Erinnerung: Sei R ein Hauptidealring.

4.10.2 Satz: Für jeden endlich erzeugten R-Modul M existieren Zahlen $r, k \geqslant 0$ und Elemente $e_1, \ldots, e_k \in R \setminus (\{0\} \cup R^\times)$ mit $e_1 | e_2 | \ldots | e_k$, so dass gilt

$$\boxed{M \cong R^r \boxplus \bigboxplus_{i=1}^{k} R/(e_i)}$$

4.10.3 Definition: Elemente $m_1, \ldots, m_\ell$ von M heissen *linear unabhängig*, wenn für alle $a_1, \ldots, a_\ell \in R$ gilt $a_1 m_1 + \ldots + a_\ell m_\ell = 0 \Rightarrow a_1 = \ldots = a_\ell = 0$.

4.10.4 Zusatz: (a) Die Zahl r ist die maximale Anzahl linear unabhängiger Elemente von M. Insbesondere ist sie eindeutig bestimmt. Sie heisst der *„freie Rang" von M.*

(b) Die Zahl $r + k$ ist die minimale Anzahl von Erzeugenden von M. Insbesondere ist k eindeutig bestimmt.

(c) Die Elemente $e_1, \ldots, e_k$ sind bis auf Assoziiertheit durch M eindeutig bestimmt. Sie heissen die *Elementarteiler von M.*

Beweis (a): Seien $m_1, \ldots, m_s \in M$ lin. unabh.

m_i entspreche (v_i, w_i) mit $v_i \in R^r$, $w_i \in \bigboxplus_{i=1}^{k} R/(e_i)$

$\Rightarrow e_k m_i$ entspricht $(e_k v_i, e_k w_i)$ mit $e_k w_i = 0$

$\Rightarrow e_k v_i \,|_{i=1,..,s}$ lin. unabh. in R^r.

Sei $K := \mathrm{Quot}(R) \Rightarrow e_k v_i \in K^r$.

Annahme: $s > r$.

$\Rightarrow \exists\, x_1, \ldots, x_s \in K$, nicht alle 0, mit $\sum_{i=1}^{s} x_i e_k v_i = 0$.

Schreibe $x_i = \frac{a_i}{b}$ mit $a_i, b \in R$; $b \neq 0$

nicht alle $a_i = 0$. $\Rightarrow \sum_{i=1}^{s} \underbrace{a_i e_k}_{\text{nicht alle } 0} \cdot v_i = 0$.

$\boxed{\sum_{i=1}^{s} a_i e_k m_i = 0.}$

Also ist $s \leq r$.

$\Rightarrow m_1, \dots, m_s$ lin. abh. (W).

Sei $e_1, \dots, e_r$ die Standardbasis von R^r

$\Rightarrow$ lin. unabh. von $(e_1, 0), \dots, (e_r, 0)$ entsprechen lin. unabh. Elementen von M. ✓

(b) M von $r+k$ Elementen erzeugt.

Wähle $p \in R$ prim mit $p \mid e_i$ für alle i. $\Rightarrow F := R/(p)$ Körper

$$\Rightarrow M/pM \cong (R/pR)^r \oplus \bigoplus_{i=1}^{k} \underbrace{(R/(e_i))/p \cdot (R/(e_i))}_{R/pR}$$

$$\cong F^r \oplus \bigoplus_{i=1}^{k} F \cong F^{r+k}.$$

R operiert darauf durch $R \twoheadrightarrow F$, und M/pM hat minimale Erzeugendenzahl $\dim_F (M/pM) = r+k$.

$M \twoheadrightarrow M/pM \Rightarrow M$ kann nicht von $< r+k$ Elementen erzeugt werden. ✓

(c) weggelassen.

gez.

4.10.5 Satz: Für jeden endlich erzeugten R-Modul M existieren Zahlen $r, \ell \geqslant 0$ und Primelemente $p_i \in R$ und Exponenten $\nu_i \geqslant 1$, so dass gilt

$$M \cong R^r \boxplus \bigboxplus_{i=1}^{\ell} R/(p_i^{\nu_i}).$$

Bew.: Seien r, ℓ, e_i wie in 4.10.2.

Schreibe $e_1 = \text{Einheit} \cdot p_1^{\nu_1} \cdots p_s^{\nu_s}$ mit p_i prim, inäquivalent, $\nu_i > 0$.

$\Rightarrow R/(e_1) = R/(p_1^{\nu_1} \cdots p_s^{\nu_s}) \cong \bigboxplus_{i=1}^{s} R/(p_i^{\nu_i})$. Chines. Restsatz.

übrige $R/(e_i)$ analog. qed.

