# Algebra 2

Achim Krause

14. Juli 2023

Dies ist das Skript zur Vorlesung Algebra 2 im Sommersemester 2023 an der Uni Heidelberg. Es wird im Laufe des Semesters schrittweise erweitert werden.

## Inhaltsverzeichnis



# 1 Ringe, Moduln und Kategorien

## 1.1 Grundbegriffe

**Definition 1.1.1.** *Ein* Ring *ist eine Menge $R$ mit Elementen $0, 1 \in R$ und Abbildungen $+ : R \times R \to R$, $\cdot : R \times R \to R$, sodass gilt:*

1. *$(R, +, 0)$ ist eine abelsche Gruppe.*
2. *$\cdot$ ist assoziativ und $1$ ist neutrales Element bzgl. $\cdot$ ($(R, \cdot, 1)$ ist ein Monoid)*
3. *Es gilt das Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$.*

**Definition 1.1.2.** *Für einen Ring $R$ ist ein Linksmodul eine Menge $M$ mit einem Element $0 \in M$ und Abbildungen $+ : M \times M \to M$ und $\cdot : R \times M \to M$, sodass gilt:*

1. *$(M, +, 0)$ ist eine abelsche Gruppe.*
2. *Die Wirkung von $R$ auf $M$ ist "assoziativ" und "unital", d.h. $a \cdot (b \cdot m) = (a \cdot b) \cdot m$ und $1 \cdot m = m$ für alle $a, b \in R$ und $m \in M$.*
3. *Es gilt $(a + b) \cdot m = a \cdot m + b \cdot m$ und $a \cdot (m + n) = a \cdot m + a \cdot n$.*

Rechtsmoduln werden analog definiert.

**Beispiel 1.1.3.**

1. Ein Körper $K$ ist insbesondere ein Ring, und $K$-Moduln sind das gleiche wie Vektorräume.
2. $\mathbb{Z}$ ist ein Ring, und $\mathbb{Z}$-Moduln sind abelsche Gruppen.
3. $K[x]$ ist ein Ring, und ein $K[x]$-Modul ist das gleiche wie ein $K$-Vektorraum zusammen mit einem $K$-linearen Endomorphismus (gegeben durch die Wirkung von $x$). Wir haben den Jordan-Normalformensatz in Lineare Algebra II bewiesen, indem wir die Struktur von $K[x]$-Moduln analysiert haben.
4. Für einen Ring $R$ bildet $\mathrm{Mat}_{n\times n}(R)$ wieder einen Ring, und z.B. $R^n$ lässt sich als Modul darüber auffassen.

**Bemerkung 1.1.4.** Für einen kommutativen Ring $R$ können wir einen $R$-Linksmodul auch als $R$-Rechtsmodul auffassen und umgekehrt. Für einen nichtkommutativen Ring geht das nicht!

Wenn wir $R^{\mathrm{op}}$ als den Ring mit derselben unterliegenden Menge $R$, aber neuer Multiplikation $a \cdot_{R^{\mathrm{op}}} b = b \cdot_R a$ definieren, dann sind $R$-Linksmoduln das gleiche wie $R^{\mathrm{op}}$-Rechtsmoduln, aber $R$ und $R^{\mathrm{op}}$ sind im allgemeinen nicht isomorph.

Wie bei anderen algebraischen Begriffen haben wir auch für Ringe und Moduln *Homomorphismen*: Für Ringe $R, S$ ist ein Homomorphismus eine Abbildung $f : R \to S$ die die Struktur erhält (also $f(x + y) = f(x) + f(y)$ etc.). Für $R$-Moduln $M, N$ ist ein Homomorphismus entsprechend eine Abbildung $f : M \to N$ die $R$-linear ist.

**Definition 1.1.5.** *Eine Kategorie $\mathcal{C}$ besteht aus:*

1. *Einer Kollektion von* Objekten *(wir schreiben $x \in \mathcal{C}$ wenn $x$ ein Objekt von $\mathcal{C}$ ist).*
2. *Für je zwei Objekte $x, y \in \mathcal{C}$ eine Menge von* Morphismen $\mathrm{Hom}_{\mathcal{C}}(x, y)$.

3. *Für jedes Objekt $x \in \mathcal{C}$ einen Morphismus* $\mathrm{id}_x \in \mathrm{Hom}_{\mathcal{C}}(x,x)$*, und für je drei Objekte $x, y, z \in \mathcal{C}$ eine Abbildung*

$$\circ : \mathrm{Hom}_{\mathcal{C}}(y,z) \times \mathrm{Hom}_{\mathcal{C}}(x,y) \to \mathrm{Hom}_{\mathcal{C}}(x,z).$$

*sodass $(f \circ g) \circ h = f \circ (g \circ h)$, $f \circ \mathrm{id}_x = f$ und $\mathrm{id}_y \circ f = f$, wann immer das Sinn macht.*

Wenn $f \in \mathrm{Hom}_{\mathcal{C}}(x,y)$, so schreiben wir auch $f : x \to y$. Ein $f : x \to y$ heißt *Isomorphismus*, wenn es ein $g : y \to x$ gibt, sodass $g \circ f = \mathrm{id}_x$ und $f \circ g = \mathrm{id}_y$.

**Beispiel 1.1.6.**

1. Die Kategorie Set, deren Objekte Mengen, und deren Morphismen Abbildungen von Mengen sind.
2. Die Kategorie $\mathrm{LMod}_R$, deren Objekte Linksmoduln über einem Ring $R$, und deren Morphismen $R$-lineare Abbildungen sind.
3. Die Kategorie Ring, deren Objekte Ringe, und deren Morphismen Ringhomomorphismen sind.
4. Die Kategorie Grp, deren Objekte Gruppen, und deren Morphismen Gruppenhomomorphismen sind.

Eine *Unterkategorie* $\mathcal{C}'$ einer Kategorie $\mathcal{C}$ besteht aus einer Teilkollektion der Objekte von $\mathcal{C}$ und für $x, y \in \mathcal{C}'$ einer Teilmenge $\mathrm{Hom}_{\mathcal{C}'}(x,y) \subseteq \mathrm{Hom}_{\mathcal{C}}(x,y)$, sodass $\mathcal{C}'$ eine Kategorie bildet, also für jedes darin enthaltene Objekt den zugehörigen Identitätsmorphismus, und für darin enthaltene komponierbare Morphismen auch die Komposition enthält. Von besonderer Relevanz sind *volle* Unterkategorien, das sind die Unterkategorien wo $\mathrm{Hom}_{\mathcal{C}'}(x,y) = \mathrm{Hom}_{\mathcal{C}}(x,y)$ für alle Objekte $x, y \in \mathcal{C}'$. Volle Unterkategorien sind also durch die darin enthaltenen Objekte spezifiziert (zum Beispiel können wir die volle Unterkategorie von Grp auf allen abelschen Gruppen, oder endlichen Gruppen, etc. betrachten).

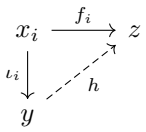
**Bemerkung 1.1.7.** Wir sprechen in der Definition von Kategorien bewusst nicht von einer *Menge* von Objekten, da wir Beispiele wie Set inkludieren wollen, aber eine Menge aller Mengen zu problematischen Paradoxa führen würde. Es gibt verschiedene Varianten, zu formalisieren was mit "Kollektion" gemeint ist, z.B. Mengentheorie mit *Klassen* oder *Universen*, aber wir werden uns damit nicht genauer befassen, da dieser Punkt unproblematisch ist solange wir "normale Mathematik" in unseren Kategorien machen.

Wir stellen uns Kategorien wie verschiedene "Welten" vor, in denen wir arbeiten können. Beschäftigen wir uns mit Gruppen, so arbeiten wir z.B. in Grp. Durch diese Perspektive entpuppen sich viele verschieden aussehende Konstruktionen in Algebra und anderen Teilgebieten der Mathematik als die gleiche Konstruktion, ausgeführt in verschiedenen Kategorien. Wir wollen dieses Semester lernen, diese Sprache zu benutzen, aber versuchen diese parallel zu konkreter Algebra zu entwickeln.

**Definition 1.1.8.** *Sei $\mathcal{C}$ eine Kategorie und $(x_i)_{i\in I}$ eine Familie von Objekten in $\mathcal{C}$. Ein* Koprodukt *von $(x_i)_{i\in I}$ besteht aus*

1. *einem Objekt $y \in \mathcal{C}$,*
2. *sowie Morphismen $\iota_i : x_i \to y$,*

*sodass gilt: Für jedes andere Objekt $z \in \mathcal{C}$ mit Morphismen $f_i : x_i \to z$ existiert genau ein Morphismus $h : y \to z$ mit $h \circ \iota_i = f_i$ für alle $i$.*




**Beispiel 1.1.9.**

1. In Set ist ein Koprodukt einer Familie von Mengen $X_i$ gegeben durch die disjunkte Vereinigung $\coprod X_i$, mit $\iota_i : X_i \to \coprod X_i$ die kanonische Inklusion. Ist nämlich $Z$ eine andere Menge mit irgendwelchen Abbildungen $f_i : X_i \to Z$, so können (und müssen!) wir $h : \coprod X_i \to Z$ definieren durch $h(x) = f_i(x)$ wenn $x \in X_i$, und dann gilt $h \circ \iota_i = f_i$.
2. In $\mathrm{LMod}_R$ ist ein Koprodukt einer Familie von Moduln $M_i$ die *direkte Summe* $\bigoplus M_i$, definiert als die Teilmenge der $(m_i) \in \prod M_i$ die für alle bis auf endlich viele $i$ null sind. (Übungsaufgabe!)

Die Definition von Koprodukten ist ein Beispiel einer *universellen Eigenschaft*. Diese charakterisiert das Koprodukt eindeutig bis auf (eindeutigen!) Isomorphismus:

**Lemma 1.1.10.** *Sei $(x_i)$ eine Familie von Objekten einer Kategorie $\mathcal{C}$. Wenn $(y, \iota_i)$ und $(y', \iota_i')$ zwei verschiedene Koprodukte von $(x_i)_{i\in I}$ sind, dann sind $y$ und $y'$ isomorph.*

*Beweis.*
1. Wir erhalten durch Anwenden der universellen Eigenschaft des Koprodukts $(y, \iota_i)$ auf das andere Objekt $(y', \iota_i')$ ein eindeutiges $h : y \to y'$ mit $\iota_i' = h \circ \iota_i$ für alle $i$,
2. Durch Anwenden der universellen Eigenschaft des Koprodukts $(y', \iota_i')$ auf das andere Objekt $(y, \iota_i)$ erhalten wir ein eindeutiges $h : y' \to y$ mit $\iota_i = h' \circ \iota_i'$ für alle $i$.
3. Laut universeller Eigenschaft von $y$ angewandt auf das gleiche Objekt $(y, \iota_i)$ gibt es ein *eindeutiges* $f : y \to y$ mit $f \circ \iota_i = \iota_i$ für alle $i$. Nach Konstruktion tut $h' \circ h$ das, aber natürlich auch $\mathrm{id}_y$. Also ist $h' \circ h = \mathrm{id}_y$.
4. Umgekehrt ist auch $h \circ h' = \mathrm{id}_y'$, also sind $h, h'$ zueinander inverse Isomorphismen.

□

Wir schreiben $\coprod_{i\in I} x_i$ für das Koprodukt der Familie $x_i$. In Moduln schreiben wir stattdessen auch $\bigoplus_{i\in I}$.

Etwas weniger präzise ausgedrückt besagt die universelle Eigenschaft des Koprodukts, dass eine Abbildung aus $y$ heraus "das gleiche" ist wie eine Familie von Abbildungen aus allen $x_i$. Andere universelle Eigenschaften dieser Form, die uns vielleicht schon begegnet sind (und die wir zu gegebenener Zeit wiederholen), sind zum Beispiel:

- Ein Ringhomomorphismus $\mathbb{Z}[x] \to R$ ist "das gleiche" wie ein Element von $R$.
- Ein $K$-Vektorraumhomomorphismus $V \otimes W \to U$ ist "das gleiche" wie eine $K$-bilineare Abbildung $V \times W \to U$.

Andere universelle Eigenschaften charakterisieren ein Objekt über Abbildungen hinein, zum Beispiel definieren wir ein *Produkt* einer Familie $(x_i)$ von Objekten komplett dual:

**Definition 1.1.11.** *Für eine Familie von Objekten $(x_i)_{i\in I}$ in $\mathcal{C}$ ist ein Produkt ein Objekt $y$ mit Abbildungen $p_i : y \to x_i$ sodass für jedes andere Objekt $z$ mit Abbildungen $f_i : z \to x_i$ ein eindeutiges $h : z \to y$ existiert mit $f_i = p_i \circ h$ für alle $i$.*

Der Vorteil darin, Konstruktionen durch universelle Eigenschaften zu charakterisieren, ist dass es nicht darauf ankommt wie genau man sie baut. Zum Beispiel gibt es verschiedene Arten, "die" disjunkte Vereinigung von Mengen $(X_i)$ zu bauen, die universelle Eigenschaft des Koprodukts liefert kanonische Isomorphismen zwischen ihnen.

**Beispiel 1.1.12** (Freie Moduln)**.** Für einen Ring $R$ und eine Menge $I$ haben wir das Koprodukt

$$\coprod_{i\in I} R = \bigoplus_{i\in I} R.$$

in $\mathrm{LMod}_R$. Wir schreiben $e_i$ für das Bild von 1 unter $\iota_i : R \to \bigoplus_{i\in I} R$. Elemente von $\bigoplus_{i\in I} R$ lassen sich also eindeutig schreiben als endliche Linearkombinationen der $e_i$, mit $R$-Koeffizienten. Wir nennen $\bigoplus_{i\in I} R$ auch den *freien $R$-(Links)modul auf den Erzeugern $e_i$*, und schreiben auch $R\{(e_i)_{i\in I}\}$. Er erfüllt die folgende universelle Eigenschaft: $R\{(e_i)_{i\in I}\}$ enthält eine Familie von Elementen $(e_i)_{i\in I}$, und für jeden anderen Modul $M$ mit Elementen $(m_i)_{i\in I}$ existiert eine eindeutige Abbildung

$$f : R\{(e_i)_{i\in I}\} \to M$$

mit $f(e_i) = m_i$.

Wie in den Übungsaufgaben gesehen, ist ein Koprodukt einer Familie von Moduln $M_i$ gegeben durch den Untermodul $\bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i$ bestehend aus allen $(m_i)_{i\in I}$ wo alle bis auf endlich viele Einträge $m_i$ null sind. Insbesondere stimmen *endliche* Koprodukte in $\mathrm{LMod}_R$ (und $\mathrm{RMod}_R$) mit Produkten überein! Endliche direkte Summen haben also zwei universelle Eigenschaften:

1. Um eine Abbildung $\bigoplus_{i\in I} M_i \to N$ zu beschreiben, genügt es, eine Familie von Abbildungen $f_i : M_i \to N$ auf den Summanden zu spezifizieren.
2. Um eine Abbildung $N \to \bigoplus_{i\in I} M_i$ für endliches $I$ zu beschreiben, genügt es, eine Familie von Abbildungen $f_i : N \to M_i$ in die einzelnen Faktoren zu spezifizieren.

Das können wir kombinieren wie folgt:

**Lemma 1.1.13.** *Seien $(M_j)_{j\in J}$ und $(N_i)_{i\in I}$ endliche Familien von $R$-Moduln. Dann sind Abbildungen*

$$f : \bigoplus_{j\in J} M_j \to \bigoplus_{i\in I} N_i$$

*in Bijektion mit Familien $(f_{ij})_{(i,j)\in I\times J}$ wo $f_{ij} : M_j \to N_i$.*

*Beweis.* Mit der universellen Eigenschaft des Koprodukts ist ein $f : \bigoplus_{j\in J} M_j \to \bigoplus_{i\in I} N_i$ das gleiche wie eine Familie von Abbildungen

$$f_j : M_j \to \bigoplus_{i\in I} N_i.$$

Mit der universellen Eigenschaft des Produkts ist das wiederum das gleiche wie eine Familie

$$f_{ij} : M_j \to N_i,$$

wie behauptet. □

**Beispiel 1.1.14.** Für freie Moduln $R^n = \bigoplus_{i=1}^n R$ auf endlich vielen Erzeugern erhalten wir dass wir einen Homomorphismus $R^m \to R^n$ beschreiben können durch eine $n \times m$-Matrix, deren Einträge Homomorphismen $R \to R$ sind. Diese wiederum sind in Bijektion zu Elementen von $R$. (Das schauen wir uns in einer Übungsaufgabe auch genauer an.)

## 1.2 Zerlegungen von Moduln

In linearer Algebra haben wir Moduln über Vektorräumen klassifiziert:

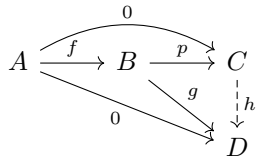
**Theorem 1.2.1** (Lineare Algebra, Existenz von Basen)**.** *Jeder $K$-Modul ist isomorph zu $\bigoplus_{i\in I} K$ für eine Menge $I$.*

In diesem Abschnitt widmen wir uns der Frage, in welcher Allgemeinheit wir Moduln über einem beliebigen Ring entsprechend zerlegen können. Beliebige Moduln haben natürlich nicht mehr unbedingt Basen (z.B. ist der $\mathbb{Z}$-Modul $\mathbb{Z}/3\mathbb{Z}$ nicht von der Form $\bigoplus_{i\in I} \mathbb{Z}$). Unsere Version für allgemeine Ringe wird so aussehen, dass wir geeignet "endliche" Moduln in kleinere Bausteine zerlegen. Wir betrachten zunächst einen Begriff von "Zerlegung", der etwas schwächer als direkte Summen ist.

Analog zur linearen Algebra haben wir für einen Modul $M$ mit Untermodul $N \subseteq M$ den Quotient (oder Faktormodul) $M/N$, definiert als Menge der Äquivalenzklassen nach $x \sim y \Leftrightarrow x - y \in N$. Dieser erfüllt ebenfalls eine universelle Eigenschaft:

**Definition 1.2.2.** *Sei $f : A \to B$ ein Morphismus von R-Moduln. Ein* Kokern *von $f$ ist ein Modul $C$ mit Morphismus $p : B \to C$, sodass:*

1. *$p \circ f = 0$*
2. *Für jeden anderen Modul $D$ mit Morphismus $g : B \to D$ mit $g \circ f = 0$ existiert ein eindeutiges $h : C \to D$ mit $h \circ p = g$.*




**Lemma 1.2.3.** *Für $f : A \to B$ ist $B/f(A)$ mit der kanonischen Projektion $p : B \to B/f(A)$ ein Kokern von $f$, also existieren Kokerne (und sind eindeutig bis auf kanonischen Isomorphismus).*

*Beweis.* Gegeben $g : B \to D$ mit $g \circ f = 0$, müssen wir ein $h : B/f(A) \to D$ mit $h \circ p = g$ finden. Wenn $[x] \in B/f(A)$ die Äquivalenzklasse von $x \in B$ bezeichnet, dann muss bereits $h([x]) = g(x)$ sein, also ist $h$ eindeutig festgelegt. Aus $g \circ f = 0$ folgt Wohldefiniertheit.

Also ist die universelle Eigenschaft des Kokerns erfüllt. Eindeutigkeit folgt mit dem gleichen Argument wie bei Koprodukten. □

Dual erhalten wir die universelle Eigenschaft des *Kerns*, von der man leicht überprüft dass sie vom Kern im üblichen Sinn erfüllt ist.

**Beispiel 1.2.4** (Präsentation eines Moduls)**.** Oft beschreiben wir algebraische Objekte durch *Erzeuger* und *Relationen*. Wir haben schon den freien Modul auf einer Menge $I$ von Erzeugern $e_i$ kennengelernt, dieser war gegeben durch $\bigoplus_{i \in I} R$. Gegeben eine Familie $(r_j)_{j \in J}$ von Linearkombinationen der $e_i$, also Elementen $r_j \in \bigoplus_{i \in I} R$, so ist der *R-Modul mit Erzeugern $e_i$ und Relationen $r_j$* gegeben durch den Kokern

$$R\{(e_i)_{i \in I} | (r_j)_{j \in J}\} = \operatorname{coker}\left( \bigoplus_{j \in J} R \xrightarrow{(r_j)} \bigoplus_{i \in I} R \right).$$

Er lässt sich auch beschreiben durch die folgende universelle Eigenschaft: $R\{(e_i)_{i \in I} | (r_j)_{j \in J}\}$ enthält Elemente $e_i$ die die Relationen $r_j$ erfüllen, und für jeden anderen Modul $M$ mit einer Liste von Elementen $m_i$ die dieselben Relationen erfüllen gibt es eine eindeutige Abbildung

$$f : R\{(e_i)_{i \in I} | (r_j)_{j \in J}\} \to M$$

mit $f(e_i) = m_i$.

Zum Beispiel ist $\mathbb{Z}\{x | 3x\}$ isomorph zu $\mathbb{Z}/3$.

