5.18 Satz: R faktorieller Ring $p \in R$ Primelement und $f \in R[x]$ ein Polynom dessen Leitkoeffizient nicht von p geteilt wird. Sei

$$\Phi : R[x] \to R/(p)[x]$$

die Koeffizientenreduktion nach p. Dann gilt: Ist $\Phi(f)$ irreduzibel in $R/(p)[x]$, dann ist f irreduzibel in $Q(R)[x]$. Ist f darüber hinaus primitiv, dann ist f auch irreduzibel in $R[x]$.

Beweis: Wir nehmen zunächst an, dass f primitiv ist. Ist dann f reduzibel in $Q(R)[x]$, dann ist nach dem Satz von Gauß f reduzibel in $R[x]$. Es gibt also eine Zerlegung $f = g \cdot h$ mit $g, h \in R[x]$ und $\deg g, \deg h > 0$. Dabei sind die Leitkoeffizienten von g und h nicht durch p teilbar, da dies für f der Fall ist. Damit ist $\Phi(P) = \Phi(g)\Phi(h) \in R/(p)[x]$ ebenfalls reduzibel. Also die Irreduzibilität von $\Phi(f)$ impliziert die Irreduzibilität von f

Im Allgemeinen schreiben wir $f = a\tilde{f}$ mit Konstanten $a \in R$ ($\tilde{f}$ primitiv), die p nicht von p geteilt wird. Ist $\Phi(f)$ irreduzibel dann ist auch $\Phi(\tilde{f})$ irreduzibel. Nach dem schon bewiesenen folgt $\tilde{f}$ ist irreduzibel in $R[x]$ und daher f irreduzibel $Q(R)[x]$ $\square$

Beispiel $f = x^3 + 3x^2 - 4x - 1 \in \mathbb{Q}[x]$
Reduktion mod 3 führt die Irreduzibilität von f auf die $x^3 - x - 1 \in \underbrace{\mathbb{F}_3}_{=\mathbb{Z}/(3)}[x]$ zurück.
Dies gilt, da dieses Polynom in $\mathbb{F}_3$ keine Nullstelle hat.

§6 Moduln und euklidische Ringe

Gruppen operieren auf Mengen. Die natürlichen Objekte auf denen Ringe operieren sind Moduln.

6.1 <u>Def</u> Sei R ein Ring. Ein R-Modul ist eine Menge M zusammen mit zwei Verknüpfungen

$M \times M \to M \quad (a,b) \mapsto a+b$

$R \times M \to M \quad (r,a) = ra$

den folgenden Axiomen genügt:

(M1) $(M,+)$ ist eine abelsche Gruppe

(M2) Die Multiplikation erfüllt $r(s\cdot a) = (r\cdot s)a$ und $1\cdot a = a \ \forall r,s \in R, \forall a \in M$

(M3) Es gelten die Distributivgesetze $r(a+b) = ra+rb$ und $(r+s)a = ra+sa \quad \forall r,s\in R, \forall a,b \in M$

<u>Bem</u> Ist $R=K$ ein Körper, dann ist R-Modul nichts anderes als ein K-Vektorraum. Die Theorie der R-Moduln ist aber deutlich verschieden von der Theorie der Vektorräume.

Zum Beispiel hat nicht jeder R-Modul eine Basis.

<u>Beispiele</u>: 1) Sei V ein K-Vektorraum. Dann definiert die Operation $\mathrm{End}(V) \times V \to V$

$$f, v \mapsto f(v)$$

eine $\mathrm{End}(V)$-Modulstruktur auf V.

2) Sei $A \in K^{n\times n}$ eine Matrix. Dann definiert die Substitution von t durch A einen K-Algebra Homomorphismus

$K[t] \to \mathrm{End}(K^n)$

und demzufolge eine $K[t]$-Modulstruktur auf $K^n = V$ in dem t wie A operiert.

