3. Moduln und der Elementarteilersatz

3.1 Matrizen über Ringen und die Smith-Normalform

In Lineare Algebra 1 haben wir für $A \in Mat(m \times n, K)$ (K Körper) mit Hilfe des Gauß-Algorithmus eine Normalform

$$SAT = \left(\begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

erzielt, wobei $S \in GL(m, K)$, $T \in GL(n, K)$, $r = rang(A)$.

Def Adjunkte:

$$A^{\#} = (a_{ij}^{\#})_{ij}, \quad a_{ij}^{\#} = (-1)^{i+j} \det(A_{ji})$$

wobei A_{ji} die Streichungsmatrix von A ist, bei der die j-te Zeile und die i-te Spalte gestrichen wird.

3.1.1 Satz Sei R ein kommutativer Ring mit 1, $A \in Mat(n, R)$.

$$A^{\#} \cdot A = A \cdot A^{\#} = \det(A) \cdot \mathbb{1}_n.$$

Beweis wie in lineare Algebra, mit Verallgemeinerung.

3.1.2 Korollar

$A \in \mathrm{Mat}(n, R)$ invertierbar $\Leftrightarrow$ $\det(A) \in R^*$

Beweis: „$\Leftarrow$" $\det(A) \in R^* \Rightarrow$ $\frac{1}{\det(A)} \cdot A^{\#}$ ist die Inverse von A.

„$\Rightarrow$" $A^{-1} \cdot A = 1_n \Rightarrow \det(A)^{-1} \cdot \det(A) = 1$

$\Rightarrow \det(A) \in R^*$. □

Bemerkung:
Über Ringen gilt nicht: voller Rang $\Rightarrow$ invertierbar.
z. B. $(2) \in \mathrm{Mat}(1, \mathbb{Z})$ hat vollen Rang, aber $\det(2) = 2 \notin \mathbb{Z}^*$
$\Rightarrow (2)$ ist nicht invertierbar
(über $\mathbb{Q}$ wäre $(1/2)$ die inverse Matrix).

3.1.3 Satz (Smith-Normalform)

Sei R ein euklidischer Ring, $A \in \mathrm{Mat}(m \times n, R)$. Dann $\exists$ $S \in GL(m, R)$, $T \in GL(n, R)$, $r \leq \min\{m, n\}$ mit

$$SAT = D = \left(\begin{array}{c|c} d_1 & \\ \ddots & 0 \\ d_r & \\ \hline 0 & 0 \end{array}\right)$$

mit $d_i \mid d_{i+1}$ $\forall$ $i = 1, \ldots, r-1$.

Die d_i sind (bis auf Einheiten) durch A eindeutig bestimmt und heißen Elementarteiler von A.

D heißt Smith-Normalform von A.

Bem Der Satz gilt allgemeiner für Hauptidealringe R, wir werden ihn jedoch nur für euklidische Ringe beweisen.

Der Beweis ist konstruktiv:

3.1.4 Algorithmus (Smith-Normalform)

Sei R mit $v: R \to \mathbb{N}$ euklidischer Ring, $A \in \mathrm{Mat}(m \times n, R)$, $A \neq 0$.

1. Schritt: Zeilen- und Spaltenvertauschungen, so daß $a_{11} \neq 0$ und $v(a_{11}) \leq v(a_{ij})$ $\forall\, a_{ij} \neq 0$ $\forall\, (i,j) \neq (1,1)$.

2. Schritt: Schreibe jedes a_{1j} und a_{j1}, das nicht durch a_{11} teilbar ist, als $a_{1j} = q \cdot a_{11} + r$ mit $v(r) < v(a_{11})$ und reduziere entsprechend mit der 1. Zeile bzw. Spalte.

Zurück nach Schritt 1.

Da $v(a_{11})$ in jedem Schritt echt kleiner wird, terminiert der Prozeß und wir enden mit einer Matrix, in der alle Einträge der 1. Zeile und Spalte durch a_{11} teilbar sind.

3. Schritt Addiere Vielfache der 1. Zeile bzw. Spalte und erhalte

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

Sind nicht alle Einträge von A' durch a_{11} teilbar, so addiere z.B. a_{ij} nicht teilbar, die i-te zur 1. Zeile und gehe wieder nach Schritt 2.

Der nicht teilbare Eintrag ist jetzt in der 1. Zeile, wir verwenden wieder Division mit Rest und gehen zurück nach Schritt 1 usw. Da $\min\{v(a_{ij})\}$ bei jedem Durchlaufen von Schritt 2 echt kleiner wird, terminiert dieser Prozeß und wir enden mit einem A', in dem alle Einträge durch a_{11} teilbar sind.

Sind alle Einträge von A' durch a_{11} teilbar, beginne mit A' bei Schritt 1.

Beweis: Terminierung siehe Zwischenkommentare. Korrektheit: Rekursiv erhalten wir

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & a_{22} & 0 & \cdots \\ \hline \vdots & 0 & a_{33} & \cdots \\ 0 & \vdots & & \end{array}\right) \Big\} \text{ Output von } A'$$

Da alle Einträge von A' durch a_{11} teilbar sind, sind auch alle Einträge, die während des Prozesses auftauchen, durch a_{11} teilbar, insbesondere a_{22}. Die Korrektheit folgt per Induktion. Für den Induktionsanfang beachte, daß für $n=1$ oder $m=1$ der Algorithmus einfach Division mit Rest ist und den ggT der Einträge der Zeile bzw. Spalte produziert. □

Bem Die Matrizen S, T erhält man durch Mitprotokollieren der Zeilen- bzw. Spaltenoperationen.

Bsp: $A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \in \mathrm{Mat}(2\times 3, \mathbb{Z})$

Die euklidische Norm ist

$v: \mathbb{Z} \to \mathbb{N}: a \mapsto |a|.$

Schritt 1: 6 hat schon kleinste Norm, weiter nach Schritt 2.

Schritt 2: $9 = 1 \cdot 6 + 3$, reduziere mit 1. Spalte:

$$\left(\begin{array}{cc|ccc} 1 & 0 & 6 & 9 & 6 \\ 0 & 1 & 6 & 6 & 7 \\ \hline & & 1 & 0 & 0 \\ & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{array}\right) \xrightarrow{\text{Spalte } II \mapsto II - I} \left(\begin{array}{cc|ccc} 1 & 0 & 6 & 3 & 6 \\ 0 & 1 & 6 & 0 & 7 \\ \hline & & 1 & -1 & 0 \\ & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{array}\right)$$

Zurück nach Schritt 1, Spalten vertauschen:

$$\xrightarrow{\text{Spalte } I \leftrightarrow II} \left(\begin{array}{cc|ccc} 1 & 0 & 3 & 6 & 6 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 1 & 0 \\ & & 1 & 0 & 0 \\ & & 0 & 0 & 1 \end{array}\right)$$

Jetzt sind alle in der 1. Zeile und Spalte durch 3 teilbar, reduziere mit Schritt 3:

$$\xrightarrow{\substack{\text{Spalte } II \mapsto II - 2I \\ III \mapsto III - 2I}} \left(\begin{array}{cc|ccc} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

$A' = (6\ 7)$, 7 ist nicht durch 3 teilbar, addiere 2. Zeile zur 1. und weiter mit Schritt 1

$$\xrightarrow{\text{Zeile } I \mapsto I + II} \left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 7 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

3 ist das kleinste, Schritt 2:

$7 = 3 \cdot 2 + 1$, reduziere mit Spalte 1:

$$\left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 7 \\ 0 & 1 & 0 & 6 & 7 \\ & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

