Jetzt ist R ein Hauptidealring, also noethersch, kommutativ, Integritätsbereich.
Unser Ziel ist eine Klassifikation von Moduln, genauer von endlich erzeugten Moduln.
Ein endlich erzeugter Modul M ist ein Quotient von R^n (für irgendein n), denn:
$m_1,\dots,m_n$ Erzeugendensystem $\Rightarrow$ $\varphi: R^n \longrightarrow M$ ist ein surjektiver Modulhomomorphismus.
$$(0,\dots,\underset{i}{1},\dots,0) \mapsto m_i$$

5.9 $\Rightarrow$ M ist noethersch.

Umgekehrt ist ein noetherscher Modul endlich erzeugt. Wir wollen also auch die ~~endl~~ noetherschen Moduln klassifizieren, bis auf Isomorphie.

Wenn $R = K$ ein Körper ist, ist das Ergebnis der Klassifikation genau die Menge der Vektorräume K^n, $n \in \mathbb{N}_0$. Diese kennen wir eigentlich schon, wenn wir K selbst kennen, denn $K^n \cong \underbrace{K \oplus K \oplus \dots \oplus K}_{n \text{ Summanden}}$, eine direkte Summe.

Direkte Summen kann man auch bei Moduln bilden: Seien M_1 und M_2 R-Moduln, dann ist $M := \underline{M_1 \oplus M_2}$, die <u>direkte Summe</u>, auch ein R-Modul,
$$= \{(m_1,m_2) : m_1 \in M_1, m_2 \in M_2\} \quad \leftarrow \text{siehe 5.4}$$
mit komponentenweiser Addition und R-Operation.

5.10 Definition: Ein R-Modul $M \neq 0$ heißt <u>zerlegbar</u> $:\Leftrightarrow$ $\exists$ Untermoduln M_1 und M_2 von M, beide $\neq 0$, so daß $M = M_1 \oplus M_2$. Sonst heißt M <u>unzerlegbar</u>.
alternativ: $M \xrightarrow[f]{\sim} M_1' \oplus M_2'$ dann ist $M = f^{-1}(M_1') \oplus f^{-1}(M_2')$

Ein K-Vektorraum ist unzerlegbar, wenn er isomorph zu K ist, sonst nicht.
Das ist schon bei $R = \mathbb{Z}$ nicht mehr so einfach. $\mathbb{Z}$ selbst ist unzerlegbar. $\mathbb{Z}/6\mathbb{Z}$ ist zerlegbar in $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ und diese sind unzerlegbar.
Wie zeigt man, daß ein Modul unzerlegbar ist?
Kann man jeden endlich erzeugten Modul in eine direkte Summe von unzerlegbaren Moduln zerlegen?
Ist so eine Zerlegung "im wesentlichen" eindeutig? D.h. folgt z.B. aus
$M = M_1 \oplus M_2 = M_3 \oplus M_4$, daß $M_1 \cong M_3$ (oder M_4) ist und $M_2 \cong M_4$ (oder M_3)?
alle unzerlegbar — nicht: $=$
Und daß es keine Zerlegung mit drei Summanden gibt?

Beispiel: Ein Ideal $\underset{\neq 0}{I} \subset R$ (Integritätsbereich) ist unzerlegbar.

Denn: Angenommen $\underset{\neq 0}{I} = \underset{\neq 0}{I_1} \oplus \underset{\neq 0}{I_2}$. Sei $\underset{\neq 0}{a} \in I_1$ und $\underset{\neq 0}{b} \in I_2$. Was ist ab? Wie folgt ein Widerspruch?

Eine Methode, Unzerlegbarkeit zu testen:

Sei M ein R-Modul (R irgendein Ring). Falls M zerfällt in

$$M = M_1 \oplus M_2, \quad M_1 \text{ und } M_2 \neq 0$$

Dann gibt es diverse Modulhomomorphismen nachprüfen

$$\begin{tikzcd} & M_1 \\ M \arrow[ur, "p_1"] \arrow[dr, "p_2"'] & \\ & M_2 \end{tikzcd} \qquad \text{Projektionen: } \begin{array}{l} p_1 : (m_1, m_2) \longmapsto m_1 \\ p_2 : (m_1, m_2) \longmapsto m_2 \end{array} \quad \text{surjektiv}$$

$$\text{und} \quad \begin{tikzcd} M_1 \arrow[dr, hook, "i_1"] & \\ & M \\ M_2 \arrow[ur, hook, "i_2"'] & \end{tikzcd} \qquad \text{Inklusionen: } \begin{array}{l} i_1 : m_1 \longmapsto (m_1, 0) \\ i_2 : m_2 \longmapsto (0, m_2) \end{array} \quad \text{injektiv}$$

Also auch $i_1 \circ p_1 : M \to M_1 \to M$ und analog $i_2 \circ p_2$

$p_1 \circ i_1 : M_1 \to M \to M_1$ $\qquad p_2 \circ i_2$

Diese Homomorphismen erfüllen interessante Gleichungen:

$$p_1 \circ i_1 : m_1 \longmapsto (m_1, 0) \longmapsto m_1 \Rightarrow p_1 \circ i_1 = id_{M_1} \in End(M_1)$$

$$p_2 \circ i_2 = id_{M_2}$$

$$(i_1 \circ p_1) \circ (i_1 \circ p_1) = i_1 \circ (p_1 \circ i_1) \circ p_1 = \underbrace{i_1 \circ p_1}_{=: e_1} \in End(M)$$

also: $e_1^2 = e_1$

Ebenso: $e_2^2 = e_2$

$$e_1 + e_2 : \begin{tikzcd} M \arrow[r, "p_1"] \arrow[dr, "p_2"'] & M_1 \arrow[r, "i_1"] & M \\ & \oplus & \\ & M_2 \arrow[uur, "i_2"'] & \end{tikzcd}, \quad (m_1, m_2) \longmapsto \begin{array}{c} m_1 \\ + \\ m_2 \end{array} \longmapsto \begin{array}{c} (m_1, 0) \\ + \\ (0, m_2) \end{array} = (m_1, m_2)$$

$\Rightarrow e_1 + e_2 = id_M$

oder: $e_2 = 1 - e_1 \quad (1 = id_M)$

$\Rightarrow \underbrace{(1 - e_1)}_{\substack{\shortparallel \\ e_2}} \cdot e_1 = 1 \cdot e_1 - e_1^2 = 0$, ebenso $e_1(1 - e_1) = 0$

nachprüfen

5.11 Definition: Ein Element e in einem Ring heißt Idempotent $:\Leftrightarrow e^2=e$.
(oder: Idempotents)

1 ist immer idempotent, 0 auch. 0 ist das einzige Element, das nilpotent und idempotent ist.
Mit e ist auch $1-e$ idempotent: $(1-e)^2=1-2e+e^2=1-e$.
e und $1-e$ sind (zueinander) orthogonale Idempotente: $e(1-e)=(1-e)e=0$.

