KOMMUTATIVE ALGEBRA

Burkhard Külshammer

Universität Jena, WS 2015/16

Inhaltsverzeichnis

0. Geordnete Mengen und topologische Räume

Eine **(partielle) Ordnung** auf einer Menge P ist eine Relation $\leq$ auf P mit folgenden Eigenschaften:

- (**Reflexivität**) $a \leq a$ für alle $a \in P$;
- (**Antisymmetrie**) $a \leq b \wedge b \leq a \Longrightarrow a = b$;
- (**Transitivität**) $a \leq b \wedge b \leq c \Longrightarrow a \leq c$.

Ggf. nennt man das Paar $(P, \leq)$ eine **geordnete Menge**. Ist $\leq$ aus dem Zusammenhang klar, so sagt man auch: P ist eine geordnete Menge. Auf jeder Teilmenge $Q \subseteq P$ induziert $\leq$ wieder eine Ordnung; so wird Q zu einer **geordneten Teilmenge** von P.

Elemente x, y einer geordneten Menge P mit $x \leq y$ oder $y \leq x$ heißen **vergleichbar**. Sind je zwei Elemente in P vergleichbar, so spricht man von einer **totalen Ordnung**; man nennt $(P, \leq)$ dann auch eine **Kette**.

Ist Q eine Teilmenge einer geordneten Menge P, so heißt ein $s \in P$ mit $q \leq s$ für alle $q \in Q$ eine **obere Schranke** von Q in P. (Analog definiert man **untere Schranken**.) I.a. hat nicht jede Teilmenge von P eine obere Schranke, und i.a. gibt es Teilmengen von P mit mehreren oberen Schranken.

Ein Element $m \in P$ heißt **maximal**, falls kein $p \in P$ mit $m < p$ existiert. (Analog definiert man **minimale** Elemente in P.) Wir werden verwenden:

Zorns Lemma. *Sei $(P, \leq)$ eine nichtleere geordnete Menge. Hat jede total geordnete Teilmenge von P eine obere Schranke in P, so enthält P ein maximales Element.*

Bekanntlich ist Zorns Lemma zum **Auswahlaxiom** der Mengenlehre äquivalent.

0.0 Satz. *Für jede geordnete Menge $(P, \leq)$ sind äquivalent:*
(1) (**Maximalbedingung**) *Jede nichtleere Teilmenge von P enthält ein maximales Element.*
(2) (**Aufsteigende-Ketten-Bedingung**) *Zu jeder aufsteigenden Kette $p_1 \leq p_2 \leq p_3 \leq \ldots$ von Elementen in P existiert ein $k \in \mathbb{N}$ mit $p_k = p_{k+1} = \ldots$.*

Beweis. (1) $\Longrightarrow$ (2): Sei (1) erfüllt und $p_1 \leq p_2 \leq p_3 \ldots$ eine aufsteigende Kette von Elementen in P. Dann existiert in der Menge $\{p_1, p_2, p_3, \ldots\}$ ein maximales Element p_k. Folglich gilt: $p_k = p_{k+1} = \ldots$.
(2) $\Longrightarrow$ (1): Sei (2) erfüllt und $\emptyset \neq Q \subseteq P$. Wähle $p_1 \in Q$. Ist p_1 maximal, so sind wir fertig. Andernfalls existiert ein $p_2 \in Q$ mit $p_1 < p_2$. Ist p_2 maximal, so sind wir fertig. Andernfalls existiert ein $p_3 \in Q$ mit $p_1 < p_2 < p_3$. So fahren wir fort. Wegen (2) geht das nicht ewig.

Analog ist die **Minimalbedingung** zur **Absteigende-Ketten-Bedingung** äquivalent.

Eine **Topologie** auf einer Menge M ist eine Menge $\mathfrak{T}$ von Teilmengen von M mit folgenden Eigenschaften:

- $\emptyset, M \in \mathfrak{T}$;
- $\mathfrak{U} \subseteq \mathfrak{T} \Longrightarrow \bigcup_{U \in \mathfrak{U}} U \in \mathfrak{T}$;
- $U_1, \ldots, U_n \in \mathfrak{T} \Longrightarrow U_1 \cap \ldots \cap U_n \in \mathfrak{T}$.

Das bedeutet, dass $\mathfrak{T}$ gegenüber endlichen Durchschnitten und beliebigen Vereinigungen abgeschlossen ist. Das Paar $(M, \mathfrak{T})$ heißt dann **topologischer Raum**. Ist $\mathfrak{T}$ aus dem Zusammenhang klar, so sagt man auch kurz: M ist ein topologischer Raum. Ggf. heißen die Elemente in $\mathfrak{T}$ die **offenen** Teilmengen von M.

Eine Teilmenge $A \subseteq M$ mit $M \setminus A \in \mathfrak{T}$ heißt **abgeschlossen** in M (bzgl. $\mathfrak{T}$). Dann gilt:

- $\emptyset, M$ sind abgeschlossen in M;
- Für jede (nichtleere) Menge $\mathfrak{A}$ abgeschlossener Teilmengen von M ist auch $\bigcap_{A \in \mathfrak{A}} A$ abgeschlossen in M;
- Für abgeschlossene Teilmengen $A_1, \ldots A_n$ von M ist auch $A_1 \cup \ldots \cup A_n$ abgeschlossen in M.

Für eine beliebige Teilmenge $N \subseteq M$ ist der Durchschnitt $\overline{N}$ aller abgeschlossenen Teilmengen von M, die N enthalten, eine abgeschlossene Teilmenge von M; diese heißt **Abschluss** von N in M (bzgl. $\mathfrak{T}$). Im Fall $\overline{N} = M$ heißt N **dicht** in M.

Für jeden topologischen Raum $(M, \mathfrak{T})$ und jede Teilmenge $N \subseteq M$ ist

$$\mathfrak{U} := \{T \cap N : T \in \mathfrak{T}\}$$

eine Topologie auf N, die von $\mathfrak{T}$ **induzierte** Topologie; ggf. heißt $(N, \mathfrak{U})$ **topologischer Unterraum** von $(M, \mathfrak{T})$. Also ist eine Teilmenge B von N genau dann abgeschlossen in N, wenn eine abgeschlossene Teilmenge A von M mit $B = A \cap N$ existiert.

Eine Abbildung $f : M \longrightarrow M'$ zwischen topologischen Räumen $(M, \mathfrak{T})$, $(M', \mathfrak{T}')$ mit $f^{-1}(U') \in \mathfrak{T}$ für alle $U' \in \mathfrak{T}'$ heißt **stetig**. Das bedeutet, dass Urbilder offener Mengen wieder offen sind. Dazu ist äquivalent, dass die Urbilder abgeschlossener Mengen wieder abgeschlossen sind.

Für jeden topologischen Unterraum N von M ist offenbar die Inklusionsabbildung $i : N \longrightarrow M$ stetig.

Ist in der obigen Situation f bijektiv und sind f, f^{-1} beide stetig, so heißt f **Homöomorphismus**. Ggf. gilt für jede Teilmenge $X \subseteq M$: $X \in \mathfrak{T} \Longleftrightarrow f(X) \in \mathfrak{T}'$. Existiert ein Homöomorphismus $f : M \longrightarrow M'$ zwischen topologischen Räumen M, M', so nennt man M und M' **homöomorph** und schreibt: $M \sim M'$. Dann ist $\sim$ eine Äquivalenzrelation.

Sei wieder $(M, \mathfrak{T})$ ein topologischer Raum. Eine Teilmenge $\mathfrak{B} \subseteq \mathfrak{T}$ heißt **Basis** von $\mathfrak{T}$, wenn sich jedes $T \in \mathfrak{T}$ als Vereinigung von Elementen in $\mathfrak{B}$ schreiben lässt. Sei jetzt $(N, \mathfrak{U})$ auch ein topologischer Raum. Eine Abbildung $f : N \longrightarrow M$ ist genau dann stetig, wenn $f^{-1}(B) \in \mathfrak{U}$ für alle $B \in \mathfrak{B}$ gilt.

Ein topologischer Raum $(M, \mathfrak{T})$ heißt **quasikompakt**, falls zu jeder Teilmenge $\mathfrak{S} \subseteq \mathfrak{T}$ mit $M = \bigcup_{S \in \mathfrak{S}} S$ Elemente $S_1, \ldots, S_n \in \mathfrak{S}$ mit $M = S_1 \cup \ldots \cup S_n$ existieren. Das bedeutet, dass jede offene Überdeckung von M eine endliche Teilüberdeckung hat. Man zeigt leicht, dass jede abgeschlossene Teilmenge eines quasikompakten topologischen Raums wieder quasikompakt (bzgl. der induzierten Topologie) ist.

Ein topologischer Raum $(M, \mathfrak{T})$ heißt T_0**-Raum**, wenn für alle $x, y \in M$ mit $x \neq y$ gilt: $\overline{\{x\}} \neq \overline{\{y\}}$. Man nennt $(M, \mathfrak{T})$ einen T_1**-Raum**, wenn für alle $x, y \in M$ mit $x \neq y$ gilt: $\exists U, V \in \mathfrak{T} : x \in U \setminus V, y \in V \setminus U$. Man nennt $(M, \mathfrak{T})$ einen T_2**-Raum** (**Hausdorff-Raum**), wenn für alle $x, y \in M$ mit $x \neq y$ gilt: $\exists U, V \in \mathfrak{T} : x \in U, y \in V, U \cap V = \emptyset$. Man zeigt leicht, dass jeder T_1-Raum ein T_0-Raum und dass jeder T_2-Raum ein T_1-Raum ist.

Ein topologischer Raum $(M, \mathfrak{T})$ mit $M \neq \emptyset$ heißt **zusammenhängend**, falls keine echten abgeschlossenen Teilmengen M_1, M_2 von M mit $M = M_1 \cup M_2$ und $M_1 \cap M_2 = \emptyset$ existieren. Er heißt **irreduzibel**, falls keine echten abgeschlossenen Teilmengen M_1, M_2 von M mit $M = M_1 \cup M_2$ existieren. Offenbar sind einelementige topologische Räume stets irreduzibel. Ferner ist jeder irreduzible topologische Raum auch zusammenhängend; die Umkehrung gilt i.a. nicht.

0.1 Satz. *Für einen nichtleeren topologischen Raum $(M, \mathfrak{T})$ sind äquivalent:*
(1) M ist irreduzibel;
(2) $U, U' \in \mathfrak{T} \wedge U \neq \emptyset \neq U' \Longrightarrow U \cap U' \neq \emptyset$;
(3) $\emptyset \neq U \in \mathfrak{T} \Longrightarrow \overline{U} = M$.

Beweis. (1) $\Longrightarrow$ (2): Sei M irreduzibel, und seien $U, U' \in \mathfrak{T}$ mit $U \cap U' = \emptyset$. Dann ist $M = M \setminus \emptyset = M \setminus (U \cap U') = (M \setminus U) \cup (M \setminus U')$ mit abgeschlossenen Teilmengen $M \setminus U, M \setminus U'$ von M. Also ist $M \setminus U = M$ oder $M \setminus U' = M$, d.h. $U = \emptyset$ oder $U' = \emptyset$.
(2) $\Longrightarrow$ (3): Sei (2) erfüllt und $U \in \mathfrak{T}$ mit $\overline{U} \neq M$. Dann ist $M \setminus \overline{U} \in \mathfrak{T}$ mit $U \cap (M \setminus \overline{U}) = \emptyset$. Wegen (2) und $M \setminus \overline{U} \neq \emptyset$ folgt $U = \emptyset$.
(3) $\Longrightarrow$ (1): Sei (3) erfüllt und $M = M_1 \cup M_2$ mit abgeschlossenen Teilmengen M_1, M_2 von M. Dabei sei $M_1 \neq M$, d.h. $\emptyset \neq M \setminus M_1 \in \mathfrak{T}$. Wegen (3) ist dann $\overline{M \setminus M_1} = M$. Wegen $M \setminus M_1 \subseteq M_2$ ist also auch $M = \overline{M \setminus M_1} \subseteq M_2$, d.h. $M = M_2$.

Die Eigenschaft (3) besagt, dass jede nichtleere offene Teilmenge von M dicht ist.
Eine Teilmenge N eines topologischen Raums M heißt **irreduzibel**, wenn sie als topologischer Raum mit der induzierten Topologie irreduzibel ist.

0.2 Satz. *Für topologische Räume M, N und stetige Abbildungen $f : M \longrightarrow N$ gilt: M irreduzibel $\Longrightarrow$ $f(M)$ irreduzibel.*

Beweis. Sei $f(M) = B_1 \cup B_2$ mit abgeschlossenen Teilmengen B_1, B_2 von $f(M)$. Für $i = 1, 2$ existiert dann eine abgeschlossene Teilmenge A_i von N mit $B_i = A_i \cap f(M)$. Also ist $M = f^{-1}(f(M)) = f^{-1}(B_1 \cup B_2) = f^{-1}(A_1 \cup A_2) = f^{-1}(A_1) \cup f^{-1}(A_2)$ mit abgeschlossenen Teilmengen $f^{-1}(A_1), f^{-1}(A_2)$ von M. Ist M irreduzibel, so existiert ein $i \in \{1, 2\}$ mit $M = f^{-1}(A_i)$. Daher ist $f(M) \subseteq A_i \cap f(M) = B_i$, d.h. $f(M) = B_i$.

0.3 Satz. *Eine Teilmenge N eines topologischen Raums M ist genau dann irreduzibel, wenn ihr Abschluss $\overline{N}$ in M irreduzibel ist.*

Beweis. "$\Longrightarrow$": Sei $\overline{N} = M_1 \cup M_2$ mit abgeschlossenen Teilmengen M_1, M_2 von $\overline{N}$. Dann ist $N = (M_1 \cap N) \cup (M_2 \cap N)$ mit abgeschlossenen Teilmengen $M_1 \cap N, M_2 \cap N$ von N. Ist N irreduzibel, so folgt: $N = M_i \cap N \subseteq M_i$ für ein $i \in \{1, 2\}$. Also ist $\overline{N} \subseteq M_i$, d.h. $M_i = \overline{N}$.
"$\Longleftarrow$": Sei $N = N_1 \cup N_2$ mit abgeschlossenen Teilmengen N_1, N_2 von N. Für $i = 1, 2$ existiert dann eine abgeschlossene Teilmenge M_i von M mit $N_i = M_i \cap N$. Also ist $N = N_1 \cup N_2 \subseteq M_1 \cup M_2$. Da $M_1 \cup M_2$ abgeschlossen in M ist, folgt $\overline{N} \subseteq M_1 \cup M_2$, d.h. $\overline{N} = (M_1 \cap \overline{N}) \cup (M_2 \cap \overline{N})$ mit abgeschlossenen Teilmengen $M_1 \cap \overline{N}$, $M_2 \cap \overline{N}$ von $\overline{N}$. Ist $\overline{N}$ irreduzibel, so folgt $\overline{N} = M_i \cap \overline{N} \subseteq M_i$ für ein $i \in \{1, 2\}$. Daher ist $N \subseteq M_i \cap N = N_i$, d.h. $N = N_i$.

0.4 Satz. *Jede irreduzible Teilmenge N eines topologischen Raums M ist in einer maximalen irreduziblen Teilmenge von M enthalten.*

Beweis. Die Menge $\mathfrak{X}$ aller irreduziblen Teilmengen von M, die N enthalten, ist nichtleer und durch "$\subseteq$" geordnet. Sei $\mathfrak{Y}$ eine nichtleere total geordnete Teilmenge von $\mathfrak{X}$. Dann ist $N \subseteq \bigcup_{Y \in \mathfrak{Y}} Y =: S$. Wir zeigen, dass S irreduzibel ist. Dazu seien U, U' nichtleere offene Teilmengen von S. Wir wählen $u \in U$ und $u' \in U'$. Wegen $u, u' \in S$ existieren $Y, Y' \in \mathfrak{Y}$ mit $u \in Y$ und $u' \in Y'$. Dabei sei o.B.d.A. $Y' \subseteq Y$, also $u, u' \in Y$. Dann sind $U \cap Y$

und $U' \cap Y$ nichtleere offene Teilmengen von Y. Da Y irreduzibel ist, folgt mit Satz 0.1: $U \cap U' \cap Y \neq \emptyset$; insbesondere ist $U \cap U' \neq \emptyset$.
Dies zeigt, dass S irreduzibel ist. Also ist S eine obere Schranke von $\mathfrak{Y}$ in $\mathfrak{X}$. Mit Zorns Lemma folgt, dass $\mathfrak{X}$ maximale Elemente (bzgl. $\subseteq$) enthält. Das bedeutet, dass N in einer maximalen irreduziblen Teilmenge von M enthalten ist.

Die maximalen irreduziblen Teilmengen eines topologischen Raums M heißen **irreduzible Komponenten** von M. Aus Satz 0.3 folgt, dass die irreduziblen Komponenten von M stets abgeschlossene Teilmengen von M mit Vereinigung M sind.

Ein topologischer Raum M heißt **noethersch**, wenn er die **Minimalbedingung** für abgeschlossene Teilmengen erfüllt. Das bedeutet, dass jede nichtleere Menge abgeschlossener Teilmengen von M ein minimales Element enthält. Dies ist genau dann der Fall, wenn M die **Absteigende-Ketten-Bedingung** für abgeschlossene Teilmengen erfüllt. Das bedeutet, dass zu jeder Kette $A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots$ abgeschlossener Teilmengen von M ein $i \in \mathbb{N}$ mit $A_i = A_{i+1} = \ldots$ existiert. Natürlich ist die Minimalbedingung (bzw. die Absteigende-Ketten-Bedingung) für abgeschlossene Teilmengen äquivalent zur **Maximalbedingung** (bzw. zur **Aufsteigende-Ketten-Bedingung**) für offene Teilmengen.

0.5 Satz. *Für jeden noetherschen topologischen Raum M gilt:*
(i) Jeder topologische Unterraum N von M ist noethersch.
(ii) M ist quasikompakt.
(iii) M hat nur endlich viele irreduzible Komponenten $M_1, \ldots M_n$.

Beweis. (i) Sei $B_1 \supseteq B_2 \supseteq B_3 \supseteq \ldots$ eine Kette abgeschlossener Teilmengen von N. Für $i \in \mathbb{N}$ existiert dann eine abgeschlossene Teilmenge A_i von M mit $B_i = A_i \cap N$. Dann ist $A_1 \supseteq A_1 \cap A_2 \supseteq A_1 \cap A_2 \cap A_3 \supseteq \ldots$ eine Kette abgeschlossener Teilmengen von M. Da M noethersch ist, existiert ein $i \in \mathbb{N}$ mit $A_1 \cap \ldots \cap A_i = A_1 \cap \ldots \cap A_i \cap A_{i+1} = \ldots$. Der Durchschnitt mit N ergibt $B_i = B_{i+1} = \ldots$.
(ii) Sei $\mathfrak{U}$ eine offene Überdeckung von M. Dann ist $\emptyset = \bigcap_{U \in \mathfrak{U}} M \setminus U$ mit abgeschlossenen Teilmengen $M \setminus U$ von M. Da M noethersch ist, enthält die Menge $\mathfrak{A}$ der Durchschnitte von endlich vielen der Mengen $M \setminus U$ mit $U \in \mathfrak{U}$ ein minimales Element Z. Offensichtlich ist $Z = \emptyset$. Also ist M eine endliche Vereinigung von Mengen in $\mathfrak{U}$.
(iii) Sei $\mathfrak{A}$ die Menge aller abgeschlossenen Teilmengen von M mit unendlich vielen irreduziblen Komponenten. Wir nehmen $\mathfrak{A} \neq \emptyset$ an. Da M noethersch ist, enthält $\mathfrak{A}$ ein minimales Element Z. Dann ist Z nicht irreduzibel, also $Z = Z_1 \cup Z_2$ mit echten abgeschlossenen Teilmengen Z_1, Z_2 von Z. Dabei sind Z_1, Z_2 auch abgeschlossen in M. Nach Wahl von Z haben Z_1, Z_2 nur endlich viele irreduzible Komponenten. Daher sind Z_1, Z_2, Z jeweils Vereinigungen endlich vieler irreduzibler Teilmengen. Daher ist Z eine Vereinigung endlich vieler irreduzibler Komponenten $K_1, \ldots, K_n$.
Ist jetzt K eine beliebige irreduzible Komponente von Z, so ist $K = (K \cap K_1) \cup \ldots \cup (K \cap K_n)$ mit abgeschlossenen Teilmengen $K \cap K_1, \ldots, K \cap K_n$. Da K irreduzibel ist, existiert ein $i \in \{1, \ldots, n\}$ mit $K = K \cap K_i \subseteq K_i$, d.h. $K = K_i$. Dies zeigt, dass $K_1, \ldots, K_n$ die einzigen irreduziblen Komponenten von Z sind.

Bemerkung. Der Beweis zeigt, dass auch $M_i \not\subseteq \bigcup_{j \neq i} M_j$ für $i = 1, \ldots, n$ gilt.

0.6 Satz. *Eine offene Teilmenge U eines nichtleeren noetherschen topologischen Raums M ist genau dann dicht in M, wenn sie jede irreduzible Komponente von M schneidet.*

Beweis. Sei M ein nichtleerer noetherscher topologischer Raum mit irreduziblen Komponenten $M_1, \ldots, M_n$.
"$\Longrightarrow$": Sei U eine offene dichte Teilmenge von M. Im Fall $U \cap M_1 = \emptyset$ wäre $U \subseteq M_2 \cup \ldots \cup M_n$, also auch $M_1 \subseteq M = \overline{U} \subseteq M_2 \cup \ldots \cup M_n$. Dies steht im Widerspruch zu der obigen Bemerkung.
"$\Longleftarrow$": Sei U eine offene Teilmenge von M mit $U \cap M_i \neq \emptyset$ für $i = 1, \ldots, n$. Für $i = 1, \ldots, n$ ist dann $\overline{U} \cap M_i$ abgeschlossen in M_i und $U \cap M_i \subseteq \overline{U} \cap M_i$. Da $U \cap M_i$ offen und nach Satz 0.1 dicht in M_i ist, folgt $M_i = \overline{U} \cap M_i \subseteq \overline{U}$. Also ist $M = M_1 \cup \ldots \cup M_n \subseteq \overline{U}$, d.h. $\overline{U} = M$.

Die **Krulldimension** $\mathrm{Dim}(M)$ eines topologischen Raums M ist definiert als das Supremum der **Längen** n aller Ketten $M_0 \subset M_1 \subset \ldots \subset M_n$ irreduzibler abgeschlossener Teilmengen $M_0, \ldots, M_n$ von M. Der Fall $\mathrm{Dim}(M) = \infty$ ist möglich, auch wenn M noethersch ist.

0.7 Satz. *Für jeden topologischen Raum M ist* $\mathrm{Dim}(M)$ *das Supremum der Krulldimensionen der irreduziblen Komponenten von M.*

Beweis. Jede Kette $B_0 \subset B_1 \subset \ldots \subset B_n$ irreduzibler abgeschlossener Teilmengen einer irreduziblen Komponente K von M ist auch eine Kette irreduzibler abgeschlossener Teilmengen von M. Daher ist $n \leq \mathrm{Dim}(M)$. Folglich ist auch $\mathrm{Dim}(K) \leq \mathrm{Dim}(M)$.
Ist umgekehrt $A_0 \subset A_1 \subset \ldots \subset A_m$ eine Kette irreduzibler abgeschlossener Teilmengen von M, so existiert eine irreduzible Komponente C von M mit $A_m \subseteq C$. Daher ist $A_0 \subset A_1 \subset \ldots \subset A_m$ auch eine Kette irreduzibler abgeschlossener Teilmengen von C; insbesondere ist $m \leq \mathrm{Dim}(C) \leq \sup\{\mathrm{Dim}(K) : K \text{ irreduzible Komponente von } M\}$, und die Behauptung folgt.

1. Ringe

In dieser Vorlesung sind **Ringe** stets kommutativ, assoziativ und unitär, d.h. sie haben ein Einselement 1. Der **Nullring** $\{0\} =: 0$ ist zugelassen, aber nicht sehr aufregend. Wichtige Beispiele für uns sind die Polynomringe $\mathbb{Z}[X_1, \ldots, X_n]$ und $K[X_1, \ldots, X_n]$ für einen Körper K sowie Ringe, die sich leicht daraus konstruieren lassen. Ziel der Vorlesung ist u.a., Grundlagen für die Algebraische Geometrie und die Algebraische Zahlentheorie bereitzustellen. Für Ringe $R_1, \ldots, R_n$ ist auch ihr **direktes Produkt**

$$R_1 \times \cdots \times R_n = \{(r_1, \ldots, r_n) : r_1 \in R_1, \ldots, r_n \in R_n\}$$

ein Ring mit

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$$

$(a_1, b_1 \in R_1, \ldots, a_n, b_n \in R_n)$. Eine Teilmenge S eines Rings R mit $1 \in S$ und $a-b, a\cdot b \in S$ für alle $a, b \in S$ heißt **Teilring** von R. Ggf. ist S selbst ein Ring, und man nennt R auch **Ringerweiterung** von S. Zum Beispiel kann man den Polynomring $R[X_1, \ldots, X_n]$ und den Potenzreihenring $R[[X_1, \ldots, X_n]]$ als Ringerweiterungen von R ansehen.

Eine nichtleere Teilmenge $I \subseteq R$ mit $ax + by \in I$ für alle $a, b \in R$, $x, y \in I$ heißt **Ideal** von R. Wir schreiben $I \trianglelefteq R$, im Fall $I \neq R$ auch $I \triangleleft R$. Für jede Teilmenge $X \subseteq R$ ist

$$(X) := \{\sum_{i=1}^{n} a_i x_i : a_1, \ldots, a_n \in R,\ x_1, \ldots, x_n \in X,\ n \in \mathbb{N}_0\} \trianglelefteq R;$$

man nennt (X) das von X **erzeugte** Ideal von R. Im Spezialfall $X = \{x_1, \ldots, x_n\}$ ist

$$(x_1, \ldots, x_n) := (\{x_1, \ldots, x_n\}) = \{\sum_{i=1}^{n} a_i x_i : a_1, \ldots, a_n \in R\}.$$

(In der Regel wird aus dem Zusammenhang klar sein, ob mit $(x_1, \ldots, x_n)$ das n-Tupel mit den Komponenten $x_1, \ldots, x_n$ oder das von $x_1, \ldots, x_n$ erzeugte Ideal gemeint ist.) Für $x \in R$ heißt $(x) := \{ax : a \in R\} =: Rx$ das von x erzeugte **Hauptideal**.

Für jede nichtleere Menge $\mathfrak{I}$ von Idealen von R sind auch $\bigcap_{I\in\mathfrak{I}} I$ und $\sum_{I\in\mathfrak{I}} I$ Ideale in R; dabei besteht $\sum_{I\in\mathfrak{I}} I$ aus den Elementen $x_1 + \cdots + x_n$ mit $x_1 \in I_1, \ldots, x_n \in I_n$ und $I_1, \ldots, I_n \in \mathfrak{I}$.

Für Ideale $I, J \trianglelefteq R$ ist auch das Produkt $IJ \trianglelefteq R$; dabei besteht IJ aus den Elementen $\sum_{k=1}^{n} x_k y_k$ mit $x_1, \ldots, x_n \in I$, $y_1, \ldots, y_n \in J$ und $n \in \mathbb{N}_0$. I.A. ist aber

$$IJ \neq \{xy : x \in I, y \in J\}.$$

Für jedes weitere Ideal $K \trianglelefteq R$ ist $(IJ)K = I(JK)$; man schreibt dafür auch kurz IJK. Für $n \in \mathbb{N}_0$ definiert man die n-te Potenz I^n induktiv durch $I^0 := R$ und $I^n := I^{n-1}I$ für $n \in \mathbb{N}$.

Ist $I^m = 0$ für ein $m \in \mathbb{N}$, so heißt I **nilpotent**. Man beachte, dass genau dann $I^m = 0$ gilt, wenn $x_1 \cdots x_m = 0$ für alle $x_1, \ldots, x_m \in I$ gilt. Insbesondere ist dann $x^m = 0$ für alle $x \in I$; aber i.A. ist diese Eigenschaft schwächer als die Bedingung $I^m = 0$.

Für nilpotente Ideale $I, J \trianglelefteq R$ ist auch $I + J$ nilpotent; denn sind $m, n \in \mathbb{N}$ mit $I^m = 0 = I^n$, so ist $(I+J)^{m+n}$ in der Summe der Ideale $K_1 \cdots K_{m+n}$ mit $K_1, \ldots, K_{m+n} \in \{I, J\}$ enthalten. Da jedes solche Produkt mindestens m Faktoren I oder mindestens n Faktoren J enthält, ist es in $I^m = 0$ oder $J^n = 0$ enthalten. Also ist $(I + J)^{m+n} = 0$.

Für $I \trianglelefteq R$ ist $R/I := \{a + I : a \in R\}$, die Menge aller **Restklassen**

$$a + I := \{a + x : x \in I\} \qquad (a \in R),$$

ein Ring mit

$$(a + I) + (b + I) := (a + b) + I \quad \text{und} \quad (a + I) \cdot (b + I) := ab + I$$

$(a, b \in R)$; dieser heißt **Restklassenring** von R nach I.

Sind R, S Ringe, so heißt eine Abbildung $f : R \longrightarrow S$ mit

$$f(1_R) = 1_S \quad \text{und} \quad f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b)$$

$(a, b \in R)$ **(Ring-)Homomorphismus**. Ggf. ist der **Kern**

$$\mathrm{Ker}(f) := \{x \in R : f(x) = 0\}$$

von f ein Ideal in R, und das **Bild** $\mathrm{Bld}(f) := \{f(a) : a \in R\} = f(R)$ von f ist ein Teilring von S. Wie üblich definiert man **Monomorphismen**, **Epimorphismen**, **Isomorphismen**, **Endomorphismen** und **Automorphismen** von Ringen. Die **Isomorphie** von Ringen bezeichnen wir mit dem Symbol $\cong$. Wir setzen den **Homomorphiesatz**, die **Isomorphiesätze** und den **Chinesischen Restsatz** für Ringe als bekannt voraus.

Ein Element a eines Rings R heißt **Nullteiler**, falls ein Element $b \in R\backslash\{0\}$ mit $ab = 0$ existiert. Die Menge aller Nullteiler in R bezeichnen wir mit $\mathrm{Z}(R)$ (zero-divisor). Außer im Fall $R = 0$ ist also $0 \in \mathrm{Z}(R)$. Ist $\mathrm{Z}(R) = \{0\}$ (also insbesondere $R \neq 0$), so heißt R **Integritätsbereich**.

Ein Element u eines Rings R heißt **invertierbar** oder **Einheit**, falls ein $v \in R$ mit $uv = 1$ existiert. Dann ist

$$R^\times := \{u \in R : u \text{ Einheit}\}$$

eine Gruppe bzgl. der Multiplikation, die **Einheitengruppe** von R.

Ein Element $x \in R$ heißt **nilpotent**, falls ein $n \in \mathbb{N}$ mit $x^n = 0$ existiert. Ggf. ist $1 - x \in R^\times$; denn

$$(1-x)(\sum_{i=0}^{n} x^i) = \sum_{i=0}^{n} x^i - \sum_{i=1}^{n+1} x^i = 1 - x^{n+1} = 1.$$

Das **Nilradikal**

$$\mathrm{nil}(R) := \{x \in R : x \text{ nilpotent}\}$$

von R ist ein Ideal in R; denn sind $x, y \in R$ und $m, n \in \mathbb{N}$ mit $x^m = 0 = y^n$, so ist

$$(x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i} = 0,$$

weil stets $i \geq m$ (d.h. $x^i = 0$) oder $m + n - i > n$ (d.h. $y^{m+n-i} = 0$) ist.

Ein Ideal $I \trianglelefteq R$ mit $I \subseteq \mathrm{nil}(R)$ heißt **Nilideal**. Also ist $\mathrm{nil}(R)$ das größte Nilideal in R. Im Fall $\mathrm{nil}(R) = 0$ nennt man R **reduziert**. Man zeigt leicht, dass $R/\mathrm{nil}(R)$ für jeden Ring R reduziert ist.

Offenbar ist jedes nilpotente Ideal auch ein Nilideal. Die Umkehrung gilt i.A. nicht.

Ein Element e eines Rings R mit $e^2 = e$ heißt **idempotent** (oder ein **Idempotent**). Ggf. ist auch $1 - e$ idempotent (wegen $(1-e)^2 = 1 - 2e + e^2 = 1 - e$), und $e(1-e) = 0$. Daher ist

$$R = Re \oplus R(1-e)$$

mit Idealen $Re, R(1-e)$ von R; denn einerseits ist $r = r1 = r(e+1-e) = re + r(1-e)$ für $r \in R$, und andererseits gilt für $s \in Re \cap R(1-e)$: $s = se = se(1-e) = s0 = 0$. Ferner sind Re und $R(1-e)$ selbst Ringe mit Einselementen e bzw. $1-e$ (aber nach unserer Konvention nicht unbedingt Teilringe von R), und

$$f : Re \times R(1-e) \longrightarrow R, \quad (x, y) \longmapsto x + y,$$

ist ein Ringisomorphismus. Stets sind $0, 1$ Idempotente in R. Enthält R genau zwei Idempotente (nämlich 0 und 1), so heißt R **zusammenhängend**. Der Nullring ist also nicht zusammenhängend. Dagegen ist jeder Integritätsbereich zusammenhängend.

1.1 Satz. (Heben von Idempotenten)
Zu jedem Nilideal $I \trianglelefteq R$ und jedem Idempotent $\epsilon \in R/I$ existiert genau ein Idempotent $e \in R$ mit $\epsilon = e + I$. So erhält man eine Bijektion zwischen der Menge der Idempotente in R und der Menge der Idempotente in R/I.

Beweis. Sei $u \in R$ mit $\epsilon = u + I$, und sei $v := 1 - u$. Wegen $u^2 + I = \epsilon^2 = \epsilon = u + I$ ist $z := u - u^2 \in I$. Sei $n \in \mathbb{N}$ mit $0 = z^n = (u(1-u))^n = u^n v^n$. Dann ist

$$1 = 1^{2n} = (u+v)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} u^i v^{2n-i}.$$

Wir setzen $e := \sum_{j=n+1}^{2n} \binom{2n}{j} u^j v^{2n-j}$. Dann ist $1 - e = \sum_{i=0}^{n} \binom{2n}{i} u^i v^{2n-i}$ und

$$e(1-e) = \sum_{j=n+1}^{2n} \sum_{i=0}^{n} \binom{2n}{j} \binom{2n}{i} u^j v^{2n-j} u^i v^{2n-i} = 0;$$

denn jeder Summand verschwindet wegen $j > n$ und $2n - i \geq n$. Also ist $e = e^2$ und

$$e + I = \sum_{j=n+1}^{2n} \binom{2n}{j} \epsilon^j (1-\epsilon)^{2n-j} = \epsilon^{2n}(1-\epsilon)^0 = \epsilon.$$

Damit ist die Existenz gezeigt. Zum Beweis der Eindeutigkeit sei $y \in I$ mit

$$e + y = (e+y)^2 = e^2 + 2ey + y^2,$$

d.h. $y^2 = (1-2e)y$ und $y^3 = (1-2e)y^2 = (1-2e)^2 y = (1 - 4e + 4e^2)y = y$. Da y nilpotent ist, folgt: $y = 0$.

Bemerkung. Der Satz gilt nicht für beliebige Ideale.

Beispiel. In $\mathbb{Z}$ sind 0 und 1 die einzigen Idempotente; aber in $\mathbb{Z}/6\mathbb{Z}$ sind $0 + 6\mathbb{Z}$, $1 + 6\mathbb{Z}$, $3 + 6\mathbb{Z}$ und $4 + 6\mathbb{Z}$ Idempotente.

2. Moduln

Sei R ein Ring. Ein **R-Modul** ist eine abelsche Gruppe $(V,+)$, auf der eine Multiplikation mit Skalaren

$$R \times V \longrightarrow V, \quad (a,v) \longmapsto av,$$

mit folgenden Eigenschaften definiert ist:

- $a(v+w) = av + aw$
- $(a+b)v = av + bv$
- $(ab)v = a(bv)$
- $1v = v$

($a, b \in R$, $v, w \in V$). Für jeden Körper K sind also die K-Moduln genau die K-Vektorräume.

Eine nichtleere Teilmenge U eines beliebigen R-Moduls V mit $au + bv \in U$ für alle $a, b \in R$, $u, v \in U$ heißt **Untermodul** von V. Ggf. ist U selbst ein R-Modul, und die Menge

$$V/U := \{v + U : v \in V\}$$

der **Nebenklassen** $v + U := \{v + u : u \in U\}$ ($v \in V$) ist ein R-Modul mit

$$(v+U) + (w+U) := (v+w) + U \quad \text{und} \quad a(v+U) = av + U$$

($v, w \in V$, $a \in R$); dieser heißt **Faktormodul** von V nach U.

Der **Nullmodul** $0 := \{0\}$ ist sicher ein R-Modul. Den Ring R selbst kann man in offensichtlicher Weise als R-Modul betrachten; dieser heißt **regulärer** R-Modul. Seine Untermoduln sind genau die Ideale in R.

Für jede (nichtleere) Familie $(V_i)_{i \in I}$ von R-Moduln ist auch ihr **direktes Produkt**

$$\mathop{\mathbf{X}}_{i \in I} V_i := \prod_{i \in I} V_i := \{(v_i)_{i \in I} : v_i \in V_i \text{ für alle } i \in I\}$$

ein R-Modul mit

$$(v_i)_{i \in I} + (w_i)_{i \in I} := (v_i + w_i)_{i \in I} \quad \text{und} \quad a(v_i)_{i \in I} := (av_i)_{i \in I}$$

für $(v_i)_{i \in I}, (w_i)_{i \in I} \in \prod_{i \in I} V_i$, $a \in R$. Im Fall $I = \{1, \ldots, n\}$ schreibt man das direkte Produkt auch in der Form

$$V_1 \times \cdots \times V_n = \{(v_1, \ldots, v_n) : v_1 \in V_1, \ldots, v_n \in V_n\}.$$

Ist $V_1 = \ldots = V_n =: V$, so schreibt man V^n statt $V \times \cdots \times V$. Insbesondere haben wir den R-Modul $R^n = R \times \cdots \times R$.

Für jede (nichtleere) Familie $(V_i)_{i \in I}$ von R-Moduln bilden die Elemente $(v_i)_{i \in I}$ mit $|\{i \in I : v_i \neq 0\}| < \infty$ einen Untermodul $\coprod_{i \in I} V_i$ von $\prod_{i \in I} V_i$, den man als **Koprodukt** von $(V_i)_{i \in I}$ bezeichnet. Ist I endlich, so ist also $\coprod_{i \in I} V_i = \prod_{i \in I} V_i$.

Für jede (nichtleere) Familie $(U_i)_{i \in I}$ von Untermoduln eines R-Moduls V sind auch ihr **Durchschnitt** $\bigcap_{i \in I} U_i$ und ihre **Summe** $\sum_{i \in I} U_i$ Untermoduln von V; dabei besteht $\sum_{i \in I} U_i$ aus allen Elementen der Form $u_{i_1} + \cdots + u_{i_k}$ mit $i_1, \ldots, i_k \in I$ und $u_{i_1} \in$

$U_{i_1}, \ldots, u_{i_k} \in U_{i_k}$ $(k \in \mathbb{N}_0)$. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man statt $\sum_{i \in I} U_i$ auch

$$U_1 + \cdots + U_n = \{u_1 + \cdots + u_n : u_1 \in U_1, \ldots, u_n \in U_n\}.$$

Dabei sind die folgenden Aussagen äquivalent:

(1) Jedes Element $u \in U_1 + \cdots + U_n$ lässt sich in der Form $u = u_1 + \cdots + u_n$ mit *eindeutig bestimmten* Elementen $u_1 \in U_1, \ldots, u_n \in U_n$ schreiben.

(2) Aus $u_1 + \cdots + u_n = 0$ mit Elementen $u_1 \in U_1, \ldots, u_n \in U_n$ folgt stets $u_1 = \ldots = u_n = 0$.

(3) $U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_n) = 0$ für $i = 1, \ldots, n$.

(4) $U_i \cap (U_1 + \cdots + U_{i-1}) = 0$ für $i = 2, \ldots, n$.

Ggf. spricht man von einer **direkten Summe** und schreibt

$$U_1 + \cdots + U_n =: U_1 \oplus \cdots \oplus U_n.$$

Für Untermoduln U, U' eines R-Moduls V gilt also genau dann $V = U \oplus U'$, wenn $V = U + U'$ und $U \cap U' = 0$ ist. Ggf. heißt U' ein **Komplement** von U in V. (I.a. ist U' durch U nicht eindeutig bestimmt.)

Oft ist **Dedekinds Lemma** nützlich. Dieses besagt, dass für Untermoduln A, B, C eines R-Moduls V stets gilt:

$$A \subseteq C \Longrightarrow A + (B \cap C) = (A + B) \cap C;$$

Der Beweis ist Routine.

Für jedes Ideal $I \trianglelefteq R$ und jeden R-Modul V ist

$$IV := \{\sum_{j=1}^{n} x_j v_j : x_1, \ldots, x_n \in I;\ v_1, \ldots, v_n \in V;\ n \in \mathbb{N}_0\} \subseteq V$$

ein Untermodul. Ggf. wird der Faktormodul V/IV zu einem R/I-Modul durch

$$(a + I)(v + IV) := av + IV \qquad (a \in R,\ v \in V).$$

Eine Abbildung $f : V \longrightarrow W$ zwischen R-Moduln V, W mit $f(ax + by) = af(x) + bf(y)$ für alle $a, b \in R$, $x, y \in V$ heißt ein R-**Homomorphismus** (oder R-**linear**). Ggf. ist der **Kern**

$$\mathrm{Ker}(f) := \{v \in V : f(v) = 0\}$$

von f ein Untermodul von V, und das **Bild** $\mathrm{Bld}(f) := \{f(v) : v \in V\} = f(V)$ von f ist ein Untermodul von W.

Wie üblich definiert man R-**Monomorphismen**, R-**Epimorphismen**, R-**Isomorphismen**, R-**Endomorphismen** und R-**Automorphismen**. Die **Isomorphie** von R-Moduln bezeichnen wir mit dem Symbol $\simeq$ oder genauer mit $\simeq_R$. Für R-Moduln V, W setzen wir

$$\mathrm{Hom}_R(V, W) := \{f : V \longrightarrow W \mid f\ R\text{-linear}\} \quad \text{und} \quad \mathrm{End}_R(V) := \mathrm{Hom}_R(V, V).$$

Dann wird $\mathrm{Hom}_R(V,W)$ zu einem R-Modul mit

$$(f+g)(v) := f(v)+g(v) \quad \text{und} \quad (af)(v) := af(v)$$

($f, g \in \mathrm{Hom}_R(V,W)$, $a \in R$, $v \in V$).

Den **Homomorphiesatz** und die **Isomorphiesätze** für R-Moduln setzen wir als bekannt voraus. Ein R-Modul $E \neq 0$ heißt **einfach**, falls 0 und E die einzigen Untermoduln von E sind. Eine aufsteigende Folge

$$0 = U_0 \subset U_1 \subset \ldots \subset U_m = V$$

von Untermoduln $U_0, \ldots, U_m$ eines R-Moduls V heißt **Kompositionsreihe** von V, falls U_i/U_{i-1} für $i = 1, \ldots, m$ ein einfacher R-Modul ist. Nicht jeder R-Modul hat eine Kompositionsreihe. Hat aber der R-Modul V zwei Kompositionsreihen

$$0 = U_0 \subset U_1 \subset \ldots \subset U_m = V \quad \text{und} \quad 0 = W_0 \subset W_1 \subset \ldots \subset W_n = V,$$

so besagt der bekannte **Satz von Jordan-Hölder**, dass $m = n$ ist und eine Permutation σ von $\{1, \ldots, n\}$ existiert mit der Eigenschaft, dass $U_i/U_{i-1} \simeq W_{\sigma(i)}/W_{\sigma(i)-1}$ für $i = 1, \ldots, n$ ist. Die R-Moduln $U_1/U_0, \ldots, U_n/U_{n-1}$ sind also durch V bis auf Isomorphie und Reihenfolge eindeutig bestimmt. Sie heißen **Kompositionsfaktoren** von V. Ihre Anzahl $n =: \ell(V)$ ist die **Kompositionslänge** von V. Daher ist $\ell(0) = 0$, und $\ell(V) = 1$ genau dann, wenn V einfach ist.

Eine Folge $U \xrightarrow{f} V \xrightarrow{g} W$ von R-Moduln U, V, W und R-Homomorphismen f, g mit $\mathrm{Bld}(f) = \mathrm{Ker}(g)$ heißt **exakt**. Eine (endliche oder unendliche) Folge von R-Moduln und R-Homomorphismen

$$\cdots \longrightarrow V_{i-1} \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1} \longrightarrow \cdots$$

heißt **exakt**, wenn jede Teilfolge $V_{i-1} \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1}$ exakt ist.

Zum Beispiel ist eine Folge der Form $0 \longrightarrow U \xrightarrow{f} V$ genau dann exakt, wenn f injektiv ist. Analog ist eine Folge der Form $V \xrightarrow{g} W \longrightarrow 0$ genau dann exakt, wenn g surjektiv ist. Daher ist eine Folge der Form $0 \longrightarrow U \xrightarrow{f} V \longrightarrow 0$ genau dann exakt, wenn f bijektiv ist. Eine exakte Folge von R-Moduln und R-Homomorphismen der Form

$$0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$$

heißt **kurze exakte Folge**.