Spalte
$\text{III} \mapsto \text{III} - 2\,\text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 1 \\ 0 & 1 & 0 & 6 & 7 \\ & & -1 & 3 & 4 \\ & & 1 & -2 & -4 \\ & & 0 & 0 & 1 \end{array}\right)$$

Schritt 1: vertausche III und I Spalte, damit 1 als kleinstes nach vorne kommt

Spalte
$\text{III} \hookrightarrow \text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 6 & 3 \\ 0 & 1 & 7 & 6 & 0 \\ & & 4 & 3 & -1 \\ & & -4 & -2 & 1 \\ & & 1 & 0 & 0 \end{array}\right)$$

alle in 1. Zeile & Spalte teilbar durch 1 → Schritt 3, reduziere

Spalte
$\text{II} \mapsto \text{II} - 6\,\text{I}$
$\text{III} \mapsto \text{III} - 3\,\text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 7 & -36 & -21 \\ & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right)$$

Zeile
$\text{II} \mapsto \text{II} - 7 \cdot \text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -36 & -21 \\ & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right)$$

$A' = (-36 \; -21)$
alle Einträge durch 1 teilbar
weiter mit A' nach Schritt 1

$v(-21) = 21$ ist das kleinste taugliche Spalten:

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -36 & -21 \\ & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right) \xrightarrow{\text{Spalte } II \hookrightarrow III} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -21 & -36 \\ & & 4 & -13 & -21 \\ & & -4 & 13 & 22 \\ & & 1 & -3 & -6 \end{array}\right)$$

Schritt 2: Division mit Rest

$-36 = -21 - 15$

$$\xrightarrow{\text{Spalte } III \mapsto III - II} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -21 & -15 \\ & & 4 & -13 & -8 \\ & & -4 & 13 & 9 \\ & & 1 & -3 & -3 \end{array}\right)$$

Schritt 1: tausche Spalten

$$\xrightarrow{\text{Spalte } II \hookrightarrow III} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -15 & -21 \\ & & 4 & -8 & -13 \\ & & -4 & 9 & 13 \\ & & 1 & -3 & -3 \end{array}\right)$$

Schritt 2: Division mit Rest

$-21 = -15 - 6$

reduziere

$$\xrightarrow{\text{Spalte } III \mapsto III - II} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -15 & -6 \\ & & 4 & -8 & -5 \\ & & -4 & 9 & 4 \\ & & 1 & -3 & 0 \end{array}\right)$$

Schritt 1: tausche Spalten

$$\xrightarrow{\text{Spalte } III \hookrightarrow II}$$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -6 & -15 \\ \hline & & 4 & -5 & -8 \\ & & -4 & 4 & 9 \\ & & 1 & 0 & -3 \end{array}\right)$$

Schritt 2:
Division mit Rest
$-15 = 2 \cdot (-6) - 3$

Spalte III $\mapsto$ III -2 II $\longrightarrow$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -6 & -3 \\ \hline & & 4 & -5 & 2 \\ & & -4 & 4 & 1 \\ & & 1 & 0 & -3 \end{array}\right)$$

Schritt 1:
Spalte tauschen

Spalte II $\leftrightarrow$ III $\longrightarrow$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -3 & -6 \\ \hline & & 4 & 2 & -5 \\ & & -4 & 1 & 4 \\ & & 1 & -3 & 0 \end{array}\right)$$

alle Einträge durch -3 teilbar, reduzieren mit Schritt 3:

Spalte III $\mapsto$ III -2 II $\longrightarrow$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -3 & 0 \\ \hline & & 4 & 2 & -9 \\ & & -4 & 1 & 2 \\ & & 1 & -3 & 6 \end{array}\right)$$

Die Elementarteiler sind $1, 3$
(bis auf Einheiten in $\mathbb{Z}$, i.e. Vorzeichen).

Es gilt $\begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \cdot \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \cdot \begin{pmatrix} 4 & 2 & -9 \\ -4 & 1 & 2 \\ 1 & -3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix}$.

Zur Eindeutigkeit der Elementarteiler:

3.1.5 Satz

Sei $A \in \mathrm{Mat}(m \times n, R)$.

Für $I \subset \{1, \dots, m\}$, $J \subset \{1, \dots, n\}$ sei $A_{I,J}$ die Streichungsmatrix mit den Zeilen in I und Spalten in J.

Die Menge $\{ \det(A_{I,J}) \mid |I| = |J| = i \}$ ist die Menge aller $i \times i$- Minoren von A.

Seien $d_1, \dots, d_r$ die Elementarteiler von A

Dann gilt:

$$d_1 \cdots d_i = gg^T \left(\det(A_{I,J}) \mid (|I| = |J| = i) \right) =: D_i$$

Insbesondere sind die Elementarteiler bis auf Einheiten eindeutig, und

$$d_1 = D_1 = gg^T(\text{alle Einträge von } A).$$

Beweisidee: (benötigt äußere Algebra, LA2)

Die Einträge der i-ten äußeren Potenz $\Lambda^i A$ sind genau die $i \times i$- Minoren von A (bei geeigneter Basiswahl).

Es gilt $\Lambda^i S \cdot \Lambda^i A = \Lambda^i (S \cdot A)$

Beh: $ggT(\text{Einträge von } \Lambda^i(SA)) = ggT(\text{Einträge } \Lambda^i(A))$ für S invertierbar

Jeder Eintrag von $\Lambda^i(S\cdot A) = \Lambda^i S \cdot \Lambda^i A$ ist eine Linearkombination von Einträgen von $\Lambda^i A \Rightarrow ggT(\Lambda^i A) \mid ggT(\Lambda^i(SA))$

Da S invertierbar ist, gilt $A = S^{-1}(SA)$ und wir können mit demselben Argument folgern, daß $ggT(\Lambda^i(SA)) \mid ggT(\Lambda^i A)$.

Analog gilt $ggT(\Lambda^i A) = ggT(\Lambda^i(AT))$ für T invertierbar.

Damit folgt für $SAT = D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ mit $d_i \mid d_{i+1}$ $\quad i = 1, \dots, r-1$

$ggT(\Lambda^i A) = ggT(\Lambda^i(SAT)) = ggT(\Lambda^i D) = ggT(d_{j_1} \cdots d_{j_i} \mid 1 \le j_1 < \cdots < j_i \le r)$

$= d_1 \cdots d_i$, denn $d_j \mid d_k$ für $j \le k$ □

Bsp: $A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix}$

$d_1 = ggT(\text{alle Einträge}) = 1$

2×2-Minoren sind $\det\begin{pmatrix} 6 & 9 \\ 6 & 6 \end{pmatrix} = -18$,

$\det\begin{pmatrix} 6 & 6 \\ 6 & 7 \end{pmatrix} = 6$, $\det\begin{pmatrix} 9 & 6 \\ 6 & 7 \end{pmatrix} = 27$,

$ggT(-18, 6, 27) = d_1 \cdot d_2 = 3$

$\Rightarrow d_2 = 3.$

3.2 Moduln

3.2.1 Def Sei R ein Ring.

Ein **R-Modul** $(M, +, \cdot)$ ist eine Menge M mit zwei Verknüpfungen

$+ : M \times M \longrightarrow M$ und

$\cdot : R \times M \longrightarrow M$ so daß

1) $(M, +)$ ist abelsche Gruppe

2) $r \cdot (m_1 + m_2) = r m_1 + r m_2$ (Distributivität)

$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

3) $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$ (Assoziativität)

4) $1 \cdot m = m$

3.2.2 Bsp

1) Sei $R = K$ ein Körper, dann ist jeder K-Vektorraum ein K-Modul.