**Definition 1.2.5.** *Eine* exakte Folge *von R-Linksmoduln ist ein Diagramm*

$$\ldots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \ldots$$

*sodass an jeder Stelle* $\ker(f_i) = \operatorname{im}(f_{i-1})$. *Eine* kurze exakte Folge *ist eine exakte Folge der Form*

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

*Wenn nur* $0 \to M_1 \to M_2 \to M_3$ *exakt ist, nennen wir die Folge linksexakt, analog rechtsexakt.*

**Lemma 1.2.6.** *Für ein Diagramm*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

*gilt:*

1. *Die Folge ist linksexakt genau wenn* $g \circ f = 0$ *und* $M_1$ *mit der Abbildung* $f : M_1 \to M_2$ *ist ein Kern von* $g$. *(Äquivalent: Die Abbildung* $M_1 \to \ker(g)$ *ist ein Isomorphismus)*

2. *Die Folge ist rechtsexakt genau wenn* $g \circ f = 0$ *und* $M_3$ *mit der Abbildung* $g : M_2 \to M_3$ *ist ein Kokern von* $f$. *(Äquivalent: Die Abbildung* $\operatorname{coker}(f) \to M_3$ *ist ein Isomorphismus)*

*Beweis.* Linksexaktheit der Folge ist gleichbedeutend damit dass $M_1 \to M_2$ injektiv mit Bild $\ker(g)$ ist, also dass $M_1 \to \ker(g)$ ein Isomorphismus ist.

Rechtsexaktheit der Folge ist gleichbedeutend damit dass $M_2 \to M_3$ surjektiv mit Kern $\operatorname{im}(f)$ ist, also dass $M_2/\operatorname{im}(f) \to M_3$ ein Isomorphismus ist. □

Wir können eine kurze exakte Folge $0 \to A \to B \to C \to 0$ also so lesen dass wir einen Untermodul $A$ in $B$ haben, sodass der Quotient $B/A$ durch $C$ gegeben ist. Gewissermaßen wird also $B$ in $A$ und $C$ zerlegt, und in dieser Situation bezeichnen wir $B$ als *Erweiterung von* $C$ *durch* $A$. Rein die Kenntnis von $A$ und $C$ legt die Erweiterung nicht fest, zum Beispiel gibt es exakte Folgen

$$0 \to \mathbb{Z}/2 \xrightarrow{2} \mathbb{Z}/4 \to \mathbb{Z}/2 \to 0$$

$$0 \to \mathbb{Z}/2 \xrightarrow{\binom{1}{0}} \mathbb{Z}/2 \oplus \mathbb{Z}/2 \xrightarrow{(01)} \mathbb{Z}/2 \to 0.$$

Allerdings gilt folgendes wichtiges Lemma:

**Lemma 1.2.7** (5-Lemma)**.** *Wenn in einem Diagramm von Moduln*

$$\begin{array}{ccccccccc} A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & D_2 & \longrightarrow & E_2 \end{array}$$

*die Zeilen exakt, und alle bis auf den mittleren vertikalen Morphismus Isomorphismen sind, so ist auch der mittlere Morphismus ein Isomorphismus.*

*Insbesondere erhalten wir für $A_1 = A_2 = E_1 = E_2 = 0$, dass eine Abbildung zwischen kurzen exakten Folgen, die ein Isomorphismus auf den äußeren Termen ist, auch ein Isomorphismus auf den mittleren Termen ist.*

*Beweis.* Wir zeigen erst Injektivität: Sei $c_1 \in C_1$, mit Bild in $C_2$ gegeben durch 0. Da $D_1 \to D_2$ ein Isomorphismus ist, folgt dass $c_1 \mapsto 0 \in D_1$, also existiert wegen Exaktheit ein $b_1 \in B_1$ mit $b_1 \mapsto c_1$. Jetzt $b_1 \mapsto b_2 \in B_2$, und $b_2 \mapsto 0 \in C_2$, also existiert ein $a_2 \in A_2$ mit $a_2 \mapsto b_2$, und weil $A_1 \to A_2$ ein Isomorphismus ist, auch ein $a_1 \in A_1$ mit $a_1 \mapsto a_2 \in A_2$. Da sowohl $b_1$ als auch das Bild von $a_1$ in $B_1$ auf $b_2$ in $B_2$ abbilden, und $B_1 \to B_2$ ein Isomorphismus ist, ist $a_1 \mapsto b_1$, und wegen Exaktheit somit $b_1 \mapsto c_1 = 0$ wie gewünscht.

Für Surjektivität beginnen wir mit einem $c_2 \in C_2$. Das Bild $d_2 \in D_2$ besitzt ein Urbild $d_1 \in D_1$. Da $d_2 \mapsto 0 \in E_2$, und $E_1 \to E_2$ ein Isomorphismus ist, ist $d_1 \mapsto 0 \in E_1$. Also finden wir ein $c_1 \in C_1$ mit $c_1 \mapsto d_1$. Bezeichnen wir das Bild von $c_1$ in $C_2$ mit $c_2'$, so würde man hoffen dass $c_2 = c_2'$. Das wissen wir aber nicht, wir haben nur dass $c_2 - c_2' \mapsto 0 \in D_2$, da nach Konstruktion beide auf $d_2$ abbilden. Also finden wir ein $b_2 \in B_2$ mit $b_2 \mapsto c_2 - c_2'$. Da $B_1 \to B_2$ ein Isomorphismus ist, finden wir nun ein Urbild $b_1$, und wir bezeichnen dessen Bild in $C_1$ mit $h$. $c_1 + h$ bildet nun wie gewünscht auf $c_2' + (c_2 - c_2') = c_2 \in C_2$ ab. □

**Lemma 1.2.8.** *Sei $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ eine kurze exakte Folge. Die folgenden Aussagen sind äquivalent:*

1. *Es existiert ein $s : C \to B$ mit $g \circ s = \mathrm{id}_C$.*
2. *Es existiert ein $r : B \to A$ mit $r \circ f = \mathrm{id}_A$.*
3. *Es existiert ein Isomorphismus $B \cong A \oplus C$, sodass das Diagramm*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\ 0 & \longrightarrow & A & \xrightarrow[\binom{\mathrm{id}_A}{0}]{} & A \oplus C & \xrightarrow[(0\,\mathrm{id}_C)]{} & C & \longrightarrow & 0 \end{array}$$

*kommutiert, wo $i$ und $p$ die kanonische Inklusion bzw. Projektion sind.*

*Beweis.* Wir zeigen zunächst 2 ⇔ 3. Eine Abbildung $B \to A \oplus C$ für die das Diagramm aus 3 kommutiert is gegeben durch $\binom{r}{g}$, mit $r \circ f = \mathrm{id}_A$. Also ist 2 äquivalent zu 3 ohne die Bedingung dass $B \to A \oplus C$ ein Isomorphismus ist, diese ist aber automatisch aufgrund des Fünferlemmas.

Für 1 ⇔ 3 gehen wir genau so vor, wir lesen das Diagramm in 3 aber von unten nach oben, konstruieren also eine Abbildung $A \oplus C \to B$. □

Wir sagen eine kurze exakte Folge *spaltet* wenn eine der äquivalenten Bedingungen oben erfüllt ist. In dem Fall bezeichnen wir $B$ auch als *triviale Erweiterung* von $C$ durch $A$.

**Beispiel 1.2.9.** 1. In $\mathrm{LMod}_K$ für einen Körper $K$ spaltet jede kurze exakte Folge (Basisergänzungssatz!)

2. Über den meisten anderen Ringen ist das falsch, man betrachte zum Beispiel die Folge von $\mathbb{Z}$-Moduln

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

**Definition 1.2.10.** *Für $R$-Moduln $A, C$ definieren wir $\mathrm{Ext}^1(C, A)$ als Menge der Isomorphieklassen von Erweiterungen von $C$ durch $A$. Genauer sind Elemente repräsentiert durch kurze exakte Folgen*

$$0 \to A \to B \to C \to 0,$$

*und zwei solcher Sequenzen repräsentieren das gleiche Element wenn es ein Diagramm*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \longrightarrow & B' & \longrightarrow & C & \longrightarrow & 0, \end{array}$$

*gibt. (Die mittlere Abbildung ist automatisch ein Isomorphismus).*

Strikt gesprochen ist nicht klar dass diese Äquivalenzklassen tatsächlich eine Menge bilden (die Kollektion aller $R$-Moduln bildet ja keine Menge, genauso wie es keine "Menge aller Mengen" gibt). Die nächste Aussage beweist aber insbesondere, dass es sich um eine Menge handelt:

**Proposition 1.2.11.** *Seien $A, C$ $R$-Moduln, und $F$ ein freier Modul mit surjektiver Abbildung $F \to C$. Sei $K$ der Kern. Dann gibt es eine Bijektion*

$$\mathrm{coker}(\mathrm{Hom}(F, A) \to \mathrm{Hom}(K, A)) \cong \mathrm{Ext}^1(C, A)$$

*Beweis.* Um die Bijektion explizit zu machen führen wir temporär Terminologie ein: Wir nennen eine Erweiterung von $0 \to A \to B \to C \to 0$ und eine Abbildung $K \to A$ assoziiert zueinander wenn es ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & F & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \vdots & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

gibt. Wir beobachten:

1. Für jede Erweiterung existiert eine assoziierte Abbildung, und diese ist eindeutig bis auf addieren von Einschränkungen von Homomorphismen $F \to B$. Wir müssen ja eine Abbildung $F \to B$ wählen, die $F \to C$ liftet (das geht, weil wir einfach nur für jeden Erzeuger in $F$ ein Urbild seines Bildes in $C$ wählen müssen), und dann ist $K \to A$ bereits als Einschränkung eindeutig festgelegt. Wenn wir den Lift anders wählen, unterscheiden sich die beiden Lifts um eine Abbildung $F \to A$.

2. Die Abbildung legt die assoziierte Erweiterung bis auf Isomorphismus eindeutig fest. Und zwar behaupten wir dass $B \cong (F \oplus A)/K$, wo $F \oplus A \to B$ mittels der Differenz der beiden Abbildungen $F \to B$ und $A \to B$ abbildet, und $K \to F \oplus A$ diagonal. Hierfür wenden wir das Fünferlemma auf

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & (F \oplus A)/K & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

an.

Insgesamt erhalten wir also eine Bijektion

$$\mathrm{Ext}^1(C, A) \cong \mathrm{coker}(\mathrm{Hom}(F, A), \mathrm{Hom}(K, A)).$$

□

**Bemerkung 1.2.12.** Es gibt auch höhere $\mathrm{Ext}^i$, die durch eine lange exakte Folge zusammenhängen, die obige Aussage verallgemeinert. Diese sind zentrales Objekt der *Homologischen Algebra* (die uns in der Vorlesung nur oberflächlich begegnen wird, aber zu der es parallel ein Seminar gibt!)

**Beispiel 1.2.13.**

1. Über $\mathbb{Z}$ ist $\mathrm{Ext}(\mathbb{Z}/n, \mathbb{Z}) = \mathbb{Z}/n$. Insbesondere gibt es $n$ Äquivalenzklassen von Erweiterungen von $\mathbb{Z}/n$ durch $\mathbb{Z}$. (Achtung, verschiedene Klassen in $\mathrm{Ext}(C, A)$ können abstrakt isomorphe $B$ haben!)

2. Über einem Körper ist jeder Modul frei, also können wir in der obigen Diskussion $F = C$ und $K = 0$ wählen, und lernen $\mathrm{Ext}(C, A) = 0$. Das korrespondiert zu der Beobachtung dass jede kurze exakte Folge spaltet, und alle Vektorräume wirklich direkte Summen sind.

Wie soll man sich diese Klassifikation von Erweiterungen vorstellen? Gegeben eine Präsentation eines Moduls in Termen von Erzeugern und Relationen, $C = F/K$, wo $F$ ein freier Modul und $K$ ein Untermodul davon ist, so gelten die Relationen, die durch Elemente in $K$ kodiert werden, in $B$ nur noch "mod $A$". Somit misst für eine Erweiterung $A \to B \to C$ die Abbildung $K \to A$ welche der Relationen in $B$ immer noch gelten. Wenn alle Relationen in $B$ immer noch gelten, also wir eine wohldefinierte Abbildung $C \to B$ erhalten, spaltet die Sequenz. Das ist genau der Fall wenn $K \to A$ null ist. (Zumindest modulo $\mathrm{Hom}(F, A)$.)

Wir verstehen jetzt also ungefähr auf wie viele Weisen man aus zwei Moduln einen größeren bauen kann, oder zumindest dass man das im Prinzip für gegebene Moduln berechnen kann. Jetzt wollen wir verstehen, was die Bausteine hierfür sind.

**Definition 1.2.14.** *Ein Modul $M$ heißt* einfach*, wenn er nicht null ist, und für jeden Untermodul $N \subseteq M$ gilt $N = 0$ oder $N = M$.*

Die einfachen Moduln sind also genau die die sich nur auf triviale Weise als Erweiterung schreiben lassen. Zum Beispiel sind über einem Körper genau die 1-dimensionalen Vektorräume einfache Moduln.

**Proposition 1.2.15.** *Jeder einfache $R$-Linksmodul ist isomorph zu $R/I$ für einen maximalen echten Unter-Linksmodul $I \subseteq R$ (ein maximales* Linksideal *in $R$).*

*Beweis.* Sei $M$ einfach und $x \in M$ mit $x \neq 0$. Dann ist die Abbildung $R \to M$, die $1 \mapsto x$ schickt, surjektiv: Ihr Bild ist ein nichttrivialer Untermodul von $M$, der also ganz $M$ sein muss. Sei $I$ der Kern, dann ist also $M \cong R/I$. Wenn $I$ jetzt kein maximaler echter Untermodul wäre, es also ein $I' \supsetneq I$ gäbe, dann wäre $I'/I$ ein nichttrivialer echter Untermodul von $R/I$, im Widerspruch dazu dass $M$ einfach ist. □

Über $\mathbb{Z}$ zum Beispiel sind die einfachen Moduln genau $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen $p$. Allgemeiner ist über einem kommutativen Ring ein Linksideal $I$ wie oben bereits auch ein Rechtsideal, sodass $R/I$ eine wohldefinierte Ringstruktur hat, Maximalität von $I$ bedeutet dann dass $R/I$ ein Körper ist. Dazu später mehr, wenn wir uns Ideale genauer anschauen.

Unser Ziel ist es nun, Moduln in einfache Moduln zu zerlegen.

**Definition 1.2.16.** *Sei $M$ ein $R$-Modul. Eine* Kompositionsreihe *ist eine Folge von Untermoduln*

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_{n-1} \subseteq M_n = M$$

*sodass alle Quotienten $M_i/M_{i-1}$ einfache Moduln sind.*

**Beispiel 1.2.17.** Jeder endlichdimensionale Vektorraum besitzt eine Kompositionsreihe, deren Länge gleich der Dimension ist.

**Definition 1.2.18.** *Ein Modul heißt*

1. Noethersch*, wenn jede aufsteigende Folge*

   $$\ldots \subseteq M_i \subseteq M_{i+1} \subseteq \ldots$$

   *von Untermoduln stabil wird, also $M_i = M_{i+1}$ für $i > I$.*

2. Artinsch*, wenn jede absteigende Folge*

   $$\ldots \supseteq M_i \supseteq M_{i+1} \supseteq \ldots$$

   *von Untermoduln stabil wird, also $M_i = M_{i+1}$ für $i > I$.*

3. Modul endlicher Länge*, wenn er Noethersch und Artinsch ist.*

**Lemma 1.2.19.** *Ein Modul $M$ ist*

1. *Noethersch, genau wenn jede nichtleere Menge von Untermoduln von $M$ ein maximales Element besitzt.*

2. *Artinsch, genau wenn jede nichtleere Menge von Untermoduln von $M$ ein minimales Element besitzt.*

*Beweis.* Wir beweisen die erste Aussage, die zweite geht komplett analog. Sei $M$ Noethersch und $S$ eine nichtleere Menge von Untermoduln von $M$. Angenommen, es gibt kein maximales Element in $S$, dann muss es ja für jedes $N \in S$ ein $N' \in S$ mit $N' \supsetneq N$ geben. Wir erhalten induktiv eine unendliche Folge von ineinander echt enthaltenen Untermoduln, im Widerspruch zu Noethersch. Das beweist eine Richtung der ersten Aussage, die andere ist trivial. □

**Lemma 1.2.20.** *Sei $0 \to A \to B \to C \to 0$ eine kurze exakte Folge von Moduln. Dann gilt:*

1. *$B$ ist Noethersch genau dann wenn $A$ und $C$ Noethersch sind.*
2. *$B$ ist Artinsch genau dann wenn $A$ und $C$ Artinsch sind.*

*Beweis.* Wir beweisen die erste Aussage, die zweite geht analog. Sei zunächst $B$ Noethersch. Wir haben eine bijektive Korrespondenz zwischen Untermoduln von $A$, und Untermoduln von $B$, die im Bild von $A \to B$ enthalten sind. Gegeben irgendeine Folge von aufsteigenden Untermoduln von $A$, so stabilisiert sich die korrespondierende Folge von Untermoduln in $B$, also auch die ursprüngliche, somit ist $A$ Noethersch. Genauso haben wir eine Korrespondenz zwischen Untermoduln von $C$ und Untermoduln von $B$, die $A$ enthalten (via Urbild nehmen). Für eine aufsteigende Folge von Untermoduln von $C$ stabilisiert sich die korrespondierende Folge von Untermoduln in $B$, also wiederum die ursprüngliche Folge in $C$, somit ist auch $C$ Noethersch.

Für die Umkehrung seien $A$ und $C$ Noethersch, und

$$\ldots \subseteq B_i \subseteq B_{i+1} \subseteq \ldots$$

eine Folge von Untermoduln von $B$. Sei $C_i$ das Bild von $B_i$ unter $B \to C$, und sei $A_n$ der Kern von $B_i \to C_i$ (identifiziert mit einem Untermodul von $A$, entlang des Isomorphismus $A \to \mathrm{im}(A \to B)$). Wir haben also eine Folge von exakten Folgen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_{i+1} & \longrightarrow & B_{i+1} & \longrightarrow & C_{i+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
\end{array}$$

wo die $A_i$ Untermoduln von $A$, und die $C_i$ Untermoduln von $C$ sind. Da $A$ und $C$ noethersch sind gibt es ein $I$ sodass für $i \geq I$ die vertikalen Abbildungen außen Isomorphismen sind. Nach Fünferlemma also auch die innen, somit ist auch $B$ Noethersch. □

**Proposition 1.2.21.** *Ein Modul besitzt genau dann eine Kompositionsreihe, wenn er von endlicher Länge ist.*

*Beweis.* Sei $M$ von endlicher Länge. In der partiell geordneten Menge der echten Untermoduln von $M$ gibt es maximale Elemente. Sei $M_1$ eines davon. Dann ist $M/M_1$ ein einfacher Modul, weil für einen echten Untermodul $N \subseteq M/M_1$ das Urbild in $M$ echt zwischen $M_1$ und $M$ liegen würde. Induktiv konstruieren wir so eine Folge von jeweils ineinander maximalen Untermoduln

$$\dots M_2 \subsetneq M_1 \subsetneq M$$

wo alle Quotienten einfache Moduln sind. Weil $M$ Artinsch ist muss diese Konstruktion irgendwann aufhören, das passiert nur wenn wir den Nullmodul erreichen, und dann haben wir eine Kompositionsreihe für $M$ gefunden.

Für die Umkehrung beobachten wir, dass wenn in einer Erweiterung

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

sowohl $A$ als auch $C$ Moduln endlicher Länge sind, auch $B$ von endlicher Länge ist. Einfache Moduln sind offenbar von endlicher Länge, und wenn ein Modul eine Kompositionsreihe hat lässt er sich induktiv als Erweiterung von Moduln endlicher Länge schreiben, also folgt die Aussage. □

**Beispiel 1.2.22.** Die Folge der Quotienten $M_i/M_{i-1}$ in einer Kompositionsreihe ist nicht eindeutig, wir wir am Beispiel $M = \mathbb{Z}/6$ über $\mathbb{Z}$ sehen. Hier haben wir eine Kompositionsreihe

$$0 \subseteq \mathbb{Z}/2 \subseteq \mathbb{Z}/6$$

mit Quotienten $\mathbb{Z}/2$ und $\mathbb{Z}/3$, sowie eine Kompositionsreihe

$$0 \subseteq \mathbb{Z}/3 \subseteq \mathbb{Z}/6$$

mit Quotienten $\mathbb{Z}/3$ und $\mathbb{Z}/2$.

**Lemma 1.2.23** (Schur)**.** *Seien $M$, $N$ einfache Moduln und $f : M \to N$ ein Morphismus. Dann ist entweder $f = 0$, oder $f$ ist ein Isomorphismus.*

*Beweis.* $f(M)$ ist ein Untermodul von $N$, also entweder 0 oder ganz $N$. Genauso ist der Kern von $f$ entweder 0 oder ganz $M$. Wenn $f$ also nicht 0 ist, ist $f$ bereits surjektiv und injektiv. □

**Theorem 1.2.24** (Jordan-Hölder)**.** *Sei $M$ ein Modul endlicher Länge. Dann haben je zwei Kompositionsreihen die gleiche Länge, und bis auf Umordnung die gleichen Quotienten.*

*Beweis.* Seien

$$0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_n = M$$

und

$$0 = M'_0 \subseteq M'_1 \subseteq \dots \subseteq M'_m = M$$

zwei verschiedene Kompositionsreihen von $M$.

