1. Quotientenringe, Quotientenmoduln und Lokalisierung

Sei A ein kommutativer Ring mit 1.

Definition 1.1. Sei S eine multiplikativ abgesclossene Teilmenge von A. Auf dem kartesischen Produkt $A \times S$ betrachten wir die Relation "$\sim$" :

$$A \times S \ni (a_1, s_1) \sim (a_2, s_2) \in A \times S \Longleftrightarrow (\exists\, t,\ t \in S : t\, a_2\, s_1 = t\, a_1\, s_2)\,.$$

Es ist leicht nachzuprüfen, daß "$\sim$" in der Tat eine Äquivalenzrelation ist. (Mit $\dfrac{a}{s}$ bezeichnen wir die Äquivalenzklasse von $(a, s) \in A \times S$). Auf

$$\boxed{S^{-1}A := A \times S \;/ \sim}$$

definiert man Addition und Multiplikation:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}\ .$$

Hiermit wird $S^{-1}A$ zu einem Ring, den sog. *Quotientenring von A nach der Nennermenge S.*

Bemerkung. (i) $\frac{0}{1} = \frac{0}{s}$ (für jedes $s \in S$) ist das neutrale Element von $S^{-1}A$ und $\frac{-a}{s}$ das inverse Element von $\frac{a}{s}$ bzgl. der Addition. $\frac{1}{1} = \frac{s}{s}$ (für jedes $s \in S$) ist das neutrale Element von $S^{-1}A$ bzgl. der Multiplikation.

(ii) Die Abbildung

$$\iota_{A,S} : A \longrightarrow S^{-1}A, \quad a \longmapsto \frac{a}{1}$$

ist offensichtlich ein Ringhomomorphismus. Witerhin gilt:

(a) $\iota_{A,S}$ ist injektiv$\Longleftrightarrow$ S besteht aus lauter Nichtnullteilern.

(b) Ist $S \subset A^*$, so ist $\iota_{A,S}$ ein Ringisomorphismus.

(c) Ist A ein Integritätsbereich und $S = A \smallsetminus \{0\}$, so ist $S^{-1}A = \mathrm{Quot}(A)$ der Quotientenkörper von A und $\iota_{A,S}$ injektiv. (Beispiel: $\mathbb{Z} \hookrightarrow \mathbb{Q}$).

Definition 1.2. Ist $\mathfrak{p}$ ein Primideal in A und $S := A \smallsetminus \mathfrak{p}$, so heißt

$$\boxed{A_{\mathfrak{p}} := S^{-1}A}$$

die *Lokalisierung* von A in $\mathfrak{p}$. Bei Problemstellungen, die sich auf ein einziges Primideal $\mathfrak{p}$ beziehen, ist es oft günstig, von A zur Lokalisierung $A_{\mathfrak{p}}$ überzugehen. Sie vergißt alles, was nichts mit $\mathfrak{p}$ zu tun hat und bringt dafür die auf $\mathfrak{p}$ bezogenen Eigenschaften klarer heraus. (Zum Beispiel ist die Zuordnung $\mathfrak{q} \longmapsto \mathfrak{q}\, A_{\mathfrak{p}}$ eine 1-1 Korrespondenz zwischen den Primidealen $\mathfrak{q} \subset \mathfrak{p}$ und den Primidealen von $A_{\mathfrak{p}}$).

Beispiel. Sei $V \subset \mathbb{A}^n_K$ eine irreduzible affine K-Varietät mit Koordinatenring

$$K\,[V] := K\,[X_1, \ldots, X_n] \;\; / \; \mathbb{J}\,(V)\ .$$

Wir haben schon gezeigt, daß es einen Ringisomorphismus

$$\varphi : K\,[V] \xrightarrow{\cong} \mathcal{O}\,(V) := \left\{ \begin{array}{c} \text{Ring der regulären} \\ \text{Funktionen auf } V \end{array} \right\}$$

gibt. φ induziert für jeden Punkt $P \in V$ einen Monomorphismus

$$K[V]_{\mathfrak{m}_{V,P}} \hookrightarrow \mathcal{O}_{V,P}$$

(s. 1.9(iii)), der eigentlich einen Isomorphismus bildet. Hierbei ist $\mathfrak{m}_P$ das (eindeutige) maximale Ideal des lokalen Ringes von P auf V, d.h.

$$\mathfrak{m}_{V,P} = \left\{\overline{f} \in K[V] : f(P) = 0\right\} \subset \mathcal{O}_{V,P} \ .$$

Der Körper

$$\mathsf{k}(P) := \mathcal{O}_{V,P}/\mathfrak{m}_{V,P}$$

wird oft *Residuenklassenkörper* von V im Punkte P genannt.

Beispiel. Sei $V \subset \mathbb{P}_K^n$ eine irreduzible projektive K-Varietät mit homogenem Koordinatenring $K[V]$ (K algebraisch abgeschlossen). Wir haben schon gezeigt, daß $\mathcal{O}(V) \cong K$. Ist $\mathfrak{m}_{V,P} \subset K[V]$ das Ideal, das von der Menge der homogenen Elemente $\overline{f} \in K[V]$ mit $f(P) = 0$ erzeugt wird, so ist $\mathfrak{m}_{V,P}$ das maximale Ideal zu dem lokalen Ring $\mathcal{O}_{V,P}$ und es gilt:

$$\mathcal{O}_{V,P} \cong K[V]_{\mathfrak{m}_{V,P}} \qquad \text{und} \qquad K[V]_{(\{0\})} \cong K(V) \ .$$

Lemma 1.3. *Sei A ein kommutativer Ring mit 1 und*

$$A^* := \{a \in A \mid \exists b,\ b \in A : ab = 1\}$$

die Menge der Einheiten in A. Dann gilt:

(i) $A^* = A \smallsetminus \bigcup \{\mathfrak{m} \mid \mathfrak{m} \text{ maximales Ideal von } A\}$,

(ii) $A \smallsetminus A^*$ *bildet genau dann ein Ideal von A, wenn A genau ein maximales Ideal besitzt.*

Beweis. (i) "$\subset$": Sei $a \in A^*$ und $b \in A$ derart, daß $ab = 1$. Gäbe es ein maximales Ideal $\mathfrak{m}$ von A mit $a \in \mathfrak{m}$, so wäre auch $1 = ab \in \mathfrak{m}$, im Widerspruch zu $\mathfrak{m} \neq A$.

"$\supset$": Sei $a \in A \smallsetminus \bigcup \{\mathfrak{m} \mid \mathfrak{m} \text{ maximales Ideal von } A\}$. Dann ist $Aa \nsubseteq \mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$ von A. Da jedes echte Ideal von A in einem maximalen Ideal von A enthalten ist, gilt $Aa = A$, woraus die Behauptung folgt.

(ii) Sei $\mathfrak{n}$ ein maximales Ideal von A. Da $\mathfrak{n} \subset A \smallsetminus A^*$ und $A \smallsetminus A^*$ ein Ideal ist, folgt $\mathfrak{n} = A \smallsetminus A^*$. Die Umkehrung ergibt sich aus (i). □

Proposition 1.4. *Sei $\mathfrak{p}$ ein Primideal von A. Dann ist $A_{\mathfrak{p}}$ ein lokaler Ring mit dem maximalen Ideal*

$$\boxed{\mathfrak{p} A_{\mathfrak{p}} := \left\{\tfrac{p}{s} \mid p \in \mathfrak{p},\ s \in A \smallsetminus \mathfrak{p}\right\}}$$

($\mathfrak{p} A_{\mathfrak{p}}$ ist das von $\iota_{A, A \smallsetminus \mathfrak{p}}(\mathfrak{p})$ in $A_{\mathfrak{p}}$ erzeugte Ideal und $A_{\mathfrak{p}} / \mathfrak{p} A_{\mathfrak{p}} \cong \mathrm{Quot}(A / \mathfrak{p})$).