3) Jede abelsche Gruppe G ist ein $\mathbb{Z}$-Modul

$n \cdot a = \underbrace{a + \dots + a}_{n \text{ Kopie}} \quad n \geq 0$

$(-n) \cdot a = -(na)$

4) R bel. Ring, I eine Indexmenge. Dann ist

$R^{(J)} = \bigoplus_{j \in J} R$ ist ein R-Modul

Insbesondere ist $R^n = R \oplus \dots \oplus R = \left\{ \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \middle| r_i \in R \right\}$

ein R-Modul sogenannte freie Modul

5) $I \subset R$ ein Ideal $\Leftrightarrow$ ~~Dann ist~~ $I \subset R$ ist ein R-Untermodul

6) $N \subset M$ ein Untermodul. Dann trägt $M/N = \{m + N \mid m \in M\}$ eine R-Modulstruktur.

6.2 Def M und N R-Moduln. Dann ist ein R-Modulhomomorphismus eine Abbildung $\varphi: M \to N$, der $\varphi(a+b) = \varphi(a) + \varphi(b)$ erfüllt und $\varphi(ra) = r\varphi(a)$.

Beispiele:

1) Jeder Gruppenhomomorphismus zwischen abelschen Gruppen ist ein $\mathbb{Z}$-Modul Homom.

2) R-Modulo Homomorphismen

$\varphi: R^n \to R^m$

werden durch Matrizen $A(m \times n)$ mit Einträgen in R beschreiben. In der j-ten Spalte von A steht das Bild des $j$ten Einheitsvektors e_j.

6.3 Def Sei M ein R-Modul. M heißt endl erzeugt, wenn es endlich viele Elemente $m_1, \dots, m_n \in M$ gibt, s.d. jedes Element $m \in M$ eine Darstellung

$m = \sum_{i=1}^{n} r_i m_i$ hat.

Mit anderen Worten: Wenn der R-Modulhomomorphismus

$R^n \to M$
$e_i \mapsto m_i$ surjektiv ist.

M heißt endl. präsentiert, wenn darüber hinaus auch $\ker \varphi$ endlich erzeugt ist, es also eine Abbildung geht noch weiter, sorry....

$R^m \to R^n \to M$ gibt mit $\operatorname{Im} A = \ker \varphi$

M wird dann durch Erzeuger und Relationen zwischen den Erzeugern beschrieben.

$M \cong R^n$ heißt frei, da die Erzeuger frei von Relationen sind.

<u>Beispiel</u>

1) $\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2$

eine Präsentation von $\mathbb{Z}/2$

2) $\mathbb{Z}^2 \xrightarrow{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}} \mathbb{Z}^2 \to G \to 0$ (Ordnung $= |\det A|$)

6.4 <u>Def + Satz</u> Ein R-Modul heißt noethersch wenn die folgenden äquivalenten Bedingungen erfüllt sind.

(1) Jeder Untermodul $N \subset M$ ist endlich erzeugt

(2) Jede aufsteigende Kette von Untermoduln

$N_1 \subset N_2 \subset N_3 \subset \dots$ wird schließl. stationär.

(3) Jede nichtleere Teilmenge $\mathcal{M}$ von Untermoduln von M hat ein bez. Inklusion maximales Element.

<u>Bem:</u> R ist noethersch als R-Modul $\iff$ R noetherscher Ring

da Untermodule von R Ideale sind.

<u>Beweis auf Zuruf:</u>

(1)$\Rightarrow$(2) Sei $N_1 \subset N_2 \subset \dots$ eine aufsteigende Kette von Untermoduln. Dann ist $\bigcup_{i=1}^{\infty} N_i = N$ ebenfalls ein Untermodul, weil $a, b \in N$ $\exists\, i_1, i_2$ $a \in N_{i_1}, b \in N_{i_2} \Rightarrow a+b \in N_{\max(i_1,i_2)}$

Nach (1) ist N endlich erzeugt etwa $N = \langle a_1, \dots, a_n \rangle$.