Wir bilden ein $(n+1) \times (m+1)$-Diagramm von Moduln $M_{ij}$, mit $M_{ij} = M_i \cap M'_j$. Wir beobachten nun: In jedem Quadrat

$$\begin{array}{ccc} M_{ij} & \longrightarrow & M_{i(j+1)} \\ \downarrow & & \downarrow \\ M_{(i+1)j} & \longrightarrow & M_{(i+1)(j+1)} \end{array}$$

gilt:

1. Die Abbildung $M_{(i+1)j}/M_{ij} \to M_{(i+1)(j+1)}/M_{i(j+1)}$ ist injektiv,
2. die Abbildung $M_{i(j+1)}/M_{ij} \to M_{(i+1)(j+1)}/M_{(i+1)j}$ ist injektiv,
3. die eine Abbildung ist ein Isomorphismus genau dann wenn die andere Abbildung ebenfalls ein Isomorphismus ist. Beides ist nämlich äquivalent dazu dass $M_{(i+1)j}$ und $M_{i(j+1)}$ zusammen $M_{(i+1)(j+1)}$ erzeugen.

In unserem Diagramm sind also alle Quotienten null oder einfache Moduln, und für jedes Quadrat gibt es nur zwei Möglichkeiten:

1. Sowohl die horizontalen Quotienten als auch die vertikalen Quotienten stimmen überein.
2. Die Morphismen aus der linken oberen Ecke sind beides Isomorphismen. In dem Fall stimmen die Quotienten der beiden anderen Morphismen ebenfalls überein.

In beiden Fällen sehen wir entlang eines Pfads von der linken oberen Ecke zur rechten unteren Ecke die gleichen Isomorphietypen von einfachen Moduln als Quotienten. Insgesamt gilt das also auch für das große Diagramm. □

Insbesondere ist die "Länge" in "Modul endlicher Länge" eine wohldefinierte Zahl!

Wir wollen nun noch Zerlegungen in direkte Summen betrachten.

**Definition 1.2.25.** *Sei $M$ ein Modul. Ein Untermodul $N \subseteq M$ heißt* direkter Summand von $M$*, wenn es einen Untermodul $N' \subseteq M$ gibt, für den die kanonische Abbildung*

$$N \oplus N' \to M$$

*ein Isomorphismus ist. Wir nennen $N'$ auch ein* Komplement *von $N$.*

Explizit bedeutet Surjektivität der Abbildung $N \oplus N' \to M$, dass jedes Element von $M$ eine Linearkombination von Elementen von $N$ und $N'$ ist, also dass $N$ und $N'$ $M$ erzeugen. Injektivität bedeutet, dass $N \cap N' = 0$.

**Lemma 1.2.26.** *Ein Untermodul $N \subseteq M$ ist direkter Summand von $M$ genau dann wenn es ein $r : M \to N$ mit $r \circ i = \mathrm{id}$ gibt, wo $i : N \to M$ die Inklusionsabbildung ist.*

*Beweis.* Wenn es ein solches $r$ gibt, dann spaltet die kurze exakte Folge

$$0 \to N \to M \to M/N \to 0,$$

also ist $M \cong N \oplus M/N$ und $N$ ist direkter Summand von $M$. Umgekehrt gibt es wenn $M \cong N \oplus N'$ ist ja auch ein $r$, nämlich die Projektion $M \cong N \oplus N' \to N$. □

**Definition 1.2.27.** *Ein Modul $M$ heißt* unzerlegbar*, wenn er keine nichttrivialen direkten Summanden besitzt, genauer: Wenn aus $N, N' \subseteq M$ mit $N \oplus N' \cong M$ bereits folgt dass $N = 0$ oder $N' = 0$.*

**Beispiel 1.2.28.**

1. Einfache Moduln sind unzerlegbar.
2. $\mathbb{Z}$ als $\mathbb{Z}$-Modul ist unzerlegbar: Nichttriviale Untermoduln sind von der Form $n\mathbb{Z}$, und $n\mathbb{Z} \cap m\mathbb{Z} \neq 0$, da $nm$ darin enthalten ist.

**Definition 1.2.29.** *Sei $M$ ein Modul. Ein Morphismus*

$$e : M \to M$$

*heißt* idempotent*, wenn $e \circ e = e$.*

**Proposition 1.2.30.** *Sei $M$ ein Modul. Zerlegungen von $M$ sind in Bijektion mit idempotenten Abbildungen $e : M \to M$.*

*Beweis.* Sei $M' \oplus M'' \cong M$ eine Zerlegung von $M$. Wir erhalten eine idempotente Abbildung $e : M \to M$ über das kommutative Diagramm

$$\begin{array}{ccc} M' \oplus M'' & \xrightarrow{\begin{pmatrix} \mathrm{id} & 0 \\ 0 & 0 \end{pmatrix}} & M' \oplus M'' \\ \downarrow \cong & & \downarrow \cong \\ M & \xrightarrow{\quad e \quad} & M. \end{array}$$

Umgekehrt ist für eine idempotente Abbildung $e : M \to M$ auch $\mathrm{id} - e$ idempotent, da

$$(\mathrm{id} - e) \circ (\mathrm{id} - e) = \mathrm{id} - e - e + e \circ e = \mathrm{id} - e,$$

und wir behaupten, dass die Bilder $e(M)$ und $(\mathrm{id} - e)(M)$ eine Zerlegung von $M$ bilden, also $e(M) \oplus (\mathrm{id} - e)(M) \cong M$. Die beiden Bilder erzeugen $M$, da $m = e(m) + (\mathrm{id} - e)(m)$, und wir haben $e(M) \cap (\mathrm{id} - e)(M) = 0$, da wenn $e(x) = (\mathrm{id} - e)(y)$, dann ist

$$e(x) = e(e(x)) = e(y - e(y)) = e(y) - e(e(y)) = 0.$$

□

**Bemerkung 1.2.31.** Da $R$-Linksmodulhomomorphismen $f : R \to R$ von der Form $f(x) = xr$ für ein Element $r \in R$ sind, sind idempotente Homomorphismen $R \to R$ das gleiche wie idempotente *Elemente* von $R$, also Elemente $e \in R$ mit $e^2 = e$. Diese Gleichung ist äquivalent zu $(1-e)e = 0$. Wenn $R$ *nullteilerfrei* ist, also Produkte von Elementen die nicht 0 sind wieder nicht 0 sind, so hat diese Gleichung nur die trivialen Lösungen $e = 0$ und $e = 1$, und $R$ ist unzerlegbar als $R$-Modul.

Ähnlich wie bei einfachen Moduln und Erweiterungen fragen wir uns jetzt, wann sich Moduln als direkte Summe von unzerlegbaren Moduln schreiben lassen.

**Definition 1.2.32.** *Ein Modul $M$ heißt* vollständig zerlegbar*, wenn es eine Familie von unzerlegbaren Untermoduln $(M_i)_{i\in I}$ gibt, für die die kanonische Abbildung*

$$\bigoplus_{i\in I} M_i \to M$$

*ein Isomorphismus ist.*

**Theorem 1.2.33.** *Sei $M$ Noethersch* oder *Artinsch. Dann ist $M$ vollständig zerlegbar, in endlich viele Untermoduln.*

*Beweis.* Wir nehmen zunächst an, dass $M$ Noethersch ist. Wenn $M$ nicht 0 ist, so können wir unter allen direkten Summanden von $M$, die echte Untermoduln sind, einen maximalen wählen, und wenn $N$ in $M = N \oplus N'$ maximal ist, dann muss $N'$ unzerlegbar sein. Falls nämlich $N' = N'_1 \oplus N'_2$, dann wäre $N \oplus N'_1$ ein echt größerer direkter Summand von $M$. Es folgt also dass jeder nichttriviale Noethersche Modul unzerlegbare direkte Summanden hat.

Nun wählen wir unter allen vollständig zerlegbaren Untermoduln von $M$, die direkte Summanden sind, einen maximalen. Sei die entsprechende Zerlegung wieder $M = N \oplus N'$. Wenn $N' = 0$, dann sind wir fertig. Andernfalls ist $N'$ Noethersch, besitzt also einen unzerlegbaren direkten Summanden $N'_1$. Dann ist $N \oplus N'_1$ ein vollständig zerlegbarer Untermodul von $M$ der echt größer als $N$ ist, Widerspruch.

Wenn $M$ Artinsch ist gehen wir ähnlich vor: Wenn $M \neq 0$, dann gibt es unter allen direkten Summanden von $M$, die nicht 0 sind, einen minimalen. Dieser ist wiederum unzerlegbar. Also besitzt jeder nichttriviale Artinsche Modul unzerlegbare direkte Summanden. Nun betrachten wir die Menge aller Untermoduln von $M$, die direkte Summanden sind, und ein vollständig zerlegbares Komplement haben, und wählen davon einen minimalen, $M = N \oplus N'$ mit $N'$ unzerlegbar. Falls $N = 0$ sind wir fertig. Andernfalls besitzt $N$ eine Zerlegung $N = N_1 \oplus N_2$ mit $N_1$ unzerlegbar, und dann ist $N_2$ ein echt kleinerer direkter Summand von $M$, der ebenfalls unzerlegbares Komplement hat. □

Im Gegensatz zum Fall von einfachen Moduln gilt hier keine Variante von Jordan-Hölder, die Summanden sind im allgemeinen nicht eindeutig bis auf Isomorphie. Auch handelt es sich um keine exakte Charakterisierung (was man

vielleicht auch an der seltsamen Bedingung "Noethersch *oder* Artinsch" erahnen kann), aber irgendeine Art von Endlichkeitsbedingung ist nötig, wie das folgende Beispiel zeigt.

**Beispiel 1.2.34.** Sei $C \subseteq \mathbb{R}$ die Cantormenge, bestehend aus allen Zahlen der Form $\sum_{i=1}^{\infty} a_i \frac{1}{3^i}$ wo alle $a_i \in \{0, 2\}$. Sei $R = C^0(C; \mathbb{R})$ der Ring, dessen Elemente *stetige* Funktionen $f : C \to \mathbb{R}$ sind, mit punktweiser Addition und Multiplikation. Dann besitzt $R$ (aufgefasst als $R$-Modul über sich selbst) keine unzerlegbaren Summanden.

*Beweis.* Direkte Summanden von $R$ korrespondieren zu idempotenten Elementen, also $f$ mit $f \cdot f = f$. So ein $f$ ist eine Funktion die nur die Werte 0 oder 1 annimmt. Angenommen $M$ ist ein nichttrivialer Summand von $R$, mit korrespondierender Idempotente $f$, also $M = f \cdot R$. Dann ist $f(c) = 1$ für irgendein $c$. Aufgrund von Stetigkeit existiert ein Intervall $(c_0, c_1) \ni c$ sodass $f$ auf ganz $(c_0, c_1) \cap C$ den Wert 1 annimmt. Wir wählen nun ein $a \in (c_0, c_1)$ mit $a \in C$, und so dass $(c_0, c_1) \cap C$ sowohl links als auch rechts von $a$ Elemente enthält. (Wähle $a$ dessen Dezimaldarstellung zur Basis 3 die Ziffer 1 enthält und das nah genug an $c$ liegt). Nun ist die Funktion $g : C \to \mathbb{R}$ mit

$$g(x) = \begin{cases} 1 \text{ wenn } x < a \\ 0 \text{ sonst} \end{cases}$$

stetig, und sowohl $f \cdot g$ als auch $f \cdot (1 - g)$ sind idempotent, und nicht 0. Wir sehen dass $f \cdot R \cong fg \cdot R \oplus (f \cdot (1-g)) \cdot R$, und somit war $M$ nicht unzerlegbar. □

Außerdem sind unzerlegbare Moduln viel "wilder" als einfache Moduln, die wir in 1.2.15 recht überschaubar klassifizieren konnten.

**Beispiel 1.2.35.** Über $\mathbb{Z}$ sind die Moduln $\mathbb{Z}$ und $\mathbb{Z}/p$ unzerlegbar, aber auch $\mathbb{Z}[1/p]$ oder $\mathbb{Q}$. Tatsächlich kann man beweisen, dass es *sehr viele* Isomorphieklassen von unzerlegbaren abelschen Gruppen gibt, nämlich mehr als jede beliebige Kardinalzahl $\kappa$.

Zum Abschluss betrachten wir noch eine Klasse von Moduln, die sich besonders schön zerlegen lässt:

**Definition 1.2.36.** *Ein Modul $M$ heißt* halbeinfach*, wenn er vollständig zerlegbar in einfache Moduln ist, also es existiert eine Familie von einfachen Untermoduln $(M_i)_{i \in I}$ für die die kanonische Abbildung*

$$\bigoplus M_i \to M$$

*ein Isomorphismus ist.*

In diesem Fall sind die Summanden tatsächlich (bis auf Reihenfolge) eindeutig festgelegt, im Fall von endlich vielen Summanden folgt dies z.B. aus dem Satz von Jordan-Hölder. Halbeinfache Moduln lassen sich schön intrinsisch charakterisieren. Dafür erinnern wir zunächst an das *Zornsche Lemma*:

**Lemma 1.2.37** (Zorn)**.** *Sei $P$ eine partiell geordnete Menge in der gilt: Für jede total geordnete Teilmenge $S \subseteq P$ existiert ein $x \in P$ mit $x \geq s$ für alle $s \in S$ ("Jede Kette hat eine obere Schranke"). Dann existiert ein maximales Element von $P$.*

**Lemma 1.2.38.** *Sei $M = \bigoplus_{i \in I} M_i$ halbeinfach und $N \subseteq M$ ein Untermodul. Dann existiert eine Teilmenge $J \subseteq I$ sodass die kanonische Abbildung $N \oplus \bigoplus_{i \in J} M_i \to M$ ein Isomorphismus ist.*

*Beweis.* Wir betrachten alle $J \subseteq I$ für die $N \cap \bigoplus_{i \in J} M_i = 0$. Wenn $J_s$ eine Kette von ineinander enthaltenen $J_s \subseteq I$ mit dieser Eigenschaft ist, dann hat auch $\bigcup J_s$ diese Eigenschaft, wegen $\bigoplus_{i \in \bigcup J_s} M_i = \bigcup_s \bigoplus_{i \in J_s} M_i$. Wir können also das Zornsche Lemma anwenden und erhalten ein maximales $J$ mit $N \cap \bigoplus_{i \in J} M_i = 0$. Äquivalent dazu handelt es sich auch um ein maximales $J$ mit der Eigenschaft dass die Komposition

$$N \to \bigoplus_{i \in I} M_i \to \bigoplus_{i \notin J} M_i$$

injektiv ist. Für jedes $j \notin J$ ist also die Komposition

$$N \to \bigoplus_{i \notin J} M_i \to \bigoplus_{i \notin J \cup \{j\}} M_i$$

nicht injektiv. Somit enthält das Bild von $N$ in $\bigoplus_{i \notin J} M_i$ einen nichttrivialen Untermodul von $M_j$ (der Kern der zweiten Projektion), also wegen Einfachheit der $M_j$ bereits $M_j$. Also ist die Abbildung $N \to \bigoplus_{i \notin J} M_i$ ein Isomorphismus, und die Komposition

$$M \to \bigoplus_{i \notin J} M_i \to N$$

spaltet die Inklusion $N \to M$, also ist $N$ direkter Summand mit Komplement $\bigoplus_{j \in J} M_i$. □

**Lemma 1.2.39.** *Sei $M$ ein Modul. Dann sind äquivalent:*

1. *$M$ ist halbeinfach.*
2. *$M$ wird erzeugt von seinen einfachen Untermoduln.*
3. *Jeder Untermodul $N \subseteq M$ ist direkter Summand.*

*Beweis von Lemma 1.2.39.* $1 \Rightarrow 3$: Sei $M$ halbeinfach und $N \subseteq M$ Untermodul. Nach dem vorherigen Lemma ist $N$ direkter Summand.

$3 \Rightarrow 2$: Sei $M$ ein Modul der 3 erfüllt. Dann erfüllt auch jeder Untermodul 3, weil für $M' \subseteq M$ und einen Untermodul $N \subseteq M'$ die Inklusion $N \to M$ ein linksinverses $r : M \to N$ besitzt, und dann die Komposition $M' \to M \to N$ auch ein linksinverses zu $N \to M'$ ist. Sei nun $M' \subseteq M$ der Untermodul, der von allen einfachen Untermoduln von $M$ erzeugt wird, und $M''$ ein Komplement. Wenn $M'' = 0$, so sind wir fertig. Wir nehmen an, dass $M'' \neq 0$, wenn

wir zeigen können dass $M''$ einen einfachen Untermodul enthält erhalten wir einen Widerspruch. Sei $0 \neq x \in M''$ ein Element und $R \cdot x$ der von $x$ erzeugte Untermodul. Dann sind die echten Untermoduln von $R \cdot x$ genau die, die $x$ nicht enthalten, und für eine Kette von Untermoduln die $x$ nicht enthalten liegt $x$ auch nicht in der Vereinigung. Also hat $R \cdot x$ einen maximalen echten Untermodul $N$ nach Zorn, und dann ist $R \cdot x/N$ einfach. Da $R \cdot x$ ebenfalls 3 erfüllt, ist $R \cdot x/N$ Summand von $R \cdot x$, und $M''$ enthält einen einfachen Untermodul, im Widerspruch zur Konstruktion von $M'$ und $M''$.

$2 \Rightarrow 1$: Sei $(M_i)_{i \in I}$ die Familie aller einfachen Untermoduln von $M$. Sei $N$ der Kern von

$$\bigoplus_{i \in I} M_i \to M.$$

Dann existiert eine Teilmenge $J \subseteq I$ sodass $\bigoplus_{i \in J} M_i$ Komplement zu $N$ ist, also die Abbildung

$$\bigoplus_{i \in J} M_i \to M$$

ein Isomorphismus ist. □

**Bemerkung 1.2.40.** Obige Charakterisierung zeigt direkt dass für einen halbeinfachen Modul $M$ auch jeder Untermodul von $M$ (wegen 3) und jeder Quotient von $M$ (wegen 2) halbeinfach ist.

## 1.3 Halbeinfache Ringe

**Definition 1.3.1.** *Ein Ring $R$ heißt* halbeinfach*, wenn $R$ als $R$-Linksmodul halbeinfach ist.*

Wir werden später sehen, dass das auch äquivalent dazu ist, dass $R$ als $R$-Rechtsmodul halbeinfach ist.

**Beispiel 1.3.2.** Ein *Divisionsring* ist ein (nicht notwendigerweise kommutativer) Ring $R$ in dem jedes $x \neq 0$ ein Inverses $x^{-1}$ hat, also ein Element mit $x^{-1}x = xx^{-1} = 1$.

$R$, aufgefasst als Modul über sich selbst, ist *einfach* genau dann wenn $R$ ein Divisionsring ist. Inbesondere sind Divisionsringe halbeinfache Ringe.

*Beweis.* Sei $R$ Divisionsring und $N \subseteq R$ ein Untermodul. Entweder $N = 0$, oder $N$ enthält ein $x \neq 0$. Dann ist aber wegen $(yx^{-1}) \cdot x = y$ bereits $N = R$.

Umgekehrt sei $R$ einfacher $R$-Modul und $x \in R$ ein Element mit $x \neq 0$. Dann muss der von $x$ erzeugte Untermodul $R \cdot x$ bereits ganz $N$ sein, es gibt also $y \in R$ mit $yx = 1$, $x$ hat also ein Linksinverses. Genauso finden wir ein linksinverses zu $y$, also $z$ mit $zy = 1$. Nun sehen wir $x = zyx = z$, also ist $y$ inverses zu $x$. □

Kommutative Divisionsringe sind genau Körper, aber es gibt auch nichtkommutative Beispiele, wie zum Beispiel die Quaternionen $\mathbb{H}$.

**Beispiel 1.3.3.** Sei $R$ halbeinfacher Ring. Dann ist auch $\mathrm{Mat}_{n\times n}(R)$ halbeinfacher Ring.

*Beweis.* Als Linksmodul über $\mathrm{Mat}_{n\times n}(R)$ ist

$$\mathrm{Mat}_{n\times n}(R) \cong \bigoplus_{i=1}^{n} R^n,$$

wo wir $R^n$ als Linksmodul über $\mathrm{Mat}_{n\times n}(R)$ auffassen indem wir Elemente von $R^n$ als Spaltenvektoren schreiben. Die Zerlegung oben korrespondiert dann dazu, eine Matrix durch ihre $n$ Spaltenvektoren auszudrücken. Es genügt nun also zu zeigen dass $R^n$ als $\mathrm{Mat}_{n\times n}(R)$-Modul halbeinfach ist.

Untermoduln von $R^n$ sind nun immer von der Form $N^n$, wo $N \subseteq R$ ein $R$-Untermodul ist. Wenn $M \subseteq R^n$, dann sei $N \subseteq R$ der Untermodul der in $R$ von allen Einträgen von Elementen von $M$ erzeugt wird. Klar gilt $M \subseteq N^n$. Umgekehrt liegt das Bild jeder der kanonischen Inklusionen $N \to N^n$, da für ein Element $(x_1, \ldots, x_n) \in M$ auch $(0, \ldots, 0, x_j, 0, \ldots, 0) \in M$ mit $x_j$ an der $i$-ten Stelle (Multiplikation mit einer Matrix mit einer 1 an der Stelle $ij$), also ist $N^n \subseteq M$.