2) $\{$ abelsche Gruppen $\} \overset{1:1}{\longleftrightarrow} \{\mathbb{Z}$-Moduln$\}$

Sei $(G, +)$ abelsche Gruppe.

Setze $\mathbb{Z} \times G \to G$:

$(n, g) \mapsto \underbrace{g + \dots + g}_{n\text{-mal}}$ für $n \geq 0$

$(-1) \cdot g \mapsto -g$

Dann gilt die Distributivität:

$n(g_1 + g_2) = g_1 + g_2 + \dots + g_1 + g_2 \overset{\text{abelsch}}{=}$

$g_1 + \dots + g_1 + g_2 + \dots + g_2 = n g_1 + n g_2$

$(n_1 + n_2) g = \underbrace{g + \dots + g}_{n_1 + n_2} = \underbrace{g + \dots + g}_{n_1} + \underbrace{g + \dots + g}_{n_2} =$

$n_1 g + n_2 g$

Assoziativität:

$(n_1 \cdot n_2) \cdot g = \underbrace{g + \dots + g}_{n_1 \cdot n_2} = \underbrace{(\underbrace{g + \dots + g}_{n_2}) + \dots + (\underbrace{g + \dots + g}_{n_2})}_{n_1}$

$= n_1 \cdot (n_2 \cdot g)$

und $1 \cdot g = g$ $\Rightarrow$ G ist ein $\mathbb{Z}$-Modul

Umgekehrt ist jeder $\mathbb{Z}$-Modul abelsche Gruppe $(G, +)$.

3) Sei R ein Ring,

$I \subset R$ ist Ideal $\Leftrightarrow$ I ist R-Modul

„$\Rightarrow$" $(I, +)$ ist abelsche Gruppe

Distributivität, Assoziativität und $1 \cdot m = m$ gelten, da dies Rechnungen in R sind

„$\Leftarrow$" Die Abgeschlossenheit bezüglich der R-Skalarmultiplikation folgt aus der Def.

Insbesondere ist R selbst ein R-Modul.

4) Sei I ein Ideal, dann ist R/I ein R-Modul.

5) Seien M_1, M_2 R-Moduln, dann ist $M_1 \times M_2$ mit komponentenweise definierter Addition und Skalarmultiplikation ein Modul.
Insbesondere ist $R^n = R \times \dots \times R$ ein R-Modul.

6) Sei $\varphi: R \longrightarrow S$ ein Ringhomomorphismus, dann ist S mit der Addition und mit der Skalarmultiplikation definiert durch
$r \circ s := \varphi(r) \cdot s$ ein R-Modul,
denn $(S,+)$ ist abelsche Gruppe,
$r \circ (s_1 + s_2) = \varphi(r) \cdot (s_1 + s_2) = \varphi(r) \cdot s_1 + \varphi(r) \cdot s_2$,
$(r_1 + r_2) \circ s = \varphi(r_1 + r_2) \cdot s = (\varphi(r_1) + \varphi(r_2)) \cdot s$
$= \varphi(r_1) \cdot s + \varphi(r_2) \cdot s$,

$(r_1 \cdot r_2) \circ s = \varphi(r_1 \cdot r_2) \circ s = \varphi(r_1) \circ \varphi(r_2) \circ s =$
$r_1 \circ (r_2 \circ s)$ und $1 \circ s = \varphi(1) \circ s = 1 \circ s = s$.

Insbesondere sind $\mathbb{Q}$, $\mathbb{R}$ $\mathbb{Z}$-Moduln.

7) Sei $R = K[X]$, V ein K-Vektorraum
$\varphi : V \longrightarrow V$ ein Endomorphismus.

Wir definieren
$X \cdot v := \varphi(v) \in V$ für $v \in V$
und erhalten einen $K[X]$-Modul V:
$(V, +)$ ist abelsche Gruppe,

$f(X) \circ (v_1 + v_2) = (a_n X^n + \dots + a_0) \cdot (v_1 + v_2)$
$= (a_n X \cdots X + \dots + a_0)(v_1 + v_2) =$
$a_n \cdot (X \cdots X) \cdot (v_1 + v_2) + \dots + a_0 (v_1 + v_2) =$
$a_n \varphi^n (v_1 + v_2) + \dots + a_0 (v_1 + v_2) =$
$a_n (\varphi^n(v_1) + \varphi^n(v_2)) + \dots + a_0 (v_1 + v_2) =$
$a_n \varphi^n(v_1) + a_n \varphi^n(v_2) + \dots + a_0 v_1 + a_0 v_2 =$
$a_n \varphi^n(v_1) + \dots + a_0 v_1 + a_n \varphi^n(v_2) + \dots + a_0 v_2 =$
$f(X) \cdot v_1 + f(X) \cdot v_2$

$(f(x)+g(x))\cdot v = f(x)\cdot v + g(x)\cdot v$

und $(f(x)\cdot g(x))\cdot v = f(x)\cdot(g(x)\cdot v)$

analog, $1\cdot v = v$.

Umgekehrt, gegeben ein $K[x]$-Modul V, so erhalten wir durch die Einschränkung der Skalarmultiplikation auf K einen K-Vektorraum V, und durch

$\varphi: V \longrightarrow V;\ v \longmapsto x\cdot v$

einen Endomorphismus, denn

$\varphi(v+w) = x\cdot(v+w) = x\cdot v + x\cdot w = \varphi(v) + \varphi(w)$ und $\varphi(\lambda\cdot v) = x\cdot\lambda\cdot v = \lambda\cdot x\cdot v = \lambda\cdot\varphi(v)$.

$$\left\{\begin{array}{l}\text{Tupel } (V,\varphi)\\ \text{mit } V \ K\text{-Vektorraum},\\ \varphi: V\longrightarrow V\\ \text{Endomorphismus}\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}K[x]\text{-}\\ \text{Moduln}\\ V\end{array}\right\}$$

3.2.3 Lemma

Sei M ein R-Modul, $m \in M$.

Es gilt $0_R\cdot m = 0_M$ und

$-m = (-1_R)\cdot m$.

Beweis: $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m \Rightarrow$
$0 \cdot m = 0$. $0 = 0 \cdot m = (1-1) \cdot m = 1 \cdot m + (-1) \cdot m =$
$m + (-1) \cdot m \Rightarrow -m = -1 \cdot m$. □

3.2.4 Def Ein Untermodul $U \subset M$ ist eine Teilmenge, die selbst wieder ein Modul ist.

3.2.5 Lemma (Untermodulkriterium)

Sei $U \subset M$ eine Teilmenge.

U ist Untermodul $\Leftrightarrow$

$U \neq \emptyset$, $m_1 + m_2 \in U \; \forall \; m_1, m_2 \in U$

und $r \cdot m \in U \; \forall \; r \in R, \; m \in U$.

Beweis: „$\Rightarrow$" Da $+ : U \times U \to U$,

$\cdot : R \times U \to U$.

„$\Leftarrow$" Aus dem Untergruppenkriterium folgt, daß $(U, +)$ eine Untergruppe bezüglich $+$ ist, denn $m_1 + m_2 \in U$ und $-m = (-1) \cdot m \in U$.