Eine Zerlegung $_R M=M_1\oplus M_2$ liefert orthogonale Idempotente e und $1-e$ in $\mathrm{End}_R(M)$. Die Umkehrung gilt auch: Sei $e\in\mathrm{End}_R(M)$ idempotent, d.h. $e=e^2$.
$e:M\to M$ ist ein Modulhomomorphismus $\Rightarrow$

$$M_1:=\mathrm{Im}(e)=\{e(m): m\in M\} \text{ und}$$
$$M_2:=\mathrm{Kern}(e)$$

sind Untermoduln von M.
Wir zeigen: $M=M_1\oplus M_2$.
$M_1\cap M_2=\{0\}$: Sei $e(m)\in M_1\cap M_2$, d.h. $\overbrace{e(e(m))}^{e^2(m)=e(m)}=0$
$M_1+M_2=M$: Sei $m\in M\Rightarrow m=\underset{\substack{\cap\\ M_1}}{e(m)}+\underbrace{(m-e(m))}_{(1-e)(m)\,\in M_2}$ warum?
$\Rightarrow$

5.12 Proposition: Eine Zerlegung des Moduls M in $M=\underset{\neq 0}{M_1}\oplus \underset{\neq 0}{M_2}$ entspricht einer Zerlegung $1_M=\underset{\neq 0}{e}+\underset{\neq 0}{(1-e)}$ mit $e^2=e$ in $\mathrm{End}(M)$.

Insbesondere ist der Modul M unzerlegbar genau dann, wenn 0 und 1 die einzigen Idempotente in $\mathrm{End}(M)$ sind.

Anwendung: R Integritätsbereich $\Rightarrow {}_R R$ unzerlegbar
Denn: $\mathrm{End}_R(R)\simeq R$ $\quad\alpha: R\to R$ ist durch $\alpha(1)$ festgelegt und $\alpha(1)$ kann gewählt werden
und $e\neq 0,1\Rightarrow 1-e\neq 0,1$ $\lightning$
$\rightsquigarrow$ z.B. $\mathbb{Z}$ ist unzerlegbar als abelsche Gruppe
$\mathbb{Z}\oplus\mathbb{Z}$ zerlegbar, z.B. $\mathrm{End}(\mathbb{Z}\oplus\mathbb{Z})=\mathrm{Mat}(2\times 2,\mathbb{Z})\ni\begin{pmatrix}1&0\\0&0\end{pmatrix}=e$

nachprüfen

Wenn M zerlegbar ist, gibt es eine Zerlegung $M = M_1 \oplus M_2$. Wenn M_1 und M_2 nicht unzerlegbar sind, gibt es eine verfeinerte Zerlegung

$$M = \underbrace{M_1' \oplus M_1''}_{M_1} \oplus \underbrace{M_2' \oplus M_2''}_{M_2}$$ usw und das geht vielleicht immer so weiter.

(Es gibt sogar "super-zerlegbare" Moduln: $M \neq 0$, hat aber keinen unzerlegbaren direkten Summanden.)

Bei noetherschen Moduln kann das nicht passieren:

5.13 Proposition: Sei M ein noetherscher R-Modul. Dann gibt es eine Zerlegung $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$, wobei die Untermoduln $M_1, \ldots, M_n$ unzerlegbar sind.

Beweis: $M = 0$ ist $M = \bigoplus_{\emptyset}$ (leere Summe). Sei also jetzt $M \neq 0$.

Sei $\mathcal{U} := \{ U$ Untermodul von M : U ist keine endliche direkte Summe von unzerlegbaren Teilmoduln$\}$

Angenommen der Satz ist falsch, d.h. $M \in \mathcal{U}$.

Sei $M' \in \mathcal{U}$. Also $M' \neq 0$ und $\exists$ Zerlegung $M' = M_1 \oplus M_2$, beide $\neq 0$. $M_1 \oplus M_2$ ~~können~~ kann wegen $M' \in \mathcal{U}$ auch keine endliche direkte Summe von unzerlegbaren Teilsummen sein $\Rightarrow M_1 \in \mathcal{U}$ oder $M_2 \in \mathcal{U}$.

Sei $\mathcal{X} := \{ N \subset M$ Untermodul, echt d.h. $N \neq M$, und $\exists M' \in \mathcal{U}$ mit $M = N \oplus M' \}$

$\ni$ z.B. $N = 0$, mit $M' = M$

M noethersch $\Rightarrow$ in $\mathcal{X} \neq \emptyset$ gibt es ein maximales Element bezüglich Inklusion. Sei $M' \in \mathcal{U}$ mit $M = N \oplus M'$ für dieses N.

$M' \in \mathcal{U} \Rightarrow \exists M_1, M_2 \subset M'$ mit $M_1 \neq 0 \neq M_2$, $M' = M_1 \oplus M_2$ und $M_2 \in \mathcal{U}$

Sei $N' := N \oplus M_1 \Rightarrow M = N' \oplus M_2$ mit $M_2 \in \mathcal{U}$ und $N' \neq M$ (da $M_2 \neq 0$)

$\Rightarrow N' \in \mathcal{X}$. Aber $N \subseteq N'$, wegen $M_1 \neq 0$ sogar $N \subsetneq N'$ $\lightning$ zu N maximal.

$\Rightarrow$ Widerspruch zur Annahme $M \in \mathcal{U}$, d.h. zur Annahme, daß der Satz falsch ist. $\square$

Zur "Eindeutigkeit" der Zerlegung kommen wir erst später.

R ist weiterhin ein Hauptidealring und das wird jetzt immer häufiger benutzt werden. Noethersche R-Moduln sind endlich erzeugt, also Quotienten von Moduln R^n ($n \in \mathbb{N}$). R^n ist unzerlegbar genau für $n=1$. warum? Die freien Moduln R^n kennen wir schon ganz gut. Ihre Isomorphie Klasse ist durch den Rang bestimmt – R^n hat Rang n.

Wie gehen wir nun mit allgemeinen noetherschen Moduln M um? Es gibt einen surjektiven Homomorphismus $R^n \xrightarrow{\varphi} M$ für ein $n \in \mathbb{N}$

$$\Rightarrow \exists \text{ kurze exakte Sequenz } \quad 0 \to \operatorname{Kern}(\varphi) \to R^n \to M \to 0$$

Wir sollten uns also Teilmoduln von R^n anschauen, wie $\operatorname{Kern}(\varphi)$.

Außerdem können wir M zerlegen und manche direkten Summanden können selbst freie Moduln sein, während andere vielleicht keine Basen haben. Also sollten wir auch freie direkte Summanden von den anderen trennen.

