

§1.6 Endlich erzeugte Moduln über Hauptidealringen

Definition 1.6.1. Sei R ein Integritätsring. Dann heißt eine Funktion $\delta: R \rightarrow \mathbb{N}_0$ eine *euklidische Funktion* auf R , wenn es für alle $a \in R$ und $b \in R \setminus \{0\}$ Elemente $q \in R$ („Quotient“) und $r \in R$ („Rest“) gibt mit $a = bq + r$ und $\delta(r) < \delta(b)$ („Division mit Rest“). Es heißt R *euklidisch*, wenn R eine euklidische Funktion besitzt.

Beispiel 1.6.2. (a) \mathbb{Z} ist euklidisch mit euklidischer Funktion $\delta: \mathbb{Z} \rightarrow \mathbb{N}_0, a \mapsto |a|$.

(b) Ist K ein Körper, so ist $K[X]$ euklidisch mit euklidischer Funktion

$$\delta: K[X] \rightarrow \mathbb{N}_0, p \mapsto \begin{cases} 0 & \text{falls } p = 0, \\ 1 + \deg p & \text{falls } p \neq 0. \end{cases}$$

(c) Der Ring der Gaußschen Zahlen [Johann Friedrich Gauß *1777 †1855]

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

ist euklidisch mit euklidischer Funktion $\delta: \mathbb{Z}[i] \rightarrow \mathbb{N}_0, z \mapsto |z|^2$, denn zu $a \in \mathbb{Z}[i]$ und $b \in \mathbb{Z}[i] \setminus \{0\}$ gibt es $q \in \mathbb{Z}[i]$ mit $|\frac{a}{b} - q|^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$ und für $r := a - bq$ gilt $\delta(r) = |r|^2 = |\frac{a}{b} - q|^2 |b|^2 \leq \frac{1}{2} \delta(b) < \delta(b)$.

Proposition 1.6.3. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R ein Integritätsring und $\delta: R \rightarrow \mathbb{N}_0$ eine euklidische Funktion. Sei I ein Ideal in $R, \mathbb{C} I \neq (0)$. Wähle $a \in I \setminus \{0\}$ mit kleinstmöglichem $\delta(a)$. Wir zeigen $I = (a)$. Sei hierzu $x \in I$. Zu zeigen: $x \in (a)$. Schreibe $x = aq + r$ mit $q, r \in R$ und $\delta(r) < \delta(a)$. Dann $r = x - aq \in I$ und folglich $r = 0$ gemäß Wahl von a . Also $x = aq \in (a)$. \square

Notation 1.6.4. Sei R ein Hauptidealring. Dann fixieren wir oft stillschweigend eine Menge \mathbb{P}_R von irreduziblen Elementen von R derart, dass jedes irreduzible Element von R zu genau einem Element von \mathbb{P}_R assoziiert ist, zum Beispiel $\mathbb{P}_{\mathbb{Z}} := \mathbb{P} := \{2, 3, 5, 7, 11, 13, 17, \dots\}$ und $\mathbb{P}_{K[X]} := \{p \in K[X] \mid p \text{ normiert und irreduzibel}\}$ (K Körper). Betrachte

$$N_R := \{0\} \cup \left\{ \prod_{i=1}^n p_i \mid n \in \mathbb{N}_0, p_1, \dots, p_n \in \mathbb{P} \right\},$$

zum Beispiel $N_{\mathbb{Z}} = \mathbb{N}_0$ und

$$N_{K[X]} = \{p \in K[X] \mid p = 0 \text{ oder } p \text{ normiert}\} \quad (K \text{ Körper}).$$

Da R faktoriell ist, ist jedes Element von R zu genau einem Element von N_R assoziiert.

Definition 1.6.5. Sei R ein Integritätsring und M ein R -Modul. Dann bildet die Menge der Torsionselemente von M [\rightarrow 1.2.4] einen Untermodul

$$T(M) := \{x \in M \mid \exists a \in R \setminus \{0\} : ax = 0\}$$

von M , den wir den *Torsionsteil* nennen.

Lemma 1.6.6. Sei R ein Hauptidealring.