$\exists\, i_j : a_j \in N_{i_j} \Rightarrow a_1, \dots, a_n \in N_{\underset{k}{\underbrace{\max(i_j)}}}$

$$N_k = N_{k+1} = \dots = N$$

(2)$\Rightarrow$(3) Angenommen $\mathcal{M}$ eine Menge von Untermoduln, die kein maximales Element enthält. Zu $N_k \in \mathcal{M}$ $\exists\, N_{k+1} \in \mathcal{M}$ $N_k \subsetneq N_{k+1}$ dies liefert eine aufsteigende

Kette, die nicht stationär wird.

(3) ⇒ (1) Sei N ein Untermodul von M.
Sei $\mathcal{M} = \{N' \subset N ; N'$ endl. erzeugt$\}$ $\mathcal{M} \neq \emptyset$, da $\{0\} \in \mathcal{M}$
Sei $N' \in \mathcal{M}$ ein maximales Element, etwa $N' = \langle a_1, \dots, a_n \rangle$
und $a \in N$. Dann ist auch $\langle a_1, \dots, a_n, a \rangle$ endl. erzeugt
Untermodul von N und daher $\langle a_1, \dots, a_n, a \rangle = N'$
$= \langle a_1, \dots, a_n \rangle \Rightarrow a \in N'$ und daher $N' = N$ ∎

6.5 Def Ein Komplex von R-Moduln ist eine
Sequenz von R-Modulhomomorph.

$$M_{i+1} \to M_i \to M_{i-1}$$

so dass $\ker(M_i \to M_{i-1}) \supset \operatorname{Im}(M_{i+1} \to M_i)$ $\forall i$ gilt.
Ein Komplex von R-Moduln heißt exakt, wenn
Gleichheit gilt $\ker(M_i \to M_{i-1}) = \operatorname{Im}(M_{i+1} \to M_i)$
Besonders wichtig sind kurze exakte Sequenzen

$$0 \to M' \to M \to M'' \to 0$$

also Sequenzen, wo $M' \to M$ injektiv ist, $M \to M''$
surjektiv und $\operatorname{Im}(M' \to M) = \ker(M \to M'')$

6.6 Satz Sei $0 \to M' \hookrightarrow M \to M'' \to 0$ eine
kurze exakte Sequenz von R-Moduln
Dann ist M noethersch genau dann, wenn M' und M''
noethersch sind.

Beweis Sei M noethersch. Dann ist M' isomorph zu
einem Untermodul von M.
Untermoduln von diesem Modul sind endl. erzeugt, das
gleiche trifft auf den isomorphen Modul M' zu
Sei $N_1'' \subset N_2'' \subset \dots \subset M''$ eine aufsteigende
Kette in Untermoduln $\varphi : M \to M''$, dann ist
$\varphi^{-1}(N_1'') = N_1 \subset \varphi^{-1}(N_2'') = N_2 \subset \dots$ eine Kette in M

Diese wird stationär und damit wegen $\varphi(\varphi^{-1}(N_k''))=N_k''$ wird auch Kette in M'' stationär.

$\Longleftarrow$ Sei $N\subset M$ ein Untermodul. Dann ist $\varphi(N)\subset M''$ ein Untermodul und $N'=N\cap M'$, wobei ~~wir~~ $M'\subset M$ vermöge der Injektion als Teilmenge auffassen. Untermoduln in M'' bzw M'. Diese sind endlich erzeugt, etwa $N'=\langle a_1',\dots,a_n'\rangle$, $N''=\langle a_{n+1}'',\dots,a_s''\rangle$.

Es seien $a_{n+1},\dots,a_s$ Urbilder von a_j'' in N und $a_1,\dots,a_n$ die Bilder von a_i' unter der inklusion $N'\subset M'\hookrightarrow M$.

Dann gilt: $N=\langle a_1,\dots,a_n,a_{n+1},\dots,a_s\rangle$.

in der Tat $a\in N$ dann ist $\varphi(a)$ ~~eine~~ $=r_{n+1}a_{n+1}''+\dots+r_s a_s''$ und $a-\sum_{j=n+1}^{s} r_j a_j\in \ker\varphi\cap N$, was von $a_1,\dots,a_n$ erzeugt wird.