5.14 Proposition: Seien M_1 und M_2 R-Moduln mit $M_1 \oplus R \cong M_2 \oplus R$. Dann gilt $M_1 \cong M_2$.

Beweis: Die Voraussetzung können wir, durch Anwendung eines Isomorphismus, so umschreiben: $\exists$ R-Modul M mit Untermoduln M_1, M_2, N_1, N_2 so daß $M = M_1 \oplus N_1 = M_2 \oplus N_2$ und $N_1 \cong R \cong N_2$.

Diese Moduln können wir auch so schreiben: $M \xrightarrow{p_1} N_1$, $M \xrightarrow{p_2} N_2$ seien die Projektionen

$\Rightarrow N_1 = \operatorname{Im}(p_1)$, $N_2 = \operatorname{Im}(p_2)$

$M_1 = \operatorname{Kern}(p_1)$, $M_2 = \operatorname{Kern}(p_2)$

Idee: p_1 bezieht sich auf die erste Zerlegung, aber wir können es auch auf die zweite Zerlegung anwenden, z.B. auf M_2. $p_1(M_2)$ ist 0 oder nicht.

Erster Fall: $p_1(M_2) = 0$. $\Rightarrow M_2 \subset \operatorname{Kern}(p_1) = M_1$. Wir wollen: $M_2 = M_1$

$N_1 = p_1(M) = p_1(M_2 + N_2) \overset{\text{warum?}}{=} p_1(N_2)$

$N_1 \cong R \cong N_2 \Rightarrow N_2 = R v_2$ für ein Element v_2 (das Bild von 1 unter $R \xrightarrow{\sim} N_2$, $1 \mapsto v_2$)

Falls $p_1(a v_2) = 0$ für ein $a \in R$, also $a \underbrace{p_1(v_2)}_{\substack{\cap \\ N_1 \cong R}} = 0 \Longrightarrow a = 0$ oder $p_1(v_2) = 0$

unter Isom $N_1 \xrightarrow{\sim} R$, R Int bereich

Aber $N_1 = p_1(N_2) = p_1(Rv_2)$

$\Rightarrow p_1(v_2) = 0$ ist unmöglich

$\Rightarrow N_2 \cap \underbrace{\mathrm{Kern}(p_1)}_{=M_1} = 0$, also $N_2 \cap M_1 = 0$

und damit: $M_1 = M_1 \cap M = M_1 \cap (M_2 + N_2) = \underbrace{(M_1 \cap M_2)}_{=M_2} + (M_1 \cap N_2) =$
$= M_2 + \underbrace{(M_1 \cap N_2)}_{=0} = M_2$ ✓

Zweiter Fall: $p_1(M_2) \neq 0$.

Nach Definition von p_1: $0 \to \mathrm{Kern}(p_1) \to M \xrightarrow{p_1} \mathrm{Im}(p_1) \to 0$

$$\begin{array}{ccccc} \mathrm{Kern}(p_1) & & M & & \mathrm{Im}(p_1) & \\ \shortparallel & & \cup & & \shortparallel & \\ M_1 & & M_2 & & N_1 \simeq R & I \\ & & & & & \shortparallel \end{array}$$

$p_1(M_2)$ ist ein Teilmodul von $N_1 \simeq R$, also ist $p_1(M_2) \simeq$ Ideal in R $\neq 0$
R Hauptidealring $\Rightarrow \exists\, a \in R: I = Ra,\ a \neq 0$
Sei $\varphi: p_1(M_2) \xrightarrow{\sim} Ra$ ein Isomorphismus und $\tau: R \to Ra$, $b \mapsto ba$
$\mathrm{Kern}(\tau) = \{b \in R : ba = 0\}$, aber R ist ein Integritätsbereich $\Rightarrow \mathrm{Kern}(\tau) = 0 \Rightarrow \tau$ injektiv und natürlich auch surjektiv. Insgesamt ist also $p_1(M_2) \simeq R$.
Daraus erhalten wir eine neue exakte Folge:

$$0 \to \underbrace{\mathrm{Kern}(p_1)}_{M_1} \cap M_2 \to M_2 \xrightarrow{p_1} \underbrace{p_1(M_2)}_{\simeq R} \to 0$$

R ist freier Modul mit Basis 1, also ist $p_1(M_2)$ auch frei vom Rang 1, mit Basis w_1 $\Rightarrow \exists$ Modulhomomorphismus $R \xrightarrow{\sim} p_1(M_2) \xrightarrow{\alpha} M_2$, $1 \longmapsto w_1 \longmapsto u_1$
wobei u_1 ein frei wählbares p_1-Urbild von w_1 ist.
Dann ist $p_1 \circ \alpha: p_1(M_2) \to p_1(M_2)$ die identische Abbildung warum?
und es folgt: $M_2 \simeq (M_1 \cap M_2) \oplus p_1(M_2) \simeq (M_1 \cap M_2) \oplus R$ Details?
↑ warum?

Das reicht noch nicht, wir müssen genau dieselbe Rechnung mit ~~M_2~~ $p_2(M_1)$ machen.
Wieder gibt es zwei Fälle. Im ersten Fall folgt $M_2 = M_1$. Im zweiten Fall erhalten wir $M_1 \simeq (M_1 \cap M_2) \oplus R \overset{\text{s. oben}}{\simeq} M_2$. □

Induktiv können wir damit beweisen: $R^n \cong R^m \Rightarrow m=n$, also nochmal die Wohldefiniertheit des Rangs.
Vor allem aber: Einen beliebigen noetherschen Modul kann man in einen freien Summanden R^n und ein bis auf Isomorphie eindeutiges Komplement zerlegen.

Als nächstes betrachten wir Untermoduln von freien Moduln. $M \subset \mathbb{Z}$, $M \neq 0$ bedeutet: $M = n\mathbb{Z} \cong \mathbb{Z}$. Im Beweis von 5.14 haben wir gesehen, daß auch Teilmoduln (Ideale) von R selbst frei vom Rang 1 sind (oder 0).
Wie sieht es mit Teilmoduln von R^n aus?

5.15 Theorem: Sei M ein freier R-Modul vom Rang $n \in \mathbb{N}$. Dann ist jeder Untermodul von M frei vom Rang $\leq n$.