(a) Seien $k, k' \in \mathbb{N}_0$ und $a_1, \dots, a_k, a'_1, \dots, a'_{k'} \in R \setminus \{0\}$ mit $a_1 | a_2 | \dots | a_k, a'_1 | a'_2 | \dots | a'_{k'}$ und

$$\prod_{i=1}^k R/a_i R \cong \prod_{i=1}^{k'} R/a'_i R.$$

Dann gilt $k = k'$ und $a_i = a'_i$ für alle $i \in \{1, \dots, k\}$.

(b) Seien $\ell, n, \ell', n' \in \mathbb{N}_0$ und $(p_1, k_1), \dots, (p_\ell, k_\ell), (p'_1, k'_1), \dots, (p'_{\ell'}, k'_{\ell'}) \in \mathbb{P}_R \times \mathbb{N}$ mit

$$\left(\prod_{i=1}^{\ell} R/p_i^{k_i} R \right) \times R^n \cong \left(\prod_{i=1}^{\ell'} R/p'_i^{k'_i} R \right) \times R^{n'}.$$

Dann gilt $\ell = \ell', n = n'$ und es gibt ein $\sigma \in S_\ell$ mit $(p_i, k_i) = (p'_{\sigma(i)}, k'_{\sigma(i)})$ für alle $i \in \{1, \dots, \ell\}$.

Beweis. (b) Indem man auf beiden Seiten der Isomorphie den Torsionsteil und den Quotienten nach dem Torsionsteil nimmt, erhält man $\prod_{i=1}^{\ell} R/p_i^{k_i} R \cong \prod_{i=1}^{\ell'} R/(p'_i)^{k'_i} R$ und $R^n \cong R^{n'}$. Aus der zweiten Isomorphie folgt $n = \text{rk}(R^n) = \text{rk}(R^{n'}) = n'$ mit 1.2.13. In der ersten Isomorphie sind alle Faktoren nach 1.5.4 unzerlegbar (wie auch in der zweiten Isomorphie) und nach 1.4.17(b) von endlicher Länge (anders als möglicherweise in der ersten Isomorphie!), weshalb wir darauf den Satz von Krull-Remak-Schmidt 1.5.13 anwenden können. Es gilt also $\ell = \ell'$ und es gibt $\sigma \in S_\ell$ mit $R/p_i^{k_i} R \cong R/(p'_{\sigma(i)})^{k'_{\sigma(i)}} R$ für alle $i \in \{1, \dots, \ell\}$. Da zwei isomorphe Moduln offenbar denselben Annihilator [\rightarrow 1.4.15] haben, folgt daraus mit 1.4.16, dass $p_i^{k_i} R = (p'_{\sigma(i)})^{k'_{\sigma(i)}} R$ für alle $i \in \{1, \dots, \ell\}$. Da R als Hauptidealring insbesondere faktoriell ist, folgt $(p_i, k_i) = (p'_{\sigma(i)}, k'_{\sigma(i)})$ für alle $i \in \{1, \dots, \ell\}$.

(a) Indem man die a_i mit $a_i \neq 0$ und die a'_i mit $a'_i \neq 0$ in Produkte von Potenzen von paarweise verschiedenen Primfaktoren zerlegt, kann man mit dem Chinesischen Restsatz [\rightarrow A2.8.6] (vgl. Beweis von 1.5.4) die Isomorphie aus (a) wie in (b) schreiben. Weil (b) schon bewiesen ist, gilt dabei

$$k_{=0} := \#\{i \in \{1, \dots, k\} \mid a_i = 0\} = n = n' = \#\{i \in \{1, \dots, k'\} \mid a'_i = 0\} =: k'_{=0}.$$

Als nächstes zeigen wir

$$k_{\neq 0} := \#\{i \in \{1, \dots, k\} \mid a_i \neq 0\} = \#\{i \in \{1, \dots, k'\} \mid a'_i \neq 0\} =: k'_{\neq 0}.$$