Da $R$ halbeinfach ist, besitzt $N$ in $R$ ein Komplement $N'$. Dann ist auch $(N')^n$ in $R^n$ ein Komplement zu $N^n$. Also ist $R^n$ halbeinfacher Modul. □

**Beispiel 1.3.4.** Seien $R$ und $S$ halbeinfache Ringe. Dann ist auch $R \times S$ halbeinfach.

*Beweis.* Wir können $R$ bzw. $S$ vermöge der Projektionen $R \times S \to R$ bzw. $R \times S \to S$ als $R \times S$-Modul auffassen. Dann ist

$$R \times S \cong R \oplus S$$

als $R \times S$-Modul. Es genügt also, zu zeigen, dass $R$ bzw. $S$ als $R \times S$-Moduln halbeinfach sind. Eine Teilmenge $N \subseteq R$ ist $R$-Untermodul genau wenn sie $R\times S$-Untermodul ist, also folgt aus der Halbeinfachkeit von $R$ dass jeder $R\times S$-Untermodul in $R$ ein Komplement hat. Analog sehen wir dass auch $S$ als $R\times S$-Modul halbeinfach ist. □

**Proposition 1.3.5.** *Sei $R$ ein Ring. Die folgenden Aussagen sind äquivalent:*

1. *$R$ ist halbeinfach.*
2. *Jeder $R$-Modul ist halbeinfach.*
3. *Jede kurze exakte Folge von $R$-Moduln spaltet.*

*Beweis.* $1 \Leftrightarrow 2$: Wenn $R$ halbeinfach ist, dann sind auch freie Moduln $\bigoplus_{i\in I} R$ halbeinfach. Da jeder Modul Quotient eines freien Moduls ist, ist damit jeder Modul halbeinfach. Die Umkehrung ist trivial.

$2 \Leftrightarrow 3$: Das ist einfach die Charakterisierung von halbeinfachen Moduln als diejenigen Moduln in denen jeder Untermodul direkter Summand ist. □

Wir haben oben gesehen, dass endliche Produkte von Matrixringen über Divisionsringen halbeinfach sind. Wir werden nun halbeinfache Ringe klassifizieren, und sehen dass auch die Umkehrung gilt. Dazu beobachten wir zunächst:

**Lemma 1.3.6.** *Sei $R$ halbeinfacher Ring. Dann ist $R$* endliche *Summe von einfachen $R$-Moduln (insbesondere Modul endlicher Länge!), und jede Isomorphieklasse einfacher $R$-Moduln kommt als Summand von $R$ vor. Inbesondere gibt es über einem halbeinfachen Ring nur endlich viele Isomorphieklassen von einfachen Moduln.*

*Beweis.* Da $R$ halbeinfach ist ist $R \cong \bigoplus_{i\in I} M_i$ mit einfachen $M_i$. Betrachte das Element $1 \in R$. Sei $J \subseteq I$ die Teilmenge aller $j \in I$ für die das Bild von 1 unter der Projektion

$$R \cong \bigoplus_{i\in I} M_i \to M_j$$

nicht null ist. Dann ist $J$ endlich (weil $\bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i$ genau aus Elementen besteht die an allen bis auf endlich vielen Stellen den Eintrag 0 haben). Für $j \in I\setminus J$ schickt dann $R \to M_j$ $1 \mapsto 0$, also handelt es sich um die Nullabbildung. Das kann aber nicht sein, weil $R \to M_j$ auf $M_j$ selbst ja die Identität ist. Also folgt $J = I$ und $I$ ist endlich.

Um zu sehen dass jeder einfache Modul isomorph zu einem der Summanden von $R$ ist, erinnern wir uns dass jeder einfache Modul isomorph zu $R/I$ für einen maximalen Untermodul in $R$ ist. Aber wenn $R$ halbeinfach ist spaltet die exakte Folge $0 \to I \to R \to R/I \to 0$ und $R/I$ ist direkter Summand von $R$. □

**Lemma 1.3.7.** *Sei $R$ ein Ring und $M$ ein einfacher $R$-Modul. Dann ist*

$$D = \mathrm{End}_{\mathrm{LMod}_R}(M)$$

*ein Divisionsring.*

*Beweis.* Nach dem Lemma von Schur ist jede Abbildung $f : M \to M$ entweder 0 oder Isomorphismus. Das bedeutet genau dass $D$ Divisionsring ist. □

**Theorem 1.3.8** (Artin-Wedderburn)**.** *Sei $R$ ein halbeinfacher Ring, $M_i$ Repräsentanten der Isomorphieklassen von einfachen $R$-Moduln, $D_i = \mathrm{End}_{\mathrm{LMod}_R}(M_i)$, und $n_i \in \mathbb{N}$ so dass*

$$R \cong \bigoplus_i M_i^{n_i}$$

*als $R$-Linksmodul. Dann ist $R \cong \prod \mathrm{Mat}_{n_i\times n_i}(D_i^{\mathrm{op}})$ als Ring.*

*Beweis.* Wir haben

$$R^{\mathrm{op}} \cong \mathrm{End}_{\mathrm{LMod}_R}(R) = \mathrm{End}_{\mathrm{LMod}_R}(\bigoplus_i M_i^{n_i}).$$

Da nach Annahme für $i \neq j$ auch $M_i \ncong M_j$, ist nach Schur jeder Morphismus $M_i \to M_j$, und damit auch jeder Morphismus $M_i^{n_i} \to M_j^{n_j}$, null. Also gilt

$$\mathrm{End}_{\mathrm{LMod}_R}(\bigoplus_i M_i^{n_i}) \cong \prod_i \mathrm{End}_{\mathrm{LMod}_R}(M_i^{n_i}) \cong \prod_i \mathrm{Mat}_{n_i\times n_i}(D_i).$$

Indem wir auf beiden Seiten dieses Isomorphismus zu $R^{\mathrm{op}}$ übergehen erhalten wir die Behauptung. □

**Korollar 1.3.9.** $R$ ist halbeinfach genau wenn $R^{\mathrm{op}}$ halbeinfach ist. Also macht es in der Definition von halbeinfach keinen Unterschied ob wir $R$ als Links- oder als Rechtsmodul über sich selbst auffassen.

*Beweis.* Wenn $R$ halbeinfach ist ist $R \cong \prod \mathrm{Mat}_{n_i \times n_i}(D_i)$ und $R^{\mathrm{op}} \cong \prod \mathrm{Mat}_{n_i \times n_i}(D_i^{\mathrm{op}})$. Da für einen Divisionsring $D$ auch $D^{\mathrm{op}}$ Divisionsring ist, ist $R^{\mathrm{op}}$ ebenfalls halbeinfach. □

Theorem 1.3.8 ist dann mächtig, wenn wir es mit einem halbeinfachen Ring zu tun haben der nicht offensichtlich mit Matrixringen zu tun hat. Ein Beispiel dieser Art wollen wir nun betrachten.

**Definition 1.3.10.** *Sei $G$ eine Gruppe und $R$ ein Ring. Der* Gruppenring *von $G$ mit Koeffizienten in $R$, ist gegeben durch*

$$R[G] := \{\sum_{g \in G} r_g g \mid r_g \in R, \text{ fast alle } r_g = 0\},$$

*mit "komponentenweiser" Addition, und Multiplikation bestimmt durch die Multiplikation auf $R$ und die Gruppenstruktur (also $g \cdot h = gh$, und dann $R$-bilinear fortgesetzt).*

$R[G]$ enthält somit einerseits den Ring $R$ (via des injektiven Ringhomomorphismus $r \mapsto r \cdot e$, wo $e$ das neutrale Element von $G$ ist), als auch $G$, via $g \mapsto 1 \cdot g$.

**Bemerkung 1.3.11.** Sei $K$ ein Körper und $V$ ein $K$-Vektorraum. Gegeben eine $K[G]$-Modulstruktur auf $V$, die die $K$-Modulstruktur auf $V$ fortsetzt, also mit $(r \cdot e) \cdot v = rv$, so erhalten wir für jedes $g \in G$ einen $K$-linearen Homomorphismus

$$\rho_g : V \to V, v \mapsto g \cdot v.$$

Dann ist $\rho_{gh} = \rho_g \circ \rho_h$ und $\rho_e = \mathrm{id}_V$, also ist jedes $\rho_g$ wegen $\rho_g \circ \rho_{g^{-1}} = \rho_e = \mathrm{id}_V$ invertierbar, und somit definiert $\rho$ einen Gruppenhomomorphismus $\rho : G \to \mathrm{Aut}_K(V)$, wo $\mathrm{Aut}_K(V)$ die Gruppe der $K$-linearen Automorphismen von $V$ bezeichnet.

Umgekehrt erhalten wir für ein solches $\rho$ eine $K[G]$-Modulstruktur auf $V$, via

$$(\sum_{g \in G} r_g g) \cdot v = \sum_{g \in G} r_g \rho_g(v).$$

Insbesondere korrespondieren für $V = K^n$ $K[G]$-Modulstrukturen auf $K^n$ zu Gruppenhomomorphismen $G \to \mathrm{GL}_n(K)$.

**Theorem 1.3.12** (Maschke)**.** *Sei $G$ endlich und $K$ ein Körper von Charakteristik 0. Dann ist $K[G]$ halbeinfach.*

*Beweis.* Wir zeigen, dass jede kurze exakte Folge von $K[G]$-Moduln spaltet. Sei also

$$0 \to A \to B \to C \to 0$$

exakt. Wir suchen einen Schnitt der surjektiven Abbildung $p : B \to C$. In der Kategorie von $K$-Moduln (also Vektorräumen) ist das kein Problem: Da Körper halbeinfach sind (oder wegen linearer Algebra) finden wir ein $K$-lineares $s : C \to B$ mit $p \circ s = \mathrm{id}_C$. Nun ist $s$ aber nicht unbedingt $K[G]$-linear, dazu müsste für jedes $g \in G$

$$s \circ \rho_{g,C} = \rho_{g,B} \circ s$$

gelten, wo $\rho_{g,C} : C \to C$ die $K$-lineare Abbildung gegeben durch Linksmultiplikation mit $g \in K[G]$ ist. Wir können diese Bedingung auch als $\rho_{g^{-1},B} \circ s \circ \rho_{g,C} = s$ schreiben. So formuliert wollen wir also ein $s$, was unter der $G$-Wirkung auf $\mathrm{Hom}_{\mathrm{LMod}_K}(C, B)$ durch $\rho_{g^{-1},B} \circ s \circ \rho_{g,C}$ invariant ist.

Wir definieren nun ein neues $s'$ als "Mittelwert":

$$s' := \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1},B} \circ s \circ \rho_{g,C}.$$

Dann ist immer noch

$$p \circ s' = \frac{1}{|G|} \sum_{g \in G} p \circ \rho_{g^{-1},B} \circ s \circ \rho_{g,C} = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1},C} \circ p \circ s \circ \rho_{g,C} = \mathrm{id}_C,$$

aber auch

$$\rho_{h^{-1},C} \circ s' \circ \rho_{h,B} = \frac{1}{|G|} \sum_{g \in G} \rho_{(gh)^{-1},C} \circ s' \circ \rho_{gh,B} = s',$$

also haben wir einen $K[G]$-linearen Schnitt zu $p : B \to C$ gefunden. □

Wir lernen also direkt:

1. Jeder $K[G]$-Modul ist direkte Summe von einfachen $K[G]$-Moduln (die sogenannten *irreduziblen ($K$-linearen) Darstellungen von $G$*.
2. Es gibt nur endlich viele Isomorphieklassen von irreduziblen $G$-Darstellungen.

Wir wollen nun die auftretenden Isomorphieklassen quantitativ studieren.

**Lemma 1.3.13.** *Sei $G$ eine endliche Gruppe, $K$ ein Körper von Charakteristik 0, $V_i$ eine Liste von Repräsentanten der Isomorphieklassen einfacher $K[G]$-Moduln, $D_i = \mathrm{End}_{\mathrm{LMod}_{K[G]}}(V_i)$ die assoziierten Divisionsringe, und $d_i = \dim_K D_i$. Sei $K[G] = \bigoplus_i V_i^{n_i}$ als $K[G]$-Linksmodul. Dann gilt:*

$$\dim_K V_i = d_i \cdot n_i$$

$$|G| = \sum d_i n_i^2 = \sum \frac{(\dim_K V_i)^2}{d_i}$$

*Beweis.* Wir berechnen

$$V_j \cong \mathrm{Hom}_{\mathrm{LMod}_{K[G]}}(K[G], V_j) \cong \mathrm{Hom}_{\mathrm{LMod}_{K[G]}}(\bigoplus_i V_i^{n_i}, V_j) \cong D_j^{n_j},$$

also $\dim V_j = d_j \cdot n_j$. Für die zweite Gleichung wenden wir den Satz von Artin-Wedderburn an um

$$K[G] \cong \prod \mathrm{Mat}_{n_i \times n_i}(D_i^{\mathrm{op}})$$

zu folgern, und beobachten dass die linke Seite Dimension $|G|$, die rechte Seite Dimension $\sum d_i n_i^2$ hat. □

**Lemma 1.3.14.** *Sei $K$ ein* algebraisch abgeschlossener *Körper von Charakteristik* 0. *Dann sind die $D_i = \mathrm{End}_{\mathrm{LMod}(K[G])}(V_i)$ immer isomorph zu $K$, also $d_i = 1$.*

*Beweis.* Die $V_i$ sind ja endlichdimensionale $K$-Vektorräume (weil Summanden von $K[G]$). Wenn $f : V_i \to V_i$ ein Endomorphismus ist, gibt es also einen Eigenwert $\lambda \in K$. Damit ist $f - \lambda \cdot \mathrm{id}$ ein Endomorphismus der nicht Isomorphismus ist, also nach Schur schon gleich null, also $f = \lambda \cdot \mathrm{id}$. □

Wir erhalten also insgesamt, dass über algebraisch abgeschlossenem $K$ gilt $\sum(\dim V_i)^2 = |G|$, wo die $V_i$ Repräsentanten von einfachen $K[G]$-Moduln sind.

**Beispiel 1.3.15.** Sei $G = \Sigma_3$ die symmetrische Gruppe, und $K$ ein algebraisch abgeschlossener Körper von Charakteristik 0. Wir erhalten zwei verschiedene einfache $K[G]$-Moduln, die eindimensional über $K$ sind, indem wir die Homomorphismen $K[\Sigma_3] \to K$, $\sigma \mapsto 1$ bzw. $\sigma \mapsto \mathrm{sgn}(\sigma)$ benutzen. Es können nicht alle einfachen $K[\Sigma_3]$-Moduln 1-dimensional über $K$ sein, da wir sonst nach dem Satz von Artin-Wedderburn eine Beschreibung von $K[G]$ als Produkt von $1 \times 1$-Matrixringen über $K$ erhalten würden, also $K[G]$ kommutativ wäre. Wir erhalten also mindestens einen weiteren einfachen $K[G]$-Modul, der mindestens Dimension 2 hat, und wegen $1^2 + 1^2 + 2^2 = 6$ muss es sich um genau einen weiteren von Dimension 2 handeln.

In der sogenannten Darstellungstheorie endlicher Gruppen studiert man einfache $K[G]$-Moduln systematischer indem man sich nicht nur die Dimension der $V_i$ merkt, sondern auch für jedes $g \in G$ die Spur der $K$-linearen Abbildung $\rho_g : V_i \to V_i$. Diese kann man in die sogenannte *Charaktertabelle* der Gruppe organisieren, und Verallgemeinerungen unserer Beobachtung $|G| = \sum \frac{(\dim V_i)^2}{d_i}$ (die sogenannten Orthogonalitätsrelationen) erlauben im Stil von Beispiel 1.3.15 sehr viel über die einfachen $K[G]$-Moduln herauszufinden, ohne sie explizit konstruieren zu müssen.

## 1.4 Ideale und das Radikal

**Definition 1.4.1.** *Sei $R$ ein Ring.*

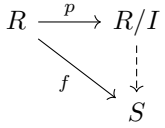
1. *Ein* Linksideal $I \subseteq R$ *ist ein unter-$R$-Linksmodul.*

2. *Ein* Rechtsideal $I \subseteq R$ *ist ein unter-R-Rechtsmodul.*

3. *Ein* beidseitiges Ideal $I \subseteq R$ *ist eine Teilmenge, die sowohl Links- als auch Rechtsideal ist, also unter Multiplikation mit Elementen aus* $r$ *von beiden Seiten abgeschlossen ist.*

Für kommutative Ringe fallen alle drei Begriffe zusammen. Links- und Rechtsideale sind uns bereits in der Modultheorie begegnet, beidseitige Ideale sind aber der richtige Begriff wenn es um Quotienten von Ringen geht: Für ein beidseitiges Ideal $I \subseteq R$ erhalten wir auf $R/I$ eine wohldefinierte Ringstruktur. Umgekehrt ist für einen Ringhomomorphismus $f : R \to S$ der Kern $I$ ein beidseitiges Ideal, und das Bild $f(R) \subseteq S$ als Ring isomorph zu $R/I$.

**Bemerkung 1.4.2.** Für ein beidseitiges Ideal $I \subseteq R$ hat der Quotient $R/I$ folgende universelle Eigenschaft: Er ist ein Ring mit Ringhomomorphismus $p : R \to R/I$ mit $p(I) = 0$, und für jeden Ringhomomorphismus $f : R \to S$ mit $f(I) = 0$ existiert eine eindeutige Faktorisierung durch $p$:




**Beispiel 1.4.3.** Sei $K$ ein Körper und $R = \mathrm{Mat}_{n\times n}(K)$. Dann enthält $R$ viele Linksideale (und analog Rechtsideale), zum Beispiel haben wir in Beispiel 1.3.3 gesehen dass $\mathrm{Mat}_{n\times n}(K) \cong \bigoplus_{i=1}^{n} K^n$ als Linksmodul.

$R$ enthält aber nicht viele beidseitige Ideale: Sei $I \subseteq R$ beidseitiges Ideal. Dann ist entweder $I = 0$, oder wir haben ein $f \in I$ mit $f \neq 0$. Sei $v \in K^n$ ein Vektor mit $f(v) \neq 0$, $h : K^n \to K^n$ die lineare Abbildung mit $e_1 \mapsto v$, $e_j \mapsto 0$ für $j \neq 1$, $g : K^n \to K^n$ eine lineare Abbildung mit $f(v) \mapsto e_1$. Dann ist $g \circ f \circ h$ die Abbildung mit $e_1 \mapsto e_1$ und $e_j \mapsto 0$ für $j \neq 1$, also die $n \times n$-Matrix mit einer 1 oben links und allen anderen Einträgen 0. Wir haben gezeigt dass diese Matrix in $I$ liegt, und indem wir diese von rechts und links mit Permutationsmatrizen multiplizieren erhalten wir Matrizen mit 1 an beliebiger Stelle, und indem wir Linearkombinationen bilden sehen wir dass $I = \mathrm{Mat}_{n\times n}(K)$.

**Definition 1.4.4.** *Ein Ring heißt* einfach *wenn er nicht* 0 *ist, und die einzigen beidseitigen Ideale von* $R$ *durch* 0 *und* $R$ *gegeben sind.*

**Bemerkung 1.4.5.** Einfache Ringe sind nicht immer halbeinfach! Das liegt daran, dass *halbeinfach* für Ringe über die Kategorie der Linksmoduln definiert haben ($R$ ist halbeinfach wenn $R \in \mathrm{LMod}_R$ in einfache Moduln zerlegbar ist), aber *einfach* für Ringe über die Kategorie der Ringe definiert ist ($R$ ist einfach wenn $R$ in Ring keine nichttrivialen Quotienten besitzt, analog dazu dass ein $R$-Modul $M$ einfach ist wenn er in $\mathrm{LMod}_R$ keine nichttrivialen Quotienten besitzt).

**Definition 1.4.6.** *Ein beidseitiges Ideal* $I \subseteq R$ *heißt* maximal, *wenn es sich um ein echtes Ideal handelt (also* $I \neq R$*), und für jedes echte Ideal* $J \subsetneq R$ *mit* $I \subseteq J$ *bereits* $J = I$ *gilt. Analog definieren wir maximale Links- und Rechtsideale.*

**Lemma 1.4.7.** *1. Ein beidseitiges Ideal $I \subseteq R$ ist genau dann maximal, wenn $R/I$ einfacher Ring ist.*

*2. Ein Linksideal (Rechtsideal) $I \subseteq R$ ist genau dann maximal, wenn $R/I$ einfacher Linksmodul (Rechtsmodul) ist.*

*Beweis.* Beidseitige Ideale in $R/I$ korrespondieren zu beidseitigen Idealen in $R$, die $I$ enthalten (via Urbild/Bild nehmen). Das zeigt den ersten Teil. Den zweiten haben wir schon im Beweis von Proposition 1.2.15 gesehen, er folgt aber auch komplett analog indem man beobachtet dass Links-Untermoduln von $R/I$ genau zu Linksidealen in $R$, die $I$ enthalten, korrespondieren. □

Insbesondere sehen wir dass ein *kommutativer* Ring $R$ genau dann einfach ist, wenn er Divisionsring, also Körper ist.

