mathbb{Z} nicht endlich erzeugt, denn: seien a_1, \dots, a_n ein \mathbb{Z} -Erzeugendensystem von $\mathbb{Z}[\frac{1}{2}]$. Dann ist jeder a_i ein Bruch $\frac{b_i}{c_i}$ mit $b_i \in \mathbb{Z}, c_i$ eine Potenz von 2, $c_i = 2^{d_i}$. Sei $d = \max\{d_i\}$.

Dann kann $\frac{1}{2^d}$ keine \mathbb{Z} -Lineare Kombination von a_1, \dots, a_n sein.

• Ein Körper K ist ein noetherscher Ring, aber ein unendlich-dimensionaler K -Vektorraum, z.B. $\bigoplus K$, ist nicht noethersch, da er nicht einmal endlich erzeugt sein kann.

Wählt man eine Basis b_1, b_2, \dots (mindestens abzählbar viele), dann ist $\langle b_1 \rangle \subset \langle b_1, b_2 \rangle \subset \dots$ eine nicht-stationäre aufsteigende Kette.

Ein endlich-dimensionaler K -Vektorraum V ist dagegen noethersch: V selbst und alle Unterräume sind endlich erzeugt. Und alle aufsteigenden Ketten müssen stationär sein. *warum?*

Bei Vektorräumen ist noethersch also dieselbe Bedingung wie ~~noethersch~~ endlich-dimensionale.

Frage: Sind Teiltringe oder Quotientenringe noetherscher Ringe selbst noethersch?

Sind Teilmoduln oder Quotientenmoduln noetherscher Moduln selbst noethersch?

Dazu auch passende Begriffe und Theorie:

5.8 Definition: Sei R ein Ring, $(M_i)_{i \in \mathbb{I}}$ eine Menge von R -Moduln und $(f_i: M_i \rightarrow M_{i+1})_{i \in \mathbb{I}}$ Modulhomomorphismen (für $I \subset \mathbb{I}, M_{i+1} = 0$ falls $i+1 \notin \mathbb{I}$). Diese Daten bilden eine exakte Folge von R -Moduln, wenn für alle $i \in \mathbb{I}$ gilt: $\text{Im } f_i = \text{Ker } f_{i+1}$.

Bezeichnung: $\dots \rightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \rightarrow \dots$

Spezialfall: Eine kurze exakte Folge (oder: kurze exakte Sequenz) ist eine exakte Folge der Form $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$

\uparrow hier muß die Nullabbildung stehen \uparrow

Was bedeutet eine kurze exakte Sequenz

$$0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0 \quad ?$$

Bedingungen: $\text{Im}(f) = \text{Ker}(g)$ $\text{Im}(g) = \text{Ker}(0)$
 \uparrow \uparrow
 f ist injektiv g surjektiv
 $\text{Im}(f) = \text{Ker}(g)$

Also: $f: M' \rightarrow M$ ist injektiv,
 $g: M \rightarrow M''$ ist surjektiv
 und zusätzlich gilt:
 $\text{Im}(f) = \text{Ker}(g)$

Wenn M' ein Teilmodul von M ist, können wir für f die Inklusion wählen.

Dann muß $M'' \cong M/M'$ sein: $M' \xrightarrow[\text{inkl.}]{i=f} M \xrightarrow{g} M''$
 $\searrow \text{Proj} \quad \text{? warum?}$
 M/M'

Wenn M'' ein Quotientenmodul von M ist, können wir für g die Projektion wählen. Dann muß M' isomorph zum Kern der Projektion sein.

Typisches Beispiel einer kurzen exakten Folge von \mathbb{Z} -Modulen:

über \mathbb{Z} : $0 \rightarrow 4\mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow 0$
 aber auch $0 \rightarrow \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$
 wie setzen die Abbildungen aus?

5-9 Lemma: Sei R ein Ring und $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ eine kurze exakte

Folge von R -Modulen. Dann gilt: M noethersch $\Leftrightarrow M'$ und M'' beide noethersch.

Beweis: Sei M noethersch, $\Leftrightarrow M'$ und M'' sind noethersch. Wir zeigen in beiden Fällen, daß Untermoduln endlich erzeugt sind.

M' : Sei $N \subset M'$ ein Untermodul. Dann ist $f(N)$ ein Untermodul von M *warum?*
 $\Rightarrow f(N)$ ist endlich erzeugt $\Rightarrow N \cong f(N)$ ist endlich erzeugt.