Wegen $a_i \neq 1 \neq a'_i$ gilt $k_{\neq 0} = 0 \iff \ell = 0 \iff \ell' = 0 \iff k'_{\neq 0} = 0$, denn $\ell = \ell'$ nach (b). Daher kann man $k_{\neq 0} > 0$ und $k'_{\neq 0} > 0$ voraussetzen. Wieder wegen $a_i \neq 1 \neq a'_i$, wegen der „Teilerkettenvoraussetzung“ und wegen (b) gilt dann

$$\begin{aligned} k_{\neq 0} &= \max\{\#\{j \in \{1, \dots, \ell\} \mid p_j = p_i\} \mid i \in \{1, \dots, \ell\}\} \\ &= \max\{\#\{j \in \{1, \dots, \ell'\} \mid p'_j = p'_i\} \mid i \in \{1, \dots, \ell'\}\} = k'_{\neq 0}. \end{aligned}$$

Es folgt $k = k_{=0} + k_{\neq 0} = k'_{=0} + k'_{\neq 0} = k'$. Schließlich gilt für $i \in \{1, \dots, k_{\neq 0}\}$, für $p \in \mathbb{P}_R$ und $\alpha \in \mathbb{N}$ wieder wegen der „Teilerkettenvoraussetzung“ und wegen (b), dass

$$\begin{aligned} p^\alpha | a_i &\iff \#\{i \in \{1, \dots, \ell\} \mid p_i = p, k_i \geq \alpha\} \geq \#\{i, \dots, k_{\neq 0}\} \\ &\iff \#\{i \in \{1, \dots, \ell'\} \mid p'_i = p, k'_i \geq \alpha\} \geq \#\{i, \dots, k'_{\neq 0}\} \iff p^\alpha | a'_i. \end{aligned}$$

Daraus folgt $a_i = a'_i$ für alle $i \in \{1, \dots, k_{\neq 0}\}$. Wegen $a_i = 0 = a'_i$ für alle $i \in \{k_{\neq 0} + 1, \dots, k\}$ ist damit alles gezeigt. \square

Satz 1.6.7. Sei R ein Hauptidealring und M ein freier R -Modul von endlichem Rang [→1.2.13]. Sei N ein Untermodul von M . Dann ist N frei mit $\text{rk } N \leq \text{rk } M$.

Beweis. Wir führen Induktion nach $n := \text{rk } M \in \mathbb{N}_0$. Für $n = 0$ ist nichts zu zeigen. Sei nun $n > 0$ und gelte die Aussage bereits für alle Moduln vom Rang $n - 1$. Wähle eine Basis x_1, \dots, x_n von M . Der Untermodul $L := \sum_{i=1}^{n-1} Rx_i$ ist frei vom Rang $n - 1$. Betrachte den R -Modulhomomorphismus

$$f: M \rightarrow R, \quad \sum_{i=1}^n a_i x_i \mapsto a_n \quad (a_i \in R).$$

Dann induziert die kurze exakte Folge

$$0 \longrightarrow L \longrightarrow M \xrightarrow{f} R \longrightarrow 0$$

eine weitere kurze exakte Folge

$$0 \longrightarrow L \cap N \longrightarrow N \xrightarrow{f|_N} f(N) \longrightarrow 0.$$

Nun ist aber $f(N)$ ein Hauptideal in R und damit ein freier R -Modul vom Rang 0 oder 1. Nach Aufgabe 4(a) auf Übungsblatt 4 zerfällt diese Sequenz. Mit Bedingung (iii) von Aufgabe 1(f) auf Übungsblatt 3 folgt insbesondere

$$N \cong (L \cap N) \times f(N).$$

Nach Induktionsvoraussetzung ist $L \cap N$ frei vom Rang $\leq n - 1$. Daher ist $(L \cap N) \times f(N)$ und damit auch N frei vom Rang $\leq (n - 1) + 1 = n$. \square

Definition und Übung 1.6.8. [\rightarrow 1.5.6, \rightarrow LA 7.1.6] Sei R ein kommutativer Ring und M und N R -Moduln. Dann bildet

$$\text{Hom}(M, N) := \{f \mid f: M \rightarrow N \text{ Homomorphismus}\}$$

einen Untermodul des R -Moduls N^M . Man nennt $M^* := \text{Hom}(M, R)$ den zu M dualen Modul und seine Elemente Linearformen auf M .