Also $\exists\, r_1,\dots,r_n$ mit $a-\sum_{j=n+1}^{s} r_j a_j=\sum_{i=1}^{n} r_i a_i$ und somit $a\in\langle a_1,\dots,a_s\rangle$ ■

<u>6.7 Korollar</u> Sei R ein noetherscher Ring.

1) Dann ist R^n ein noetherscher R-Modul

2) Ein Modul über einen noetherscher Ring R ist noethersch genau dann wenn R endlich präsentiert ist.

<u>Beweis</u> 1) Induktion nach n mit Hilfe der kurzen exakten Sequenzen $0\to R\xrightarrow{1\mapsto e_n} R^n\to R^{n+1}\to 0$

$r_i\mapsto e_i$ für $i<n$

$e_n\mapsto 0$

2) M noethersch $\Rightarrow$ M ist endl. erzeugt

$R^n\xrightarrow{A} R^m\xrightarrow{\varphi} M\to 0$ die Komposition gibt die Präsentationsmatrix.

$0\to\ker\varphi\to 0$

$\ker\varphi$ ist ebenfalls endl. erzeugt.

Umgekehrt ist M als homomorphes Bild des noetherschen Moduls R^n ebenfalls noethersch. $\square$

<u>6.8 Satz</u> Sei R ein Hauptidealring.
Jeder endlich erzeugte R-Modul M ist isomorph zu einer direkten Summe von zyklischer Module

$$M = R/(f_1) \oplus \dots \oplus R/(f_s) \oplus R^r$$

wobei $f_1, \dots, f_s \in R\setminus\{0\}$

<u>Beweis</u>: Wir betrachten eine Präsentation

$$0 \leftarrow M \leftarrow R^m \xleftarrow{A} R^n$$

und bringen durch Zeilen- und Spaltenoperationen auf Diagonalgestalt.

Ist (a,b) eine 1×2 Matrix mit Einträgen in R und $d = ggT(a,b)$, etwa $a = \alpha d$, $b = \beta d$ dann sind α, β teilerfremd also das Hauptideal $(\alpha, \beta) = (1)$

Es gibt also $u, v \in R$ mit $1 = u\alpha + v\beta$

Wir betrachten jetzt die Matrix $\begin{pmatrix} u & -\beta \\ v & \alpha \end{pmatrix}$

Diese Matrix ist invertierbar, da $\det\begin{pmatrix} u & -\beta \\ v & \alpha \end{pmatrix} = u\alpha + v\beta = 1$

(Die Inverse ist $\begin{pmatrix} \alpha & \beta \\ -v & u \end{pmatrix}$)

Die 1×2 Präsentationsmatrix

$$\begin{array}{ccccccc} 0 & \leftarrow & M & \leftarrow & R & \xleftarrow{(a,b)} & R^2 \\ & & \| & & \| & & \uparrow \cong \begin{pmatrix} u & -\beta \\ v & \alpha \end{pmatrix} \\ 0 & \leftarrow & M & \leftarrow & R & \xleftarrow{(d,0)} & R^2 \end{array}$$

können wir so abändern, dass sie die gewünschte Gestalt hat.

Im Allgemeinen

$$\begin{array}{ccccc} 0 \leftarrow M & \leftarrow & R^m & \xleftarrow{A} & R^n \\ \| & & \uparrow S & & \uparrow T \\ M & \leftarrow & R^m & \longleftarrow & R^n \end{array} \qquad \tilde{A} = S^{-1}AT$$

Sei $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ eine Präsentationsmatrix.

Dann können wir durch Anwenden von Permutationsmatrizen erreichen, dass $a_{11} \neq 0$, es sei denn $A = 0$ für die nichts zu zeigen ist.

Anschließend können wir auf (a_{11}, a_{12}) die Vorbem. anwenden und mit einer Matrix T der Form

$$T = \begin{pmatrix} u & -\beta & & & \\ v & \alpha & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

A in die Form $\begin{pmatrix} d_1, & 0, & a_{13} & \cdots & a_{1n} \\ a_{21}' & a_{22}' & & & \\ \vdots & & & & \\ a_{m1} & \cdots & & & a_{mn} \end{pmatrix}$

Das gleiche mit der 1. und 3. Zeile usw erlaubt es uns die Matrix in die Gestalt $\begin{pmatrix} d_2 & 0 \cdots & 0 \\ & * & \end{pmatrix}$ zu bringen.