Distributivität, Assoziativität und $1 \cdot m = m$ $\forall m \in U$ gelten, da sie in M gelten. □

3.2.6 Lemma Sei $U \subset M$ Untermodul, dann ist M/U mit $r \cdot [m] = [r \cdot m]$ ein R-Modul.

Beweis: $(M/U, +)$ ist abelsche Gruppe.
Die Skalarmultiplikation ist wohldefiniert, denn falls $[m_1] = [m_2] \Rightarrow m_1 - m_2 \in U$
$\Rightarrow r \cdot (m_1 - m_2) \in U \Rightarrow rm_1 - rm_2 \in U$
$\Rightarrow [rm_1] = [rm_2]$.
Die Rechenregeln werden vererbt. □

3.2.7 Def
Ein R-Modul-Homomorphismus $f: M \to N$ ist ein R-linearer Gruppenhomomorphismus, i.e.
$f(m_1 + m_2) = f(m_1) + f(m_2) \quad \forall m_1, m_2 \in M$
$f(r \cdot m) = r \cdot f(m) \quad \forall r \in R, m \in M.$

3.2.8 Satz (Homomorphiesatz)
Sei $f: M \to N$ ein R-Modulhomomorphismus. $\ker(f)$, $\mathrm{Im}(f)$ sind Untermoduln von M bzw. N und es gilt
$$\tilde{f}: M/\ker(f) \xrightarrow{\cong} \mathrm{Im}(f)$$
$$[m] \longmapsto f(m)$$

Beweis: Folgt aus dem Homomorphiesatz für Gruppen, nur die Verträglichkeit mit der Skalarmultiplikation ist zu prüfen:

$\tilde{f}(r \cdot [m]) = \tilde{f}([r \cdot m]) = f(r \cdot m) =$

$r \cdot f(m) = r \cdot \tilde{f}([m])$. □

3.2.9 Def

M heißt endlich erzeugt $\Leftrightarrow$

$\exists \; f: R^n \twoheadrightarrow M$

(surjektiver Modulhomomorphismus).

3.2.10 Bemerkung

Seien $e_1, \dots, e_n$ die Standard-Einheits-Vektoren von R^n, setze $m_i := f(e_i)$.

f surjektiv $\Leftrightarrow$ jedes Element von M läßt sich in der Form

$f(r) = f(r_1 e_1 + \dots + r_n e_n) =$

$r_1 f(e_1) + \dots + r_n f(e_n) = r_1 m_1 + \dots + r_n m_n$

schreiben, also als R-Linearkombination der m_i. $\Leftrightarrow$ die m_i erzeugen M als R-Modul, $M = \langle m_1, \dots, m_n \rangle_R$

Die m_i müssen keine Basis bilden, die Darstellung als R-Linearkombination des m_i muß nicht eindeutig sein:

Bsp $\mathbb{Z}_3$ ist ein $\mathbb{Z}$-Modul, und endlich erzeugt, denn $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$ ist ein surjektiver $\mathbb{Z}$-Modulhomomorphismus. Aber $[0] = 3 \cdot [1] = 0 \cdot [1]$ hat keine eindeutige Darstellung als $\mathbb{Z}$-Linearkombination des Erzugers $[1]$.

3.2.11 Def Ein endlich erzeugter R-Modul M heißt frei $\Leftrightarrow$
$\exists$ Isomorphismus $M \cong R^n$
Insbesondere bilden die Bilder m_i der e_i dann eine Basis von M, i.e. jedes Element von M läßt sich eindeutig als R-Linearkombination der m_i darstellen.

Bsp
1) $\mathbb{Q}$ als $\mathbb{Z}$-Modul ist nicht endlich erzeugt: Angenommen, $\mathbb{Q}$ wäre von $r_1, \dots, r_n$ erzeugt. Wähle d teilerfremd zu den Nennern der r_i. Sei

$a \in \langle r_1, \dots, r_n \rangle_{\mathbb{Z}} \Rightarrow a = a_1 r_1 + \dots + a_n r_n$
mit $a_i \in \mathbb{Z}$. Sei $r_i = \frac{p_i}{q_i} \Rightarrow$

$$a = a_1 \frac{p_1}{q_1} + \dots + a_n \frac{p_n}{q_n} = \frac{\dots}{kgV(q_1, \dots, q_n)} \neq \frac{1}{d}$$

$$\Rightarrow \frac{1}{d} \notin \langle r_1, \dots, r_n \rangle_{\mathbb{Z}}.$$

2) Ein K- Vektorraum ist ein freier K- Modul.

3) Sei $R = K[x_i \mid i \in \mathbb{N}]$ der Polynomring in abzählbar vielen Variablen.
R als R- Modul ist endlich erzugt, sogar frei mit Basis 1.
Betrachte $U = \{ f \in R \mid f(0) = 0 \}$ die Polynome ohne konstanten Koeffizienten.
Da $0 \in U$ ist $U \neq \emptyset$.
Sind $f, g \in U \Rightarrow f+g\,(0) =$
$f(0) + g(0) = 0+0 = 0 \Rightarrow f+g \in U$.
Ist $f \in U$ und $r \in R \Rightarrow r \cdot f(0) =$
$r \cdot 0 = 0 \Rightarrow r \cdot f \in U$
Nach dem Untermodulkriterium 3.2.5

ist U ein Untermodul.

Beh: U ist nicht endlich erzeugt

($U = \langle x_i \mid i \in \mathbb{N} \rangle_R$)

Angenommen, $U = \langle f_1, \dots, f_k \rangle_R$.

In jedem f_i gibt es nur endlich viele Variablen, seien $x_1, \dots, x_n$ die Variablen, die in allen f_i vorkommen.

Betrachte eine R-Linearkombination $r_1 f_1 + \dots + r_k f_k$ mit $r_i \in R$.

Die f_i haben keinen konstanten Anteil, i.e. jeder Term eines f_i enthält ein x_j, $j = 1, \dots, n$. Damit enthält auch jeder Term von $r_1 f_1 + \dots + r_k f_k$ ein x_j, $j = 1, \dots, n$.

Aber $x_{n+1} \in U$ und x_{n+1} läßt sich nicht als Summe von Termen darstellen, von denen jeder ein x_j, $j = 1, \dots, n$ enthält.

$\Rightarrow U \neq \langle f_1, \dots, f_k \rangle_R$.

U ist nicht endlich erzeugt.

Insbesondere können Untermoduln von endlich erzeugten Moduln selbst nicht endlich erzeugt sein.

3.2.12 Def (Exakte Sequenzen)

Eine Sequenz von R-Moduln und R-Modul-Homomorphismen

$$\dots \; M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow \dots$$

heißt <u>exakt</u> bei M_i $:\Leftrightarrow$

$$\ker(\varphi_i) = \operatorname{Im}(\varphi_{i-1})$$

Eine Sequenz heißt exakt, wenn sie exakt bei jedem inneren Eintrag ist.

<u>Bsp</u>

1) $N \xrightarrow{\varphi} M \longrightarrow 0$ ist exakt $\Leftrightarrow$

$\ker$(Nullabbildung) $= M = \operatorname{Im}\varphi$ $\Leftrightarrow$

φ surjektiv

2) $0 \longrightarrow N \xrightarrow{\varphi} M$ ist exakt $\Leftrightarrow$

Bild(Inklusion der 0) $= \{0\} = \ker(\varphi)$ $\Leftrightarrow$

φ injektiv.

3.3 Endlich präsentierte Moduln

3.3.1 Def M heißt *endlich präsentiert* wenn M durch $\varphi: R^m \to M$ endlich erzeugt wird und $\ker(\varphi)$ selbst wieder endlich erzeugt wird.