Satz und Definition 1.6.9 (Elementarteilersatz). Sei R ein Hauptidealring, M ein freier R -Modul vom Rang $n \in \mathbb{N}_0$ [\rightarrow 1.2.13] und N ein Untermodul von M . Dann gibt es eine Basis x_1, \dots, x_n von M und $a_1, \dots, a_n \in N_R$ mit $N = \sum_{i=1}^n Ra_i x_i$ und $a_1 \mid a_2 \mid \dots \mid a_n$. Dabei sind die a_1, \dots, a_n durch das Paar (M, N) eindeutig bestimmt und man nennt sie die Elementarteiler von N in M .

Beweis. Zunächst zur Eindeutigkeit: Sind x_1, \dots, x_n und a_1, \dots, a_n wie angegeben, so gilt

$$M/N = \bigoplus_{i=1}^n Rx_i / \bigoplus_{i=1}^n Ra_i x_i \cong R^n / \prod_{i=1}^n a_i R \cong \prod_{i=1}^n (R/a_i R) \cong \prod_{i=n-k+1}^n (R/a_i R)$$

mit $k := \#\{i \in \{1, \dots, n\} \mid a_i \neq 1\}$. Nach Lemma 1.6.6(a) sind k und a_{n-k+1}, \dots, a_n eindeutig bestimmt. Schließlich gilt $a_1 = \dots = a_{n-k} = 1$.

Nun zur Existenz: Wir führen Induktion nach n . Für $n = 0$ ist nichts zu zeigen. Sei also nun $n \in \mathbb{N}$ und die Behauptung bereits für alle Moduln vom Rang $\leq n - 1$ gezeigt. Ist $N = 0$, so können wir eine beliebige Basis von M nehmen und $a_i := 0$ für alle i nehmen. Sei nun $N \neq 0$. Die Menge

$$\mathcal{I} := \{\varphi(N) \mid \varphi \in M^*\}$$

von Idealen von R besitzt wegen $N \neq 0$ Elemente $\neq (0)$, wie man mit 1.2.5(c) leicht sieht. Da R als Hauptidealring noethersch ist, besitzt \mathcal{I} mindestens ein maximales Element. Wähle $a_1 \in N_R \setminus \{0\}$ derart, dass (a_1) maximal in \mathcal{I} ist. Wähle dazu $\varphi_1 \in M^*$ und $y_1 \in N$ mit $\varphi_1(y_1) = a_1$.

Hilfsbehauptung: $\psi(y_1) \in (a_1)$ für alle $\psi \in M^*$

Begründung: Sei $\psi \in M^*$. Wähle $a \in R$ mit $(a) = (\psi(y_1), a_1) = (\psi(y_1), \varphi_1(y_1))$. Wähle $b, b_1 \in R$ mit $a = b\psi(y_1) + b_1\varphi_1(y_1) = (b\psi + b_1\varphi_1)(y_1)$. Es folgt $(a_1) \subseteq (a) \subseteq (b\psi + b_1\varphi_1)(N) \in \mathcal{I}$. Wegen der Maximalität von (a_1) in \mathcal{I} , muss $(a_1) = (a)$ gelten und damit $\psi(y_1) \in (a) = (a_1)$.

Wir nehmen nun kurzzeitig eine beliebige Basis z_1, \dots, z_n von M zur Hilfe. Es gibt $c_1, \dots, c_n \in R$ mit $y_1 = \sum_{i=1}^n c_i z_i$. Wendet man die Hilfsbehauptung für jedes $j \in \{1, \dots, n\}$ an auf die Linearform $M \rightarrow R, \sum_{i=1}^n d_i z_i \mapsto d_j$ ($d_i \in R$) an, so erhält man $a_1 \mid c_i$ für alle $i \in \{1, \dots, n\}$. Daher gibt es $c'_i \in R$ mit $c_i = a_1 c'_i$. Setze $x_1 := \sum_{i=1}^n c'_i z_i$.