Beweis: Induktion nach n. $n=0$: nichts zu zeigen.
$n=1$: Untermoduln von R sind 0 oder $\cong R$, schon gezeigt.
Sei $n>1$: Sei $b_1, \dots, b_n$ eine Basis von M und $M' := \langle v_1, \dots, v_{n-1} \rangle$ der von $v_1, \dots, v_{n-1}$ erzeugte Untermodul von M. M' ist frei vom Rang $n-1$. warum?
M' können wir als Kern eines Modulhomomorphismus schreiben:

$$M \xrightarrow{f} R \quad \text{mit } f\left(\sum_{i=1}^{n} a_i v_i\right) := a_n, \text{ d.h. } f: \begin{array}{l} v_1 \mapsto 0 \\ \vdots \\ v_{n-1} \mapsto 0 \\ v_n \mapsto 1 \end{array}$$

hat $\mathrm{Kern}(f) = M'$. f ist surjektiv
$\Rightarrow$ Kurze exakte Folge $0 \to M' \to M \xrightarrow{f} R \to 0$
Sei nun $N \subset M$ ein Untermodul. Dann gibt es eine weitere kurze exakte Folge: $0 \to M' \cap N \to \underbrace{M \cap N}_{=N} \to f(N) \to 0$

$f(N) \subset R \Rightarrow f(N) = 0$ oder frei vom Rang 1. Wie im Beweis von 5.14 gibt es eine Abbildung $f(N) \to N$ sodaß

$$N = \underbrace{M' \cap N}_{\substack{\text{nach Ind:}\\ \text{frei, Rang} \leq n-1}} \oplus \underbrace{f(N)}_{\text{frei, Rang} \leq 1} \quad \Rightarrow N \text{ frei vom Rang} \leq n. \qquad \square$$

Ein endlich erzeugter Modul M ist von der Form
$$M = R^a/U \text{ mit } U = R^b,\ b \le a.$$
R^a hat eine Basis aus a Elementen, U eine aus b Elementen. Wir können aber nicht erwarten, daß wir eine Basis von U zu einer Basis von R^a fortsetzen können.

Beispiel: $R = \mathbb{Z}$, Basis 1 (oder -1), $U = 2\mathbb{Z}$, Basis 2 (oder -2)
$\rightsquigarrow$ keine Fortsetzung möglich.

Andererseits ist das Beispiel nicht so schlecht: R/U ist leicht zu bestimmen, weil die Basis von U aus Vielfachen von Basisvektoren von R besteht.
Überraschung: man kann die Basis von R^a immer so wählen, daß U von Vielfachen der Basisvektoren erzeugt ist.

5.16 Theorem (Elementarteilersatz): Sei F ~~M~~ ein freier R-Modul mit ~~Basis~~ Rang $n \in \mathbb{N}$ und U ein Untermodul von F. Dann existiert eine R-Basis $v_1, v_2, \dots, v_n$ von F und es existieren $a_1, a_2, \dots, a_n \in R$ so daß
$$U = \sum_{i=1}^{n} R a_i v_i \text{ und } a_1 | a_2 | \dots | a_n.$$

($a_1, a_2, \dots, a_n$ heißen Elementarteiler. 0 ist hier erlaubt, die $a_i v_i$ müssen nicht linear unabhängig sein – der Rang von U kann ja viel kleiner sein als n. Später wird noch gezeigt: Die Hauptideale $Ra_1, \dots, Ra_n$ sind hier sogar eindeutig bestimmt.)

welcher Satz aus der linearen Algebra wird hier verallgemeinert?

5.17 Korollar: Sei M $\neq 0$ ein endlich erzeugter R-Modul. Dann existieren Elemente $a_1, \dots, a_m \in R$, die nicht invertierbar sind, so daß
$$M = R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle \oplus \dots \oplus R/\langle a_m \rangle$$
$$\text{und } a_1 | a_2 | \dots | a_m.$$

welcher Satz aus linearer Algebra könnte hier drinstecken?

5.17 ist noch nicht die endgültige Lösung des Klassifikationsproblems – M könnte ja auch $R/\langle b_1 \rangle \oplus \dots \oplus R/\langle b_2 \rangle$ sein, für $\ell \neq m$, b's verschieden von a's.

Zurück zur linearen Algebra: $R=K$ ein Körper, F ein n-dimensionaler K-Vektorraum, U ein Unterraum. 5.16 sagt: $\exists$ Basis $v_1,\dots,v_n$ von F, $a_1,\dots,a_n \in R=K$: $U=\sum K a_i v_i$, $a_1 | a_2 | \dots | a_n$.

Das können wir aus dem Basisergänzungssatz ablesen: Wähle eine Basis $v_1,\dots,v_e$ von U und ergänze durch $v_{e+1},\dots,v_n$ zu Basis von V. und die a_i's?

Oder in Matrizen: Bezüglich Basen von U und V können wir die Inklusion $U \hookrightarrow V$ durch eine Matrix beschreiben und diese in ?-Normalform bringen $\rightsquigarrow$ das liefert 5.16 wie?

(Für Matrizen über Hauptidealringen redet man von der Smith-Normalform.)

5.17 könnte für $R=K$ die Aussage sein, daß ein endlich-dimensionaler Vektorraum isomorph zu K^m für ein m ist.

Beweis von Korollar 5.17: Sei $M \neq 0$ ein endlich erzeugter R-Modul.

Dann $\exists n \in \mathbb{N}$ und $\varphi: R^n \to M$ surjektiver Modulhomomorphismus, also kurze exakte Folge $0 \to U = \mathrm{Kern}(\varphi) \to R^n \to M \to 0$

Nach 5.16 gibt es eine Basis von R^n: $v_1,\dots,v_n$, und Elemente von R: $b_1,\dots,b_n$ so daß $U = \bigoplus_{i=1}^n R b_i v_i$ warum direkte Summe?

$$\Rightarrow M \cong R^n/U \cong \bigoplus_{i=1}^n \begin{array}{ccc} \underbrace{Rv_i/Rb_iv_i} & \ni & r\cdot v_i + Rb_iv_i \\ \uparrow \cong & & \updownarrow \\ R/\langle b_i\rangle & \ni & r + \langle b_i\rangle \end{array}$$

nachprüfen: Modulhomomorphismus bijektiv

$$\Rightarrow M \cong \bigoplus_{i=1}^n R/\langle b_i\rangle$$

Aber manche Summanden können 0 sein. Welche?

$R/\langle b_i\rangle = 0 \Leftrightarrow R = \langle b_i\rangle \overset{\text{warum}}{\Leftrightarrow} b_i$ invertierbar (d.h. Einheit) in R

Diese Summanden lassen wir weg.

Eine Einheit teilt jedes Element und jeder Teiler einer Einheit ist selbst eine Einheit warum $\Rightarrow \exists j$: $b_1,\dots,b_j$ sind Einheiten, $b_{j+1},\dots,b_n$ nicht.

Wir setzen also $a_1 := b_{j+1}, \dots, a_m := b_n$ mit $m = n-j$. was bedeutet $j=n$?

$\square$

Beweis von Theorem 5.16: Falls $U=0$: nichts zu zeigen, wähle alle $a_i=0$.
Induktion nach $n=$ Rang von F, U sei $\neq 0$:
Sei $F^* := \mathrm{Hom}_R(F,R)$, die R-Modulhomomorphismen von F nach R
(für $R=\mathbb{C}$ ist das der Dualraum). Das ist eine abelsche Gruppe und sogar
ein R-Modul durch $(r\varphi): F \to R$

$x \mapsto r\varphi(x)$

wo wird hier verwendet, daß R kommutativ ist?