Anschließend können wir das gleiche Verfahren mit Hilfe von Matrizen S auf die erste Spalte anwenden.

$$\begin{pmatrix} d_3 & * \\ 0 & \\ \vdots & * \\ 0 & \end{pmatrix}$$

Leider wird damit erst die 1. Zeile wieder $\neq 0$.

Wir erhalten auf diese Weise eine Folge
$(d_1) \subset (d_2) \subset \ldots$ von Hauptidealen
die schließlich stationär wird.

Erreichen wir $\begin{pmatrix} d_k & a_{12}'' \cdots & a_{1n}'' \\ 0 & & \\ \vdots & & \\ 0 & & \end{pmatrix}$ sodass $d_k \mid ggT(a_{12}'', \ldots, a_{1n}'')$, so können wir Matrizen $\begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix}$ verwenden, welche die 1. Spalte unverändert lässt.

Wir können also dann die erste Zeile und Spalte gleichzeitig ausräumen und erhalten eine Matrix $\left(\begin{array}{c|c} \tilde{a}_{11} & 0 \\ \hline 0 & \tilde{A} \end{array}\right)$

wobei $\tilde{a}_{11} = d_k$ und $d_k = d_{k+1} = \ldots$.

Auf die kleine Matrix $\tilde{A}$ können wir das obige Verfahren erneut anwenden und erhalten schließlich

$$\begin{array}{c} \\ \\ m-s\{ \end{array}\left(\begin{array}{cccc|c} \tilde{a}_{11} & & & 0 & \\ & \tilde{a}_{22} & & & 0 \\ & & \ddots & & \\ 0 & & & \tilde{a}_{ss} & \\ \hline & & & & \end{array}\right) \overset{n-s}{} = B$$

Es folgt $M = \operatorname{coker} B = R^m / \operatorname{Im} B \cong R/(\tilde{a}_{11}) \oplus R/(\tilde{a}_{22}) \oplus \dots \oplus R/(\tilde{a}_{ss}) \oplus R^r$
wobei $r = m - s$ (Die letzten $n-s$ Spalten in B kann man auch weglassen, da sie zum Bild von B nichts beitragen) $\square$

Zyklische Moduln der Gestalt $R/(a)$ lassen sich häufig noch weiter zerlegen. R Hauptidealring und $a = \varepsilon p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung so werden wir sehen, dass

$$R/(a) \cong R/(p_1^{\nu_1}) \oplus \dots \oplus R/(p_r^{\nu_r})$$

Dies ist eine Konsequenz aus dem chinesischen Restsatz den wir in voller Allgemeinheit formulieren.

6.9 Def R Ring; I, J ideale

Dann $I + J = \{a + b \mid a \in I, b \in J\}$

I und J heißen coprim, wenn $I + J = (1)$ gilt

6.10 Chinesischer Restsatz

Sei R ein Ring, $I_1, \dots, I_n$ paarweise coprime Ideale in R. Dann ist der Ringhomomorphismus

$$\varphi : R \to R/I_1 \times \dots \times R/I_n$$
$$r \mapsto (r + I_1, \dots, r + I_n)$$

Surjektiv mit $\ker \varphi = I_1 \cap \dots \cap I_n = I_1 I_2 \cdots I_n$

und $R/I_1 \cdots I_n \cong R/I_1 \times \dots \times R/I_n$

Beweis. (1) Seien $r_i + I_i \in R/I_i$ vorgegeben.