Wir haben also $x_1 \in M$ gefunden mit $a_1 x_1 = y_1 \in N$. Aus $\varphi_1(y_1) = a_1$ folgt nun $\varphi_1(x_1) = 1$, denn $a_1 \neq 0$. Daher spaltet die Abbildung $R \rightarrow M, a \mapsto ax_1$ ($a \in R$) die kurze exakte Folge

$$0 \longrightarrow \ker \varphi_1 \longrightarrow M \xrightarrow{\varphi_1} R \longrightarrow 0$$

und es gilt (siehe Aufgabe 4(b) auf Übungsblatt 4)

$$M = Rx_1 \oplus \ker \varphi_1. \quad (*)$$

Ebenso spaltet $a_1R \rightarrow N$, $aa_1 \mapsto ay_1 = aa_1x_1$ ($a \in R$) die kurze exakte Folge

$$0 \longrightarrow N \cap \ker \varphi_1 \longrightarrow N \xrightarrow{\varphi_1|_N} a_1R \longrightarrow 0$$

und es gilt

$$N = Ra_1x_1 \oplus (N \cap \ker \varphi_1). \quad (**)$$

Nach Satz 1.6.7 ist $\ker \varphi_1$ ein freier R -Modul. Aus (*) folgt $\text{rk}(\ker \varphi_1) = n - 1$, wobei zu beachten ist, dass $x_1 \neq 0$ (was natürlich aus $y_1 \neq 0$ also letztlich aus $a_1 \neq 0$ folgt). Die Induktionsvoraussetzung liefert nun eine Basis x_2, \dots, x_n von $\ker \varphi_1$ sowie $a_2, \dots, a_n \in N_R$ mit $N \cap \ker \varphi_1 = \sum_{i=2}^n Ra_ix_i$ und $a_2 | \dots | a_n$. Aus (**) folgt nun $N = \sum_{i=1}^n Ra_ix_i$. Wegen (*) ist x_1, \dots, x_n eine Basis von M . Es bleibt damit nur noch $a_1 | a_2$ zu zeigen sofern $n \geq 2$.

Sei also $n \geq 2$ und betrachte die Linearform

$$\varphi: M \rightarrow R, \quad \sum_{i=1}^n b_ix_i \mapsto b_1 + b_2 \quad (b_i \in R).$$

Es gilt $(a_1) \subseteq (a_1, a_2) = \varphi(N) \in \mathcal{S}$. Aus der Maximalität von (a_1) in \mathcal{S} folgt $(a_1) = (a_1, a_2)$, also $a_1 | a_2$. \square

Korollar 1.6.10 (Smithsche Normalform von Homomorphismen). [Henry John Stephen Smith *1826 †1883] Sei R ein Hauptidealring. Sei N ein freier R -Modul vom Rang $n \in \mathbb{N}_0$, M ein freier R -Modul vom Rang $m \in \mathbb{N}_0$ und $f: N \rightarrow M$ ein Homomorphismus. Dann gibt es ein eindeutig bestimmtes $r \in \{0, \dots, \min\{m, n\}\}$ und eindeutig bestimmte $a_1, \dots, a_r \in N_R \setminus \{0\}$ mit $a_1 | a_2 | \dots | a_r$, für die gilt: Es gibt Basen y_1, \dots, y_n von N und x_1, \dots, x_m von M mit

$$f(y_i) = \begin{cases} a_ix_i & \text{für alle } i \in \{1, \dots, r\} \text{ und} \\ 0 & \text{für alle } i \in \{r+1, \dots, n\}. \end{cases}$$

Beweis. Die Eindeutigkeit folgt sofort aus der Eindeutigkeitsaussage des Elementarteilersatzes, denn offenbar sind

$$a_1, \dots, a_r, \underbrace{0, \dots, 0}_{m-r \text{ mal}}$$

zwangsläufig die Elementarteiler des Bildes von f in M .

Zur Existenz: Wähle mit dem Elementarteilersatz eine Basis x_1, \dots, x_m von M und $a_1, \dots, a_m \in N_R$ mit $\text{im } f = \sum_{i=1}^m Ra_ix_i$ und $a_1 | \dots | a_m$. Dann gibt es $r \in \{0, \dots, m\}$ mit $a_1, \dots, a_r \in N_R \setminus \{0\}$ und $a_{r+1} = \dots = a_m = 0$. Es ist dann a_1x_1, \dots, a_rx_r eine Basis von

im f , denn a_1x_1, \dots, a_rx_r sind linear unabhängig, weil R ein Integritätsring ist. Weil im f nach Satz 1.6.7 frei ist, zerfällt die kurze exakte Sequenz