2.1 Satz. *Für eine kurze exakte Folge $\mathcal{F} : 0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$ von R-Moduln und R-Homomorphismen sind äquivalent:*
(1) Es existiert ein $s \in \mathrm{Hom}_R(V,U)$ mit $s \circ f = \mathrm{id}_U$.
(2) Es existiert ein $t \in \mathrm{Hom}_R(W,V)$ mit $g \circ t = \mathrm{id}_W$.
(3) $\mathrm{Bld}(f) = \mathrm{Ker}(g)$ hat ein Komplement K in V.

Beweis. (1) $\Longrightarrow$ (3): Sei (1) erfüllt. Wir zeigen: $V = \mathrm{Bld}(f) \oplus \mathrm{Ker}(s)$.
Für $v \in V$ ist $s(f(s(v))) = s(v)$, d.h. $v - f(s(v)) \in \mathrm{Ker}(s)$ und $v = f(s(v)) + (v - f(s(v))) \in \mathrm{Bld}(f) + \mathrm{Ker}(s)$. Also gilt: $V = \mathrm{Bld}(f) + \mathrm{Ker}(s)$.
Sei $v \in \mathrm{Bld}(f) \cap \mathrm{Ker}(s)$, und sei $v = f(u)$ mit $u \in U$. Dann ist $0 = s(v) = s(f(u)) = u$, d.h. $v = f(u) = f(0) = 0$. Dies zeigt: $V = \mathrm{Bld}(f) \oplus \mathrm{Ker}(s)$.
(3) $\Longrightarrow$ (1): Sei (3) erfüllt. Dann kann man jedes $v \in V$ in der Form $v = f(u) + k$ mit eindeutig bestimmten $u \in U$, $k \in K$ schreiben. Wir setzen $s(v) := u \in U$ und erhalten so eine Abbildung $s : V \longrightarrow U$. Man sieht leicht, dass s R-linear ist.
Für $u \in U$ ist $f(u) \in \mathrm{Bld}(f) \subseteq V$ und $s(f(u)) = u$. Daher gilt: $s \circ f = \mathrm{id}_U$.
(2) $\Longleftrightarrow$ (3): Analog.

In der obigen Situation sagt man: $\mathcal{F}$ **zerfällt**.
Für jede Teilmenge X eines R-Moduls V ist

$$\mathrm{Span}_R(X) := RX := \{\sum_{i=1}^{n} r_i x_i : r_1, \ldots, r_n \in R;\ x_1, \ldots, x_n \in X;\ n \in \mathbb{N}_0\} \subseteq V$$

ein Untermodul, der von X **erzeugte** Untermodul. Die Elemente in RX nennt man **Linearkombinationen** von X. Im Fall $RX = V$ heißt X ein **Erzeugendensystem** von V. Hat V ein endliches Erzeugendensystem, so heißt V **endlich erzeugt**. Ggf. bezeichnet man die minimale Erzeugendenzahl von V mit $\mu(V) := \mu_R(V)$. Ist $\mu(V) \leq 1$, d.h. $V = Rx := \{rx : r \in R\}$ für ein $x \in V$, so heißt V **zyklisch**.

Eine Teilmenge X eines R-Moduls V heißt (R-)**linear unabhängig**, falls für paarweise verschiedene $x_1, \ldots, x_n \in X$ stets gilt:

$$a_1, \ldots, a_n \in R \wedge a_1 x_1 + \cdots + a_n x_n = 0 \Longrightarrow a_1 = \ldots = a_n = 0.$$

Jedes linear unabhängige Erzeugendensystem B von V heißt (R-)**Basis** von V. Man beachte aber, dass (im Gegensatz zur Situation bei Vektorräumen) nicht jeder R-Modul eine Basis hat. (Z.B. hat der $\mathbb{Z}$-Modul $\mathbb{Z}/6\mathbb{Z}$ keine Basis.) Hat der R-Modul V eine Basis, so nennt man V **frei**. Z.B. ist R^n für $n \in \mathbb{N}$ (im Fall $R \neq 0$) frei mit **Standardbasis**

$$e_1 := (1, 0, \ldots, 0), \ldots, e_n := (0, \ldots, 0, 1).$$

Allgemeiner ist $\coprod_{i \in I} R$ für jede (nichtleere) Menge I frei mit **Standardbasis** $e_i = (e_{ij})_{j \in I}$ ($i \in I$); dabei ist $e_{ij} := 1$ im Fall $i = j$ und $e_{ij} := 0$ sonst.

2.2 Satz. *Jeder (endlich erzeugte) R-Modul V ist zu einem Faktormodul eines (endlich erzeugten) freien R-Moduls isomorph.*

Beweis. Sei X ein Erzeugendensystem von V (notfalls $X = V$). Dann ist $F := \coprod_{x \in X} R$ ein freier R-Modul, und $f : F \longrightarrow V$, $(r_x)_{x \in X} \longmapsto \sum_{x \in X} r_x x$, ist ein R-Epimorphismus. Nach dem Homomorphiesatz ist also $V \simeq F/\mathrm{Ker}(f)$.

3. Algebren

Sei R ein Ring. Eine R-**Algebra** ist ein Paar (S, f), das aus einem Ring S und einem Ringhomomorphismus $f : R \longrightarrow S$ besteht. Ist z.B. S eine Ringerweiterung von R und $i : R \longrightarrow S$ die Inklusionsabbildung, so ist (S, i) eine R-Algebra.

Ist (S, f) eine beliebige R-Algebra, so wird jeder S-Modul W zu einem R-Modul mit

$$rw := f(r)w \qquad (r \in R,\ w \in W).$$

Insbesondere wird der reguläre S-Modul S zu einem R-Modul mit

$$rs := f(r)s \qquad (r \in R,\ s \in S).$$

Dann ist $f(r) = r1_S$ für $r \in R$. Man sagt daher auch kurz: S ist eine R-Algebra. Es ist klar, wie man **Teilalgebren** einer R-Algebra definiert.

Man nennt eine R-Algebra S **endlich**, wenn S als R-Modul endlich erzeugt ist. Analog spricht man von einer **endlichen Ringerweiterung**.

Für eine beliebige R-Algebra S, ein Polynom

$$p = \sum_{i_1=0}^{k_1} \dots \sum_{i_n=0}^{k_n} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} \in R[X_1, \dots, X_n]$$

und Elemente $s_1, \dots, s_n \in S$ setzt man

$$p(s_1, \dots, s_n) := \sum_{i_1=0}^{k_1} \dots \sum_{i_n=0}^{k_n} a_{i_1 \dots i_n} s_1^{i_1} \dots s_n^{i_n} \in S.$$

Dann ist

$$R[s_1, \dots, s_n] := \{p(s_1, \dots, s_n) : p \in R[X_1, \dots, X_n]\} \subseteq S$$

eine Teilalgebra. Existieren Elemente $s_1, \dots, s_n \in S$ mit $R[s_1, \dots, s_n] = S$, so nennt man S eine **endlich erzeugte** R-Algebra. (Analog spricht man von einer **endlich erzeugten** Ringerweiterung.) Sicher ist jede endliche R-Algebra auch endlich erzeugt; die Umkehrung gilt i.a. nicht. Z.B. ist der Polynomring $R[X]$ eine endlich erzeugte R-Algebra, aber (im Fall $R \neq 0$) keine endliche R-Algebra. Der Ring $\mathbb{Z}[\sqrt{5}]$ ist ein Beispiel für eine endliche $\mathbb{Z}$-Algebra.

Sei wieder S eine beliebige R-Algebra. Ein Element $s \in S$ heißt **ganz** über R, falls ein normiertes Polynom $p \in R[X]$ mit $p(s) = 0$ existiert. Z.B. ist $\sqrt{2}$ ganz über $\mathbb{Z}$ als Nullstelle von $X^2 - 2$; dagegen zeigt man leicht, dass $\frac{1}{3}$ nicht ganz über $\mathbb{Z}$ ist (vgl. auch Satz 3.1 unten). Ist K ein Teilkörper eines Körpers L, so ist ein Element in L genau dann ganz über K, wenn es algebraisch über K ist.

Für eine beliebige R-Algebra S heißt

$$\widetilde{R} := \{s \in S : s \text{ ganz über } R\}$$

ganzer Abschluss von R in S. Sicher ist $R1_S \subseteq \widetilde{R} \subseteq S$. Im Fall $\widetilde{R} = S$ nennt man S **ganz** über R; im Fall $\widetilde{R} = R1_S$ heißt R **ganz abgeschlossen** in S. Ähnliche Begriffe hat man

für Ringerweiterungen. Ein Integritätsbereich heißt **normal** (oder ganz abgeschlossen), wenn er in seinem Quotientenkörper ganz abgeschlossen ist.

Bekanntlich heißt ein Integritätsbereich R ein **faktorieller** Ring, wenn sich jedes Element $0 \neq x \in R \setminus R^\times$ als Produkt von Primelementen schreiben lässt. (Ein Element $0 \neq p \in R \setminus R^\times$ heißt **Primelement**, wenn für alle $a, b \in R$ gilt: $ab \in pR \Longrightarrow a \in pR \vee b \in pR$.) Aus der Algebra ist bekannt, dass für einen faktoriellen Ring R auch der Polynomring $R[X]$ faktoriell ist.

3.1 Satz. *Jeder faktorielle Ring R ist normal.*

Beweis. Sei K der Quotientenkörper von R, und sei $x \in K$ ganz über R; o.B.d.A. $x \neq 0$. Wir schreiben $x = \frac{r}{s}$ mit teilerfremden $r, s \in R$. Nach Voraussetzung existieren $a_0, \ldots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, d.h. $r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$. Jeder Primteiler von s ist also auch einer von r^n und damit einer von r. Da andererseits r, s teilerfremd sind, muss s eine Einheit in R sein. Also ist $x = rs^{-1} \in R$.

Sei R wieder ein beliebiger Ring. Für $n \in \mathbb{N}$ und jede Matrix $A = (a_{ij}) \in R^{n\times n}$ heißt

$$\det(A) := |A| := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \in R$$

Determinante von A; dabei ist S_n die **symmetrische Gruppe** des Grades n, und $\operatorname{sgn}(\sigma)$ bezeichnet das **Vorzeichen** einer Permutation σ. Es gelten die üblichen Rechenregeln für Determinanten.

Die **Adjunkte** $\widetilde{A} := (\widetilde{a}_{ij}) \in R^{n\times n}$ von A ist definiert durch

$$\widetilde{a}_{ij} := (-1)^{i+j} |A_{ji}| \qquad (i, j = 1, \ldots, n);$$

dabei entsteht die Matrix $A_{ji} \in R^{(n-1)\times(n-1)}$ aus A durch Streichen der j-ten Zeile und der i-ten Spalte. Wichtig ist die folgende Tatsache:

$$A\widetilde{A} = \widetilde{A}A = |A| 1_n;$$

dabei bezeichnet $1_n \in R^{n\times n}$ die Einheitsmatrix.

Zur Erläuterung: Aus der Linearen Algebra ist bekannt, dass die Gleichung $A\widetilde{A} = |A|1_n$ gilt, falls die Koeffizienten von A aus einem Körper K stammen, z.B. aus dem rationalen Funtionenkörper $\mathbb{Q}(X_1, \ldots, X_t)$. Insbesondere gilt sie, falls die Koeffizienten aus dem Polynomring $\mathbb{Z}[X_1, \ldots, X_t]$ stammen. Die Koeffizienten von A dürfen also die Unbestimmten $X_{11}, \ldots, X_{nn}$ im Polynomring $\mathbb{Z}[X_{ij} : i, j = 1, \ldots, n]$ sein. Man kann dann für die Unbestimmten X_{ij} die Elemente $a_{ij} \in R$ einsetzen und erhält so die gewünschte Formel.

Ähnlich kann man bei analogen Fragestellungen vorgehen.

Sei $R[X]$ der Polynomring in der Variablen X über R, und sei $A = (a_{ij}) \in R^{n\times n}$ für ein $n \in \mathbb{N}$. Dann heißt

$$\chi_A(X) := |X \cdot 1_n - A| \in R[X]$$

charakteristisches Polynom von A. Dieses hat die Form

$$\chi_A(X) = X^n + r_{n-1}X^{n-1} + \cdots + r_1X + r_0$$

mit $r_0 = (-1)^n|A|, r_1, \ldots, r_{n-1} = -a_{11} - a_{22} - \cdots - a_{nn} = -\text{spur}(A) \in R$.

3.2 Satz. (Cayley-Hamilton)
In der obigen Situation gilt in $R^{n\times n}$:

$$\chi_A(A) := A^n + r_{n-1}A^{n-1} + \cdots + r_1A + r_0 1_n = 0.$$

Dies erhält man mit der oben skizzierten Methode.

3.3 Satz. *Für jedes Ideal $I \trianglelefteq R$, jeden R-Modul V mit Erzeugendensystem $v_1, \ldots, v_n$ und jedes $\phi \in \text{End}_R(V)$ mit $\phi(V) \subseteq IV$ existieren Elemente $a_1 \in I$, $a_2 \in I^2$, ..., $a_n \in I^n$ mit*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n\text{id}_V = 0 \quad \textit{in} \quad \text{End}_R(V).$$

Beweis. Sicher ist $IV = Iv_1 + \cdots + Iv_n$. Wir schreiben $\phi(v_j) = \sum_{i=1}^n a_{ij}v_i$ mit $a_{ij} \in I$ für alle i, j und setzen $A := (a_{ij}) \in R^{n\times n}$. Sei $B(X) := (b_{ij}(X)) \in R[X]^{n\times n}$ die Adjunkte von $X \cdot 1_n - A \in R[X]^{n\times n}$. Nach den obigen Überlegungen ist $(X \cdot 1_n - A)B(X) = \chi_A(X)1_n$. Daher gilt für $i, k = 1, \ldots, n$ in $R[X]$:

$$\chi_A(X)\delta_{ik} = \sum_{j=1}^n (X\delta_{ij} - a_{ij})b_{jk}(X) = \sum_{j=1}^n b_{jk}(X)(X\delta_{ij} - a_{ij}).$$

Einsetzen von ϕ liefert die folgenden Gleichungen in $\text{End}_R(V)$:

$$\chi_A(\phi)\delta_{ik} = \sum_{j=1}^n b_{jk}(\phi)(\phi\delta_{ij} - a_{ij}\text{id}_V).$$

Wegen $0 = \sum_{i=1}^n (\phi\delta_{ij} - a_{ij})v_i$ für $j = 1, \ldots, n$ folgt:

$$0 = \sum_{j=1}^n b_{jk}(\phi) \sum_{i=1}^n (\phi\delta_{ij} - a_{ij})v_i = \sum_{i,j=1}^n b_{jk}(\phi)(\phi\delta_{ij} - a_{ij})v_i = \sum_{i=1}^n \chi_A(\phi)\delta_{ik}v_i = \chi_A(\phi)v_k$$

für $k = 1, \ldots, n$. Also ist $\chi_A(\phi)v = 0$ für alle $v \in V$, d.h. $\chi_A(\phi) = 0$. Dies liefert die gewünschte Gleichung.

Bemerkung. Zu jedem endlich erzeugten R-Modul V und jedem Ideal $I \trianglelefteq R$ mit $IV = V$ existiert also ein $a \in I$ mit $(1 + a)V = 0$; zum Beweis wenden wir Satz 3.3 mit $\phi := \text{id}_V$ an und erhalten eine Gleichung

$$0 = \text{id}_V^n + a_1\text{id}_V^{n-1} + \cdots + a_{n-1}\text{id}_V^1 + a_n\text{id}_V = (1 + a_1 + \cdots + a_n)\text{id}_V$$

mit $a_1, \ldots, a_n \in I$. Also ist $(1+a)V = 0$ mit $a := a_1 + \cdots + a_n \in I$.

3.4 Satz. *Für jede R-Algebra S und jedes Element $s \in S$ sind äquivalent:*
(1) s ist ganz über R;
(2) $R[s]$ ist eine endliche R-Algebra;
(3) Es existiert eine endliche Unteralgebra $T \subseteq S$ mit $s \in T$.

Beweis. (1) $\Longrightarrow$ (2): Sei (1) erfüllt. Dann existieren $r_0, \ldots, r_{n-1} \in R$ mit $0 = s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 1$. Daher ist $R[s] = R1 + Rs + \cdots + Rs^{n-1}$ ein endlich erzeugter R-Modul.
(2) $\Longrightarrow$ (3): Setze $T := R[s]$.
(3) $\Longrightarrow$ (1): Sei (3) erfüllt. Dann ist $\phi : T \longrightarrow T$, $t \longmapsto st$, R-linear. Nach Satz 3.3 existieren $a_0, \ldots, a_{n-1} \in R$ mit $\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 \mathrm{id}_V = 0$. Anwendung auf 1_T ergibt: $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 1 = 0$.

Bemerkung. Jede endliche R-Algebra ist also ganz über R.

3.5 Satz. *Sei S eine R-Algebra, und sei T eine S-Algebra (also auch eine R-Algebra).*
(i) Ist S eine endliche R-Algebra und ist T eine endliche S-Algebra, so ist T eine endliche R-Algebra.
(ii) Sind $s_1, \ldots, s_m \in S$ ganz über R, so ist $R[s_1, \ldots, s_m]$ eine endliche R-Algebra; insbesondere ist die Teilalgebra $R[s_1, \ldots, s_m]$ von S ganz über R.
(iii) Ist S ganz über R und ist T ganz über S, so ist T auch ganz über R.
(iv) Der ganze Abschluss $\widetilde{R}$ von R in S ist eine R-Teilalgebra von S.
(v) Ist $s \in S$ ganz über dem Teilring $\widetilde{R}$ von S, so ist $s \in \widetilde{R}$. Es gilt also: $\widetilde{\widetilde{R}} = \widetilde{R}$.

Beweis. (i) Aus $S = Rs_1 + \cdots + Rs_m$ und $T = St_1 + \cdots + St_n$ folgt: $T = \sum_{i=1}^m \sum_{j=1}^n Rs_i t_j$.
(ii) Seien $s_1, \ldots, s_m \in S$ ganz über R. Nach Satz 3.4 ist $R[s_1]$ eine endliche R-Algebra. Ferner ist s_2 ganz über $R[s_1]$. Nach Satz 3.4 ist $R[s_1, s_2]$ eine endliche $R[s_1]$-Algebra. Wegen (i) ist $R[s_1, s_2]$ auch eine endliche R-Algebra. Fährt man so fort, erhält man die erste Aussage. Die zweite Aussage folgt dann aus Bemerkung 3.4.
(iii) Sei $t \in T$. Dann existieren $s_0, \ldots, s_{n-1} \in S$ mit $t^n + s_{n-1}t^{n-1} + \cdots + s_1 t + s_0 1_T = 0$. Daher ist t ganz über $R[s_0, \ldots, s_{n-1}]$. Nach (ii) ist $R[s_0 1_T, \ldots, s_{n-1}1_T, t]$ eine endliche $R[s_0, \ldots, s_{n-1}]$-Algebra. Wegen (ii) ist ferner $R[s_0, \ldots, s_{n-1}]$ eine endliche R-Algebra. Wegen (i) ist also $R[s_0 1_T, \ldots, s_{n-1}1_T, t]$ eine endliche R-Algebra. Nach Satz 3.4 ist damit t ganz über R.
(iv) Sicher ist $1_S \in \widetilde{R}$. Seien $s, t \in \widetilde{R}$. Wegen (ii) ist $R[s,t]$ eine endliche R-Algebra. Wegen $s - t, st \in R[s,t]$ sind nach Satz 3.4 auch $s - t, st$ ganz über R.
(v) Sei $s \in S$ ganz über $\widetilde{R}$. Nach Satz 3.4 ist $\widetilde{R}[s]$ eine endliche $\widetilde{R}$-Algebra. Daher ist $\widetilde{R}[s]$ ganz über $\widetilde{R}$ nach Bemerkung 3.4. Wegen (iii) ist $\widetilde{R}[s]$ ganz über R. Insbesondere ist s ganz über R, d.h. $s \in \widetilde{R}$.

Beispiel. Sei $d \in \mathbb{Z}$ quadratfrei und R der ganze Abschluss von $\mathbb{Z}$ in $K := \mathbb{Q}(\sqrt{d})$. Dann ist $R = \mathbb{Z} + \mathbb{Z}\alpha$ mit $\alpha := \frac{1+\sqrt{d}}{2}$ für $d \equiv 1 \pmod 4$ und $\alpha := \sqrt{d}$ sonst.

Zum Beweis seien $a, b \in \mathbb{Q}$ mit $\beta := a + b\sqrt{d} \in R$. Bekanntlich ist $K \longrightarrow K$, $\xi = x + y\sqrt{d} \longmapsto x - y\sqrt{d} =: \widetilde{\xi}$ für $x, y \in \mathbb{Q}$, ein Ringautomorphismus von K. Ist also $f \in \mathbb{Z}[X]$ normiert mit $f(\beta) = 0$, so ist $0 = \widetilde{f(\beta)} = f(\widetilde{\beta})$, d.h. $\widetilde{\beta} \in R$. Daher ist insbesondere $2a = \beta + \widetilde{\beta} \in R \cap \mathbb{Q} = \mathbb{Z}$ und $a^2 - b^2 d = \beta\widetilde{\beta} \in R \cap \mathbb{Q} = \mathbb{Z}$ nach Satz 3.1.

Im Fall $a \in \mathbb{Z}$ ist auch $b^2 d \in \mathbb{Z}$. Da d quadratfrei ist, folgt: $b \in \mathbb{Z}$ und damit $\beta = a + b\sqrt{d} \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Sei also $a \notin \mathbb{Z}$, d.h. $a_1 := 2a \in \mathbb{Z}$ ist ungerade. Wegen $(2a)^2 - (2b)^2 d \in \mathbb{Z}$ ist daher analog $b_1 := 2b \in \mathbb{Z}$. Ferner ist $0 \equiv a_1^2 - b_1^2 d \equiv 1 - b_1^2 d \pmod 4$, d.h. b_1 ist ungerade, und $d \equiv 1 \pmod 4$. Außerdem ist $\beta = \frac{a_1 - b_1}{2} + b_1 \frac{1+\sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$.

Daher gilt: $R \subseteq \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$ im Fall $d \equiv 1 \pmod 4$ und $R \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{d}$ sonst. Die Behauptung folgt, da $\sqrt{d}$ eine Nullstelle von $X^2 - d \in \mathbb{Z}[X]$ und $\frac{1+\sqrt{d}}{2}$ eine Nullstelle von $X^2 - X + \frac{d-1}{4} \in \mathbb{Z}[X]$ im Fall $d \equiv 1 \pmod 4$ ist.

4. Primideale

Sei R ein Ring.

4.1 Definition. Ein Ideal $P \lhd R$ heißt **Primideal**, falls für alle $a, b \in R$ gilt:

$$ab \in P \Longrightarrow a \in P \vee b \in P.$$

Ferner heißt $\mathrm{Spec}(R) := \{P \trianglelefteq R : P \text{ Primideal}\}$ (**Prim-**)**Spektrum** von R.

Bemerkung. Bekanntlich gilt für jedes Ideal $I \trianglelefteq R$:

$$I \in \mathrm{Spec}(R) \Longleftrightarrow R/I \text{ Integritätsbereich.}$$

Ist R ein Integritätsbereich und $0 \neq p \in R$, so gilt:

$$(p) \in \mathrm{Spec}(R) \Longleftrightarrow p \text{ Primelement.}$$

Beispiel. Sei R ein **Hauptidealring** (HIR), d.h. ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist. Dann ist R bekanntlich faktoriell mit

$$\mathrm{Spec}(R) = \{(0)\} \cup \{(p) : p \in R \text{ Primelement}\}.$$

Wichtige Beispiele für Hauptidealringe sind $\mathbb{Z}$ und der Polynomring $K[X]$ für einen Körper K.

4.2 Bemerkung. Für jeden Ring S, jeden Ringhomomorphismus $f : R \longrightarrow S$ und jedes $Q \in \mathrm{Spec}(S)$ ist $P := f^{-1}(Q) \in \mathrm{Spec}(R)$, wie man leicht nachrechnet.

Satz. (Primideal-Vermeidungs-Satz)

Seien $P_1, \ldots, P_n \trianglelefteq R$ Ideale mit $P_3, \ldots, P_n \in \mathrm{Spec}(R)$, und sei $S \subseteq R$ mit $s \pm t, s \cdot t \in S$ für alle $s, t \in S$. Ist $S \subseteq P_1 \cup \ldots \cup P_n$, so ist $S \subseteq P_j$ für ein $j \in \{1, \ldots, n\}$.

Beweis. (Induktion nach n)
Im Fall $n = 1$ ist nichts zu tun.
Sei jetzt $n = 2$, d.h. $S \subseteq P_1 \cup P_2$ mit $P_1, P_2 \trianglelefteq R$. Wir nehmen an: $S \not\subseteq P_1$ und $S \not\subseteq P_2$. Für $j = 1, 2$ sei $a_j \in S \setminus P_j$, d.h. $a_1 \in P_2$ und $a_2 \in P_1$. Wegen $a_1 + a_2 \in S \subseteq P_1 \cup P_2$ ist $a_1 + a_2 \in P_1$ oder $a_1 + a_2 \in P_2$; o.B.d.A. sei $a_1 + a_2 \in P_1$. Dann haben wir den Widerspruch $a_1 = (a_1 + a_2) - a_2 \in P_1$.
Sei schließlich $n \geq 3$ und die Behauptung für $n - 1$ schon bewiesen. Wir können dann für $j = 1, \ldots, n$ annehmen: $S \not\subseteq \bigcup_{i=1, i\neq j}^{n} P_i$, etwa $a_j \in S \setminus \bigcup_{i=1, i\neq j}^{n} P_i$, also $a_j \in P_j$. Wegen $P_n \in \mathrm{Spec}(R)$ ist $a_1 \cdots a_{n-1} \notin P_n$, d.h. $a_1 \cdots a_{n-1} \in \bigcap_{i=1}^{n-1} P_i \setminus P_n$ und $a_n \in P_n \setminus \bigcup_{i=1}^{n-1} P_i$. Also ist $b := a_1 \cdots a_{n-1} + a_n \in S$. Im Fall $b \in P_n$ hätte man den Widerspruch $a_1 \cdots a_{n-1} = b - a_n \in P_n$. Also ist $b \in P_j$ für ein $j \in \{1, \ldots, n-1\}$. Dann haben wir aber den Widerspruch $a_n = b - a_1 \cdots a_{n-1} \in P_j$.

4.3 Definition. Eine Teilmenge $A \subseteq R$ mit $1 \in A$ und $ab \in A$ für alle $a, b \in A$ heißt **multiplikativ**.

Beispiele. Für $a \in R$ ist $\{1, a, a^2, \ldots\} \subseteq R$ multiplikativ. Für $P \in \mathrm{Spec}(R)$ ist $R \setminus P \subseteq R$ multiplikativ. Ferner ist $R \setminus \mathrm{Z}(R) \subseteq R$ multiplikativ.

4.4 Satz. (i) *Sei $A \subseteq R$ eine multiplikative Teilmenge, und sei $I \trianglelefteq R$ mit $I \cap A = \emptyset$. Dann existiert ein $P \in \mathrm{Spec}(R)$ mit $I \subseteq P$ und $P \cap A = \emptyset$.*
(ii) *Für $P \in \mathrm{Spec}(R)$ existiert ein minimales Primideal $Q \trianglelefteq R$ mit $Q \subseteq P$.*

Bemerkung. Ein $Q \in \mathrm{Spec}(R)$ heißt **minimal**, falls kein $I \in \mathrm{Spec}(R)$ mit $I \subset Q$ existiert. Die Menge aller minimalen Primideale in R bezeichnen wir mit $\mathrm{Min}(R)$.

Beweis. (i) $\mathfrak{M} := \{P \trianglelefteq R : I \subseteq P,\ P \cap A = \emptyset\}$ ist durch $\subseteq$ geordnet und wegen $I \in \mathfrak{M}$ nichtleer. Ist $\mathfrak{N}$ eine nichtleere total geordnete Teilmenge von $\mathfrak{M}$, so ist $S := \bigcup_{N \in \mathfrak{N}} N \in \mathfrak{M}$, wie man sich leicht überlegt. Damit ist S eine obere Schranke von $\mathfrak{N}$ in $\mathfrak{M}$. Nach Zorns Lemma enthält $\mathfrak{M}$ ein maximales Element P; insbesondere ist $I \subseteq P \trianglelefteq R$ und $P \cap A = \emptyset$, also $P \neq R$. Wir zeigen: $P \in \mathrm{Spec}(R)$.
Dazu seien $a_1, a_2 \in R \setminus P$. Für $i = 1, 2$ ist dann $P < P + (a_i) \trianglelefteq R$. Daher ist $P + (a_i) \notin \mathfrak{M}$ nach Wahl von P. Also ist $(P + (a_i)) \cap A \neq \emptyset$. Wähle $p_i \in P$, $r_i \in R$ mit $p_i + r_i a_i \in A$. Dann enthält A auch $(p_1 + r_1 a_1)(p_2 + r_2 a_2) = p_1 p_2 + p_1 r_2 a_2 + r_1 a_1 p_2 + r_1 r_2 a_1 a_2 =: b$. Wegen $P \cap A = \emptyset$ ist $b \notin P$, also $r_1 r_2 a_1 a_2 \notin P$; insbesondere ist $a_1 a_2 \notin P$.
(ii) $\mathfrak{M} := \{Q \in \mathrm{Spec}(R) : Q \subseteq P\}$ ist durch $\subseteq$ geordnet und nichtleer wegen $P \in \mathfrak{M}$. Ist $\mathfrak{N}$ eine nichtleere total geordnete Teilmenge von $\mathfrak{M}$, so ist $S := \bigcap_{N \in \mathfrak{N}} N \trianglelefteq R$ und $S \subseteq P$. Wir zeigen: $S \in \mathrm{Spec}(R)$.
Dazu seien $a_1, a_2 \in R \setminus S$. Für $i = 1, 2$ existiert dann ein $N_i \in \mathfrak{N}$ mit $a_i \notin N_i$. O.B.d.A. sei $N_1 \subseteq N_2$. Dann gilt: $a_1, a_2 \notin N_1$, also auch $a_1 a_2 \notin N_1$ und damit $a_1 a_2 \notin S$.

Dies zeigt, dass S eine untere Schranke von $\mathfrak{N}$ in $\mathfrak{M}$ ist. Nach Zorns Lemma enthält $\mathfrak{M}$ ein minimales Element Q. Damit ist $Q \in \mathrm{Min}(R)$.

4.5 Satz. *Stets ist* $\mathrm{nil}(R) = \bigcap_{P\in\mathrm{Spec}(R)} P = \bigcap_{Q\in\mathrm{Min}(R)} Q$ *und* $\bigcup_{Q\in\mathrm{Min}(R)} Q \subseteq \mathrm{Z}(R)$. *Ist* R *reduziert, so ist* $\bigcup_{Q\in\mathrm{Min}(R)} Q = \mathrm{Z}(R)$.

Beweis. Sei $x \in \mathrm{nil}(R)$, d.h. $x^n = 0$ für ein $n \in \mathbb{N}$. Für $P \in \mathrm{Spec}(R)$ ist dann $x \in P$. Also ist $x \in \bigcap_{P\in\mathrm{Spec}(R)} P$.

Sei $x \in R \setminus \mathrm{nil}(R)$. Dann ist $A := \{1, x, x^2, \ldots\}$ eine multiplikative Teilmenge von R. Nach Satz 4.4 (i) (mit $I := 0$) existiert ein $M \in \mathrm{Spec}(R)$ mit $M \cap A = \emptyset$. Insbesondere ist $x \notin M$, also auch $x \notin \bigcap_{P\in\mathrm{Spec}(R)} P$.

Nach Satz 4.4 (ii) ist $\bigcap_{P\in\mathrm{Spec}(R)} P = \bigcap_{P\in\mathrm{Min}(R)} P$.

Sei $Q \in \mathrm{Min}(R)$. Dann ist $A := \{ab : a \in R \setminus Q,\ b \in R \setminus \mathrm{Z}(R)\} \subseteq R$ multiplikativ mit $0 \notin A$. Nach Satz 4.4 existiert ein $P \in \mathrm{Spec}(R)$ mit $P \cap A = \emptyset$; insbesondere ist $P \subseteq Q \cap \mathrm{Z}(R)$. Wegen $Q \in \mathrm{Min}(R)$ folgt $Q = P \subseteq \mathrm{Z}(R)$.

Sei jetzt R reduziert, d.h. $0 = \mathrm{nil}(R) = \bigcap_{P\in\mathrm{Min}(R)} P$, und sei $x \in \mathrm{Z}(R)$, d.h. $xy = 0$ für ein $y \in R \setminus \{0\}$. Wegen $y \neq 0$ existiert ein $P \in \mathrm{Min}(R)$ mit $y \notin P$. Wegen $xy \in P$ ist also $x \in P$.

4.6 Definition. Für $I \trianglelefteq R$ heißt $\mathrm{rad}(I) := \{a \in R : \exists n \in \mathbb{N} : a^n \in I\}$ **Radikal** von I.

Bemerkung. (i) Für $a \in R$ gilt offenbar: $a \in \mathrm{rad}(I) \Longleftrightarrow a + I \in \mathrm{nil}(R/I)$.

(ii) Daher ist $\mathrm{rad}(I) \trianglelefteq R$ mit $I \subseteq \mathrm{rad}(I) = \mathrm{rad}(\mathrm{rad}(I))$ und $\mathrm{rad}(I)/I = \mathrm{nil}(R/I)$.

(iii) Für $I, J \trianglelefteq R$ mit $I \subseteq J$ ist sicher $\mathrm{rad}(I) \subseteq \mathrm{rad}(J)$.

(iv) Für $I, J \trianglelefteq R$ ist $\mathrm{rad}(IJ) = \mathrm{rad}(I \cap J) = \mathrm{rad}(I) \cap \mathrm{rad}(J)$.

[Denn wegen $IJ \subseteq I \cap J \subseteq I$ folgt aus (iii): $\mathrm{rad}(IJ) \subseteq \mathrm{rad}(I \cap J) \subseteq \mathrm{rad}(I)$. Analog ist $\mathrm{rad}(I \cap J) \subseteq \mathrm{rad}(J)$, also $\mathrm{rad}(I \cap J) \subseteq \mathrm{rad}(I) \cap \mathrm{rad}(J)$. Umgekehrt existieren für $x \in \mathrm{rad}(I) \cap \mathrm{rad}(J)$ Zahlen $m, n \in \mathbb{N}$ mit $x^m \in I$ und $x^n \in J$, d.h. $x^{m+n} \in IJ$. Daher ist $x \in \mathrm{rad}(IJ)$.]

(v) Für $I \trianglelefteq R$ und $n \in \mathbb{N}$ ist $\mathrm{rad}(I^n) = \mathrm{rad}(I)$ nach (iv).

(vi) Aus Satz 4.5 folgt leicht: $\mathrm{rad}(I) = \bigcap_{I\subseteq P\in\mathrm{Spec}(R)} P = \bigcap_{Q\in\mathfrak{X}} Q$; dabei ist $\mathfrak{X}$ die Menge der minimalen Elemente (bzgl. $\subseteq$) in $\{P \in \mathrm{Spec}(R) : I \subseteq P\}$.

(vii) Für $I \trianglelefteq R$ gilt: $I = \mathrm{rad}(I) \Longleftrightarrow \exists J \trianglelefteq R : I = \mathrm{rad}(J)$. Ggf. heißt I **Radikalideal** in R. Offenbar ist jedes Primideal in R auch ein Radikalideal in R. Ferner ist jeder Durchschnitt einer nichtleeren Familie von Radikalidealen wieder ein Radikalideal.

Beispiel. Für $R = \mathbb{Z}$ und $I = (12)$ ist $\mathrm{rad}(I) = (6)$.

5. Maximale Ideale

Sei R ein Ring.

5.1 Definition. Ein Ideal $M \triangleleft R$ heißt **maximal**, wenn kein Ideal $I \triangleleft R$ mit $M \subset I$ existiert. Die Menge $\mathrm{Max}(R)$ aller maximalen Ideale von R heißt **Maximalspektrum** von R.

Bemerkung. (i) Bekanntlich gilt für alle $I \trianglelefteq R$: $I \in \mathrm{Max}(R) \Longleftrightarrow R/I$ Körper. Insbesondere ist $\mathrm{Max}(R) \subseteq \mathrm{Spec}(R)$.

(ii) Aus dem Beweis von Satz 4.4 (i) folgt leicht, dass jedes echte Ideal von R in einem maximalen Ideal von R enthalten ist. Insbesondere ist $\mathrm{Max}(R) \neq \emptyset$ für $R \neq 0$.
(iii) Aus Satz 4.4 (i) folgt auch leicht: $R \setminus R^\times = \bigcup_{M \in \mathrm{Max}(R)} M$.

Beispiel. Ist R ein HIR, aber kein Körper, so ist $\mathrm{Max}(R) = \{(p) : p \in R \text{ Primelement}\}$.

5.2 Definition. Das Ideal $\mathrm{J}(R) := \bigcap_{M \in \mathrm{Max}(R)} M$ von R heißt (**Jacobson-**)**Radikal** von R.

Satz. *Stets ist* $\mathrm{nil}(R) \subseteq \mathrm{J}(R) = \{a \in R : 1 + ab \in R^\times \text{ für alle } b \in R\}$.

Beweis. Die erste Inklusion folgt aus Satz 4.5.
Seien $a \in \mathrm{J}(R)$ und $b \in R$. Für $M \in \mathrm{Max}(R)$ ist dann $1 + ab \notin M$; denn sonst wäre auch $1 = (1 + ab) - ab \in M$ wegen $a \in M$. Also ist $1 + ab \notin \bigcup_{M \in \mathrm{Max}(R)} M = R \setminus R^\times$, d.h. $1 + ab \in R^\times$.
Sei $a \in R \setminus \mathrm{J}(R)$, also $a \notin M$ für ein $M \in \mathrm{Max}(R)$. Dann ist $0 \neq a + M \in R/M$. Da R/M ein Körper ist, existiert ein $b \in R$ mit $1 = (a + M)(b + M) = ab + M$. Folglich ist $1 - ab \in M$, d.h. $1 - ab \notin R^\times$.

Beispiel. Da $\mathbb{P} := \{p \in \mathbb{Z} : p \text{ Primzahl}\}$ unendlich ist, ist $\mathrm{J}(\mathbb{Z}) = 0$.

5.3 Satz. *Es gilt:* $|\mathrm{Max}(R)| = 1 \iff R \setminus R^\times \trianglelefteq R$.

Beweis. "$\Longrightarrow$": Ist $\mathrm{Max}(R) = \{M\}$, so gilt nach Bemerkung 5.1 (iii): $R \setminus R^\times = M \trianglelefteq R$.
"$\Longleftarrow$": Sei $M := R \setminus R^\times \trianglelefteq R$. Dann ist $M \in \mathrm{Max}(R)$. Für $N \in \mathrm{Max}(R)$ ist ferner $N \subseteq R \setminus R^\times = M$, d.h. $N = M$. Also ist $\mathrm{Max}(R) = \{M\}$.

Definition. Ggf. heißt R **lokal**.

Beispiele. (i) Jeder Körper ist ein lokaler Ring, der Nullring nicht.
(ii) Für jeden Körper K ist der Potenzreihenring $K[[X]]$ ein lokaler Ring, und $(X) \in \mathrm{Max}(K[[X]])$.

Bemerkung. (i) In der Kommutativen Algebra versucht man häufig, Fragen über beliebige Ringe auf Fragen über lokale Ringe zurückzuführen.
(ii) Ist R lokal, so ist R zusammenhängend, und $\mathrm{Max}(R) = \{\mathrm{J}(R)\}$.
[Zum Beweis sei $e = e^2 \in R$. Im Fall $e \in \mathrm{J}(R)$ ist $1 - e \in R^\times$ nach Satz 5.2. Wegen $e(1 - e) = 0$ folgt also $e = 0$. Im Fall $e \notin \mathrm{J}(R)$ ist $e \in R^\times$. Wegen $e^2 = e$ folgt also $e = 1$. Daher sind 0 und 1 die einzigen Idempotente in R. Wegen $R \neq 0$ folgt $1 \neq 0$.]

5.4 Satz. (Nakayamas Lemma)
Sei $I \trianglelefteq R$ mit $1 + I \subseteq R^\times$ (z.B. $I = \mathrm{J}(R)$), und sei V ein endlich erzeugter R-Modul mit $V = IV$. Dann ist $V = 0$.

Beweis. Dies folgt sofort aus Bemerkung 3.3.

Bemerkung. Für jeden Untermodul U eines endlich erzeugten R-Moduls V mit $V = U + \mathrm{J}(R)V$ ist also $U = V$. Dies folgt nämlich, indem man Satz 5.4 auf den R-Modul V/U anwendet.

Beispiel. Sei R lokal und $M := \mathrm{J}(R)$, also $\mathrm{Max}(R) = \{M\}$. Für jeden endlich erzeugten R-Modul V ist dann V/MV auch ein endlich erzeugter R-Modul. Wie in §2 können wir V/MV auch als (endlich erzeugten) Modul über dem Körper $K := R/M$, d.h. als endlichdimensionalen K-Vektorraum auffassen. Für jede K-Basis $b_1 + MV, \ldots, b_n + MV$ von V/MV ist dann $V = \mathrm{Span}_R(b_1, \ldots, b_n)$ nach Nakayamas Lemma. Daher gilt: $\mu_R(V) = \dim_K V/MV$. So kann man manchmal Fragen der Kommutativen Algebra auf Fragen der Linearen Algebra zurückführen.

5.5 Satz. *Sei $R \neq 0$ und V ein endlich erzeugter freier R-Modul. Dann ist jede Basis von V endlich, und je zwei Basen von V haben die gleiche Anzahl von Elementen.*

Beweis. Seien B eine Basis und E ein endliches Erzeugendensystem von V. Dann kann man jedes $e \in E$ als endliche Linearkombination von Elementen in B schreiben. Die dabei auftretenden Elemente in B bilden eine endliche Teilmenge C von B. Dann ist C ein linear unabhängiges Erzeugendensystem von V. Folglich ist $B = C$; insbesondere ist B endlich. Nach Bemerkung 5.1 existiert ein $M \in \mathrm{Max}(R)$. Ferner ist V/MV ein Vektorraum über dem Körper $K := R/M$, und die Elemente $b + MV$ $(b \in B)$ erzeugen den K-Vektorraum V/MV. Zum Beweis der linearen Unabhängigkeit dieser Elemente sei

$$0 = \sum_{b \in B} (r_b + M)(b + MV) = \sum_{b \in B} r_b b + MV$$

mit $r_b \in R$ für $b \in B$. Wegen $V = \sum_{b \in B} Rb$ ist $\sum_{b \in B} r_b b \in MV = \sum_{b \in B} Mb$, d.h. $r_b \in M$ und damit $r_b + M = 0$ für $b \in B$. Dies zeigt, dass die Elemente $b + MV$ $(b \in B)$ eine K-Basis von V/MV bilden. Also ist $|B| = \dim_K V/MV$. Da dies für jede R-Basis von V gilt, folgt die Behauptung.

Definition. Die Anzahl n der Elemente in jeder Basis von V heißt **Rang** von V. Man schreibt: $n = \mathrm{rg}(V) = \mathrm{rg}_R(V)$.

Beispiel. Sei $R := \mathcal{C}(X)$ der Ring der stetigen Funktionen $f : X \longrightarrow \mathbb{R}$ auf dem kompakten Intervall $X := [0, 1]$ in $\mathbb{R}$. Für $a \in X$ ist dann $R \longrightarrow \mathbb{R}$, $f \longmapsto f(a)$ ein Ringepimorphismus mit Kern

$$M_a := \{f \in R : f(a) = 0\}.$$

Nach dem Homomorphiesatz ist $R/M_a \cong \mathbb{R}$ ein Körper, d.h. $M_a \in \mathrm{Max}(R)$. Wir behaupten:

$$\mathrm{Max}(R) = \{M_a : a \in X\}.$$

Zum Beweis nehmen wir an, dass ein $M \in \mathrm{Max}(R)$ mit $M \neq M_a$, also auch $M \not\subseteq M_a$ für alle $a \in X$ existiert. Für $a \in X$ sei $f_a \in M \setminus M_a$, d.h. $f_a(a) \neq 0$. Da f_a stetig ist, existiert auch eine offene Teilmenge $U_a \subseteq X$ mit $a \in U_a$ und $f_a(x) \neq 0$ für alle $x \in U_a$. Offenbar ist $X = \bigcup_{a \in X} U_a$. Da X kompakt ist, existieren $a_1, \ldots, a_n \in X$ mit $X = U_{a_1} \cup \ldots \cup U_{a_n}$. Dann ist $f := f_{a_1}^2 + \cdots + f_{a_n}^2 \in M$ und $f(a) \neq 0$ für alle $a \in X$. Damit haben wir den Widerspruch $f \in R^\times$.

Sicher ist $A := R \setminus \mathrm{Z}(R) \subseteq R$ multiplikativ mit $\{0\} \cap A = \emptyset$. Nach Satz 4.4 existiert ein $P \in \mathrm{Spec}(R)$ mit $P \cap A = \emptyset$, d.h. $P \subseteq \mathrm{Z}(R)$. Wir nehmen an: $P = M_a$ für ein $a \in X$.

Sicher existiert ein $g_a \in M_a$ mit $g_a(b) \neq 0$ für alle $a \neq b \in X$. Wegen $g_a \in M_a = P \subseteq \mathrm{Z}(R)$ existiert auch ein $0 \neq h_a \in R$ mit $g_a h_a = 0$. Dann ist $h_a(b) = 0$ für alle $a \neq b \in X$, also auch $h_a(a) = 0$, da h_a stetig ist. Damit haben wir den Widerspruch $h_a = 0$.

Dieser Widerspruch zeigt: $\mathrm{Spec}(R) \neq \mathrm{Max}(R)$.

6. Kettenbedingungen

Sei R ein Ring.

6.1 Satz. *Für jeden R-Modul V sind äquivalent:*

(1) Jede nichtleere Menge von Untermoduln von V enthält ein maximales Element (bzgl. $\subseteq$).