Sei $\psi \in F^*$, $\psi: F \to R$. U Teilmodul von $F \Rightarrow \psi(U)$ Teilmodul von R.
R (und F und U) sind noethersch, also gibt es unter den Teilmoduln $\psi(U)$
ein bezüglich Inklusion maximales Element, dazu $\exists\, \varphi_1 \in F^*$: $\varphi_1(U)$ ist maximal.
$\varphi_1(U)$ ist ein Ideal in R, also ein Hauptideal: $\exists\, a_1 \in R$ mit $\varphi_1(U) = Ra_1$
und $\exists\, x_1 \in U$: $\varphi_1(x_1) = a_1$. $\quad a_1 \neq 0$ da $U \neq 0$

wie sieht man an dem Satz, daß wir a_1 so wählen sollten?

Behauptung (*): $\forall\, \psi \in F^*$: $\psi(x_1) \in Ra_1$
Beweis: $\psi(x_1) \in R$, $\psi(x_1)$ erzeugt Hauptideal $R\psi(x_1)$. Die Summe von zwei
Idealen ist wieder ein Ideal $\Rightarrow R\psi(x_1) + \underset{R\varphi_1(x_1)}{\underset{\shortparallel}{Ra_1}}$ ist ein Hauptideal $=: Ra$ für
ein $a \in R$.

$a \in Ra = R\psi(x_1) + Ra_1 \Rightarrow \exists\, b, c \in R$: $a = \underbrace{b\psi(x_1) + c\varphi_1(x_1)}_{=(b\psi + c\varphi_1)(x_1)}$
$b\psi + c\varphi_1$ ist auch in F^* und
erfüllt $(b\psi + c\varphi_1)(U) \supset Ra \supset Ra_1$
Ra_1 ist maximal $\Rightarrow Ra_1 = Ra \Rightarrow \psi(x_1) \in Ra = Ra_1$, wie behauptet. $\Rightarrow$ (*)

Wir wissen noch nichts über die gesuchte Basis von F. Deshalb wählen wir
zunächst irgendeine Basis: $w_1, \dots, w_n$ ($n=$ Rang liegt fest).
x_1 muß eine Linearkombination sein: $\exists\, c_i \in R$: $x_1 = \sum_{i=1}^{n} c_i w_i$.
Wir suchen nun ein $v_1 \in F$ so daß $a_1 v_1 = x_1 \in U$ (und danach wenden wir
Induktion an, um $v_2, \dots, v_n$ zu bestimmen).
Dazu wenden wir (*) auf Projektionsabbildungen $F \cong R^n \to R$ an

$$p_j: F \to R, \quad \sum_{i=1}^{n} d_i w_i \mapsto d_j \qquad (\text{für festes } j) \qquad p_j \in F^* \overset{(*)}{\Rightarrow} p_j(x_1) \in Ra_1$$

Wegen $x_1 = \sum_{i=1}^n c_i w_i$ ist $p_j(x_1) = c_j$. $\Rightarrow$ alle $c_j \in Ra_1$, lauter Vielfache von a_1

$\Rightarrow \exists c_1', \dots, c_n' \in R : c_j = a_1 c_j'$ für $j = 1, \dots, n$

Sei nun $v_1 := \sum_{i=1}^n c_i' w_i \Rightarrow a_1 v_1 = \sum_{i=1}^n \underbrace{a_1 c_i'}_{c_i} w_i = x_1 \Rightarrow$

Wir haben v_1 gefunden mit $x_1 = a_1 v_1$.

Was ist $\varphi_1(v_1)$? x_1 war so gewählt, daß $\underbrace{\varphi_1(x_1)}_{\parallel} = a_1$

Kürzungsregel in $R \Rightarrow \varphi_1(v_1) = 1$ $\qquad \varphi_1(a_1 v_1) = a_1 \varphi_1(v_1)$

$\varphi_1 : F \to R$ ist also surjektiv.

Damit bekommen wir eine kurze exakte Folge

$$(**) \quad 0 \to \mathrm{Kern}(\varphi_1) \to F \xrightarrow{\varphi_1} R \to 0$$

$\exists \alpha : a \mapsto a v_1$

und eine Abbildung $\alpha : R \to F$ mit

$\varphi_1 \circ \alpha = id_R$, denn $1 \overset{\alpha}{\longmapsto} v_1 \overset{\varphi_1}{\longmapsto} 1$

Basis von R

Wie oben folgt:

$F \simeq R \oplus \mathrm{Kern}(\varphi_1)$ bzw $F = \underbrace{Rv_1}_{= \mathrm{Im}(\alpha)} \oplus \mathrm{Kern}(\varphi_1)$, v_1 passt also gut in eine Basis von F.
(***)

Können wir U passend zerlegen?

Wir können in (**) F und $\mathrm{Kern}(\varphi_1)$ und Rv_1 mit U schneiden und erhalten die kurze exakte Folge $0 \to U \cap \mathrm{Kern}(\varphi_1) \to U \xrightarrow{\varphi_1} \varphi_1(U) \to 0$

$U \cap F$ $\qquad \varphi_1(U) = Ra_1$ (siehe Anfang des Beweises)

$\alpha : a_1 \mapsto a_1 v_1$

$a a_1 \mapsto a a_1 v_1$

$\Rightarrow U = U \cap \mathrm{Kern}(\varphi_1) \oplus Ra_1 v_1$ nachprüfen

$\mathrm{Kern}(\varphi_1) \subset F$ ist ein freier Modul.

Wegen $F = Rv_1 \oplus \mathrm{Kern}(\varphi_1)$ ist $\mathrm{Kern}(\varphi_1)$ frei vom Rang $n-1$.

($Ra_1 v_1 \neq 0$ weil $a_1 \neq 0$, also hat $Ra_1 v_1$ Rang 1.)

Auf $\mathrm{Kern}(\varphi_1)$ und seinen Teilmodul $U \cap \mathrm{Kern}(\varphi_1)$ können wir Induktion anwenden und erhalten eine Basis $v_2, \dots, v_n$ von $\mathrm{Kern}(\varphi_1)$ und $a_2, \dots, a_n \in R$ mit $U \cap \mathrm{Kern}(\varphi_1) = \sum_{i=2}^n Ra_i v_i$ und $a_2 | \dots | a_n$. (***) $\Rightarrow v_1, v_2, \dots, v_n$ ist eine Basis von F.

das ist ein Modulhomom

Noch zz: $a_1 | a_2$. Sei $\tau : F \to R$ mit $\sum_{i=1}^n b_i v_i \mapsto b_1 + b_2$, dann ist $\tau(U) = Ra_1 + Ra_2$, und $Ra_1 + Ra_2 \supset Ra_1$. Aber Ra_1 war maximal unter allen Bildern von U in R
$\Rightarrow Ra_1 = Ra_1 + Ra_2 \Rightarrow Ra_2 \subset Ra_1 \Rightarrow a_1 | a_2$. $\square$