Beweis. Daß $\mathfrak{p} A_{\mathfrak{p}}$ in der Tat ein Ideal von $A_{\mathfrak{p}}$ ist, verifiziert man folgendermaßen: Sei $\frac{a}{t} \in A_{\mathfrak{p}}$ und $\frac{p_1}{s_1}, \frac{p_2}{s_2} \in \mathfrak{p} A_{\mathfrak{p}}$. Dann ist

$$\frac{a}{t} \cdot \frac{p_1}{s_1} = \frac{a p_1}{t s_1} \quad \text{mit} \quad a p_1 \in \mathfrak{p}, \quad t s_1 \in S,$$

und

$$\frac{p_1}{s_1} + \frac{p_2}{s_2} = \frac{p_1 s_2 + p_2 s_1}{s_1 s_2} \quad \text{mit} \quad s_1, s_2 \in S, \quad p_1 s_2 + p_2 s_1 \in \mathfrak{p} \; .$$

Um zu beweisen, daß $\mathfrak{p}\, A_{\mathfrak{p}}$ das eindeutige maximale Ideal von $A_{\mathfrak{p}}$ ist, genügt es nach Lemma 1.3, zu zeigen: $\mathfrak{p}\, A_{\mathfrak{p}}$ besteht aus allen Nichteinheiten von $A_{\mathfrak{p}}$. Sei $\frac{a}{s}$ eine Einheit in $A_{\mathfrak{p}}$, d.h. es gebe $\frac{a'}{s'} \in A_{\mathfrak{p}}$, so daß $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{1}{1}$. Dann gibt es ein $t \in A \smallsetminus \mathfrak{p}$ mit

$$taa' = tss' \in A \smallsetminus \mathfrak{p}$$

also $a \in A \smallsetminus \mathfrak{p}$, da $\mathfrak{p}$ ein Ideal ist und sonst $taa' \in \mathfrak{p}$ gälte. Wir haben deswegen gezeigt:

$$(A_{\mathfrak{p}})^* \subset A_{\mathfrak{p}} \smallsetminus \mathfrak{p}\, A_{\mathfrak{p}} \; .$$

Die umgekehrte Inklusion "$\supset$" ist klar, denn aus $\frac{a}{s} \in A_{\mathfrak{p}} \smallsetminus \mathfrak{p}\, A_{\mathfrak{p}}$ folgt, daß $a, s \notin \mathfrak{p}$, somit $\frac{a}{1}, \frac{1}{s} \in (A_{\mathfrak{p}})^*$ und deswegen $\frac{a}{s} \in (A_{\mathfrak{p}})^*$. □

Beispiel. $A = \mathbb{Z}$, $\mathfrak{p} = \mathbb{Z}p$, p Primzahl. Dann ist

$$\mathbb{Z}_{\mathfrak{p}} = \mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \quad \text{und} \quad p \nmid n \right\}, \quad \mathfrak{p}\, \mathbb{Z}_{\mathfrak{p}} = \left\{ \frac{m}{n} \in \mathbb{Z}_{(p)} \mid m \in \mathbb{Z}p \right\} \; .$$

Definition 1.5. Falls I ein Ideal von A und S eine multiplikativ abgeschlossene Teilmenge von A ist, setzten wir

$$\boxed{S^{-1}I := \left\{ \tfrac{a}{s} \mid a \in I \quad \text{und} \quad s \in S \right\}}$$

Proposition 1.6. (i) *$S^{-1}I$ ist ein Ideal von $S^{-1}A$. Wenn $I \cap S \neq \varnothing$, folgt $S^{-1}I = S^{-1}A$.*

(ii) *Sei J ein Ideal von $S^{-1}A$ und $I := \iota_{A,S}^{-1}(J)$. Dann ist $J = S^{-1}I$. Insbesondere hat jedes Primideal von $S^{-1}A$ die Form $S^{-1}\mathfrak{p}$, wobei $\mathfrak{p}$ ein Primideal von A ist.*

(iii) *Wenn $\mathfrak{p}$ ein Primideal von A ist mit $\mathfrak{p} \cap S = \varnothing$, dann ist $S^{-1}\mathfrak{p}$ ein Primideal von $S^{-1}A$.*

(iv) *Wenn $\mathfrak{p}$ ein Primideal von A ist mit $\mathfrak{p} \cap S = \varnothing$, dann gilt: $\iota_{A,S}^{-1}\left(S^{-1}\mathfrak{p}\right) = \mathfrak{p}$.*

Beweis. (i) Daß $S^{-1}I$ ein Ideal ist, zeigt man wie im Beweis von 1.4 für $\mathfrak{p}\, A_{\mathfrak{p}}$. Falls $I \cap S \neq \varnothing$, enthält $S^{-1}I$ eine Einheit des Ringes $S^{-1}A$.

(ii) "$\supset$": Für ein beliebiges Element $\frac{b}{s} \in J$ gilt:

$$\frac{b}{s} \in J \Longrightarrow \frac{b}{1} = \frac{s}{1} \cdot \frac{b}{s} \in J \Longrightarrow b \in I \Longrightarrow \frac{b}{s} \in S^{-1}I \, .$$

Die Inklusion "$\subset$" ist klar, denn $\iota_{A,S}$ induziert eine Einbettung von $A/\iota_{A,S}^{-1}(J)$ in den Integritätsring $\left(S^{-1}A\right)/J$.

(iii) Seien $\frac{a_1}{s_1}, \frac{a_2}{s_2} \in S^{-1}A$ mit $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in S^{-1}\mathfrak{p}$. Dann ist

$$\frac{a_1 a_2}{s_1 s_2} = \frac{p}{s_3} \quad \text{für ein } p \in \mathfrak{p}, \; s_3 \in S \; .$$

Daher gibt es ein $t \in S$ mit $ts_3 a_1 a_2 = ts_1 s_2 p \in \mathfrak{p}$, und wegen t, $s_3 \notin \mathfrak{p}$ gilt:

$$(\text{entweder} \quad a_1 \in \mathfrak{p} \quad \text{oder} \quad a_2 \in \mathfrak{p}) \Longrightarrow \left(\text{entweder} \quad \frac{a_1}{s_1} \in S^{-1}\mathfrak{p} \quad \text{oder} \quad \frac{a_2}{s_2} \in S^{-1}\mathfrak{p} \right),$$

woraus die Behauptung folgt.
(iv) "$\supset$" ist klar. Zu "$\subset$": Sei $x \in A$ mit $\iota_{A,S}^{-1}(x) \in S^{-1}\mathfrak{p}$. Dann ist $\frac{x}{1} = \frac{p}{s}$ für gewisse $p \in \mathfrak{p}$ und $s \in S$. Aus diesem Grund gibt es ein $t \in S$ mit $tsx = p$. Daraus ergibt sich $x \in \mathfrak{p}$, da $st \in S$ und deshalb ist $st \notin \mathfrak{p}$. $\square$

Definition 1.7. Sei S eine multiplikativ abgeschlossene Teilmenge von A und M ein A-Modul. Auf dem kartesischen Produkt $M \times S$ betrachten wir die Relation "$\sim$" :

$$M \times S \ni (m_1, s_1) \sim (m_2, s_2) \in M \times S \Longleftrightarrow (\exists\, t,\ t \in S : t\, m_2\, s_1 = t\, m_1\, s_2).$$

Es ist leicht zu beweisen, daß auch diese "$\sim$" eine Äquivalenzrelation ist. (Mit $\dfrac{m}{s}$ bezeichnen wir die Äquivalenzklasse von $(m, s) \in M \times S$). Man kann

$$\boxed{S^{-1}M := M \times S \,/ \sim}$$

vermöge

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}, \qquad \frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$$

als einen $S^{-1}A$-Modul, den sog. *Quotientenmodul von M nach der Nennermenge S*, auffassen. Analog definiert man die Abbildung $\iota_{M,S} : M \longrightarrow S^{-1}M$, und für Primideale $\mathfrak{p}$ von A den $A_{\mathfrak{p}}$-Modul $M_{\mathfrak{p}}$. ($S^{-1}M$ ist natürlich durch $\iota_{A,S} : A \longrightarrow S^{-1}A$ auch ein A-Modul).

Definition 1.8. Sei M ein A-Modul. Ein Element $a \in A$ wird *Nullteiler bezüglich M* genannt, wenn es ein $m \in M \setminus \{0\}$ so gibt, daß $am = 0$. Weiterhin setzen wir: $\mathrm{NT}(M) := \{\text{alle Nullteiler bezüglich } M\}$.

Die wichtigsten Eigenschaften der Quotientenmoduln werden in der folgenden Proposition zusammengefaßt.

Proposition 1.9. *Seien $M, N, L, \{M_i, i \in I\}$ A-Moduln und S eine multiplikativ abgeschlossene Teilmenge von A. Dann gilt:*
(i) $S^{-1}\left(\bigoplus_{i\in I} M_i\right) \cong \bigoplus_{i \in I} S^{-1}M_i$.
(ii) $\iota_{M,S} : M \longrightarrow S^{-1}M$ *ist injektiv* $\Longleftrightarrow$ *S besteht aus lauter Nichtnullteilern bzgl. M.*
(iii) *Sei $\varphi : M \to N$ A-linear. Dann gibt es genau eine $S^{-1}A$-lineare Abbildung $S^{-1}\varphi : S^{-1}M \to S^{-1}N$, so daß das Diagramm*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \iota_{M,S}\downarrow & \circlearrowright & \downarrow \iota_{N,S} \\ S^{-1}M & \xrightarrow[S^{-1}\varphi]{} & S^{-1}N \end{array}$$

kommutativ wird. (Außerdem, falls $\varphi : M \to N$, $\psi : N \to L$ A-linear sind, gilt: $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi$).
(iv) *Ist*

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} L$$

eine exakte Folge von A-Modulhomomorphismen, so ist auch

$$S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}N \xrightarrow{S^{-1}\psi} S^{-1}L$$

exakt.