(2) Zu jeder aufsteigenden Kette $U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$ von Untermoduln von V existiert ein $k \in \mathbb{N}$ mit $U_k = U_{k+1} = \ldots$.

(3) Jeder Untermodul U von V ist endlich erzeugt.

Beweis. (1) $\Longleftrightarrow$ (2): Dies folgt aus Satz 0.0.
(1) $\Longrightarrow$ (3): Sei (1) erfüllt. Dann ist die Menge $\mathfrak{U}$ aller endlich erzeugten Untermoduln von U nichtleer wegen $0 \in \mathfrak{U}$. Wegen (1) enthält $\mathfrak{U}$ ein maximales Element W. Im Fall $W \neq U$ könnte man ein Element $u \in U \setminus W$ wählen. Dann wäre $W < W + Ru \in \mathfrak{U}$ im Widerspruch zur Wahl von W. Also ist $U = W$ endlich erzeugt.
(3) $\Longrightarrow$ (2): Sei (3) erfüllt und $U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$ wie in (2). Man zeigt leicht, dass $U := \bigcup_{k=1}^{\infty} U_k$ ein Untermodul von V ist. Wegen (3) ist U endlich erzeugt, etwa $U = Ru_1 + \cdots + Ru_n$. Jedes u_i ist in einem U_{k_i} enthalten. Sei $k := \max\{k_1, \ldots, k_n\}$. Dann gilt: $u_1, \ldots, u_n \in U_k$, d.h. $U \subseteq U_k \subseteq U_{k+1} \subseteq \ldots \subseteq U$. Insbesondere ist $U_k = U_{k+1} = \ldots$.

Definition. Ggf. heißt V **noethersch**.

Bemerkung. Analog sind für jeden R-Modul V äquivalent:
(1) Jede nichtleere Menge von Untermoduln von V enthält ein minimales Element.
(2) Zu jeder absteigenden Kette $U_1 \supseteq U_2 \supseteq U_3 \supseteq \ldots$ von Untermoduln von V existiert ein $k \in \mathbb{N}$ mit $U_k = U_{k+1} = \ldots$.
Ggf. heißt V **artinsch**.

6.2 Satz. *Für jeden Untermodul U eines R-Moduls V gilt:*

$$V \text{ noethersch (bzw. artinsch)} \Longleftrightarrow U \text{ und } V/U \text{ noethersch (bzw. artinsch).}$$

Beweis. Wir zeigen nur die Aussage über noethersche Moduln; der Rest geht analog.
"$\Longrightarrow$": Sei V noethersch. Dann ist jede nichtleere Menge von Untermoduln von U auch eine nichtleere Menge von Untermoduln von V, enthält also ein maximales Element. Daher ist U noethersch.
Sei $W_1/U \subseteq W_2/U \subseteq W_3/U \subseteq \ldots$ eine aufsteigende Folge von Untermoduln von V/U. Dann ist $W_1 \subseteq W_2 \subseteq W_3 \subseteq \ldots$ eine aufsteigende Folge von Untermoduln von V. Also

existiert ein $k \in \mathbb{N}$ mit $W_k = W_{k+1} = \ldots$. Dann ist auch $W_k/U = W_{k+1}/U = \ldots$. Daher ist V/U noethersch.
"$\Longleftarrow$": Seien U und V/U noethersch, und sei $W_1 \subseteq W_2 \subseteq W_3 \subseteq \ldots$ eine aufsteigende Folge von Untermoduln von V. Dann ist $W_1 + U/U \subseteq W_2 + U/U \subseteq W_3 + U/U \subseteq \ldots$ eine aufsteigende Folge von Untermoduln von V/U. Daher existiert ein $k \in \mathbb{N}$ mit $W_k + U/U = W_{k+1} + U/U = \ldots$, d.h. $W_k + U = W_{k+1} + U = \ldots$.
Analog ist $W_1 \cap U \subseteq W_2 \cap U \subseteq W_3 \cap U \subseteq \ldots$ eine aufsteigende Folge von Untermoduln von U. Daher existiert ein $l \in \mathbb{N}$ mit $W_l \cap U = W_{l+1} \cap U = \ldots$. Mit Dedekinds Lemma folgt für $n \geq \max\{k, l\}$:

$$W_n = W_n + (U \cap W_n) = W_n + (U \cap W_{n+1}) = (W_n + U) \cap W_{n+1} = (W_{n+1} + U) \cap W_{n+1} = W_{n+1}.$$

Bemerkung. (i) Für noethersche (bzw. artinsche) Untermoduln U, U' eines beliebigen R-Moduls ist auch $U + U'$ noethersch (bzw. artinsch); denn der Untermodul U' von $U + U'$ ist noethersch (bzw. artinsch), und der Faktormodul $U + U'/U' \simeq U/U \cap U'$ ist auch noethersch (bzw. artinsch).
(ii) Induktiv folgt: Für noethersche (bzw. artinsche) Untermoduln $U_1, \ldots, U_n$ eines beliebigen R-Moduls ist auch $U_1 + \cdots + U_n$ noethersch (bzw. artinsch).

6.3 Definition. Ist der reguläre R-Modul R noethersch (bzw. artinsch), so heißt R ein **noetherscher** (bzw. **artinscher**) Ring.

Bemerkung. (i) Ggf. ist auch R/I noethersch (bzw. artinsch) für jedes Ideal $I \trianglelefteq R$; denn jeder R/I-Untermodul von R/I hat die Form U/I mit einem R-Untermodul U von R, der I enthält.
(ii) Wir werden später zeigen, dass jeder artinsche Ring auch noethersch ist.

Satz. *Ist R noethersch, so ist jeder endlich erzeugte R-Modul V noethersch; insbesondere ist jeder Untermodul von V endlich erzeugt.*

Beweis. Wir schreiben $V = Rv_1 + \cdots + Rv_n$ mit $v_1, \ldots, v_n \in V$. Für $i = 1, \ldots, n$ ist dann $f_i : R \longrightarrow Rv_i$, $a \longmapsto av_i$, ein R-Epimorphismus; insbesondere ist $Rv_i \simeq R/\mathrm{Ker}(f_i)$ noethersch. Daher ist auch $V = Rv_1 + \cdots + Rv_n$ noethersch.

Beispiel. Jeder HIR ist noethersch; insbesondere sind $\mathbb{Z}$ und jeder Körper noethersch.

6.4 Satz. (Hilberts Basissatz)
Ist R ein noetherscher Ring, so ist auch $R[X]$ ein noetherscher Ring.

Beweis. Wir nehmen an, dass $R[X]$ nicht noethersch ist. Dann enthält $R[X]$ ein Ideal I, das nicht endlich erzeugt ist; insbesondere ist $I \neq 0$. Wir wählen ein Polynom f_1 minimalen Grades in $I \setminus \{0\}$. Dann ist $I \neq (f_1)$. Wir wählen ein Polynom f_2 minimalen Grades in $I \setminus (f_1)$. Dann ist $I \neq (f_1, f_2)$. Wir wählen ein Polynom f_3 minimalen Grades in $I \setminus (f_1, f_2)$, usw. Wir erhalten so Polynome $f_1, f_2, f_3, \ldots \in I$. Für $k \in \mathbb{N}$ sei n_k der Grad und a_k der höchste Koeffizient von f_k. Dann ist $n_1 \leq n_2 \leq n_3 \leq \ldots$ und $(a_1) \subseteq$

$(a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$. Da R noethersch ist, existiert ein $k \in \mathbb{N}$ mit $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1})$. Es existieren also $b_1, \ldots, b_k \in R$ mit $a_{k+1} = \sum_{i=1}^{k} b_i a_i$. Daher ist

$$g := f_{k+1} - \sum_{i=1}^{k} b_i X^{n_{k+1}-n_i} f_i \in I \setminus (f_1, \ldots, f_k)$$

und $\deg(g) < \deg(f_{k+1})$ im Widerspruch zur Wahl von f_{k+1}.

Bemerkung. (i) Induktiv folgt, dass mit R auch der Polynomring $R[X_1, \ldots, X_n]$ in endlich vielen Variablen $X_1, \ldots, X_n$ noethersch ist. Insbesondere sind $\mathbb{Z}[X_1, \ldots, X_n]$ und $K[X_1, \ldots, X_n]$ für jeden Körper K noethersche Ringe. Dagegen ist der Polynomring $\mathbb{Z}[X_1, X_2, \ldots]$ in unendlich vielen Variablen $X_1, X_2, \ldots$ nicht noethersch. (Warum?)
(ii) Ist R ein noetherscher Ring, so ist auch jede endlich erzeugte R-Algebra S ein noetherscher Ring; denn S ist zu einem Restklassenring eines Polynomrings in endlich vielen Variablen über R isomorph.

6.5 Bemerkung. Für jedes Ideal $I \trianglelefteq R$ und jedes Element $a \in R$ ist $f : R \longrightarrow R/I$, $r \longmapsto ra + I$, R-linear mit Bild $Ra + I/I$ und Kern $\{r \in R : ra \in I\} =: (I : a)$; insbesondere ist $I \subseteq (I : a) \trianglelefteq R$, und f induziert eine exakte Folge von R-Moduln und R-Homomorphismen $0 \longrightarrow R/(I : a) \longrightarrow R/I \longrightarrow R/I + Ra \longrightarrow 0$.

Satz. *Sind in dieser Situation $(I : a)$ und $I + Ra$ endlich erzeugt, so ist auch I endlich erzeugt.*

Beweis. Wir schreiben $(I : a) = (c_1, \ldots, c_t)$ und $I + Ra = (b_1, \ldots, b_n, a)$ mit $c_1, \ldots, c_t$, $b_1, \ldots, b_n \in R$; dabei seien o.B.d.A. $b_1, \ldots, b_n \in I$. Dann ist $J := (c_1 a, \ldots, c_t a, b_1, \ldots, b_n) \subseteq I$.
Sei $x \in I \subseteq I + Ra$. Wir schreiben $x = \sum_{i=1}^{n} r_i b_i + ra$ mit $r_1, \ldots, r_n, r \in R$. Dann ist $ra = x - \sum_{i=1}^{n} r_i b_i \in I$, d.h. $r \in (I : a)$. Wir schreiben $r = \sum_{j=1}^{t} s_j c_j$ mit $s_1, \ldots, s_t \in R$. Dann ist $x = \sum_{i=1}^{n} r_i b_i + \sum_{j=1}^{t} s_j c_j a \in J$. Dies zeigt: $I = J$; insbesondere ist I endlich erzeugt.

6.6 Satz. (Cohen)
Genau dann ist R noethersch, wenn alle $P \in \mathrm{Spec}(R)$ endlich erzeugt sind.

Beweis. Sei R nichtnoethersch. Dann ist die Menge $\mathfrak{A}$ aller nicht endlich erzeugten Ideale von R nichtleer und durch $\subseteq$ geordnet. Sei $\mathfrak{B}$ eine nichtleere total geordnete Teilmenge von $\mathfrak{A}$. Dann ist $S := \bigcup_{B \in \mathfrak{B}} B = \sum_{B \in \mathfrak{B}} B \trianglelefteq R$. Ferner ist S nicht endlich erzeugt; denn ein endliches Erzeugendensystem X von S wäre bereits in einem $B \in \mathfrak{B}$ enthalten. Also wäre $B \subseteq S = RX \subseteq B$, d.h. $B = S$ wäre endlich erzeugt.
Also ist S eine obere Schranke von $\mathfrak{B}$ in $\mathfrak{A}$. Nach Zorns Lemma enthält $\mathfrak{A}$ ein maximales Element P. Wir nehmen $P \notin \mathrm{Spec}(R)$ an. Dann existieren $a, b \in R \setminus P$ mit $ab \in P$. Also ist $P < P + Ra$ und $P < (P : a)$ wegen $b \in (P : a)$. Nach Wahl von P sind $P + Ra$ und $(P : a)$ endlich erzeugt. Nach Satz 6.5 ist auch P endlich erzeugt. Damit haben wir einen Widerspruch.
Dies zeigt, dass R ein nicht endlich erzeugtes Primideal enthält.

6.7 Satz. *Sei $R[[X]]$ der Potenzreihenring über R. Dann ist*

$$\phi : R[[X]] \longrightarrow R, \quad \sum_{i=0}^{\infty} a_i X^i \longmapsto a_0,$$

ein Ringepimorphismus. Für $I \trianglelefteq R[[X]]$ ist also $\phi(I) \trianglelefteq R$. Für $P \in \mathrm{Spec}(R[[X]])$ gilt dabei: P endlich erzeugt $\iff$ $\phi(P)$ endlich erzeugt.

Beweis. Sicher ist ϕ ein Epimorphismus, Für jedes Ideal I von $R[[X]]$ ist also $\phi(I) \trianglelefteq R$, und aus $I = (f_1, \ldots, f_r)$ folgt $\phi(I) = (\phi(f_1), \ldots, \phi(f_r))$.
Sei jetzt umgekehrt $P \in \mathrm{Spec}(R[[X]])$ und $\phi(P) = (a_1, \ldots, a_r)$ mit $a_1, \ldots, a_r \in R$. Für $i = 1, \ldots, r$ enthält also P ein Element der Form $f_i = a_i + b_{i1}X + b_{i2}X^2 + \cdots$.
Im Fall $X \in P$ ist dann $P = (X, f_1, \ldots, f_r)$; denn ist $f = a + b_1X + b_2X^2 + \cdots \in P$, so ist $a \in \phi(P) = (a_1, \ldots, a_r)$. Daher existieren $c_1, \ldots, c_r \in R$ mit $a = c_1a_1 + \cdots + c_ra_r$. Dann ist $f - \sum_{i=1}^r c_if_i \in \mathrm{Ker}(\phi) = (X)$, d.h. $f \in (X, f_1, \ldots, f_r)$.
Im Fall $X \notin P$ ist $P = (f_1, \ldots, f_r)$; denn ist $f = a + b_1X + b_2X^2 + \cdots \in P$, so ist wieder $a \in \phi(P) = (a_1, \ldots, a_r)$. Daher existieren $c_1, \ldots, c_r \in R$ mit $a = c_1a_1 + \cdots + c_ra_r$. Dann ist $f - \sum_{i=1}^r c_if_i \in \mathrm{Ker}(\phi) = (X)$. Wir schreiben $f - \sum_{i=1}^r c_if_i = Xg$ mit $g \in R[[X]]$. Dann ist $Xg \in P$, also $g \in P$ wegen $X \notin P$. Analog existieren $d_1, \ldots, d_r \in R$ und $h \in R[[X]]$ mit $g - \sum_{i=1}^r d_if_i = Xh$. Fährt man so fort, so ist schließlich $f = \sum_{i=1}^r (c_i + d_iX + \cdots)f_i \in (f_1, \ldots, f_r)$.

Bemerkung. Aus Satz 6.7 folgt also: R noethersch $\iff$ $R[[X]]$ noethersch.

7. Spektrum und Zariski-Topologie

Sei R ein Ring.

7.1 Definition. Für $T \subseteq R$ sei

$$\mathcal{V}(T) := \mathcal{V}_R(T) := \{P \in \mathrm{Spec}(R) : T \subseteq P\} \subseteq \mathrm{Spec}(R).$$

Bemerkung. (i) Für $I := (T)$ ist dann $\mathcal{V}(T) = \mathcal{V}(I) = \mathcal{V}(\mathrm{rad}(I))$. Der Buchstabe $\mathcal{V}$ steht für *Varietät*, einen Begriff aus der Algebraischen Geometrie.
(ii) Offenbar ist $\mathcal{V}(\emptyset) = \mathrm{Spec}(R)$ und $\mathcal{V}(R) = \emptyset$.
(iii) Für jede nichtleere Familie $(I_\gamma)_{\gamma\in\Gamma}$ von Idealen in R ist

$$\mathcal{V}(\sum_{\gamma\in\Gamma} I_\gamma) = \bigcap_{\gamma\in\Gamma} \mathcal{V}(I_\gamma).$$

(iv) Für $I, J \trianglelefteq R$ mit $I \subseteq J$ ist offenbar $\mathcal{V}(J) \subseteq \mathcal{V}(I)$.
(v) Für $I, J \trianglelefteq R$ ist ferner $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J) = \mathcal{V}(IJ)$; denn wegen $IJ \subseteq I \cap J \subseteq I$ ist einerseits $\mathcal{V}(I) \subseteq \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ)$ und analog $\mathcal{V}(J) \subseteq \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ)$, d.h. $\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ)$. Andererseits gilt für $P \in \mathrm{Spec}(R)$ mit $P \notin \mathcal{V}(I) \cup \mathcal{V}(J)$: $I \not\subseteq P$ und $J \not\subseteq P$. Daher ist $IJ \not\subseteq P$ und damit $P \notin \mathcal{V}(IJ)$.

(vi) Daher existiert genau eine Topologie $\mathcal{Z}$, die **Zariski-Topologie**, auf $\mathrm{Spec}(R)$ mit der Eigenschaft, dass die Mengen $\mathcal{V}(I)$ $(I \trianglelefteq R)$ genau die abgeschlossenen Mengen bzgl. $\mathcal{Z}$ sind.
(vii) Der topologische Raum $(\mathrm{Spec}(R), \mathcal{Z})$ ist quasikompakt.
[Zum Beweis sei eine Überdeckung von $\mathrm{Spec}(R)$ mit offenen Mengen $\mathrm{Spec}(R) \setminus \mathcal{V}(I)$ gegeben; dabei durchläuft I eine Menge $\mathfrak{I}$ von Idealen von R. Dann ist $\emptyset = \bigcap_{I\in\mathfrak{I}} \mathcal{V}(I) = \mathcal{V}(\sum_{I\in\mathfrak{I}} I)$, d.h. es gibt kein Primideal von R, das $\sum_{I\in\mathfrak{I}} I$ enthält. Daher ist $\sum_{I\in\mathfrak{I}} I = R$. Folglich existieren $I_1, \ldots, I_n \in \mathfrak{I}$ mit $1 \in I_1 + \cdots + I_n$. Daher ist

$$\emptyset = \mathcal{V}(R) = \mathcal{V}(I_1 + \cdots + I_n) = \bigcap_{j=1}^{n} \mathcal{V}(I_j)$$

und $\mathrm{Spec}(R) = \bigcup_{j=1}^{n} (\mathrm{Spec}(R) \setminus \mathcal{V}(I_j))$.]

Beispiel. In $\mathrm{Spec}(\mathbb{Z})$ sind genau $\mathrm{Spec}(\mathbb{Z})$ selbst und die Mengen $\{(p_1), \ldots, (p_r)\}$ mit $p_1, \ldots, p_r \in \mathbb{P}$ und $r \in \mathbb{N}_0$ abgeschlossen. Daher ist die einelementige Menge $\{(0)\}$ nicht abgeschlossen in $\mathrm{Spec}(\mathbb{Z})$. Daher ist $\mathrm{Spec}(\mathbb{Z})$ kein T_1-Raum, also auch kein T_2-Raum (Hausdorff-Raum).

Satz. *(i) Jeder Ringhomomorphismus $f : R \longrightarrow S$ induziert eine stetige Abbildung*

$$f^* : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R), \quad Q \longmapsto f^{-1}(Q).$$

(ii) Ist $I \trianglelefteq R$ und $f : R \longrightarrow S := R/I$ kanonisch, so ist

$$f' : \mathrm{Spec}(R/I) \longrightarrow \mathcal{V}(I), \quad Q \longmapsto f^{-1}(Q),$$

ein Homöomorphismus; dabei fasst man $\mathcal{V}(I)$ als topologischen Unterraum von $\mathrm{Spec}(R)$ *auf.*

(iii) Insbesondere ist $\mathrm{Spec}(R/I) \sim \mathrm{Spec}(R)$ *für* $I := \mathrm{nil}(R)$.

Beweis. (i) Für $Q \in \mathrm{Spec}(S)$ ist $f^{-1}(Q) \in \mathrm{Spec}(R)$ nach Bemerkung 4.2, und für $I \trianglelefteq R$ gilt:

$$Q \in (f^*)^{-1}(\mathcal{V}(I)) \Longleftrightarrow f^*(Q) \in \mathcal{V}(I) \Longleftrightarrow I \subseteq f^{-1}(Q) \Longleftrightarrow f(I) \subseteq Q.$$

Daher ist $(f^*)^{-1}(\mathcal{V}(I)) = \mathcal{V}(f(I)) \subseteq \mathrm{Spec}(S)$ abgeschlossen. Also sind Urbilder abgeschlossener Teilmengen wieder abgeschlossen. Folglich ist f^* stetig.

(ii) Seien I, S, f wie oben. Dann ist f^* injektiv mit Bild $\mathcal{V}(I)$, d.h. f' ist bijektiv und stetig. Ist $\mathfrak{A} \subseteq \mathrm{Spec}(R/I)$ abgeschlossen, so existiert ein $J \trianglelefteq R$ mit $I \subseteq J$ und $\mathfrak{A} = \mathcal{V}(J/I)$. Dann ist $f'(\mathfrak{A}) = \mathcal{V}(J)$ abgeschlossen in $\mathrm{Spec}(R)$ und $\mathcal{V}(I)$. Dies zeigt, dass f' ein Homöomorphismus ist.

(iii) ist ein Spezialfall von (ii).

7.2 Bemerkung. (i) Für $\mathfrak{Q} \subseteq \mathrm{Spec}(R)$ ist $\mathcal{I}(\mathfrak{Q}) := \bigcap_{P\in\mathfrak{Q}} P \trianglelefteq R$ ein Radikalideal nach Bemerkung 4.6 (vii). Man nennt $\mathcal{I}\mathfrak{Q}$ das **Verschwindungsideal** von $\mathfrak{Q}$.
(ii) Für $\mathfrak{P} \subseteq \mathfrak{Q} \subseteq \mathrm{Spec}(R)$ ist $\mathcal{I}(\mathfrak{Q}) \subseteq \mathcal{I}(\mathfrak{P})$.

(iii) Für $I \trianglelefteq R$ ist

$$\mathcal{I}(\mathcal{V}(I)) = \bigcap_{P \in \mathcal{V}(I)} P = \bigcap_{I \subseteq P \in \mathrm{Spec}(R)} P = \mathrm{rad}(I).$$

(iv) Für $\mathfrak{Q} \subseteq \mathrm{Spec}(R)$ ist umgekehrt $\mathcal{V}(\mathcal{I}(\mathfrak{Q}))$ der Abschluss $\overline{\mathfrak{Q}}$ von $\mathfrak{Q}$ in $\mathrm{Spec}(R)$; denn für $Q \in \mathfrak{Q}$ ist $\mathcal{I}(\mathfrak{Q}) = \bigcap_{P \in \mathfrak{Q}} P \subseteq Q$, d.h. $Q \in \mathcal{V}(\mathcal{I}(\mathfrak{Q}))$. Daher ist $\mathfrak{Q}$ in der abgeschlossenen Teilmenge $\mathcal{V}(\mathcal{I}(\mathfrak{Q}))$ von $\mathrm{Spec}(R)$ enthalten. Also gilt auch $\overline{\mathfrak{Q}} \subseteq \mathcal{V}(\mathcal{I}(\mathfrak{Q}))$. Ist $I \trianglelefteq R$ mit $\overline{\mathfrak{Q}} = \mathcal{V}(I)$, so ist $I \subseteq \mathrm{rad}(I) = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\overline{\mathfrak{Q}}) \subseteq \mathcal{I}(\mathfrak{Q})$ und damit $\overline{\mathfrak{Q}} = \mathcal{V}(I) \supseteq \mathcal{V}(\mathcal{I}(\mathfrak{Q}))$.
(v) Durch $\mathcal{V}$ und $\mathcal{I}$ erhält man zueinander inverse Bijektionen

$$\{\text{Radikalideale von } R\} \longleftrightarrow \{\text{abgeschlossene Teilmengen von } \mathrm{Spec}(R)\};$$

denn für jedes Radikalideal $J \trianglelefteq R$ ist $\mathcal{V}(J) \subseteq \mathrm{Spec}(R)$ abgeschlossen, und für jede abgeschlossene Teilmenge $\mathfrak{Q} \subseteq \mathrm{Spec}(R)$ existiert ein Ideal $I \trianglelefteq R$ mit $\mathfrak{Q} = \mathcal{V}(I)$. Daher ist $\mathcal{I}(\mathfrak{Q}) = \mathcal{I}(\mathcal{V}(I)) = \mathrm{rad}(I) \trianglelefteq R$ ein Radikalideal. Dabei ist $\mathcal{I}(\mathcal{V}(J)) = \mathrm{rad}(J) = J$ und $\mathcal{V}(\mathcal{I}(\mathfrak{Q})) = \overline{\mathfrak{Q}} = \mathfrak{Q}$.
(vi) Für $P \in \mathrm{Spec}(R)$ ist $\mathcal{I}(\{P\}) = P$, also $\overline{\{P\}} = \mathcal{V}(\mathcal{I}(\{P\})) = \mathcal{V}(P) = \{Q \in \mathrm{Spec}(R) : P \subseteq Q\}$; insbesondere ist P das kleinste Element in $\overline{\{P\}}$. Dies zeigt, dass $\mathrm{Spec}(R)$ ein T_0-Raum ist.

7.3 Satz. *Für jede abgeschlossene Teilmenge $\mathfrak{A} \subseteq \mathrm{Spec}(R)$ gilt: $\mathfrak{A}$ irreduzibel $\Longleftrightarrow \mathcal{I}(\mathfrak{A}) \in \mathrm{Spec}(R)$.*

Beweis. "$\Longrightarrow$": Sei $\mathcal{I}(\mathfrak{A}) \notin \mathrm{Spec}(R)$. Dann existieren $a, b \in R \setminus \mathcal{I}(\mathfrak{A})$ mit $ab \in \mathcal{I}(\mathfrak{A})$. Wir setzen $I := \mathcal{I}(\mathfrak{A}) + Ra$ und $J := \mathcal{I}(\mathfrak{A}) + Rb$. Wegen $\mathcal{I}(\mathfrak{A}) \subseteq I$ ist $\mathcal{V}(I) \subseteq \mathcal{V}(\mathcal{I}(\mathfrak{A})) = \mathfrak{A}$. Analog ist $\mathcal{V}(J) \subseteq \mathfrak{A}$. Andererseits ist $IJ \subseteq \mathcal{I}(\mathfrak{A})$, d.h.

$$\mathfrak{A} = \mathcal{V}(\mathcal{I}(\mathfrak{A})) \subseteq \mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathfrak{A}.$$

Insgesamt ist also $\mathfrak{A} = \mathcal{V}(I) \cup \mathcal{V}(J)$. Im Fall $\mathfrak{A} = \mathcal{V}(I)$ hätte man den Widerspruch $a \in I \subseteq \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathfrak{A})$. Daher ist $\mathfrak{A} \neq \mathcal{V}(I)$ und analog $\mathfrak{A} \neq \mathcal{V}(J)$. Also ist $\mathfrak{A}$ nicht irreduzibel.
"$\Longleftarrow$": Sei $\mathfrak{A} = \mathfrak{A}_1 \cup \mathfrak{A}_2$ mit echten abgeschlossenen Teilmengen $\mathfrak{A}_1, \mathfrak{A}_2$. Dann ist

$$\mathcal{V}(\mathcal{I}(\mathfrak{A})) = \mathfrak{A} = \mathfrak{A}_1 \cup \mathfrak{A}_2 = \mathcal{V}(\mathcal{I}(\mathfrak{A}_1)) \cup \mathcal{V}(\mathcal{I}(\mathfrak{A}_2)) = \mathcal{V}(\mathcal{I}(\mathfrak{A}_1) \cap \mathcal{I}(\mathfrak{A}_2));$$

dabei ist $\mathcal{I}(\mathfrak{A}_1) \cap \mathcal{I}(\mathfrak{A}_2) = \mathcal{I}(\mathfrak{A}_1 \cup \mathfrak{A}_2) \trianglelefteq R$ ein Radikalideal. Also ist $\mathcal{I}(\mathfrak{A}) = \mathcal{I}(\mathfrak{A}_1) \cap \mathcal{I}(\mathfrak{A}_2) \supseteq \mathcal{I}(\mathfrak{A}_1)\mathcal{I}(\mathfrak{A}_2)$. Wegen $\mathcal{I}(\mathfrak{A}_1) \supset \mathcal{I}(\mathfrak{A}) \subset \mathcal{I}(\mathfrak{A}_2)$ folgt : $\mathcal{I}(\mathfrak{A}) \notin \mathrm{Spec}(R)$.

Bemerkung. Die Bijektionen aus Bemerkung 7.2 (iv) liefern also Bijektionen

$$\mathrm{Spec}(R) \longleftrightarrow \{\text{irreduzible abgeschlossene Teilmengen von } \mathrm{Spec}(R)\}.$$

Diese induzieren offenbar Bijektionen

$$\mathrm{Min}(R) \longleftrightarrow \{\text{irreduzible Komponenten von } \mathrm{Spec}(R)\}.$$

7.4 Satz. *Die Abbildung*

$$\alpha\colon \{e \in R\colon e^2 = e\} \longrightarrow \{\mathfrak{Q} \subseteq \operatorname{Spec}(R)\colon \mathfrak{Q} \text{ offen und abgeschlossen}\},\ \ e \longmapsto \mathcal{V}(e) := \mathcal{V}(Re),$$

ist bijektiv.

Beweis. Für jedes Idempotent $e \in R$ ist $\operatorname{Spec}(R) = \mathcal{V}(0) = \mathcal{V}(e(1-e)) = \mathcal{V}(e) \cup \mathcal{V}(1-e)$ und $\mathcal{V}(e) \cap \mathcal{V}(1-e) \subseteq \mathcal{V}(1) = \emptyset$, d.h. $\operatorname{Spec}(R)$ ist die disjunkte Vereinigung von $\mathcal{V}(e)$ und $\mathcal{V}(1-e)$; insbesondere ist $\mathcal{V}(e) \subseteq \operatorname{Spec}(R)$ offen und abgeschlossen.

Sei $N := \operatorname{nil}(R)$. Satz 1.1 liefert eine Bijektion $e \longmapsto e+N$ zwischen den Idempotenten von R und denen von R/N, und Satz 7.1 liefert eine Bijektion $\mathfrak{Q} \longmapsto \widetilde{\mathfrak{Q}} := \{P/N : P \in \mathfrak{Q}\}$ zwischen den offenen abgeschlossenen Teilmengen von $\operatorname{Spec}(R)$ und denen von $\operatorname{Spec}(R/N)$. Dabei gilt: $\mathcal{V}(e+N) = \widetilde{\mathcal{V}(e)}$, wie man leicht nachrechnet. Daher genügt es, die Aussage für R/N statt R zu zeigen. Wir können also o.B.d.A. $N = 0$ annehmen.

Für jedes Idempotent $e \in R$ ist $Re \subseteq \operatorname{rad}(Re) = \mathcal{I}(\mathcal{V}(Re)) = \mathcal{I}(\mathcal{V}(e)) =: I$. Analog ist $R(1-e) \subseteq \mathcal{I}(\mathcal{V}(1-e)) =: J$, und

$$IJ \subseteq I \cap J = \bigcap_{P \in \mathcal{V}(e)} P \cap \bigcap_{P \in \mathcal{V}(1-e)} P = \bigcap_{P \in \operatorname{Spec}(R)} P = N = 0,$$

also $I \subseteq Ie + I(1-e) = Ie \subseteq Re$. Folglich ist $\mathcal{I}(\mathcal{V}(e)) = I = Re$; insbesondere ist e das Einselement von $\mathcal{I}(\mathcal{V}(e))$. Dies zeigt die Injektivität von α.

Zum Beweis der Surjektivität sei $\mathfrak{Q} \subseteq \operatorname{Spec}(R)$ offen und abgeschlossen. Dann ist auch $\mathfrak{Q}' := \operatorname{Spec}(R) \setminus \mathfrak{Q} \subseteq \operatorname{Spec}(R)$ offen und abgeschlossen. Ferner sind $\mathcal{I}(\mathfrak{Q}) = \bigcap_{P \in \mathfrak{Q}} P$ und $\mathcal{I}(\mathfrak{Q}') = \bigcap_{P \in \mathfrak{Q}'} P$ Ideale in R mit $\mathcal{I}(\mathfrak{Q})\mathcal{I}(\mathfrak{Q}') \subseteq \mathcal{I}(\mathfrak{Q}) \cap \mathcal{I}(\mathfrak{Q}') = \bigcap_{P \in \operatorname{Spec}(R)} P = N = 0$.

Andererseits ist $\mathcal{V}(\mathcal{I}(\mathfrak{Q}) + \mathcal{I}(\mathfrak{Q}')) = \mathcal{V}(\mathcal{I}(\mathfrak{Q})) \cap \mathcal{V}(\mathcal{I}(\mathfrak{Q}')) = \mathfrak{Q} \cap \mathfrak{Q}' = \emptyset$, d.h. $R = \mathcal{I}(\mathfrak{Q}) + \mathcal{I}(\mathfrak{Q}') = \mathcal{I}(\mathfrak{Q}) \oplus \mathcal{I}(\mathfrak{Q}')$. Daher existieren $e \in \mathcal{I}(\mathfrak{Q})$, $f \in \mathcal{I}(\mathfrak{Q}')$ mit $1 = e + f$. Wegen $e(1-e) = ef \in \mathcal{I}(\mathfrak{Q})\mathcal{I}(\mathfrak{Q}') = 0$ ist $e^2 = e$. Wegen $Re \subseteq \mathcal{I}(\mathfrak{Q}) \subseteq \mathcal{I}(\mathfrak{Q})e + \mathcal{I}(\mathfrak{Q})f = \mathcal{I}(\mathfrak{Q})e \subseteq Re$ ist $\mathcal{I}(\mathfrak{Q}) = Re$ und damit $\mathfrak{Q} = \mathcal{V}(\mathcal{I}(\mathfrak{Q})) = \mathcal{V}(Re) = \mathcal{V}(e)$. Damit ist die Surjektivität von α gezeigt.

Bemerkung. (i) Für Idempotente $e, f \in R$ ist auch ef ein Idempotent. Dabei gilt: $\mathcal{V}(ef) = \mathcal{V}(e) \cup \mathcal{V}(f)$.
(ii) Der Beweis von Satz 7.4 zeigt: $\mathcal{V}(1-e) = \operatorname{Spec}(R) \setminus \mathcal{V}(e)$.
(iii) Für Idempotente $e, f \in R$ ist auch $e \vee f := e + f - ef$ ein Idempotent mit $\mathcal{V}(e \vee f) = \mathcal{V}(e) \cap \mathcal{V}(f)$; dies rechnet man leicht nach.

7.5 Satz. *Ist $R \neq 0$, so gilt: R zusammenhängend $\iff \operatorname{Spec}(R)$ zusammenhängend.*

Beweis. Enthält R ein Idempotent e mit $0 \neq e \neq 1$, so ist $\operatorname{Spec}(R)$ nach Satz 7.4 die disjunkte Vereinigung der abgeschlossenen Teilmengen $\mathcal{V}(e)$ und $\operatorname{Spec}(R) \setminus \mathcal{V}(e)$ mit $\operatorname{Spec}(R) = \mathcal{V}(0) \neq \mathcal{V}(e) \neq \mathcal{V}(1) = \emptyset$. Die Umkehrung zeigt man analog.

7.6 Bemerkung. Die Mengen

$$\mathcal{D}(a) := \mathcal{D}_R(a) := \{P \in \operatorname{Spec}(R) : a \notin P\} = \operatorname{Spec}(R) \setminus \mathcal{V}(a)$$

($a \in R$) bilden eine Basis der Zariski-Topologie auf $\mathrm{Spec}(R)$; denn für $I \trianglelefteq R$ gilt:

$$\mathrm{Spec}(R) \setminus \mathcal{V}(I) = \{P \in \mathrm{Spec}(R) : I \not\subseteq P\} = \bigcup_{a \in I} \{P \in \mathrm{Spec}(R) : a \notin P\} = \bigcup_{a \in I} \mathcal{D}(a).$$

Satz. *Für $a, b \in R$ gilt:*
(i) $\mathcal{D}(ab) = \mathcal{D}(a) \cap \mathcal{D}(b)$;
(ii) $\mathcal{D}(a) = \emptyset \iff a \in \mathrm{nil}(R)$;
(iii) $\mathcal{D}(a) = \mathrm{Spec}(R) \iff a \in R^\times$.

Beweis. (i) Für $P \in \mathrm{Spec}(R)$ gilt: $P \in \mathcal{D}(ab) \iff ab \notin P \iff a \notin P \wedge b \notin P \iff P \in \mathcal{D}(a) \wedge P \in \mathcal{D}(b) \iff P \in \mathcal{D}(a) \cap \mathcal{D}(b)$.
(ii) $\mathcal{D}(a) = \emptyset \iff a \in P$ für alle $P \in \mathrm{Spec}(R) \iff a = \bigcap_{P \in \mathrm{Spec}(R)} P = \mathrm{nil}(R)$.
(iii) $\mathcal{D}(a) = \mathrm{Spec}(R) \iff a \notin P$ für alle $P \in \mathrm{Spec}(R) \iff a \in R^\times$.

7.7 Satz. *Ist R ein noetherscher Ring, so ist $\mathrm{Spec}(R)$ ein noetherscher topologischer Raum. Insbesondere ist jede Teilmenge von $\mathrm{Spec}(R)$ quasikompakt (in der induzierten Topologie).*

Beweis. Sei R noethersch und $\mathfrak{A}_1 \supseteq \mathfrak{A}_2 \supseteq \mathfrak{A}_3 \supseteq \ldots$ eine Folge abgeschlossener Teilmengen von $\mathrm{Spec}(R)$. Dann ist $\mathcal{I}(\mathfrak{A}_1) \subseteq \mathcal{I}(\mathfrak{A}_2) \subseteq \mathcal{I}(\mathfrak{A}_3) \subseteq \ldots$ eine Folge von Idealen in R. Also existiert ein $k \in \mathbb{N}$ mit $\mathcal{I}(\mathfrak{A}_k) = \mathcal{I}(\mathfrak{A}_{k+1}) = \ldots$. Anwendung von $\mathcal{V}$ liefert dann $\mathfrak{A}_k = \mathfrak{A}_{k+1} = \ldots$. Dies zeigt, dass $\mathrm{Spec}(R)$ noethersch ist. Der Rest folgt aus Satz 0.5.

Beispiel. Sei R ein HIR (z.B. $R = \mathbb{Z}$), und sei $0 \neq r \in R$ mit Primfaktorzerlegung $r = p_1^{t_1} \cdots p_s^{t_s}$. Dann ist

$$\mathcal{V}(r) := \mathcal{V}(\{r\}) = \{(p_1), \ldots, (p_s)\} = \{(p_1)\} \cup \ldots \cup \{(p_s)\}$$

mit abgeschlossenen Teilmengen $\{(p_1)\}, \ldots, \{(p_s)\} \subseteq \mathrm{Spec}(R)$. Daher sind $\{(p_1)\}, \ldots, \{(p_s)\}$ die irreduziblen Komponenten von $\mathcal{V}(r)$.

7.8 Satz. *Sei R noethersch und $I \trianglelefteq R$, und seien $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ die irreduziblen Komponenten von $\mathcal{V}(I)$. Dann sind $P_1 := \mathcal{I}(\mathfrak{A}_1), \ldots, P_k := \mathcal{I}(\mathfrak{A}_k)$ genau die minimalen Elemente in $\mathcal{V}(I)$, und es gilt: $\mathrm{rad}(I) = P_1 \cap \ldots \cap P_k$. Dabei kann man kein P_i weglassen.*

Beweis. Nach Satz 7.7 ist $\mathcal{V}(I)$ ein noetherscher topologischer Raum. Nach Satz 0.5 hat $\mathcal{V}(I)$ nur endlich viele irreduzible Komponenten $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$. Diese sind abgeschlossen und irreduzibel in $\mathrm{Spec}(R)$. Nach Bemerkung 7.3 gilt für $i = 1, \ldots, k$: $P_i := \mathcal{I}(\mathfrak{A}_i) \in \mathrm{Spec}(R)$. Wegen $\mathcal{V}(I) = \mathfrak{A}_1 \cup \cdots \cup \mathfrak{A}_k$ ist $I \subseteq \mathrm{rad}(I) = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathfrak{A}_1) \cap \cdots \cap \mathcal{I}(\mathfrak{A}_k) = P_1 \cap \cdots \cap P_k$. Insbesondere gilt für $i = 1, \ldots, k$: $P_i \in \mathcal{V}(I)$.

Ist $Q \in \mathcal{V}(I)$ mit $Q \subseteq P_i$, so ist $\mathfrak{A}_i = \mathcal{V}(P_i) \subseteq \mathcal{V}(Q) \subseteq \mathcal{V}(I)$. Da $\mathcal{V}(Q)$ abgeschlossen und irreduzibel in $\mathrm{Spec}(R)$ und $\mathcal{V}(I)$ ist, folgt: $\mathfrak{A}_i = \mathcal{V}(Q)$ und damit $P_i = \mathcal{I}(\mathfrak{A}_i) = \mathcal{I}(\mathcal{V}(Q)) = Q$. Also ist P_i minimal in $\mathcal{V}(I)$.

Sei jetzt $P \in \mathcal{V}(I)$ beliebig. Wegen $I \subseteq P$ ist dann $\mathcal{V}(P)$ eine irreduzible abgeschlossene Teilmenge von $\mathrm{Spec}(R)$ und $\mathcal{V}(I)$. Folglich ist $\mathcal{V}(P) \subseteq \mathfrak{A}_j$ für ein $j \in \{1, \ldots, k\}$. Daher

ist $P_j = \mathcal{I}(\mathfrak{A}_j) \subseteq \mathcal{I}(\mathcal{V}(P)) = P$. Dies zeigt, dass $P_1, \ldots, P_k$ genau die minimalen Elemente in $\mathcal{V}(I)$ sind.

Im Fall $\mathrm{rad}(I) = P_2 \cap \cdots \cap P_k$ wäre $\mathcal{V}(I) = \mathcal{V}(\mathrm{rad}(I)) = \mathcal{V}(P_2) \cup \cdots \cup \mathcal{V}(P_k) = \mathfrak{A}_2 \cup \cdots \cup \mathfrak{A}_k$ im Widerspruch zu Bemerkung 0.5.

7.9 Satz. *Sei R noethersch. Dann enthält R nur endlich viele minimale Primideale $P_1, \ldots, P_s$. Dabei ist $P_1 \cup \cdots \cup P_s \subseteq \mathrm{Z}(R)$. Ist R auch reduziert, so gilt sogar: $P_1 \cup \cdots \cup P_s = \mathrm{Z}(R)$.*

Beweis. Dies folgt aus Satz 7.8 (mit $I := 0$) und aus Satz 4.5.

8. Quotientenringe und Quotientenmoduln

Sei A eine multiplikative Teilmenge eines Rings R.

8.1 Bemerkung. (i) Für jeden R-Modul V erhält man eine Äquivalenzrelation $\sim$ auf $V \times A$ durch:

$$(v, a) \sim (w, b) :\Longleftrightarrow \exists c \in A : caw = cbv :$$

Reflexivität: Für $v \in V$, $a \in A$ ist $(v, a) \sim (v, a)$ wegen $1 \cdot av = 1 \cdot av$.

Symmetrie: Seien $(v, a), (w, b) \in V \times A$ mit $(v, a) \sim (w, b)$. Dann existiert ein $c \in A$ mit $caw = cbv$, d.h. $(w, b) \sim (v, a)$.

Transitivität: Seien $(u, a), (v, b), (w, c) \in V \times A$ mit $(u, a) \sim (v, b)$ und $(v, b) \sim (w, c)$. Dann existieren $d, e \in A$ mit $dav = dbu$ und $ebw = ecv$. Daher ist $bde \in A$ und $bdecu = ecdav = daebw = bdeaw$, d.h. $(u, a) \sim (w, c)$.

(ii) Für $v \in V$ und $a \in A$ sei $\frac{v}{a}$ die Äquivalenzklasse von (v, a) bzgl. $\sim$. Für $b \in A$ ist dann $\frac{v}{a} = \frac{bv}{ba}$; denn wegen $1bav = 1abv$ ist $(v, a) \sim (bv, ba)$. Man kann so **Brüche** *erweitern* und *kürzen*.

(iii) $A^{-1}V := \{\frac{v}{a} : v \in V,\ a \in A\}$ wird zu einer abelschen Gruppe durch

$$\frac{v}{a} + \frac{w}{b} := \frac{bv + aw}{ab} \qquad (v, w \in V;\ a, b \in A) :$$

Wohldefiniertheit: Sei $\frac{v}{a} = \frac{v'}{a'}$. Dann existiert ein $c \in A$ mit $ca'v = cav'$. Daher gilt:

$$\frac{bv + aw}{ab} = \frac{ca'bv + ca'aw}{ca'ab} = \frac{cabv' + ca'aw}{ca'ab} = \frac{bv' + a'w}{a'b}.$$

Analog argumentiert man im Fall $\frac{w}{b} = \frac{w'}{b'}$.

Kommutativität: $\frac{u}{a} + \frac{v}{b} = \frac{bu+av}{ab} = \frac{av+bu}{ba} = \frac{v}{b} + \frac{u}{a}$.

Assoziativität: $(\frac{u}{a} + \frac{v}{b}) + \frac{w}{c} = \frac{bu+av}{ab} + \frac{w}{c} = \frac{cbu+cav+abw}{abc} = \frac{u}{a} + \frac{cv+bw}{bc} = \frac{u}{a} + (\frac{v}{b} + \frac{w}{c})$.

Neutrales Element: $\frac{u}{a} + \frac{0}{1} = \frac{1u+a0}{a1} = \frac{u}{a}$.

Negative Elemente: $\frac{u}{a} + \frac{-u}{a} = \frac{au+a(-u)}{a^2} = \frac{0}{a^2} = \frac{0a^2}{a^2} = \frac{0}{1}$.