Wenn wir einen Modul wie in 5.17 zerlegen:

$$M \simeq R/\langle a_1\rangle \oplus \dots \oplus R/\langle a_m\rangle \text{ mit } a_1 | a_2 | \dots | a_m$$

können etwa $a_e = \dots = a_m = 0$ sein und die anderen nicht.
Dann sind $R/\langle 0\rangle \oplus \dots \oplus R/\langle 0\rangle \simeq R^{m-e+1}$ die freien Summanden.
Laut 5.14 ist der Rest eindeutig bis auf Isomorphie.
Aber wie trennt man den freien Anteil vom Rest (oder umgekehrt), wenn man M und seine Elemente kennt, aber nicht die Zerlegung?
Wie unterscheiden sich $\mathbb{Z} \oplus \mathbb{Z}$ und $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$?
Sei $a \in \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$, dann gilt $35 \cdot a = 0$. Für $b \in \mathbb{Z}\oplus\mathbb{Z}$, $b \neq 0$ ist dagegen $nb \neq 0$ $\forall n \in \mathbb{Z}-\{0\}$.
Diese Eigenschaft formalisieren und verwenden wir.

5.18 Definition: Sei R ein Integritätsbereich und M ein R-Modul. M heißt
torsionsfrei $:\Leftrightarrow [\forall a \in R\ \forall x \in M: ax = 0 \Rightarrow a = 0 \text{ oder } x = 0]$
Sei N ein R-Modul. Ein Element $x \in N$ heißt Torsionselement $:\Leftrightarrow \exists a \in R$, $a \neq 0$ und $ax = 0$.
Die Menge $T(N) := \{x \in N : x \text{ Torsionselement}\}$ heißt Torsionsuntermodul von N.   Ist die Bezeichnung berechtigt?
N ist ein Torsionsmodul $:\Leftrightarrow N = T(N)$
M torsionsfrei $\Leftrightarrow T(M) = 0$

R ist wieder Hauptidealring

5.19 Proposition: (a) Sei M ein endlich erzeugter R-Modul. Dann existiert ein freier Untermodul $F \subset M$ mit $M = T(M) \oplus F$.
(b) Sei M ein endlich erzeugter R-Modul. Dann gilt: M frei $\Leftrightarrow$ M torsionsfrei.
Beweis: (a) Nach 5.17 hat M eine Zerlegung $M = \bigoplus_{i=1}^m M_i$, $M_i \cong R/\langle a_i\rangle$.
$F := \bigoplus_{a_i=0} M_i$ ist frei, da solche $M_i \simeq R$, das frei ist. z.z. $\bigoplus_{a_i\neq 0} M_i = T(M)$
Sei $m \in M_i \cong R/\langle a_i\rangle \Rightarrow a_i \cdot m = 0$
$\Rightarrow \bigoplus_{a_i\neq 0} M_i \subset T(M)$. Sei $(x,y) \in F \oplus (\bigoplus_{a_i\neq 0} M_i)$ ein Torsionselement: $\underbrace{a(x,y)}_{=(ax,ay)} = 0$, $a \neq 0$
$\Rightarrow ax = 0 \Rightarrow a = 0$ oder $x = 0$
$\Rightarrow T(M) \subset \bigoplus_{a_i\neq 0} M_i$, also Gleichheit

(b) M endlich erzeugt frei $\Rightarrow M \cong R^n$ für ein $n \Rightarrow M$ torsionsfrei

Umgekehrt: M endlich erzeugt torsionsfrei $\Rightarrow T(M) = 0 \overset{(a)}{\Rightarrow} M$ frei □

Daß ein Element ein Torsionselement ist, kann man ihm direkt ansehen. Aber die Elemente des freien Anteils kann man nicht so leicht einsammeln, der freie Anteil F in $M = T(M) \oplus F$ ist auch nicht eindeutig bestimmt. In $\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ ist das Element $(1,1)$ nicht Torsion, aber es liegt auch nicht in dem gewählten freien Anteil.

Nach 5.17 können wir einen endlich erzeugten Modul M zerlegen in

$$M = R/\langle a_1\rangle \oplus R/\langle a_2\rangle \oplus \dots \oplus R/\langle a_m\rangle \quad \text{mit } a_1 | a_2 | \dots | a_m$$

Rist faktoriell $\Rightarrow$ wir können $a_1, a_2, \dots, a_m$ in Produkte von Primelementen zerlegen. Zwei Primelemente p und q können assoziiert sein, in $\mathbb{Z}$: $p = \pm q$, allgemein: $p = u \cdot q$, u Einheit; äquivalent dazu: $\langle p\rangle = \langle q\rangle$, dasselbe Ideal. Sei P ein Repräsentantensystem der Klassen assoziierter Primelemente, in $\mathbb{Z}$ z.B. $P = \{$positive Primzahlen$\}$

Ein Hauptidealring muß nicht euklidisch sein, aber auch ohne euklidischen Algorithmus gilt: $\forall r, s \geq 0$: für p und q nicht assoziiert ist $Rp^s + Rq^r = R$.

Denn: $Rp^s + Rq^r$ ist ein Ideal, also ein Hauptideal

$$\Rightarrow \exists a: \; Rp^s + Rq^r = Ra$$

$$\Rightarrow Rp^s \subset Ra, \text{ also } a | p^s \text{ und } Rq^r \subset Ra, \text{ also } a | q^r$$

warum?

$$\Rightarrow a \text{ Einheit}$$

Anders gesagt: Rp^s und Rq^r sind teilerfremde Ideale.

Ein beliebiges Element $b \in R$, $b \neq 0$ können wir schreiben als

$$b = u\, p_1^{r_1} \cdots p_m^{r_m} \quad (u \text{ Einheit}, p_1, \dots, p_m \text{ prim}, r_1, \dots, r_m > 0, m > 0, \text{ falls } b \text{ keine Einheit ist})$$

$$\Rightarrow R/\langle b\rangle = R/\langle \prod p_i^{r_i}\rangle \xrightarrow{\sim} R/\langle p_1^{r_1}\rangle \times R/\langle p_2^{r_2}\rangle \times \dots \times R/\langle p_m^{r_m}\rangle$$

oder $\oplus$

("chinesischer Restsatz")

warum ist das ein Isomorphismus von R-Moduln

$$x + \langle b\rangle \longmapsto (x + \langle p_1^{r_1}\rangle, x + \langle p_2^{r_2}\rangle, \dots, x + \langle p_m^{r_m}\rangle)$$