(v) *Wenn U ein A-Untermodul von M ist, so kann man auf kanonische Weise $S^{-1}U$ als $S^{-1}A$-Untermodul von $S^{-1}M$ auffassen. Man hat dann einen kanonischen Isomorphismus*

$$S^{-1}(M/U) \cong S^{-1}M \ / \ S^{-1}U \ .$$

(vi) *Jeder $S^{-1}A$-Untermodul N von $S^{-1}M$ ist von der Form $S^{-1}U$, wobei U ein A-Untermodul von M ist.*

(vii) *Sind N_1, N_2 Untermoduln von M, so gilt:*

$$S^{-1}(N_1 \cap N_2) = \left(S^{-1}N_1\right) \cap \left(S^{-1}N_2\right) \subset S^{-1}M \ .$$

(viii) *Wenn M ein* endlich erzeugter (bzw. Noetherscher) *A-Modul ist, so ist $S^{-1}M$ ein* endlich erzeugter (bzw. Noetherscher) *$S^{-1}A$-Modul. Insbesonder ist $S^{-1}A$ ein* Noetherscher *Ring, wenn A ein solcher ist.*

Beweis. (i) Leichte Übung.

(ii) $\iota_{M,S}(m) = \frac{m}{1} = 0 \Longleftrightarrow (\exists\, t,\ t \in S : t\,m = 0)$. Da t Nichtnullteiler für M ist, folgt $m = 0$.

(iii) Zum Beweis setze man $S^{-1}\varphi\left(\frac{m}{s}\right) := \frac{\varphi(m)}{s}$ für alle $\frac{m}{s} \in S^{-1}M$. Wegen der Forderung der $S^{-1}A$-Linearität und der Kommutativität des Diagramms muß in der Tat gelten:

$$\begin{aligned} S^{-1}\varphi\left(\frac{m}{s}\right) &= S^{-1}\varphi\left(\frac{1}{s}\cdot\frac{m}{1}\right) = \frac{1}{s}S^{-1}\varphi\left(\frac{m}{1}\right) = \frac{1}{s}\left(S^{-1}\varphi\circ\iota_{M,S}\right)(m) = \\ &= \frac{1}{s}\left(\iota_{N,S}\circ\varphi\right)(m) = \frac{1}{s}\cdot\frac{\varphi(m)}{1} = \frac{\varphi(m)}{s} \,. \end{aligned}$$

Ferner ist die obige Abbildung $S^{-1}\varphi$ wohldefiniert: Ist $(m,s) \sim (m',s')$, so gibt es ein $t \in S$ mit $ts'm = tsm'$, also $ts'\varphi(m) = ts\varphi(m')$. Es folgt

$$S^{-1}\varphi\left(\frac{m}{s}\right) = \frac{\varphi(m)}{s} = \frac{\varphi(m')}{s'} = S^{-1}\varphi\left(\frac{m'}{s'}\right) \ .$$

Schließlich ist $S^{-1}\varphi$ eine A-lineare Abbildung, weil

$$\frac{a}{s'}\cdot S^{-1}\varphi\left(\frac{m}{s}\right) = \frac{a}{s'}\cdot\frac{\varphi(m)}{s} = \frac{a\varphi(m)}{ss'} = S^{-1}\varphi\left(\frac{am}{ss'}\right)$$

und

$$\begin{aligned} S^{-1}\varphi\left(\frac{m_1}{s_1}+\frac{m_2}{s_2}\right) &= S^{-1}\varphi\left(\frac{m_1s_2+m_2s_1}{s_1s_2}\right) = \frac{\varphi(m_1s_2+m_2s_1)}{s_1s_2} = \\ &= \frac{s_2\varphi(m_1)+s_1\varphi(m_2)}{s_1s_2} = \frac{\varphi(m_1)}{s_1}+\frac{\varphi(m_2)}{s_2} = S^{-1}\varphi\left(\frac{m_1}{s_1}\right)+S^{-1}\varphi\left(\frac{m_2}{s_2}\right) \ . \end{aligned}$$

(iv) Zuerst ist $S^{-1}\psi\circ S^{-1}\varphi = S^{-1}(\psi\circ\varphi) = S^{-1}(0) = 0$, d.h. $\mathrm{Im}\left(S^{-1}\varphi\right) \subset \mathrm{Ker}\left(S^{-1}\psi\right)$. Betrachte nun umgekehrt $\frac{m}{s} \in \mathrm{Ker}\left(S^{-1}\psi\right)$. Es existiert ein $t \in S$

mit $t\psi(m) = 0 \Longrightarrow \psi(tm) = 0$. Nach Voraussetzung gibt es ein $m' \in M$ mit $\varphi(m') = tm$. Aus diesem Grunde ist

$$S^{-1}\varphi\left(\frac{m'}{st}\right) = \frac{\varphi(m')}{ts} = \frac{tm}{st} = \frac{m}{s} \Longrightarrow \frac{m}{s} \in \operatorname{Im}\left(S^{-1}\varphi\right) .$$

(v) Man wendet (iv) auf die exakte Sequenz $0 \longrightarrow U \longrightarrow M \longrightarrow M/U \longrightarrow 0$ an.

(vi) Wähle hierfür $U = \iota_{M,S}^{-1}(N)$. Wenn $x \in U$, ist $\frac{x}{1} \in N$, also $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in N$ für jedes $s \in S$. Mithin ist $S^{-1}U \subset N$. Wenn umgekehrt $\frac{x}{s} \in N$, dann ist $\frac{x}{1} = \frac{s}{1} \cdot \frac{x}{s} \in N$, also $x \in U$ und $\frac{x}{s} \in S^{-1}U$, d.h. $S^{-1}U \supset N$.

(vii) Man wendet (iv) auf die folgende kurze exakte Sequenz an:

$$0 \longrightarrow N_1 \cap N_2 \longrightarrow N_1 \longrightarrow M/N_2 \longrightarrow 0$$

(viii) Wenn M von $m_1, \ldots, m_k$ über A erzeugt wird, so ist $\left\{\frac{m_1}{1}, \ldots, \frac{m_k}{1}\right\}$ offenbar ein Erzeugendensystem von $S^{-1}M$ über $S^{-1}A$. Daß mit M auch $S^{-1}M$ Noethersch ist, folgt aus (vi). $\square$

2. Annulatoren, Träger und assoziierte Primideale von Moduln

Definition 2.1. Sei M ein A-Modul.

$$\boxed{\operatorname{Ann}_A(M) := \{a \in A \mid am = 0, \forall m,\ m \in M\}}$$

heißt der *Annulator* von M. Für ein $m \in M$ heißt

$$\boxed{\operatorname{Ann}_A(m) := \{a \in A \mid am = 0\}}$$

der *Annulator* von m. Im Sinne dieser Definition bestehen die Nichtnullteiler von M aus

$$A \smallsetminus \bigcup_{m \in M \smallsetminus \{0\}} \operatorname{Ann}_A(m).$$

Lemma 2.2. (i) $\operatorname{Ann}_A(M)$ *und* $\operatorname{Ann}_A(m)$ *sind Ideale von* A.

(ii) *Maximale Elemente der Menge* $\{\operatorname{Ann}_A(m) \mid m \in M \smallsetminus \{0\}\}$ *sind Primideale.*

Beweis. (i) ist trivial. Zu (ii): Sei $\mathfrak{p} = Ann_A(m)$ maximal und betrachte $a, b \in A$ mit $ab \in \mathfrak{p}$, $b \notin \mathfrak{p}$. Definiere $I := Ann_A(bm)$. Für $p \in \mathfrak{p}$ gilt $p(bm) = b(pm) = 0$; somit ist $\mathfrak{p} \subset I$. Wegen der Maximalität von $\mathfrak{p}$ hat man $\mathfrak{p} = I$. Da $abm = 0$, folgt $a \in I = \mathfrak{p}$. $\square$

Definition 2.3. Definiere

$$\boxed{\operatorname{Ass}_A(M) := \left\{\mathfrak{p} \;\middle|\; \begin{array}{l} \mathfrak{p} \text{ Primideal von } A \text{ derart,} \\ \text{daß } \exists\, m,\ m \in M, \text{mit } \mathfrak{p} = \operatorname{Ann}_A(m) \end{array}\right\}}$$

Die Elemente von $\operatorname{Ass}_A(M)$ heißen *die zu* M *assoziierten Primideale.*

Lemma 2.4. (i) $Am \cong A \ / \ \mathrm{Ann}_A(m)$ (Als A-Moduln!)

(ii) *Ein Primideal* $\mathfrak{p}$ *von* A *liegt genau dann in* $\mathrm{Ass}_A(M)$, *wenn es eine injektive* A-*linerare Abbildung* $A \ / \ \mathfrak{p} \hookrightarrow M$ *gibt.*

(iii) *Ist* $\mathfrak{p}$ *ein Primideal von* A, *so ist* $A \ / \ \mathfrak{p}$ *ein* A-*Modul und* $\mathrm{Ass}_A(A \ / \ \mathfrak{p}) = \{\mathfrak{p}\}$. *Es gilt sogar* $\mathrm{Ass}_A(U) = \{\mathfrak{p}\}$ *für alle von* 0 *verschiedenen Untermoduln* U *von* $A \ / \ \mathfrak{p}$.

Beweis. (i) und (ii) sind klar. Zu (iii) merke, daß für jedes $x \in A \ / \ \mathfrak{p} \setminus \{\overline{0}\}$, man $\mathrm{Ass}_A(x) = \mathfrak{p}$ hat. $\square$

Lemma 2.5. *Sei* A *Noethersch und* M *ein* A-*Modul. Die folgenden Bedingungen sind äquivalent*:

(i) $M = 0$.