**Lemma 1.4.8.** *Sei $I \subseteq R$ ein echtes (Links-, Rechts-,) beidseitiges Ideal. Dann ist $I$ enthalten in einem maximalen (Links-, Rechts-,) beidseitigen Ideal $J \subseteq R$.*

*Beweis.* Der Beweis geht für alle Varianten analog, also schreiben wir im Folgenden einfach "Ideal": Ein Ideal ist genau dann echtes Ideal, wenn es das Element $1 \in R$ nicht enthält. Für eine Kette von echten Idealen ist die Vereinigung demnach ebenfalls ein echtes Ideal. Also können wir das Lemma von Zorn anwenden auf die Menge aller echten Ideale, die $I$ enthalten. □

**Definition 1.4.9.** *Sei $R$ ein Ring und $M$ ein $R$-Linksmodul. Für $x \in M$ definieren wir den* Annulator von $x$ *durch*

$$\operatorname{ann}_R(x) = \{r \in R \mid rx = 0\} = \ker(R \to M, r \mapsto rx),$$

*und den* Annulator von $M$ *durch*

$$\operatorname{ann}_R(M) = \bigcap_{x \in M} \operatorname{ann}_R(x).$$

**Lemma 1.4.10.** *Für $x \in M$ ist $\operatorname{ann}_R(x) \subseteq R$ ein Linksideal, und $\operatorname{ann}_R(M) \subseteq R$ ein beidseitiges Ideal.*

*Beweis.* Wir haben $\operatorname{ann}_R(x) = \ker(R \to M, r \mapsto rx)$, also handelt es sich um einen links-Untermodul von $R$. Für die zweite Aussage beobachten wir, dass die Wirkung von $R$ auf $M$ einen Ringhomomorphismus

$$R \to \operatorname{End}_{\mathbb{Z}}(M), r \mapsto (x \mapsto rx)$$

liefert, dessen Kern $\operatorname{ann}_R(M)$ ist. □

**Definition 1.4.11.** *Für einen Modul $M$ definieren wir einen Untermodul $\operatorname{rad}_R(M) \subseteq M$ als Durchschnitt aller maximalen (echten) Untermoduln von $M$.*

**Beispiel 1.4.12.** 1. $\operatorname{rad}_{\mathbb{Z}} \mathbb{Z} = 0$, da der Schnitt aller maximalen Untermoduln $p\mathbb{Z}$ trivial ist.

2. $\mathrm{rad}_{\mathbb{Z}}\, \mathbb{Z}/p^n\mathbb{Z} = p\mathbb{Z}/p^n\mathbb{Z}$, der eindeutige maximale Untermodul.

3. Wenn $M$ keine maximalen Untermoduln hat, dann ist $\mathrm{rad}_R(M) = M$ (leerer Durchschnitt), z.B. $\mathrm{rad}_{\mathbb{Z}}\, \mathbb{Q} = \mathbb{Q}$.

**Lemma 1.4.13.** *Wir haben*

$$\mathrm{rad}_R(M) = \bigcap_{\varphi: M \to E} \ker(\varphi)$$

*wo der Schnitt über alle Homomorphismen $M \to E$ zu* einfachen $R$*-Moduln $R$ ist.*

*Beweis.* Für einen maximalen Untermodul $N \subseteq M$ ist $M/N$ einfacher $R$-Modul, und $N$ der Kern von $M \to M/N$. Also ist $\bigcap \ker(\varphi) \subseteq \mathrm{rad}_R(M)$. Umgekehrt ist jedes $\varphi : M \to E$ entweder 0 oder surjektiv (da $E$ einfach ist), und damit $\ker(\varphi)$ entweder $M$ oder ein maximaler Untermodul. Also ist auch $\mathrm{rad}_R(M) \subseteq \ker(\varphi)$. □

**Lemma 1.4.14.** *1. Sei $f : M \to N$ ein $R$-Modulhomomorphismus. Dann ist $f(\mathrm{rad}_R(M)) \subseteq \mathrm{rad}_R(N)$.*

*2. Sei $N \subseteq \mathrm{rad}_R(M)$. Dann ist $\mathrm{rad}_R(M/N) = \mathrm{rad}_R(M)/N$.*

*Beweis.* Für die erste Aussage beobachten wir dass nach Lemma 1.4.13 die Elemente des Radikals genau diejenigen sind, die unter allen Homomorphismen zu einfachen Moduln auf 0 gehen. Sei $x \in \mathrm{rad}_R(M)$ und $\varphi : N \to E$ ein Homomorphismus, dann schickt die Komposition $\varphi \circ f : M \to N \to E$ ja $x \mapsto 0$, also ist $\varphi(f(x)) = 0$. Da dies für alle $\varphi$ funktioniert, ist $f(x) \in \mathrm{rad}_R(N)$.

Für die zweite Aussage beobachten wir dass wegen $N \subseteq \mathrm{rad}_R(M)$ jeder maximale Untermodul von $M$ $N$ enthält. Durch Bild bzw. Urbild nehmen erhalten wir also eine Bijektion zwischen den maximalen Untermoduln von $M$, und den maximalen Untermoduln von $M/N$. Da Urbilder mit Schnitten kompatibel sind, folgt dass $\mathrm{rad}_R(M)$ das Urbild von $\mathrm{rad}_R(M/N)$ ist, also $\mathrm{rad}_R(M/N) = \mathrm{rad}_R(M)/N$. □

Wenn $M$ halbeinfach ist, also $M = \bigoplus_{i \in I} M_i$, dann ist $\mathrm{rad}_R(M) = 0$, da die Untermoduln $\bigoplus_{i \in I \setminus \{j\}} M_i$ für alle $j \in I$ maximal sind, und Schnitt 0 haben. Wir haben die folgende partielle Umkehrung:

**Lemma 1.4.15.** *Sei $M$ Artinsch. Dann ist $M/\mathrm{rad}_R(M)$ halbeinfacher $R$-Modul.*

*Beweis.* Wir betrachten die Familie aller maximalen echten Untermoduln $N_i \subseteq M$, mit Indexmenge $I$. Unter den endlichen Durchschnitten (also $\bigcap_{i \in J} N_i$) für endliche Teilmengen $J \subseteq I$) gibt es einen minimalen. Dieser muss dann bereits mit $\bigcap_{i \in I} N_i = \mathrm{rad}_R(M)$ übereinstimmen. Wir finden also eine endliche Teilmenge $J \subseteq I$, sodass

$$M/\mathrm{rad}_R(M) \to \bigoplus_{i \in J} M/N_i$$

injektiv ist. Aber damit ist $M/\operatorname{rad}_R(M)$ Untermodul eines halbeinfachen Modul, also selbst halbeinfach. □

Allgemein sind Moduln mit $\operatorname{rad}_R(M) = 0$ genau die, die zu Untermoduln von Produkten $\prod_{i\in I} M_i$ einfacher Moduln isomorph sind. Diese sind nicht immer halbeinfach. Zum Beispiel ist $\mathbb{Z}$ Untermodul von $\prod_{p\in\mathbb{P}} \mathbb{Z}/p\mathbb{Z}$.

Wir werden nun öfter Bedingungen der Form "$R$ ist Artinsch/Noethersch als Links- oder Rechtsmodul über sich selbst" sehen. Man definiert:

**Definition 1.4.16.** *Sei $R$ ein Ring.*

1. *$R$ heißt linksartinsch (rechtsartinsch), wenn $R$ als $R$-Linksmodul (Rechtsmodul) artinsch ist.*
2. *$R$ heißt linksnoethersch (rechtsnoethersch), wenn $R$ als $R$-Linksmodul (Rechtsmodul) Noethersch ist.*

**Beispiel 1.4.17.** Ein halbeinfacher Ring $R$ ist links- und rechtsnoethersch und links- und rechtsartinsch, da er sich als endliche direkte Summe von einfachen Moduln schreiben lässt.

Das Radikal von $R$ als $R$-Modul spielt eine besondere Rolle.

**Definition 1.4.18.** *Wir schreiben* $\operatorname{Jac}(R) := \operatorname{rad}_R(R)$*, das sogenannte* Jacobson-Radikal *von $R$.*

**Lemma 1.4.19.** $\operatorname{Jac}(R) = \bigcap_{E\ einfach} \operatorname{ann}_R(E)$. *Insbesondere ist* $\operatorname{Jac}(R)$ *ein echtes beidseitiges Ideal in $R$.*

*Beweis.* Sei $E$ einfacher $R$-Modul und $x \in E$. Dann ist entweder $x = 0$ und $\operatorname{ann}_R(x) = R$, oder $R \to E, 1 \mapsto x$ ist surjektiv mit Kern $\operatorname{ann}_R(x)$, sodass in diesem Fall $\operatorname{ann}_R(x)$ ein maximaler Untermodul von $R$ ist. Umgekehrt tritt jeder maximale Untermodul $I \subseteq R$ als Annulator vom Bild von 1 im einfachen Modul $R/I$ auf. Somit stimmt $\bigcap_{E \text{ einfach}} \operatorname{ann}_R(E)$ überein mit dem Schnitt aller maximalen Untermoduln von $R$, also mit $\operatorname{Jac}(R)$. Die $\operatorname{ann}_R(E)$ sind aber beidseitige Ideale. Da nach Lemma 1.4.8 $R$ maximale Ideale besitzt, ist $\operatorname{Jac}(R) \neq R$, also echtes beidseitiges Ideal. □

$R/\operatorname{Jac}(R)$ hat also immer eine kanonische Ringstruktur.

A priori macht es einen Unterschied, ob wir hier $R$ als Links- oder als Rechtsmodul über sich selbst auffassen, also ob wir $\operatorname{Jac}(R)$ als Schnitt aller maximalen Linksideale oder aller maximalen Rechtsideale definieren. Im Folgenden sehen wir eine äquivalente Charakterisierung, die symmetrisch ist:

**Lemma 1.4.20.** *Sei $R$ ein Ring und $x \in R$. Die folgenden Aussagen sind äquivalent:*

1. $x \in \operatorname{Jac}(R)$
2. *Für jedes $r \in R$ existiert ein Linksinverses zu $(1 - rx)$, also $u$ mit $u(1 - rx) = 1$.*

3. *Für jedes $r, s \in R$ ist $(1 - rxs)$ invertierbar.*

*Beweis.* Wir zeigen erst $1 \Leftrightarrow 2$. Angenommen $x \notin \mathrm{Jac}(R)$. Dann existiert ein maximales Linksideal $I \subseteq R$ mit $x \notin I$, also $Rx + I = R$, also finden wir $r \in R$ mit $1 - rx \in I$. Also hat $1 - rx$ kein Linksinverses. Wenn umgekehrt für ein $r$ $(1 - rx)$ kein Linksinverses existiert, gibt es ein maximales Linksideal $I$ mit $1 - rx \in I$, also ist $x \notin I$ und somit $x \notin \mathrm{Jac}(R)$.

Nun zeigen wir $1 \Leftrightarrow 3$ und benutzen die Äquivalenz von 1 und 2. Es gilt klar $3 \Rightarrow 2$, man setze einfach $s = 1$. Für die Umkehrung ist mit $x \in \mathrm{Jac}(R)$ auch $xs \in \mathrm{Jac}(R)$, also existiert nach 2 ein $u$ mit $u(1 - rxs) = 1$, also $1 + urxs = u$. Mit demselben Argument finden wir ein $v$ mit $v(1 + urxs) = 1$, also $vu = 1$. Insgesamt folgt $v = vu(1 - rxs) = 1 - rxs$, und somit sind $u$ und $1 - rxs$ invers zueinander. □

**Lemma 1.4.21.** *Ein Ring $R$ ist halbeinfach genau wenn $R$ linksartinsch (oder rechtsartinsch) ist und* $\mathrm{Jac}(R) = 0$*. Insbesondere ist für Artinsche Ringe $R/\mathrm{Jac}(R)$ immer halbeinfach.*

*Beweis.* Wenn $R$ Artinsch ist und $\mathrm{Jac}(R) = 0$ gilt, dann ist $R$ nach Lemma 1.4.15 halbeinfach. Umgekehrt ist ein halbeinfacher Ring automatisch Artinsch (weil $R$ endliche direkte Summe einfacher Moduln ist), und $\mathrm{Jac}(R) = 0$ da das Radikal halbeinfacher Moduln trivial ist. □

**Korollar 1.4.22.** Ein einfacher Ring ist genau dann halbeinfach, wenn er linksartinsch (oder rechtsartinsch) ist.

Für zwei beidseitige Ideale $I, J$ schreiben wir $I \cdot J \subseteq R$ für die Untergruppe erzeugt von Elementen der Form $i \cdot j$ mit $i \in I$ und $j \in J$, also die Teilmenge bestehend aus Summen solcher Elemente. Diese ist automatisch selbst ein beidseitiges Ideal. Wir schreiben $I^n$ für $I \cdots I$.

**Lemma 1.4.23.** *Sei $R$ linksartinsch (oder rechtsartinsch). Dann ist* $\mathrm{Jac}(R)^n = 0$ *für ein $n$.*

*Beweis.* Da $\mathrm{Jac}(R)^{n+1} \subseteq \mathrm{Jac}(R)^n$ und $R$ Artinsch ist, gibt es ein $n$ mit $\mathrm{Jac}(R)^{n+1} = \mathrm{Jac}(R)^n$. Wir behaupten dass dann schon $\mathrm{Jac}(R)^n = 0$. Sei dazu $M = \{x \in R \mid \mathrm{Jac}(R)^n \cdot x = 0\}$. Es reicht zu zeigen, dass $M = R$. Wenn $M \neq R$, dann gibt es unter den echt größeren Moduln $M \subsetneq M' \subseteq R$ einen minimalen. Dann ist $M'/M$ einfach, insbesondere $\mathrm{Jac}(R) \cdot M' \subseteq M$, also $\mathrm{Jac}(R)^n \cdot M' = \mathrm{Jac}(R)^{n+1} \cdot M' = 0$. Aber $M$ war ja definiert als Untermodul bestehend aus allen $x$ mit $\mathrm{Jac}(R)^n \cdot x = 0$, also folgt $M' = M$ im Widerspruch zur Konstruktion von $M'$. □

**Korollar 1.4.24.** Wenn $R$ linksartinsch ist, dann sind für einen $R$-Linksmodul $M$ die folgenden Aussagen äquivalent:

1. $M$ ist artinsch
2. $M$ ist noethersch
3. $M$ ist von endlicher Länge

4. $M$ ist endlich erzeugt

*Beweis.* Sei $n$ so, dass $\mathrm{Jac}(R)^n = 0$. Dann ist für einen beliebigen Modul

$$M \supseteq \mathrm{Jac}(R) \cdot M \supseteq \mathrm{Jac}(R)^2 \cdot M \supseteq \ldots \supseteq \mathrm{Jac}(R)^n \cdot M = 0$$

eine Folge von Untermoduln. Wir zeigen zunächst $1 \Rightarrow 3$. Sei also $M$ Artinsch, es genügt zu zeigen dass die Quotienten $\mathrm{Jac}(R)^i M/\mathrm{Jac}(R)^{i+1}M$ von endlicher Länge sind. Da diese jeweils $R/\mathrm{Jac}(R)$-Moduln sind, sind sie halbeinfach (über $R/\mathrm{Jac}(R)$, also auch über $R$). Sie sind aber auch Artinsch (weil sie Quotienten von Untermoduln des Artinschen Modul $M$ sind), und ein halbeinfacher Modul ist nur Artinsch wenn er eine *endliche* direkte Summe von einfachen Moduln ist. Also sind die Quotienten von endlicher Länge, somit auch $M$. $2 \Rightarrow 3$ geht genauso, und die Rückrichtungen sind jeweils trivial. Somit ist $1 \Leftrightarrow 2 \Leftrightarrow 3$ gezeigt.

Da Noethersche Moduln immer endlich erzeugt sind (ansonsten gäbe es einen maximalen endlich erzeugten Untermodul $M' \subseteq M$, aber $M' + Rx$ für irgendein $x \notin M'$ ist größer), ist $2 \Rightarrow 4$ klar. Für die letzte Richtung $4 \Rightarrow 1$ sei $M$ endlich erzeugt. Wir erhalten eine surjektive Abbildung

$$\bigoplus R \to M,$$

von einem endlich erzeugten freien Modul, also ist $M$ Quotient eines Artinschen Moduls selbst Artinsch. □

**Korollar 1.4.25.** Linksartinsche Ringe sind Linksnoethersch.

Eine weitere Konsequenz der Nilpotenz von $\mathrm{Jac}(R)$ ist folgende:

**Proposition 1.4.26.** *Sei $R$ linksartinsch und $M$ ein $R$-Linksmodul mit $M/\mathrm{Jac}(R)M = 0$. Dann ist $M = 0$.*

*Beweis.* $M/\mathrm{Jac}(R)M = 0$ ist äquivalent dazu, dass $\mathrm{Jac}(R) \cdot M = M$. Dann ist auch $\mathrm{Jac}(R)^n \cdot M = M$ für alle $n$. Für $n$ ausreichend groß ist aber $\mathrm{Jac}(R)^n = 0$. □

Für einen $R$-Modul $M$ ist $M/\mathrm{Jac}(R) \cdot M$ ein $R/\mathrm{Jac}(R)$-Modul. Wir können uns nun fragen, in welcher Allgemeinheit Proposition 1.4.26 für allgemeinere Ringe gilt.

**Definition 1.4.27.** *Sei $M$ ein $R$-Modul und $M' \subseteq M$ ein Untermodul. Dann heißt $M'$* überflüssig in *$M$, wenn die Abbildung $M \to M/M'$ echte Untermoduln $N \subsetneq M$ auf echte Untermoduln von $M/M'$ abbildet.*

Anders gesagt ist $M'$ überflüssig wenn für jedes $N$ mit $M' + N = M$ bereits $N = M$ gilt.

**Lemma 1.4.28.** *Sei $M' \subseteq M$ überflüssig und $M'' \subseteq M'$. Dann ist auch $M''$ überflüssig in $M$.*

*Beweis.* Nach Annahme schickt die Projektion $M \to M/M'$ echte Untermoduln von $M$ auf echte Untermoduln. Wir können diese als $M \to M/M'' \to M/M'$ faktorisieren. Wenn $N \subsetneq M$ echter Untermodul ist, dann muss sein Bild in $M/M''$ also echter Untermodul sein, andernfalls wäre das Bild in $M/M'$ ja auch alles. Also ist $M''$ ebenfalls überflüssig in $M$. □

**Beispiel 1.4.29.** $\mathrm{Jac}(R)$ ist überflüssig in $R$. Insbesondere ist das Maximalideal eines lokalen Rings überflüssig.

*Beweis.* Sei $I \subseteq R$ irgendein echtes Ideal. Dann ist $I$ enthalten in einem maximalen Linksideal $J$, und $\mathrm{Jac}(R) \subseteq J$ nach Definition. Das Bild von $J$ unter $R \to R/\mathrm{Jac}(R)$ ist ein echter Untermodul (da das Urbild des Bilds wieder $J$ ist), also ist auch das Bild von $I$ unter $R \to R/\mathrm{Jac}(R)$ ein echter Untermodul. □

**Lemma 1.4.30.** *Sei $M$ ein $R$-Modul. Die folgenden Aussagen sind äquivalent:*

1. *$M$ ist endlich erzeugt.*
2. *$M/\mathrm{rad}_R(M)$ ist endlich erzeugt und $\mathrm{rad}_R(M)$ ist überflüssig in $M$.*

*Beweis.* Sei $M$ endlich erzeugt, von $m_1, \ldots, m_n$. Dann ist auch $M/\mathrm{rad}_R(M)$ endlich erzeugt. Außerdem sind die echten Untermoduln von $M$ genau die, die nicht alle Erzeuger $m_1, \ldots, m_n$ enthalten. Für eine Kette von Untermoduln, die nicht $m_1, \ldots, m_n$ enthalten, enthält auch die Vereinigung nicht alle von $m_1, \ldots, m_n$, nach Zorn ist also jeder Untermodul von $M$ in einem maximalen echten Untermodul enthalten. Wie im vorhergehenden Beispiel folgt, dass $\mathrm{rad}_R(M)$ überflüssig ist.

Wenn umgekehrt $\mathrm{rad}_R(M)$ überflüssig ist, und $M/\mathrm{rad}_R(M)$ endlich erzeugt, z.B. von den Bildern von $m_1, \ldots, m_n \in M$, dann sei $N \subseteq M$ der von $m_1, \ldots, m_n$ erzeugte Untermodul. Wenn $N \neq M$, dann wäre das Bild von $N$ in $M/\mathrm{rad}_R(M)$ ebenfalls ein echter Untermodul, Widerspruch. Also ist $N = M$ und $M$ ist endlich erzeugt. □

**Lemma 1.4.31** (Nakayama)**.** *Sei $M$ ein endlich erzeugter $R$-Modul mit*

$$M/\mathrm{Jac}(R) \cdot M = 0.$$

*Dann ist bereits $M = 0$.*

*Beweis.* Für jedes $x \in M$ schickt die Modulabbildung $R \to M$, $r \mapsto rx$ wegen Lemma 1.4.14 $\mathrm{Jac}(R)$ auf eine Teilmenge von $\mathrm{rad}_R(M)$. Also ist $\mathrm{Jac}(R) \cdot x \subseteq \mathrm{rad}_R(M)$, und damit $\mathrm{Jac}(R) \cdot M \subseteq \mathrm{rad}_R(M)$. Insbesondere ist $\mathrm{Jac}(R) \cdot M$ als Untermodul eines überflüssigen Moduls in $M$ ebenfalls überflüssig. Also schickt die Abbildung

$$M \to M/\mathrm{Jac}(R) \cdot M = 0$$

echte Untermoduln auf echte Untermoduln. Das kann nur sein wenn es links keine echten Untermoduln gibt, also $M = 0$. □

Die Konklusion von Proposition 1.4.26 gilt also für beliebige Ringe, wenn wir uns auf endlich erzeugte Moduln beschränken.