3.3.2 Lemma

M endlich präsentiert $\Leftrightarrow$
$\exists$ exakte Sequenz $R^n \xrightarrow{f} R^m \to M \to 0$

Beweis:

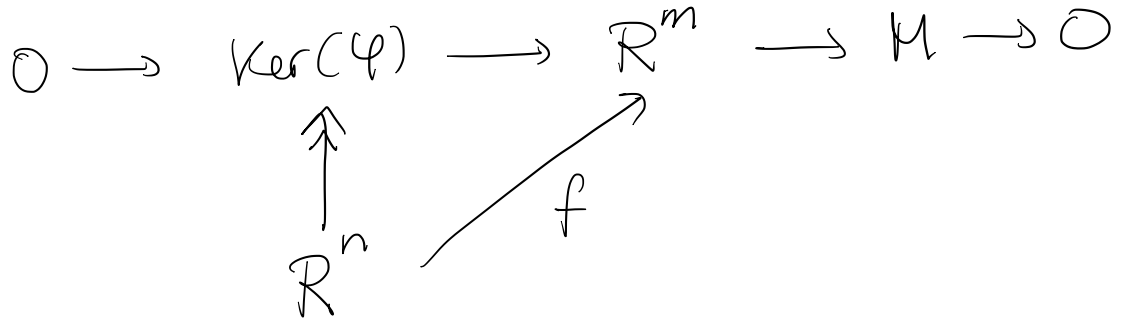
„$\Rightarrow$" M ist endlich erzeugt durch $\varphi: R^m \to M$, φ ist surjektiv $\Rightarrow$

$R^m \xrightarrow{\varphi} M \to 0$ ist exakt

$\Rightarrow$ $0 \to \ker(\varphi) \to R^m \to M \to 0$ ist exakt.

Da $\ker(\varphi)$ endlich erzeugt, $\exists$

$R^n \twoheadrightarrow \ker(\varphi)$



Damit existiert

$$R^n \xrightarrow{f} R^m \longrightarrow M \longrightarrow 0$$

und ist exakt.

„⇐" Sei $R^n \xrightarrow{f} R^m \xrightarrow{\varphi} M \longrightarrow 0$ exakt $\Rightarrow$ φ ist surjektiv $\Rightarrow$ M ist endlich erzeugt.

Außerdem gilt $\operatorname{Ker}(\varphi) = \operatorname{Im}(f)$

$\Rightarrow$ $R^n \xrightarrow{f} \operatorname{Im}(f)$ zeigt, daß $\operatorname{Ker}(\varphi)$ selbst endlich erzeugt ist

$\Rightarrow$ M ist endlich präsentiert. □

3.3.3 Def Die Abb $R^n \xrightarrow{f} R^m$ ist ein Morphismus freier Moduln und daher durch die Bilder $f(e_1), \dots, f(e_n)$ festgelegt. Diese Bilder schreiben wir in der Basis

$e_1, \dots, e_m$ und erhalten so eine eine $m \times n$ Matrix $A \in Mat(m \times n, R)$, die Präsentationsmatrix von M.

Es gilt $M = Im\varphi \cong R^m / ker(\varphi) = R^m / Im(f) = R^m / Im(A)$,

das heißt, M ist durch A vollständig beschrieben.

$Im(A)$ liefert alle Relationen zwischen den Erzeugen $\varphi(e_i)$ von M, i.e. für alle Gleichungen $r_1 \varphi(e_1) + \dots + r_m \varphi(e_m) = 0$ die die Erzeuger $\varphi(e_i)$ erfüllen, gilt $\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \in Im(A)$.

3.3.4 Satz

M sei ein R-Modul. Äquivalent sind:

1) Jede aufsteigende Kette von Untermoduln wird stationär.
2) Jeder Untermodul von M ist endlich erzeugt
3) Jede Teilmenge von Untermoduln enthält ein maximales Element.

Beweis wie bei Ringen.

3.3.5 Def

Ein Modul, der die Eigenschaften aus 3.3.4 erfüllt, heißt noethersch.

3.3.6 Prop

Sei $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow 0$ eine exakte Sequenz von R-Moduln.

M noethersch $\Leftrightarrow$ M', M'' noethersch.

Beweis:

Beh: $N_1, N_2 \subset M$ Untermoduln mit $N_1 \subset N_2$, $\pi(N_1) = \pi(N_2)$, $i(M') \cap N_1 = i(M') \cap N_2 \Rightarrow N_1 = N_2$

Sei $x \in N_2 \Rightarrow \pi(x) \in \pi(N_2) = \pi(N_1)$

$\Rightarrow \exists\, x' \in N_1 : \pi(x) = \pi(x') \Rightarrow$

$\pi(x - x') = 0 \Rightarrow x - x' \in \ker(\pi) = \operatorname{Im}(i) = i(M')$. Da $x' \in N_1 \subset N_2$, $x \in N_2$

$\Rightarrow x - x' \in N_2 \Rightarrow x - x' \in N_2 \cap i(M') = N_1 \cap i(M') \Rightarrow x - x' \in N_1$, da $x' \in N_1 \Rightarrow x \in N_1$.

"$\Leftarrow$" Seien M', M'' noethersch,

$M_1 \subset M_2 \subset \dots$ eine Kette von Untermoduln in M $\Rightarrow$

$\pi(M_1) \subset \pi(M_2) \subset \dots$ ist eine Kette in M''

$i(M') \cap M_1 \subset i(M') \cap M_2 \subset \dots$ " " M'

Da beide noethersch, stabilisieren beide Ketten

Wähle n groß genug, daß beide stabil sind $\Rightarrow$ $\pi(M_N) = \pi(M_n) \quad \forall N \geq n$

$i(M') \cap M_N = i(M') \cap M_n \quad \forall N \geq n$

Beh $\Rightarrow$ $M_N = M_n \quad \forall N \geq n$

$\Rightarrow$ die Kette wird stationär

$\Rightarrow$ M ist noethersch.

"$\Rightarrow$" Sei M noethersch.

Jede Kette in M' oder M'' induziert eine Kette in M via i bzw. π^{-1}, die stationär wird, die ursprüngliche deshalb auch. □

3.3.7 Lemma

R noethersch $\Rightarrow$ R^n noethersch

Beweis Induktion über n.

$n=1$ klar. Sei R^{n-1} noethersch.

Betrachte

$$R^{n-1} \xrightarrow{i} R^n \xrightarrow{\pi} R$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ 0 \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \longmapsto v_n$$

i ist injektiv, π ist surjektiv,

$\ker(\pi) = \operatorname{Im}(i)$ $\Rightarrow$

$0 \to R^{n-1} \to R^n \to R \to 0$ ist exakt, da R^{n-1}, R noethersch folgt mit Prop. 3.3.6 R^n noethersch. □

3.3.8 Satz

Endlich erzeugte Moduln über noetherschen Ringen sind schon endlich präsentiert.

Beweis:

M endlich erzeugt $\Rightarrow \exists\ R^m \twoheadrightarrow M$.

Dann ist

$0 \longrightarrow \ker(\varphi) \longrightarrow R^m \longrightarrow M \longrightarrow 0$

exakt, R^m ist noethersch wegen 3.3.7 $\overset{3.3.6}{\Longleftrightarrow}$ $\ker(\varphi)$ noethersch $\overset{3.3.4}{\Longrightarrow}$ $\ker(\varphi)$ endlich erzeugt $\Rightarrow$ M endlich präsentiert. □

3.3.9 Korollar

Endlich erzeugte Moduln über noetherschen Ringen sind noethersch.