$$0 \longrightarrow \ker f \longrightarrow N \xrightarrow{f} \operatorname{im} f \longrightarrow 0$$

wegen Aufgabe 4(a) auf Übungsblatt 4. Gemäß Bedingung (ii) in Aufgabe 1(f) auf dem Übungsblatt 3 gibt es einen Homomorphismus $g: \operatorname{im} f \rightarrow N$, welcher diese Sequenz spaltet, das heißt $f \circ g = \operatorname{id}_{\operatorname{im} f}$ (insbesondere ist g injektiv). Nach Aufgabe 4(b) auf dem Übungsblatt 4 gilt dann $N = \ker f \oplus \operatorname{im} g$. Setze $y_i := g(a_ix_i)$ für alle $i \in \{1, \dots, r\}$. Weil $g: \operatorname{im} f \rightarrow \operatorname{im} g$ ein Isomorphismus ist, bilden y_1, \dots, y_r eine Basis von $\operatorname{im} g$. Nach Satz 1.6.7 gilt insbesondere $r \leq n$, also $r \leq \min\{m, n\}$. Weil auch $\ker f$ nach Satz 1.6.7 frei ist und weil $N = \ker f \oplus \operatorname{im} g$ gilt, können wir y_1, \dots, y_r mit einer Basis y_{r+1}, \dots, y_n von $\ker f$ zu einer Basis y_1, \dots, y_n von N ergänzen. Schließlich gilt $f(y_i) = f(g(a_ix_i)) = a_ix_i$ für $i \in \{1, \dots, r\}$ und $f(y_i) = 0$ für $i \in \{r+1, \dots, n\}$. \square

Korollar 1.6.11 (Struktursatz für endlich erzeugte Moduln über Hauptidealringen). *Sei R ein Hauptidealring und M ein endlich erzeugter R -Modul. Dann gibt es eindeutig bestimmte*

(a) $k \in \mathbb{N}_0$ und $a_1, \dots, a_k \in N_R \setminus \{1\}$ mit $a_1 | a_2 | \dots | a_k$ und

$$M \cong \prod_{i=1}^k R/a_iR.$$

(b) $\ell, n \in \mathbb{N}_0$ und bis auf Reihenfolge eindeutige $(p_1, k_1), \dots, (p_\ell, k_\ell) \in \mathbb{P}_R \times \mathbb{N}$ mit

$$M \cong \left(\prod_{i=1}^{\ell} R/p_i^{k_i}R \right) \times R^n.$$

Beweis. Die Eindeutigkeit wurde in Lemma 1.6.6 schon bewiesen. Die Existenzaussage in (b) erhält man aus der Existenzaussage in (a) mit dem Chinesischen Restsatz wie in den ersten Zeilen des Beweises von Lemma 1.6.6(a). Schließlich zeigen wir die Existenzaussage in (a): Da M endlich erzeugt ist, findet man ein $n \in \mathbb{N}$ und einen Epimorphismus $R^n \rightarrow M$. Mit dem Isomorphiesatz findet man einen Untermodul N von R^n derart, dass $M \cong R^n/N$. Jetzt schaut man die Elementarteiler von N in R^n an und argumentiert genau wie im Beweis der Eindeutigkeitsaussage des Elementarteilersatzes 1.6.9. \square

Korollar 1.6.12. *Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem direkten Produkt endlich vieler zyklischer Gruppen.*

Korollar 1.6.13. *Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt von zyklischen Gruppen von Primzahlpotenzordnung.*

Bemerkung 1.6.14. Sei R ein Hauptidealring. Aus 1.5.4 und dem Struktursatz 1.6.11 folgt, dass die endlich erzeugten unzerlegbaren R -Moduln bis auf Isomorphie genau R und die $R/(p^k)$ mit $p \in \mathbb{P}_R$ und $k \in \mathbb{N}$ sind. Könnte man das ohne Benutzung des Struktursatzes zeigen, dann wäre die Existenzaussage in Teil (b) des Struktursatzes eine direkte Konsequenz aus Satz 1.5.5, denn endlich erzeugte R -Moduln sind nach 1.4.7 noethersch.