Wir müssen ein $r \in R$ konstruieren mit $r + I_i = r_i + I_i \; \forall i$

Ist $i \neq j$ so existieren nach Voraussetzung ein $a_{ij} \in I_i$ und $b_{ij} \in I_j$ mit $a_{ij} + b_{ij} = 1$

Für $s_i := \prod_{i \neq j} a_{ij} = \prod_{i \neq j} (1 - b_{ij})$ gilt:

$$s_i \text{ ist in } I_j \; \forall i \neq j \text{ und } s_i \in 1 + I_j$$

Dann ist $r = \sum_{i=1}^{n} r_i s_i$ das gesuchte Element:

$r + I_i = r_i s_i + I_i = (r_i + I_i)(s_i + I_i)$

$= (r_i + I_i)(1 + I_i)$
$= (r_i + I_i)$

Die Ringhom φ ist also surjektiv.

(2) $\ker \varphi = I_1 \cap \dots \cap I_n$ ist klar. Es bleibt

$I_1 \cap \dots \cap I_n = I_1 \cdot \ldots \cdot I_n$ zu zeigen.

Für $n=1$ ist nichts zu zeigen. Für $n=2$ müssen wir $I_1 \cap I_2 = I_1 \cdot I_2$ zeigen. $I_1 I_2 \subset I_1 \cap I_2$ ist klar.

Sei $a \in I_1 \cap I_2$ $\quad a = a \cdot 1 = \underset{\in I_1}{a} \cdot (a_{12} + b_{12}) = \underset{\subset I_2}{\underset{I_1 \cap I_2}{\underset{\cap}{a}}}\underset{I_2}{\underset{\cap}{a_{12}}} + \underset{\in I_1 \cap I_2 \subset I_1}{a}\underset{I_2}{\underset{\cap}{b_{12}}} \in I_1 \cdot I_2$

Sei nun $n \geq 2$ und $I_1 \cdot \ldots \cdot I_{n-1} = I_1 \cap \dots \cap I_{n-1}$ schon gezeigt. Dann gilt

$$1 = \prod_{i=1}^{n-1} (a_{in} + b_{in}) \in I_1 \dots I_{n-1}$$

$I_1 \cdot \ldots \cdot I_{n-1}$ und I_n sind also coprim und nach oben gezeigtem gilt $(I_1 \cdot \ldots \cdot I_{n-1}) I_n = (I_1 \cdot \ldots \cdot I_{n-1}) \cap I_n$

$= I_1 \cap \dots \cap I_{n-1} \cap I_n$

<u>Bem.</u>: Den Isomorphismus $R/I_1 \dots I_n \cong R/I_1 \times \dots \times R/I_n$ können wir als R-Modulisomorphismus auffassen und daher:

$$R/I_1 \dots I_n = R/I_1 \oplus \dots \oplus R/I_n \text{ als R-Modul}$$

Der Spezialfall $R = \mathbb{Z}$ ist der Chinesische Restsatz, welcher im Lehrbuch Sun Zis Handbuch d. Arithmetik ca im 2-3 Jhd notiert wurde, in folgender Form

0.11 <u>Satz</u> (Sun Zis)

Es seien $m_1, \dots, m_n \in \mathbb{Z}_{>0}$ paarweise teilerfremde Zahlen. Dann existiert für $a_1, \dots, a_n \in \mathbb{Z}$ bel. ein $x \in \mathbb{Z}$ dass die Kongruenzen $x \equiv a_1 \mod m_1$

$\vdots$

$x \equiv a_n \mod m_n$

simultan erfüllt. Die Lösung x ist bis auf Vielfache von $m_1 \cdot \ldots \cdot m_n$ eindeutig bestimmt.

Bem Sind $m_1, \dots, m_n$ nicht teilerfremd. Dann ist
$a_i \equiv a_j \mod d$ wobei $d = ggT(m_1, \dots, m_n)$
eine notwendige Bedingung für die Lösbarkeit.

Anwendung auf endlich erzeugte abelsche Gruppen

6.12 Satz Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem Produkt von zyklischen Gruppen von Primpotenzordnung und der freien zyklischen Gruppe $\mathbb{Z}$.