(iv) $A^{-1}V$ wird zu einem R-Modul mit

$$r \cdot \frac{v}{a} := \frac{rv}{a} \qquad (r \in R,\ v \in V,\ a \in A):$$

Wohldefiniertheit: Sei $\frac{v}{a} = \frac{v'}{a'}$. Dann existiert ein $b \in A$ mit $ba'v = bav'$. Daher gilt: $\frac{rv}{a} = \frac{ba'rv}{ba'a} = \frac{barv'}{ba'a} = \frac{rv'}{a'}$.

Assoziativität: $r(s\frac{v}{a}) = r\frac{sv}{a} = \frac{r\cdot sv}{a} = \frac{rs\cdot v}{a} = (rs)\frac{v}{a}$.

Distributivität: $r(\frac{v}{a} + \frac{w}{b}) = r\frac{bv+aw}{ab} = \frac{rbv+raw}{ab} = \frac{rv}{a} + \frac{rw}{b} = r\frac{v}{a} + r\frac{w}{b}$ und $(r+s)\frac{v}{a} = \frac{(r+s)v}{a} = \frac{a(r+s)v}{a^2} = \frac{arv+asv}{a^2} = \frac{rv}{a} + \frac{sv}{a} = r\frac{v}{a} + s\frac{v}{a}$.

Neutrales Element: $1 \cdot \frac{v}{a} = \frac{1v}{a} = \frac{v}{a}$.

Der R-Modul $A^{-1}V$ heißt **Quotientenmodul** von V bzgl. A.

(v) Die **kanonische** Abbildung $\lambda : V \longrightarrow A^{-1}V$, $v \longmapsto \frac{v}{1}$, ist ein R-Homomorphismus; denn für $v, w \in V$, $r, s \in R$ gilt:

$$\lambda(rv + sw) = \frac{rv + sw}{1} = \frac{rv}{1} + \frac{sw}{1} = r\frac{v}{1} + s\frac{w}{1} = r\lambda(v) + s\lambda(w).$$

(vi) Für $v \in V$, $a \in A$ gilt in $A^{-1}V$:

$$\frac{v}{a} = 0 \Longleftrightarrow \exists b \in A : b1v = ba0 \Longleftrightarrow \exists b \in A : bv = 0.$$

Daher ist $\mathrm{T}_A(V) := \{v \in V : \exists b \in A : bv = 0\} = \mathrm{Ker}(\lambda)$; man nennt $\mathrm{T}_A(V)$ den **A-Torsionsmodul** von V. Dann gilt:

$$A^{-1}V = 0 \Longleftrightarrow \forall v \in V \exists b \in A : bv = 0 \Longleftrightarrow \mathrm{T}_A(V) = V.$$

(vii) Für $a \in A$ ist die **Multiplikationsabbildung** $\mu_a : A^{-1}V \longrightarrow A^{-1}V$, $\frac{v}{b} \longmapsto a\frac{v}{b}$, bijektiv; denn im Fall $0 = \mu_a(\frac{v}{b}) = \frac{av}{b}$ existiert ein $c \in A$ mit $cav = 0$. Nach (vi) ist also $\frac{v}{b} = 0$. Daher ist μ_a injektiv.

Für $w \in V$ und $d \in A$ ist ferner $\mu_a(\frac{w}{ad}) = a\frac{w}{ad} = \frac{aw}{ad} = \frac{w}{d}$. Daher ist μ_a auch surjektiv.

Satz. (Universelle Eigenschaft des Quotientenmoduls)
Sei V ein R-Modul, und sei $\lambda : V \longrightarrow A^{-1}V$ kanonisch. Dann existiert zu jedem R-Modul W mit der Eigenschaft, dass $\mu_a : W \longrightarrow W$, $w \longmapsto aw$, für $a \in A$ bijektiv ist, und zu jedem $f \in \mathrm{Hom}_R(V, W)$ genau ein $F \in \mathrm{Hom}_R(A^{-1}V, W)$ mit $F \circ \lambda = f$.

Beweis. Zum Beweis der Eindeutigkeit sei $F \in \mathrm{Hom}_R(A^{-1}V, W)$ mit $F \circ \lambda = f$. Für $v \in V$, $a \in A$ gilt dann:

$$\mu_a(F(\frac{v}{a})) = aF(\frac{v}{a}) = F(a\frac{v}{a}) = F(\frac{av}{a}) = F(\frac{v}{1}) = F(\lambda(v)) = f(v),$$

d.h. $F(\frac{v}{a}) = \mu_a^{-1}(f(v))$.

Zum Beweis der Existenz definieren wir $F : A^{-1}V \longrightarrow W$ durch $F(\frac{v}{a}) = \mu_a^{-1}(f(v))$ für $v \in V$, $a \in A$. Dann ist F wohldefiniert; denn im Fall $\frac{v}{a} = \frac{v'}{a'}$ existiert ein $b \in A$ mit

$ba'v = bav'$. Daher ist $ba'f(v) = f(ba'v) = f(bav') = baf(v')$. Also ist $a'f(v) = af(v')$, d.h. $f(v) = \mu_{a'}^{-1}(af(v')) = a\mu_{a'}^{-1}(f(v'))$ und damit $\mu_a^{-1}(f(v)) = \mu_{a'}^{-1}(f(v'))$.

Ferner ist F ein R-Homomorphismus; denn für $u, v \in V$, $a, b \in A$, $r \in R$ gilt:

$$\begin{aligned} F(\frac{u}{a} + \frac{v}{b}) &= F(\frac{bu + av}{ab}) = \mu_{ab}^{-1}(f(bu + av)) = \mu_a^{-1}(\mu_b^{-1}(bf(u) + af(v))) \\ &= \mu_a^{-1}(f(u) + a\mu_b^{-1}(f(v))) = \mu_a^{-1}(f(u)) + \mu_b^{-1}(f(v)) = F(\frac{u}{a}) + F(\frac{v}{b}) \end{aligned}$$

und

$$F(r\frac{u}{a}) = F(\frac{ru}{a}) = \mu_a^{-1}(f(ru)) = r\mu_a^{-1}(f(u)) = rF(\frac{u}{a}).$$

Schließlich ist $F \circ \lambda = f$ wegen $F(\lambda(v)) = F(\frac{v}{1}) = \mu_1^{-1}(f(v)) = f(v)$ für $v \in V$.

8.2 Bemerkung. (i) $A^{-1}R$ wird zu einem Ring durch

$$\frac{r}{a} \cdot \frac{s}{b} := \frac{rs}{ab} \qquad (r, s \in R;\ a, b \in A)$$

Wohldefiniertheit: Ist $\frac{r}{a} = \frac{r'}{a'}$, so existiert ein $c \in A$ mit $ca'r = car'$. Daher gilt: $\frac{rs}{ab} = \frac{ca'rs}{ca'ab} = \frac{car's}{ca'ab} = \frac{r's}{a'b}$. Analog argumentiert man im Fall $\frac{s}{b} = \frac{s'}{b'}$.

Assoziativität: Für $r, s, t \in R$, $a, b, c \in A$ gilt:

$$(\frac{r}{a} \cdot \frac{s}{b}) \cdot \frac{t}{c} = \frac{rs}{ab} \cdot \frac{t}{c} = \frac{rst}{abc} = \frac{r}{a} \cdot \frac{st}{bc} = \frac{r}{a} \cdot (\frac{s}{b} \cdot \frac{t}{c}).$$

Kommutativität: $\frac{r}{a}\frac{s}{b} = \frac{rs}{ab} = \frac{sr}{ba} = \frac{s}{b}\frac{r}{a}$.

Distributivität: $\frac{r}{a}(\frac{s}{b} + \frac{t}{c}) = \frac{r}{a}\frac{cs+bt}{bc} = \frac{rcs+rbt}{abc} = \frac{acrs+abrt}{a^2bc} = \frac{rs}{ab} + \frac{rt}{ac} = \frac{r}{a}\frac{s}{b} + \frac{r}{a}\frac{t}{c}$.

Neutrales Element: $\frac{1}{1}\frac{r}{a} = \frac{1r}{1a} = \frac{r}{a}$.

Man nennt $A^{-1}R$ **Quotientenring** von R bzgl. A.

(ii) Die kanonische Abbildung $\rho : R \longrightarrow A^{-1}R$, $r \longmapsto \frac{r}{1}$, ist ein Ringhomomorphismus; denn für $r, s \in R$ gilt:

$$\rho(rs) = \frac{rs}{1} = \frac{r}{1}\frac{s}{1} = \rho(r)\rho(s) \quad \text{und} \quad \rho(1) = \frac{1}{1} = 1_{A^{-1}R}.$$

Wir können also $A^{-1}R$ als R-Algebra auffassen. Dabei ist $\rho(A) \subseteq (A^{-1}R)^\times$ wegen $\rho(a)\frac{1}{a} = \frac{a}{1}\frac{1}{a} = \frac{a}{a} = \frac{1}{1}$ für $a \in A$.

Satz. (Universelle Eigenschaft des Quotientenrings)
Sei $\rho : R \longrightarrow A^{-1}R$ kanonisch. Dann existiert zu jedem Ring S und jedem Ringhomomorphismus $g : R \longrightarrow S$ mit $g(A) \subseteq S^\times$ genau ein Ringhomomorphismus $G : A^{-1}R \longrightarrow S$ mit $G \circ \rho = g$.

Beweis. Eindeutigkeit: Sei $G : A^{-1}R \longrightarrow S$ ein Ringhomomorphismus mit $G \circ \rho = g$. Für $r \in R$, $a \in A$ gilt dann:

$$g(a)G(\frac{r}{a}) = G(\rho(a))G(\frac{r}{a}) = G(\frac{a}{1})G(\frac{r}{a}) = G(\frac{a}{1}\frac{r}{a}) = G(\frac{r}{1}) = G(\rho(r)) = g(r),$$

d.h. $G(\frac{r}{a}) = g(a)^{-1}g(r)$.

Existenz: Wir setzen $G(\frac{r}{a}) := g(a)^{-1}g(r)$ für $r \in R$, $a \in A$. Dies ist wohldefiniert; denn im Fall $\frac{r}{a} = \frac{r'}{a'}$ existiert ein $b \in A$ mit $ba'r = bar'$. Dann ist $g(b)g(a')g(r) = g(b)g(a)g(r')$ und damit $g(a)^{-1}g(r) = g(a')^{-1}g(r')$.

Ferner ist G ein Ringhomomorphismus, da für $r, s \in R$, $a, b \in A$ gilt:

$$G(\frac{r}{a} + \frac{s}{b}) = G(\frac{br + as}{ab}) = g(ab)^{-1}g(br + as) = g(a)^{-1}g(b)^{-1}(g(b)g(r) + g(a)g(s))$$
$$= g(a)^{-1}g(r) + g(b)^{-1}g(s) = G(\frac{r}{a}) + G(\frac{b}{s}),$$

$$G(\frac{r}{a}\frac{s}{b}) = G(\frac{rs}{ab}) = g(ab)^{-1}g(rs) = g(a)^{-1}g(b)^{-1}g(r)g(s) = G(\frac{r}{a})G(\frac{s}{b}),$$

und $G(\frac{1}{1}) = g(1)^{-1}g(1) = 1^{-1}1 = 1$.

Schließlich ist $G \circ \rho = g$ wegen $G(\rho(r)) = G(\frac{r}{1}) = g(1)^{-1}g(r) = g(r)$ für $r \in R$.

Beispiel. Nach Bemerkung 8.1 (vi) gilt: $A^{-1}R = 0 \iff R = \mathrm{T}_A(R) \iff \forall r \in R \exists a \in A : ar = 0 \iff 0 \in A \iff A$ enthält ein nilpotentes Element $\iff A \cap \mathrm{nil}(R) \neq \emptyset$.

8.3 Bemerkung. Sei W ein R-Modul derart, dass $\mu_a : W \longrightarrow W$, $w \longmapsto aw$, für $a \in A$ bijektiv ist.
(i) Dann wird W zu einem $A^{-1}R$-Modul mit

$$\frac{r}{a}w := \mu_a^{-1}(rw) \qquad (r \in R,\ a \in A,\ w \in W).$$

Wohldefiniertheit: Ist $\frac{r}{a} = \frac{r'}{a'}$, so existiert ein $b \in A$ mit $ba'r = bar'$, d.h. $ba'rw = bar'w$. Daher ist $aa'\mu_a^{-1}(rw) = a'rw = ar'w = aa'\mu_{a'}^{-1}(r'w)$, d.h. $\mu_a^{-1}(rw) = \mu_{a'}^{-1}(r'w)$.

Assoziativität: $\frac{r}{a}(\frac{s}{b}w) = \mu_a^{-1}(r\mu_b^{-1}(sw)) = \mu_a^{-1}(\mu_b^{-1}(rsw)) = \mu_{ab}^{-1}(rsw) = \frac{rs}{ab}w = (\frac{r}{a}\frac{s}{b})w$.

Distributivität: $(\frac{r}{a} + \frac{s}{b})w = \frac{br+as}{ab}w = \mu_{ab}^{-1}((br + as)w) = \mu_a^{-1}(\mu_b^{-1}(brw + asw)) = \mu_a^{-1}(rw + a\mu_b^{-1}(sw)) = \mu_a^{-1}(rw) + \mu_b^{-1}(sw) = \frac{r}{a}w + \frac{s}{b}w$ und $\frac{r}{a}(v + w) = \mu_a^{-1}(r(v + w)) = \mu_a^{-1}(rv + rw) = \mu_a^{-1}(rv) + \mu_a^{-1}(rw) = \frac{r}{a}v + \frac{r}{a}w$.

Neutrales Element: $\frac{1}{1}w = \mu_1^{-1}(1w) = w$.
(ii) Für jeden R-Modul V wird also insbesondere $A^{-1}V$ zu einem $A^{-1}R$-Modul mit

$$\frac{r}{a} \cdot \frac{v}{b} := \mu_a^{-1}(r\frac{v}{b}) = \frac{rv}{ab} \qquad (r \in R;\ a, b \in A;\ v \in V).$$

Dann wird auch die Abbildung F aus Satz 8.1 zu einem $A^{-1}R$-Homomorphismus; denn für $r \in R$, $a, b \in A$, $v \in V$ gilt:

$$F(\frac{r}{a}\frac{v}{b}) = F(\frac{rv}{ab}) = \mu_{ab}^{-1}(f(rv)) = \mu_a^{-1}(\mu_b^{-1}(rf(v))) = \mu_a^{-1}(r\mu_b^{-1}(f(v))) = \frac{r}{a}F(\frac{v}{b}).$$

8.4 Bemerkung. (i) Für R-Moduln V, W und $f \in \mathrm{Hom}_R(V, W)$ ist

$$A^{-1}f : A^{-1}V \longrightarrow A^{-1}W, \quad \frac{v}{a} \longmapsto \frac{f(v)}{a},$$

$A^{-1}R$-linear; denn sind $\lambda_V : V \longrightarrow A^{-1}V$ und $\lambda_W : W \longrightarrow A^{-1}W$ kanonisch, so existiert zu $\lambda_W \circ f \in \mathrm{Hom}_R(V, A^{-1}W)$ nach Satz 8.1 ein $F \in \mathrm{Hom}_R(A^{-1}V, A^{-1}W)$ mit $F \circ \lambda_V = \lambda_W \circ f$, d.h. $F(\frac{v}{1}) = \frac{f(v)}{1}$ für $v \in V$. Nach Bemerkung 8.3 (ii) ist $F \in \mathrm{Hom}_{A^{-1}R}(A^{-1}V, A^{-1}W)$, d.h. für $v \in V$, $a \in A$ gilt:

$$F(\frac{v}{a}) = F(\frac{1}{a}\frac{v}{1}) = \frac{1}{a}F(\frac{v}{1}) = \frac{1}{a}\frac{f(v)}{1} = \frac{f(v)}{a}.$$

Also ist $A^{-1}f := F$ wohldefiniert und $A^{-1}R$-linear.
(ii) Für $f, g \in \mathrm{Hom}_R(V, W)$ und $r, s \in R$ gilt ferner:

$$A^{-1}(rf + sg) = r(A^{-1}f) + s(A^{-1}g);$$

dies rechnet man leicht nach. Daher ist

$$\mathrm{Hom}_R(V, W) \longrightarrow \mathrm{Hom}_{A^{-1}R}(A^{-1}V, A^{-1}W), \quad f \longmapsto A^{-1}f,$$

ein R-Homomorphismus.
(iii) Für R-Moduln U, V, W und $f \in \mathrm{Hom}_R(U, V)$, $g \in \mathrm{Hom}_R(V, W)$ gilt auch:

$$A^{-1}(g \circ f) = (A^{-1}g) \circ (A^{-1}f) \quad \text{und} \quad A^{-1}(\mathrm{id}_V) = \mathrm{id}_{A^{-1}V};$$

dies rechnet man wieder schnell nach.

Satz. *Für jede exakte Folge $U \xrightarrow{f} V \xrightarrow{g} W$ von R-Moduln und R-Homomorphismen ist*

$$A^{-1}U \xrightarrow{A^{-1}f} A^{-1}V \xrightarrow{A^{-1}g} A^{-1}W$$

eine exakte Folge von $A^{-1}R$-Moduln und $A^{-1}R$-Homomorphismen.

Beweis. Wegen $\mathrm{Bld}(f) \subseteq \mathrm{Ker}(g)$ ist $g \circ f = 0$, d.h.

$$0 = A^{-1}0 = A^{-1}(g \circ f) = (A^{-1}g) \circ (A^{-1}f).$$

Daher gilt: $\mathrm{Bld}(A^{-1}f) \subseteq \mathrm{Ker}(A^{-1}g)$.

Sei umgekehrt $\frac{v}{a} \in \mathrm{Ker}(A^{-1}g)$, d.h. $0 = (A^{-1}g)(\frac{v}{a}) = \frac{g(v)}{a}$. Daher existiert ein $b \in A$ mit $0 = bg(v) = g(bv)$. Also ist $bv \in \mathrm{Ker}(g) = \mathrm{Bld}(f)$, d.h. $bv = f(u)$ für ein $u \in U$. Folglich gilt:

$$\frac{v}{a} = \frac{bv}{ba} = \frac{f(u)}{ba} = (A^{-1}f)(\frac{u}{ba}) \in \mathrm{Bld}(A^{-1}f).$$

Beispiel. Für jeden R-Monomorphismus $f : U \longrightarrow V$ ist $0 \longrightarrow U \xrightarrow{f} V$ exakt. Daher ist auch $0 = A^{-1}0 \longrightarrow A^{-1}U \xrightarrow{A^{-1}f} A^{-1}V$ exakt, d.h. $A^{-1}f$ ist ein $A^{-1}R$-Monomorphismus.

Für jeden R-Epimorphismus $g : V \longrightarrow W$ ist analog $A^{-1}g : A^{-1}V \longrightarrow A^{-1}W$ ein $A^{-1}R$-Epimorphismus.

8.5 Bemerkung. Sei U ein Untermodul eines R-Moduls V mit Inklusionsabbildung $i : U \longrightarrow V$. Dann ist

$$A^{-1}i : A^{-1}U \longrightarrow A^{-1}V, \quad \frac{u}{a} \longmapsto \frac{i(u)}{a} = \frac{u}{a},$$

injektiv. Man kann so $A^{-1}U$ mit seinem Bild in $A^{-1}V$ identifizieren und als Untermodul von $A^{-1}V$ auffassen.

Satz. *Für Untermoduln U, U' eines R-Moduls V gilt:*
(i) $U \subseteq U' \Longrightarrow A^{-1}U \subseteq A^{-1}U'$;
(ii) $A^{-1}(U + U') = A^{-1}U + A^{-1}U'$;
(iii) $A^{-1}(U \cap U') = A^{-1}U \cap A^{-1}U'$;
(iv) $A^{-1}(V/U) \simeq_{A^{-1}R} A^{-1}V/A^{-1}U$.

Beweis. (i) Klar!

(ii) Für $a, a' \in A$, $u \in U$, $u' \in U'$ gilt: $\frac{u}{a} + \frac{u'}{a'} = \frac{a'u+au'}{aa'} \in A^{-1}(U + U')$ und $\frac{u+u'}{a} = \frac{u}{a} + \frac{u'}{a} \in A^{-1}U + A^{-1}U'$.

(iii) Wegen $U \cap U' \subseteq U$ und (i) ist $A^{-1}(U \cap U') \subseteq A^{-1}U$. Analog ist $A^{-1}(U \cap U') \subseteq A^{-1}U'$, also auch $A^{-1}(U \cap U') \subseteq A^{-1}U \cap A^{-1}U'$.

Seien umgekehrt $a, a' \in A$, $u \in U$, $u' \in U'$ mit $\frac{u}{a} = \frac{u'}{a'}$. Dann existiert ein $b \in A$ mit $ba'u = bau' \in U \cap U'$. Also ist $\frac{u}{a} = \frac{ba'u}{ba'a} \in A^{-1}(U \cap U')$.

(iv) Seien $i : U \longrightarrow V$ und $f : V \longrightarrow V/U$ kanonisch. Dann ist

$$0 \longrightarrow U \xrightarrow{i} V \xrightarrow{f} V/U \longrightarrow 0$$

exakt. Daher ist auch

$$0 \longrightarrow A^{-1}U \xrightarrow{A^{-1}i} A^{-1}V \xrightarrow{A^{-1}f} A^{-1}(V/U) \longrightarrow 0$$

exakt. Insbesondere gilt:

$$A^{-1}(V/U) = \mathrm{Bld}(A^{-1}f) \simeq A^{-1}V/\mathrm{Ker}(A^{-1}f) = A^{-1}V/\mathrm{Bld}(A^{-1}i) = A^{-1}V/A^{-1}U.$$

8.6 Bemerkung. Sei V ein R-Modul und $\lambda : V \longrightarrow A^{-1}V$ kanonisch. Wir untersuchen Beziehungen zwischen den Untermoduln von V und $A^{-1}V$.
(i) Jeder $A^{-1}R$-Untermodul $W \subseteq A^{-1}V$ ist auch ein R-Untermodul. Daher ist $\lambda^{-1}(W) \subseteq V$ ein R-Untermodul.

Für $v \in \lambda^{-1}(W)$ und $a \in A$ ist $\frac{v}{1} = \lambda(v) \in W$ und damit $\frac{v}{a} = \frac{1}{a}\frac{v}{1} \in W$.

Für $v \in V$ und $a \in A$ mit $\frac{v}{a} \in W$ ist umgekehrt $\lambda(v) = \frac{v}{1} = \frac{a}{1}\frac{v}{a} \in W$, d.h. $v \in \lambda^{-1}(W)$ und $\frac{v}{a} \in A^{-1}(\lambda^{-1}(W))$. Dies zeigt: $A^{-1}(\lambda^{-1}(W)) = W$.

Außerdem ist $\mathrm{T}_A(V/\lambda^{-1}(W)) = 0$; denn sind $v \in V$ und $a \in A$ mit

$$0 = a(v + \lambda^{-1}(W)) = av + \lambda^{-1}(W),$$

so ist $av \in \lambda^{-1}(W)$, d.h. $\lambda(av) \in W$. Also ist auch $\lambda(v) = \frac{1}{a}\lambda(av) \in W$, d.h. $v \in \lambda^{-1}(W)$ und $v + \lambda^{-1}(W) = 0$.

(ii) Für jeden R-Untermodul $U \subseteq V$ ist $A^{-1}U \subseteq A^{-1}V$ ein $A^{-1}R$-Untermodul mit

$$\lambda^{-1}(A^{-1}U) = \{v \in V : \exists a \in A : av \in U\} \supseteq U;$$

denn sind $v \in V$ und $a \in A$ mit $av \in U$, so ist $\lambda(v) = \frac{v}{1} = \frac{av}{a} \in A^{-1}U$, d.h. $v \in \lambda^{-1}(A^{-1}U)$.

Ist umgekehrt $v \in \lambda^{-1}(A^{-1}U)$, so ist $\frac{v}{1} = \lambda(v) \in A^{-1}U$, d.h. $\frac{v}{1} = \frac{u}{b}$ mit $u \in U$ und $b \in A$. Dann existiert ein $c \in A$ mit $cbv = c1u \in U$.

(iii) Die Abbildungen $U \longmapsto A^{-1}U$ und $W \longmapsto \lambda^{-1}(W)$ liefern daher zueinander inverse Bijektionen

$$\{U \subseteq V : U \text{ } R\text{-Untermodul mit } \mathrm{T}_A(V/U) = 0\} \leftrightarrow \{W \subseteq A^{-1}V : W \text{ } A^{-1}R\text{-Untermodul}\};$$

denn für jeden R-Untermodul $U \subseteq V$ mit $\mathrm{T}_A(V/U) = 0$ gilt:

$$\begin{aligned}\lambda^{-1}(A^{-1}U) &= \{v \in V : \exists a \in A : av \in U\} = \{v \in V : \exists a \in A : a(v+U) = 0\} \\ &= \{v \in V : v + U \in \mathrm{T}_A(V/U)\} = \{v \in V : v + U = 0\} = U.\end{aligned}$$

(iv) Aus (iii) folgt, dass mit V auch $A^{-1}V$ noethersch (bzw. artinsch) ist.

8.7 Satz. *Für $I, J \trianglelefteq R$ gilt:*
(i) $A^{-1}(IJ) = (A^{-1}I)(A^{-1}J)$;
(ii) $A^{-1}(\mathrm{rad}(I)) = \mathrm{rad}(A^{-1}I)$;
(iii) $A^{-1}I = A^{-1}R \iff A \cap I \neq \emptyset$.
(iv) Betrachtet man $\mathfrak{P} := \{P \in \mathrm{Spec}(R) : A \cap P = \emptyset\}$ als topologischen Unterraum von $\mathrm{Spec}(R)$, so ist $\mathfrak{P} \longrightarrow \mathrm{Spec}(A^{-1}R)$, $P \longmapsto A^{-1}P$, ein Homöomorphismus.
(v) R noethersch (bzw. artinsch) $\Longrightarrow$ $A^{-1}R$ noethersch (bzw. artinsch).

Beweis. (i) Sei $z \in A^{-1}(IJ)$. Dann existieren $r \in IJ$, $a \in A$ mit $z = \frac{r}{a}$. Ferner existieren $x_1, \ldots, x_n \in I$, $y_1, \ldots, y_n \in J$ mit $r = x_1y_1 + \cdots + x_ny_n$. Daher ist $z = \frac{x_1}{1}\frac{y_1}{a} + \cdots + \frac{x_n}{1}\frac{y_n}{a} \in (A^{-1}I)(A^{-1}J)$.

Seien umgekehrt $x \in I$, $y \in J$, $a, b \in A$. Dann ist $\frac{x}{a}\frac{y}{b} = \frac{xy}{ab} \in A^{-1}(IJ)$. Dies zeigt: $(A^{-1}I)(A^{-1}J) \subseteq A^{-1}(IJ)$.

(ii) Seien $a \in A$, $r \in \mathrm{rad}(I)$ und $n \in \mathbb{N}$ mit $r^n \in I$. Dann ist $(\frac{r}{a})^n = \frac{r^n}{a^n} \in A^{-1}I$, d.h. $\frac{r}{a} \in \mathrm{rad}(A^{-1}I)$.

Seien umgekehrt $r \in R$ und $a \in A$ mit $\frac{r}{a} \in \mathrm{rad}(A^{-1}I)$. Dann existiert ein $n \in \mathbb{N}$ mit $\frac{r^n}{a^n} \in A^{-1}I$. Also existieren $x \in I$, $b \in A$ mit $\frac{r^n}{a^n} = \frac{x}{b}$, d.h. es existiert ein $c \in A$ mit $cbr^n = ca^nx \in I$. Wegen $c^nb^nr^n \in I$ ist also $cbr \in \mathrm{rad}(I)$, d.h. $\frac{r}{a} = \frac{cbr}{cba} \in A^{-1}(\mathrm{rad}(I))$.

(iii) "$\Longrightarrow$": Sei $A^{-1}I = A^{-1}R$, d.h. $\frac{1}{1} \in A^{-1}I$. Dann existieren $a \in A$, $x \in I$ mit $\frac{1}{1} = \frac{x}{a}$. Also existiert ein $b \in A$ mit $ba1 = b1x \in A \cap I$.

"$\Longleftarrow$": Sei $a \in A \cap I$. Dann ist $\frac{1}{1} = \frac{a}{a} \in A^{-1}I$, d.h. $A^{-1}I = A^{-1}R$.

(iv) Sei $\lambda : R \longrightarrow A^{-1}R$ kanonisch. Nach Satz 7.1 ist dann

$$\lambda^* : \mathrm{Spec}(A^{-1}R) \longrightarrow \mathrm{Spec}(R), \quad Q \longmapsto \lambda^{-1}(Q),$$

stetig. Nach Bemerkung 8.6 (i) gilt für $Q \in \mathrm{Spec}(A^{-1}R)$ auch: $Q = A^{-1}(\lambda^{-1}(Q))$, d.h. λ^* ist injektiv. Ferner ist $A \cap \lambda^{-1}(Q) = \emptyset$ wegen (iii), d.h. $\lambda^*(Q) = \lambda^{-1}(Q) \in \mathfrak{P}$.

Sei umgekehrt $P \in \mathfrak{P}$. Dann ist $A^{-1}P \lhd A^{-1}R$ nach (iii). Seien $a, b \in A$, $r, s \in R$ mit $\frac{r}{a}\frac{s}{b} \in A^{-1}P$. Dann existieren $p \in P$, $c \in A$ mit $\frac{rs}{ab} = \frac{p}{c}$. Daher existiert ein $d \in A$ mit $dcrs = dabp \in P$. Wegen $c, d \notin P$ ist $rs \in P$, also $r \in P$ oder $s \in P$. Daher ist $\frac{r}{a} \in A^{-1}P$ oder $\frac{s}{b} \in A^{-1}P$. Dies zeigt: $A^{-1}P \in \mathrm{Spec}(A^{-1}R)$. Ferner gilt:

$$\lambda^{-1}(A^{-1}P) = \{x \in R : \exists a \in A : ax \in P\} = P.$$

Also ist $\mathrm{Bld}(\lambda^*) = \mathfrak{P}$, und wir haben eine stetige Bijektion

$$\lambda' : \mathrm{Spec}(A^{-1}R) \longrightarrow \mathfrak{P}, \quad Q \longmapsto \lambda^{-1}(Q),$$

mit Umkehrabbildung $P \longmapsto A^{-1}P$. Für $J \trianglelefteq A^{-1}R$ gilt:

$$\begin{aligned}\lambda'(\mathcal{V}(J)) &= \{\lambda^{-1}(Q) : Q \in \mathcal{V}(J)\} = \{\lambda^{-1}(Q) : J \subseteq Q \in \mathrm{Spec}(A^{-1}R)\} \\ &\subseteq \{P \in \mathfrak{P} : \lambda^{-1}(J) \subseteq P\}.\end{aligned}$$

Ist umgekehrt $P \in \mathfrak{P}$ mit $\lambda^{-1}(J) \subseteq P$, so ist $J = A^{-1}(\lambda^{-1}(J)) \subseteq A^{-1}P \in \mathrm{Spec}(A^{-1}R)$ und $\lambda^{-1}(A^{-1}P) = P$. Dies zeigt, dass $\lambda'(\mathcal{V}(J)) = \mathfrak{P} \cap \mathcal{V}(\lambda^{-1}(J))$ abgeschlossen in $\mathfrak{P}$ ist. Also ist λ' ein Homöomorphismus, und die Behauptung folgt.

(v) folgt aus Bemerkung 8.6 (iv).

8.8 Satz. *Für jede nichtleere Familie $(V_i)_{i\in I}$ von R-Moduln gilt:*

$$A^{-1}(\coprod_{i\in I} V_i) \simeq_{A^{-1}R} \coprod_{i\in I}(A^{-1}V_i).$$

Beweis. Sei $V := \coprod_{i\in I} V_i$ mit Projektoren $p_j : V \longrightarrow V_j$ $(j \in I)$. Dann ist $A^{-1}p_j \in \mathrm{Hom}_{A^{-1}R}(A^{-1}V, A^{-1}V_j)$ für $j \in I$, d.h.

$$f : A^{-1}V \longrightarrow \prod_{j\in I}(A^{-1}V_j), \quad x \longmapsto ((A^{-1}p_j)(x))_{j\in I},$$

ist $A^{-1}R$-linear. Für $v = (v_i)_{i\in I} \in V$ und $a \in A$ gilt:

$$f(\frac{v}{a}) = ((A^{-1}p_j)(\frac{v}{a}))_{j\in I} = (\frac{p_j(v)}{a})_{j\in I} = (\frac{v_j}{a})_{j\in I} \in \coprod_{j\in I}(A^{-1}V_j).$$

Daher können wir f auch als Abbildung $A^{-1}V \longrightarrow \coprod_{j\in I}(A^{-1}V_j)$ auffassen.

Ist $\frac{v}{a} \in \mathrm{Ker}(f)$, so ist $\frac{v_j}{a} = 0$ für $j \in I$. Für $j \in I$ existiert also ein $b_j \in A$ mit $b_j v_j = 0$. Wegen $v \in \coprod_{i\in I} V_i$ existiert sogar ein $b \in A$ mit $bv_i = 0$ für alle $i \in I$. Dann ist $bv = 0$, d.h. $\frac{v}{a} = 0$. Dies zeigt: f injektiv.

Zum Beweis der Surjektivität von f sei $y = (y_j)_{j\in I} \in \coprod_{j\in I}(A^{-1}V_j)$. Für $j \in I$ existieren also $v_j \in V_j$, $a_j \in A$ mit $y_j = \frac{v_j}{a_j}$. Dabei sei o.B.d.A. $|\{j \in I : v_j \neq 0\}| < \infty$ und $a_j = a$ für alle $j \in I$. Dann ist $v := (v_i)_{i\in I} \in V$, also $\frac{v}{a} \in A^{-1}V$ und $f(\frac{v}{a}) = y$.

Bemerkung. Für jede nichtleere Menge I ist also $A^{-1}(\coprod_{i\in I} R) \simeq_{A^{-1}R} \coprod_{i\in I}(A^{-1}R)$. Für jeden freien R-Modul F ist also $A^{-1}F$ ein freier $A^{-1}R$-Modul vom gleichen Rang.

8.9 Satz. *Für $I \trianglelefteq R$ ist $\overline{A} := A + I/I$ eine multiplikative Teilmenge von $\overline{R} := R/I$ mit $\overline{A}^{-1}\overline{R} \cong A^{-1}R/A^{-1}I$.*

Beweis. Sicher ist $\overline{A} \subseteq \overline{R}$ multiplikativ. Ferner ist $f : A^{-1}R \longrightarrow \overline{A}^{-1}\overline{R}$, $\frac{r}{a} \longmapsto \frac{r+I}{a+I}$, wohldefiniert; denn im Fall $\frac{r}{a} = \frac{r'}{a'}$ existiert ein $b \in A$ mit $ba'r = bar'$. Daher ist $(b + I)(a' + I)(r + I) = (b + I)(a + I)(r' + I)$, d.h. $\frac{r+I}{a+I} = \frac{r'+I}{a'+I}$.

Ferner ist f sicher ein Ringepimorphismus, und für $x \in I$, $a \in A$ gilt: $f(\frac{x}{a}) = \frac{x+I}{a+I} = \frac{0}{a+I} = 0$. Dies zeigt: $A^{-1}I \subseteq \mathrm{Ker}(f)$.

Sei umgekehrt $\frac{r}{a} \in \mathrm{Ker}(f)$, d.h. $0 = f(\frac{r}{a}) = \frac{r+I}{a+I}$. Dann existiert ein $b \in A$ mit $0 = (b + I)(r + I) = br + I$, d.h. $br \in I$. Also ist $\frac{r}{a} = \frac{br}{ba} \in A^{-1}I$.

Dies zeigt: $\mathrm{Ker}(f) = A^{-1}I$. Die Behauptung folgt also aus dem Homomorphiesatz.

8.10 Satz. *Sei B eine multiplikative Teilmenge von R mit $A \subseteq B$, und sei $\rho : R \longrightarrow A^{-1}R =: \widetilde{R}$ kanonisch. Dann ist $\widetilde{B} := \rho(B) \subseteq \widetilde{R}$ eine multiplikative Teilmenge mit $\widetilde{B}^{-1}\widetilde{R} \cong B^{-1}R$.*

Beweis. Sicher ist $\widetilde{B} \subseteq \widetilde{R}$ multiplikativ. Seien $\widetilde{\rho} : \widetilde{R} \longrightarrow \widetilde{B}^{-1}\widetilde{R}$ und $\sigma : R \longrightarrow B^{-1}R$ kanonisch. Dann ist $\widetilde{\rho} \circ \rho : R \longrightarrow \widetilde{R} \longrightarrow \widetilde{B}^{-1}\widetilde{R}$ ein Ringhomomorphismus mit $(\widetilde{\rho} \circ \rho)(B) = \widetilde{\rho}(\widetilde{B}) \subseteq (\widetilde{B}^{-1}\widetilde{R})^\times$, induziert also einen Ringhomomorphismus $\tau : B^{-1}R \longrightarrow \widetilde{B}^{-1}\widetilde{R}$ mit $\tau \circ \sigma = \widetilde{\rho} \circ \rho$, d.h.

$$\tau(\frac{r}{1}) = \tau(\sigma(r)) = \widetilde{\rho}(\rho(r)) = \widetilde{\rho}(\frac{r}{1}) = \frac{\frac{r}{1}}{\frac{1}{1}} \quad \text{für} \quad r \in R.$$

Sei $\frac{r}{b} \in \mathrm{Ker}(\tau)$, also auch $\frac{r}{1} = \frac{b}{1}\frac{r}{b} \in \mathrm{Ker}(\tau)$, d.h.

$$0 = \tau(\frac{r}{1}) = \frac{\frac{r}{1}}{\frac{1}{1}} \in \widetilde{B}^{-1}\widetilde{R}.$$

Daher existiert ein $\widetilde{b} \in \widetilde{B}$ mit $0 = \widetilde{b}\frac{r}{1} \in \widetilde{R} = A^{-1}R$. Wir schreiben $\widetilde{b} = \rho(b') = \frac{b'}{1}$ mit $b' \in B$. Dann ist $0 = \frac{b'}{1}\frac{r}{1} = \frac{b'r}{1} \in A^{-1}R$. Daher existiert ein $a \in A$ mit $0 = ab'r \in R$. Folglich ist

$$\frac{r}{b} = \frac{ab'r}{abb'} = \frac{0}{abb'} = 0 \in B^{-1}R.$$

Dies zeigt, dass τ injektiv ist. Andererseits hat jedes Element in $\widetilde{B}^{-1}\widetilde{R}$ die Form

$$\begin{aligned}\frac{\frac{r}{a}}{\frac{b}{1}} &= \frac{\frac{a}{1}\frac{r}{a}}{\frac{a}{1}\frac{b}{1}} = \frac{\frac{r}{1}}{\frac{ab}{1}} = \left(\frac{\frac{ab}{1}}{\frac{1}{1}}\right)^{-1}\left(\frac{\frac{r}{1}}{\frac{1}{1}}\right) = (\widetilde{\rho} \circ \rho)(ab)^{-1}(\widetilde{\rho} \circ \rho)(r) \\ &= (\tau \circ \sigma)(ab)^{-1}(\tau \circ \sigma)(r) = \tau(\sigma(ab)^{-1})\tau(\sigma(r)) = \tau(\sigma(ab)^{-1}\sigma(r)) \in \mathrm{Bld}(\tau)\end{aligned}$$

mit $a \in A$, $b \in B$. Also ist τ bijektiv.

9. Lokalisierung

Sei R ein Ring.

9.1 Bemerkung. Für $P \in \mathrm{Spec}(R)$ ist $A := R \setminus P \subseteq R$ eine multiplikative Teilmenge. Man nennt $R_P := A^{-1}R$ **Lokalisierung** von R an P. Für jeden R-Modul V heißt analog $V_P := A^{-1}V$ **Lokalisierung** von V an P. Für jeden weiteren R-Modul W und $f \in \mathrm{Hom}_R(V, W)$ schreibt man $f_P := A^{-1}f : V_P \longrightarrow W_P$.

Satz. *Dann ist R_P ein lokaler Ring mit maximalem Ideal $P_P := A^{-1}P$, und R_P/P_P ist zum Quotientenkörper* $\mathrm{Quot}(R/P)$ *von R/P isomorph.*

Beweis. Satz 8.7 (iv) liefert eine inklusionserhaltende Bijektion

$$\{Q \in \mathrm{Spec}(R) : Q \subseteq P\} \longrightarrow \mathrm{Spec}(R_P), \quad Q \longmapsto A^{-1}Q = Q_P.$$

Daher gilt: $\mathrm{Max}(R_P) = \{P_P\}$. Nach Satz 8.9 ist $\overline{A} := A+P/P = \overline{R}\setminus\{0\}$ eine multiplikative Teilmenge des Integritätsbereichs $\overline{R} := R/P$ mit

$$\mathrm{Quot}(\overline{R}) = \overline{A}^{-1}\overline{R} \cong A^{-1}R/A^{-1}P = R_P/P_P.$$

Beispiel. Ist $R = \mathbb{Z}$ und $P = (p)$ für ein $p \in \mathbb{P}$, so ist

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \not\equiv 0 \pmod{p}\}$$

ein lokaler Ring mit maximalem Ideal

$$\{\frac{a}{b} : a, b \in \mathbb{Z},\ a \equiv 0 \not\equiv b \pmod{p}\} = p\mathbb{Z}_{(p)},$$

und $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathrm{Quot}(\mathbb{Z}/(p)) = \mathbb{Z}/(p) = \mathbb{F}_p$. In $\mathbb{Z}_{(p)}$ gilt: $\frac{a}{b} = \frac{a'}{b'} \iff \exists b'' \in \mathbb{Z} \setminus (p) : b''b'a = b''ba' \iff b'a = ba' \iff \frac{a}{b} = \frac{a'}{b'} \in \mathbb{Q}$. Man kann also $\mathbb{Z}_{(p)}$ als Teilring von $\mathbb{Q}$ auffassen.

9.2 Satz. *Für jeden R-Modul V gilt:*

$$V = 0 \iff \forall P \in \mathrm{Spec}(R) : V_P = 0 \iff \forall M \in \mathrm{Max}(R) : V_M = 0.$$

Beweis. Sei $V \neq 0$ und $0 \neq v \in V$. Dann ist $I := \{r \in R : rv = 0\} \lhd R$. Sei $I \subseteq M \in \mathrm{Max}(R)$. Dann ist $0 \neq \frac{v}{1} \in V_M$; denn sonst gäbe es ein $a \in R \setminus M$ mit $av = 0$, d.h. wir hätten den Widerspruch $a \in I \subseteq M$.

Definition. $\mathrm{Supp}(V) := \mathrm{Supp}_R(V) := \{P \in \mathrm{Spec}(R) : V_P \neq 0\}$ heißt **Träger** (support) von V.

Bemerkung. Ist $P \in \mathrm{Supp}(V)$ und $Q \in \mathcal{V}(P)$, so ist auch $Q \in \mathrm{Supp}(V)$; denn wegen $V_P \neq 0$ existiert ein $v \in V$ mit $av \neq 0$ für alle $a \in R \setminus P$, also auch für alle $a \in R \setminus Q$. Daher ist $V_Q \neq 0$.

Es gilt also: $P \in \mathrm{Supp}(V) \Longrightarrow \mathcal{V}(P) \subseteq \mathrm{Supp}(V)$.

9.3 Satz. *Für R-Moduln U, V und $f \in \mathrm{Hom}_R(U, V)$ sind äquivalent:*
(1) f injektiv (bzw. surjektiv);
(2) $\forall P \in \mathrm{Spec}(R) : f_P : U_P \longrightarrow V_P$ injektiv (bzw. surjektiv);
(3) $\forall M \in \mathrm{Max}(R) : f_M : U_M \longrightarrow V_M$ injektiv (bzw. surjektiv).

Beweis. Wir zeigen nur die Aussage über die Injektivität; der Rest geht analog. Ist f injektiv, so auch f_P für $P \in \mathrm{Spec}(R)$ (vgl. Beispiel 8.4).

Sei umgekehrt f_M injektiv für alle $M \in \mathrm{Max}(R)$. Dann ist

$$0 \longrightarrow K := \mathrm{Ker}(f) \xrightarrow{i} U \xrightarrow{f} V$$

exakt, wobei i die Inklusionsabbildung bezeichnet. Für $M \in \mathrm{Max}(R)$ ist also auch

$$0 \longrightarrow K_M \xrightarrow{i_M} U_M \xrightarrow{f_M} V_M$$

exakt. Da f_M injektiv ist, folgt $0 = \mathrm{Ker}(f_M) = \mathrm{Bld}(i_M)$. Da i_M injektiv ist, folgt $K_M = 0$. Nach Satz 9.2 ist also $K = 0$, d.h. f ist injektiv.

Bemerkung. Aus Satz 9.2 folgt leicht, dass für Untermoduln U, V eines R-Moduls W gilt:
(i) $U \subseteq V \Longleftrightarrow \forall P \in \mathrm{Spec}(R) : U_P \subseteq V_P \Longleftrightarrow \forall M \in \mathrm{Max}(R) : U_M \subseteq V_M$;
(ii) $U = V \Longleftrightarrow \forall P \in \mathrm{Spec}(R) : U_P = V_P \Longleftrightarrow \forall M \in \mathrm{Max}(R) : U_M = V_M$.
[Wir zeigen nur (i). Aus $U \subseteq V$ folgt natürlich $U_P \subseteq V_P$ für $P \in \mathrm{Spec}(R)$. Sei umgekehrt $U_M \subseteq V_M$ für alle $M \in \mathrm{Max}(R)$. Dann ist

$$(U + V/V)_M \simeq (U + V)_M / V_M = U_M + V_M / V_M = 0$$

für alle $M \in \mathrm{Max}(R)$, also $U + V/V = 0$ und damit $U \subseteq V$.]