(Das ist sogar ein Ringisomorphismus. $R \to R/\langle p_i^{r_i}\rangle$ ist ein Ringhomomorphismus mit Kern $\langle p_i^{r_i}\rangle$, $R \to R/\langle p_1^{r_1}\rangle \times \ldots \times R/\langle p_m^{r_m}\rangle$ hat Kern $\bigcap_i \langle p_i^{r_i}\rangle = \langle \prod p_i^{r_i}\rangle$.)
Wenn wir $a_1 | a_2 | \ldots | a_m$ in Primfaktoren zerlegen und die freien Summanden von M nicht vergessen (die zu $a_j = 0$ gehören), ergibt sich der erste Teil von:

5.20 Theorem: Sei M ein endlich erzeugter R-Modul. Dann existieren $n(0) \in \mathbb{N}_0$ und $n(p,r) \in \mathbb{N}_0$ für $p \in P$, $r \in \mathbb{N}$, fast alle $n(p,r) = 0$, so daß

$$M \simeq R^{n(0)} \oplus \bigoplus_{p \in P} \bigoplus_{r \geq 0} \left(R/\langle p^r\rangle\right)^{n(p,r)}$$

Dabei gilt: Die Moduln R und $R/\langle p^r\rangle$ sind unzerlegbar (und jeder unzerlegbare R-Modul ist isomorph zu R oder zu einem $R/\langle p^r\rangle$). Diese Moduln sind paarweise nicht-isomorph.
Die Zahlen $n(0)$ und $n(p,r)$ sind durch M eindeutig bestimmt.

Das Theorem gibt also eine Klassifikation aller unzerlegbaren Moduln bis auf Isomorphie und eine ~~eindeutige~~ Zerlegung der zerlegbaren Moduln in direkte Summen von unzerlegbaren Moduln, wobei der Isomorphietyp und die Vielfachheit der Summanden eindeutig bestimmt ist.

Die Zerlegung in 5.20 haben wir schon hergeleitet. Die weiteren Behauptungen folgen aus den folgenden Lemmata:

5.21 Lemma: $R/\langle p^r\rangle$ und R sind unzerlegbar

Beweis: Daß R (Integritätsbereich) unzerlegbar ist, wissen wir schon.
Um $R/\langle p^r\rangle$ als unzerlegbar nachzuweisen, betrachten wir die Teilmoduln.
$R \to R/\langle p^r\rangle$ ist ein surjektiver Ringhomomorphismus $\Rightarrow$ die Urbilder der Ideale in $R/\langle p^r\rangle$ sind die Ideale I in R mit $I \supset \langle p^r\rangle$.

$I = Ra$ Hauptideal, a erfüllt $a | p^r$

R faktoriell $\Rightarrow$ für a kommt nur p^s in Frage mit $s \leq r$.

$\Rightarrow$ die Ideale von $R/\langle p^r\rangle$ und damit auch die R-Teilmoduln sind von der Form $\langle p^s\rangle/\langle p^r\rangle$ ~~für~~ mit $0 \le s \le r$. Diese sind ineinander enthalten:

$$R/\langle p^r\rangle = \langle p^0\rangle/\langle p^r\rangle \supset \langle p^1\rangle/\langle p^r\rangle \supset \langle p^2\rangle/\langle p^r\rangle \supset \ldots \supset \langle p^{r-1}\rangle/\langle p^r\rangle \supset \langle p^r\rangle/\langle p^r\rangle = 0$$

Der Durchschnitt von zwei Teilmoduln ist also einer von den beiden $\Rightarrow$ $R/\langle p^r\rangle$ kann nicht in $\underset{\neq 0}{M_1} \oplus \underset{\neq 0}{M_2}$ zerlegt werden $\Rightarrow$ $R/\langle p^r\rangle$ ist unzerlegbar. $\square$

In Hauptidealringen sind $\underset{\neq 0}{\text{Primideale}}$ maximal (Algebra 1.14) $\Rightarrow$ Für $p \in P$ ist $R/\langle p\rangle$ ein Körper.

Wenn M ein R-Modul ist, dann ist $pM = \underbrace{\langle p\rangle}_{\text{Ideal}} M$ ein Teilmodul und M/pM ist ein $R/\langle p\rangle$-Modul, also ein Vektorraum. Warum?

Genauso ist $p^d M/p^{d+1}M$ ein $R/\langle p\rangle$-Vektorraum.

Das betrachten wir genauer für zwei Fälle: $M = R/\langle p^r\rangle$ und $M = R/\langle q^s\rangle$, $q \neq p$:

<u>5.22 Lemma:</u> Sei $p \in P$

(a) $\forall n \in \mathbb{N}$: $\dim_{R/\langle p\rangle} (p^n R/p^{n+1}R) = 1$.

(b) Sei $M = R/\langle p^r\rangle$ $(r \in \mathbb{N}) \Rightarrow \dim_{R/\langle p\rangle}(p^n M/p^{n+1}M) = \begin{cases} 1 & \text{für } n < r \\ 0 & \text{für } \ge r \end{cases}$

(c) Sei $N = R/\langle q^r\rangle$ $(r \in \mathbb{N}, q \in P \setminus \{p\}) \Rightarrow$

$$\forall n \in \mathbb{N}: \dim_{R/\langle p\rangle} (p^n N/p^{n+1} N) = 0.$$

(Der Vergleich von (b) und (c) sagt uns, daß wir M und N unterscheiden können.)

Beweis: ~~(a)~~ In allen Fällen sei $\pi: R \to M$ die Restklassenabbildung, in (a) ist also $\pi = id: R \to R$. Dann ist $M = R\pi(1)$, $p^n M = R p^n \pi(1)$.

$\Rightarrow p^n M/p^{n+1}M$ wird von $p^n \pi(1)$ erzeugt, als $R/\langle p\rangle$-Vektorraum

$\Rightarrow$ die Dimension kann nur 0 oder 1 sein

(a) Primfaktorzerlegung in R ist eindeutig $\Rightarrow Rp^n \neq Rp^{n+1} \Rightarrow$ (a).

Für $n<r$ folgt (b) aus (a). Für $n \geq r$ ist $p^n M = 0$.

(c) Für $q \in P \setminus \{p\}$ ist $Rp^n + Rq^s = R$.

$\Rightarrow \underbrace{p^n N}_{Rp^n N} = (Rp^n + Rq^r) N = RN = N$, also $p^n N = N \; \forall n$

$\uparrow$ denn: $q^r N = 0$ $\qquad \Rightarrow p^n N = p^{n+1} N$ □

5.23 Lemma: Die Zahlen $n(0)$ und $n(p,r)$ sind durch M eindeutig bestimmt.

Beweis: $M \simeq \underbrace{R^{n(0)}}_{\text{freier Teil}} \oplus \underbrace{T(M)}_{\text{Torsionsteil (eindeutig)}} \Rightarrow R^{n(0)} \cong M/T(M) \Rightarrow n(0)$ eindeutig bestimmt

Für $M = M_1 \oplus \dots \oplus M_s$ ist $p^n M = p^n M_1 \oplus \dots \oplus p^n M_s$

$p^{n+1} M = p^{n+1} M_1 \oplus \dots \oplus p^{n+1} M_s$

$$\Rightarrow p^n M / p^{n+1} M \simeq \frac{p^n M_1}{p^{n+1} M_1} \oplus \dots \oplus \frac{p^n M_s}{p^{n+1} M_s}$$

$\overset{5.22}{\Rightarrow}$ für $p \in P, n \in \mathbb{N}$: $\dim_{R/\langle p \rangle} (p^n M / p^{n+1} M) = n(0) + \sum_{r=n+1}^{\infty} n(p,r) \Rightarrow$ die Differenz zweier solcher Dimensionen bestimmt $n(p,r)$ eindeutig □

Wir können auch $T(M)$ in „p-Anteile" zerlegen, wobei p durch P läuft.