**Beispiel 1.4.32.** Die Bedingung, dass $M$ endlich erzeugt ist, kann nicht weggelassen werden: Sei

$$R = \mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}.$$

Dann ist $\mathrm{Jac}(R) = pR$. Wenn nämlich $I \subseteq R$ ein echtes Ideal ist, und $\frac{a}{b} \in I$ mit $p \not| a$, dann wäre auch $1 = \frac{b}{a} \cdot \frac{a}{b} \in I$ und $I$ kein echtes Ideal. Also ist $I \subseteq pR$, und insbesondere ist $pR$ das einzige maximale Ideal.

Sei nun $M = \mathbb{Q}$, aufgefasst als $\mathbb{Z}_{(p)}$-Modul. Dann ist $\mathrm{Jac}(R) = pR$, $M/pM = 0$, aber $M \neq 0$.

Ringe wie $\mathbb{Z}_{(p)}$ spielen eine wichtige Rolle:

**Definition 1.4.33.** *Ein Ring $R$ heißt* lokal*, wenn er ein eindeutiges maximales Linksideal besitzt.*

**Beispiel 1.4.34.**

1. Divisionsringe sind lokale Ringe, mit maximalem Ideal (0).
2. Der Ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}$ ist lokal, mit maximalem Ideal $p\mathbb{Z}_{(p)}$.
3. Der Ring $K[[x]]$ der *formalen Potenzreihen mit Koeffizienten in $K$* für einen Körper $K$ ist lokal, mit maximalem Ideal $xK[[x]]$ (also dem Ideal bestehend aus allen Potenzreihen mit konstantem Term 0).

**Lemma 1.4.35.** *Das maximale Linksideal in einem lokalen Ring ist automatisch beidseitig. Insbesondere ist $R$ genau dann lokal wenn $R^{\mathrm{op}}$ lokal ist, und in der Definition von lokal hätten wir auch "Rechtsideal" schreiben können.*

*Beweis.* Es ist $I = \mathrm{Jac}(R)$, also ist es ein beidseitiges Ideal. □

Man kann allerdings lokale Ringe *nicht* definieren als Ringe mit eindeutigem maximalen beidseitigen Ideal. Zum Beispiel hat $\mathrm{Mat}_{n\times n}(K)$ für einen Körper $K$ nach Beispiel 1.4.3 das eindeutige maximale beidseitige Ideal 0, aber verschiedene maximale Linksideale.

**Lemma 1.4.36.** *Sei $R$ ein lokaler Ring mit Maximalideal $I$. Dann besteht das Komplement $R \setminus I$ genau aus den invertierbaren Elementen von $R$.*

*Beweis.* $I$ enthält kein invertierbares Element. Wenn nämlich $x \in I$ invertierbar wäre, dann wäre auch $y = (yx^{-1})x \in I$ für jedes $y$, also $I = R$, aber maximale Ideale müssen echte Ideale sein. Sei nun umgekehrt $x \neq I$, dann wollen wir zeigen dass $x$ invertierbar ist. Sei $Rx$ das von $x$ erzeugte Linksideal. Wenn $Rx$ ein echtes Ideal wäre, dann wäre $Rx \subseteq I$. Also muss $Rx = R$ sein, und es gibt ein $y$ mit $yx = 1$. Weil $I$ beidseitiges Ideal ist, gilt nun $y \neq I$, also gibt es entsprechend ein $z$ mit $zy = 1$, und $z = zyx = x$, also $yx = xy = 1$ und $x$ ist invertierbar. □

**Bemerkung 1.4.37.** Das zeigt, dass sich die lokalen Ringe auch charakterisieren lassen als diejenigen Ringe in denen die nicht-invertierbaren Elemente eine abelsche Untergruppe bilden. Wenn die nichtinvertierbaren Elemente von $R$ nämlich unter Addition abgeschlossen sind, so bilden sie ein beidseitiges Ideal, was automatisch jedes echte Linksideal enthält (da echte Ideale nie invertierbare Elemente enthalten).

Als Anwendung der Theorie lokaler Ringe erinnern wir uns nochmal an die Diskussion von Zerlegungen von Moduln als direkte Summen. In Theorem 1.2.33 hatten wir gesehen dass Artinsche oder Noethersche Moduln immer eine Zerlegung als endliche direkte Summe von unzerlegbaren Moduln besitzen, aber angemerkt dass diese Zerlegung nicht unbedingt eindeutig ist. Wir beweisen nun, dass für Moduln endlicher Länge eine stärkere Aussage gilt.

**Lemma 1.4.38** (Fitting)**.** *Sei $R$ ein Ring und $M$ ein unzerlegbarer Modul endlicher Länge. Dann ist jeder Endomorphismus $f : M \to M$ entweder Isomorphismus oder nilpotent.*

*Beweis.* Sei $f : M \to M$ ein Endomorphismus. Dann bilden die Bilder $f^n(M)$ eine absteigende, und die Kerne $\ker(f^n)$ eine aufsteigende Folge von Untermoduln. Aufgrund endlicher Länge können wir $n$ so wählen dass beide stabil sind. Wir behaupten $M \cong \ker(f^n) \oplus f^n(M)$.

Wir beobachten zunächst $\ker(f^n) \cap f^n(M) = 0$: Wenn $x$ im Schnitt liegt, dann ist $x = f^n(y)$, und $f^n(x) = 0$, also $f^{2n}(y) = 0$. Aber da nach Konstruktion $\ker(f^n) = \ker(f^{2n})$, ist dann auch $f^n(y) = 0$, also $x = 0$.

Es folgt, dass die Abbildung $f^n : M \to M$ auf dem Untermodul $f^n(M)$ injektiv ist, mit Bild $f^{2n}(M) = f^n(M)$. Also schränkt $f^n$ auf $f^n(M)$ zu einem *Isomorphismus* $f^n(M) \to f^n(M)$ ein, dessen Inverses die kurze exakte Folge

$$0 \to \ker(f^n) \to M \xrightarrow{f^n} f^n(M) \to 0$$

spaltet. □

In einem kommutativen Ring ist die Summe nilpotenter Elemente wieder nilpotent, und die nilpotenten Elemente bilden ein Ideal. Im nichtkommutativen Fall ist das nicht der Fall (z.B. kann man leicht Beispiele von Summen oberer- und unterer Dreiecksmatrizen hinschreiben, die nicht nilpotent sind), aber in der Situation wie im Fitting-Lemma, wo alle Elemente entweder nilpotent oder invertierbar sind, bilden die nilpotenten Elemente ein Ideal. Allgemeiner zeigen wir:

**Lemma 1.4.39.** *Sei $R$ ein Ring, in dem jedes Element entweder invertierbar oder nilpotent ist. Dann ist $R$ lokal, mit Maximalideal gegeben durch die nilpotenten Elemente.*

*Beweis.* Wir behaupten: Die nilpotenten Elemente sind enthalten im Jacobson-Radikal. Dann folgt automatisch dass das Jacobson-Radikal das eindeutige Maximalideal ist, da ja invertierbare Elemente nicht in echten Idealen enthalten

sein können. Dafür genügt es zu zeigen dass für nilpotentes $x$ und jedes $r$ gilt, dass $(1 - rx)$ invertierbar ist. Zunächst beobachten wir dass $rx$ nicht invertierbar ist: Sei $n$ minimal mit $x^n = 0$, dann wäre für invertierbares $rx$ auch $x^{n-1} = (rx)^{-1}rx^n = 0$. Also ist $rx$ nilpotent, und wenn $(rx)^n = 0$, dann ist

$$1 + rx + (rx)^2 + \ldots + (rx)^{n-1}$$

ein Inverses zu $1 - rx$. □

**Korollar 1.4.40.** Für einen unzerlegbaren Modul $M$ endlicher Länge ist $\mathrm{End}_R(M)$ lokaler Ring.

**Theorem 1.4.41** (Krull-Schmidt)**.** *Sei $M$ ein Modul endlicher Länge. Dann ist die Zerlegung in endlich viele nichttriviale unzerlegbare Summanden (die nach Theorem 1.2.33 existiert) eindeutig bis auf Umordnung der Summanden.*

*Beweis.* Seien $M \cong \bigoplus_{i=1}^n M_i \cong \bigoplus_{i=1}^m M_i'$ zwei solche Zerlegungen. Wir betrachten die Inklusion $M_1 \to M$ und die Projektion $M \to M_1$ als Abbildungen

$$M_1 \xrightarrow{(f_i)} \bigoplus_{i=1}^m M_i' \xrightarrow{(g_i)} M_1.$$

In $\mathrm{End}_R(M_1)$ haben wir also $\sum_{i=1}^m (g_i \circ f_i) = 1$. Da es sich um einen lokalen Ring handelt ist jeder der Summanden entweder invertierbar oder im Maximalideal enthalten, aber da das Maximalideal 1 nicht enthält ist $g_i \circ f_i$ bereits invertierbar für ein $i$. So sehen wir dass $M_1$ direkter Summand von $M_i'$ ist, also sind aufgrund der Unzerlegbarkeit von $M_i'$ bereits $f_i$ und $g_i$ Isomorphismen zwischen $M_1$ und $M_i'$. Nun sind auch Komplemente von $M_1$ bzw. $M_i'$ in $M$ isomorph, also die verbleibenden direkten Summen. Induktiv erhalten wir somit dass jeder Summand in $\bigoplus_{i=1}^n M_i$ zu genau einem aus $\bigoplus_{i=1}^m M_i'$ isomorph ist, und umgekehrt. □

# 2 Kommutative Algebra

## 2.1 Tensorprodukte

Ab jetzt beschäftigten wir uns mit kommutativen Ringen. Für einen kommutativen Ring können wir (wie bereits erwähnt) unkompliziert zwischen Links- und Rechtsmoduln übersetzen.

**Definition 2.1.1.** *Sei $R$ kommutativer Ring. Für $R$-Moduln $M$, $N$ und $U$ heißt eine Abbildung von Mengen*

$$b : M \times N \to U$$

bilinear, *wenn $b(m, -) : N \to U$ für jedes $m \in M$, und $b(-, n) : M \to U$ für jedes $n \in N$, $R$-Modulhomomorphismen sind.*

**Definition 2.1.2.** *Sei $R$ kommutativer Ring und $M$, $N$ $R$-Moduln. Ein* Tensorprodukt *von $M$ und $N$ ist ein $R$-Modul $M \otimes_R N$, zusammen mit einer bilinearen Abbildung*

$$b : M \times N \to M \otimes_R N,$$

*sodass für jeden Modul $U$ mit bilineare Abbildung $b' : M \times N \to U$, ein eindeutiger $R$-Modulhomomorphismus $h : M \otimes_R N \to U$ existiert mit $h \circ b = b'$.*

$$\begin{array}{ccc} M \times N & \xrightarrow{b} & M \otimes_R N \\ & \searrow^{b'} & \downarrow h \\ & & U \end{array}$$

**Lemma 2.1.3.** *Für $R$-Moduln $M$ und $N$ existiert ein Tensorprodukt und ist eindeutig bis auf kanonischen Isomorphismus.*

*Beweis.* Die Eindeutigkeit folgt wie üblich aus der universellen Eigenschaft. Für die Existenz konstruieren wir explizit ein Tensorprodukt. Sei $M \otimes_R N$ ein $R$-Modul

- mit Erzeugern $m \otimes n$ für $(m, n) \in M \times N$ (also Erzeuger in Bijektion mit der Menge $M \times N$, "$m \otimes n$" ist nur Notation für den Erzeuger der dem Paar $(m, n)$ entspricht),
- und Relationen

$$\begin{gathered} (m + m') \otimes n - m \otimes n - m' \otimes n \\ m \otimes (n + n') - m \otimes n - m \otimes n' \\ (rm) \otimes n - r \cdot (m \otimes n) \\ m \otimes (rn) - r \cdot (m \otimes n) \end{gathered}$$

Nun verifizieren wir die universelle Eigenschaft. Wir definieren eine Abbildung $b : M \times N \to M \otimes_R N$, $b(m, n) = m \otimes n$. Dann ist $b$ bilinear, aufgrund der Relationen in $M \otimes_R N$. Für eine bilineare Abbildung $b' : M \times N \to U$ definieren wir nun ein $h : M \otimes_R N \to U$ durch $h(m \otimes n) = b'(m, n)$. Für Wohldefiniertheit müssen wir überprüfen dass die Relationen unter $h$ auf 0 gehen, aber das ist genau Bilinearität von $b'$. Also haben wir ein $h$ mit $h \circ b = b'$ gefunden, umgekehrt muss jedes $h$ mit dieser Eigenschaft ja $h(m \otimes n) = b'(m, n)$ erfüllen, also ist $h$ auch eindeutig. □

**Beispiel 2.1.4.**

1. Sei $M$ frei mit Basis $(x_i)_{i \in I}$ und $N$ frei mit Basis $(y_j)_{j \in J}$. Dann ist $M \otimes_R N$ frei mit Basis $(x_i \otimes y_j)_{(i,j) \in I \times J}$.
2. Es ist $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

**Bemerkung 2.1.5.** Elemente von $M \otimes_R N$ sind *nicht* von der Form $m \otimes n$, sondern Linearkombinationen solcher "Elementartensoren" $\sum m_i \otimes n_i$. Im Allgemeinen ist es leichter, mit der universellen Eigenschaft zu arbeiten.

**Bemerkung 2.1.6.** Eine Variante für nichtkommutative Ringe existiert ebenfalls: Hier muss $M$ ein Rechtsmodul und $N$ ein Linksmodul sein, und $M \otimes_R N$ ist nur noch eine abelsche Gruppe. Insbesondere ist die universelle Eigenschaft eine andere.

## 2.2 Funktoren

**Definition 2.2.1.** *Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Ein* Funktor $F : \mathcal{C} \to \mathcal{D}$ *ist eine Zuordnung, die*

- *jedem Objekt $c \in \mathcal{C}$ ein Objekt $F(c) \in \mathcal{D}$ zuordnet, und*
- *jedem Morphismus $f : c \to d$ in $\mathcal{C}$ einen Morphismus $F(f) : F(c) \to F(d)$ in $\mathcal{D}$ zuordnet*

*sodass die folgenden Eigenschaften erfüllt sind:*

1. $F(\mathrm{id}_c) = \mathrm{id}_{F(c)}$ *für jedes $c \in \mathcal{C}$,*
2. $F(g \circ f) = F(g) \circ F(f)$.

Wenn wir uns Kategorien als algebraische Struktur (Kollektion von Objekten, Kollektion von Morphismen, Verkettungsabbildung etc.) vorstellen, dann sind Funktoren also genau die Homomorphismen solcher Strukturen.

**Beispiel 2.2.2.** 1. Wir haben *Vergissfunktoren*

$$\begin{aligned} \mathrm{LMod}_R &\to \mathrm{Ab} \\ \mathrm{Ab} &\to \mathrm{Grp} \\ \mathrm{Ring} &\to \mathrm{Ab} \\ \mathrm{Grp} &\to \mathrm{Set} \end{aligned}$$

   die $X$ auf $X$ (aufgefasst als Objekt der Zielkategorie) und $f : X \to Y$ auf $f$ (aufgefasst als Morphismus in der Zielkategorie) abbilden, also einfach Struktur vergessen.

2. Wir haben für einen Ringhomomorphismus $\varphi : R \to S$ einen "Einschränkungsfunktor" $\mathrm{LMod}_S \to \mathrm{LMod}_R$, der einen $S$-Modul $M$ als $R$-Modul auffasst, via $r \cdot m := \varphi(r)m$.

3. Für einen kommutativen Ring $R$ und einen festen $R$-Modul $N$ gibt es einen Funktor $F : \mathrm{Mod}_R \to \mathrm{Mod}_R$, der $F(M) = M \otimes_R N$ erfüllt. Er schickt eine Abbildung $f : M \to M'$ auf die induzierte Abbildung $M \otimes_R N \to M' \otimes_R N$, mit $m \otimes n \mapsto f(m) \otimes n$ (äquivalent: Die Abbildung die man aus der universellen Eigenschaft von $M \otimes_R N$ erhält, angewandt auf die bilineare Abbildung $M \times N \to M' \otimes_R N$, $(m, n) \mapsto f(m) \otimes n$).

4. Sei $\mathrm{Ar}(\mathcal{C})$ die Kategorie, deren Objekte gegeben sind durch Morphismen $f : A \to B$ in $\mathcal{C}$, und wo

$$\mathrm{Hom}_{\mathrm{Ar}(\mathcal{C})}(A \to B, A' \to B')$$

besteht aus der Menge aller Diagramme

$$\begin{array}{ccc} A & \longrightarrow & A' \\ \downarrow & & \downarrow \\ B & \longrightarrow & B' \end{array}$$

Dann definieren ker und coker Funktoren $\mathrm{Ar}(\mathrm{LMod}_R) \to \mathrm{LMod}_R$.

**Definition 2.2.3.** *Für Kategorien $\mathcal{C}$ und $\mathcal{D}$ definieren wir $\mathcal{C} \times \mathcal{D}$ als die Kategorie, deren Objekte gegeben sind durch Paare $(c, d)$ mit $c \in \mathcal{C}$, $d \in \mathcal{D}$, und* $\mathrm{Hom}_{\mathcal{C}\times\mathcal{D}}((c, d), (c', d')) = \mathrm{Hom}_{\mathcal{C}}(c, c') \times \mathrm{Hom}_{\mathcal{D}}(d, d')$.

**Beispiel 2.2.4.** Funktoren "in mehreren Variablen" können wir als Funktoren auf einem Produkt von Kategorien auffassen. Zum Beispiel definiert $(M, N) \mapsto M \oplus N$ einen Funktor $\mathrm{LMod}_R \times \mathrm{LMod}_R \to \mathrm{LMod}_R$, und für kommutatives $R$ definiert $(M, N) \mapsto M \otimes_R N$ ebenfalls einen solchen Funktor.

Manche Konstruktionen, wie z.B. der Dualraum von Vektorräumen, kehren Komposition von Morphismen um.

**Definition 2.2.5.** *Für eine Kategorie $\mathcal{C}$ sei $\mathcal{C}^{\mathrm{op}}$ die Kategorie mit denselben Objekten, aber* $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(x, y) = \mathrm{Hom}_{\mathcal{C}}(y, x)$*, mit umgekehrter Komposition.*

**Beispiel 2.2.6.** Für kommutatives $R$ und festes $N \in \mathrm{Mod}_R$ definiert $M \mapsto \mathrm{Hom}_R(M, N)$ einen Funktor $\mathrm{Mod}_R^{\mathrm{op}} \to \mathrm{Mod}_R$. Ein Spezialfall ist der Funktor, der jedem $K$-Vektorraum $V$ seinen Dualraum $V^*$ zuordnet. Wir können $(M, N) \mapsto \mathrm{Hom}_R(M, N)$ auch auffassen als Funktor "in zwei Variablen" $\mathrm{Mod}_R^{\mathrm{op}} \times \mathrm{Mod}_R \to \mathrm{Mod}_R$.

Für Kategorien $\mathcal{C}$ und $\mathcal{D}$ können wir zwischen Funktoren $\mathcal{C} \to \mathcal{D}$ eine Art "Morphismen zwischen Funktoren" definieren:

**Definition 2.2.7.** *Für Kategorien $\mathcal{C}$, $\mathcal{D}$, und zwei Funktoren $F, G : \mathcal{C} \to \mathcal{D}$ besteht eine* natürliche Transformation $\eta : F \to G$ *aus Morphismen*

$$\eta_x : F(x) \to G(x) \quad \textit{für alle } x \in \mathcal{C},$$

*die "zusammenpassen": Für jeden Morphismus $f : x \to y$ in $\mathcal{C}$ soll das Diagramm*

$$\begin{array}{ccc} F(x) & \xrightarrow{\eta_x} & G(x) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(y) & \xrightarrow{\eta_y} & G(y) \end{array}$$

*kommutieren.*

**Bemerkung 2.2.8.** Für Kategorien $\mathcal{C}$ und $\mathcal{D}$, wo $\mathcal{C}$ *klein* ist (die Objekte bilden eine Menge) bilden die Funktoren $\mathcal{C} \to \mathcal{D}$ eine Kategorie $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$, wo die Morphismen durch natürliche Transformationen gegeben sind.

Invertierbare natürliche Transformationen heißen *natürliche Isomorphismen*. Sie erlauben uns, auszudrücken dass zwei Funktoren "gleich" sind.