9.4 Bemerkung. Für jede Teilmenge T eines R-Moduls V ist

$$\mathrm{Ann}(T) := \mathrm{Ann}_R(T) := \{r \in R : rT = 0\}$$

ein Ideal in R, der **Annullator** von T. Dann ist $\mathrm{Ann}(T) = \mathrm{Ann}(RT)$. Im Fall $T = \{t\}$ schreibt man $\mathrm{Ann}(T) =: \mathrm{Ann}(t) =: \mathrm{Ann}_R(t)$.

Satz. *Für jeden R-Modul V gilt:*

(i) Ist $V = \sum_{j\in J} V_j$ *mit einer Familie* $(V_j)_{j\in J}$ *von Untermoduln von* V*, so ist*

$$\mathrm{Supp}(V) = \bigcup_{j\in J} \mathrm{Supp}(V_j).$$

(ii) Ist V *endlich erzeugt, so ist* $\mathrm{Supp}(V) = \mathcal{V}(\mathrm{Ann}(V))$.
(iii) Für jeden Untermodul $U \subseteq V$ *ist* $\mathrm{Supp}(V) = \mathrm{Supp}(U) \cup \mathrm{Supp}(V/U)$.

Beweis. (i) Sei $P \in \mathrm{Supp}(V)$, d.h. $V_P \neq 0$, und sei $0 \neq \frac{v}{a} \in V_P$. Wir schreiben $v = v_1 + \cdots + v_n$ mit $v_1 \in V_{j_1}, \ldots, v_n \in V_{j_n}$ und $j_1, \ldots, j_n \in J$. Dann ist $0 \neq \frac{v}{a} = \frac{v_1}{a} + \cdots + \frac{v_n}{a}$, d.h. $0 \neq \frac{v_i}{a} \in (V_{j_i})_P$ für ein $i \in \{1, \ldots, n\}$. Daher ist $P \in \mathrm{Supp}(V_{j_i}) \subseteq \bigcup_{j\in J} \mathrm{Supp}(V_j)$.

Sei umgekehrt $P \in \mathrm{Spec}(R) \setminus \mathrm{Supp}(V)$, d.h. $V_P = 0$. Für $j \in J$ ist dann auch $(V_j)_P = 0$, d.h. $P \notin \mathrm{Supp}(V_j)$. Also ist $P \notin \bigcup_{j\in J} \mathrm{Supp}(V_j)$.

(ii) Zunächst sei V zyklisch, d.h. $V = Rv$ für ein $v \in V$. Für $P \in \mathrm{Spec}(R)$ ist dann

$$V_P = \{\frac{x}{a} : x \in V, a \in R \setminus P\} = \{\frac{rv}{a} : r \in R, a \in R \setminus P\} = R_P \frac{v}{1}.$$

Daher gilt: $V_P = 0 \iff \frac{v}{1} = 0 \in V_P \iff \exists a \in R \setminus P : av = 0 \iff (R \setminus P) \cap \mathrm{Ann}(v) \neq \emptyset$. Folglich gilt: $P \in \mathrm{Supp}(V) \iff V_P \neq 0 \iff \mathrm{Ann}(v) \subseteq P \iff P \in \mathcal{V}(\mathrm{Ann}(v))$. Damit ist die Aussage für zyklische Moduln bewiesen.

Sei jetzt $V = Rv_1 + \cdots + Rv_n$. Dann gilt nach (i):

$$\mathrm{Supp}(V) = \bigcup_{i=1}^{n} \mathrm{Supp}(Rv_i) = \bigcup_{i=1}^{n} \mathcal{V}(\mathrm{Ann}(v_i)) = \mathcal{V}(\bigcap_{i=1}^{n} \mathrm{Ann}(v_i)) = \mathcal{V}(\mathrm{Ann}(V)).$$

(iii) Wir betrachten die kurze exakte Folge $0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} V/U \longrightarrow 0$, wobei f und g kanonisch sind. Für $P \in \mathrm{Spec}(R)$ ist dann auch $0 \longrightarrow U_P \xrightarrow{f_P} V_P \xrightarrow{g_P} (V/U)_P \longrightarrow 0$ exakt. Daher gilt: $P \in \mathrm{Supp}(V) \iff V_P \neq 0 \iff U_P \neq 0 \vee (V/U)_P \neq 0 \iff P \in \mathrm{Supp}(U) \vee P \in \mathrm{Supp}(V/U) \iff P \in \mathrm{Supp}(U) \cup \mathrm{Supp}(V/U)$.

9.5 Satz. *Für* $P \in \mathrm{Spec}(R)$ *und jeden* R*-Modul* V *sind äquivalent:*
(1) V *hat einen zu* R/P *isomorphen Untermodul* U*;*
(2) $P = \mathrm{Ann}(v)$ *für ein* $v \in V$*.*

Beweis. "(1) $\Longrightarrow$ (2)": Sei (1) erfüllt, sei $f : R/P \longrightarrow U$ ein R-Isomorphismus, und sei $v := f(1 + P) \in U$. Für $r \in R$ gilt dann: $r \in \mathrm{Ann}(v) \iff 0 = rv = rf(1 + P) = f(r + P) \iff r + P = 0 \iff r \in P$.

"(2) $\Longrightarrow$ (1)": Sei (2) erfüllt. Dann ist $f : R \longrightarrow V$, $r \longmapsto rv$, R-linear mit Bild Rv und Kern $\mathrm{Ann}(v) = P$. Daher gilt: $R/P \simeq Rv \subseteq V$.

Definition. Ggf. heißt P ein zu V **assoziiertes** Primideal. Die Menge aller zu V assoziierten Primideale von R bezeichnen wir mit $\mathrm{Ass}(V) = \mathrm{Ass}_R(V)$.

Bemerkung. Ist $P \in \mathrm{Ass}(V)$ und ist $v \in V$ mit $P = \mathrm{Ann}(v)$, so ist auch $P = \mathrm{Ann}(w)$ für alle $w \in Rv \setminus \{0\}$.

[Zum Beweis sei $r \in R$ mit $w = rv$. Für $y \in \mathrm{Ann}(w)$ ist dann $0 = yw = yrv$, d.h. $yr \in \mathrm{Ann}(v) = P$. Wegen $0 \neq w = rv$ ist $r \notin \mathrm{Ann}(v) = P \in \mathrm{Spec}(R)$, also $y \in P$.

Für $p \in P$ ist umgekehrt $pw = rpv = r0 = 0$, d.h. $p \in \mathrm{Ann}(w)$.]

Beispiel. Im Fall $R = \mathbb{Z}$ und $V = \mathbb{Z}/6\mathbb{Z}$ ist $\mathrm{Ass}(V) = \{(2), (3)\}$.

9.6 Satz. *Für jeden R-Modul V gilt:*
(i) $P \in \{\mathrm{Ann}(v) : 0 \neq v \in V\}$ maximal $\Longrightarrow P \in \mathrm{Ass}(V)$;
(ii) R noethersch und $V \neq 0 \Longrightarrow \mathrm{Ass}(V) \neq \emptyset$.
(iii) $U \subseteq V$ Untermodul $\Longrightarrow \mathrm{Ass}(U) \subseteq \mathrm{Ass}(V) \subseteq \mathrm{Ass}(U) \cup \mathrm{Ass}(V/U)$.

Beweis. (i) Sei $P \in \{\mathrm{Ann}(v) : 0 \neq v \in V\}$ maximal, und sei $0 \neq x \in V$ mit $P = \mathrm{Ann}(x)$. Dann ist $P \triangleleft R$. Seien $a, b \in R$ mit $ab \in P$, d.h. $abx = 0$. Im Fall $bx = 0$ ist $b \in \mathrm{Ann}(x) = P$. Sei also $bx \neq 0$. Wegen $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(bx)$ folgt aus der Wahl von P: $P = \mathrm{Ann}(x) = \mathrm{Ann}(bx)$ enthält a.

(ii) folgt aus (i).

(iii) Sicher ist $\mathrm{Ass}(U) \subseteq \mathrm{Ass}(V)$.

Sei $P \in \mathrm{Ass}(V)$, und sei $v \in V$ mit $P = \mathrm{Ann}(v)$. Dann ist $f : R \longrightarrow V$, $r \longmapsto rv$, R-linear mit Bild Rv und Kern $\mathrm{Ann}(v) = P$; insbesondere ist $R/P \simeq Rv$. Im Fall $Rv \cap U = 0$ ist $R/P \simeq Rv/Rv \cap U \simeq Rv + U/U \subseteq V/U$, also $P \in \mathrm{Ass}(V/U)$. Im Fall $Rv \cap U \neq 0$ sei $0 \neq u \in Rv \cap U$. Nach Bemerkung 9.5 ist dann $P = \mathrm{Ann}(u) \in \mathrm{Ass}(U)$.

Beispiel. Für $R := \mathbb{Z}$, $V := \mathbb{Z}$ und $U := 2\mathbb{Z}$ ist $\mathrm{Ass}(V) = \{(0)\}$, aber $(2) \in \mathrm{Ass}(V/U)$, also $\mathrm{Ass}(V) \neq \mathrm{Ass}(U) \cup \mathrm{Ass}(V/U)$.

Bemerkung. Ist R noethersch und V beliebig, so folgt aus (i):

$$\bigcup_{P \in \mathrm{Ass}(V)} P = \bigcup_{0 \neq v \in V} \mathrm{Ann}(v) = \{r \in R : \exists v \in V : rv = 0 \neq v\}.$$

Die Elemente in dieser Menge heißen **Nullteiler** für V in R. Insbesondere ist also $\mathrm{Z}(R) = \bigcup_{P \in \mathrm{Ass}(R)} P$.

9.7 Satz. *Für jeden R-Modul V ist $\mathrm{Ass}(V) \subseteq \mathrm{Supp}(V)$. Ist R noethersch, so gehört umgekehrt jedes minimale Element in $\mathrm{Supp}(V)$ zu $\mathrm{Ass}(V)$.*

Beweis. (i) Sei $P \in \mathrm{Ass}(V)$, und sei $U \subseteq V$ ein Untermodul mit $U \simeq R/P$. Dann ist $P \in \mathrm{Supp}(V)$ wegen $V_P \supseteq U_P \simeq (R/P)_P \simeq R_P/P_P \simeq \mathrm{Quot}(R/P) \neq 0$.

(ii) Sei R noethersch und $P = (f_1, \ldots, f_k) \in \mathrm{Supp}(V)$ minimal. Dann ist R_P noethersch und $V_P \neq 0$. Nach Satz 9.6 (ii) ist

$$\emptyset \neq \mathrm{Ass}_{R_P}(V_P) \subseteq \mathrm{Supp}_{R_P}(V_P) \subseteq \mathrm{Spec}(R_P) = \{Q_P : P \supseteq Q \in \mathrm{Spec}(R)\}.$$

Sei $P \supseteq Q \in \mathrm{Spec}(R)$ mit $Q_P \in \mathrm{Ass}_{R_P}(V_P)$. Im Fall $Q \neq P$ wäre $V_Q = 0$, also auch $(V_P)_{Q_P} = 0$; denn sind $v \in V$ und $a \in R \setminus P$, so existiert ein $b \in R \setminus Q$ mit $bv = 0$. Dann ist $\frac{b}{1}\frac{v}{a} = \frac{bv}{a} = \frac{0}{a} = 0$ und $\frac{b}{1} \notin Q_P$; denn sonst gäbe es $q \in Q$, $c \in R \setminus P$ mit $\frac{b}{1} = \frac{q}{c}$. Dann gäbe es ein $d \in R \setminus P$ mit $dcb = d1q \in Q$. Wegen $b, c, d \notin Q$ hätte man dann einen Widerspruch.

Also wäre $Q_P \notin \mathrm{Supp}_{R_P}(V_P)$ und damit $Q_P \notin \mathrm{Ass}_{R_P}(V_P)$. Dieser Widerspruch zeigt: $\mathrm{Ass}_{R_P}(V_P) = \{P_P\}$.

Sei $\frac{v}{a} \in V_P$ mit $P_P = \mathrm{Ann}_{R_P}(\frac{v}{a})$. Für $i = 1, \ldots, k$ ist dann $0 = \frac{f_i}{1}\frac{v}{a} = \frac{f_i v}{a}$. Daher existiert ein $t_i \in R \setminus P$ mit $t_i f_i v = 0$. Also ist $t f_i v = 0$ mit $t := t_1 \cdots t_k \in R \setminus P$, d.h. $P \subseteq \mathrm{Ann}(tv)$.

Für $u \in \mathrm{Ann}(tv)$ ist umgekehrt $utv = 0$, also auch $0 = \frac{utv}{a} = \frac{u}{1}\frac{t}{1}\frac{v}{a}$. Daher ist $u \in P$; denn sonst wäre $\frac{u}{1}, \frac{t}{1} \in (R_P)^\times$, d.h. $\frac{v}{a} = 0$. Also gilt: $P = \mathrm{Ann}(tv) \in \mathrm{Ass}(V)$.

9.8 Satz. *Sei R noethersch, sei V ein endlich erzeugter R-Modul, und seien $P_1, \ldots, P_k$ die endlich vielen minimalen Elemente in $\mathcal{V}(\mathrm{Ann}(V))$. Dann gilt:*

$$\mathrm{Supp}(V) = \bigcup_{i=1}^{k} \mathcal{V}(P_i) \quad \text{und} \quad P_1, \ldots, P_k \in \mathrm{Ass}(V).$$

Beweis. Nach Bemerkung 4.6 (vi) ist $\mathrm{rad}(\mathrm{Ann}(V)) = \bigcap_{i=1}^{k} P_i$. Nach Satz 9.4 (ii) gilt also:

$$\mathrm{Supp}(V) = \mathcal{V}(\mathrm{Ann}(V)) = \mathcal{V}(\mathrm{rad}(\mathrm{Ann}(V))) = \mathcal{V}(\bigcap_{i=1}^{k} P_i) = \bigcup_{i=1}^{k} \mathcal{V}(P_i).$$

Jedes P_i ist minimal in $\mathrm{Supp}(V)$. Nach Satz 9.7 gilt also: $P_i \in \mathrm{Ass}(V)$.

9.9 Satz. *Sei R noethersch und V ein endlich erzeugter R-Modul. Dann existieren $P_1, \ldots, P_n \in \mathrm{Spec}(R)$ und Untermoduln $V_0, \ldots, V_n$ mit $0 = V_0 \subseteq V_1 \subseteq \ldots \subseteq V_n = V$ und $V_i/V_{i-1} \simeq R/P_i$ für $i = 1, \ldots, n$. Daher ist $\mathrm{Ass}(V) \subseteq \{P_1, \ldots, P_n\}$ endlich.*

Beweis. Wir zeigen zunächst die erste Aussage. O.B.d.A. sei dabei $V \neq 0$. Nach Satz 9.6 (ii) existiert dann ein $P_1 \in \mathrm{Ass}(V)$. Sei $R/P_1 \simeq V_1 \subseteq V$. Im Fall $V_1 = V$ sind wir fertig. Sei also $V_1 \neq V$. Nach Satz 9.6 (ii) existiert dann ein $P_2 \in \mathrm{Ass}(V/V_1)$. Sei $R/P_2 \simeq V_2/V_1 \subseteq V/V_1$. So fahren wir fort. Da V noethersch ist, existiert ein $n \in \mathbb{N}$ mit $V_n = V$. Damit ist die erste Aussage bewiesen.

Mit Satz 9.6 (iii) folgt:

$$\begin{aligned}\mathrm{Ass}(V) &\subseteq \mathrm{Ass}(V_1) \cup \mathrm{Ass}(V/V_1) \subseteq \{P_1\} \cup \mathrm{Ass}(V_2/V_1) \cup \mathrm{Ass}(V/V_2) \\ &\subseteq \{P_1, P_2\} \cup \mathrm{Ass}(V/V_2) \subseteq \ldots \subseteq \{P_1, \ldots, P_n\}.\end{aligned}$$

10. Primärzerlegungen

Sei R ein Ring.

10.1 Definition. (E. Lasker, 1868-1941)
Ein Ideal $Q \lhd R$ heißt **primär** (oder **Primärideal**), falls für alle $a, b \in R$ gilt: $ab \in Q \Longrightarrow a \in Q \vee b \in \mathrm{rad}(Q)$ [d.h. $b^n \in Q$ für ein $n \in \mathbb{N}$].

Bemerkung. (i) Für $Q \lhd R$ gilt: Q primär $\iff$ jeder Nullteiler in R/Q ist nilpotent.

[Denn ist Q primär und $b+Q \in \mathrm{Z}(R/Q)$, so existiert ein $a \in R \setminus Q$ mit $0 = (a+Q)(b+Q) = ab+Q$, d.h. $ab \in Q$. Wegen $a \notin Q$ existiert also ein $n \in \mathbb{N}$ mit $b^n \in Q$, d.h. $0 = b^n + Q = (b+Q)^n$.

Sei umgekehrt $\mathrm{Z}(R/Q) \subseteq \mathrm{nil}(R/Q)$, und seien $a, b \in R$ mit $ab \in Q$, aber $a \notin Q$. Dann ist $0 = ab+Q = (a+Q)(b+Q)$ und $0 \neq a+Q$, d.h. $b+Q \in \mathrm{Z}(R/Q)$. Daher existiert ein $n \in \mathbb{N}$ mit $0 = (b+Q)^n = b^n + Q$, d.h. $b^n \in Q$.]

(ii) Ist $Q \lhd R$ primär, so ist $P := \mathrm{rad}(Q) \in \mathrm{Spec}(R)$. Man sagt dann: Q ist P-primär.

[Denn sind $a, b \in R$ mit $ab \in P$, so existiert ein $n \in \mathbb{N}$ mit $a^n b^n = (ab)^n \in Q$. Also ist $a^n \in Q$ oder $b^{nm} \in Q$ für ein $m \in \mathbb{N}$. Daher ist $a \in \mathrm{rad}(Q) = P$ oder $b \in \mathrm{rad}(Q) = P$.]

(iii) Für $P \in \mathrm{Spec}(R)$ und P-primäre $Q_1, Q_2 \lhd R$ ist auch $Q_1 \cap Q_2 \lhd R$ ein P-Primärideal.

[Denn nach Bemerkung 4.6 gilt zunächst: $\mathrm{rad}(Q_1 \cap Q_2) = \mathrm{rad}(Q_1) \cap \mathrm{rad}(Q_2) = P \cap P = P$.

Seien jetzt $a, b \in R$ mit $ab \in Q_1 \cap Q_2$, aber $a \notin Q_1 \cap Q_2$; o.B.d.A. sei $a \notin Q_1$. Wegen $ab \in Q_1$ ist $b^n \in Q_1$ für ein $n \in \mathbb{N}$, also $b \in \mathrm{rad}(Q_1) = P = \mathrm{rad}(Q_1 \cap Q_2)$.]

(iv) Ist $Q \lhd R$ ein P-Primärideal und ist P endlich erzeugt, so existiert ein $n \in \mathbb{N}$ mit $P^n \subseteq Q$.

[Denn ist $P = (a_1, \ldots, a_k)$, so existiert für $i = 1, \ldots, k$ ein $n_i \in \mathbb{N}$ mit $a_i^{n_i} \in Q$. Setzt man $n := n_1 + \cdots + n_k$, so gilt nach der binomischen Formel: $P^n \subseteq Q \subseteq P$.]

Beispiel. (i) In $\mathbb{Z}$ ist (p^k) primär für $k \in \mathbb{N}$ und $p \in \mathbb{P}$; denn aus $ab \in (p^k)$ und $a \notin (p^k)$ folgt $b \in (p)$, also $b^k \in (p^k)$.

(ii) Sei K ein Körper, sei $R := K[X,Y]$, und sei $I := (X^2, XY)$. Dann ist $\mathrm{rad}(I) = (X) \in \mathrm{Spec}(R)$ und $(X)^2 = (X^2) \subseteq I$. Aber I ist nicht primär in R wegen $XY \in I$, aber $X \notin I$ und $Y^n \notin I$ für alle $n \in \mathbb{N}$. Die Bedingung in Bemerkung 10.1 (iv) ist also nicht hinreichend dafür, dass $Q \lhd R$ primär ist.

Satz. *Sei $Q \trianglelefteq R$ und $M := \mathrm{rad}(Q) \in \mathrm{Max}(R)$. Dann ist Q primär.*

Beweis. Seien $a, b \in R$ mit $ab \in Q$, aber $a \notin Q$. Dann ist $Q \subseteq I := \{c \in R : ac \in Q\} \lhd R$. Sei $I \subseteq N \in \mathrm{Max}(R)$. Dann ist $Q \subseteq N$, also auch $M = \mathrm{rad}(Q) \subseteq N$, d.h. $M = N$; insbesondere ist $b \in I \subseteq N = M = \mathrm{rad}(Q)$.

10.2 Satz. *Ist R noethersch, so gilt für $Q \trianglelefteq R$ und $P \in \mathrm{Spec}(R)$:*

$$Q \text{ ist } P\text{-primär} \iff \mathrm{Ass}(R/Q) = \{P\}.$$

Beweis. "$\Longrightarrow$": Sei Q P-primär, d.h. sicher $Q \neq R$. Nach Satz 9.6 ist $\mathrm{Ass}(R/Q) \neq \emptyset$. Sei $P_0 \in \mathrm{Ass}(R/Q)$, und sei $a \in R$ mit $P_0 = \mathrm{Ann}(a+Q) \supseteq Q$. Dann ist $a \notin Q$ und $P_0 \supseteq \mathrm{rad}(Q) = P$. Für $b \in P_0$ ist andererseits $0 = b(a+Q) = ba + Q$, d.h. $ba \in Q$. Daher ist $b \in \mathrm{rad}(Q) = P$. Dies zeigt: $P_0 = P$.

"$\Longleftarrow$": Sei $\mathrm{Ass}(R/Q) = \{P\}$, also auch $Q \neq R$. Wir behaupten, dass für jeden Untermodul $0 \neq V \subseteq R/Q$ gilt: $\mathrm{rad}(\mathrm{Ann}(V)) = P$.

Zum Beweis dieser Behauptung seien $P_1, \ldots, P_k$ die endlich vielen minimalen Elemente in $\mathcal{V}(\mathrm{Ann}(V))$. Nach Satz 9.8 gilt dann: $P_1, \ldots, P_k \in \mathrm{Ass}(V) \subseteq \mathrm{Ass}(R/Q) = \{P\}$. Daher ist $\mathrm{rad}(\mathrm{Ann}(V)) = P_1 \cap \ldots \cap P_k = P$, und unsere Behauptung ist bewiesen.

Wegen $Q = \mathrm{Ann}(R/Q)$ ist also insbesondere $\mathrm{rad}(Q) = \mathrm{rad}(\mathrm{Ann}(R/Q)) = P$. Seien jetzt $a, b \in R$ mit $ab \in Q$, aber $a \notin Q$. Mit $\overline{a} := a + Q \in R/Q$ gilt dann nach unserer Behauptung:: $b \in \mathrm{Ann}(R\overline{a}) \subseteq \mathrm{rad}(\mathrm{Ann}(R\overline{a})) = P = \mathrm{rad}(Q)$.

10.3 Definition. Ein Ideal $I \lhd R$ heißt **unzerlegbar**, falls gilt:

$$\text{Sind } J, K \trianglelefteq R \text{ mit } I = J \cap K, \text{ so ist } I = J \text{ oder } I = K.$$

Beispiel. Jedes $P \in \mathrm{Spec}(R)$ ist unzerlegbar; denn sind $J, K \trianglelefteq R$ mit $P = J \cap K \supseteq JK$, so ist $J \subseteq P$ oder $K \subseteq P$, d.h. $J = P$ oder $K = P$.

Satz. *Ist R noethersch, so ist jedes unzerlegbare Ideal $Q \lhd R$ primär.*

Beweis. Für $\overline{R} := R/Q$ gilt:
(i) Q unzerlegbar in $R \iff 0$ unzerlegbar in $\overline{R}$.
(ii) Q primär in $R \iff 0$ primär in $\overline{R}$.
Daher kann man R durch $\overline{R}$ ersetzen und $Q = 0$ annehmen. Seien jetzt $x, y \in R$ mit $xy = 0$, d.h. $y \in \mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \ldots$. Da R noethersch ist, existiert ein $n \in \mathbb{N}$ mit $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \ldots$.

Für $a \in (x^n) \cap (y)$ existiert ein $b \in R$ mit $a = bx^n$. Wegen $yx = 0$ ist andererseits $0 = ax = bx^{n+1}$, d.h. $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$, also $a = bx^n = 0$. Dies zeigt: $(x^n) \cap (y) = 0$. Da 0 unzerlegbar ist, folgt: $x^n = 0$ oder $y = 0$.

10.4 Definition. Sei $I \trianglelefteq R$. Sind $Q_1, \ldots, Q_n \lhd R$ primär mit $I = Q_1 \cap \ldots \cap Q_n$, so spricht man von einer **Primärzerlegung** von I. Diese heißt **unverkürzbar**, falls gilt:
(i) $I \neq \bigcap_{i \neq j} Q_i$ für $j = 1, \ldots, n$;
(ii) $\mathrm{rad}(Q_1), \ldots, \mathrm{rad}(Q_n)$ sind paarweise verschieden.

Bemerkung. Man kann jede Primärzerlegung unverkürzbar machen, indem man überflüssige Q_i's streicht und Q_i's mit dem gleichen Radikal zusammenfasst.

Satz. *Ist R noethersch, so hat jedes Ideal $I \trianglelefteq R$ eine (unverkürzbare) Primärzerlegung.*

Beweis. Nach Satz 10.3 genügt zu zeigen, dass sich jedes Ideal von R als Durchschnitt endlich vieler unzerlegbarer Ideale schreiben lässt. Nehmen wir also an, dass die Menge $\mathfrak{I}$ aller Ideale von R, die sich nicht so schreiben lassen, nichtleer ist. Da R noethersch ist, enthält $\mathfrak{I}$ ein maximales Element I. Dann ist $I \neq R$, und I ist nicht unzerlegbar. Daher ist $I = J \cap K$ mit echt größeren Idealen $J, K \trianglelefteq R$. Wegen $J, K \notin \mathfrak{I}$ sind J und K Durchschnitte endlich vieler unzerlegbarer Ideale. Folglich ist auch I ein Durchschnitt endlich vieler unzerlegbarer Ideale, im Widerspruch zu $I \in \mathfrak{I}$.

10.5 Satz. (Erster Eindeutigkeitssatz)
Sei R noethersch, sei $I \trianglelefteq R$ mit unverkürzbarer Primärzerlegung $I = Q_1 \cap \ldots \cap Q_k$, und sei $P_i := \mathrm{rad}(Q_i)$ für $i = 1, \ldots, k$. Dann ist $\mathrm{Ass}(R/I) = \{P_1, \ldots, P_k\}$; insbesondere sind $P_1, \ldots, P_k$ bis auf die Reihenfolge eindeutig bestimmt.

Beweis. Da $f : R/I \longrightarrow R/Q_1 \times \cdots \times R/Q_k$, $a + I \longmapsto (a + Q_1, \ldots, a + Q_k)$, ein R-Monomorphismus ist, gilt nach Satz 10.2:

$$\mathrm{Ass}(R/I) \subseteq \mathrm{Ass}(R/Q_1 \times \cdots \times R/Q_k) \subseteq \mathrm{Ass}(R/Q_1) \cup \ldots \cup \mathrm{Ass}(R/Q_k) = \{P_1, \ldots, P_k\}.$$

Sei umgekehrt $j \in \{1, \ldots, k\}$ und $N := \bigcap_{i \neq j} Q_i/I$, also $0 \neq N \subseteq R/I$. Dann gilt:

$$N = \bigcap_{i \neq j} Q_i/(\bigcap_{i \neq j} Q_i) \cap Q_j \simeq (\bigcap_{i \neq j} Q_i) + Q_j/Q_j \subseteq R/Q_j,$$

d.h. $\emptyset \neq \mathrm{Ass}(N) \subseteq \mathrm{Ass}(R/Q_j) = \{P_j\}$. Daher ist $\{P_j\} = \mathrm{Ass}(N) \subseteq \mathrm{Ass}(R/I)$.

10.6 Satz. *Sei $A \subseteq R$ eine multiplikative Teilmenge, und sei $\rho : R \longrightarrow A^{-1}R$ kanonisch. Sei $P \in \mathrm{Spec}(R)$ mit $P \cap A = \emptyset$, und sei $Q \trianglelefteq R$ ein P-Primärideal. Dann ist $A^{-1}Q \trianglelefteq A^{-1}R$ ein $A^{-1}P$-Primärideal mit $\rho^{-1}(A^{-1}Q) = Q$.*

Beweis. Nach Satz 8.7 ist $A^{-1}Q \trianglelefteq A^{-1}R$ mit $\mathrm{rad}(A^{-1}Q) = A^{-1}(\mathrm{rad}(Q)) = A^{-1}P \in \mathrm{Spec}(A^{-1}R)$. Wir zeigen jetzt, dass $A^{-1}Q$ primär in $A^{-1}R$ ist. Dazu seien $\frac{x}{a}, \frac{y}{b} \in A^{-1}R$ mit $\frac{x}{a}\frac{y}{b} \in A^{-1}Q$, aber $\frac{x}{a} \notin A^{-1}Q$. Wir schreiben $\frac{xy}{ab} = \frac{z}{c}$ mit $z \in Q$, $c \in A$. Dann existiert ein $d \in A$ mit $dcxy = dabz \in Q$. Wegen $x \notin Q$ ist also $cdy \in \mathrm{rad}(Q) = P$, und wegen $c, d \notin P$ folgt $y \in P$. Daher ist $\frac{y}{b} \in A^{-1}P = \mathrm{rad}(A^{-1}Q)$.

Zum Schluss zeigen wir: $Q = \rho^{-1}(A^{-1}Q)$. Sicher ist $Q \subseteq \rho^{-1}(A^{-1}Q)$. Sei umgekehrt $x \in \rho^{-1}(A^{-1}Q)$, d.h. $\frac{x}{1} = \rho(x) \in A^{-1}Q$. Wir schreiben $\frac{x}{1} = \frac{y}{a}$ mit $y \in Q$, $a \in A$. Dann existiert ein $b \in A$ mit $bax = b1y \in Q$. Im Fall $x \notin Q$ wäre $ab \in \mathrm{rad}(Q) = P$, und man hätte den Widerspruch $a \in P$ oder $b \in P$. Also gilt: $x \in Q$.

10.7 Satz. *Sei $A \subseteq R$ eine multiplikative Teilmenge, und sei $\rho : R \longrightarrow A^{-1}R$ kanonisch. Sei $I \trianglelefteq R$ mit unverkürzbarer Primärzerlegung $I = Q_1 \cap \ldots \cap Q_n$, und sei $P_i := \mathrm{rad}(Q_i)$ für $i = 1, \ldots, n$. Dabei sei $A \cap P_i = \emptyset$ für $i = 1, \ldots, m$ und $A \cap P_i \neq \emptyset$ für $i = m+1, \ldots, n$. Dann ist $A^{-1}I = A^{-1}Q_1 \cap \ldots \cap A^{-1}Q_m$ eine unverkürzbare Primärzerlegung, und $\rho^{-1}(A^{-1}I) = Q_1 \cap \ldots \cap Q_m$.*

Beweis. Für $i = m+1, \ldots, n$ existiert ein $a_i \in A \cap P_i$. Also existiert ein $k_i \in \mathbb{N}$ mit $a_i^{k_i} \in A \cap Q_i$. Daher ist $A \cap Q_i \neq \emptyset$, also $A^{-1}Q_i = A^{-1}R$ nach Satz 8.7. Aus $I = Q_1 \cap \ldots \cap Q_n$ folgt mit Satz 8.5:

$$A^{-1}I = A^{-1}Q_1 \cap \ldots \cap A^{-1}Q_n = A^{-1}Q_1 \cap \ldots \cap A^{-1}Q_m;$$

dabei ist $A^{-1}Q_i$ für $i = 1, \ldots, m$ ein $A^{-1}P_i$-Primärideal in $A^{-1}R$ nach Satz 10.6. Ferner sind $A^{-1}P_1, \ldots, A^{-1}P_m$ nach Satz 8.7 paarweise verschieden.

Wir nehmen an: $A^{-1}Q_2 \cap \ldots \cap A^{-1}Q_m \subseteq A^{-1}Q_1$. Wegen $Q_2 \cap \ldots \cap Q_m \not\subseteq Q_1$ existiert ein $x \in (Q_2 \cap \ldots \cap Q_m) \setminus Q_1$. Dann ist

$$\frac{x}{1} \in A^{-1}(Q_2 \cap \ldots \cap Q_m) = A^{-1}Q_2 \cap \ldots \cap A^{-1}Q_m \subseteq A^{-1}Q_1.$$

Wir schreiben $\frac{x}{1} = \frac{y}{a}$ mit $y \in Q_1$, $a \in A$. Dann existiert ein $b \in A$ mit $bax = b1y \in Q_1$, d.h. $ba \in P_1$. Damit haben wir den Widerspruch $a \in P_1$ oder $b \in P_1$.

Dieser Widerspruch zeigt, dass $A^{-1}I = A^{-1}Q_1 \cap \ldots \cap A^{-1}Q_m$ eine unverkürzbare Primärzerlegung ist. Zum Schluss zeigen wir: $\rho^{-1}(A^{-1}I) = Q_1 \cap \ldots \cap Q_m$. Für $x \in Q_1 \cap \ldots \cap Q_m$ ist sicher $\rho(x) = \frac{x}{1} \in A^{-1}(Q_1 \cap \ldots \cap Q_m) = A^{-1}Q_1 \cap \ldots \cap A^{-1}Q_m = A^{-1}I$, d.h. $x \in \rho^{-1}(A^{-1}I)$.

Sei umgekehrt $x \in \rho^{-1}(A^{-1}I)$, d.h. $\frac{x}{1} = \rho(x) \in A^{-1}I = A^{-1}(Q_1 \cap \ldots \cap Q_m)$. Wir schreiben $\frac{x}{1} = \frac{y}{a}$ mit $y \in Q_1 \cap \ldots \cap Q_m$, $a \in A$. Dann existiert ein $b \in A$ mit $bax = b1y \in Q_1 \cap \ldots \cap Q_m$. Im Fall $x \notin Q_1 \cap \ldots \cap Q_m$ wäre $x \notin Q_i$ für ein $i \in \{1, \ldots, m\}$, d.h. $ba \in P_i$, und wir hätten den Widerspruch $a \in P_i$ oder $b \in P_i$. Dieser Widerspruch zeigt: $x \in Q_1 \cap \ldots \cap Q_m$.

10.8 Satz (Zweiter Eindeutigkeitssatz)
Sei R noethersch, sei $I \trianglelefteq R$ mit unverkürzbarer Primärzerlegung $I = Q_1 \cap \ldots \cap Q_n$, und sei $P_i := \mathrm{rad}(Q_i)$ für $i = 1, \ldots, n$. Ist P_i minimal in $\{P_1, \ldots, P_n\}$, $A := R \setminus P_i$ und $\rho : R \longrightarrow A^{-1}R$ kanonisch, so ist $Q_i = \rho^{-1}(A^{-1}I)$; insbesondere ist Q_i durch I und P_i eindeutig bestimmt.

Beweis. Für $j \neq i$ ist $P_j \not\subseteq P_i$, d.h. $P_j \cap A = P_j \cap (R \setminus P_i) \neq \emptyset$. Nach Satz 10.7 ist also $A^{-1}I = A^{-1}Q_i$ und $Q_i = \rho^{-1}(A^{-1}I)$.

Beispiel. Sei K ein Körper, sei $R := K[X, Y]$, und sei $I := (X^2, XY)$. Dann ist

$$I = (X) \cap (X, Y)^2$$

eine unverkürzbare Primärzerlegung mit $\mathrm{rad}((X, Y)^2) = (X, Y) \in \mathrm{Max}(R)$ und $\mathrm{rad}((X)) = (X)$. Für $\alpha \in K$ ist auch

$$I = (X) \cap (X^2, Y - \alpha X)$$

eine unverkürzbare Primärzerlegung mit $\mathrm{rad}((X^2, Y - \alpha X)) = (X, Y) \in \mathrm{Max}(R)$. Daher sind unverkürzbare Primärzerlegungen i.a. nicht eindeutig.

11. Artinsche Ringe

Sei R ein Ring.

11.1 Satz. *Ist R artinsch, so gilt:*
(i) $J := \mathrm{J}(R)$ ist nilpotent;
(ii) $\mathrm{J}(R)$ ist Durchschnitt von endlich vielen maximalen Idealen in R;
(iii) Jeder endlich erzeugte R-Modul V hat eine Kompositionsreihe; insbesondere ist V noethersch.
(iv) R ist noethersch;
(v) $\mathrm{Spec}(R) = \mathrm{Max}(R)$.

Beweis. (i) Zu der absteigenden Folge $J \supseteq J^2 \supseteq \ldots$ existiert ein $n \in \mathbb{N}$ mit $J^n = J^{n+1} = \ldots$. Wir nehmen an: $J^n \neq 0$. Dann ist $\mathfrak{I} := \{I \trianglelefteq R : IJ^n \neq 0\} \neq \emptyset$. Da R artinsch ist, existiert ein minimales Element $I \in \mathfrak{I}$. Wegen $IJ^n \neq 0$ existiert ferner ein $x \in I$ mit $0 \neq xJ^n \trianglelefteq R$. Wegen $xJ^nJ^n = xJ^{2n} = xJ^n \neq 0$ ist $xJ^n \in \mathfrak{I}$ und $xJ^n \subseteq I$. Nach Wahl von I ist $I = xJ^n$. Wir schreiben $x = xy$ mit $y \in J^n \subseteq J$. Dann ist $0 = x(1 - y)$, und wir haben wegen $1 - y \in R^\times$ den Widerspruch $x = 0$.

(ii) Wir nehmen das Gegenteil an. Sei $M_1 \in \mathrm{Max}(R)$ beliebig. Dann ist $J \neq M_1$. Also existiert ein $M_2 \in \mathrm{Max}(R)$ mit $M_1 \cap M_2 \subset M_1$. Dann ist $J \neq M_1 \cap M_2$. Also existiert

ein $M_3 \in \mathrm{Max}(R)$ mit $M_1 \cap M_2 \cap M_3 \subset M_1 \cap M_2$. So fährt man fort und erhält einen Widerspruch, da R artinsch ist.

(iii) Seien $M_1, \ldots, M_r \in \mathrm{Max}(R)$ mit $J = M_1 \cap \ldots \cap M_r$, und sei $n \in \mathbb{N}$ mit $J^n = 0$. Jeder Faktor der Folge

$$V \supseteq M_1 V \supseteq M_1^2 V \supseteq \ldots \supseteq (M_1 \cdots M_r)^n V = 0$$

hat die Form U/MU mit einem Untermodul $U \subseteq V$ und einem $M \in \mathrm{Max}(R)$. Nach Voraussetzung ist V artinsch. Daher sind auch U und U/MU artinsch. Man kann U/MU auch als Vektorraum über dem Körper R/M auffassen. Als solcher ist er ebenfalls artinsch, d.h. endlich-dimensional. Daher hat U/MU als R/M-Modul und als R-Modul eine Kompositionsreihe. Also hat auch V eine Kompositionsreihe.

(iv) Wir setzen $V := R$ in (iii).

(v) Für $P \in \mathrm{Spec}(R)$ ist $S := R/P$ ein artinscher Integritätsbereich. Für $0 \neq a \in S$ ist ferner $Sa \supseteq Sa^2 \supseteq \ldots$. Daher existiert ein $n \in \mathbb{N}$ mit $Sa^n = Sa^{n+1} = \ldots$. Wir schreiben $a^n = a^{n+1}x$ mit $x \in S$. Dann ist $ax = 1$. Dies zeigt, dass S ein Körper ist. Also ist $P \in \mathrm{Max}(R)$.

Bemerkung. Da jeder noethersche Ring nur endlich viele minimale Primideale hat, besitzt jeder artinsche Ring R nur endlich viele Primideale (maximale Ideale) $M_1, \ldots, M_k$. Für $i = 1, \ldots, k$ ist $\mathcal{V}(M_i) = \{M_i\} \subseteq \mathrm{Spec}(R)$ abgeschlossen. Daher ist jede Teilmenge von $\mathrm{Spec}(R)$ offen und abgeschlossen. Da $\mathrm{Spec}(R)$ genau 2^k Teilmengen hat, enthält R genau 2^k Idempotente. Für jedes Idempotent $e \in R$ ist

$$R = Re \oplus R(1-e) \cong Re \times R(1-e)$$

mit artinschen Ringen Re, $R(1-e)$. Induktiv folgt, dass

$$R \cong R_1 \times \cdots \times R_k$$

mit lokalen artinschen Ringen $R_1, \ldots, R_k$ ist.

Beispiel. Für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{a_1} \cdots p_r^{a_r}$ ist $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$.

11.2 Satz. *Sei R noethersch und* $\mathrm{Spec}(R) = \mathrm{Max}(R)$. *Dann ist R artinsch.*

Beweis. Wir nehmen das Gegenteil an. Dann ist die Menge aller Ideale $I \trianglelefteq R$ mit der Eigenschaft, dass R/I nichtartinsch ist, nichtleer, enthält also ein maximales Element M. Sicher ist $M \neq R$.

Hat man Elemente $a, b \in R \setminus M$ mit $ab \in M$, so gilt: $M \neq M + Ra$ und $M \neq (M : a)$. Daher sind $R/M+Ra$ und $R/(M : a)$ artinsch. Bemerkung 6.5 liefert eine exakte Folge von R-Moduln und R-Homomorphismen $0 \longrightarrow R/(M : a) \longrightarrow R/M \longrightarrow R/M+Ra \longrightarrow 0$. Also ist auch R/M artinsch, und wir haben einen Widerspruch. Dieser zeigt: $M \in \mathrm{Spec}(R) = \mathrm{Max}(R)$. Dann ist aber R/M artinsch, und wir haben einen Widerspruch.

11.3 Satz. *Sei R noethersch, sei $I \trianglelefteq R$, und sei U ein Untermodul eines endlich erzeugten R-Moduls V. Dann existiert ein Untermodul $W \subseteq V$, der maximal bzgl. $W \cap U = IU$ ist, und es existiert ein $k \in \mathbb{N}$ mit $I^k V \subseteq W$.*

Beweis. Da V noethersch ist, existiert W. Da I endlich erzeugt ist, genügt zu zeigen, dass für $a \in I$ ein $n \in \mathbb{N}$ mit $a^n V \subseteq W$ existiert. Sei also $a \in I$ fest und $V_r := \{v \in V : a^r v \in W\}$ für $r \in \mathbb{N}$. Dann sind $V_1, V_2, \ldots \subseteq V$ Untermoduln mit $V_1 \subseteq V_2 \subseteq \ldots$. Daher existiert ein $n \in \mathbb{N}$ mit $V_n = V_{n+1} = \ldots$. Wegen der Maximalität von W genügt zu zeigen: $(a^n V + W) \cap U = IU$; denn dann ist $a^n V \subseteq a^n V + W = W$.

Sicher ist $IU \subseteq (a^n V + W) \cap U$. Sei umgekehrt $u \in (a^n V + W) \cap U$, und seien $v \in V$, $w \in W$ mit $u = a^n v + w$. Dann ist $a^{n+1} v = au - aw \in IU + W = W$, d.h. $v \in V_{n+1} = V_n$. Folglich ist $a^n v \in W$ und damit $u = a^n v + w \in W \cap U = IU$.

11.4 Satz. (Krulls Durchschnittssatz)
Sei R noethersch, sei $I \trianglelefteq R$, und sei V ein endlich erzeugter R-Modul. Für $U := \bigcap_{n\in\mathbb{N}} I^n V$ gilt dann: $IU = U$.

Beweis. Wir wählen W und k wie oben. Dann ist $U \subseteq I^k V \subseteq W$, d.h. $U = W \cap U = IU$.

Bemerkung. Insbesondere folgt für $I^\infty := \bigcap_{n\in\mathbb{N}} I^n$, indem man $V := R$ setzt: $I \cdot I^\infty = I^\infty$.

11.5 Satz. *Sei R noethersch, und sei V ein endlich erzeugter R-Modul. Dann ist $\bigcap_{n\in\mathbb{N}} \mathrm{J}(R)^n V = 0$. Insbesondere ist also $\bigcap_{n\in\mathbb{N}} J(R)^n = 0$.*

Beweis. Sei $U := \bigcap_{n\in\mathbb{N}} \mathrm{J}(R)^n V$. Nach Satz 11.4 ist $\mathrm{J}(R)U = U$. Da U endlich erzeugt ist, folgt aus Nakayamas Lemma: $U = 0$.

12. Die Krulldimension

Sei R ein Ring.

12.1 Satz. *(i) Für $u \in R \setminus \mathrm{Z}(R)$ und $y \in R$ gilt: $Ry + Ru/Ru \simeq Ruy + Ru^2/Ru^2$.*
(ii) Für $u, y \in R \setminus \mathrm{Z}(R)$ mit $(Ry : u) = (Ry : u^2)$ gilt: $Ry + Ru^2/Ruy + Ru^2 \simeq Ru/Ru^2$.
(iii) Sind $u, y \in R \setminus \mathrm{Z(R)}$ mit $(Ry : u) = (Ry : u^2)$ und hat der R-Modul $Ru + Ry/Ru^2$ eine Kompositionsreihe, so ist $Ru + Ry = Ru^2 + Ry$.

Beweis. (i) Sicher ist $f : Ry + Ru \longrightarrow Ruy + Ru^2/Ru^2$, $x \longmapsto ux + Ru^2$, ein R-Epimorphismus mit $Ru \subseteq \mathrm{Ker}(f)$. Sei umgekehrt $x \in \mathrm{Ker}(f)$, d.h. $0 = f(x) = ux + Ru^2$. Dann ist $ux \in Ru^2$, also $ux = ru^2$ für ein $r \in R$. Daher ist $u(x - ru) = 0$, d.h. $x = ru$. Dies zeigt: $\mathrm{Ker}(f) = Ru$. Die Aussage folgt also aus dem Homomorphiesatz.