Für $p \in P$ sei $T_p(M) := \{x \in M : \exists n \in \mathbb{N}$ so daß $p^n x = 0\}$

$T_p(M)$ ist ein Teilmodul von M

$T_p(R) = 0$, $T_p(R/\langle p^r \rangle) = R/\langle p^r \rangle$

$T_p(M_1 \oplus \dots \oplus M_s) = T_p(M_1) \oplus \dots \oplus T_p(M_s)$

$q \in P \setminus \{p\} \Rightarrow T_p(R/\langle q^r \rangle) = 0$ für $r > 0$: Sei $p^n x = 0$ für $x \in R/\langle q^r \rangle \Rightarrow$

$0 = (Rp^n + Rq^r) x = Rx$, also $x = 0$

In der Zerlegung von M in 5.20 ist $T_p(M)$ die $\underbrace{\text{Summe aller } M_i = R/\langle q_i^{r_i} \rangle}_{\text{In der Notation von 5.20: } p \text{ fest, } \bigoplus_{r>0} (R/\langle p^r \rangle)^{n(p,r)}}$ mit $q_i = p$ und $T(M) = \bigoplus_{p \in P} T_p(M)$.

Damit ist der Klassifikationssatz 5.20 bewiesen.

Wir müssen aber noch nachprüfen, daß auch in 5.16 und 5.17 Eindeutigkeit vorliegt:

<u>5.24 Proposition:</u> In Theorem 5.16 sind die Hauptideale Ra_i durch F und U eindeutig bestimmt. Im Korollar 5.17 sind die Hauptideale Ra_i durch M eindeutig bestimmt.

(Die Elementarteiler in 5.16 sind deshalb bis auf Einheiten eindeutig bestimmt.)

Beweis: Zuerst 5.17: $\underset{\neq 0}{a_1} | \ldots | \underset{\neq 0}{a_t} | a_{t+1} = 0 | \ldots | a_m = 0$ für geeignetes t

$\Rightarrow T(M) = \bigoplus_{i \leq t} R/\langle a_i \rangle$, $M/T(M) \simeq R^{m-t}$

$\Rightarrow$ $m-t$ ist durch M bestimmt, da der Rang eines freien Moduls eindeutig bestimmt ist.

Für $i \leq 0$ ist $a_i = u_i \prod_{p \in P} p^{s(i,p)}$ Primfaktorzerlegung mit u_i Einheit

$T(M) \simeq \bigoplus_{i=1}^{t} R/\langle a_i \rangle \simeq \bigoplus_{i=1}^{t} \bigoplus_{p \in P} R/\langle p^{s(i,p)} \rangle$. In der Zerlegung in 5.20 sind die Vielfachheiten $n(p,r)$ eindeutig, zu den Exponenten r von p. $n(p,r)$ ist genau die Anzahl der i, für die $s(i,p) = r$ ist.

Wegen $a_1 | a_2 | \ldots$ gilt $s(1,p) \leq s(2,p) \leq \ldots \leq s(t,p)$ folgt, daß die $n(p,r)$ die $s(i,p)$ bestimmen. genauer?

$\Rightarrow$ die a_i sind eindeutig festgelegt (die a_i sind keine Einheiten, haben also Primteiler p).

$\Rightarrow$ die Ra_i in 5.17 sind durch M festgelegt.

In 5.16 sind F und U gegeben. Wählt man $M = F/U$ in 5.17, folgt die Eindeutigkeit der Ra_i, deren a_i keine Einheit ist.

a_i Einheit bedeutet $Ra_i = R$, die Anzahl dieser Summanden ist die Differenz Rang von F minus Anzahl der Summanden von F/U. □

5.16 und 5.24 können wir auf Bilder R-linearer Abbildungen (R-Modulhomomorphismen) zwischen freien Moduln von endlichem Rang anwenden:

5.25 Proposition: Seien F_1 und F_2 freie R-Moduln, Rang $(F_1) = s$ und Rang $(F_2) = t$, und $f \neq 0$: $F_1 \to F_2$ ein Homomorphismus von R-Moduln. Dann gibt es eine Basis $x_1, \dots, x_s$ von F_1 und eine Basis $y_1, \dots, y_t$ von F_2, eine ganze Zahl $r \leq \min\{s,t\}$ und Elemente $a_1, a_2, \dots, a_r \in R$ mit $a_1 \mid a_2 \mid \dots \mid a_r$, alle $\neq 0$, so daß

$$f(x_i) = \begin{cases} a_i y_i & \text{für } 1 \leq i \leq r \\ 0 & \text{für } i > r \end{cases}$$

Die Zahl r und die Ideale Ra_i sind durch f eindeutig festgelegt.

Beweis: $f(F_1)$ ist ein Teilmodul von F_2 $\overset{5.16/5.24}{\Longrightarrow}$ $\exists$ Basis $y_1, \dots, y_t$ von F_2 und $a_1, a_2, \dots, a_t \in R$ mit $a_1 \mid a_2 \mid \dots \mid a_t$ und $f(F_1) = \sum_{i=1}^{t} Ra_i y_i$. Außerdem $\exists r \leq t$ mit $a_i = 0$ für $i > r$ und $a_i \neq 0$ für $i \leq r$.

$f(F_1)$ ist frei vom Rang r und hat Basis $a_1 y_1, \dots, a_r y_r$.

$f: F_1 \to f(F_1)$ ist surjektiv und wir können die Basis von $f(F_1)$ abbilden durch $g: f(F_1) \to F_1$ mit $a_i y_i \overset{g}{\longmapsto} x_i$, so daß $f \circ g = \mathrm{id}_{f(F_1)}$. D.h. x_i's sind Urbilder.

Das Bild $g(f(F_1))$ hat Basis $x_1, \dots, x_r$ und $F_1 = \underset{\mathrm{Im}(g)}{\underbrace{g(f(F_1))}} \oplus \mathrm{Kern}(f)$.

$x_1, \dots, x_r$ kann man durch $x_{r+1}, \dots, x_s$ zu einer Basis von F_1 ergänzen. $\square$

Details?

Im nächsten Kapitel folgen Anwendungen der Modultheorie von Hauptidealringen.