**Bemerkung 2.2.9.** Funktoren sind selten tatsächlich *gleich*, zum Beispiel ist für Mengen nicht wirklich $X \times (Y \times Z) = (X \times Y) \times Z$, aber es gibt einen natürlichen Isomorphismus (zwischen Funktoren $\mathrm{Set} \times \mathrm{Set} \times \mathrm{Set} \to \mathrm{Set}$), den man aus den universellen Eigenschaften konstruieren kann. Natürlicher Isomorphismus von Funktoren ist also der nützlichere Äquivalenzbegriff.

**Beispiel 2.2.10.**

1. Wir können $(M_1, M_2) \mapsto M_1 \oplus M_2$ sowie $(M_1, M_2) \mapsto M_1$, $(M_1, M_2) \mapsto M_2$ als Funktoren $\mathrm{Mod}_R \times \mathrm{Mod}_R \to \mathrm{Mod}_R$ auffassen. Dann sind die Inklusionsabbildungen

   $$M_1 \to M_1 \oplus M_2, \quad M_2 \to M_1 \oplus M_2$$

   sowie die Projektionsabbildungen

   $$M_1 \oplus M_2 \to M_1, \quad M_1 \oplus M_2 \to M_2$$

   natürliche Transformationen zwischen Funktoren $\mathrm{Mod}_R \times \mathrm{Mod}_R \to \mathrm{Mod}_R$.

2. Die universelle Eigenschaft des Tensorprodukts liefert für Moduln $M, N, U$ einen Isomorphismus

   $$\mathrm{Hom}_R(M \otimes N, U) \cong \mathrm{Bil}_R(M \times N, U).$$

   Für festes $U$ können wir beide Seiten als Funktoren

   $$\mathrm{Mod}_R^{\mathrm{op}} \times \mathrm{Mod}_R^{\mathrm{op}} \to \mathrm{Set}$$

   auffassen, und den Isomorphismus als natürliche Transformation.

3. Wir haben einen natürlichen Isomorphismus

   $$\mathrm{Bil}_R(M \times N, U) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, U))$$

   der eine bilineare Abbildung $b$ schickt auf

   $$m \mapsto (n \mapsto b(m, n)),$$

   und umgekehrt ein $f : M \to \mathrm{Hom}_R(N, U)$ auf die bilineare Abbildung

   $$(m, n) \mapsto f(m)(n)$$

**Lemma 2.2.11.** *Sei $R$ kommutativer Ring,*

$$A \to B \to C \to 0$$

*eine exakte Folge von $R$-Moduln, und $M$ ein $R$-Modul. Dann ist*

$$A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

*ebenfalls exakt. (Man sagt: $(- \otimes_R M)$ ist ein* rechtsexakter *Funktor* $\mathrm{Mod}_R \to \mathrm{Mod}_R$*)*

*Beweis.* Es genügt zu zeigen dass $B \otimes_R M \to C \otimes_R M$ ein Kokern von $A \otimes_R M \to B \otimes_R M$ ist, also dass

$$0 \to \mathrm{Hom}_R(C \otimes_R M, U) \to \mathrm{Hom}_R(B \otimes_R M, U) \to \mathrm{Hom}_R(A \otimes_R M, U)$$

exakt ist (Exaktheit hier bedeutet ja genau dass eine Abbildung $B \otimes_R M \to U$ eindeutig durch $C \otimes_R M$ faktorisiert wenn die Komposition $A \otimes_R M \to B \otimes_R M \to U$ null ist.)

Aber obige Folge ist isomorph zu der Folge

$$0 \to \mathrm{Hom}_R(C, \mathrm{Hom}_R(M, U)) \to \mathrm{Hom}_R(B, \mathrm{Hom}_R(M, U)) \to \mathrm{Hom}_R(A, \mathrm{Hom}_R(M, U)).$$

Diese ist exakt weil $C$ ein Kokern von $A \to B$ ist, und somit eine Abbildung $B \to \mathrm{Hom}_R(M, U)$ eindeutig durch $C$ faktorisiert wenn die Komposition $A \to B \to \mathrm{Hom}_R(M, U)$ null ist. □

**Definition 2.2.12.** *Sei $R$ kommutativer Ring. Ein $R$-Modul $M$ heißt* flach*, wenn für jede exakte Folge von $R$-Moduln*

$$0 \to A \to B \to C \to 0$$

*auch*

$$0 \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

*exakt ist.*

**Beispiel 2.2.13.**

1. $R$ als $R$-Modul ist flach, da $A \otimes_R R \cong A$ (natürlich). Allgemeiner ist ein freier $R$-Modul $\bigoplus_{i \in I} R$ flach, da $A \otimes_R \bigoplus_{i \in I} R \cong \bigoplus_{i \in I} A$ (ebenfalls natürlich), und direkte Summen von exakten Folgen wieder exakt sind.

2. $M = \mathbb{Z}/n\mathbb{Z}$ als $\mathbb{Z}$-Modul ist nicht flach, da die Folge

   $$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

   nach Tensorieren mit $M$ die Folge

   $$0 \to \mathbb{Z} \otimes M \xrightarrow{n} \mathbb{Z} \otimes M \to \mathbb{Z}/n\mathbb{Z} \otimes M \to 0$$

   ergibt, aber $\mathbb{Z} \otimes M \cong M$, die linke Abbildung ist die Multiplikation-mit-$n$-Abbildung $M \to M$, und diese ist nicht injektiv.

## 2.3 Lokalisierungen von Ringen

**Definition 2.3.1.** *Sei $R$ kommutativ. Ein Element $r \neq 0 \in R$ heißt* Nullteiler*, wenn es ein $s \neq 0$ gibt mit $rs = 0$. Ein Ring $R$ heißt* nullteilerfrei*, $1 \neq 0$ und wenn aus $rs = 0$ bereits $r = 0$ oder $s = 0$ folgt, er also keine Nullteiler enthält.*

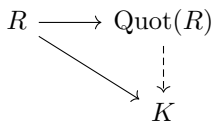
Zum Beispiel sind Körper und $\mathbb{Z}$ nullteilerfrei, und wenn $R$ nullteilerfrei ist ist auch $R[x]$ nullteilerfrei. Nullteilerfreie Ringe werden auch "Integritätsbereiche" (engl. "integral domain") genannt.

Für einen nullteilerfreien Ring $R$ können wir einen Körper $\mathrm{Quot}(R)$ bauen, den *Quotientenkörper* von $R$, indem wir die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ imitieren:

- Elemente von $\mathrm{Quot}(R)$ sind Äquivalenzklassen von Paaren $(a, b) \in R^2$ mit $b \neq 0$, wo $(a, b) \sim (a', b')$ genau dann wenn $ab' = a'b$, und wir schreiben die Äquivalenzklasse von $(a, b)$ als $\frac{a}{b}$.
- Die Ringstruktur ist definiert als $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ und $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ (mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$).

Zum Beispiel ist $Q(\mathbb{Z}) = \mathbb{Q}$. Wir haben eine Abbildung $R \to \mathrm{Quot}(R)$, $r \mapsto \frac{r}{1}$, und $\mathrm{Quot}(R)$ hat die folgende universelle Eigenschaft:

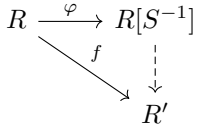
Jeder *injektive* Ringhomomorphismus $R \to K$, wo $K$ ein Körper ist, faktorisiert eindeutig durch $R \to \mathrm{Quot}(R)$.




Man kann sich $\mathrm{Quot}(R)$ als die universelle Art vorstellen, alle Elemente $r \neq 0$ in $R$ invertierbar zu machen. Wir werden nun eine allgemeinere Konstruktion betrachten, die beliebige Elemente invertiert.

**Definition 2.3.2.** *Sei $R$ ein kommutativer Ring, und $S \subseteq R$ eine Teilmenge. Eine* Lokalisierung von $R$ an $S$ *ist ein Ring $R[S^{-1}]$*

1. *mit einem Homomorphismus $\varphi : R \to R[S^{-1}]$, sodass $\varphi(s)$ in $R[S^{-1}]$ invertierbar ist für alle $s \in S$,*
2. *sodass jeder Homomorphismus $f : R \to R'$, wo $f(s)$ in $R'$ invertierbar ist für alle $s \in S$, eindeutig durch $\varphi$ faktorisiert.*




Wir werden gleich sehen, dass Lokalisierungen immer existieren, und eine explizite Beschreibung angeben. Wir beobachten zunächst: Wenn $R \to R'$ Elemente $r, s$ auf invertierbare Elemente schickt, dann natürlich auch $rs$.

**Definition 2.3.3.** *Eine Teilmenge $S \subseteq R$ heißt* multiplikativ abgeschlossen *wenn $1 \in S$ und mit $s, s' \in S$ auch $ss' \in S$ gilt. Für eine Teilmenge $S \subseteq R$ definieren wir den* multiplikativen Abschluss $\overline{S}$ *als die kleinste multiplikativ abgeschlossene Teilmenge von $R$, die $S$ enthält.*

Zum Beispiel besteht der multiplikative Abschluss von $\{2, 3\} \in \mathbb{Z}$ aus allen Zahlen der Form $2^n 3^m$.

**Proposition 2.3.4.** *Für $S \subseteq R$ stellt der folgende Ring eine Lokalisierung von $R$ an $S$ dar (den wir deshalb als $R[S^{-1}]$ schreiben):*

- *Elemente von $R[S^{-1}]$ sind Äquivalenzklassen von Paaren $(r, s)$ mit $s \in \overline{S}$ und $r \in R$, wobei $(r, s) \sim (r', s')$ wenn es ein $t \in \overline{S}$ gibt mit $trs' = tr's$. Wir schreiben $\frac{r}{s}$ für die Äquivalenzklasse von $(r, s)$.*
- *Die Ringstruktur ist gegeben durch $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ und $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ (mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$).*
- *Die Abbildung $R \to R[S^{-1}]$ ist gegeben durch $r \mapsto \frac{r}{1}$.*

*Insbesondere bedeutet das: Lokalisierungen existieren und sind eindeutig bis auf kanonischen Isomorphismus.*

*Beweis.* Zunächst überprüfen wir, dass es sich um eine Äquivalenzrelation handelt. Offenbar ist sie reflexiv und symmetrisch, für Transitivität seien $(r, s)$, $(r', s')$, $(r'', s'')$, $t$, $t'$ mit $trs' = tr's$ und $t'r's'' = t'r''s'$ gegeben. Dann ist

$$(tt's')rs'' = tt'r'ss'' = (tt's')r''s,$$

also (da $tt's' \in \overline{S}$) $(r, s) \sim (r'', s'')$).

Nun überprüft man leicht, dass es sich um eine Ringstruktur handelt. Die Abbildung $R \to R[S^{-1}]$ schickt außerdem $s \in \overline{S}$ auf ein invertierbares Element in $R[S^{-1}]$, da $\frac{s}{1} \cdot \frac{1}{s} = 1$. Sei schließlich $f : R \to R'$ ein Ringhomomorphismus mit der Eigenschaft dass $f(s)$ in $R'$ invertierbar ist für alle $s \in S$. Dann definiert

$$R[S^{-1}] \to R', \quad \frac{r}{s} \mapsto f(r) \cdot f(s)^{-1}$$

einen wohldefinierten Ringhomomorphismus: Wenn $\frac{r}{s} = \frac{r'}{s'}$, also existiert $t \in S$ mit $trs' = tr's$, dann ist ja

$$f(t)f(r)f(s') = f(t)f(r')f(s) \quad \text{in } R',$$

also $f(r)f(s') = f(r')f(s)$ nach Multiplikation mit $f(t)^{-1}$. Außerdem sieht man leicht dass jeder Homomorphismus $R[S^{-1}] \to R'$, der $f$ faktorisiert, diese Form haben muss, indem man ihn auf $\frac{s}{1} \cdot \frac{r}{s} = \frac{r}{1}$ anwendet. □

Wir beobachten, dass die Lokalisierung an $S$ nur von $\overline{S}$ abhängt. Trotzdem ist es nützlich, diese Konstruktion (und ihre universelle Eigenschaft) auch für nicht multiplikativ abgeschlossene Teilmengen betrachten zu können (z.B. einzelne Elemente).

**Beispiel 2.3.5.**

- Wenn $0 \in \overline{S}$, dann ist $R[S^{-1}] = 0$.
- Für einen nullteilerfreien Ring $R$ ist $\mathrm{Quot}(R) = R[S^{-1}]$ für $S = R \setminus \{0\}$ (Nullteilerfreiheit bedeutet genau dass diese Menge bereits multiplikativ abgeschlossen ist).
- Allgemeiner liegt $r \in R$ im Kern von $R \to R[S^{-1}]$ genau wenn es ein $s \in \overline{S}$ mit $rs = 0$ gibt. Insbesondere ist für nullteilerfreies $R$ und $0 \notin S$ die Abbildung injektiv. Da in diesem Fall auch $R[S^{-1}]$ nullteilerfrei ist, können wir $R[S^{-1}]$ als Unterring von $\mathrm{Quot}(R)$ auffassen.
- Für eine Teilmenge von Primzahlen $S \subseteq \mathbb{P}$ besteht die Lokalisierung $\mathbb{Z}[S^{-1}]$ aus allen Brüchen $\frac{a}{b}$ wo $b$ nur Primfaktoren aus $S$ hat. Zum Beispiel erhalten wir $\mathbb{Z}_{(p)}$ (der uns im Kontext lokaler Ringe begegnet ist) für $S = \{\text{alle Primzahlen außer } p\}$. Tatsächlich sind alle Unterringe von $\mathbb{Q}$ von der Form $\mathbb{Z}[S^{-1}]$ für eine Menge von Primzahlen.

Wir wollen schließlich noch darauf eingehen was Lokalisierungen mit lokalen Ringen zu tun haben.

**Definition 2.3.6.** *Sei $R$ ein kommutativer Ring. Ein Ideal $I \subseteq R$ heißt* Primideal*, wenn es ein echtes Ideal ist, und aus $ab \in I$ bereits $a \in I$ oder $b \in I$ folgt.*

**Lemma 2.3.7.** *Sei $R$ kommutativer Ring und $I \subseteq R$ ein Ideal. Die folgenden Aussagen sind äquivalent:*

1. *$I$ ist Primideal.*
2. *$R/I$ ist nullteilerfrei.*
3. *Das Komplement $R \setminus I$ ist multiplikativ abgeschlossen.*

*Beweis.* $1 \Leftrightarrow 2$: Wenn $a, b \in R$ Elemente sind, dann ist $ab + I = 0 + I$ in $R/I$ genau wenn $ab \in I$, und $a + I = 0 + I$ genau wenn $a \in I$, etc. Also ist Nullteilerfreiheit von $R/I$ genau die Aussage, dass aus $ab \in I$ folgt $a \in I$ oder $b \in I$, also dass $I$ Primideal ist.

$1 \Leftrightarrow 3$: Die Definition von Primidealen übersetzt sich zu $1 \in R \setminus I$ und $a, b \in R \setminus I \Rightarrow ab \in R \setminus I$, also dass $R \setminus I$ multiplikativ abgeschlossen ist. □

Die Primideale sind also genau die Kerne von Homomorphismen $R \to R'$ mit $R'$ nullteilerfrei. Wir beobachten auch, dass Maximalideale Primideale sind, da $I \subseteq R$ maximal ist genau wenn $R/I$ ein Körper ist.

**Definition 2.3.8.** *Wir schreiben*

$$\mathrm{Spec}(R) := \{I \subseteq R \mid I \textit{ prim}\}$$
$$\mathrm{mSpec}(R) := \{I \subseteq R \mid I \textit{ maximal}\}$$

**Lemma 2.3.9.** *Für einen Ringhomomorphismus $f : R \to R'$ und ein Primideal $\mathfrak{p} \subseteq R'$ ist das Urbild $f^{-1}(\mathfrak{p})$ ein Primideal in $R$. Insbesondere definiert* $\mathrm{Spec} : \mathrm{CRing}^{\mathrm{op}} \to \mathrm{Set}$ *einen Funktor.*

*Beweis.* Das Urbild $f^{-1}(\mathfrak{p})$ ist der Kern der Komposition $R \to R' \to R'/\mathfrak{p}$. Wenn $\mathfrak{p}$ prim ist, ist $R'/\mathfrak{p}$ nullteilerfrei, also der Kern $R \to R'/\mathfrak{p}$ ebenfalls prim. □

**Lemma 2.3.10.** *Sei $S \subseteq R$. Dann ist*

$$\mathrm{Spec}(R) \to \mathrm{Spec}(R[S^{-1}])$$

*injektiv, mit Bild*

$$\{\mathfrak{p} \in \mathrm{Spec}(R) \mid S \cap \mathfrak{p} = \emptyset\}.$$

*Beweis.* Sei $\mathfrak{p} \subseteq R[S^{-1}]$ ein Primideal. Dann ist das Urbild $f^{-1}(\mathfrak{p})$ unter $f : R \to R[S^{-1}]$ ein Primideal in $R$ (der Kern der Komposition $R \to R[S^{-1}] \to R[S^{-1}]/\mathfrak{p}$), und $f^{-1}(\mathfrak{p}) \cap S = \emptyset$. Wäre nämlich $s \in f^{-1}(\mathfrak{p}) \cap S$, so wäre $f(s) \in \mathfrak{p}$, aber andererseits in $R[S^{-1}]$ invertierbar.

Sei umgekehrt $\mathfrak{p} \subseteq R$ ein Primideal mit $\mathfrak{p} \cap S = \emptyset$. Dann ist $R/\mathfrak{p}$ nullteilerfrei, und das Bild von $S$ in $R/\mathfrak{p}$ enthält nicht die 0. Wir können also $R/\mathfrak{p}[S^{-1}]$ bilden und erhalten wieder einen nullteilerfreien Ring. Ferner ist die kanonische Abbildung $R[S^{-1}] \to R/\mathfrak{p}[S^{-1}]$ surjektiv, und ihr Kern ist ein Primideal in $R[S^{-1}]$ (das sich explizit beschreiben lässt als $R[S^{-1}]f(\mathfrak{p})$). Da der Kern von $R \to R[S^{-1}] \to R/\mathfrak{p}[S^{-1}]$ wieder $\mathfrak{p}$ ist, sind diese beiden Konstruktionen invers zueinander. □

**Korollar 2.3.11.** Sei $\mathfrak{p} \subseteq R$ ein Primideal. Dann ist $S = R \setminus \mathfrak{p}$ multiplikativ abgeschlossen, und

$$R_{\mathfrak{p}} := R[S^{-1}]$$

ist ein lokaler Ring mit Maximalideal $R_{\mathfrak{p}} \cdot \mathfrak{p}$ und Restklassenkörper $R_{\mathfrak{p}}/R_{\mathfrak{p}} \cdot \mathfrak{p} \cong \mathrm{Quot}(R/\mathfrak{p})$.

*Beweis.* Nach dem vorangehenden Lemma korrespondieren die Primideale in $R_{\mathfrak{p}}$ zu den Primidealen von $R$, die $S = R \setminus \mathfrak{p}$ nicht enthalten. Jedes Primideal von $R_{\mathfrak{p}}$ ist also in $R_{\mathfrak{p}} \cdot \mathfrak{p}$ enthalten. Insbesondere ist $R_{\mathfrak{p}} \cdot \mathfrak{p}$ das eindeutige Maximalideal (da jedes Maximalideal prim ist, und jedes Ideal in einem Maximalideal enthalten ist).

Schließlich ist $R_{\mathfrak{p}}/R_{\mathfrak{p}} \cdot \mathfrak{p}$ die Lokalisierung von $R/\mathfrak{p}$ am Bild von $S$. Dieses besteht allerdings aus allen Elementen, die nicht 0 sind. □

Ein Beispiel ist $\mathbb{Z}_{(p)}$, wo wir beim Primideal $(p) \subseteq \mathbb{Z}$ lokalisiert haben.

**Bemerkung 2.3.12.** Lokalisieren an $S$ entfernt also aus $\mathrm{Spec}(R)$ genau diejenigen $\mathfrak{p} \subseteq R$, die Elemente von $S$ enthalten, macht also $\mathrm{Spec}(R)$ kleiner. In Algebraischer Geometrie wird diese Idee weiter ausgebaut, indem man $\mathrm{Spec}(R)$ mit einer Topologie versieht, die Teilmengen $\mathrm{Spec}(R[S^{-1}])$ sind die "offenen

Umgebungen", und viele Eigenschaften von Ringen lassen sich "lokal", also auf einer offenen Überdeckung verifizieren.

Lokale Ringe sind diejenigen Ringe, wo $\mathrm{Spec}(R)$ bereits besonders klein ist: Lokal ist äquivalent dazu, dass $\mathrm{mSpec}(R) \subseteq \mathrm{Spec}(R)$ aus exakt einem Element besteht.