(ii) Sicher ist $g : R \longrightarrow Ry + Ru^2/Ruy + Ru^2$, $x \longmapsto xy + Ruy + Ru^2$, ein R-Epimorphismus mit $Ru \subseteq \mathrm{Ker}(g)$. Sei umgekehrt $x \in \mathrm{Ker}(g)$, d.h. $0 = g(x) = xy + Ruy + Ru^2$. Dann ist $xy \in Ruy + Ru^2$. Daher existieren $a, b \in R$ mit $xy = auy + bu^2$. Also ist $b \in (Ry : u^2) = (Ry : u)$. Daher existiert ein $c \in R$ mit $bu = cy$. Dann ist $xy = auy + cuy \in Ruy$. Wegen $y \notin \mathrm{Z}(R)$ folgt: $x \in Ru$. Dies zeigt: $\mathrm{Ker}(g) = Ru$. Der

Homomorphiesatz impliziert also: $R/Ru \simeq Ry + Ru^2/Ruy + Ru^2$. Aus (i) (mit $y := 1$) folgt außerdem: $R/Ru \simeq Ru/Ru^2$.

(iii) Wir berechnen die Kompositionslänge von $V := Ru + Ry/Ru^2$ auf zwei Arten. Einerseits ist $\ell(V) = \ell(Ru + Ry/Ru) + \ell(Ru/Ru^2)$. Andererseits ist

$$\ell(V) = \ell(Ru + Ry/Ru^2 + Ry) + \ell(Ru^2 + Ry/Ru^2 + Ruy) + \ell(Ru^2 + Ruy/Ru^2).$$

Wegen $Ru + Ry/Ru \simeq Ru^2 + Ruy/Ru^2$ und $Ru/Ru^2 \simeq Ru^2 + Ry/Ru^2 + Ruy$ folgt: $0 = \ell(Ru + Ry/Ru^2 + Ry)$, und die Behauptung ist bewiesen.

12.2 Definition. Man nennt die Krulldimension des topologischen Raums $\mathrm{Spec}(R)$ auch **Krulldimension** von R: $\mathrm{Dim}(R) := \mathrm{Dim}(\mathrm{Spec}(R))$.

Bemerkung. Nach Satz 7.3 ist also $\mathrm{Dim}(R)$ das Supremum der Längen s von Primidealketten $P_0 \supset P_1 \supset \ldots \supset P_s$ in $\mathrm{Spec}(R)$. Für $P \in \mathrm{Spec}(R)$ heißt das Supremum $\mathrm{ht}(P)$ der Längen s von Primidealketten der Form $P = P_0 \supset P_1 \supset \ldots \supset P_s$ in $\mathrm{Spec}(R)$ **Höhe** (height) von P. Nach Satz 8.7 ist also $\mathrm{ht}(P) = \mathrm{Dim}(R_P)$ und

$$\mathrm{Dim}(R) = \sup\{\mathrm{ht}(P) : P \in \mathrm{Spec}(R)\} = \sup\{\mathrm{ht}(M) : M \in \mathrm{Max}(R)\}.$$

Satz. (Krulls Hauptidealsatz)
Sei R noethersch, sei $x \in R$, und sei $P \in \mathcal{V}(Rx)$ minimal. Dann ist $\mathrm{ht}(P) \leq 1$. *Im Fall $x \notin \mathrm{Z}(R)$ ist sogar* $\mathrm{ht}(P) = 1$.

Beweis. Wir nehmen zunächst $\mathrm{ht}(P) > 1$ an. Dann existiert in $\mathrm{Spec}(R)$ eine Kette $P \supset P' \supset P''$. Nach Übergang zu R/P'' können wir o.B.d.A. $P'' = 0$ annehmen. Analog können wir nach Übergang zu R_P annehmen: $\mathrm{Max}(R) = \{P\}$. Also ist jetzt R ein lokaler noetherscher Integritätsbereich mit $x \neq 0$; denn sonst wäre $P = 0$.

Sei $0 \neq y \in P'$ und $I_k := (Ry : x^k)$ für $k \in \mathbb{N}$. Wegen $I_1 \subseteq I_2 \subseteq \ldots$ existiert ein $n \in \mathbb{N}$ mit $I_n = I_{n+1} = \ldots$. Für $u := x^n$ ist also $(Ry : u) = (Ry : u^2)$. Ferner ist R/Ru^2 ein lokaler Ring mit $\mathrm{Spec}(R/Ru^2) = \{P/Ru^2\}$; denn jedes Primideal zwischen P und Ru^2 würde mit $u^2 = x^{2n}$ auch x enthalten. Nach Satz 11.2 ist R/Ru^2 artinsch, hat also eine Kompositionsreihe. Folglich hat jeder endlich erzeugte R/Ru^2-Modul eine Kompositionsreihe, insbesondere $Ru + Ry/Ru^2$. Da R ein Integritätsbereich ist, folgt aus Satz 12.1: $Ru + Ry = Ru^2 + Ry$. Daher existieren $c, d \in R$ mit $u = cu^2 + dy$, d.h. $u(1 - cu) = dy \in Ry$. Wegen $1 - cu \in R^\times$ folgt $u \in Ry \subseteq P'$. Damit haben wir den Widerspruch $x \in P'$.

Im Fall $\mathrm{ht}(P) = 0$ ist $P \in \mathrm{Min}(R)$, also $x \in \mathrm{Z}(R)$ nach Satz 4.5.

Beispiel. Der Nullring erhält die Krulldimension -1. Jeder von 0 verschiedene artinsche Ring hat Krulldimension 0. Jeder Hauptidealring, der kein Körper ist, hat Krulldimension 1.

12.3 Satz. (Krulls verallgemeinerter Hauptidealsatz)
Sei R noethersch und $I = (a_1, \ldots, a_n) \trianglelefteq R$. Dann ist $\mathrm{ht}(P) \leq n$ *für jedes minimale Element $P \in \mathcal{V}(I)$.*

Beweis. Wir nehmen das Gegenteil an und wählen ein Gegenbeispiel mit möglichst kleinem n. Nach Satz 12.2 ist $n \geq 2$. Also existiert in $\mathrm{Spec}(R)$ eine Kette $P = P_0 \supset P_1 \supset \ldots \supset P_{n+1}$. O.B.d.A. sei dabei P_1 maximal in der Menge der Primideale von R, die echt in P_0 enthalten sind. Nach Übergang zu R_P können wir annehmen, dass R lokal und $\mathrm{Max}(R) = \{P\}$ ist. Wegen $I \not\subseteq P_1$ existiert ein $i \in \{1, \ldots, n\}$ mit $a_i \notin P_1$; o.B.d.A. sei $a_1 \notin P_1$. Dann ist P das einzige Primideal in R, das $Ra_1 + P_1$ enthält, d.h. $P = \mathrm{rad}(Ra_1 + P_1)$. Daher existiert ein $t \in \mathbb{N}$ mit $P^t \subseteq Ra_1 + P_1$. Für $i = 2, \ldots, n$ sei $a_i^t = c_i a_1 + p_i$ mit $c_i \in R$ und $p_i \in P_1$. Dann ist $J := (p_2, \ldots, p_n) \subseteq P_1$.

Wäre P_1 minimal in $\mathcal{V}(J)$, so hätten wir nach Induktion den Widerspruch $n \leq \mathrm{ht}(P_1) \leq n-1$. Folglich existiert ein $Q \in \mathrm{Spec}(R)$ mit $J \subseteq Q \subset P_1$.

Sei $P' \in \mathrm{Spec}(R)$ mit $Ra_1 + Q \subseteq P'$. Für $i = 2, \ldots, n$ ist dann $a_i^t \in Ra_1 + J \subseteq Ra_1 + Q \subseteq P'$, also auch $a_i \in P'$. Wegen $I = (a_1, \ldots, a_n)$ folgt: $P' = P$.

Dies zeigt, dass P das einzige Primideal in R ist, das $Ra_1 + Q$ enthält. Setzt man $\overline{R} := R/Q$ und $\overline{a}_1 := a_1 + Q$, so ist also P/Q minimal in $\mathcal{V}(\overline{R}\overline{a}_1)$, und $P/Q \supset P_1/Q \supset Q/Q = 0$ ist eine Primidealkette in $\overline{R}$. Dies widerspricht Satz 12.2.

Bemerkung. In einem noetherschen Ring hat also jedes Primideal P endliche Höhe. Genauer gilt: $\mathrm{ht}(P) \leq \mu(P)$. Es gibt aber auch noethersche Ringe unendlicher Krulldimension.

Beispiel. Ist R ein faktorieller Ring (nicht unbedingt noethersch), so gilt:

$$\{P \in \mathrm{Spec}(R) : \mathrm{ht}(P) = 1\} = \{(p) : p \in R \text{ Primelement}\}.$$

Zum Beweis sei $P \in \mathrm{Spec}(R)$ mit $\mathrm{ht}(P) = 1$, d.h. $P \neq 0$. Sei $0 \neq x \in P$, und sei $x = p_1 \cdots p_r$ mit Primelementen $p_1, \ldots, p_r \in R$. Dann existiert ein $i \in \{1, \ldots, r\}$ mit $p_i \in P$. Wegen $0 \neq (p_i) \in \mathrm{Spec}(R)$ folgt: $(p_i) = P$.

Sei umgekehrt $p \in R$ ein Primelement, also $0 \neq (p) \in \mathrm{Spec}(R)$. Ist $P \in \mathrm{Spec}(R)$ mit $P \subset (p)$, so existiert für $x \in P$ ein $y \in R$ mit $x = py$. Wegen $py \in P$ und $p \notin P$ folgt $y \in P$. Also existiert analog ein $z \in P$ mit $y = pz$, d.h. $x = p^2 z$. So fährt man fort und erhält, dass x für $k \in \mathbb{N}$ durch p^k teilbar ist. Also ist $x = 0$. Dies zeigt: $P = 0$, d.h. $\mathrm{ht}(Rp) = 1$.

Man kann auch zeigen, dass ein noetherscher Integritätsbereich R genau dann faktoriell ist, wenn jedes Primideal in R der Höhe 1 ein Hauptideal ist.

12.4 Satz. *Sei R noethersch und $I = (a_1, \ldots, a_n) \trianglelefteq R$. Für $P \in \mathcal{V}(I)$ gilt dann:*

$$\mathrm{ht}(P) \leq \mathrm{ht}(P/I) + n.$$

Beweis. (Induktion nach $k := \mathrm{ht}(P/I)$)

Im Fall $k = 0$ ist P minimal in $\mathcal{V}(I)$, und die Behauptung folgt aus Satz 12.3. Sei also $k > 0$, und seien $P_1, \ldots, P_s$ die minimalen Elemente in $\mathcal{V}(I)$. Wegen $P \notin \{P_1, \ldots, P_s\}$ ist $P \not\subseteq P_1 \cup \ldots \cup P_s$ nach Satz 4.2. Sei $y \in P \setminus (P_1 \cup \ldots \cup P_s)$. Dann ist $J := I + Ry \subseteq P$. Wegen $J \not\subseteq P_1 \cup \ldots \cup P_s$ ist $\mathrm{ht}(P/J) \leq k-1$. Nach Induktion ist also $\mathrm{ht}(P) \leq \mathrm{ht}(P/J) + (n+1) \leq k + n$.

12.5 Satz. *Sei R noethersch, und seien $I, J \trianglelefteq R$ mit $J \subseteq I$ und $\mathcal{V}(I) = \mathcal{V}(J)$. Ferner sei $m := \mu(I/J)$, und es seien $P_1, \ldots, P_s \in \operatorname{Spec}(R)$ mit $I \not\subseteq \bigcup_{j=1}^{s} P_j$. Dann existieren $a_1, \ldots, a_m \in I$ mit folgenden Eigenschaften:*
(i) $I = (a_1, \ldots, a_m) + J$;
(ii) $a_i \notin \bigcup_{j=1}^{s} P_j$ *für* $j = 1, \ldots, m$;
(iii) $\operatorname{ht}(P) \geq m$ *für alle* $P \in \mathcal{V}((a_1, \ldots, a_m)) \setminus \mathcal{V}(I)$.

Beweis. Wir konstruieren induktiv Elemente $a_1, \ldots, a_r \in I \setminus \bigcup_{j=1}^{s} P_j$ derart, dass $a_1 + J, \ldots, a_r + J$ zu einem m-elementigen Erzeugendensystem von I/J gehören und $\operatorname{ht}(P) \geq r$ für alle $P \in \mathcal{V}((a_1, \ldots, r)) \setminus \mathcal{V}(I)$ gilt.

Im Fall $r = 0$ ist nichts zu tun. Sei also $0 \leq r < m$, und seien bereits $a_1, \ldots, a_r$ mit den gewünschten Eigenschaften konstruiert. Zunächst wählen wir $a \in I$ so, dass $a_1 + J, \ldots, a_r + J, a + J$ zu einem m-elementigen Erzeugendensystem von I/J gehören. Ferner seien $Q_1, \ldots, Q_t$ die minimalen Elemente in $\mathcal{V}((a_1, \ldots, a_r))$, die nicht zu $\mathcal{V}(I)$ gehören, und $\mathfrak{X}$ sei die Menge der maximalen Elemente in $\{P_1, \ldots, P_s, Q_1, \ldots, Q_t\}$. Dann ist $\mathfrak{X} = \mathfrak{X}_1 \cup \mathfrak{X}_2$ mit $\mathfrak{X}_1 := \{P \in \mathfrak{X} : a \in P\}$ und $\mathfrak{X}_2 := \{P \in \mathfrak{X} : a \notin P\}$.

Im Fall $J \subseteq \bigcup_{P \in \mathfrak{X}} P$ wäre $J \subseteq P$ für ein $P \in \mathfrak{X}$ nach Satz 4.2, d.h. $P \in \mathcal{V}(J) = \mathcal{V}(I)$. Also wäre $I \subseteq P = P_i$ für ein $i \in \{1, \ldots, s\}$. Damit hätten wir den Widerspruch $I \subseteq \bigcup_{j=1}^{s} P_j$.

Dieser Widerspruch zeigt, dass ein Element $b \in J \setminus \bigcup_{P \in \mathfrak{X}} P$ existiert.

Wir nehmen an: $\bigcap_{P \in \mathfrak{X}_2} P \subseteq \bigcup_{P \in \mathfrak{X}_1} P$. Nach Satz 4.2 ist dann $\prod_{P \in \mathfrak{X}_2} P \subseteq \bigcap_{P \in \mathfrak{X}_2} P \subseteq Q$ für ein $Q \in \mathfrak{X}_1$, d.h. $P \subseteq Q$ für ein $P \in \mathfrak{X}_2$. Damit haben wir den Widerspruch $P = Q \in \mathfrak{X}_2 \cap \mathfrak{X}_1 = \emptyset$.

Dieser Widerspruch zeigt, dass ein Element $c \in \bigcap_{P \in \mathfrak{X}_2} P \setminus \bigcup_{P \in \mathfrak{X}_1} P$ existiert. Dann ist $a_{r+1} := a + bc \in I$.

Wir nehmen an: $a_{r+1} \in P$ für ein $P \in \mathfrak{X}$. Im Fall $P \in \mathfrak{X}_2$ ist $c \in P$, und wir haben den Widerspruch $a \in P$. Im Fall $P \in \mathfrak{X}_1$ ist $a \in P$. Dann ist $bc \in P$, also $c \in P$ wegen $b \notin P$. Damit haben wir auch in diesem Fall einen Widerspruch.

Also ist $a_{r+1} \notin P$ für alle $P \in \mathfrak{X}$; insbesondere ist $a_{r+1} \notin P_j$ für $j = 1, \ldots, s$. Wegen $a_{r+1} + J = a + J$ gehören $a_1 + J, \ldots, a_r + J, a_{r+1} + J$ zu einem m-elementigen Erzeugendensystem von I/J.

Sei jetzt $P \in \mathcal{V}((a_1, \ldots, a_r, a_{r+1})) \setminus \mathcal{V}(I)$. Wegen $P \in \mathcal{V}((a_1, \ldots, a_r))$ ist dann $P \supseteq Q_i$ für ein $i \in \{1, \ldots, t\}$. Wegen $a_{r+1} \in P$, aber $a_{r+1} \notin Q_i$ ist $P \neq Q_i$, also $\operatorname{ht}(P) > \operatorname{ht}(Q_i) \geq r$ wegen $Q_i \in \mathcal{V}((a_1, \ldots, a_r)) \setminus \mathcal{V}(I)$. Daher ist $\operatorname{ht}(P) \geq r + 1$. Damit ist der Satz bewiesen.

12.6 Satz. *Sei R noethersch, sei $P \in \operatorname{Spec}(R)$, und sei $m := \operatorname{ht}(P)$. Dann existieren $a_1, \ldots, a_m \in P$ derart, dass P minimal in $\mathcal{V}((a_1, \ldots, a_m))$ ist.*

Bemerkung. Dies ist eine Umkehrung des verallgemeinerten Hauptidealsatzes.

Beweis. Wir setzen $I := P$ und $J := P^2$. Dann ist $\mathcal{V}(I) = \mathcal{V}(J)$ und $\mu(P/P^2) \geq \mu(P_P/P_P^2) = \mu(P_P) \geq \operatorname{ht}(P_P) = \operatorname{ht}(P) = m$. Im Beweis des vorigen Satzes wurden Elemente $a_1, \ldots, a_m \in P$ mit $\operatorname{ht}(Q) \geq m$ für alle $Q \in \mathcal{V}((a_1, \ldots, a_m)) \setminus \mathcal{V}(P)$ konstruiert. Dann ist P minimal in $\mathcal{V}((a_1, \ldots, a_m))$; denn sonst würde ein $Q \in \mathcal{V}((a_1, \ldots, a_m))$ mit $Q \subset P$ existieren. Dann wäre $Q \in \mathcal{V}((a_1, \ldots, a_m)) \setminus \mathcal{V}(P)$, und wir hätten den Widerspruch $\operatorname{ht}(P) > \operatorname{ht}(Q) \geq m$.

12.7 Satz. *Seien $Q, Q' \in \mathrm{Spec}(R[X])$ mit $Q \subset Q'$ und $Q \cap R = Q' \cap R =: P$. Dann ist $Q = P \cdot R[X] =: P[X]$.*

Beweis. Wir setzen $\overline{R} := R/P$. Dann ist $R[X]/P[X] \cong \overline{R}[X]$ ein Integritätsbereich, also $P[X] \in \mathrm{Spec}(R[X])$ und $P[X] \subseteq Q \subset Q'$. Wir nehmen $P[X] \subset Q \subset Q'$ an. Damit haben wir eine Primidealkette der Länge 2 in $R[X]$. Übergang zu $R[X]/P[X] \cong \overline{R}[X]$ liefert eine Primidealkette $0 \subset \overline{Q} \subset \overline{Q}'$ in $\overline{R}[X]$ mit $\overline{Q} \cap \overline{R} = \overline{Q}' \cap \overline{R} = 0$. Setzt man $\overline{A} := \overline{R} \setminus \{0\}$, so ist also $\overline{Q} \cap \overline{A} = \overline{Q}' \cap \overline{A} = \emptyset$. Daher erhält man eine Primidealkette der Länge 2 in $\overline{A}^{-1}(\overline{R}[X]) \cong (\overline{A}^{-1}\overline{R})[X]$. Da $\overline{A}^{-1}\overline{R}$ ein Körper, also $(\overline{A}^{-1}\overline{R})[X]$ ein Hauptidealring ist, haben wir einen Widerspruch.

Beispiel. Seien R ein HIR (z.B. $R = \mathbb{Z}$ oder $R = k[Y]$ für einen Körper k) und $K := \mathrm{Quot}(R)$. Bekanntlich ist $S := R[X]$ faktoriell und noethersch, aber i.a. kein HIR. Da S ein Integritätsbereich ist, ist $\mathrm{Min}(S) = \{0\}$. Nach Beispiel 12.3 sind die Primideale der Höhe 1 in S genau die von Primelementen in S erzeugten Hauptideale.

Sei also $Q \in \mathrm{Spec}(S)$ mit $\mathrm{ht}(Q) \geq 2$. Dann existiert ein $Q' \in \mathrm{Spec}(S)$ mit $Q \supset Q' \supset 0$.

Im Fall $Q \cap R = 0$ wäre auch $Q' \cap R = 0$. Mit Satz 12.7 hätten wir also den Widerspruch $Q' = 0 \cdot S = 0$.

Also ist $0 \neq Q \cap R \in \mathrm{Spec}(R)$. Daher existiert ein Primelement p in R mit $Q \cap R = Rp$. Ferner ist $F := R/Rp$ ein Körper. Sei $\phi : R[X] \longrightarrow F[X]$ kanonisch, also $\mathrm{Ker}(\phi) = pR[X] \subseteq Q$. Dann ist $\phi(Q) \in \mathrm{Spec}(F[X])$. Da $F[X]$ ein HIR ist, existiert ein irreduzibles Polynom $\overline{h}$ in $F[X]$ mit $\phi(Q) = (\overline{h})$. Sei $h \in R[X]$ mit $\overline{h} = \phi(h)$. Dann ist $Q = (p, h)$. Nach Satz 12.3 ist $\mathrm{ht}(Q) = 2$ und $Q \in \mathrm{Max}(S)$. Insbesondere ist $\mathrm{Dim}(S) \leq 2$.

12.8 Satz. *Ist R noethersch und $P \in \mathrm{Spec}(R)$, so ist $\mathrm{ht}_R(P) = \mathrm{ht}_{R[X]}(P[X])$.*

Beweis. Sei $n := \mathrm{ht}_R(P)$. Nach Satz 12.6 existieren dann $a_1, \ldots, a_n \in P$ derart, dass P minimal in $\mathcal{V}((a_1, \ldots, a_n))$ ist. Wir setzen $I := (a_1, \ldots, a_n)$. Dann ist $I[X] := I \cdot R[X] = a_1R[X] + \cdots + a_nR[X]$.

Wir nehmen an, dass ein $P' \in \mathrm{Spec}(R[X])$ mit $P[X] \supset P' \supseteq I[X]$ existiert. Dann ist $P = P[X] \cap R \supseteq P' \cap R \supseteq I$ mit $P' \cap R \in \mathrm{Spec}(R)$, also $P' \cap R = P$. Aus Satz 12.7 folgt daher der Widerspruch $P' = PR[X] = P[X]$.

Dieser Widerspruch zeigt, dass $P[X]$ minimal in $\mathcal{V}(I[X])$ ist. Aus dem verallgemeinerten Hauptidealsatz folgt also: $\mathrm{ht}_{R[X]}(P[X]) \leq n$.

Andererseits existiert eine Kette $P_0 \subset P_1 \subset \ldots \subset P_n = P$ in $\mathrm{Spec}(R)$. Daher ist $P_0[X] \subset P_1[X] \subset \ldots \subset P_n[X] = P[X]$ eine Kette in $\mathrm{Spec}(R[X])$. Also gilt: $\mathrm{ht}_{R[X]}(P[X]) \geq n$.

12.9 Satz. *Ist R noethersch, so ist $\mathrm{Dim}(R[X]) = \mathrm{Dim}(R) + 1$.*

Beweis. Ist $P_0 \subset \ldots \subset P_n$ eine Kette in $\mathrm{Spec}(R)$, so ist

$$P_0[X] \subset \ldots \subset P_n[X] \subset P_n[X] + XR[X]$$

eine Kette in $\mathrm{Spec}(R[X])$. Daher ist $\mathrm{Dim}(R[X]) \geq \mathrm{Dim}(R) + 1$.

Sei umgekehrt $Q_0 \subset \ldots \subset Q_r$ eine Kette in $\mathrm{Spec}(R[X])$. Wir werden zeigen, dass $\mathrm{Dim}(R) \geq r - 1$ gilt. Dazu sei $P_i := Q_i \cap R$ für $i = 1, \ldots, r$. Dann ist $P_0 \subseteq \ldots \subseteq P_r$. Im

Fall $P_0 \subset \ldots \subset P_r$ ist sogar $\mathrm{Dim}(R) \geq r$. Sei also $P_j = P_{j+1}$ für ein $j \in \{0, \ldots, r-1\}$; dabei sei j möglichst groß gewählt. Aus Satz 12.7 folgt dann: $Q_j = P_j[X]$. Nach Satz 12.8 ist also $\mathrm{ht}_R(P_j) = \mathrm{ht}_{R[X]}(Q_j) \geq j$. Nach Wahl von j ist außerdem $P_{j+1} \subset \ldots \subset P_r$. Daher gilt: $\mathrm{Dim}(R) \geq \mathrm{ht}_R(P_r) \geq r - j - 1 + \mathrm{ht}_R(P_j) \geq r - 1$.

Bemerkung. Induktiv folgt: $\mathrm{Dim}(R[X_1, \ldots, X_n]) = \mathrm{Dim}(R) + n$ für $n \in \mathbb{N}$.

Beispiel. $\mathrm{Dim}(K[X_1, \ldots, X_n]) = n$ für jeden Körper K, und $\mathrm{Dim}(\mathbb{Z}[X_1, \ldots, X_n]) = n+1$.

13. Ganze Ringerweiterungen

Sei $R \subseteq S$ eine Ringerweiterung.

13.1 Satz. *Sei S Integritätsbereich und ganz über R. Dann ist R auch ein Integritätsbereich, und es gilt: R Körper $\iff$ S Körper.*

Beweis. "$\Longrightarrow$": Sei R Körper und $0 \neq s \in S$. Dann existieren $r_0, \ldots, r_{n-1} \in R$ mit $0 = s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$. Dabei sei o.B.d.A. $r_0 \neq 0$; denn sonst können wir s kürzen. Dann ist $1 = r_0^{-1}s(-s^{n-1} - r_{n-1}s^{n-1} - \cdots - r_1)$, d.h. $s \in S^\times$.

"$\Longleftarrow$": Sei S Körper und $0 \neq r \in R \subseteq S$, d.h. $r^{-1} \in S$. Dann existieren $a_0, \ldots, a_{n-1} \in R$ mit $(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_1 r^{-1} + a_0 = 0$. Multiplikation mit $r^{n-1} \in R$ ergibt: $r^{-1} = -a_{n-1} - \cdots - a_1 r^{n-2} - a_0 r^{n-1} \in R$.

13.2 Satz. *Ist S ganz über R, so gilt für $Q \in \mathrm{Spec}(S)$ und $P := Q \cap R$: $Q \in \mathrm{Max}(S) \iff P \in \mathrm{Max}(R)$.*

Beweis. Nach Bemerkung 4.2 ist $P \in \mathrm{Spec}(R)$. Ferner ist $f : R/P \longrightarrow S/Q$, $a + P \longmapsto a + Q$, ein Ringmonomorphismus. So kann man R/P als Teilring des Integritätsbereichs S/Q auffassen. Offenbar ist S/Q ganz über R/P. Nach Satz 13.1 gilt also: R/P Körper $\iff$ S/Q Körper. Daraus folgt die Behauptung.

13.3 Satz. *Sei S ganz über R.*
(i) Für jede multiplikative Teilmenge $A \subseteq R$ ist dann $A^{-1}S$ eine ganze Ringerweiterung von $A^{-1}R$.
(ii) Sind $Q, Q' \in \mathrm{Spec}(S)$ mit $Q \subseteq Q'$ und $R \cap Q = R \cap Q' =: P$, so ist $Q = Q'$.

Beweis. (i) Seien $s \in S$ und $a \in A$. Dann existieren $r_0, \ldots, r_{n-1} \in R$ mit $s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$. Dann sind $\frac{r_0}{a^n}, \ldots, \frac{r_{n-1}}{a} \in A^{-1}R$ mit

$$(\frac{s}{a})^n + \frac{r_{n-1}}{a}(\frac{s}{a})^{n-1} + \cdots + \frac{r_1}{a^{n-1}}\frac{s}{a} + \frac{r_0}{a^n} = 0.$$

(ii) Nach Bemerkung 4.2 ist $P \in \mathrm{Spec}(R)$. Daher ist $A := R \setminus P \subseteq R$ multiplikativ. Nach (i) ist also $A^{-1}S$ ganz über $A^{-1}R = R_P$; dabei ist R_P lokal und $A^{-1}P = P_P \in \mathrm{Max}(R_P)$. Nach Satz 8.7 sind $A^{-1}Q, A^{-1}Q' \in \mathrm{Spec}(A^{-1}S)$ mit $A^{-1}Q \subseteq A^{-1}Q'$. Nach Bemerkung 4.2 sind $A^{-1}Q \cap A^{-1}R, A^{-1}Q' \cap A^{-1}R \in \mathrm{Spec}(A^{-1}R)$ mit $A^{-1}P \subseteq A^{-1}Q \cap A^{-1}R \subseteq$

$A^{-1}Q' \cap A^{-1}R$. Daher gilt: $A^{-1}P = A^{-1}Q \cap A^{-1}R = A^{-1}Q' \cap A^{-1}R$. Nach Satz 13.2 ist $A^{-1}Q \in \mathrm{Max}(A^{-1}S)$, also $A^{-1}Q = A^{-1}Q'$ und damit $Q = Q'$ nach Satz 8.7.

Bemerkung. In dieser Situation liefert jede Kette $Q_0 \supset Q_1 \supset \ldots \supset Q_s$ in $\mathrm{Spec}(S)$ eine Kette $Q_0 \cap R \supset Q_1 \cap R \supset \ldots \supset Q_s \cap R$ in $\mathrm{Spec}(R)$. Daher ist $\mathrm{Dim}(S) \leq \mathrm{Dim}(R)$. Wir werden Gleichheit zeigen.

13.4 Satz. (Lying-over)
Sei S ganz über R. Dann existiert zu jedem $P \in \mathrm{Spec}(R)$ ein $Q \in \mathrm{Spec}(S)$ mit $P = Q \cap R$.

Beweis. Da $A := R \setminus P \subseteq R$ eine multiplikative Teilmenge ist, ist $A^{-1}S$ ganz über $A^{-1}R = R_P$; dabei ist R_P lokal und $A^{-1}P = P_P \in \mathrm{Max}(R_P)$. Sei $M \in \mathrm{Max}(A^{-1}S)$. Nach Satz 13.2 ist $M \cap A^{-1}R \in \mathrm{Max}(A^{-1}R)$, d.h. $M \cap A^{-1}R = A^{-1}P$. Sei $\sigma : S \longrightarrow A^{-1}S$ kanonisch. Dann ist $\sigma^{-1}(M) \in \mathrm{Spec}(S)$ und $\sigma^{-1}(M) \cap A = \emptyset$. Daher ist $R \cap \sigma^{-1}(M) \in \mathrm{Spec}(R)$ und $R \cap \sigma^{-1}(M) \cap A = \emptyset$, d.h. $R \cap \sigma^{-1}(M) \subseteq P$. Andererseits ist $P \subseteq R$ und $P \subseteq \sigma^{-1}(M)$ wegen $\sigma(P) \subseteq A^{-1}P \subseteq M$. Also gilt: $P = R \cap \sigma^{-1}(M)$.

Bemerkung. In der obigen Situation ist $f : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R)$, $Q \longmapsto Q \cap R$, nicht nur stetig, sondern auch **abgeschlossen**; das bedeutet, dass $f(\mathfrak{B})$ für jede abgeschlossene Teilmenge $\mathfrak{B} \subseteq \mathrm{Spec}(S)$ abgeschlossen in $\mathrm{Spec}(R)$ ist.

Zum Beweis sei $J \trianglelefteq S$. Dann ist

$$f(\mathcal{V}_S(J)) = \{Q \cap R : J \subseteq Q \in \mathrm{Spec}(S)\} \subseteq \{P \in \mathrm{Spec}(R) : J \cap R \subseteq P\} = \mathcal{V}_R(J \cap R).$$

Ist umgekehrt $P \in \mathrm{Spec}(R)$ mit $J \cap R \subseteq P$, so ist $P/J \cap R \in \mathrm{Spec}(R/J \cap R)$. Da $R/J \cap R \longrightarrow R + J/J$, $a + (J \cap R) \longmapsto a + J$, ein Ringisomorphismus ist, ist $P + J/J \in \mathrm{Spec}(R/J)$. Da S/J ganz über $R + J/J$ ist, existiert ein $Q \in \mathrm{Spec}(S)$ mit $J \subseteq Q$ und $(Q/J) \cap (R + J/J) = P + J/J$. Dann ist $P + J = Q \cap (R + J) = (Q \cap R) + J$ nach Dedekinds Lemma. Also ist $P = Q \cap R \in f(\mathcal{V}_S(J))$. Dies zeigt: $f(\mathcal{V}_S(J)) = \mathcal{V}_R(J \cap R)$.

13.5 Satz. (Going-up)
Sei S ganz über R. Seien ferner $P_1 \subset P_2 \subset \ldots \subset P_m$ und $Q_1 \subset Q_2 \subset \ldots \subset Q_n$ Ketten in $\mathrm{Spec}(R)$ *bzw.* $\mathrm{Spec}(S)$ *mit $n < m$ und $P_i = Q_i \cap R$ für $i = 1, \ldots, n$. Dann existieren $Q_{n+1}, \ldots, Q_m \in \mathrm{Spec}(S)$ mit $Q_1 \subset Q_2 \subset \ldots \subset Q_n \subset Q_{n+1} \subset \ldots \subset Q_m$ und $P_i = Q_i \cap R$ für $i = 1, \ldots, m$.*

Beweis. O.B.d.A. sei $m = 2$ und $n = 1$, d.h. $P_1 \subset P_2 \subset R$, $Q_1 \subset S$ und $Q_1 \cap R = P_1$. Da

$$f : \overline{R} := R/P_1 \longrightarrow \overline{S} := S/Q_1, \quad a + P_1 \longmapsto a + Q_1,$$

ein Ringmonomorphismus ist, können wir $\overline{R}$ als Teilring von $\overline{S}$ auffassen. Offenbar ist $\overline{S}$ ganz über $\overline{R}$ und $\overline{P}_2 := P_2/P_1 \in \mathrm{Spec}(\overline{R})$, d.h. $f(\overline{P}_2) \in \mathrm{Spec}(f(\overline{R}))$. Nach Satz 13.4 existiert ein $\overline{Q}_2 = Q_2/Q_1 \in \mathrm{Spec}(\overline{S})$ mit $\overline{Q}_2 \cap f(\overline{R}) = f(\overline{P}_2)$, d.h. $P_2 + Q_1 = Q_2 \cap (R + Q_1) = (Q_2 \cap R) + Q_1$ mit $Q_2 \in \mathrm{Spec}(S)$. Also ist $f(Q_2 \cap R/P_1) = f(P_2/P_1)$, d.h. $Q_2 \cap R/P_1 = P_2/P_1$ und damit $Q_2 \cap R = P_2$.

Bemerkung. Ist S ganz über R, so ist also $\mathrm{Dim}(S) = \mathrm{Dim}(R)$.

Beispiel. Sei $\mathbb{Q} \subseteq K$ eine Körpererweiterung und R der ganze Abschluss von $\mathbb{Z}$ in K. Dann ist $\mathrm{Dim}(R) = \mathrm{Dim}(\mathbb{Z}) = 1$, d.h. $\mathrm{Spec}(R) = \{0\} \cup \mathrm{Max}(R)$.

13.6 Definition. Sei $I \trianglelefteq R$. Ein Element $s \in S$ heißt **ganz** über I, falls $a_0, \ldots, a_{n-1} \in I$ mit $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$ existieren.

Satz. *Sei $\overline{R}$ der ganze Abschluss von R in S. Sei ferner $I \trianglelefteq R$ und $\overline{I} := \{s \in S : s \text{ ganz über } I\}$, also $\overline{I} \subseteq \overline{R}$. Dann ist $\overline{I} = \mathrm{rad}(I \cdot \overline{R})$; dabei bezeichnet $I \cdot \overline{R}$ das von I erzeugte Ideal von $\overline{R}$.*

Beweis. Zu $s \in \overline{I} \subseteq \overline{R}$ existieren $a_0, \ldots, a_{n-1} \in I$ mit $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$. Also ist $s^n \in I\overline{R}$, d.h. $s \in \mathrm{rad}(I\overline{R})$.

Sei umgekehrt $s \in \mathrm{rad}(I\overline{R})$ und $n \in \mathbb{N}$ mit $s^n \in I\overline{R}$. Dann existieren $a_1, \ldots, a_m \in I$ und $x_1, \ldots, x_m \in \overline{R}$ mit $s^n = a_1x_1 + \cdots + a_mx_m$. Daher ist $M := R[x_1, \ldots, x_m]$ ein endlich erzeugter R-Modul. Wir schreiben $M = Ry_1 + \cdots + Ry_k$ und $s^n y_j = \sum_{i=1}^k a_{ij}y_i$ mit $a_{ij} \in I$ für alle i, j. Dann ist $\sum_{i=1}^k (s^n\delta_{ij} - a_{ij})y_i = 0$ für $j = 1, \ldots, k$. Sei (b_{ij}) die Adjunkte von $(s^n\delta_{ij} - a_{ij})$. Dann ist $(s^n\delta_{ij} - a_{ij})(b_{ij}) = (\delta_{ij}\Delta)$ mit $\Delta := \det(s^n\delta_{ij} - a_{ij})$. Also gilt:

$$\sum_{j=1}^{k} (s^n\delta_{ij} - a_{ij})b_{jl} = \delta_{il}\Delta \qquad (i, l = 1, \ldots, k)$$

und

$$0 = \sum_{j=1}^{k} b_{jl} \sum_{i=1}^{k} (s^n\delta_{ij} - a_{ij})y_i = \sum_{i,j=1}^{k} (s^n\delta_{ij} - a_{ij})b_{jl}y_i = \sum_{i=1}^{k} \delta_{il}\Delta y_i = \Delta y_l$$

für $l = 1, \ldots, k$. Wegen $1 \in M$ folgt: $\Delta = 0$. Daher ist s ganz über I.

13.7 Satz. *Sei S ein Integritätsbereich (also auch R). Ferner seien K bzw. L die Quotientenkörper von R bzw. S. (Dann ist also $K \subseteq L$.) Sei ferner R normal, $I \trianglelefteq R$ und $s \in S$ ganz über I (also auch algebraisch über K). Dann hat das Minimalpolynom f von s über K die Form $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ mit $a_0, \ldots, a_{n-1} \in \mathrm{rad}(I)$.*

Beweis. Seien $a_0, \ldots, a_{n-1} \in K$ und $b_0, \ldots, b_{r-1} \in I$ mit $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ und $s^r + b_{r-1}s^{r-1} + \cdots + b_1 s + b_0 = 0$. Sei ferner $\overline{L}$ der algebraische Abschluss von L und $f = (X - t_1)\cdots(X - t_n)$ mit $t_1 = s, t_2, \ldots, t_n \in \overline{L}$. Da f ein Teiler von $X^r + b_{r-1}X^{r-1} + \cdots + b_1X + b_0$ in $K[X]$ ist, sind $t_1, \ldots, t_n$ ganz über I. Nach Satz 13.6 sind daher auch $a_0, \ldots, a_{n-1}$ ganz über I. Wiederum mit Satz 13.6 folgt: $a_0, \ldots, a_{n-1} \in \mathrm{rad}(I)$.

13.8 Bemerkung. Sei R ein Integritätsbereich, und sei $A \subseteq R$ eine multiplikative Teilmenge mit $0 \notin A$. Dann kann man $A^{-1}R = \{\frac{r}{a} : r \in R,\ a \in A\}$ als Teilring des Quotientenkörpers K von R auffassen. Wir haben also: $R \subseteq A^{-1}R \subseteq K$.

Satz. (Going-down)
Sei S ein Integritätsbereich (also auch R) und ganz über R. Ferner sei R normal. Sind $P_1 \supset P_2 \supset \ldots \supset P_m$ und $Q_1 \supset Q_2 \supset \ldots \supset Q_n$ Ketten in $\mathrm{Spec}(R)$ *bzw.* $\mathrm{Spec}(S)$ *mit*

$n < m$ und $Q_i \cap R = P_i$ für $i = 1, \ldots, n$, so existieren $Q_{n+1}, \ldots, Q_m \in \mathrm{Spec}(S)$ mit $Q_1 \supset Q_2 \supset \ldots \supset Q_n \supset Q_{n+1} \supset \ldots \supset Q_m$ und $Q_i \cap R = P_i$ für $i = 1, \ldots, m$.

Beweis. O.B.d.A. sei $m = 2$ und $n = 1$, d.h. $R \supset P_1 \supset P_2$, $S \supset Q_1$ und $Q_1 \cap R = P_1$. Wir setzen $K := \mathrm{Quot}(R)$, $L := \mathrm{Quot}(S)$ und können annehmen: $R \subseteq S \subseteq S_{Q_1} \subseteq L$. Dann ist $(P_2S)_{Q_1} = \{\frac{y}{s} : y \in P_2S,\ s \in S \setminus Q_1\} \trianglelefteq S_{Q_1}$. Wir behaupten: $(P_2S)_{Q_1} \cap R = P_2$.

Sicher ist $P_2 \subseteq (P_2S)_{Q_1} \cap R$. Sei umgekehrt $x \in (P_2S)_{Q_1} \cap R$; o.B.d.A. $x \neq 0$. Wir schreiben $x = \frac{y}{s}$ mit $y \in P_2S \subseteq \mathrm{rad}(P_2S)$ und $s \in S \setminus Q_1$. Nach Satz 13.6 ist y ganz über P_2. Nach Satz 13.7 hat das Minimalpolynom f von y über K die Form $f = X^n + u_{n-1}X^{n-1} + \cdots + u_1X + u_0$ mit $u_0, \ldots, u_{n-1} \in P_2$. Wir setzen $v_i := \frac{u_i}{x^{n-i}}$ für $i = 0, \ldots, n-1$. Wegen $s = \frac{y}{x}$ und $f(y) = 0$ ist dann $s^n + v_{n-1}s^{n-1} + \cdots + v_1s + v_0 = 0$. Offenbar ist $X^n + v_{n-1}X^{n-1} + \cdots + v_1X + v_0$ das Minimalpolynom von s über K. Da R normal ist, folgt aus Satz 13.7: $v_0, \ldots, v_{n-1} \in R$.

Im Fall $v_0, \ldots, v_{n-1} \in P_2$ wäre $s^n = -v_{n-1}s^{n-1} - \cdots - v_1s - v_0 \in P_2S \subseteq P_1S \subseteq Q_1$, und wir hätten den Widerspruch $s \in Q_1$.

Daher existiert ein $i \in \{0, \ldots, n-1\}$ mit $v_i \in R \setminus P_2$. Andererseits ist $x^{n-i}v_i = u_i \in P_2$, d.h. $x \in P_2$. Damit ist unsere Behauptung gezeigt.

Folglich ist $(P_2S)_{Q_1} \cap (R \setminus P_2) = \emptyset$. Nach Satz 4.4 existiert ein $Q_2' \in \mathrm{Spec}(S_{Q_1})$ mit $(P_2S)_{Q_1} \subseteq Q_2'$ und $Q_2' \cap (R \setminus P_2) = \emptyset$. Daher ist $Q_2 := Q_2' \cap S \in \mathrm{Spec}(S)$ mit $P_2 \subseteq (P_2S)_{Q_1} \cap R \subseteq Q_2' \cap R = Q_2 \cap R$ und $Q_2 \cap (R \setminus P_2) = \emptyset$, d.h. $Q_2 \cap R = P_2$. Ferner gilt: $Q_2 \subseteq Q_1$.

14. Reguläre lokale Ringe

Sei R ein Ring.

14.1 Bemerkung. Sei R lokal und noethersch, und sei $M := \mathrm{J}(R)$, d.h. $\mathrm{Max}(R) = \{M\}$. Dann ist M/M^2 ein Vektorraum über dem Körper $K := R/M$, und aus dem verallgemeinerten Hauptidealsatz folgt:

$$\mathrm{Dim}(R) = \mathrm{ht}(M) \leq \mu(M) = \dim_K(M/M^2) < \infty.$$

Man betrachtet manchmal den R/M-Vektorraum M/M^2 als Analogon des Tangentialraums aus der Differentialgeometrie.

Satz. *In der obigen Situation sei $c \in M \setminus M^2$. Dann ist $\overline{R} := R/Rc$ ein lokaler noetherscher Ring mit $\overline{M} := M/Rc = \mathrm{J}(\overline{R})$ und*

$$\dim_{R/M} M/M^2 = \dim_{\overline{R}/\overline{M}} \overline{M}/\overline{M}^2 + 1.$$

Beweis. Nach dem Homomorphiesatz ist $\overline{R}$ ein lokaler noetherscher Ring und $\overline{M} = \mathrm{J}(\overline{R})$. Sei $\overline{a}_1 + \overline{M}^2, \ldots, \overline{a}_n + \overline{M}^2$ eine $\overline{R}/\overline{M}$-Basis von $\overline{M}/\overline{M}^2$. Für $i = 1, \ldots, n$ sei $a_i \in M$ mit $\overline{a}_i = a_i + Rc$. Dann erzeugen $\overline{a}_1, \ldots, \overline{a}_n$ den $\overline{R}$-Modul $\overline{M}$, d.h.

$$M/Rc = \overline{M} = \overline{R}\overline{a}_1 + \cdots + \overline{R}\overline{a}_n = Ra_1 + \cdots + Ra_n + Rc/Rc.$$

Also ist $M = Ra_1 + \cdots + Ra_n + Rc$ und

$$M/M^2 = \sum_{i=1}^{n} Ra_i + Rc + M^2/M^2 = \sum_{i=1}^{n}(R/M)(a_i + M^2) + (R/M)(c + M^2).$$

Daher genügt zu zeigen, dass $a_1 + M^2, \ldots, a_n + M^2, c + M^2$ linear unabhängig über R/M sind. Dazu seien $r_1, \ldots, r_n, s \in R$ mit

$$0 = \sum_{i=1}^{n}(r_i + M)(a_i + M^2) + (s + M)(c + M^2) = \sum_{i=1}^{n} r_i a_i + sc + M^2,$$

d.h. $\sum_{i=1}^{n} r_i a_i + sc \in M^2$. Wir setzen $\overline{r}_i := r_i + Rc$ für $i = 1, \ldots, n$ und $\overline{s} := s + Rc$. Dann ist $\sum_{i=1}^{n} \overline{r}_i \overline{a}_i = \sum_{i=1}^{n} \overline{r}_i \overline{a}_i + \overline{sc} \in \overline{M}^2$, d.h. $\sum_{i=1}^{n}(\overline{r}_i + \overline{M})(\overline{a}_i + \overline{M}^2) = 0$. Da $\overline{a}_1, \ldots, \overline{a}_n$ linear unabhängig über $\overline{R}/\overline{M}$ sind, folgt für $i = 1, \ldots, n$: $\overline{r}_i + \overline{M} = 0$, d.h. $\overline{r}_i \in \overline{M}$, $r_i \in M$ und damit $r_i + M = 0$. Daher ist $sc + M^2 = 0$.