(ii) $\mathrm{Ass}_A(M) = \varnothing$.

Beweis. Die Richtung (i) $\Longrightarrow$ (ii) ist offensichtlich. Zu (ii) $\Longrightarrow$ (i): Ist $M \neq 0$, so ist die Menge

$$\mathcal{L}_M := \{\mathrm{Ann}_A(m) \ \mid m \in M \setminus \{0\}\}$$

von Idealen in A nicht leer. Da A Noethersch ist, besitzt $\mathcal{L}_M$ maximale Elemente, die nach Lemma 2.2(b) prim und deshalb Elemente von $\mathrm{Ass}_A(M)$ sind, d.h. $\mathrm{Ass}_A(M) \neq \varnothing$. $\square$

Lemma 2.6. *Sei* A *Noethersch und* M *ein* A-*Modul. Dann ist die Menge der Nullteiler bzgl.* M *die Vereinigung seiner assoziierten Primideale, d.h.*

$$\mathrm{NT}(M) = \bigcup \ \{\mathfrak{p} \ \mid \mathfrak{p} \ \text{ Primideal von } A \text{ mit } \ \mathfrak{p} \in \mathrm{Ass}_A(M)\}$$

Beweis. Für ein $\mathfrak{p} \in \mathrm{Ass}_A(M)$ mit $\mathfrak{p} = \mathrm{Ann}_A(m)$ gilt $am = 0$, also ist a ein Nullteiler bzgl. M. Andererseits, für einen Nullteiler a bzgl. M gibt es ein $m \in M \setminus \{0\}$ mit $am = 0$. Nach Lemma 2.2(ii) existiert ein $\mathfrak{p} \in \mathrm{Ass}_A(M)$ mit $\mathrm{Ann}_A(m) \subset \mathfrak{p}$. $\square$

Proposition 2.7. *Seien* $U \subset M \quad A$-*Moduln. Dann gilt*:

$$\mathrm{Ass}_A(U) \subset \mathrm{Ass}_A(M) \subset \mathrm{Ass}_A(U) \cup \mathrm{Ass}_A(M/U) \ .$$

Daraus folgt: *Ist*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

eine exakte Folge von A-*Moduln, so gilt*:

$$\mathrm{Ass}_A(M_1) \subset \mathrm{Ass}_A(M_2) \subset \mathrm{Ass}_A(M_1) \cup \mathrm{Ass}_A(M_3) \ .$$

Beweis. $\mathrm{Ass}_A(U) \subset \mathrm{Ass}_A(M)$ ist nach Definition unmittelbar klar. Sei $\mathfrak{p} \in \mathrm{Ass}_A(M)$ und E ein Untermodul von M, isomorph zu $A \ / \ \mathfrak{p}$. Im Falle $E \cap U \neq \{0\}$ ist (nach Lemma 2.4(iii))

$$\{\mathfrak{p}\} = \mathrm{Ass}_A(E \cap U) \subset \ \mathrm{Ass}_A(U).$$

Wenn aber $E \cap U = \{0\}$ ist, ist E isomorph zum Untermodul $(E + U) \ / \ U$ von $M \ / \ U$ (weil $(E + U) \ / \ U \cong E \ / \ E \cap U$), d.h. $\mathfrak{p} \in \mathrm{Ass}_A(M/U)$. $\square$

Proposition 2.8. *Sei M ein A-Modul und*

$$0 = M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M$$

eine aufsteigende endliche Folge von A-Moduln, so daß $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ mit Primidealen $\mathfrak{p}_i$ ist. Dann gilt:

$$\mathrm{Ass}_A(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \ .$$

Beweis. Nach 2.4(iii) und 2.7 hat man die Inklusionskette

$$\mathrm{Ass}_A(M) \subset \mathrm{Ass}_A(M_{n-1}) \cup \mathrm{Ass}_A(M_n/M_{n-1}) = \mathrm{Ass}_A(M_{n-1}) \cup \{\mathfrak{p}_n\} \subset$$

$$\subset \mathrm{Ass}_A(M_{n-2}) \cup \mathrm{Ass}_A(M_{n-1}/M_{n-2}) \cup \{\mathfrak{p}_n\} = \mathrm{Ass}_A(M_{n-2}) \cup \{\mathfrak{p}_{n-1}\} \cup \{\mathfrak{p}_n\} \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} ,$$

woraus die Behauptung folgt. □

Proposition 2.9. *Ist A Noethersch, $S \subset A$ multiplikativ abgeschlossen und M ein A-Modul, so gilt*

$$\mathrm{Ass}_{S^{-1}A}\left(S^{-1}M\right) = \left\{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}_A(M) \quad \text{mit} \quad \mathfrak{p} \cap S = \varnothing\right\} \ .$$

Beweis. "$\supset$": Sei $\mathfrak{p} \in \mathrm{Ass}_A(M)$, $\mathfrak{p} = \mathrm{Ann}_A(m)$, $\mathfrak{p} \cap S = \varnothing$. Setze $I := \mathrm{Ann}_{S^{-1}A}\left(\frac{m}{1}\right)$. Dann gilt $I = S^{-1}\mathfrak{p}$, denn man hat die Äquivalenzen

$$\frac{a}{s} \cdot \frac{m}{1} = \frac{0}{1} \Longleftrightarrow \exists t,\ t \in S : tam = 0 \Longleftrightarrow \exists t,\ t \in S : ta \in \mathfrak{p} \Longleftrightarrow a \in \mathfrak{p},$$

letzteres, weil $\mathfrak{p}$ prim ist.

"$\subset$": Sei $\mathfrak{q} = \mathrm{Ann}_{S^{-1}A}\left(\frac{m}{s}\right)$, $s \in S$. Nach Proposition 1.6 gilt $\mathfrak{q} = S^{-1}\mathfrak{p}$ für ein Primideal $\mathfrak{p}$ von A mit $\mathfrak{p} \cap S = \varnothing$. Da A Noethersch ist, gibt es Elemente $p_1, \ldots, p_r \in \mathfrak{p}$ derart, daß

$$\mathfrak{p} = A\ p_1 + A\ p_2 + \cdots + A\ p_r \ ,$$

und es gilt

$$\frac{p_i}{1} \cdot \frac{m}{s} = 0,\ \forall i,\ 1 \le i \le r \ .$$

Es gibt also für jedes i, $1 \le i \le r$, ein $t_i \in S$ mit $t_i\ p_i\ m = 0$, d.h. für $t := \prod_{i=1}^{r} t_i \in S$ gilt

$$(t\ p_i\ m = 0,\ \forall i,\ 1 \le i \le r\ ) \Longrightarrow \mathfrak{p}\ \subset \mathrm{Ann}_A(t\ m) \,.$$

Ist andererseits $atm = 0$, mithin $\frac{a}{1} \cdot \frac{tm}{ts} = 0$, also $\frac{a}{1} \in S^{-1}\mathfrak{p}$, so gibt es eine Darstellung $\frac{a}{1} = \frac{p}{s'}$, wobei $p \in \mathfrak{p}$, $s' \in S$. Deshalb gibt es ein $s'' \in S$ mit $s's''a = s''p \in \mathfrak{p}$, und es folgt aus $\mathfrak{p} \cap S = \varnothing$, daß a in $\mathfrak{p}$ liegt und damit $\mathfrak{p} \supset \mathrm{Ann}_A(t\ m)$ gilt. Insgesamt haben wir

$$\mathfrak{p}\ = \mathrm{Ann}_A(t\ m)$$

mit $S^{-1}\mathfrak{p} = \mathfrak{q}$ gezeigt. □

Definition 2.10. Sei M ein A-Modul.

$$\boxed{\mathrm{Supp}_A(M) := \{\mathfrak{p} \mid \mathfrak{p} \ \text{ Primideal von } A \text{ mit } \ M_{\mathfrak{p}} \neq 0\}}$$

heißt der *Träger* von M.

Lemma 2.11. *Wenn man A als A-Modul betrachtet, ist*

$$\operatorname{Supp}_A(A) = \{\mathfrak{p} \mid \mathfrak{p} \text{ Primideal von } A\} \quad (=: \operatorname{Spec}(A)) \ .$$

Beweis. Für jedes Primideal $\mathfrak{p}$ von A besitzt $A_\mathfrak{p}$ das maximale Ideal $\mathfrak{p}A_\mathfrak{p}$ (siehe Proposition 1.4). Also ist $A_\mathfrak{p} \neq 0$. □

Theorem 2.12. *Für einen endlich erzeugten A-Modul M gilt*:

$$\operatorname{Supp}_A(M) = \{\mathfrak{p} \mid \mathfrak{p} \text{ Primideal von } A \text{ mit } \mathfrak{p} \supseteq \operatorname{Ann}_A(M)\} \ .$$

(Für beliebige A-Moduln M gilt nur "$\subset$").