4.10.6 Zusatz: Für jedes Primelement $p \in R$ und jedes $\nu \geqslant 0$ gilt

$$\boxed{\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) = r + \big|\{1 \leqslant i \leqslant \ell \mid p_i \sim p \wedge \nu_i > \nu\}\big|.}$$

Insbesondere sind die Zahlen r und ℓ, sowie die Paare (p_i, ν_i) bis auf Vertauschung und Assoziiertheit der p_i, durch M eindeutig bestimmt.

Hierauf operiert R durch $R \twoheadrightarrow R/pR =: \mathbb{F}$ Körper.

Bew.: $$p^\nu M/p^{\nu+1}M \cong \underbrace{\left(p^\nu R/p^{\nu+1}R\right)^r}_{\cong\, \mathbb{F}^r} \boxplus \bigboxplus_{i=1}^{\ell} \underbrace{\frac{p^\nu \cdot (R/(p_i^{\nu_i}))}{p^{\nu+1} \cdot (R/(p_i^{\nu_i}))}}.$$

$R \xrightarrow[\sim]{p^\nu} p^\nu R$.

$pR \xrightarrow[\sim]{p^\nu} p^{\nu+1} R$

$\Rightarrow R/pR \xrightarrow{\sim} p^\nu R/p^{\nu+1}R$.

$\mathbb{F}$ $\Rightarrow$

Fall: $p_i \not\sim p \Rightarrow p_i^{\nu_i}, p^\nu$ teilerfremd $\Rightarrow R = (p_i^{\nu_i}) + (p^\nu)$.

$\Rightarrow p^\nu \cdot (R/(p_i^{\nu_i})) = R/(p_i^{\nu_i})$

analog: $p^{\nu+1} \cdot (R/(p_i^{\nu_i})) = R/(p_i^{\nu_i})$

$\Rightarrow$ Faktormodul $= 0$.

$$\Rightarrow p^\nu M / p^{\nu+1} M \cong \mathbb{F}^r \oplus \bigoplus_{\substack{i \text{ mit } p_i \sim p \\ \nu < \nu_i}} \mathbb{F}$$

<u>Fall $p_i \sim p$.</u>

Unterfall $\nu \geq \nu_i \Rightarrow p^\nu \cdot (R/(p_i^{\nu_i})) = 0 = p^{\nu+1}(R/(p_i^{\nu_i}))$

$\Rightarrow$ Faktormodul 0.

Unterfall $\nu < \nu_i \Rightarrow p^\nu(R/(p_i^{\nu_i})) = p^\nu R / p^{\nu_i} R$

$p^{\nu+1}(R/(p_i^{\nu_i})) = p^{\nu+1} R / p^{\nu_i} R$

Faktormodul $\cong p^\nu R / p^{\nu+1} R \cong \mathbb{F}$.

<u>qed.</u>

4.11 Abelsche Gruppen

$R = \mathbb{Z}$.

Erinnerung: Jede additiv geschriebene abelsche Gruppe G ist ein $\mathbb{Z}$-Modul mit der Multiplikation

$$\mathbb{Z} \times G \to G, \quad (n, g) \mapsto n \cdot g.$$

4.11.1 Klassifikationssatz: Für jede endlich erzeugte abelsche Gruppe G existieren eindeutige ganze Zahlen r, $k \geqslant 0$ und $1 \cancel{\neq} e_1 | \dots | e_k \neq 0$, so dass gilt

$1 < e_1 \dots$

$$\boxed{G \;\cong\; \mathbb{Z}^r \boxplus \bigboxplus_{i=1}^{k} \mathbb{Z}/e_i\mathbb{Z}.}$$

4.11.2 Klassifikationssatz: Für jede endlich erzeugte abelsche Gruppe G existieren r, $\ell \geqslant 0$ und Primzahlen p_i sowie Exponenten $\nu_i \geqslant 1$, so dass gilt

$$\boxed{G \;\cong\; \mathbb{Z}^r \boxplus \bigboxplus_{i=1}^{\ell} \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}.}$$

Dabei sind r und ℓ, sowie die Paare (p_i, ν_i) bis auf Vertauschung, eindeutig bestimmt.