Im Fall $s \notin M$ wäre $s \in R^\times$, also auch $c + M^2 = 0$, und wir hätten den Widerspruch $c \in M^2$.

Dies zeigt: $s \in M$, d.h. $s + M = 0$.

14.2 Definition. Sei R lokal und noethersch, und sei $M := \mathrm{J}(R)$. Ist $\mathrm{Dim}(R) = \dim_{R/M} M/M^2$, so heißt R **regulär**.

Bemerkung. In der Algebraischen Geometrie beschreiben reguläre lokale Ringe reguläre Punkte. Diese stehen im Gegensatz zu singulären Punkten (Singularitäten).

Satz. *Sei R ein regulärer lokaler Ring und $M := \mathrm{J}(R)$. Für $c \in M \setminus M^2$ ist dann auch $\overline{R} := R/Rc$ ein regulärer lokaler Ring mit* $\mathrm{Dim}(\overline{R}) = \mathrm{Dim}(R) - 1$.

Beweis. Nach Voraussetzung ist $\mathrm{Dim}(R) = \dim_{R/M}(M/M^2) \geq 1$. Nach Satz 14.1 ist $\overline{R}$ lokal und noethersch mit $\overline{M} := M/Rc = \mathrm{J}(\overline{R})$ und

$$\dim_{\overline{R}/\overline{M}}(\overline{M}/\overline{M}^2) = \dim_{R/M}(M/M^2) - 1.$$

Aus Satz 12.3 und Satz 12.4 folgt also:

$$\begin{aligned}\dim_{\overline{R}/\overline{M}}(\overline{M}/\overline{M}^2) = \mu_{\overline{R}}(\overline{M}) \geq \mathrm{ht}(\overline{M}) \geq \mathrm{ht}(M) - 1 = \mathrm{Dim}(R) - 1 \\ = \dim_{R/M}(M/M^2) - 1 = \dim_{\overline{R}/\overline{M}}(\overline{M}/\overline{M}^2),\end{aligned}$$

d.h. $\mathrm{Dim}(\overline{R}) = \mathrm{ht}(\overline{M}) = \dim_{\overline{R}/\overline{M}}(\overline{M}/\overline{M}^2) = \mathrm{Dim}(R) - 1$; insbesondere ist $\overline{R}$ ein regulärer lokaler Ring.

14.3 Satz. *Sei R lokal und noethersch, aber kein Integritätsbereich, und sei $p \in R$ mit $P := Rp \in \mathrm{Spec}(R)$. Dann ist* $\mathrm{ht}(P) = 0$, *d.h. $P \in \mathrm{Min}(R)$.*

Beweis. Wir nehmen $\mathrm{ht}(P) > 0$ an. Dann existiert ein $Q \in \mathrm{Spec}(R)$ mit $Q \subset P = Rp$. Also ist $p \notin Q$. Für $a \in Q$ existiert dann ein $b \in R$ mit $a = bp$. Wegen $bp \in Q$ und $p \notin Q$

ist dann $b \in Q$, d.h. $a \in Qp$. Daher ist $Q = QP$, und aus Nakayamas Lemma folgt der Widerspruch $Q = 0$.

14.4 Satz. *Jeder reguläre lokale Ring R ist ein Integritätsbereich.*

Beweis. (Induktion nach $d := \mathrm{Dim}(R)$)

Sei $M := \mathrm{J}(R)$. Im Fall $d = 0$ ist $\mu(M) = 0$, d.h. $M = 0$. Daher ist R sogar ein Körper.

Sei also $0 < d = \dim_{R/M}(M/M^2)$, d.h. $M \supset M^2$, und sei $c \in M \setminus M^2$. Nach Satz 14.2 ist R/Rc ein regulärer lokaler Ring mit $\mathrm{Dim}(R/Rc) = d - 1$. Nach Induktion ist R/Rc ein Integritätsbereich, d.h. $Rc \in \mathrm{Spec}(R)$. Wir nehmen an, dass R kein Integritätsbereich ist. Nach Satz 14.3 ist dann $Rc \in \mathrm{Min}(R)$.

Da R noethersch ist, hat R nur endlich viele minimale Primideale $P_1, \ldots, P_s$. Das obige Argument zeigt: $M \setminus M^2 \subseteq P_1 \cup \ldots \cup P_s$, d.h. $M \subseteq M^2 \cup P_1 \cup \ldots \cup P_s$. Aus dem Primideal-Vermeidungssatz folgt also: $M \subseteq M^2$ (was nicht der Fall ist) oder $M \subseteq P_i$ für ein $i \in \{1, \ldots, s\}$. Damit haben wir den Widerspruch $d = \mathrm{Dim}(R) = \mathrm{ht}(M) \leq \mathrm{ht}(P_i) = 0$.

Bemerkung. (i) Wir werden später zeigen, dass für jeden regulären lokalen Ring R und jedes $P \in \mathrm{Spec}(R)$ auch R_P ein regulärer lokaler Ring ist.
(ii) Man kann auch zeigen, dass jeder reguläre lokale Ring faktoriell (und damit normal) ist.

Beispiel. (i) Sei R noethersch, und sei $P = (a_1, \ldots, a_n) \in \mathrm{Spec}(R)$ mit $\mathrm{ht}(P) = n$. Dann ist R_P ein lokaler noetherscher Ring mit $\mathrm{J}(R_P) = P_P = (\frac{a_1}{1}, \ldots, \frac{a_n}{1})$. Ferner ist $\mathrm{Dim}(R_P) = \mathrm{ht}(P_P) = \mathrm{ht}(P) = n$. Daher ist R_P ein regulärer lokaler Ring.
(ii) Sei R noethersch und faktoriell, und sei $p \in R$ ein Primelement. Dann ist $P = (p) \in \mathrm{Spec}(R)$ und $\mathrm{ht}(P) = 1$ (nach Beispiel 12.3). Wegen (i) ist

$$R_P = \{\frac{a}{b} : a, b \in R,\ b \not\equiv 0 \pmod{p}\}$$

ein regulärer lokaler Ring.
(iii) Für $p \in \mathbb{P}$ ist $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \not\equiv 0 \pmod{p}\}$ nach (ii) ein regulärer lokaler Ring.
(iv) Jeder Körper ist ein regulärer lokaler Ring der Krulldimension 0.

14.5 Bemerkung. Sei R lokal mit $M := \mathrm{J}(R)$. Für jeden endlich erzeugten R-Modul V kann man V/MV als Vektorraum über dem Körper $K := R/M$ auffassen (vgl. Beispiel 5.4). Dabei ist $s := \mu_R(V) = \dim_K V/MV < \infty$.

Satz. *In der obigen Situation existiert ein R-Epimorphismus $\phi : R^s \longrightarrow V$ mit* $\mathrm{Ker}(\phi) \subseteq M^s = M \cdot R^s$.

Beweis. Sei $v_1 + MV, \ldots, v_s + MV$ eine R/M-Basis von V/MV. Dann ist

$$\phi : R^s \longrightarrow V, \quad (r_1, \ldots, r_s) \longmapsto r_1 v_1 + \cdots + r_n v_n,$$

R-linear. Nach Nakayamas Lemma ist $\mathrm{Bld}(\phi) = Rv_1 + \cdots + Rv_s = V$. Sei $(r_1, \ldots, r_s) \in \mathrm{Ker}(\phi)$, d.h. $0 = r_1 v_1 + \cdots + r_s v_s$ und damit $0 = \sum_{i=1}^s r_i v_i + MV = \sum_{i=1}^s (r_i + M)(v_i + MV)$. Für $i = 1, \ldots, s$ ist also $r_i + M = 0$, d.h. $r_i \in M$. Dies zeigt: $\mathrm{Ker}(\phi) \subseteq M^s = M \cdot R^s$.

14.6 Bemerkung. Sei R ein regulärer lokaler Ring mit $M := \mathrm{J}(R)$ und $d := \mathrm{Dim}(R)$. Dann existiert eine (R/M)-Basis $a_1 + M^2, \ldots, a_d + M^2$ von M/M^2. Nach Satz 14.2 ist $\overline{R} := R/(a_1)$ ein regulärer lokaler Ring mit $\mathrm{J}(\overline{R}) = \overline{M} := M/(a_1)$ und $\mathrm{Dim}(\overline{R}) = d - 1$. Ferner bilden $\overline{a}_2 + \overline{M}^2, \ldots, \overline{a}_d + \overline{M}^2$ eine $(\overline{R}/\overline{M})$-Basis von $\overline{M}/\overline{M}^2$; dabei ist $\overline{a}_i := a_i + (a_1)$ für $i = 2, \ldots, d$. Induktiv folgt, dass $R/(a_1, \ldots, a_i)$ für $i = 0, \ldots, d$ ein regulärer lokaler Ring der Krulldimension $d - i$ ist. Insbesondere ist $R/(a_1, \ldots, a_i)$ ein Integritätsbereich, d.h. $(a_1, \ldots, a_i) \in \mathrm{Spec}(R)$. Wir erhalten so eine Kette

$$(0) \subset (a_1) \subset (a_1, a_2) \subset \ldots \subset (a_1, \ldots, a_d) = M$$

der Länge $d = \mathrm{Dim}(R)$ in $\mathrm{Spec}(R)$.

14.7 Satz. *Die folgenden Aussagen sind äquivalent:*
(1) R ist ein regulärer lokaler Ring der Krulldimension 1.
(2) R ist ein lokaler HIR, aber kein Körper.
(3) R ist noethersch und normal mit $\mathrm{Spec}(R) = \{0, M\}$ *und* $0 \neq M$.

Beweis. "(1) $\Longrightarrow$ (2)": Sei (1) erfüllt und $M := \mathrm{J}(R)$. Dann ist R ein Integritätsbereich, aber kein Körper, und $\mu(M) = \mu(M/M^2) = \mathrm{Dim}(R) = 1$. Also ist $M = Rp$ für ein $p \in R$.

Sei $0 \neq I \trianglelefteq R$. Nach Krulls Durchschnittssatz existiert ein $n \in \mathbb{N}$ mit $I \subseteq M^n = Rp^n$, aber $I \not\subseteq M^{n+1}$. Sei $a \in I \setminus M^{n+1}$, und sei $b \in R$ mit $a = bp^n$. Dann ist $b \notin Rp = M$, d.h. $b \in R^\times$. Daher ist $Rp^n = Ra \subseteq I$, d.h. $I = Rp^n$.

"(2) $\Longrightarrow$ (3)": Das ist klar.

"(3) $\Longrightarrow$ (1)": Sei (3) erfüllt. Dann ist R lokal mit $\mathrm{Dim}(R) = 1$. Nach Nakayamas Lemma ist $M \neq M^2$. Sei $x \in M \setminus M^2$. Im Fall $M = Rx$ ist R ein regulärer lokaler Ring. Sei also $M \neq Rx$. Dann ist $\mathrm{Ass}(M/Rx) \neq \emptyset$ nach Satz 9.6. Wegen $0 \neq x \in \mathrm{Ann}(M/Rx)$ folgt: $\mathrm{Ass}(M/Rx) = \{M\}$. Sei $y \in M$ mit $M = \mathrm{Ann}(y + Rx)$, d.h. $My \subseteq Rx$. Dann ist $0 \neq x \in \mathrm{Quot}(R) =: K$ und $Myx^{-1} \trianglelefteq R$. Im Fall $Myx^{-1} = R$ ist $M = Rxy^{-1}$, d.h. R ist ein regulärer lokaler Ring. Sei also $Myx^{-1} \subseteq M$. Dann folgt: $M(yx^{-1})^2 \subseteq Myx^{-1} \subseteq M$, usw. Daher gilt für $n \in \mathbb{N}$: $x(yx^{-1})^n \in R$, d.h. $(yx^{-1})^n \subseteq Rx^{-1}$. Folglich ist $R[yx^{-1}] \subseteq Rx^{-1}$; insbesondere ist $R[yx^{-1}]$ ein endlich erzeugter R-Modul. Folglich ist yx^{-1} ganz über R. Da R normal ist, folgt: $yx^{-1} \in R$, d.h. $y \in Rx$. Das ergibt den Widerspruch $y + Rx = 0$.

Definition. Ggf. heißt R **diskreter Bewertungsring** (DBR).

Bemerkung. Sei R ein DBR und $M := \mathrm{J}(R)$. Dann ist $M = (p)$ für ein Primelement $p \in R$, und p ist im Wesentlichen das einzige Primelement in R. Die Primfaktorzerlegung eines Elements $a \in R \setminus \{0\}$ hat also die Form $a = up^n$ mit $u \in R^\times$ und $n \in \mathbb{N}_0$. Daher kann man jedes Element $x \in \mathrm{Quot}(R) \setminus \{0\}$ in der Form $x = vp^k$ mit $v \in R^\times$ und $k \in \mathbb{Z}$ schreiben.

Beispiel. Ist R faktoriell und noethersch, so ist $R_{(p)}$ für jedes Primelement $p \in R$ nach Beispiel 14.4 ein DBR. Insbesondere ist $\mathbb{Z}_{(p)} := \{\frac{a}{b} : a, b \in \mathbb{Z}, b \not\equiv 0 \pmod{p}\}$ für $p \in \mathbb{P}$ ein DBR.

15. Die projektive Dimension

Sei R ein Ring.

15.1 Satz. *Für einen R-Modul W sind äquivalent:*

(1) W ist zu einem direkten Summanden eines freien R-Moduls F isomorph.

(2) Sind U, V R-Moduln und ist $g : U \longrightarrow V$ ein R-Epimorphismus, so existiert zu jedem $h \in \mathrm{Hom}_R(W, V)$ ein $H \in \mathrm{Hom}_R(W, U)$ mit $g \circ H = h$.

(3) Jede kurze exakte Folge $0 \longrightarrow U \xrightarrow{\alpha} V \xrightarrow{\beta} W \longrightarrow 0$ von R-Moduln und R-Homomorphismen zerfällt.

Beweis. (1) $\Longrightarrow$ (2): Sei F ein freier R-Modul mit Basis B, und sei $F = W \oplus W'$ mit Untermoduln W, W' und Projektoren p, p'. Seien ferner U, V, g, h wie in (2). Da g surjektiv ist, existiert zu jedem $b \in B$ ein $u_b \in U$ mit $g(u_b) = h(p(b))$. Dann ist $G : F \longrightarrow U$, $\sum_{b\in B} r_b b \longmapsto \sum_{b\in B} r_b u_b$, R-linear mit

$$g(G(\sum_{b\in B} r_b b)) = g(\sum_{b\in B} r_b u_b) = \sum_{b\in B} r_b g(u_b) = \sum_{b\in B} r_b h(p(b)) = h(p(\sum_{b\in B} r_b b))$$

für alle $\sum_{b\in B} r_b b \in F$. Daher ist die Einschränkung $H : W \longrightarrow U$ von G R-linear mit $g(H(w)) = g(G(w)) = h(p(w)) = h(w)$ für alle $w \in W$.

(2) $\Longrightarrow$ (3): Sei (2) erfüllt und $(*)$ $0 \longrightarrow U \xrightarrow{\alpha} V \xrightarrow{\beta} W \longrightarrow 0$ wie in (3). Dann existiert ein $H \in \mathrm{Hom}_R(W, V)$ mit $\beta \circ H = \mathrm{id}_W$. Daher zerfällt $(*)$.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt. Nach Satz 2.2 existieren ein freier R-Modul F und ein R-Epimorphismus $g : F \longrightarrow W$. Dann ist $0 \longrightarrow K := \mathrm{Ker}(g) \longrightarrow F \xrightarrow{g} W \longrightarrow 0$ eine kurze exakte Folge von R-Moduln und R-Homomorphismen. Daher existiert ein Untermodul $K' \subseteq F$ mit $F = K \oplus K'$. Also induziert g einen R-Isomorphismus $K' \longrightarrow W$.

Definition. Ggf. heißt W **projektiv**.

Bemerkung. (i) Ist W endlich erzeugt, so kann man F in (1) auch endlich erzeugt wählen (vgl. Satz 2.2).

(ii) Jeder freie R-Modul ist nach (1) projektiv; i.A. gilt die Umkehrung nicht.

(iii) Direkte Summanden von projektiven R-Moduln sind wieder projektiv.

(iv) Da Koprodukte von freien R-Moduln wieder frei sind, sind Koprodukte von projektiven R-Moduln wieder projektiv.

15.2 Satz. *Sei R lokal. Dann ist jeder endlich erzeugte projektive R-Modul V frei.*

Beweis. Sei $M := \mathrm{J}(R)$ und $n := \mu(V)$. Nach Satz 14.5 existiert dann ein R-Epimorphismus $g : R^n \longrightarrow V$ mit $K := \mathrm{Ker}(g) \subseteq M \cdot R^n$. Dann ist $0 \longrightarrow K \longrightarrow R^n \longrightarrow V \longrightarrow 0$ eine kurze exakte Folge von R-Moduln und R-Homomorphismen. Da V projektiv ist, zerfällt diese. Daher existiert ein Untermodul $L \subseteq R^n$ mit $R^n = K \oplus L$. Dann ist $M \cdot R^n = MK \oplus ML$, d.h. $K = MK$. Aus Nakayamas Lemma folgt also: $K = 0$. Daher ist $V \simeq R^n$ frei.

Bemerkung. Die Aussage gilt auch, falls V nicht endlich erzeugt ist, ist dann aber schwerer zu beweisen.

Beispiel. (i) Ist R ein HIR, so ist jeder endlich erzeugte projektive R-Modul V ebenfalls frei; denn jeder endlich erzeugte freie (und damit jeder projektive) R-Modul ist torsionsfrei, und jeder endlich erzeugte torsionsfreie R-Modul ist frei.

(ii) Quillen und Suslin haben 1976 gezeigt, dass auch für jeden Körper K endlich erzeugte projektive $K[X_1, \ldots, X_n]$-Moduln wieder frei sind (Serre's problem).

(iii) Andererseits kann man zeigen, dass jedes Ideal eines Ganzheitsrings R eines algebraischen Zahlkörpers K ein projektiver R-Modul ist. Dabei ist I genau dann frei, wenn I ein Hauptideal ist. Dies liefert also viele Beispiele für projektive Moduln, die nicht frei sind.

15.3 Satz. (Schanuels Lemma)
Seien $0 \longrightarrow U \xrightarrow{f} F \xrightarrow{g} V \longrightarrow 0$ *und* $0 \longrightarrow U' \xrightarrow{f'} F' \xrightarrow{g'} V \longrightarrow 0$ *kurze exakte Folgen von R-Moduln und R-Homomorphismen, wobei F, F' projektiv sind. Dann gilt:* $U \times F' \simeq U' \times F$.

Beweis. Da $h : F \times F' \longrightarrow V$, $(x, x') \longmapsto g(x) + g'(x')$, R-linear ist, ist

$$K := \mathrm{Ker}(h) = \{(x, x') \in F \times F' : g'(x') = -g(x)\} \subseteq F \times F'$$

ein Untermodul, und die Projektion $F \times F' \longrightarrow F$ liefert eine kurze exakte Folge

$$0 \longrightarrow U' \longrightarrow K \longrightarrow F \longrightarrow 0$$

von R-Moduln und R-Homomorphismen. Da F projektiv ist, zerfällt diese. Folglich gilt: $K \simeq U' \times F$. Analog ist $K \simeq U \times F'$.

Definition. Man nennt R-Moduln V, V' **projektiv äquivalent** ($V \sim_{\mathrm{p}} V'$), falls projektive R-Moduln F, F' mit $V \times F \simeq V' \times F'$ existieren.

Bemerkung. (i) Man zeigt leicht, dass $\sim_{\mathrm{p}}$ eine Äquivalenzrelation ist. Die Äquivalenzklasse von V bezeichnet man mit $[V]_{\mathrm{p}}$. Insbesondere besteht $[0]_{\mathrm{p}}$ genau aus den projektiven R-Moduln.

(ii) In Schanuels Lemma setzt man $\Omega V := [U]_{\mathrm{p}}$; das ist wohldefiniert.

(iii) Für R-Moduln $V.V'$ gilt dann: $V \sim_{\mathrm{p}} V' \Longrightarrow \Omega V = \Omega V'$. Daher kann man definieren: $\Omega[V]_{\mathrm{p}} := \Omega V$. Induktiv erhält man auch: $\Omega^2[V]_{\mathrm{p}}$, $\Omega^3[V]_{\mathrm{p}}$, ... Zusätzlich setzt man $\Omega^0[V]_{\mathrm{p}} := [V]_{\mathrm{p}}$.

(iv) Sei I eine nichtleere Indexmenge. Hat man für jedes $i \in I$ eine kurze exakte Folge $0 \longrightarrow U_i \longrightarrow F_i \longrightarrow V_i \longrightarrow 0$ von R-Moduln und R-Homomorphismen, wobei jedes F_i projektiv ist, so ist

$$0 \longrightarrow \coprod_{i \in I} U_i \longrightarrow \coprod_{i \in I} F_i \longrightarrow \coprod_{i \in I} V_i \longrightarrow 0$$

eine kurze exakte Folge von R-Moduln und R-Homomorphismen, wobei $\coprod_{i \in I} F_i$ projektiv ist. Daher gilt: $\Omega[\coprod_{i \in I} V_i]_{\mathrm{p}} = [\coprod_{i \in I} U_i]_{\mathrm{p}}$.

15.4 Definition. Die **projektive Dimension** eines R-Moduls V definiert man durch

$$\mathrm{pd}(V) := \mathrm{pd}_R(V) := \inf\{n \in \mathbb{N}_0 : \Omega^n[V]_{\mathrm{p}} = [0]_{\mathrm{p}}\}.$$

Beispiel. (i) $\mathrm{pd}(V) = 0 \Longleftrightarrow V$ projektiv.

(ii) $\mathrm{pd}(V) \leq 1 \Longleftrightarrow$ es gibt projektive R-Moduln F, F' mit $F' \subseteq F$ und $V \simeq F/F'$.

Bemerkung. (i) I.A. ist $\mathrm{pd}(V)$ ein Maß für die Abweichung von der Projektivität.

(ii) Oft ist $\mathrm{pd}(V) = \infty$.

(iii) Für jede nichtleere Familie $(V_i)_{i \in I}$ von R-Moduln V_i gilt:

$$\mathrm{pd}(\coprod_{i \in I} V_i) = \sup\{\mathrm{pd}(V_i) : i \in I\}.$$

Satz. *Für jede kurze exakte Folge* $0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$ *von R-Moduln und R-Homomorphismen gilt:*

(i) Sind zwei der Zahlen $\mathrm{pd}(U)$, $\mathrm{pd}(V)$, $\mathrm{pd}(W)$ *endlich, so auch die dritte.*

(ii) $\mathrm{pd}(U) < \mathrm{pd}(V) \Longrightarrow \mathrm{pd}(W) = \mathrm{pd}(V)$.

(iii) $\mathrm{pd}(U) > \mathrm{pd}(V) \Longrightarrow \mathrm{pd}(W) = \mathrm{pd}(U) + 1$.

(iv) $\mathrm{pd}(U) = \mathrm{pd}(V) \Longrightarrow \mathrm{pd}(W) \leq \mathrm{pd}(U) + 1$.

Beweis. (I) Wir betrachten zunächst den Fall, dass W projektiv ist. Dann zerfällt unsere kurze exakte Folge, d.h. $V \simeq U \times W$. Daher gilt: $\mathrm{pd}(U) = \mathrm{pd}(V)$. Die Aussagen (i)-(iv) sind also trivial.

(II) Jetzt betrachten wir den Fall, dass V projektiv ist, W aber nicht. Dann ist $\mathrm{pd}(V) = 0 < \mathrm{pd}(W)$ und $[U]_{\mathrm{p}} = \Omega W$. Wir müssen zeigen:

(i) $\mathrm{pd}(U) < \infty \Longleftrightarrow \mathrm{pd}(W) < \infty$.

(iii) $\mathrm{pd}(U) > 0 \Longrightarrow \mathrm{pd}(W) = \mathrm{pd}(U) + 1$.

(iv) U projektiv $\Longrightarrow \mathrm{pd}(W) \leq 1$.

Diese Aussagen sind wieder trivial.

(III) Schließlich betrachten wir den Fall, dass weder V noch W projektiv ist. Wegen $U \simeq \mathrm{Bld}(f) \subseteq V$ und $W \simeq V/\mathrm{Ker}(g) = V/\mathrm{Bld}(f)$ können wir annehmen, dass $U \subseteq V$ ein Untermodul und $W = V/U$ ist. Ferner können wir annehmen, dass $V = F/G$ für einen Untermodul G eines freien R-Moduls F ist. Dann ist $U = H/G$ für einen Untermodul $H \subseteq F$ mit $G \subseteq H$, und $W = V/U = (F/G)/(H/G) \simeq F/H$. Ferner haben wir eine kurze exakte Folge

$$0 \longrightarrow G \longrightarrow H \longrightarrow U \longrightarrow 0$$

von R-Moduln und R-Homomorphismen mit $\mathrm{pd}(V) = \mathrm{pd}(G) + 1$ und $\mathrm{pd}(W) = \mathrm{pd}(H) + 1$.

Zum Beweis von (i) argumentieren wir mit Induktion nach der Summe s der beiden endlichen projektiven Dimensionen. Im Fall $s = 0$ sind zwei der Moduln U, V, W projektiv. Also ist V oder W projektiv, und wir haben einen Widerspruch.

Sei also $s > 0$. Dann sind auch zwei der Zahlen $\mathrm{pd}(G)$, $\mathrm{pd}(H)$, $\mathrm{pd}(U)$ endlich, und die Summe dieser beiden Zahlen ist kleiner als s. Nach Induktion sind daher $\mathrm{pd}(G)$, $\mathrm{pd}(H)$ und $\mathrm{pd}(U)$ endlich. Damit folgt (i).

Für den Rest des Beweises können wir annehmen, dass $\mathrm{pd}(U)$, $\mathrm{pd}(V)$ und $\mathrm{pd}(W)$ endlich sind. Wir argumentieren dann mit Induktion nach $s := \mathrm{pd}(U) + \mathrm{pd}(V) + \mathrm{pd}(W)$. Die Fälle $s \in \{0, 1\}$ werden durch (I) und (II) erledigt. Sei also $s > 1$. Aus der Induktionsvoraussetzung folgt dann:

(ii') Ist $\mathrm{pd}(G) < \mathrm{pd}(H)$, also auch $\mathrm{pd}(V) < \mathrm{pd}(W)$, so ist

$$\mathrm{pd}(U) = \mathrm{pd}(H) = \mathrm{pd}(W) - 1 \geq \mathrm{pd}(V).$$

(iii') Ist $\mathrm{pd}(G) > \mathrm{pd}(H)$, also auch $\mathrm{pd}(V) > \mathrm{pd}(W)$, so ist

$$\mathrm{pd}(U) = \mathrm{pd}(G) + 1 = \mathrm{pd}(V).$$

(iv') Ist $\mathrm{pd}(G) = \mathrm{pd}(H)$, also auch $\mathrm{pd}(V) = \mathrm{pd}(W)$, so ist

$$\mathrm{pd}(U) \leq \mathrm{pd}(G) + 1 = \mathrm{pd}(V).$$

Zum Beweis von (ii) sei jetzt $\mathrm{pd}(U) < \mathrm{pd}(V)$. Dann muss Fall (iv') vorliegen. Insbesondere ist $\mathrm{pd}(W) = \mathrm{pd}(V)$.

Zum Beweis von (iii) sei $\mathrm{pd}(U) > \mathrm{pd}(V)$. Dann muss Fall (ii') vorliegen. Insbesondere ist $\mathrm{pd}(W) = \mathrm{pd}(U) + 1$.

Zum Beweis von (iv) sei schließlich $\mathrm{pd}(U) = \mathrm{pd}(V)$. Wir wollen zeigen: $\mathrm{pd}(W) \leq \mathrm{pd}(U) + 1$. Im Fall (ii') ist sogar $\mathrm{pd}(W) = \mathrm{pd}(U) + 1$. Im Fall (iii') ist sogar $\mathrm{pd}(W) < \mathrm{pd}(V) = \mathrm{pd}(U)$. Im Fall (iv') ist sogar $\mathrm{pd}(W) = \mathrm{pd}(V) = \mathrm{pd}(U)$.

15.5 Satz. *Sei $x \in R \setminus \mathrm{Z}(R)$ und $\overline{R} := R/Rx$. Für jeden $\overline{R}$-Modul $V \neq 0$ mit $n := \mathrm{pd}_{\overline{R}}(V) < \infty$ gilt dann:* $\mathrm{pd}_R(V) = n + 1$.

Beweis. (Induktion nach n)
O.B.d.A. sei $\overline{R} \neq 0$. Dann ist $0 \longrightarrow R \simeq Rx \longrightarrow R \longrightarrow \overline{R} \longrightarrow 0$ eine kurze exakte Folge von R-Moduln und R-Homomorphismen; insbesondere ist $\Omega_R \overline{R} = [Rx]_{\mathrm{p}} = [R]_{\mathrm{p}} = [0]_{\mathrm{p}}$, d.h. $\mathrm{pd}_R(\overline{R}) \leq 1$.

Im Fall $\mathrm{pd}_R(\overline{R}) = 0$ wäre $\overline{R}$ ein projektiver R-Modul, d.h. unsere kurze exakte Folge würde zerfallen. Also gäbe es ein Ideal $I \trianglelefteq R$ mit $R = Rx \oplus I$. Dann wäre aber $Ix \subseteq I \cap Rx = 0$, d.h. $I = 0$ wegen $x \notin \mathrm{Z}(R)$. Also wäre $R = Rx$, und wir hätten den Widerspruch $\overline{R} = 0$.

Also ist $\mathrm{pd}_R(\overline{R}) = 1$. Ferner existiert ein Untermodul U eines freien $\overline{R}$-Moduls $\overline{F}$ mit $V \simeq \overline{F}/U$. Wegen $\overline{F} \neq 0$ ist dann $\mathrm{pd}_R(\overline{F}) = 1$, und wir haben eine kurze exakte Folge $(*)$ $\quad 0 \longrightarrow U \longrightarrow \overline{F} \longrightarrow V \longrightarrow 0$ von $\overline{R}$-Moduln und $\overline{R}$-Homomorphismen.

Im Fall $n = 0$ ist V projektiv, d.h. $(*)$ zerfällt. Insbesondere ist $\mathrm{pd}_R(V) \leq \mathrm{pd}_R(\overline{F}) = 1$.

Wäre $\mathrm{pd}_R(V) = 0$, so wäre V ein projektiver R-Modul, d.h. zu einem direkten Summanden eines freien R-Moduls F isomorph. Wegen $xV = 0$ gäbe es dann ein $f \in F \setminus \{0\}$ mit $xf = 0$. Wir hätten also einen Widerspruch.

Also ist $\mathrm{pd}_R(V) = 1 = n + 1$.

Jetzt sei $n \geq 1$. Wegen $\Omega_{\overline{R}} V = [U]_{\mathrm{p}}$ ist $\mathrm{pd}_{\overline{R}}(U) = n - 1$. Wegen $U \neq 0$ folgt aus der Induktionsvoraussetzung: $\mathrm{pd}_R(U) = n$.

Im Fall $n \geq 2$ ist also $\mathrm{pd}_R(U) = n > 1 = \mathrm{pd}_R(\overline{F})$. Aus Satz 15.4 folgt daher: $\mathrm{pd}_R(V) = \mathrm{pd}_R(U) + 1 = n + 1$.

Sei also $n = 1$, d.h. $\mathrm{pd}_R(U) = \mathrm{pd}_R(\overline{F})$. Aus Satz 15.4 folgt dann: $\mathrm{pd}_R(V) \leq 2$. Wir nehmen an: $\mathrm{pd}_R(V) \leq 1$. Sei T ein Untermodul eines freien R-Moduls F mit $F/T \simeq V$.

Wegen $xV = 0$ ist $xF \subseteq T$. Die kurze exakte Folge $0 \longrightarrow T \longrightarrow F \longrightarrow V \longrightarrow 0$ von R-Moduln und R-Homomorphismen induziert also eine kurze exakte Folge

$$0 \longrightarrow T/xF \longrightarrow F/xF \longrightarrow V \longrightarrow 0$$

von $\overline{R}$-Moduln und $\overline{R}$-Homomorphismen. Dabei ist F/xF ein freier $\overline{R}$-Modul. Daher ist $\mathrm{pd}_{\overline{R}}(T/xF) \leq \mathrm{pd}_{\overline{R}}(V) - 1 = 0$, d.h. der $\overline{R}$-Modul T/xF ist projektiv. Daher zerfällt die kurze exakte Folge $0 \longrightarrow xF/xT \longrightarrow T/xT \longrightarrow T/xF \longrightarrow 0$ von $\overline{R}$-Moduln und $\overline{R}$-Homomorphismen. Daher ist $V \simeq F/T \simeq xF/xT$ zu einem direkten Summanden von T/xT isomorph, also ein projektiver $\overline{R}$-Modul. Wegen $\mathrm{pd}_{\overline{R}}(V) = n = 1$ ist das ein Widerspruch.

15.6 Satz. *Sei $x \in R \setminus \mathrm{Z}(R)$ und $\overline{R} := R/Rx$. Für jeden R-Modul V mit $\{v \in V : xv = 0\} = 0$ gilt dann:* $\mathrm{pd}_{\overline{R}}(V/xV) \leq \mathrm{pd}_R(V)$.

Beweis. O.B.d.A. sei $n := \mathrm{pd}_R(V) < \infty$. Wir argumentieren mit Induktion nach n.

Im Fall $n = 0$ ist V ein projektiver R-Modul. Daher ist V/xV ein projektiver $\overline{R}$-Modul, d.h. $\mathrm{pd}_{\overline{R}}(V/xV) = 0 = \mathrm{pd}_R(V)$.

Sei also $n > 0$. Dann existiert ein Untermodul U eines freien R-Moduls F mit $F/U \simeq V$. Daher haben wir eine kurze exakte Folge von R-Moduln und R-Homomorphismen

$$0 \longrightarrow U \longrightarrow F \xrightarrow{f} V \longrightarrow 0$$

mit $\mathrm{pd}_R(U) = n-1$ und $\{u \in U : xu = 0\} = 0$. Nach Induktion ist also $\mathrm{pd}_{\overline{R}}(U/xU) \leq n-1$. Ferner gilt:

$$V/xV \simeq (F/U)/x(F/U) = (F/U)/(xF + U/U) \simeq F/xF + U \simeq (F/xF)/(U + xF/xF).$$

Wir haben also eine kurze exakte Folge von $\overline{R}$-Moduln und $\overline{R}$-Homomorphismen

$$0 \longrightarrow U + xF/xF \longrightarrow F/xF \longrightarrow V/xV \longrightarrow 0.$$

Sicher ist $xU \subseteq U \cap xF$. Sei umgekehrt $u \in U \cap xF$, d.h. $u = xy$ für ein $y \in F$. Dann ist $0 = f(u) = f(xy) = xf(y)$ mit $f(y) \in V$, d.h. $f(y) = 0$ nach Voraussetzung. Also ist $y \in U$ und damit $u \in xU$.

Dies zeigt: $U \cap xF = xU$. Folglich ist $U + xF/xF \simeq U/U \cap xF \simeq U/xU$. Wir haben also eine kurze exakte Folge $0 \longrightarrow U/xU \longrightarrow F/xF \longrightarrow V/xV \longrightarrow 0$ von $\overline{R}$-Moduln und $\overline{R}$-Homomorphismen, wobei F/xF frei ist. Daher ist $\mathrm{pd}_{\overline{R}}(V/xV) \leq \mathrm{pd}_{\overline{R}}(U/xU) + 1 \leq n$.

15.7 Satz. *Seien R noethersch, $x \in \mathrm{J}(R) \setminus \mathrm{Z}(R)$ und $\overline{R} := R/Rx$. Dann gilt für jeden endlich erzeugten R-Modul V mit $\{v \in V : xv = 0\} = 0$:* $\mathrm{pd}_{\overline{R}}(V/xV) = \mathrm{pd}_R(V)$.

Beweis. Im Fall $n := \mathrm{pd}_{\overline{R}}(V/xV) = \infty$ folgt die Behauptung aus Satz 15.6. Sei also $n < \infty$. Wir argumentieren mit Induktion nach n. Sicher existiert ein (endlich erzeugter) Untermodul U eines endlich erzeugten freien R-Moduls F mit $F/U \simeq V$. Wie oben ist

$V/xV \simeq \ldots \simeq (F/xF)/(U + xF/xF)$ und $U + xF/xF \simeq U/U \cap xF = U/xU$. Wir haben also wieder eine kurze exakte Folge

$$\mathcal{F} : 0 \longrightarrow U/xU \longrightarrow F/xF \longrightarrow V/xV \longrightarrow 0$$

von $\overline{R}$-Moduln und $\overline{R}$-Homomorphismen, wobei F/xF frei ist.

Zunächst sei $n = 0$, d.h. V/xV ist ein projektiver $\overline{R}$-Modul. Wir müssen zeigen: V ist ein projektiver R-Modul.

Zum Beweis sei zuerst V/xV ein freier $\overline{R}$-Modul. Wir werden zeigen, dass dann V ein freier R-Modul ist. Dazu sei $u_1 + xV, \ldots, u_t + xV$ eine $\overline{R}$-Basis von V/xV. Dann ist

$$V/xV = \overline{R}(u_1 + xV) + \cdots + \overline{R}(u_t + xV) = Ru_1 + \cdots + Ru_t + xV/xV,$$

d.h. $V = Ru_1 + \cdots + Ru_t + xV$ und damit $V/Ru_1 + \cdots + Ru_t = x(V/Ru_1 + \cdots + Ru_t)$. Wegen $x \in \mathrm{J}(R)$ folgt mit Nakayamas Lemma: $V/Ru_1 + \cdots + Ru_t = 0$, d.h. $V = Ru_1 + \cdots + Ru_t$.

Seien jetzt $a_1, \ldots, a_t \in R$ mit $a_1u_1 + \cdots + a_tu_t = 0$. Dann gilt auch:

$$(a_1 + Rx)(u_1 + xV) + \cdots + (a_t + Rx)(u_t + xV) = 0.$$

Für $i = 1, \ldots, t$ ist also $a_i + Rx = 0$, d.h. $a_i \in Rx$. Daher existiert ein $b_i \in R$ mit $a_i = b_ix$. Also ist $0 = x(b_1u_1 + \cdots + b_tu_t)$. Nach Voraussetzung folgt: $0 = b_1u_1 + \cdots + b_tu_t$. Dieses Argument kann man mit $b_1, \ldots, b_t$ statt $a_1, \ldots, a_t$ wiederholen. So erhält man: $a_i = xb_i = x^2c_i = \ldots$. Daher ist $a_i \in \bigcap_{j=1}^{\infty} \mathrm{J}(R)^j = 0$ nach Krulls Durchschnittssatz. Dies zeigt, dass $u_1, \ldots, u_t$ eine R-Basis von V bilden. Also ist V in der Tat ein freier R-Modul.

Damit ist der Fall erledigt, dass V/xV ein freier $\overline{R}$-Modul ist.

Jetzt betrachten wir den Fall, dass V/xV ein projektiver $\overline{R}$-Modul ist. Dann zerfällt $\mathcal{F}$. Für den endlich erzeugten R-Modul $W := U \times V$ gilt also: $\{w \in W : xw = 0\} = 0$ und

$$W/xW \simeq (U \times V)/x(U \times V) = (U \times V)/(xU \times xV) \simeq U/xU \times V/xV \simeq F/xF.$$

Da wir den "freien" Fall schon erledigt haben, folgt: W ist ein freier R-Modul. Daher ist V ein projektiver R-Modul. Damit ist der Fall $n = 0$ geschafft.

Sei also jetzt $n > 0$. Dann ist $\mathrm{pd}_{\overline{R}}(U/xU) = \mathrm{pd}_{\overline{R}}(V/xV) - 1 = n - 1$. Nach Induktion ist daher $\mathrm{pd}_R(U) = n - 1$; denn U erfüllt die Voraussetzungen des Satzes. Wir haben jetzt die kurze exakte Folge von R-Moduln und R-Homomorphismen $0 \longrightarrow U \longrightarrow F \longrightarrow V \longrightarrow 0$.

Im Fall $n \neq 1$ folgt: $\mathrm{pd}_R(V) = n$, wie gewünscht.

Sei also $n = 1$. Dann ist U ein projektiver R-Modul. Folglich ist $\mathrm{pd}_R(V) \leq 1$. Im Fall $\mathrm{pd}_R(V) = 0$ wäre V projektiv. Dann wäre aber V/xV ein projektiver $\overline{R}$-Modul, und wir hätten einen Widerspruch.

Also ist $\mathrm{pd}_R(V) = 1 = n$, und die Behauptung ist bewiesen.

16. Die globale Dimension

Sei R ein Ring.

16.1 Definition. Man nennt $\mathrm{gld}(R) := \sup\{\mathrm{pd}(V) : V \text{ endlich erzeugter } R\text{−Modul}\}$ die **globale Dimension** von R.

Bemerkung. (i) Man kann zeigen: $\mathrm{gld}(R) = \sup\{\mathrm{pd}(V) : V \text{ beliebiger } R\text{−Modul}\}$. Dazu bleibt hier aber keine Zeit.

(ii) Oft ist $\mathrm{gld}(R) = \infty$.

Beispiel. Für jeden Körper K ist $\mathrm{gld}(K) = 0$. Außerdem ist $\mathrm{gld}(\mathbb{Z}) = 1$.

Satz. *Sei* $x \in R\backslash \mathrm{Z}(R)$ *mit* $\overline{R} := R/Rx \neq 0$ *und* $n := \mathrm{gld}(\overline{R}) < \infty$. *Dann ist* $\mathrm{gld}(R) \geq n+1$.

Beweis. Wegen $\overline{R} \neq 0$ existiert ein endlich erzeugter $\overline{R}$-Modul $V \neq 0$ mit $\mathrm{pd}_{\overline{R}}(V) = n$. Wegen Satz 15.5 ist also $n + 1 = \mathrm{pd}_R(V) \leq \mathrm{gld}(R)$.

16.2 Satz. *Sei* R *noethersch, und sei* $x \in \mathrm{J}(R) \setminus \mathrm{Z}(R)$ *mit* $\overline{R} := R/Rx \neq 0$ *und* $n := \mathrm{gld}(\overline{R}) < \infty$. *Dann ist* $\mathrm{gld}(R) = n + 1$.

Beweis. Nach Satz 16.1 ist $\mathrm{gld}(R) \geq n + 1$. Zum Beweis von $\mathrm{gld}(R) \leq n + 1$ sei V ein endlich erzeugter R-Modul. Wir müssen zeigen: $k := \mathrm{pd}_R(V) \leq n + 1$. Dabei können wir $k > 0$ annehmen. Sicher existiert ein Untermodul U eines endlich erzeugten freien R-Moduls $F \neq 0$ mit $F/U \simeq V$. Dabei ist U endlich erzeugt mit $\{u \in U : xu = 0\} = 0$ und $\mathrm{pd}_R(U) = k - 1$. Aus Satz 15.7 folgt also: $k - 1 = \mathrm{pd}_R(U) = \mathrm{pd}_{\overline{R}}(U/xU) \leq \mathrm{gld}(\overline{R}) = n$, d.h. $k \leq n + 1$.

16.3 Satz. *Sei* R *noethersch und* $A \subseteq R$ *eine multiplikative Teilmenge. Dann ist* $\mathrm{gld}(A^{-1}R) \leq \mathrm{gld}(R)$.

Beweis. Sei V ein endlich erzeugter $A^{-1}R$-Modul. Dann existieren $v_1, \ldots, v_t \in V$ mit $V = A^{-1}Rv_1 + \cdots + A^{-1}Rv_t$. Wir können V auch als R-Modul ansehen. Dann ist $U := Rv_1 + \cdots + Rv_t$ ein endlich erzeugter R-Untermodul von V. Nach Satz 8.1 und Bemerkung 8.3 induziert die Inklusionsabbildung $U \longrightarrow V$ ein $f \in \mathrm{Hom}_{A^{-1}R}(A^{-1}U, V)$ mit $f(\frac{u}{1}) = u$ für $u \in U$.

Für $i = 1, \ldots, t$ ist $v_i = f(\frac{v_i}{1}) \in \mathrm{Bld}(f)$, d.h. f ist surjektiv. Sind $a \in A$ und $u \in U$ mit $0 = f(\frac{u}{a}) = \frac{1}{a}f(\frac{u}{1}) = \frac{1}{a}u$, so ist auch $0 = \frac{a}{1}(\frac{1}{a}u) = u$. Dies zeigt, dass f bijektiv ist. Also ist $A^{-1}U \simeq_{A^{-1}R} V$.