Beweis. "$\subset$": Angenommen, es gäbe $\mathfrak{p} \in \operatorname{Supp}_A(M)$ mit $\mathfrak{p} \not\supseteq \operatorname{Ann}_A(M)$. Sei dann $t \in \operatorname{Ann}_A(M) \smallsetminus \mathfrak{p}$ beliebig. Es gälte

$$\frac{m}{s} = \frac{tm}{st} = \frac{0}{st} = 0_{M_\mathfrak{p}} .$$

Dann wäre $M_\mathfrak{p} = 0$ im Widerspruch zu $\mathfrak{p} \in \operatorname{Supp}_A(M)$.

"$\supset$" : Ist

$$M = A\, m_1 + A\, m_2 + \cdots + A\, m_r,$$

so gilt

$$\operatorname{Ann}_A(M) = \bigcap_{i=1}^{r} \operatorname{Ann}_A(m_i) \supset \prod_{i=1}^{r} \operatorname{Ann}_A(m_i) .$$

Ist $\mathfrak{p} \supseteq \operatorname{Ann}_A(M)$, so existiert[1] ein Index $i_0 \in \{1, 2, \ldots, r\}$ mit $\operatorname{Ann}_A(m_{i_0}) \subset \mathfrak{p}$. Mit $\overline{\mathfrak{p}} := \mathfrak{p} \,/\, \operatorname{Ann}_A(m_{i_0})$ folgt

$$(A \,/\, \operatorname{Ann}_A(m_{i_0}))_\mathfrak{p} \cong (A \,/\, \operatorname{Ann}_A(m_{i_0}))_{\overline{\mathfrak{p}}} \neq 0$$

wegen Lemma 2.11; also ist

$$(A \,/\, \operatorname{Ann}_A(m_{i_0}))_\mathfrak{p} \cong (Am_{i_0})_\mathfrak{p}$$

(siehe Lemma 2.4(i)) und nach 1.9(v) ist $(Am_{i_0})_\mathfrak{p}$ ein nicht trivialer Untermodul von $M_\mathfrak{p}$. Deshalb auch $M_\mathfrak{p} \neq 0$! □

Proposition 2.13. (i) *Für einen endlich erzeugten Modul M über einen Noetherschen Ring A gilt*

$$\operatorname{Supp}_A(M) = \{\mathfrak{p} \text{ Primideal von } A \mid \exists \mathfrak{q}, \mathfrak{q} \in \operatorname{Ass}_A(M) : \ \mathfrak{p} \supset \mathfrak{q}\} \ .$$

(ii) *Insbesondere gehören die minimalen Primideale eines Noetherschen Rings $A \neq \{0\}$ zu $\operatorname{Ass}_A(A)$.*

Beweis. (i) *"$\supset$":* Für $\mathfrak{q} \in \operatorname{Ass}_A(M)$ gilt $\mathfrak{q} \supset \operatorname{Ann}_A(M)$, und nach Theorem 2.12 folgt $\mathfrak{q} \in \operatorname{Supp}_A(M)$. Alle $\mathfrak{q}$ umfassenden Primideale gehören ebenfalls zu $\operatorname{Supp}_A(M)$.

"$\subset$": Sei umgekehrt $M_\mathfrak{p} \neq 0$ für ein $\mathfrak{p} \in \operatorname{Spec}(A)$. Nach 2.5 enthält $\operatorname{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$ ein Element $\mathfrak{q}A_\mathfrak{p}$ mit $\mathfrak{q} \in \operatorname{Spec}(R)$, $\mathfrak{p} \supset \mathfrak{q}$. Aus Prop. 2.9 folgt $\mathfrak{q} \in \operatorname{Ass}_A(M)$.

(ii) Für ein minimales Ideal $\mathfrak{p}$ von A ist $A_\mathfrak{p} \neq \{0\}$, d.h. $\mathfrak{p} \in \operatorname{Supp}_A(A)$. Nach (i) muß $\mathfrak{p}$ ein assoziiertes Primideal $\mathfrak{q}$ von A enthalten, also muß $\mathfrak{p} = \mathfrak{q} \in \operatorname{Supp}_A(A)$ gelten. □

[1] Sind I, J Ideale in A und $\mathfrak{p}$ *prim* mit $IJ \subset \mathfrak{p}$, so ist entweder $I \subset \mathfrak{p}$ oder $J \subset \mathfrak{p}$.

Proposition 2.14. *Sei M ein A-Modul und*

$$\{0\} = M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M$$

eine aufsteigende endliche Folge von A-Moduln, so daß $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ mit Primidealen $\mathfrak{p}_i$ ist. Dann gilt:

$$\mathrm{Ass}_A(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Supp}_A(M) \ .$$

Diese drei Mengen besitzen dieselben minimalen Elemente (bzgl. Inklusion).

Beweis. Die erste Inklusion wurde schon in 2.8 bewiesen. Wegen $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ erhält man

$$0 \neq (A/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (M_i/M_{i-1})_{\mathfrak{p}_i} ,$$

also wegen Lemma 2.5 $(M_i)_{\mathfrak{p}_i} \neq 0$ und somit $M_{\mathfrak{p}_i} \neq 0$, d.h. $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Supp}_A(M)$. Es bleibt zu zeigen, daß die minimalen Elemente von $\mathrm{Supp}_A(M)$ in $\mathrm{Ass}_A(M)$ liegen. Sei $\mathfrak{p}$ ein solches. Dann ist $\mathrm{Supp}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \{\mathfrak{p}A_\mathfrak{p}\}$ (denn $(M_\mathfrak{p})_{\mathfrak{q}_\mathfrak{p}} \cong M_\mathfrak{q}$). Da $\mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p}) \neq 0$, folgt $\mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \{\mathfrak{p}A_\mathfrak{p}\}$, also mit 2.9, daß $\mathfrak{p} \in \mathrm{Ass}_A(M)$. □

Aus 2.14 folgt sofort:

Proposition 2.15. *Ist A Noethersch und I ein Ideal, so sind die minimalen Elemente von $\mathrm{Ass}_A(A/I)$ genau die minimalen Primideale von A, die I enthalten.*

3. Primärzerlegung von Moduln über Noetherschen Ringen

• Die Theorie der Zerlegungen von Idealen bzw. von endlich erzeugten Moduln über Noetherschen Ringen in Primärkomponenten wurde hauptsächlich von Emanuel Lasker (geb. 24.12.1868 - gest. 15.1.1941) und Amalie-Emmy Noether (geb. 23.3.1882 - gest. 14.4.1935) Anfang unseres Jahrhunderts[2] entwickelt. Sie verallgemeinert die wohlbekannte Faktorzerlegung in faktoriellen Ringen.

Definition 3.1. Sei M ein A-Modul. Ein Element a von A heißt *nilpotent bezüglich* M, wenn es ein $\nu \in \mathbb{N}$ gibt, so daß $a^\nu \in \mathrm{Ann}_A(M)$. Offensichtlich gilt

$$\left\{ \begin{array}{c} \text{Menge der nilpotenten} \\ \text{Elemente bezüglich } M \end{array} \right\} = \sqrt{\mathrm{Ann}_A(M)} = \bigcap \left\{ \mathfrak{p} \;\middle|\; \begin{array}{c} \mathfrak{p} \text{ Primideal von } A \\ \text{mit } \mathfrak{p} \in \mathrm{Supp}_A(M) \end{array} \right\}$$

Definition 3.2. Seien M ein A-Modul und Q ein Untermodul von M. Die folgenden Bedingungen sind äquivalent:

(i) Ist $a \in A$, $m \in M \smallsetminus Q$ und $am \in Q$, so existiert ein $\nu \in \mathbb{N}$: $a^\nu M \subset Q$.

(ii) Jeder Nullteiler bzgl. M/Q ist nilpotent bzgl. M/Q.

Falls Q eine dieser Bedingungen erfüllt, dann heißt Q *primär.* (Insbesondere heißt ein Ideal I von A *primär* oder *Primärideal*, wenn I als Untermodul des A-Moduls A primär ist, d.h wenn für $a \in A$, $b \in A \smallsetminus I$ mit $ab \in I$ ein $\nu \in \mathbb{N}$ existiert, so daß $a^\nu \in I$).

[2]Siehe: E.Lasker: *Zur Theorie der Moduln und Ideale*, Math. Ann. **60**, (1905), 20-116.

E.Noether: *Idealtheorie in Ringbereichen*, Math. Ann. **83**, (1921), 24-66.

E.Noether: *Eliminationstheorie und allgemeine Idealtheorie*, Math. Ann. **90**, (1923), 229-261.