4.11.3 Bemerkung: Die Zahl r heisst der *„freie Rang“ von G.* (Vergleiche §1.14.)

4.11.4 Proposition: Es gilt $r = 0$ genau dann, wenn G endlich ist. In diesem Fall gilt

$$\begin{aligned} |G| &= p_1^{\nu_1} \cdots p_\ell^{\nu_\ell}, \\ \exp(G) &= \mathrm{kgV}(p_1^{\nu_1}, \ldots, p_\ell^{\nu_\ell}). \end{aligned}$$

4.11.5 Beispiel: Es gibt genau zwei Isomorphieklassen von endlichen $\mathbb{Z}$-Moduln der Kardinalität $28 = 2^2 \cdot 7$, nämlich die von

$$\begin{aligned} \mathbb{Z}/28\mathbb{Z} &\cong \mathbb{Z}/7\mathbb{Z} \boxplus \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \boxplus \mathbb{Z}/14\mathbb{Z} &\cong \mathbb{Z}/7\mathbb{Z} \boxplus \mathbb{Z}/2\mathbb{Z} \boxplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

4.12 Jordansche Normalform

$R = K[X]$

4.12.1 Konstruktion: Sei K ein Körper. Jeder K-Vektorraum V mit einem Endomorphismus $\varphi \in \mathrm{End}_K(V)$ wird durch

$$(f, v) \longmapsto f(\varphi)(v)$$

$$K[X] \times V \to V, \ \left(\sum{}' a_i X^i, v\right) \mapsto \sum{}' a_i \varphi^i(v)$$

zu einem $K[X]$-Modul. Umgekehrt können wir jeden $K[X]$-Modul als einen K-Vektorraum mit dem zusätzlichen Endomorphismus $m \mapsto Xm$ ansehen. Die Theorie der $K[X]$-Moduln ist deshalb äquivalent zu der Theorie der Paare (V, φ).

4.12.2 Proposition: Sei $M \cong K[X]/(f)$ für ein normiertes Polynom $f \in K[X]$. Dann ist $\dim_K(M) = \deg(f)$, und der obige Endomorphismus $\varphi \in \mathrm{End}_K(M)$ hat das charakteristische Polynom f und das Minimalpolynom f.

Bew.: Sei $g \in K[X] \Rightarrow g(\varphi)(m_0) = g(X) + (f)$. Dies ist 0 g.d.w. $f \mid g$.

Sei $m_0 := 1 + (f)$ Erzeugendes von M. $\Rightarrow g(\varphi) = 0 \iff f \mid g$.

Also ist f das Min.Pol. von φ.

Also teilt f das char. Pol. von φ, und dieses hat Grad $\dim_K(M) = \deg(f)$ und ist normiert

$\Rightarrow f =$ Char.Pol. von φ. qed.

4.12.3 Satz: Für jeden $K[X]$-Modul V mit $\dim_K(V) < \infty$ existieren $k \geqslant 0$ und normierte irreduzible Polynome $p_i \in K[X]$ sowie Exponenten $\nu_i \geqslant 1$, so dass gilt

$$\boxed{V \cong \bigoplus_{i=1}^{k} K[X]/(p_i^{\nu_i}).}$$

Dabei sind k, und die Paare (p_i, ν_i) bis auf Vertauschung, eindeutig bestimmt.

Direkte Folge aus 4.10.5, $r = 0$ da $\dim_K V < \infty$ und $\dim_K K[X] = \infty$

4.12.4 Zusatz: Für $\varphi \in \mathrm{End}_K(V)$ wie oben gilt:

(a) Das charakteristische Polynom von φ ist gleich $p_1^{\nu_1} \cdots p_k^{\nu_k}$.

(b) Das Minimalpolynom von φ ist gleich $\mathrm{kgV}(p_1^{\nu_1}, \dots, p_k^{\nu_k})$.

(c) Der Hauptraum von φ zum normierten irreduziblen Polynom p entspricht den Summanden in der obigen Zerlegung mit $p_i = p$.

(d) Jordansche Normalform.

$\mathrm{Hau}_p(\varphi) = \mathrm{Ker}(p^N(\varphi))$

N = Exponent von p in char. Pol.

Spezialfall $p_i = X - \lambda_i$,

$\Rightarrow K[X]/((X-\lambda_i)^{\nu_i})$

Basis $[1], [p_i], [p_i^2], \dots, [p_i^{\nu_i-1}]$.

$\Rightarrow (\varphi - \lambda_i \cdot id)([p_i^j]) = p_i(\varphi)[p_i^j] = [p_i^{j+1}]$

geordnete Basis $B_i := ([p_i^{\nu_i-1}], \dots, [p_i], [1])$

$$\Rightarrow {}_{B_i}[\varphi|_{K[X]/(p_i^{\nu_i})}]_{B_i} = \begin{pmatrix} \lambda_i & 1 & & 0 \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{pmatrix}$$

Fall $n = \deg(p_i) > 1$.

A = Begleitmatrix von p_i.

$$\begin{pmatrix} \boxed{A} & 1 & & 0 \\ & \boxed{A} & 1 & \\ & & \ddots & 1 \\ 0 & & & \boxed{A} \end{pmatrix}$$

$$B_i = (\ldots, [X \cdot p_i], [p_i], [X^{n-1}], \ldots, [X], [1])$$

$\rightsquigarrow$ Darstellungsmatrix = Jordanblock.