Jetzt genügt zu zeigen: $\mathrm{pd}_{A^{-1}R}(A^{-1}U) \leq \mathrm{pd}_R(U) =: k$. Zum Beweis schreiben wir $U \simeq F/W$ mit einem Untermodul W eines endlich erzeugten freien R-Moduls F. Nach Bemerkung 8.8 ist $A^{-1}F$ ein endlich erzeugter freier $A^{-1}R$-Modul. Ferner ist $A^{-1}W$ ein $A^{-1}R$-Untermodul von $A^{-1}F$ mit $A^{-1}F/A^{-1}W \simeq A^{-1}(F/W) \simeq A^{-1}U$.

Wir argumentieren jetzt mit Induktion nach k. Im Fall $k = 0$ ist U projektiv. Daher zerfällt die kurze exakte Folge $0 \longrightarrow W \longrightarrow F \longrightarrow U \longrightarrow 0$ von R-Moduln und R-Homomorphismen; insbesondere ist $F \simeq U \times W$. Daher gilt auch: $A^{-1}F \simeq (A^{-1}U) \times (A^{-1}W)$. Also ist $A^{-1}U$ ein projektiver $A^{-1}R$-Modul, d.h. $\mathrm{pd}_{A^{-1}R}(A^{-1}U) = 0 = k$.

Sei schließlich $k > 0$, d.h. $\mathrm{pd}_R(W) = k - 1$. Da W endlich erzeugt ist, gilt nach Induktion: $\mathrm{pd}_{A^{-1}R}(A^{-1}W) \leq \mathrm{pd}_R(W) = k - 1$, d.h. $\mathrm{pd}_{A^{-1}R}(A^{-1}U) \leq \mathrm{pd}_{A^{-1}R}(A^{-1}W) + 1 \leq k$.

16.4 Satz. *Sei* R *noethersch und lokal mit* $M := \mathrm{J}(R)$ *und* $M \setminus M^2 \subseteq \mathrm{Z}(R)$. *Dann gilt:*

(i) Es existiert ein $a \in R \setminus \{0\}$ mit $aM = 0$.
(ii) Für jeden endlich erzeugten R-Modul V gilt: $\mathrm{pd}(V) \in \{0, \infty\}$.

Beweis. (i) Nach Satz 9.9 ist $\mathrm{Ass}(R)$ endlich, etwa $\mathrm{Ass}(R) = \{P_1, \ldots, P_t\}$. Nach Bemerkung 9.6 ist also $P_1 \cup \ldots \cup P_t = \{r \in R : \exists s \in R : rs = 0 \neq s\} = \mathrm{Z}(R) \supseteq M \setminus M^2$, d.h. $M \subseteq M^2 \cup P_1 \cup \ldots \cup P_t$. O.B.d.A. sei $M \neq 0$; sonst setzt man $a := 1$. Wegen $M \not\subseteq M^2$ folgt also aus dem Primidealvermeidungssatz: $M \subseteq P_j$ für ein $j \in \{1, \ldots, t\}$. Ferner existiert ein $s_j \in R$ mit $P_j = \mathrm{Ann}(s_j)$. Daher ist $s_j \neq 0$ und $Ms_j = 0$.

(ii) Wir nehmen das Gegenteil an. Dann existiert ein endlich erzeugter R-Modul V mit $\mathrm{pd}(V) = 1$. Nach Satz 14.5 existiert ein R-Epimorphismus $\phi : R^s \longrightarrow V$ mit $s := \mu(V)$ und $U := \mathrm{Ker}(\phi) \subseteq M \cdot R^s$. Nach (i) existiert ein $a \in R \setminus \{0\}$ mit $aM = 0$, also auch $aU = 0$. Da $0 \longrightarrow U \longrightarrow R^s \xrightarrow{\phi} V \longrightarrow 0$ eine kurze exakte Folge von R-Moduln und R-Homomorphismen ist, ist $\mathrm{pd}(U) = 0$. Daher ist U ein projektiver R-Modul, also sogar frei. Wegen $aU = 0$ folgt: $U = 0$. Daher ist $V \simeq R^s$, und wir haben den Widerspruch $\mathrm{pd}(V) = 0$.

16.5 Satz. *Sei R ein regulärer lokaler Ring. Dann ist* $\mathrm{gld}(R) = \mathrm{Dim}(R) < \infty$.

Beweis. Sei $M := \mathrm{J}(R)$. Im Fall $M = M^2$ ist $M = 0$ nach Nakayamas Lemma, d.h. R ist ein Körper. Also ist $\mathrm{Dim}(R) = 0$ und $\mathrm{gld}(R) = 0$.

Sei also $M \neq M^2$ und $x \in M \setminus M^2$. Da R ein Integritätsbereich ist, ist $x \notin \mathrm{Z}(R)$. Nach Satz 14.2 ist $\overline{R} := R/Rx$ ein regulärer lokaler Ring mit $\mathrm{Dim}(\overline{R}) = \mathrm{Dim}(R) - 1$. Induktiv können wir annehmen: $\mathrm{gld}(\overline{R}) = \mathrm{Dim}(\overline{R}) < \infty$. Aus Satz 16.2 folgt also: $\mathrm{gld}(R) = \mathrm{gld}(\overline{R}) + 1 = \mathrm{Dim}(\overline{R}) + 1 = \mathrm{Dim}(R)$.

16.6 Satz. *Sei R noethersch und lokal, aber kein Körper. Sei außerdem $M := \mathrm{J}(R)$ und $n := \mathrm{pd}(M) < \infty$. Dann ist R ein regulärer lokaler Ring und* $\mathrm{Dim}(R) = n + 1$.

Beweis. (I) Zunächst sei $n = 0$, d.h. M ist projektiv. Nach Satz 15.2 ist dann M sogar frei. Sei $b_1, \ldots, b_t$ eine R-Basis von M, d.h. $M = Rb_1 \oplus \cdots \oplus Rb_t$. Für $i = 2, \ldots, t$ ist dann $b_i b_1 \in Rb_i \cap Rb_1 = 0$, d.h. $b_i b_1 = 0$. Da b_1 linear unabhängig ist, folgt: $b_i = 0$. Dies zeigt: $t = 1$, d.h. $M = Rb_1$. Ferner ist $b_1 \notin \mathrm{Z}(R)$. Nach Satz 12.2 ist also $\mathrm{Dim}(R) = \mathrm{ht}(M) = 1 = \dim_{R/M}(M/M^2)$; insbesondere ist R ein regulärer lokaler Ring.

(II) Jetzt sei $M \setminus M^2 \subseteq \mathrm{Z}(R)$. Nach Satz 16.4 ist dann $n = 0$, und wir sind wieder im Fall (I).

(III) Im allgemeinen Fall argumentieren wir mit Induktion nach $k := \mathrm{Dim}(R)$. Im Fall $k = 0$ ist R artinsch, d.h. $M = \mathrm{J}(R)$ ist nilpotent. Insbesondere ist $M \subseteq \mathrm{Z}(R)$, und wir sind in Fall (II).

Sei also $k > 0$. Wegen (II) sei o.B.d.A. $M \setminus M^2 \not\subseteq \mathrm{Z}(R)$. Sei $x \in M \setminus M^2$ mit $x \notin \mathrm{Z}(R)$. Dann ist $\overline{R} := R/Rx$ noethersch und lokal mit $\overline{M} := M/Rx = \mathrm{J}(\overline{R})$. Nach Satz 12.2 gilt für jedes minimale $P \in \mathcal{V}(Rx)$: $\mathrm{ht}(P) = 1$. Daher ist $\mathrm{Dim}(\overline{R}) \leq \mathrm{Dim}(R) - 1$.

Wir behaupten, dass $\overline{M}$ zu einem direkten Summanden von M/Mx isomorph ist. Zum Beweis wählen wir eine R/M-Basis $x + M^2, y_1 + M^2, \ldots, y_r + M^2$ von M/M^2. Nach Nakayamas Lemma ist dann $M = Rx + S$ mit $S := Mx + Ry_1 + \cdots + Ry_r$. Ferner ist $Mx \subseteq Rx \cap S$. Sei umgekehrt $z \in Rx \cap S$. Dann existieren $a, b_1, \ldots, b_r \in R$ und $c \in M$

mit $z = ax = cx + b_1y_1 + \cdots + b_ry_r$. Also ist $ax - b_1y_1 - \cdots - b_ry_r = cx \in M^2$, d.h.

$$0 = (a + M)(x + M^2) - (b_1 + M)(y_1 + M^2) - \cdots - (b_r + M)(y_r + M^2) \in M/M^2.$$

Nach Wahl von $x, y_1, \ldots, y_r$ folgt $a + M = 0$. Also ist $a \in M$ und damit $z \in Mx$. Damit ist gezeigt: $M = Rx + S$ und $Rx \cap S = Mx$, d.h. $M/Mx = (Rx/Mx) \oplus (S/Mx)$ mit $S/Mx \simeq (M/Mx)/(Rx/Mx) \simeq M/Rx = \overline{M}$. Damit ist unsere Behauptung bewiesen.

Aus Satz 15.7 folgt also: $\mathrm{pd}_{\overline{R}}(\overline{M}) \leq \mathrm{pd}_{\overline{R}}(M/Mx) = \mathrm{pd}_R(M) = n < \infty$. Wir haben die kurze exakte Folge $0 \longrightarrow Rx \longrightarrow M \longrightarrow \overline{M} \longrightarrow 0$ von R-Moduln und R-Homomorphismen; dabei ist $Rx \simeq R$ projektiv, M aber o.B.d.A. nicht (wegen (I)). Aus Satz 15.4 (ii) folgt: $\mathrm{pd}_R(\overline{M}) = \mathrm{pd}_R(M) = n$. Nach Satz 15.5 ist also $\mathrm{pd}_{\overline{R}}(\overline{M}) = n - 1$.

Wäre $\overline{R}$ ein Körper, so wäre $M = Rx \simeq R$, d.h. M wäre doch projektiv, und wir wären in Fall (I).

Daher ist $\overline{R}$ kein Körper. Dann folgt aus der Induktionsvoraussetzung, dass $\overline{R}$ ein regulärer lokaler Ring und $\mathrm{Dim}(\overline{R}) = n$ ist. Nach Bemerkung 14.6 ist also $\mathrm{Dim}(\overline{R}) = \dim_{\overline{R}/\overline{M}}(\overline{M}/\overline{M}^2) = \dim_{R/M}(M/M^2) - 1$. Also gilt:

$$\mathrm{Dim}(R) \geq \mathrm{Dim}(\overline{R}) + 1 = \mu_R(M) \geq \mathrm{ht}(M) = \mathrm{Dim}(R),$$

d.h. R ist ein regulärer lokaler Ring mit $\mathrm{Dim}(R) = n + 1$.

16.7 Satz. (Auslander-Buchsbaum 1957)
Sei R noethersch und lokal mit $M := \mathrm{J}(R)$. Dann sind äquivalent:
(1) R ist ein regulärer lokaler Ring.
(2) $\mathrm{gld}(R) < \infty$.
(3) $\mathrm{pd}_R(R/M) < \infty$.
Ggf. ist $\mathrm{pd}_R(R/M) = \mathrm{gld}(R) = \mathrm{Dim}(R) = \dim_{R/M}(M/M^2)$.

Beweis. (1) $\Longrightarrow$ (2): Satz 16.5.
(2) $\Longrightarrow$ (3): Trivial.
(3) $\Longrightarrow$ (1): Sei $\mathrm{pd}_R(R/M) < \infty$. Nach Beispiel 14.4 können wir annehmen, dass R kein Körper ist. Da wir eine kurze exakte Folge $0 \longrightarrow M \longrightarrow R \longrightarrow R/M \longrightarrow 0$ von R-Moduln und R-Homomorphismen haben, ist auch $\mathrm{pd}_R(M) < \infty$. Nach Satz 16.6 ist also R ein regulärer lokaler Ring.

Seien jetzt (1), (2) und (3) erfüllt. Ist R ein Körper, so verschwindet jede der Zahlen $\mathrm{pd}_R(R/M)$, $\mathrm{gld}(R)$, $\mathrm{Dim}(R)$, $\dim_{R/M}(M/M^2)$.

Ist R kein Körper, so gilt:

$$\dim_{R/M}(M/M^2) = \mathrm{Dim}(R) = \mathrm{gld}(R) \geq \mathrm{pd}_R(R/M) = \mathrm{pd}_R(M) + 1 = \mathrm{Dim}(R).$$

16.8 Satz. *Sei R ein regulärer lokaler Ring. Für $P \in \mathrm{Spec}(R)$ ist dann auch R_P ein regulärer lokaler Ring.*

Beweis. Sicher ist R_P lokal und noethersch. Nach Satz 16.3 und Satz 16.5 ist $\mathrm{gld}(R_P) \leq \mathrm{gld}(R) < \infty$. Aus Satz 16.7 folgt also die Behauptung.

Bemerkung. Man kennt bis heute keinen ganz elementaren Beweis für Satz 16.8. Auch der Beweis der Aussage, dass reguläre lokale Ringe faktoriell sind, verwendet die obigen Methoden.

17. Faktorielle Ringe

Sei R ein Ring.

17.1 Satz. *Ein noetherscher Integritätsbereich R ist genau dann faktoriell, wenn jedes Primideal der Höhe 1 in R ein Hauptideal ist.*

Beweis. "$\Longrightarrow$": Sei R ein faktorieller Ring und $P \in \operatorname{Spec}(R)$ mit $\operatorname{ht}(P) = 1$. Sei ferner $0 \neq a \in P$, und sei $a = p_1 \dots p_r$ mit Primelementen $p_1, \dots, p_r \in R$. Dann ist $p_i \in P$ für ein $i \in \{1, \dots, r\}$. Wegen $Rp_i \in \operatorname{Spec}(R)$ und $0 \subset Rp_i \subseteq P$ folgt: $P = Rp_i$.

"$\Longleftarrow$": Da R noethersch ist, kann man jedes Element $0 \neq a \in R \setminus R^\times$ als Produkt irreduzibler Elemente schreiben. Daher genügt zu zeigen, dass jedes irreduzible Element $a \in R$ ein Primelement ist. Sei $P \in \mathcal{V}(Ra)$ minimal. Nach Satz 12.2 ist $\operatorname{ht}(P) = 1$. Daher ist $P = Rb$ für ein $b \in R$. Sei $c \in R$ mit $a = bc$. Da a irreduzibel ist, folgt: $c \in R^\times$. Also ist $Ra = Rb = P \in \operatorname{Spec}(R)$, d.h. a ist ein Primelement in R.

17.2 Satz. *Seien R ein noetherscher Integritätsbereich, $a \in R$ ein Primelement und $A := \{1, a, a^2, \dots, \}$. Ist $A^{-1}R$ faktoriell, so auch R.*

Bemerkung. Natürlich ist $A^{-1}R$ ein noetherscher Integritätsbereich.

Beweis. Sei $A^{-1}R$ faktoriell, und sei $P \in \operatorname{Spec}(R)$ mit $\operatorname{ht}(P) = 1$. Nach Satz 17.1 genügt zu zeigen, dass P ein Hauptideal in R ist.

Im Fall $P \cap A \neq \emptyset$ ist $a \in P$. Wegen $Ra \in \operatorname{Spec}(R)$ und $0 \subset Ra \subseteq P$ folgt: $P = Ra$.

Sei also $P \cap A = \emptyset$. Dann ist $A^{-1}P \in \operatorname{Spec}(A^{-1}R)$ und $\operatorname{ht}(A^{-1}P) = \operatorname{ht}(P) = 1$. Nach Satz 17.1 existieren $p \in P$, $b \in A$ mit $A^{-1}P = (A^{-1}R)\frac{p}{b}$; o.B.d.A. $b = 1$. Ferner sei p so gewählt, dass Rp maximal ist. Dann gilt: $a \not| \, p$.

Für $x \in P$ ist $\frac{x}{1} \in A^{-1}P$. Daher existieren $r \in R$, $n \in \mathbb{N}_0$ mit $\frac{x}{1} = \frac{r}{a^n}\frac{p}{1} = \frac{rp}{a^n}$, d.h. $a^n x = rp$. Daraus folgt leicht: $a^n | r$, d.h. $x \in Rp$. Dies zeigt: $P = Rp$.

17.3 Satz. *Sei R ein Integritätsbereich, und sei $I \trianglelefteq R$ mit $I \times R^n \simeq R^{n+1}$. Dann ist I ein Hauptideal in R.*

Beweis. Wir fassen $I \times R^n$ als Untermodul von $R \times R^n = R^{n+1}$ auf und bezeichnen die Standardbasis von R^{n+1} mit $e_0, e_1, \dots, e_n$. Sei $\phi : R^{n+1} \longrightarrow I \times R^n$ ein R-Isomorphismus, und sei $\phi(e_j) = \sum_{i=0}^n a_{ij} e_i$ mit $a_{ij} \in R$ für $i, j = 0, \dots, n$. Da ϕ injektiv ist, ist $d := |a_{ij}| \neq 0$. Sei $(\widetilde{a}_{jk})$ die Adjunkte von (a_{ij}), d.h. $(a_{ij})(\widetilde{a}_{jk}) = d1_{n+1}$. Für $e_0' := \sum_{k=0}^n \widetilde{a}_{k0} e_k$ gilt dann:

$$\phi(e_0') = \sum_{k=0}^n \widetilde{a}_{k0}\phi(e_k) = \sum_{k=0}^n \widetilde{a}_{k0} \sum_{i=0}^n a_{ik} e_i = \sum_{i=0}^n (\sum_{k=0}^n a_{ik}\widetilde{a}_{k0}) e_i = \sum_{i=0}^n d\delta_{i0} e_i = de_0.$$

Für $j = 1, \ldots, n$ ist $e_j \in \mathrm{Bld}(\phi)$, d.h. $e_j = \phi(e'_j)$ für ein $e'_j \in R^{n+1}$. Wir schreiben $e'_j = \sum_{k=0}^{n} b_{kj} e_k$ mit $b_{kj} \in R$ für $j, k = 0, \ldots, n$. Dann ist $b_{k0} = \widetilde{a}_{k0}$ für $k = 0, \ldots, n$, und für $j = 1, \ldots, n$ gilt:

$$e_j = \phi(e'_j) = \sum_{k=0}^{n} b_{kj}\phi(e_k) = \sum_{k=0}^{n} b_{kj} \sum_{i=0}^{n} a_{ik} e_i = \sum_{i=0}^{n} (\sum_{k=0}^{n} a_{ik} b_{kj}) e_i,$$

d.h. $\sum_{k=0}^{n} a_{ik} b_{kj} = \delta_{ij}$ für $i = 0, \ldots, n$. Das bedeutet:

$$(a_{ik})(b_{kj}) = \begin{pmatrix} d & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Ein Vergleich der Determinanten ergibt: $|b_{kj}| = 1$. Daher bilden auch $e'_0, e'_1, \ldots, e'_n$ eine Basis von R^{n+1}. Für die Projektion $\pi : R^{n+1} \longrightarrow R$ auf die 0-te Koordinate gilt also:

$$\begin{aligned} I &= \pi(I \times R^n) = \pi(\phi(R^{n+1})) = \pi(\phi(Re'_0 + Re'_1 + \ldots + Re'_n) \\ &= \pi(Rde_0 + Re_1 + \ldots + Re_n) = Rd. \end{aligned}$$

17.4 Bemerkung. Seien V, W R-Moduln, $P \in \mathrm{Spec}(R)$ und

$$\lambda : \mathrm{Hom}_R(V, W) \longrightarrow \mathrm{Hom}_R(V, W)_P$$

kanonisch. Nach Bemerkung 8.4 ist $h : \mathrm{Hom}_R(V, W) \longrightarrow \mathrm{Hom}_{R_P}(V_P, W_P)$, $f \longmapsto f_P$, R-linear. Nach Satz 8.2 existiert genau ein R-Homomorphismus

$$H : \mathrm{Hom}_R(V, W)_P \longrightarrow \mathrm{Hom}_{R_P}(V_P, W_P)$$

mit $H \circ \lambda = h$, und nach Bemerkung 8.4 ist H auch R_P-linear.

Satz. *Sei R noethersch und $P \in \mathrm{Spec}(R)$. Seien außerdem V, W R-Moduln, wobei V endlich erzeugt ist. Dann ist die Abbildung $H : \mathrm{Hom}_R(V, W)_P \longrightarrow \mathrm{Hom}_{R_P}(V_P, W_P)$ aus Bemerkung 17.4 ein R_P-Isomorphismus.*

Beweis. Zunächst sei $V = R^n$ für ein $n \in \mathbb{N}_0$. Dann ist $\mathrm{Hom}_R(R^n, W) \simeq W^n$, also $\mathrm{Hom}_R(R^n, W)_P \simeq (W^n)_P \simeq (W_P)^n$. Ferner ist $V_P = (R^n)_P \simeq (R_P)^n$, also auch $\mathrm{Hom}_{R_P}((R^n)_P, W_P) \simeq (W_P)^n$. Man zeigt leicht, dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} \mathrm{Hom}_R(R^n, W)_P & \longrightarrow & \mathrm{Hom}_{R_P}((R^n)_P, W_P) \\ \downarrow & & \downarrow \\ (W_P)^n & \longrightarrow & (W_P)^n \end{array}$$

Also ist H auch ein R_P-Isomorphismus.

Jetzt sei V beliebig. Dann existieren ein $n \in \mathbb{N}_0$ und ein (endlich erzeugter) Untermodul $U \subseteq R^n$ mit $V \simeq R^n/U$. Analog existieren ein $m \in \mathbb{N}_0$ und ein R-Epimorphismus $R^m \longrightarrow U$. Wir erhalten so eine exakte Folge von R-Moduln

$$\mathcal{F} : R^m \longrightarrow R^n \longrightarrow V \longrightarrow 0.$$

Diese induziert eine exakte Folge von R-Moduln

$$0 \longrightarrow \mathrm{Hom}_R(V, W) \longrightarrow \mathrm{Hom}_R(R^n, W) \longrightarrow \mathrm{Hom}_R(R^m, W).$$

Durch Lokalisieren erhalten wir eine exakte Folge von R_P-Moduln

$$0 \longrightarrow \mathrm{Hom}_R(V, W)_P \longrightarrow \mathrm{Hom}_R(R^n, W)_P \longrightarrow \mathrm{Hom}_R(R^m, W)_P.$$

Wegen $(R^m)_P \simeq (R_P)^m$ und $(R^n)_P \simeq (R_P)^n$ liefert $\mathcal{F}$ auch eine exakte Folge von R_P-Moduln

$$(R_P)^m \longrightarrow (R_P)^n \longrightarrow V_P \longrightarrow 0.$$

Diese induziert eine exakte Folge von R_P-Moduln

$$0 \longrightarrow \mathrm{Hom}_{R_P}(V_P, W_P) \longrightarrow \mathrm{Hom}_{R_P}((R_P)^n, W_P) \longrightarrow \mathrm{Hom}_{R_P}((R_P)^m, W_P).$$

Durch mehrfache Anwendung von Bemerkung 17.4 erhalten wir das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(V, W)_P & \longrightarrow & \mathrm{Hom}_R(R^n, W)_P & \longrightarrow & \mathrm{Hom}_R(R^m, W)_P \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_{R_P}(V_P, W_P) & \longrightarrow & \mathrm{Hom}_{R_P}((R^n)_P, W_P) & \longrightarrow & \mathrm{Hom}_{R_P}((R^m)_P, W_P). \end{array}$$

Man rechnet leicht nach, dass dieses Diagramm kommutiert. Nach dem ersten Teil des Beweises sind die senkrechten Abbildungen rechts und in der Mitte bijekiv. Mit Diagrammjagd folgt daraus leicht, dass auch H bijektiv ist.

17.5 Satz. *Sei R noethersch. Für einen endlich erzeugten R-Modul W sind äquivalent:*
(1) W ist ein projektiver R-Modul.
(2) W_P ist ein projektiver (d.h. freier) R_P-Modul für jedes $P \in \mathrm{Spec}(R)$.
(3) W_M ist ein projektiver (d.h. freier) R_M-Modul für jedes $M \in \mathrm{Max}(R)$.

Beweis. (1) $\Longrightarrow$ (2): Sei (1) erfüllt und $P \in \mathrm{Spec}(R)$. Dann existiert eine zerfallende kurze exakte Folge von R-Moduln

$$0 \longrightarrow U \longrightarrow F \longrightarrow W \longrightarrow 0,$$

wobei F ein freier R-Modul ist. Daher ist

$$0 \longrightarrow U_P \longrightarrow F_P \longrightarrow W_P \longrightarrow 0$$

eine zerfallende kurze exakte Folge von R_P-Moduln, wobei F_P ein freier R_P-Modul ist. Also ist W_P ein projektiver R_P-Modul.

(2) $\Longrightarrow$ (3): Trivial.

(3) $\Longrightarrow$ (1): Sei (3) erfüllt, und sei $f : U \longrightarrow V$ ein R-Epimorphismus zwischen R-Moduln U, V. Dann ist

$$f_* : \mathrm{Hom}_R(W, U) \longrightarrow \mathrm{Hom}_R(W, V), \quad h \longmapsto h \circ f,$$

R-linear. Wir müssen zeigen, dass f_* surjektiv ist. Dazu sei $M \in \mathrm{Max}(R)$. Nach Satz 9.5 genügt zu zeigen, dass $(f_*)_M : \mathrm{Hom}_R(W, U)_M \longrightarrow \mathrm{Hom}_R(W, V)_M$ surjektiv ist. Man zeigt leicht, dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} \mathrm{Hom}_R(W, U)_M & \longrightarrow & \mathrm{Hom}_R(W, V)_M \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{R_M}(W_M, U_M) & \longrightarrow & \mathrm{Hom}_{R_M}(W_M, V_M). \end{array}$$

Dabei sind die senkrechten Abbildungen die Isomorphismen aus Satz 17.4. Daher genügt zu zeigen, dass $(f_M)_* : \mathrm{Hom}_{R_M}(W_M, U_M) \longrightarrow \mathrm{Hom}_{R_M}(W_M, V_M)$ surjektiv ist. Da $f_M : U_M \longrightarrow V_M$ surjektiv ist, folgt dies aus der Projektivität von W_M.

Bemerkung. Sei W ein endlich erzeugter projektiver R-Modul. Für $P \in \mathrm{Spec}(R)$ ist dann W_P ein endlich erzeugter freier R_P-Modul. Man kann zeigen, dass

$$r_W : \mathrm{Spec}(R) \longrightarrow \mathbb{Z}, \quad P \longmapsto \mathrm{rg}_{R_P}(W_P),$$

eine stetige Abbildung ist, wobei man $\mathbb{Z}$ als topologischen Unterraum von $\mathbb{R}$ auffasst.

17.6 Definition. Eine **endliche freie Auflösung** eines R-Moduls V ist eine exakte Folge von R-Moduln der Form

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow V \longrightarrow 0,$$

wobei $F_0, \ldots, F_n$ endlich erzeugt und frei sind.

Bemerkung. (i) Ggf. ist auch V endlich erzeugt.

(ii) Sei R ein noetherscher lokaler Ring und V ein endlich erzeugter R-Modul mit $n := \mathrm{pd}(V) < \infty$. Dann existiert eine kurze exakte Folge von R-Moduln

$$0 \longrightarrow V_1 \longrightarrow F_0 \longrightarrow V_0 := V \longrightarrow 0,$$

wobei F_0 endlich erzeugt und frei ist. Dabei ist $\mathrm{pd}(V_1) = n - 1$ (im Fall $n > 0$), und V_1 ist auch endlich erzeugt. Daher erhält man analog eine kurze exakte Folge von R-Moduln

$$0 \longrightarrow V_2 \longrightarrow F_1 \longrightarrow V_1 \longrightarrow 0,$$

wobei F_1 endlich erzeugt und frei ist. Dabei ist $\mathrm{pd}(V_2) = n - 2$ (im Fall $n > 1$), und V_2 ist endlich erzeugt. So fahren wir fort und erhalten schließlich eine kurze exakte Folge von R-Moduln

$$0 \longrightarrow V_n \longrightarrow F_{n-1} \longrightarrow V_{n-1} \longrightarrow 0,$$

wobei F_{n-1} endlich erzeugt und frei ist. Ferner ist $\mathrm{pd}(V_n) = 0$, d.h. V_n ist projektiv und endlich erzeugt und damit frei. Setzt man diese kurzen exakten Folgen zusammen, so ergibt sich eine endliche freie Auflösung

$$0 \longrightarrow V_n \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow V \longrightarrow 0.$$

17.7 Definition. Ein R-Modul V heißt **stabil-frei**, falls $m, n \in \mathbb{N}_0$ mit $V \times R^m \simeq R^n$ existieren.

Beispiel. Jeder endlich erzeugte freie R-Modul ist stabil-frei.

Bemerkung. (i) Jeder stabil-freie R-Modul V ist endlich erzeugt und projektiv. Ferner ist (in der obigen Situation) $0 \longrightarrow R^m \longrightarrow R^n \longrightarrow V \longrightarrow 0$ eine endliche freie Auflösung von V.

(ii) Vgl. Satz 17.3.

Satz. *Sei V ein projektiver R-Modul mit einer endlichen freien Auflösung*

$$0 \longrightarrow F_n \xrightarrow{f_n} F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} V \longrightarrow 0.$$

Dann ist V stabil-frei.

Beweis. (Induktion nach n)
Im Fall $n = 0$ ist $0 \longrightarrow F_0 \longrightarrow V \longrightarrow 0$ eine kurze exakte Folge von R-Moduln. Also ist $V \simeq F_0$ sogar endlich erzeugt und frei.

Sei $n > 0$. Da $0 \longrightarrow \mathrm{Ker}(f_0) \longrightarrow F_0 \xrightarrow{f_0} V \longrightarrow 0$ eine kurze exakte Folge von R-Moduln ist, gilt: $F_0 \simeq V \times \mathrm{Ker}(f_0)$. Daher ist $\mathrm{Bld}(f_0) = \mathrm{Ker}(f_0)$ auch projektiv, und wir haben eine endliche freie Auflösung

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \longrightarrow \mathrm{Bld}(f_1) \longrightarrow 0.$$

Nach Induktion ist also $\mathrm{Bld}(f_1) = \mathrm{Ker}(f_0)$ stabil-frei, d.h. es gibt $m, n \in \mathbb{N}_0$ mit $\mathrm{Ker}(f_0) \times R^m \simeq R^n$. Daher gilt:

$$V \times R^n \simeq V \times \mathrm{Ker}(f_0) \times R^m \simeq F_0 \times R^m \simeq R^k$$

für ein $k \in \mathbb{N}_0$. Also ist V stabil-frei.

17.8 Satz. (Auslander-Buchsbaum 1959)
Jeder reguläre lokale Ring R ist faktoriell.

Beweis. (Induktion nach $d := \mathrm{Dim}R$)
Sei $M := \mathrm{J}(R)$. Im Fall $d = 0$ ist R ein Körper und damit ein faktorieller Ring. Im Fall $d = 1$ ist R ein DBR und damit ein faktorieller Ring. Sei also $d > 1$ und $x \in M \setminus M^2$, d.h. $Rx \in \mathrm{Spec}(R)$. Sei $A := \{1, x, x^2, \ldots\}$, d.h. $R \subseteq A^{-1}R \subseteq K := \mathrm{Quot}(R)$. Nach Satz 17.2 genügt zu zeigen, dass $A^{-1}R$ faktoriell ist. Sei $Q \in \mathrm{Spec}(A^{-1}R)$ mit $\mathrm{ht}(P) = 1$. Nach Satz 17.1 genügt zu zeigen, dass Q ein Hauptideal in $A^{-1}R$ ist. Bekanntlich ist

$P := Q \cap R \in \mathrm{Spec}(R)$ und $Q = A^{-1}P$. Da R ein regulärer lokaler Ring ist, hat der R-Modul P eine endliche freie Auflösung

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \ldots \longrightarrow F_0 \longrightarrow P \longrightarrow 0.$$

Daher ist

$$0 \longrightarrow A^{-1}F_n \longrightarrow A^{-1}F_{n-1} \longrightarrow \ldots \longrightarrow A^{-1}F_1 \longrightarrow A^{-1}F_0 \longrightarrow A^{-1}P \longrightarrow 0$$

eine endliche freie Auflösung des $A^{-1}R$-Moduls $A^{-1}P = Q$. Wir zeigen, dass Q ein projektiver $A^{-1}R$-Modul ist.

[Dazu sei $Q' \in \mathrm{Spec}(A^{-1}R)$. Dann ist $P' := Q' \cap R \in \mathrm{Spec}(R)$ mit $A \cap P' = \emptyset$ und $A^{-1}P' = Q'$. Man zeigt leicht, dass $(A^{-1}R)_{Q'} = R_{P'}$ gilt. Dabei ist $R_{P'}$ nach Satz 16.8 ein regulärer lokaler Ring. Wegen $x \in M$ ist $A^{-1}M = A^{-1}R$, d.h. $\mathrm{Dim}R_{P'} < d$. Nach Induktion ist also $(A^{-1}R)_{Q'} = R_{P'}$ faktoriell.

Entweder ist $Q_{Q'} = (A^{-1}R)_{Q'}$, oder es ist $Q_{Q'} \in \mathrm{Spec}((A^{-1}R)_{Q'})$ und $\mathrm{ht}(Q_{Q'}) \leq 1$. Nach Satz 17.1 ist also $Q_{Q'}$ ein Hauptideal, d.h. $Q_{Q'} \simeq (A^{-1}R)_{Q'}$. In jedem Fall ist also $Q_{Q'}$ ein freier $(A^{-1}R)_{Q'}$-Modul. Daher ist Q ein projektiver $A^{-1}R$-Modul.]

Aus Satz 17.7 folgt jetzt, dass Q ein stabil-freier $A^{-1}R$-Modul ist. Daher existieren $m, n \in \mathbb{N}_0$ mit $Q \times (A^{-1}R)^m \simeq (A^{-1}R)^n$. Lokalisierung am Nullideal ergibt: $K^{m+1} \simeq K^n$, d.h. $n = m + 1$. Also ist $Q \times (A^{-1}R)^m \simeq (A^{-1}R)^{m+1}$. Damit folgt aus Satz 17.3, dass Q ein Hauptideal in $A^{-1}R$ ist.

18. Noethers Normalisierungssatz und Hilberts Nullstellensatz

Sei K ein Körper.

18.1 Satz. *Sei $n \in \mathbb{N}$, und sei $M \subseteq \mathbb{N}_0^n$ endlich. Dann existieren* **Gewichte** $w_1 = 1, w_2, \ldots, w_n \in \mathbb{N}$ *derart, dass die Zahlen*

$$w_1 m_1 + w_2 m_2 + \cdots + w_n m_n \in \mathbb{N}_0$$

$((m_1, \ldots, m_n) \in M)$ paarweise verschieden sind.

Beweis. (Induktion nach n)

Im Fall $n = 1$ ist $M \subseteq \mathbb{N}_0$, und man kann $w_1 := 1$ nehmen. Sei also $n > 1$ und die Behauptung für $n - 1$ schon gezeigt. Dann ist

$$L := \{(m_1, \ldots, m_{n-1}) : \exists m_n \in \mathbb{N}_0 : (m_1, \ldots, m_{n-1}, m_n) \in M\} \subseteq \mathbb{N}_0^{n-1}$$

endlich. Nach Induktion existieren $w_1 = 1, w_2, \ldots, w_{n-1} \in \mathbb{N}$ derart, dass die Zahlen

$$w_1 m_1 + \cdots + w_{n-1} m_{n-1} \in \mathbb{N}_0$$

$((m_1, \ldots, m_{n-1}) \in L)$ paarweise verschieden sind. Wir wählen $w_n \in \mathbb{N}$ mit

$$w_n > \max\{w_1 m_1 + \cdots + w_{n-1} m_{n-1} : (m_1, \ldots, m_{n-1}) \in L\}.$$

Seien jetzt $(m_1,\dots,m_n),(m_1',\dots,m_n')\in M$ mit

$$w_1m_1+\cdots+w_nm_n=w_1m_1'+\cdots+w_nm_n'.$$

Im Fall $m_n\neq m_n'$ (also o.B.d.A. $m_n<m_n'$) hätte man den Widerspruch

$$\begin{aligned}w_1m_1+\cdots+w_{n-1}m_{n-1}+w_nm_n&<w_n(1+m_n)\le w_nm_n'\\&\le w_1m_1'+\cdots+w_nm_n'=w_1m_1+\cdots+w_nm_n.\end{aligned}$$

Also ist $m_n=m_n'$ und $w_1m_1+\cdots+w_{n-1}m_{n-1}=w_1m_1'+\cdots+w_{n-1}m_{n-1}'$. Nach Induktion ist also $(m_1,\dots,m_{n-1})=(m_1',\dots,m_{n-1}')$, d.h. $(m_1,\dots,m_n)=(m_1',\dots,m_n')$.

18.2 Satz. *Sei R eine K-Algebra, und seien $y_1,\dots,y_n\in R$ mit $R=K[y_1,\dots,y_n]$. Ferner gebe es ein Polynom $0\neq F\in K[Y_1,\dots,Y_n]$ mit $F(y_1,\dots,y_n)=0$. Dann existieren $y_1^*,\dots,y_{n-1}^*\in R$ derart, dass y_n ganz über $R^*:=K[y_1^*,\dots,y_{n-1}^*]$ und $R=R^*[y_n]$ ist.*

Beweis. Wir schreiben

$$F=\sum_{(m_1,\dots,m_n)\in M}\alpha_{(m_1,\dots,m_n)}Y_1^{m_1}\cdots Y_n^{m_n},$$

wobei M eine endliche Teilmenge von $\mathbb{N}_0^n$ und $0\neq\alpha_{(m_1,\dots,m_n)}\in K$ für alle $(m_1,\dots,m_n)\in M$ ist. Nach Satz 18.1 existieren Gewichte $w_1,\dots,w_{n-1}\in\mathbb{N}$, $w_n=1$ derart, dass die Zahlen

$$w_1m_1+\cdots+w_nm_n\in\mathbb{N}_0$$

($(m_1,\dots,m_n)\in M$) paarweise verschieden sind. Dann ist

$$F=\sum_{(m_1,\dots,m_n)\in M}\alpha_{(m_1,\dots,m_n)}(Y_1^*+Y_n^{w_1})^{m_1}\cdots(Y_{n-1}^*+Y_n^{w_{n-1}})^{m_{n-1}}Y_n^{m_n}$$

mit $Y_i^*:=Y_i-Y_n^{w_i}$ für $i=1,\dots,n-1$. Wir multiplizieren jeden Summanden einzeln aus und schreiben das Resultat als Polynom in Y_n mit Koeffizienten in $K[Y_1^*,\dots,Y_{n-1}^*]$. Dies ergibt jeweils ein Polynom vom Grad $w_1m_1+\cdots+w_nm_n$ mit höchstem Koeffizienten $\alpha_{(m_1,\dots,m_n)}\neq0$. Dann ist

$$F=\sum_{j=0}^{t}A_jY_n^j,$$

mit $A_j\in K[Y_1^*,\dots,Y_{n-1}^*]$ für $j=0,\dots,t$ und $0\neq A_t\in K$. Daher gilt:

$$0=F(y_1,\dots,y_n)=\sum_{j=0}^{t-1}A_j(y_1^*,\dots,y_{n-1}^*)y_n^j+A_ty_n^t$$

mit $y_i^*:=y_i-y_n^{w_i}$ für $i=1,\dots,n-1$. Division durch A_t zeigt, dass y_n ganz über $R^*:=K[y_1^*,\dots,y_{n-1}^*]$ ist. Ferner gilt:

$$R=K[y_1,\dots,y_n]=K[y_1^*,\dots,y_{n-1}^*,y_n]=R^*[y_n].$$

18.3 Definition. Elemente $y_1, \ldots, y_n$ in einer K-Algebra R heißen **algebraisch abhängig** (über K), falls ein Polynom $0 \neq F \in K[Y_1, \ldots, Y_n]$ mit $F(y_1, \ldots, y_n) = 0$ existiert. Andernfalls heißen sie **algebraisch unabhängig** (über K).

Satz. (Noethers Normalisierungssatz)
Sei R eine endlich erzeugte K-Algebra. Dann existieren $z_1, \ldots, z_m \in R$ derart, dass $z_1, \ldots, z_m$ algebraisch unabhängig über K sind und R eine endliche $K[z_1, \ldots, z_m]$-Algebra ist.

Beweis. (Induktion nach der Anzahl n der Erzeugenden von R)

Im Fall $n = 0$ ist nichts zu tun. Sei also $n > 0$ und $R = K[y_1, \ldots, y_n]$. Sind $y_1, \ldots, y_n$ algebraisch unabhängig über K, so ist auch nichts zu tun. Andernfalls existiert ein Polynom $0 \neq F \in K[Y_1, \ldots, Y_n]$ mit $F(y_1, \ldots, y_n) = 0$. Nach Satz 18.2 existieren $y_1^*, \ldots, y_{n-1}^* \in R$ derart, dass y_n ganz über $R^* := K[y_1^*, \ldots, y_{n-1}^*]$ und $R = R^*[y_n]$ ist. Nach Induktion existieren dann $z_1, \ldots, z_m \in R^*$ derart, dass $z_1, \ldots, z_m$ algebraisch unabhängig über K und R^* eine endliche $K[z_1, \ldots, z_m]$-Algebra ist. Da R eine endliche R^*-Algebra ist, ist R auch eine endliche $K[z_1, \ldots, z_m]$-Algebra.

Bemerkung. In der obigen Situation haben wir also einen Isomorphismus von K-Algebren

$$K[Z_1, \ldots, Z_m] \longrightarrow K[z_1, \ldots, z_m], \quad F \longmapsto F(z_1, \ldots, z_m).$$

Daraus folgt leicht, dass R Krulldimension m hat. Man kann sogar zeigen, dass alle maximalen Primidealketten in R Länge m haben; dabei heißt eine Primidealkette **maximal**, wenn man sie nicht durch Einschieben weiterer Primideale verlängern kann. Dagegen gibt es noethersche Ringe mit maximalen Primidealketten unterschiedlicher Länge.

18.4 Satz. (Schwacher Nullstellensatz)
Sei R eine endlich erzeugte K-Algebra. Ist R ein Körper, so ist $\dim_K R < \infty$. (Man kann R also als endliche Körpererweiterung von K auffassen.)

Beweis. Nach Satz 18.3 existieren $z_1, \ldots, z_m \in R$ derart, dass $z_1, \ldots, z_m$ algebraisch unabhängig über K sind und R eine endliche $K[z_1, \ldots, z_m]$-Algebra ist. Nach Satz 13.1 ist $K[z_1, \ldots, z_m]$ ein Körper. Also folgt: $m = 0$. Daher ist R eine endliche K-Algebra.

Bemerkung. Sei $M \in \mathrm{Max}(K[X_1, \ldots, X_n])$, und sei $L := K[X_1, \ldots, X_n]/M$. Dann ist L ein Körper, und $f : K \longrightarrow L$, $a \longmapsto a + M$, ist ein Körpermonomorphismus. Wir identifizieren K mit seinem Bild in L und fassen K so als Teilkörper von L auf. Für $i = 1, \ldots, n$ sei $x_i := X_i + M$, Dann ist $L = K[x_1, \ldots, x_n]$ eine endlich erzeugte K-Algebra. Aus Satz 18.4 folgt, dass L eine *endliche* Körpererweiterung von K ist.

18.5 Satz. (Hilberts Nullstellensatz)
Sei K algebraisch abgeschlossen und $M \in \mathrm{Max}(K[X_1, \ldots, X_n])$. Dann existieren Elemente $a_1, \ldots, a_n \in K$ mit $M = (X_1 - a_1, \ldots, X_n - a_n)$.

Beweis. $R := K[X_1, \ldots, X_n]/M$ ist ein Körper und eine endlich erzeugte K-Algebra. Nach Satz 18.4 ist $\dim_K(R) < \infty$, d.h. wir können $K \subseteq R$ als endliche Körpererweiterung auffassen. Da K algebraisch abgeschlossen ist, folgt: $\dim_K(R) = 1$, d.h. $R = K1_R$. Für

$i = 1, \ldots, n$ existiert also ein $a_i \in K$ mit $X_i + M = a_i 1_R = a_i + M$. Daher gilt: $I := (X_1 - a_1, \ldots, X_n - a_n) \subseteq M$. Wegen $K[X_1, \ldots, X_n]/I = K + I/I \cong K/K \cap I = K/0 \cong K$ ist $I \in \mathrm{Max}(K[X_1, \ldots, X_n])$, d.h. $I = M$.

Bemerkung. (i) Sei R ein noetherscher Ring der Krulldimension d, und sei $I \trianglelefteq R[X]$. Der Satz von Storch und Eisenbud-Evans (1972/73) besagt, dass Elemente $f_1, \ldots, f_{d+1} \in I$ existieren mit $\mathrm{rad}(I) = \mathrm{rad}((f_1, \ldots, f_{d+1}))$.
(ii) Daraus folgt, dass für $n \in \mathbb{N}$ und $I \trianglelefteq K[X_1, \ldots, X_n]$ Polynome $f_1, \ldots, f_n \in I$ mit $\mathrm{rad}(I) = \mathrm{rad}((f_1, \ldots, f_n))$ existieren.

Literatur

1. M.F. Atiyah-I.G. MacDonald, Introduction to Commutative Algebra
2. S. Bosch, Algebraic Geometry and Commutative Algebra
3. R. Brüske-F. Ischebeck-F. Vogel, Kommutative Algebra
4. D. Eisenbud, Commutative Algebra
5. I. Kaplansky, Fields and Rings
6. I. Kaplansky, Commutative Rings
7. G. Kemper, A Course in Commutative Algebra
8. E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry
9. H. Matsumura, Commutative Algebra
10. H. Matsumura, Commutative Ring Theory
11. M. Reid, Undergraduate Commutative Algebra

Internet

- The CRings Project
- The Stacks Project