Lemma 3.3. *Ist $Q \subset M$ ein primärer Untermodul, so ist $\sqrt{\mathrm{Ann}_A(M/Q)}$ ein Primideal. Speziell ist das Radikal $\sqrt{I}$ jedes Primärideals $I \subset A$ ein Primideal.*

Beweis. Für Elemente $a, b \in A$ sei $ab \in \sqrt{\mathrm{Ann}_A(M/Q)}$ mit $b \notin \sqrt{\mathrm{Ann}_A(M/Q)}$. Dann gibt es ein $\nu \in \mathbb{N}$, so daß

$$(ab)^\nu \in \mathrm{Ann}_A(M/Q)\,, \quad b^\nu \notin \mathrm{Ann}_A(M/Q)\,,$$

d.h. es gibt ein $x \in M/Q$ mit $b^\nu x \neq 0$. Wegen $(ab)^\nu x = a^\nu(b^\nu x) = 0$ ist a^ν ein Nullteiler von M/Q; es gibt daher ein $\mu \in \mathbb{N}$ mit $(a^\nu)^\mu \in \mathrm{Ann}_A(M/Q)$. Folglich ist $a \in \sqrt{\mathrm{Ann}_A(M/Q)}$ und deswegen $\sqrt{\mathrm{Ann}_A(M/Q)}$ ein Primideal. Die Aussage über Primideale ergibt sich aus $\mathrm{Ann}_A(A/I) = I$. □

Bemerkung. Nicht jedes Ideal $I \subset A$, dessen Radikal $\sqrt{I}$ ein Primideal ist, ist primär! Ein einfaches Beispiel ist

$$I = \langle X^2, XY \rangle \subset K[X, Y]\ .$$

Das Radikal $\sqrt{I} = \langle X \rangle$ ist offensichtlich prim und $\langle X, Y\rangle^2 \subsetneqq I \subsetneqq \langle X, Y\rangle$, aber I ist nicht primär, weil einerseits $XY \in I$ und andererseits $X \notin I$ und $Y^n \notin I$ für alle $n \in \mathbb{N}$.

Definition 3.4. Ist $Q \subset M$ ein primärer Untermodul und $\mathfrak{p} = \sqrt{\mathrm{Ann}_A(M/Q)}$, so sagt man Q sei $\mathfrak{p}$-*primär*. Entsprechend heißt ein Primärideal $I \subset A$ mit $\mathfrak{p} = \sqrt{I}$ ein $\mathfrak{p}$-*primäres Ideal*.

Proposition 3.5. *Sei A Noethersch, M ein A-Modul und $Q \subset M$ ein Untermodul.*

(i) *Ist Q primär, so besteht $\mathrm{Ass}_A(M/Q)$ aus genau ein Element $\mathfrak{p}$ und Q ist $\mathfrak{p}$-primär.*

(ii) *Ist M endlich erzeugt und besteht $\mathrm{Ass}_A(M/Q)$ aus genau einem Element $\mathfrak{p}$, so ist Q primär.*

Beweis. (i) Nach Lemma 2.5 ist $\mathrm{Ass}_A(M/Q) \neq \varnothing$. Sei $\mathfrak{p} := \sqrt{\mathrm{Ann}_A(M/Q)}$ und $\mathfrak{q} \in \mathrm{Ass}_A(M/Q)$ mit $\mathfrak{q} = \mathrm{Ann}_A(x)$ für ein $x \in M/Q$, $x \neq 0$. Dann ist $\mathrm{Ann}_A(M/Q) \subset \mathfrak{q}$ und somit $\mathfrak{p} \subset \mathfrak{q}$. Andererseits ist jedes Element von $\mathfrak{q}$ ein Nullteiler bzgl. M/Q, folglich nilpotent bzgl. M/Q. Daraus ergibt sich $\mathfrak{p} \supset \mathfrak{q}$, d.h. $\mathfrak{p} = \mathfrak{q}$.

(ii) Nach Lemma 2.6 ist $\mathfrak{p}$ genau die Menge aller Nullteiler von M/Q. Auf der anderen Seite ist aber auch $\mathfrak{p} = \sqrt{\mathrm{Ann}_A(M/Q)}$ nach 2.12 und 2.13 die Menge aller nilpotenten Elemente bzgl. M/Q. Daher ist $\mathfrak{p}$-primär. □

Proposition 3.6. *Sei M ein endlich erzeugter A-Modul. Der Durchschnitt endlich vieler $\mathfrak{p}$-primärer Untermoduln von M ist auch $\mathfrak{p}$-primär.*

Beweis. Es genügt, dies für zwei $\mathfrak{p}$-primäre Q_1, Q_2 Untermoduln von M. (Der Beweis in dem allgemeinen Fall folgt leicht mittels Induktion). Zuerst erhält man eine exakte Folge

$$0 \longrightarrow Q_1 \ / \ Q_1 \cap Q_2 \longrightarrow M \ / \ Q_1 \cap Q_2 \longrightarrow \ M \ / \ Q_1 \longrightarrow 0.$$

Nach Prop. 2.7 gilt

$$\mathrm{Ass}_A(Q_1 \ / \ Q_1 \cap Q_2) \subset \mathrm{Ass}_A(M \ / \ Q_1 \cap Q_2) \subset \mathrm{Ass}_A(Q_1 \ / \ Q_1 \cap Q_2) \cup \mathrm{Ass}_A(M \ / \ Q_1)\ .$$

Hierbei ist

$$Q_1 \ / \ Q_1 \cap Q_2 \cong Q_1 + Q_2 \ / \ Q_2$$

und nach 3.5,

$$\operatorname{Ass}_A(Q_1 + Q_2 \ / \ Q_2) \subset \operatorname{Ass}_A(M \ / \ Q_2) = \{\mathfrak{p}\}\,.$$

Da aber auch $\operatorname{Ass}_A(M \ / \ Q_1) = \{\mathfrak{p}\}$ ist, folgt $\operatorname{Ass}_A(M \ / \ Q_1 \cap Q_2) = \{\mathfrak{p}\}$. Die Behauptung ergibt sich wieder aus der Anwendung von Prop. 3.5. □

Definition 3.7. Ein Untermodul Q eines A-Moduls M wird *irreduzibel in* M genannt, falls gilt:

Sind Q', Q'' Untermoduln von M mit $Q = Q' \cap Q''$, so ist entweder $Q = Q'$ oder $Q = Q''$.

(Insbesondere sind damit auch *irreduzible Ideale* von A selbst definiert.)

Proposition 3.8. *Sei A Noethersch, M ein endlich erzeugter A-Modul und Q ein echter irreduzibler Untermodul von M. Dann ist Q primär.*

Beweis. Da Q irreduzibel in M ist, ist der Nullmodul in M/Q irreduzibel. Angenommen, $\operatorname{Ass}_A(M/Q)$ enthielte zwei verschiedene Primideale $\mathfrak{p}_1$ und $\mathfrak{p}_2$. Dann gibt es in M/Q zwei Untermoduln $Q_1 \cong A/\mathfrak{p}_1$ und $Q_2 \cong A/\mathfrak{p}_2$. Da

$$\operatorname{Ann}_A(q) = \mathfrak{p}_i \quad \text{für jedes} \quad q \in Q_i \setminus \{0\}\,, \quad i = 1, 2$$

ergibt sich $Q_1 \cap Q_2 = \{0\}$, im Widerspruch zu der Irreduzibilität von $\{0\}$. Da $\operatorname{Ass}_A(M/Q) \neq \varnothing$ (nach Lemma 2.5), enthält $\operatorname{Ass}_A(M/Q)$ somit genau ein Element und Prop. 3.5 liefert die Behauptung. □

Bemerkung. Die Umkehrung von 3.8 ist i.a. falsch! Ein einfaches Gegenbeispiel geht auf eine im Jahre 1970 veröffentlichte Arbeit[3] von R.Kummer und B.Renschuch zurück. In $A = M = K[X_1, X_2]$ läßt sich das Primärideal

$$I := \langle X_1^3, X_2^4, X_1^2 X_2 \rangle \subset A$$

als Durchschnitt von zwei Idealen $I = I' \cap I''$ darstellen, wobei

$$I' = \langle X_1^3, X_2 \rangle \supsetneqq I, \qquad I'' = \langle X_1^2, X_2^4 \rangle \supsetneqq I\ .$$

I ist also ein reduzibles Primärideal!

Definition 3.9. Sei M ein A-Modul und U ein Untermodul von M. U *besitzt eine Primärzerlegung*, wenn es primäre Untermoduln $Q_1, \ldots, Q_k$ $(k \geq 1)$ von M gibt, so daß

$$\boxed{U = Q_1 \cap \cdots \cap Q_k} \qquad (*)$$

Die Primärzerlegung $(*)$ heißt *reduziert*, wenn gilt:

(i) Ist Q_i $\mathfrak{p}_i$-primär für alle i, $1 \leq i \leq k$, so ist $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i \neq j$.

(ii) Es ist $\bigcap\limits_{i \neq j} Q_i \nsubseteq Q_j$ für $j = 1, \ldots, k$.

Die in einer reduzierten Primärzerlegung $(*)$ auftretenden Q_i's heißen *Primärkomponenten* von U.

[3] Siehe: R.Kummer, B.Renschuch: *Potenzproduktideale I*, Publ.math. Debrecen **17**, (1970), 81-98.

Beispiel. Wenn $n = p_1^{r_1} \cdots p_k^{r_k}$ die Zerlegung einer natürlichen Zahl n in verschiedene Primfaktoren ist, dann ist

$$n\,\mathbb{Z} = p_1^{r_1}\,\mathbb{Z} \cap \cdots \cap p_k^{r_k}\,\mathbb{Z}$$

eine Primärzerlegung von $n\,\mathbb{Z}$ in dem Noetherschen Ring $\mathbb{Z}$.