Beweis: Nach dem Klassifikationssatz von endl. erzeugten $\mathbb{Z}$-Moduln gilt $G \cong \mathbb{Z}/(a_1) \oplus \dots \oplus \mathbb{Z}/(a_s) \oplus \mathbb{Z}^r$

Nach dem chin. Restsatz ist

$$\mathbb{Z}/(a) \cong \mathbb{Z}/(p_1^{\nu_1}) \oplus \dots \oplus \mathbb{Z}/(p_e^{\nu_e})$$ für die paarweise verschiedenen Primfaktoren von

$0 < a = p_1^{\nu_1} \cdots p_e^{\nu_e}$ Die Beh. folgt.

6.13 Def + Satz Sei R ein Integritätsring, M ein R-Modul und $a \in M$. a heißt Torsionselement, wenn es ein $r \in R \setminus \{0\}$ mit $ra = 0$ gibt.

$T(M) = \{a \in M \mid \exists r \in R \setminus \{0\} \text{ mit } ra\}$ heißt Torsionsuntermodul von M

Beweis: $T(M)$ ist ein Untermodul:

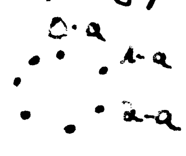
$a_i \in T(M)$ etwa $r_i a_i = 0$

dann gilt $\underbrace{r_1 r_2}_{\neq 0} (a_1 + a_2) = 0$

Also $a_1 + a_2 \in T(M)$.

Bem: Der Name Torsion kommt aus dem Lateinischen torqueo = ich drehe, winde

Es ist durch die zyklische Anordnung von $\{ra \mid r \in \mathbb{Z}\}$, $a \in T(M) \subset M$ $\mathbb{Z}$-Modul motiviert



<u>Beispiel</u> G endlich erzeugte abelsche Gruppe $G \cong \mathbb{Z}/(a_1) \oplus \dots \oplus \mathbb{Z}/(a_s) \oplus \mathbb{Z}^r$

Dann ist der Torsionsanteil $T(G) = \mathbb{Z}/(a_1) \oplus \dots \oplus \mathbb{Z}/(a_s)$ ein wohldefinierter Untermodul.

Der freie Anteil $\mathbb{Z}^r$ ist kein kanonisches Untermodul da es viele Morphismen $\mathbb{Z}^r \to \mathbb{Z}/(a_1) \oplus \dots \oplus \mathbb{Z}/(a_s)$ gibt.

Lediglich der Quotient~~enraum~~

$$G/T(G) \cong \mathbb{Z}^r \text{ ist kanonisch.}$$

r heißt Rang der abelschen Gruppe G.

Anwendung auf Polynomringe $K[x]$, K Körper

6.14 <u>Satz</u> (Hermite Interpolation)

Seien $a_1, \dots, a_s$ in $\mathbb{R}$ paarweise verschiedene Punkte und $v_1, \dots, v_s \in \mathbb{N}_{>0}$.

Zu vorgegebenen Polynomen $f_1, \dots, f_s \in \mathbb{R}[x]$ von Grad $< v_1, \dots, v_s >$ gibt es genau ein Polynom f in $\mathbb{R}[x]$ von Grad $< v_1 + \dots + v_s$, dessen ~~Ta~~ Taylorpolynome in $a_1, \dots, a_s$ von der Ordnung $v_1 - 1, \dots, v_s - 1$ mit $f_1, \dots, f_s$ übereinstimmen.

<u>Beweis</u>: Dass f das Taylorpolynom f_i in a_i hat ist zu $f \equiv f_i \mod (x - a_i)^{v_i}$ äquivalent.

Mit dem chinesischen Restsatz folgt $\mathbb{R}[x] / \prod_{i=1}^{s} (x - a_i)^{v_i}$

$$\cong \mathbb{R}[x]/(x-a_1)^{v_1} \oplus \dots \oplus \mathbb{R}[x]/(x-a_s)^{v_s}$$

da die a_i paarweise verschieden sind. Alle Elemente von $\mathbb{R}[x] / \prod_{i=1}^{s} (x - a_i)^{v_i}$ werden durch ein Polynom f von Grad $< \deg \prod_{i=1}^{s} (x - a_i)^{v_i} = \sum_{i=1}^{s} v_i$ repräsentiert. $\square$