M'' : Sei $N \subset M''$ ein Untermodul. Dann ist $g^{-1}(N)$ ein Untermodul von M *warum?*
 $\Rightarrow g^{-1}(N)$ ist endlich erzeugt $\Rightarrow N = g(g^{-1}(N))$ ist endlich erzeugt als Quotient eines endlich erzeugten Moduls *was können wir als Erzeugendensystem wählen?*

Gegenrichtung: Seien M' und M'' noethersch, $\Leftrightarrow M$ noethersch.

Sei $N \subset M$ ein Untermodul. Dann ist $f^{-1}(N)$ ein Untermodul von M' und $g(N)$ ein Untermodul von M'' . Genauer: es gibt eine kurze exakte Folge

$0 \rightarrow f^{-1}(N) \rightarrow N \xrightarrow{g} N \rightarrow 0$ (die Abbildungen sind die Einschränkungen von f bzw. von g) *nachprüfen: die Folge ist exakt*

Also genügt es zu zeigen:

Wenn in einer kurzen exakten Folge $0 \rightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \rightarrow 0$ (von R -Moduln) die beiden Endterme X und Z endlich erzeugt sind, dann ist auch der Mittelterm endlich erzeugt.

(Achtung: die Gegenrichtung ist falsch. Aus Y endlich erzeugt folgt zwar Z endlich erzeugt. Aber wenn Y nicht noethersch ist, muß X nicht endlich erzeugt sein. Hier sieht man, daß "noethersch" eine bessere Bedingung ist als "endlich erzeugt".)

Sei x_1, \dots, x_n ein R -Erzeugendensystem von X und z_1, \dots, z_k eines von Z .

Wir wählen Urbilder y_1, \dots, y_k von z_1, \dots, z_k , d.h. $g(y_i) = z_i$.

Behauptung: $f(x_1), \dots, f(x_n), y_1, \dots, y_k$ ein R -Erzeugendensystem von Y .

Beweis: Sei $y_0 \in Y$, dann ist $g(y_0) = \sum_{i=1}^k a_i z_i$ für $a_1, \dots, a_k \in R$.

$$\Rightarrow g(y_0 - \sum a_i y_i) = 0$$

warum?

$$\Rightarrow y_0 - \sum a_i y_i = f(x_0) \text{ für ein } x_0 \in X, \text{ also } y_0 - \sum a_i y_i = \sum b_j f(x_j)$$

für $b_1, \dots, b_n \in R$. \square

Aus 5-9 folgt: Ein Quotient eines noetherschen Moduls ist selbst noethersch. Ebenso überträgt sich noethersch auf Teilmoduln.

Der Beweis für Quotienten funktioniert auch bei Ringen. *nachprüfen*

Aber noethersch überträgt sich nicht auf Teilringe.

$K[x_1, x_2, \dots]$ ist nicht noethersch, aber ein Integritätsbereich

$\Rightarrow \exists$ Körper der Brüche $Q(K[x_1, x_2, \dots]) \supset K[x_1, x_2, \dots]$ und der ist wie jeder Körper noethersch.

Ein allgemeiner Satz, den wir hier nicht beweisen, liefert viele Beispiele noetherscher Ringe. Hilbertscher Basisatz: Sei R ein kommutativer noetherscher Ring. Dann ist auch der Polynomring $R[x]$ noethersch, mit Induktion also auch $R[x_1, \dots, x_n]$.

Insbesondere ist also $K[x, y]$ noetherisch (K ein Körper). Auch in diesem Ring gibt es nicht noethersche Teiltringe.

Beispiel: Sei $A := \{ \lambda + xg(x, y) \mid \lambda \in K, g(x, y) \in K[x, y] \}$

Das ist ein Teiltring *nachprüfen* $\neq 0$

und es gibt eine aufsteigende Kette von Idealen, die nicht stationär wird:

$$I_0 := \langle x \rangle = Ax$$

$$I_1 := \langle x, xy \rangle = Ax + Axy$$

$$I_2 := \langle x, xy, xy^2 \rangle = Ax + Axy + Axy^2$$

$$\vdots$$

$$I_n = \langle x, xy, xy^2, \dots, xy^n \rangle = Ax + Axy + Axy^2 + \dots + Axy^n$$

Nachzuprüfen: $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n \subsetneq \dots$ (Hinweis: wo liegt xy^{n+1} ?)

und $I = \bigcup_{n=0}^{\infty} I_n$ ist ein Ideal in A , das nicht endlich erzeugt ist.