Bemerkung. Ist A Noethersch, M endlich erzeugt und besitzt $U \subset M$ eine Primärzerlegung, dann auch eine reduzierte! Nach Prop. 3.6 kann man nämlich die Primärmoduln zum selben Primideal zum Durchschnitt bringen und damit die Bedingung 3.9(i) erreichen. Für 3.9(ii) läßt man überflüssige Primärmoduln einfach weg.

Theorem 3.10 (Existenz einer reduzierten Primärzerlegung). *Ist M ein endlich erzeugter Modul über einem Noetherschen Ring A, so besitzt jeder echte Untermodul U von dem Modul M eine reduzierte Primärzerlegung.*

Beweis. Nach Prop. 3.8 genügt es zu zeigen, daß U Durchschnitt von endlich vielen irreduziblen Untermoduln von M ist. Wäre dies nicht so, so gäbe es nach der Maximalbedingung einen größten Untermodul $U \subsetneqq M$ von M, für welchen diese Aussage falsch ist. U wäre dann irreduzibel, folglich gäbe es Untermoduln $U_1, U_2 \subsetneqq U$ von M mit $U = U_1 \cap U_2$. Da U_1, U_2 den Modul U echt umfassen, sind sie als Durchschnitt von endlich vielen irreduziblen Untermoduln von M darstellbar, also auch U, ein Widerspruch. Das Theorem ist also wahr! $\square$

Theorem 3.11 (Erster Eindeutigkeitssatz). *Sei M ein Modul über einem Noetherschen Ring A. Der Untermodul U besitzte eine reduzierte Primärzerlegung*

$$U = Q_1 \cap \cdots \cap Q_k$$

in $\mathfrak{p}_i$-primäre Moduln $Q_i \subset M$, $i = 1, \ldots, k$. Dann ist

$$\operatorname{Ass}_A(M/U) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} \ .$$

Die $\mathfrak{p}_i$'s sind somit durch M und U eindeutig bestimmt.

Beweis. Wir definieren $U_i := \bigcap_{j \neq i} Q_j$, d.h. $U = U_i \cap Q_i$ mit $U \neq U_i$, $\forall i$, $1 \le i \le k$.
Aus der Beziehung

$$U_i \ / \ U \cong U_i + Q_i \ / \ Q_i$$

folgt

$$\varnothing \neq \ \operatorname{Ass}_A(U_i \ / \ U) \subset \operatorname{Ass}_A(M \ / \ Q_i) = \{\mathfrak{p}_i\} \ .$$

Witerhin gilt:

$$\operatorname{Ass}_A(U_i \ / \ U) \subset \operatorname{Ass}_A(M \ / \ U) \Longrightarrow \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} \subset \ \operatorname{Ass}_A(M \ / \ U) \,.$$

Um die Inklusion "$\supset$" zu zeigen, benutzt man Induktion nach k. Der Fall $k = 1$ ist trivial. Sei $k > 1$. Das Theorem sei für reduzierte Primärzerlegungen mit genau $k-1$ Primärkomponenten schon bewiesen. Aus der Definition von U_i's ergibt sich dann

$$\operatorname{Ass}_A(M \ / \ U_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{i-1}, \mathfrak{p}_{i+1}, \ldots, \mathfrak{p}_k\} \ .$$

Nun ist

$$M \ / \ U_i \cong (M \ / \ U) \ / \ (U \ / \ U_i)$$

und aus der Proposition 2.7 erhalten wir

$$\mathrm{Ass}_A\,(M\ /\ U) \subset \mathrm{Ass}_A\,(U_i\ /\ U) \cup \mathrm{Ass}_A\,(M\ /\ U_i) \subset \{\mathfrak{p}_i\} \cup \{\mathfrak{p}_1,..,\mathfrak{p}_{i-1},\mathfrak{p}_{i+1},..,\mathfrak{p}_k\} = \{\mathfrak{p}_1,\ldots,\mathfrak{p}_k\}\,,$$

was noch zu zeigen war. □

Theorem 3.12 (Primaerzerlegung und Lokalisierung). *Sei M ein endlich erzeugter Modul über einem Noetherschen Ring A und S ein multiplikativ abgeschlossene Teilmenge von A.*
(i) *Ist $Q \subset M$ ein $\mathfrak{p}$-primärer Untermodul und $\mathfrak{p} \cap S = \varnothing$, so ist $S^{-1}Q \subset S^{-1}M$ ein $S^{-1}\mathfrak{p}$-primärer Untermodul. Ist andererseits $\mathfrak{p} \cap S \neq \varnothing$, so ist $S^{-1}Q = S^{-1}M$.*
(ii) *Ist*

$$U = Q_1 \cap \cdots \cap Q_k$$

eine reduzierte Primärzerlegung eines Untermoduls $U \subset M$ in $\mathfrak{p}_i$-primäre Moduln $Q_i \subset M$, $i = 1,\ldots,k$, so ist

$$S^{-1}U = \bigcap_{\{i \in \{1,\ldots,k\}\ |\ \mathfrak{p}_i \cap S = \varnothing\}} S^{-1}Q_i$$

eine reduzierte Primärzerlegung des Untermoduls $S^{-1}U$ von $S^{-1}M$.

Beweis. Die erste Aussage in (i) folgt aus Prop. 2.9 und der Definition eines Primärmoduls. Die zweite kann wie in 1.6(i) nachgewiesen werden. (ii) ergibt sich aus (i), weil Lokalisierung und Durchschnittsbildung vertauschbare Orerationen (bei endlichen Durchschnitten) sind (siehe 1.9(vii)). □

Theorem 3.13 (Zweiter Eindeutigkeitssatz). *Sei M ein endlich erzeugter Modul über einem Noetherschen Ring A. Für einen Untermodul $U \subset M$ sei*

$$U = Q_1 \cap \cdots \cap Q_k$$

eine reduzierte Primärzerlegung in $\mathfrak{p}_i$-primäre Moduln $Q_i \subset M$, $i = 1,\ldots,k$. Ist $\mathfrak{p}_i$ ein minimales Element der Menge $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_k\}$, so ist

$$Q_i = \iota^{-1}_{M,A\smallsetminus\mathfrak{p}_i}\,(U_{\mathfrak{p}_i})\,,$$

wobei wir mit $\iota_{M,A\smallsetminus\mathfrak{p}_i} : M \to M_{\mathfrak{p}_i}$ den kanonischen Homomorphismus bezeichnen. Die Primärkomponenten zu den minimalen Elementen von $\mathrm{Ass}_A\,(M/U)$ sind durch M und U eindeutig festgelegt.

Beweis. Sei $S_i := A\smallsetminus\mathfrak{p}_i$. Aus Theorem 3.12 folgt dann $S_i^{-1}U \cong S_i^{-1}Q_i$, weil $S_i^{-1}Q_j = S_i^{-1}M = M_{\mathfrak{p}_i}$ für $j \neq i$ ist. Für $m \in M$ mit $\frac{m}{1} \in S_i^{-1}Q_i$ gibt es ein $s \in S_i$ mit $sm \in Q_i$. Da Q_i $\mathfrak{p}_i$-primär ist und $s \notin \mathfrak{p}_i$, folgt $m \in Q_i$, d.h. $Q_i = \iota^{-1}_{M,S_i}\,(U_{\mathfrak{p}_i})$. □

Definition 3.14. Die Primärkomponenten, welche zu den minimalen Elementen der Menge $\mathrm{Ass}_A\,(M/U)$ gehören, heißen *isolierte Primärkomponenten* von U. Die restlichen heißen *eingebettete Primärkomponenten* von U. Der zweite Eindeutigkeitssatz beweist die Eindeutigkeit der isolierten Primärkomponenten.

Bemerkung. Die eingebetteten Primärkomponenten sind i.a. nicht eindeutig bestimmt! Zum Beispiel für

$$I = \langle X^2, XY \rangle \subset K[X,Y]$$

gibt es zwei reduzierte Primärzerlegungen

$$I = \langle X \rangle \cap \langle X^2, Y \rangle = \langle X \rangle \cap \langle X^2, X+Y \rangle \ .$$

($\langle X \rangle$ ist offensichtlich ein Primideal und $\langle X^2, Y \rangle, \langle X^2, X+Y \rangle$ Primärideale zum maximalen Ideal $\langle X, Y \rangle \subset K[X,Y]$). Auf der anderen Seite ist

$$\langle X^2, Y \rangle \neq \langle X^2, X+Y \rangle \ .$$

Bemerkung. Ist

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$$

eine Primärzerlegung eines Ideals in einem Noetherschen Ring A, wobei $\mathfrak{q}_i$ ein $\mathfrak{p}_i$-primäres Ideal ist, so gilt

$$\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_l, \quad (l \leq k) \qquad (**)$$

wobei wir mit $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\} \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ (bis auf Umnumerierung der Indizes) die minimalen Elemente der Menge $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ bezeichnen. Dies ergibt sich, weil nach 2.13(ii) genau dann $I \subset \mathfrak{p}$ gilt, wenn $\mathfrak{p}_i \subset \mathfrak{p}$ für ein $\mathfrak{p}_i \in \mathrm{Ass}_A(A/I)$. $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ sind dann gerade die minimalen Primteiler von I. $(**)$ ist natürlich die Primärzerlegung von $\sqrt{I}$.