Beweis:

Mit derselben exakten Sequenz

$0 \longrightarrow \ker(\varphi) \longrightarrow R^m \longrightarrow M \longrightarrow 0$

folgt auch M ist noethersch. □

3.4 Der Elementarteilersatz

3.4.1 Bsp Eine endlich erzeugte abelsche Gruppe (i.e. ein endlich erzeugter $\mathbb{Z}$-Modul, siehe Bsp 3.2.2 2)) läßt sich durch eine Präsentationsmatrix beschreiben (Satz 3.3.8), z.B.:

$$0 \longrightarrow \mathbb{Z}^3 \xrightarrow{A} \mathbb{Z}^4 \xrightarrow{\varphi} G \longrightarrow 0$$

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$ dann ist $G = \mathbb{Z}^4/\ker\varphi = \mathbb{Z}^4/\mathrm{Im}A$

Bestimme die Smith-Normalform von A, und die Basiswechsel:

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & -3 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & -3 \\ & & & & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$\begin{array}{l} II \mapsto II + 3I \\ III \mapsto III - I \\ \longrightarrow \\ IV \mapsto IV - I \end{array}$ Zeilen

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ -1 & 0 & 1 & 0 & 0 & -4 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ & & & & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

Spalten $\begin{array}{l} II \mapsto II - I \\ \longrightarrow \\ III \mapsto III - I \end{array}$

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ -1 & 0 & 1 & 0 & 0 & -4 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ & & & & 1 & -1 & -1 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

Weiter mit $A^1 = \begin{pmatrix} 4 & 4 \\ -4 & 0 \\ 0 & -4 \end{pmatrix}$

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ -1 & 0 & 1 & 0 & 0 & -4 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ & & & & 1 & -1 & -1 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right) \xrightarrow{\text{Zeile III} \mapsto \text{III} + \text{II}} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ 2 & 1 & 1 & 0 & 0 & 0 & 4 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ & & & & 1 & -1 & -1 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{\text{Spalte III} \mapsto \text{III} - \text{II}} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 4 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ & & & & 1 & -1 & 0 \\ & & & & 0 & 1 & -1 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

Weiter mit $A^1 = \begin{pmatrix} 4 \\ -4 \end{pmatrix}$

$$\xrightarrow{\text{Zeile IV} \mapsto \text{IV} + \text{III}} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 4 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ & & & & 1 & -1 & 0 \\ & & & & 0 & 1 & -1 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$$\Rightarrow \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{S} \cdot \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}}_{T} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}}_{D}$$

Die Elementarteiler sind 1, 4, 4.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{A} & \mathbb{Z}^4 & \longrightarrow & G & \longrightarrow & 0 \\ & & \cong\uparrow T & & \cong\downarrow S & & \cong & & \\ 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}^4 & \longrightarrow & G' & \longrightarrow & 0 \end{array}$$

$$G' \cong \mathbb{Z}^4/\mathrm{Im}D = \mathbb{Z}^4/\left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$$

das heißt, die Erzeuger $e_1, \dots, e_4$ von G' gegeben durch die kanonische Basis von $\mathbb{Z}^4$ erfüllen $e_1 = 0$, $4 \cdot e_2 = 0$, $4 \cdot e_3 = 0$.

$$G \cong \mathbb{Z}^4/\mathrm{Im}(A) = \mathbb{Z}^4/\mathrm{Im}(AT) = \mathbb{Z}^4/\mathrm{Im}(S^{-1}D) \cong \mathbb{Z}^4/\mathrm{Im}(D) \cong G'$$

Verwende die Spalten von S^{-1} als Basis,

$$S^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 1 \end{pmatrix},$$

setze $v_1 = \begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$, $v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Dann gilt $v_1, 4 \cdot v_2, 4 \cdot v_3 \in \mathrm{Im}(A)$,

denn $e_1, 4e_2, 4e_3 \in \mathrm{Im}(D) \Rightarrow \exists\, w_1, w_2, w_3 \in \mathbb{Z}^3$:

$D \cdot w_1 = e_1$, $D \cdot w_2 = 4e_2$, $D \cdot w_3 = 4e_3$

$\Rightarrow SATw_1 = e_1, \quad SATw_2 = 4e_2, \quad SATw_3 = 4e_3$

$\Rightarrow A(Tw_1) = S^{-1}e_1 = v_1, \quad A(Tw_2) = 4v_2, \quad A(Tw_3) = 4v_3.$

3.4.2 Bemerkung

Allgemein: Sei R euklidischer Ring (bzw allgemeiner: Hauptidealring), M endlich erzeugter R-Modul. Wegen Satz 3.3.8 ist M dann schon endlich präsentiert

$$R^n \xrightarrow{A} R^m \xrightarrow{\pi} M \to 0, \quad A \in Mat(m \times n, R)$$

Der Satz über die Smith-Normalform 3.1.3 liefert $S \in GL(m,R)$, $T \in GL(n,R)$ mit

$$\begin{array}{ccccccc} R^n & \xrightarrow{A} & R^m & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ {\scriptstyle T}\uparrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle S} & & {\scriptstyle \cong} & & \\ R^n & \xrightarrow{D} & R^m & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

mit $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$

Dann sind die $v_i = \pi(S^{-1} \cdot e_i)$ Erzeuger von M mit Relationen $d_1 v_1 = 0, \ldots, d_r v_r = 0$.

Ist d_i eine Einheit, so folgt aus

$d_i v_i = 0$ schon $v_i = 0$ und wir können den Erzeuger v_i streichen.

3.4.3 Def (R nullteilerfreier Ring)

1) Sei M ein Modul, $U_i \subset M$ Untermoduln, wir schreiben $M = U_1 \oplus \dots \oplus U_m$ falls sich jedes Element in M als Summe von Elementen in den U_i schreiben läßt und falls aus $u_1 + \dots + u_m = 0$ mit $u_i \in U_i$ folgt $u_i = 0 \ \forall i$.

2) M heißt zyklisch, wenn es von einem Element erzeugt wird.

3) $T = \{m \in M \mid \exists\, 0 \neq r \in R \text{ mit } r \cdot m = 0\} \subset M$ heißt Torsionsuntermodul.

3.4.4 Satz (Elementarteilersatz)

Sei R ein euklidischer Ring (bzw. allgemeiner: Hauptidealring), sei M ein endlich erzeugter Modul.

1) $\exists\ v_1, \dots, v_m$ Erzeuger von M und $d_1, \dots, d_r \in R$ (die (nicht Einheiten) Elementarteiler), $r \leq m$, $d_i \in R^*$, $d_i \mid d_{i+1}$ $i = 1, \dots, r-1$, so daß M durch die Relationen

$d_i \cdot v_i = 0$ beschrieben wird.

2) $M = U_1 \oplus \dots \oplus U_m$ ist direkte Summe zyklischer Untermoduln U_i und

$$U_i \cong \begin{cases} R/d_i R & i \le r \\ R & i > r \end{cases}$$

Anders gesagt:

$$M \cong R/\langle d_1 \rangle \times \dots \times R/\langle d_r \rangle \times R^{m-r}$$

Der Rang $m-r$ und die Elementarteiler sind durch M eindeutig bestimmt.

Beweis:

Konstruktiv, wie in Bemerkung 3.4.2 mit dem Smith-Normalform Algorithmus (Satz 3.1.3):

$$M = R^m/\mathrm{Im}(A) \cong M' = R^m/\mathrm{Im}(D)$$

$$= R^m/\langle d_1 e_1, \dots, d_r e_r \rangle$$

↳ wobei Einheiten schon weggelassen werden

Für die Basiswechsel S, T mit $SAT = D$ gilt $v_i = \pi(S^{-1} e_i)$ sind Erzeuger von M, die $d_i \cdot v_i = 0$ erfüllen, also

$$M = \frac{R^m}{\langle d_1 v_1, \dots, d_r v_r \rangle} = \frac{\langle v_1 \rangle \oplus \dots \oplus \langle v_m \rangle}{\langle d_1 v_1, \dots, d_r v_r \rangle}$$

$$= \frac{\langle v_1 \rangle}{\langle d_1 v_1 \rangle} \oplus \cdots \oplus \frac{\langle v_r \rangle}{\langle d_r v_r \rangle} \oplus \langle v_{r+1} \rangle \oplus \cdots \oplus \langle v_m \rangle$$

$$\cong \frac{R}{d_1 R} \times \cdots \times \frac{R}{d_r R} \times R^{m-r} \qquad \square$$

3.4.5 Korollar

Sei R euklidischer Ring (Hauptidealring), M endlich erzeugter Modul.
Sei T der Torsionsmodul von M, dann $\exists$ freier Untermodul $F \subset M$ mit $M = T \oplus F$.