Definition 3.15. Sei A ein kommutativer Ring mit 1. Sind I, J Ideale von A mit $I + J = A$, so heißen I und J *teilerfremd.* Offensichtlich gilt:

$$(I, J \ \text{ teilerfremd}) \Longleftrightarrow (\exists a, \ a \in I, \ \text{ und } \ \exists b, \ b \in J : a + b = 1) \ .$$

Lemma 3.16. (i) *Sind $I, J \subset A$ teilerfremd, so gilt $IJ = I \cap J$.*
(ii) *Sind $I, I' \subset A$ und $I, I'' \subset A$ jeweils teilerfremd, so auch $I, I'I''$.*

Beweis. (i) Offenbar ist $IJ \subset I \cap J$. Zu "$\supset$": Aus $a + b = 1$ mit $a \in I$, $b \in J$ folgt durch Multiplikation mit einem beliebigen $c \in I \cap J$ sofort $c = ca + cb \in IJ$.
(ii) Sind I, I' und I, I'' teilerfremd, so gibt es $a \in I$, $b \in I'$ mit $a + b = 1$ und $c \in I$, $d \in I''$ mit $c + d = 1$. Betrachte

$$bd = (1-a)(1-c) = 1 - a - c + ac.$$

Für $e := a + c - ac$ gilt dann $bd + e = 1$, d.h. auch $I, I'I''$ sind teilerfremd. □

Lemma 3.17 (Chinesischer Restsatz). (i) *Sind $I_1, \ldots, I_k \subset A$, $k \geq 2$, Ideale, die paarweise teilerfremd sind, so gilt:*

$$I_1 \cdot I_2 \ \cdots \ I_k = I_1 \cap I_2 \ \cap \cdots \cap I_k \ .$$

(ii) *Sei θ der Ringhomomorphismus*

$$A \ni a \overset{\theta}{\longmapsto} (a + I_1, a + I_2, \ldots, a + I_k) \in (A/I_1) \times (A/I_2) \times \cdots \times (A/I_k) \ .$$

Wenn $I_1, \ldots, I_k$ paarweise teilerfremd sind, dann ist θ surjektiv.
(iii) $\mathrm{Ker}(\theta) = I_1 \cap I_2 \ \cap \cdots \cap I_k$. *Also:*

$$(\theta \ \text{ ist injektiv}) \Longleftrightarrow I_1 \cap I_2 \ \cap \cdots \cap I_k = \{0\} \ .$$

Beweis. (i) Induktion nach k. Der Fall $k = 2$ ist in Lemma 3.16(i) abgehandelt. Sei $k > 2$ und die Behauptung richtig für $I_1, \ldots, I_{k-1}$ und $J := I_1 \cap I_2 \ \cap \cdots \ \cap I_{k-1}$. Nach 3.16(ii) sind I_k und J teilerfremd. Deshalb ist

$$I_1 \cdot I_2 \ \cdots \ I_k = J \cdot I_k = J \cap I_k = I_1 \cap I_2 \ \cap \cdots \ \cap I_k \ .$$

(ii) Wir beweisen die Surjektivität von θ. Sei

$$(a_1 + I_1, a_2 + I_2, \ldots, a_k + I_k) \in (A/I_1) \times (A/I_2) \times \cdots \times (A/I_k)$$

gegeben. Für $i \neq j$ wählen wir $b_{ij} \in I_i$, $c_{ij} \in I_j$ mit $1 = b_{ij} + c_{ij}$. Dann ist

$$d_j := \prod_{l \neq j} b_{lj} \in I_i, \quad \text{für } i \neq j,$$

und

$$d_j + I_j = \prod_{l \neq j} (1 - c_{lj}) + I_j = 1 + I_j \ .$$

Nun definieren wir

$$a := a_1 d_1 + a_2 d_2 + \cdots + a_k d_k \ .$$

Es gilt offensichtlich

$$\begin{aligned} a + I_i &= \sum_{j=1}^{k} a_j d_j + I_i = a_i d_i + I_i = \\ &= (a_i + I_i)\,(d_i + I_j) = (a_i + I_i)\,(1 + I_j) = a_i + I_i, \quad \forall i, \quad 1 \leq i \leq k, \end{aligned}$$

d.h. $\theta\,(a) = (a_1 + I_1, a_2 + I_2, \ldots, a_k + I_k)$. (iii) ist offenbar. □

Lemma 3.18. *Sei A ein Noetherscher Ring und $\mathfrak{m} \subset A$ ein maximales Ideal. Dann hat man für ein Ideal $\mathfrak{q} \subset A$:*

$$(\mathfrak{q} \ \text{ ist } \ \mathfrak{m}\text{-primär}) \Longleftrightarrow (\exists\ \nu,\ \nu \in \mathbb{N} : \mathfrak{m} \supset \mathfrak{q} \supset \mathfrak{m}^{\nu}) \ .$$

Beweis. Die Richtung "$\Longrightarrow$" ist per definitionem klar. Zu "$\Longleftarrow$": Ist $\mathfrak{p}$ ein Primideal mit $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{m}^{\nu}$, so gilt $\mathfrak{p} \supset \mathfrak{m}$, also $\mathfrak{p} = \mathfrak{m}$. Somit ist $\mathfrak{m}$ das einzige Primideal mit $\mathfrak{p} \subseteq \mathfrak{m}$. Aus Proposition 2.15 folgt dann $\mathrm{Ass}_A\,(A/\mathfrak{q}) = \{\mathfrak{m}\}$. Deswegen ist $\mathfrak{q}$ $\mathfrak{m}$-primär.
□

Theorem 3.19. *Sei A ein Noetherscher Ring und $I \subset A$ ein Ideal derart, daß $\mathrm{Ass}_A\,(A/I)$ nur aus maximalen Idealen von A besteht. Ist dann*

$$I = \mathfrak{q}_1 \cap \ \cdots \ \cap \mathfrak{q}_k$$

eine reduzierte Primärzerlegung von I, so sind die $\mathfrak{q}_i$'s eindeutig bestimmt (bis auf Umnumerierung) und der kanonische Homomorphismus

$$A/I \ni a + I \longmapsto (a + \mathfrak{q}_1, a + \mathfrak{q}_2, \ldots, a + \mathfrak{q}_k) \in (A/\mathfrak{q}_1) \times (A/\mathfrak{q}_2) \times \cdots \times (A/\mathfrak{q}_k)$$

ist ein Isomorphismus. Insbesondere besitzt jedes $A/\mathfrak{q}_i$ genau ein Primideal.

Beweis. Sei $\{\mathfrak{m}_i\} = \mathrm{Ass}_A(A/\mathfrak{q}_i)$, für alle i, $1 \leq i \leq k$. Nach 3.11 ist

$$Ass_A(A/I) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\} \ .$$

Da alle $\mathfrak{m}_i$'s nach Voraussetzung in A maximal sind, sind sie alle minimal in $Ass_A(A/I)$, deshalb sind nach 3.13 die $\mathfrak{q}_i$'s eindeutig bestimmt. Da für alle i, $1 \leq i \leq k$, $\mathfrak{m}_i$ das einzige minimale unter den $\mathfrak{q}_i$ enthaltenen Primidealen ist und gleichzeitig maximal ist, ist $\mathfrak{m}_i$ das einzige Primideal von A, welches $\mathfrak{q}_i$ umfaßt. Gemäß Lemma 3.18 gilt insbesondere

$$\mathfrak{m}_i \supset \mathfrak{q}_i \supset \mathfrak{m}_i^{\nu_i}, \quad \text{für gewisse } \nu_i \in \mathbb{N} \ .$$

Nach Lemma 3.16(ii) sind $\mathfrak{m}_i^{\nu_i}, \mathfrak{m}_j^{\nu_j}$ für $i \neq j$ teilerfremd und deshalb erst recht $\mathfrak{q}_i, \mathfrak{q}_j$ teilerfremd. Deswegen ist die Abbildung

$$A \ / \ I = A \ / \ \bigcap_{i=1}^{k} \mathfrak{q}_i \longrightarrow (A/\mathfrak{q}_1) \times (A/\mathfrak{q}_2) \times \cdots \times (A/\mathfrak{q}_k)$$

nach dem Chinesischen Restsatz 3.17 ein Isomorphismus. $\square$

Beispiel. Wenn $n = p_1^{r_1} \ \cdots \ p_k^{r_k}$ die Zerlegung einer natürlichen Zahl n in verschiedene Primfaktoren ist und $\mathfrak{q}_i := \langle p_i^{r_i} \rangle$ für alle i, $1 \leq i \leq k$, dann ist $\langle n \rangle = \mathfrak{q}_1 \cap \ \cdots \ \cap \mathfrak{q}_k$ eine reduzierte Primärzerlegung von $\langle n \rangle$ und

$$\mathbb{Z}_n = \mathbb{Z} \,/\, n\mathbb{Z} = \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \ .$$