Beweis: Mit dem Elementarteilersatz 3.4.4 gilt $T = U_1 \oplus \cdots \oplus U_r \cong \frac{R}{d_1 R} \times \cdots \times \frac{R}{d_r R}$
und $F = U_{r+1} \oplus \cdots \oplus U_m \cong R^{m-r}$ $\square$

Bsp (Siehe Bsp. 3.4.1)

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}, \qquad G_1 = \mathbb{Z}^4 / \mathrm{Im}(A),$$

G_1 wird erzeugt von $v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$,

$v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ mit $4 \cdot v_2 = 0$, $4 \cdot v_3 = 0$

$\Rightarrow G_1 = \langle v_2 \rangle \oplus \langle v_3 \rangle \oplus \langle v_4 \rangle$

Der Torsionsmodul T ist $T = \langle v_2, v_3 \rangle$,

$T \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, $\langle v_4 \rangle$ ist frei.
Statt v_4 kann man als freie Erzeuger auch e_2 oder e_3 wählen z.B.
T ist eindeutig.

3.4.6 Def

M heißt torsionsfrei, wenn $T = \{0\}$
und Torsionsmodul, wenn $M = T$.

3.4.7 Korollar

Sei R euklidischer Ring (Hauptidealring),
M endlich erzeugter Modul.

M frei $\Leftrightarrow$ M torsionsfrei

3.4.8 Korollar

Sei R euklidischer Ring (Hauptidealring).
Jeder Untermodul eines freien
R-Moduls ist wieder frei.

Beweis: M frei $\Rightarrow$ M torsionsfrei
$\Rightarrow$ $U \subset M$ enthält auch keine
Torsionselemente $\Rightarrow$ U frei. □

Wir können die Zerlegung
$M \cong R/\langle d_1 \rangle \times \cdots \times R/\langle d_r \rangle \times R^{m-r}$ aus dem

Elementarteilersatz 3.4.4 noch weiter verfeinern mit dem chinesischen Restsatz:

Ist $d \in R$ und $d = p_1^{r_1} \cdots p_e^{r_e}$ eine Primfaktorzerlegung mit $r_i > 0$, dann folgt mit dem chinesischen Restsatz

$$R/\langle d \rangle \cong R/\langle p_1^{r_1} \rangle \times \cdots \times R/\langle p_e^{r_e} \rangle$$

da die Ideale $\langle p_i^{r_i} \rangle$ coprim sind.

Daher folgt folgender Satz direkt aus dem Elementarteilersatz und dem chinesischen Restsatz:

3.4.9 Satz

Sei R euklidisch (bzw. allgemeiner: Hauptidealring), sei M ein endlich erzeugter R-Modul. Dann $\exists\, t \in \mathbb{N}_{\geq 0}$ und Primelemente $p_1, \ldots, p_k \in R$, $r_1, \ldots, r_k \in \mathbb{N}_{>0}$ mit

$$M \cong R/\langle p_1^{r_1} \rangle \times \cdots \times R/\langle p_k^{r_k} \rangle \times R^t$$

und diese Darstellung ist eindeutig bis auf Reihenfolge der Faktoren.

Da $\mathbb{Z}$-Moduln abelsche Gruppen sind (Bsp 3.2.2 2)) folgt insbesondere:

Satz 3.4.10 (Klassifikation der endlich erzeugten abelschen Gruppen)

Sei G eine endlich erzeugte abelsche Gruppe.

1) G ist direkte Summe von zyklischen Untergruppen.

2) $\exists\ 0 \leq r \leq m$, $d_1, \dots, d_r \geq 2$, $d_i \mid d_{i+1}\ \forall\ i = 1, \dots, r-1$ mit

$$G \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{m-r}$$

3) $\exists$ Primzahlen $p_1, \dots, p_k$ und $r_1, \dots, r_k > 0$ mit

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z}^{m-r}$$

Dabei sind r, m, d_i, p_i, r_i bis auf Reihenfolge (und Einheiten) eindeutig bestimmt.

Bsp Sei G gegeben durch die Präsentationsmatrix $\begin{pmatrix} 2 & 3 & & \\ & & 4 & \\ & & & 18 \end{pmatrix} \in \mathrm{Mat}(4, \mathbb{Z})$.

$ggT(\text{Einträge}) = 1 \Rightarrow d_1 = 1$

$ggT(2\times 2\text{-Minoren}) = ggT(6, 8, 36, 12, 54, 72)$
$= 2 \Rightarrow d_2 = 2$

$ggT(3\times 3\text{-Minoren}) = ggT(24, 108, 144, 216)$
$= 12 \Rightarrow d_3 = 6$

$\det = 2 \cdot 3 \cdot 4 \cdot 18 \Rightarrow d_4 = 2 \cdot 18 = 36$

$\Rightarrow D = \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & 6 & \\ & & & 36 \end{pmatrix}$

$\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{36}$

$6 = 2 \cdot 3, \quad 36 = 2^2 \cdot 3^2$

$\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9$

3.5 Die Jordannormalform

Bsp 3.2.27):

$$\left\{\begin{array}{l}\text{Tupel } (V,\varphi)\\ \text{mit } V \text{ } K\text{-Vektorraum},\\ \varphi: V \to V\\ \text{Endomorphismus}\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}K[x]\text{-}\\ \text{Moduln}\\ V\end{array}\right\}$$

wobei die Modulstruktur durch

$x \cdot v = \varphi(v)$ gegeben ist.

Sei $V = K^n$ und φ durch die Matrix A gegeben.

Für $f \in K[x]$ gilt dann

$f \cdot v = f(A) \cdot v$.

3.5.1 Lemma:

Sei K^n mittels $A \in \mathrm{Mat}(n, K)$ ein $K[x]$-Modul. Ein Unterraum $U \subset K^n$ ist $K[x]$-Untermodul $\Leftrightarrow A \cdot U \subset U$.

Beweis: „$\Leftarrow$" Summen sind in U, da es ein Unterraum ist.

$K[x]$-Vielfache $f \cdot v = f(A) \cdot v$ sind in U, da $A \cdot U \subset U$.

„$\Rightarrow$" $x \cdot u \in U \quad \forall u \in U \Rightarrow A \cdot u \in U$

$\forall u \in U \Rightarrow A \cdot U \subset U$. □

3.5.2 Lemma

Sei K^n ein $K[x]$- Modul mittels A.

Dann ist

$$K[x]^n \xrightarrow{x \cdot \mathbb{1}_n - A} K[x]^n \longrightarrow K^n \longrightarrow 0$$

eine endliche Präsentation von K^n.

Beweis:

$e_1, \dots, e_n \in K^n$ erzeugen K^n als $K[x]$- Modul, denn $\forall\, v \in K^n \ \exists$ $\lambda_i \in K \subset K[x]$: $v = \lambda_1 e_1 + \dots + \lambda_n e_n$

$$K[x]^n \xrightarrow{\pi} K^n : \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \longmapsto f_1(x) \cdot e_1 + \dots + f_n(x) \cdot e_n = f_1(A) \cdot e_1 + \dots + f_n(A) \cdot e_n$$

Beh $\ker(\pi)$ wird von $x \cdot e_j - A \cdot e_j$ erzeugt.

Dies folgt, da wir jeden Vektor $\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}$ durch ersetzen von $x \cdot e_j = A \cdot e_j$ in einen Vektor $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in K^n$ überführen können.

Damit $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0 \Leftrightarrow \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \in \ker(\pi) \Leftrightarrow$

$$\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} = \sum \lambda_j (x \cdot e_j - A \cdot e_j).$$

Damit gilt $\operatorname{Im}(x \mathbb{1}_n - A) = \ker(\pi)$, die Sequenz ist also exakt und liefert eine endliche Präsentation. □

<u>Bsp:</u> Sei $n = 3$ $A = (a_{ij})$.

Betrachte den Vektor $\begin{pmatrix} x^2 \\ 2x+1 \\ 2 \end{pmatrix} \in K[x]^3$.

Wir wollen ihn durch Ersetzungen $xe_j = Ae_j$ in einen Vektor in K^3 überführen. Dazu:

$$x^2 \cdot e_1 + (2x+1) \cdot e_2 + 2 \cdot e_3 =$$

$$x \cdot (x \cdot e_1) + 2 \cdot (x \cdot e_2) + e_2 + 2 \cdot e_3 =$$

$$x \cdot (a_{11} e_1 + a_{21} e_2 + a_{31} e_3) + 2(a_{12} e_1 + a_{22} e_2 + a_{32} e_3)$$

$$+ e_2 + 2e_3 = a_{11} \cdot (x e_1) + a_{21} (x e_2) +$$

$$a_{31} (x e_3) + 2a_{12} e_1 + (2a_{22}+1) e_2 + (2a_{32}+2) e_3$$

$$= a_{11} (a_{11} e_1 + a_{21} e_2 + a_{31} e_3) + a_{21} (a_{12} e_1 + a_{22} e_2 + a_{32} e_3)$$

$$+ a_{31} (a_{13} e_1 + a_{23} e_2 + a_{33} e_3) + 2a_{12} e_1 + (2a_{22}+1) e_2 +$$

$$(2a_{32}+2) e_3 = (a_{11}^2 + a_{21} a_{12} + a_{31} a_{13} + 2a_{12}) e_1$$

$$+ (a_{11} a_{21} + a_{21} a_{22} + a_{31} a_{23} + 2a_{22} + 1) e_2 +$$

$$\left(a_{11}a_{31} + a_{21}a_{32} + a_{31}a_{33} + 2a_{32} + 2\right)e_3 =$$

$$\begin{pmatrix} a_{11}^2 + a_{21}a_{12} + a_{31}a_{13} + 2a_{12} \\ a_{11}a_{21} + a_{21}a_{22} + a_{31}a_{23} + 2a_{22} + 1 \\ a_{11}a_{31} + a_{21}a_{32} + a_{31}a_{33} + 2a_{32} + 2 \end{pmatrix} \in K^3$$

3.5.3 Lemma

Das $K[x]$-Modul K^n (mittels A) ist ein Torsionsmodul.

Beweis: Nach dem Satz von Cayley-Hamilton gilt $\chi_A(A) = 0$ für das charakteristische Polynom $\chi_A = \det(x \cdot \mathbb{1}_n - A)$.

$$\Rightarrow \chi_A \cdot v = \chi_A(A) \cdot v = 0 \cdot v = 0$$

$\forall v \in V \Rightarrow v$ ist Torsionselement $\forall v \in V$. □

Bemerkung: Der Kern des Einsetzehomomorphismus

$\varphi_A : K[x] \longrightarrow \mathrm{Mat}(n, K) : f \mapsto f(A)$

ist ein Hauptideal, erzeugt vom Minimalpolynom p_A.

Es gilt auch $p_A \cdot v = 0 \quad \forall v \in V$.

$p_A \mid \chi_A$ folgt aus dem Satz von Cayley-Hamilton.

3.5.4 Lemma

χ_A zerfalle in Linearfaktoren. Dann ist K^n als $K[X]$-Modul mittels A eine direkte Summe

$$K^n = U_1 \oplus \cdots \oplus U_k$$

zyklischer Untermoduln U_i mit $U_i \cong \frac{K[X]}{\langle (X-\lambda_i)^{r_i} \rangle}$,

wobei $\chi_A = \prod_i (X-\lambda_i)^{r_i}$.

Beweis:

Bestimme die Smith-Normalform von $X \cdot \mathbb{1}_n - A$ (3.1.4), $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$, wobei $d_i \neq 0$ gelten muß, da K^n Torsionsmodul ist (Elementarteilersatz 3.4.4, 3.4.5).

Wir zerlegen weiter mit dem chinesischen Restsatz (3.4.9) und erhalten

$$K^n = U_1 \oplus \cdots \oplus U_k \quad \text{mit} \quad U_i \cong \frac{K[X]}{\langle p_i^{r_i} \rangle}$$

mit Primelementen $p_i \in K[X]$.

Es gilt $\prod p_i^{r_i} = d_1 \cdots d_r = \det(D)$

$= \det(X \mathbb{1}_n - A) = \chi_A$.

Da χ_A zerfällt, müssen die p_i von der Form $p_i = X - \lambda_i$ sein. □

3.5.5 Satz (Jordannormalform)

Sei $A \in Mat(n, K)$, χ_A zerfalle in Linearfaktoren über K.
Dann $\exists$ Basis B bezüglich der A die Form $\begin{pmatrix} J(\lambda_1, r_1) & & \\ & \ddots & \\ & & J(\lambda_k, r_k) \end{pmatrix}$ hat,

wobei die $J(\lambda_i, r_i)$ Jordankästchen der Größe r_i sind, $J(\lambda_i, r_i) = \begin{pmatrix} \lambda_i & & \\ 1 & \ddots & \\ & 1 & \lambda_i \end{pmatrix}$,

die λ_i nicht notwendig verschieden.
Bis auf Reihenfolge ist die Darstellung eindeutig.

Beweis: Wir betrachten die Zerlegung $K^n = U_1 \oplus \dots \oplus U_k$ aus Lemma 3.5.4.
mit $U_i \overset{\varphi_i}{\cong} K[X] / \langle (X - \lambda_i)^{r_i} \rangle$.

Betrachte $K[x]/\langle (x-\lambda_i)^{r_i} \rangle$ als K-Vektorraum, eine Basis ist $1, x-\lambda_i, (x-\lambda_i)^2, \dots, (x-\lambda_i)^{r_i-1}$.

Die Bilder dieser Basis unter dem Isomorphismus φ_i nennen wir $v_{ij} \in U_i$, $j = 0, \dots, r_i - 1$.

$$(A - \lambda_i \cdot \mathbb{1}_n) \cdot v_{ij} = (x - \lambda_i) \cdot \varphi_i\left((x-\lambda_i)^j\right)$$

φ_i $K[x]$-linear

$$\varphi_i\left((x-\lambda_i)^{j+1}\right) = \begin{cases} v_{i\,j+1} & j = 0, \dots, r_i - 2 \\ 0 & j = r_i - 1 \end{cases}$$

$$\Rightarrow \quad A \cdot v_{ij} = \begin{cases} \lambda_i \cdot v_{ij} + v_{i\,j+1} & j = 0, \dots, r_i - 2 \\ \lambda_i \cdot v_{ij} & \text{sonst.} \end{cases}$$

Bezüglich der Basis $\{v_{ij}\}$ hat $A|_{U_i}$ also die Form

$$\begin{pmatrix} \lambda_i & & \\ 1 & \ddots & \\ & 1 & \lambda_i \end{pmatrix}$$

und insgesamt hat A die gewünschte Form. $\square$