## 2.4 Lokalisierungen von Moduln

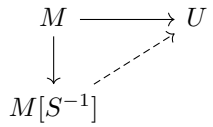
Sei $R$ ein kommutativer Ring und $M$ ein $R$-Modul. Für eine Teilmenge $S \subseteq R$ können wir aus $M$ einen $R[S^{-1}]$-Modul machen, indem wir tensorieren:

**Definition 2.4.1.** *Wir definieren*

$$M[S^{-1}] = R[S^{-1}] \otimes_R M.$$

**Lemma 2.4.2.** *1. $M[S^{-1}]$ besitzt eine explizite Beschreibung wie folgt: Elemente sind Äquivalenzklassen von Paaren $(m, s)$ mit $m \in M$, $s \in \overline{S}$, mit $(m, s) \sim (m', s')$ genau dann wenn es ein $t \in \overline{S}$ gibt mit $ts'm = tsm'$, und wir schreiben $\frac{m}{s}$ für die Äquivalenzklasse von $(m, s)$. Die Addition ist gegeben durch $\frac{m}{s} + \frac{m'}{s'} = \frac{ms'+m's}{ss'}$, und die Modulstruktur durch $\frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}$.*

*2. $M[S^{-1}]$ erfüllt die folgende universelle Eigenschaft: Er ist ausgestattet mit einer $R$-linearen Abbildung $M \to M[S^{-1}]$, und für jeden $R[S^{-1}]$-Modul $U$ und eine $R$-lineare Abbildung $M \to U$ faktorisiert diese eindeutig durch eine $R[S^{-1}]$-lineare Abbildung $M[S^{-1}] \to U$.*




*Äquivalent gibt es einen natürlichen Isomorphismus*

$$\mathrm{Hom}_{R[S^{-1}]}(M[S^{-1}], U) \cong \mathrm{Hom}_R(M, U).$$

*Beweis.* Sei $M[S^{-1}]'$ temporäre Notation für den explizit beschriebenen Modul aus 1. Dann gibt es eine $R$-bilineare Abbildung

$$b : R[S^{-1}] \times M \to M[S^{-1}]'$$

mit $(\frac{r}{s}, m) \mapsto \frac{rm}{s}$. Für jede $R$-bilineare Abbildung $b' : R[S^{-1}] \times M \to U$ in irgendeinen $R$-Modul $U$ definieren wir nun eine Abbildung $h : M[S^{-1}]' \to U$ durch $h(\frac{m}{s}) = b'(\frac{1}{s}, m)$. Diese ist wohldefiniert, da mit $tsm' = ts'm$ auch

$$b'\left(\frac{1}{s}, m\right) = b'\left(\frac{1}{tss'}, ts'm\right) = b'\left(\frac{1}{tss'}, tsm'\right) = b'\left(\frac{1}{s'}, m'\right).$$

Wir haben also ein $h$ mit $h \circ b = b'$ gefunden. Umgekehrt muss jedes solche $h$ von der Form sein, ist also eindeutig. Also erfüllt $M[S^{-1}]'$ die universelle Eigenschaft des Tensorprodukts, $b$ induziert also einen Isomorphismus $M[S^{-1}] \to M[S^{-1}]'$.

Für die zweite Aussage beobachten wir dass für $f : M \to U$ jede $R[S^{-1}]$-lineare Faktorisierung durch $M[S^{-1}]$ durch $\frac{m}{s} \mapsto \frac{1}{s} \cdot f(m)$ beschrieben wird, und das auch eine wohldefinierte Abbildung definiert. □

**Lemma 2.4.3.** *$R[S^{-1}]$ ist flacher R-Modul, d.h. für*

$$0 \to A \xrightarrow{f} B \to C \to 0$$

*eine exakte Folge von R-Moduln, ist auch*

$$0 \to A[S^{-1}] \to B[S^{-1}] \to C[S^{-1}] \to 0$$

*exakt.*

*Beweis.* Es ist nur zu zeigen, dass $A[S^{-1}] \to B[S^{-1}]$ injektiv ist. Sei $\frac{a}{s}$ ein Element im Kern. Dann ist also $\frac{f(a)}{s} = 0$ in $B[S^{-1}]$, also existiert $t \in \overline{S}$ mit $tf(a) = 0$. Also ist $f(ta) = 0$, somit $ta = 0$ aufgrund der Injektivität von $f$. Das impliziert nun aber wiederum $\frac{a}{s} = 0$ in $A[S^{-1}]$. □

Insbesondere bedeutet das dass Lokalisieren Kerne und Kokerne erhält, und somit auch Injektivität, Surjektivität und längere exakte Folgen. Was können wir umgekehrt über einen Modul sagen, wenn wir Lokalisierungen kennen? Analog zur Situation von Ringen definieren wir $M_\mathfrak{p} := M[(R \setminus \mathfrak{p})^{-1}] = R_\mathfrak{p} \otimes_R M$ für ein Primideal $\mathfrak{p} \subseteq R$.

**Lemma 2.4.4.** *Sei $R$ ein kommutativer Ring. Dann gilt:*

1. *Die kanonische Abbildung $M \to \prod_{\mathfrak{m} \subseteq R \text{ maximal}} M_\mathfrak{m}$ ist injektiv.*
2. *Für einen R-Modul $M$ ist $M = 0$ genau wenn $M_\mathfrak{m} = 0$ für alle Maximalideale $\mathfrak{m} \subseteq R$.*
3. *Eine Abbildung $f : M \to N$ ist null genau wenn $M_\mathfrak{m} \to N_\mathfrak{m}$ null ist für jedes Maximalideal $\mathfrak{m} \subseteq R$.*
4. *Für eine Abbildung $f : M \to N$ von R-Moduln ist $f$ surjektiv/injektiv/Isomorphismus genau wenn $M_\mathfrak{m} \to N_\mathfrak{m}$ surjektiv/injektiv/Isomorphismus ist für alle Maximalideale $\mathfrak{m} \subseteq R$.*
5. *Eine Folge $A \to B \to C$ von R-Moduln ist exakt genau dann wenn $A_\mathfrak{m} \to B_\mathfrak{m} \to C_\mathfrak{m}$ exakt ist für jedes Maximalideal $\mathfrak{m} \subseteq R$.*

*Beweis.* Für die erste Aussage müssen wir zeigen dass wenn $\frac{x}{1} = 0$ in $M_\mathfrak{m}$ für alle $\mathfrak{m}$, dann ist $x = 0$. Angenommen $x \neq 0$, dann ist $\operatorname{ann}_R(x) \subseteq R$ ein echtes Ideal. Wir finden also ein Maximalideal mit $\operatorname{ann}_R(x) \subseteq \mathfrak{m}$. Wenn $\frac{x}{1} = 0$ in $M_\mathfrak{m}$, dann gibt es ein $s \notin \mathfrak{m}$ mit $sx = 0$, Widerspruch. Also ist $x = 0$.

Die zweite Aussage folgt direkt aus der ersten, und die dritte ebenfalls, indem man das kommutative Diagramm

$$\begin{array}{ccc} M & \hookrightarrow & \prod M_{\mathfrak{m}} \\ \downarrow & & \downarrow 0 \\ N & \hookrightarrow & \prod M_{\mathfrak{m}} \end{array}$$

betrachten. Für die vierte benutzen wir Exaktheit von Lokalisierungen, und wenden die zweite Aussage auf Kokern bzw. Kern an. Schließlich sei $A \to B \to C$ eine Folge, für die $A_{\mathfrak{m}} \to B_{\mathfrak{m}} \to C_{\mathfrak{m}}$ für alle $\mathfrak{m}$ exakt ist. Dann ist die Komposition $A \to C$ null aufgrund der dritten Aussage. Wir haben also eine kanonische Abbildung $A \to \ker(B \to C)$, und nach Annahme ist diese nach Lokalisierung bei allen $\mathfrak{m}$ surjektiv. Also ist sie surjektiv, also $A \to B \to C$ exakt. □

**Bemerkung 2.4.5.** Es ist nicht richtig, dass wenn $M_{\mathfrak{m}} \cong N_{\mathfrak{m}}$ für jedes $\mathfrak{m}$, auch $M \cong N$ gilt, wir benötigen einen passenden Homomorphismus $M \to N$. Ein Beispiel liefert $R = \mathbb{Z}[\sqrt{-5}]$ und $M = (2, 1 + \sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$ das von $2, 1 + \sqrt{-5}$ erzeugte Ideal. Das ist kein Hauptideal, als $M \ncong R$, aber sowohl $M[2^{-1}]$ als auch $M[3^{-1}]$ sind isomorph zu freien $R[2^{-1}]$ bzw. $R[3^{-1}]$-Moduln auf einem Erzeuger. Da 2 und 3 das Einsideal erzeugen, also für jedes Maximalideal $2 \notin \mathfrak{m}$ oder $3 \notin \mathfrak{m}$, folgt dann auch $M_{\mathfrak{m}} \cong R_{\mathfrak{m}}$ für jedes $\mathfrak{m}$.

Wir haben hier also eine Reihe von Eigenschaften von $R$-Moduln, die erfüllt sind genau dann wenn sie für die durch Lokalisierung bei allen Maximalidealen $\mathfrak{m}$ erhaltenen $R_{\mathfrak{m}}$-Moduln erfüllt sind.

**Definition 2.4.6.** *Wir nennen eine Eigenschaft von Moduln* lokal*, wenn gilt:*

1. *Wenn die Eigenschaft für einen $R$-Modul $M$ erfüllt ist, dann auch für alle $R[S^{-1}]$-Moduln $M[S^{-1}]$.*
2. *Wenn für einen $R$-Modul $M$ für jedes Maximalideal $\mathfrak{m} \subseteq R$ die Eigenschaft für alle $R_{\mathfrak{m}}$-Moduln $M_{\mathfrak{m}}$ erfüllt ist, dann ist sie auch für $M$ erfüllt.*

*Analog nennen wir auch Eigenschaften von Ringen, von Modulhomomorphismen $M \to N$ etc. lokal, wenn die entsprechenden Implikationen gelten.*

**Lemma 2.4.7.** *Flachheit ist eine lokale Eigenschaft, also:*

1. *Wenn $M$ flacher $R$-Modul ist, dann ist $M[S^{-1}]$ flacher $R[S^{-1}]$-Modul für jede Teilmenge $S \subseteq R$.*
2. *Wenn für einen $R$-Modul $M_{\mathfrak{m}}$ flacher $R_{\mathfrak{m}}$-Modul für jedes Maximalideal $\mathfrak{m} \subseteq R$ ist, dann ist $M$ flacher $R$-Modul.*

*Beweis.* Für die erste Aussage sei $M$ flach über $R$, und $0 \to A \to B \to C \to 0$ eine kurze exakte Folge von $R[S^{-1}]$-Moduln. Wir behaupten, dass

$$0 \to A \otimes_{R[S^{-1}]} M[S^{-1}] \to B \otimes_{R[S^{-1}]} M[S^{-1}] \to C \otimes_{R[S^{-1}]} M[S^{-1}] \to 0$$

eine exakte Folge ist. Wir haben allerdings $A \otimes_{R[S^{-1}]} M[S^{-1}] \cong A \otimes_R M$ aufgrund der universellen Eigenschaft des Tensorprodukts, da jede $R$-bilineare Abbildung $b : A \times M \to U$ eindeutig durch eine $R[S^{-1}]$-bilineare Abbildung $b' : A \times M[S^{-1}] \to U$ faktorisiert, gegeben durch $b'(a, \frac{m}{s}) = b(\frac{1}{s}a, m)$, unter Benutzung der Tatsache dass $A$ ein $R[S^{-1}]$-Modul ist. Analog ist die gesamte Folge Isomorph zur Folge

$$0 \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0,$$

die nach Flachheit von $M$ exakt ist.

Für die zweite Aussage sei Sei $0 \to A \to B \to C \to 0$ eine kurze exakte Folge von $R$-Moduln, und $M_\mathfrak{m}$ flacher $R_\mathfrak{m}$-Modul für jedes $\mathfrak{m}$. Wir müssen zeigen, dass $0 \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$ exakt ist, und dafür genügt es zu zeigen dass $0 \to (A \otimes_R M)_\mathfrak{m} \to (B \otimes_R M)_\mathfrak{m} \to (C \otimes_R M)_\mathfrak{m} \to 0$ exakt ist für alle $\mathfrak{m}$.

Aber $(A \otimes_R M)_\mathfrak{m} \cong A \otimes_R M \otimes_R R_\mathfrak{m} \cong A \otimes_R M_\mathfrak{m} \cong A_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m}$, wieder aufgrund der universellen Eigenschaft des Tensorprodukts. Nun ist

$$0 \to A_\mathfrak{m} \to B_\mathfrak{m} \to C_\mathfrak{m} \to 0$$

exakt aufgrund der Exaktheit von Lokalisierungen, und somit

$$0 \to A_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \to B_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \to C_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \to 0$$

exakt aufgrund der Flachheit von $M_\mathfrak{m}$, somit ist

$$0 \to (A \otimes_R M)_\mathfrak{m} \to (B \otimes_R M)_\mathfrak{m} \to (C \otimes_R M)_\mathfrak{m} \to 0$$

exakt wie gewünscht. □

Lemma 2.4.4 kombiniert sich außerdem mit unserer vorherigen Form des Nakayama-Lemmas zu folgender nützlicher Aussage, die ebenfalls oft Nakayama-Lemma genannt wird:

**Lemma 2.4.8** (Nakayama-Lemma, Version 2)**.** *Sei $R$ ein kommutativer Ring, $M$ ein endlich erzeugter $R$-Modul, und $\mathfrak{m} \subseteq R$ ein Maximalideal. Die folgenden Aussagen sind äquivalent:*

1. *$M/\mathfrak{m}M = 0$*
2. *$M_\mathfrak{m} = 0$*
3. *Es existiert ein $s \notin \mathfrak{m}$ mit $sM = 0$, insbesondere $M[s^{-1}] = 0$.*

*Beweis.* (1) $\Leftrightarrow$ (2): Indem wir die exakte Folge

$$0 \to \mathfrak{m}M \to M \to M/\mathfrak{m}M \to 0$$

bei $\mathfrak{m}$ lokalisieren, erhalten wir

$$0 \to (\mathfrak{m}M)_\mathfrak{m} \to M_\mathfrak{m} \to (M/\mathfrak{m}M)_\mathfrak{m} \to 0.$$

Da $M/\mathfrak{m}M$ ein $R/\mathfrak{m}$-Modul ist, und darin bereits alle Elemente aus $R \setminus \mathfrak{m}$ auf invertierbare Elemente abbilden ($R/\mathfrak{m}$ ist ein Körper), ist ferner $(M/\mathfrak{m}M)_\mathfrak{m} \cong M/\mathfrak{m}M$, und somit sehen wir

$$M/\mathfrak{m}M \cong M_\mathfrak{m}/(\mathfrak{m}M)_\mathfrak{m}.$$

Nun ist $(\mathfrak{m}M)_\mathfrak{m} = (R_\mathfrak{m}\mathfrak{m}) \cdot M$, und $R_\mathfrak{m}\mathfrak{m} = \mathrm{Jac}(R_\mathfrak{m})$. Das Nakayama-Lemma angewandt auf den endlich erzeugten $R_\mathfrak{m}$-Modul $M_\mathfrak{m}$ liefert also $M_\mathfrak{m} = 0$, und die Rückrichtung ist klar.

(2) $\Leftrightarrow$ (3): Da $M$ endlich erzeugt ist, finden wir endlich viele Erzeuger $m_1, \ldots, m_n$. Wenn $M_\mathfrak{m} = 0$ finden wir für jeden davon ein $s_i \notin \mathfrak{m}$ mit $s_i m_i = 0$. Indem wir $s = \prod s_i$ setzen, haben wir ein $s \notin \mathfrak{m}$ mit $sm_i = 0$, also $sM = 0$, also insbesondere $M[s^{-1}] = 0$. Die Umkehrung ist trivial. □

**Bemerkung 2.4.9.** Hier wird über drei verschiedenen Ringen gearbeitet: Dem Körper $R/\mathfrak{m}$, dem lokalen Ring $R_\mathfrak{m}$, und dem Ring $R[s^{-1}]$ für ein $s \notin \mathfrak{m}$. Wir haben Abbildungen

$$R \to R[s^{-1}] \to R_\mathfrak{m} \to R/\mathfrak{m},$$

und entsprechend Abbildungen

$$\mathrm{Spec}(R) \leftarrow \mathrm{Spec}(R[s^{-1}]) \leftarrow \mathrm{Spec}(R_\mathfrak{m}) \leftarrow \mathrm{Spec}(R/\mathfrak{m}).$$

Diese sind alle injektiv, da die ersten zwei von Lokalisierungen kommen, und für die dritte beobachten wir dass $\mathrm{Spec}(R/\mathfrak{m}) = \{(0)\}$ da $R/\mathfrak{m}$ Körper ist, und das Urbild von $(0) \subseteq R/\mathfrak{m}$ in $R$ ist $\mathfrak{m}$. $\mathrm{Spec}(R/\mathfrak{m})$ besteht also exakt aus $\mathfrak{m} \in \mathrm{Spec}(R)$, $\mathrm{Spec}(R_\mathfrak{m})$ aus $\mathfrak{m}$ und allen darin enthaltenen Primidealen, $\mathrm{Spec}(R[s^{-1}])$ aus einer größeren Teilmenge die $\mathfrak{m}$ enthält. Für einen $R$-Modul $M$ können wir also die drei Aussagen aus dem Nakayama-Lemma als das Verschwinden von $M$ in verschieden kleinen Umgebungen von $\mathfrak{m} \in \mathrm{Spec}(R)$ interpretieren.

**Korollar 2.4.10.** Für eine Abbildung von Moduln $M \to N$ mit $N$ endlich erzeugt sind äquivalent:

1. $M/\mathfrak{m}M \to N/\mathfrak{m}N$ ist surjektiv.
2. $M_\mathfrak{m} \to N_\mathfrak{m}$ ist surjektiv.
3. Es gibt ein $s \notin \mathfrak{m}$ mit $M[s^{-1}] \to N[s^{-1}]$ surjektiv.

*Beweis.* Wir wenden die vorherige Aussage auf $\mathrm{coker}(M \to N)$ an. □

**Korollar 2.4.11.** Wenn $M$ endlich erzeugt und $M/\mathfrak{m}M = 0$ für alle Maximalideale $\mathfrak{m}$, dann ist $M = 0$. Wenn $M \to N$ mit $N$ endlich erzeugt und $M/\mathfrak{m}M \to N/\mathfrak{m}N$ surjektiv für alle Maximalideale $\mathfrak{m}$, dann ist $M \to N$ surjektiv.

## 2.5 Zariski-lokale Eigenschaften

Im vorherigen Abschnitt haben wir einige Eigenschaften von Moduln (und Modulhomomorphismen) kennengelernt, die *lokal* sind, also auf den Lokalisierungen $M_{\mathfrak{m}}$ überprüft werden können.

**Beispiel 2.5.1.** Endlich erzeugt zu sein ist *keine* lokale Eigenschaft. Für den $\mathbb{Z}$-Modul

$$M = \bigoplus_{p \in \mathbb{P}} \mathbb{Z}/p\mathbb{Z}$$

ist $M_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$ für jedes der Maximalideale $(p) \subseteq \mathbb{Z}$. Jede der Lokalisierungen ist also endlich erzeugt, $M$ aber nicht.

Das Problem ist gewissermaßen dass wir hier $M$ an den unendlich vielen Maximalidealen $(p) \in \operatorname{Spec}(\mathbb{Z})$ betrachten. Die folgende Definition ist eine Variante des Begriffs der lokalen Eigenschaften, die besser mit Endlichkeitsbedingungen zusammen passt:

**Definition 2.5.2.** *Wir nennen eine Eigenschaft von Moduln* Zariski-lokal*, wenn gilt:*

1. *Wenn die Eigenschaft für einen $R$-Modul $M$ gilt, dann auch für die $R[s^{-1}]$-Moduln $M[s^{-1}]$, für beliebige $s \in R$.*
2. *Wenn wir für einen $R$-Modul $M$ Elemente $s_1, \dots, s_n \in R$ haben, die das Einsideal erzeugen, und sodass die $R[s_i^{-1}]$-Moduln $M[s_i^{-1}]$ die Eigenschaft erfüllen, dann erfüllt auch $M$ die Eigenschaft.*

**Bemerkung 2.5.3.** Wenn $s_1, \dots, s_n$ das Einsideal erzeugen, dann gibt es für jedes Primideal $\mathfrak{p} \subseteq R$ ein $i$ mit $s_i \notin \mathfrak{p}$. Da $\operatorname{Spec}(R[s_i^{-1}]) \subseteq \operatorname{Spec}(R)$ aus genau den Primidealen besteht, die $i$ nicht enthalten, haben wir $\bigcup_{i=1}^{n} \operatorname{Spec}(R[s_i^{-1}]) = \operatorname{Spec}(R)$.

**Lemma 2.5.4.** *Sei $S \subseteq R$ eine Teilmenge. Die folgenden Aussagen sind äquivalent:*

1. *Wir finden endlich viele $s_1, \dots, s_n \in S$, die das Einsideal erzeugen.*
2. *Für jedes Maximalideal $\mathfrak{m}$ finden wir ein $s_{\mathfrak{m}} \in S$ mit $s_{\mathfrak{m}} \notin \mathfrak{m}$.*

*Beweis.* Wenn $s_1, \dots, s_n$ das Einsideal erzeugen, dann können $s_1, \dots, s_n$ nicht gleichzeitig in einem echten Ideal liegen. Für jedes $\mathfrak{m}$ ist also $s_i \notin \mathfrak{m}$ für ein $i$. Wenn wir umgekehrt $s_{\mathfrak{m}} \notin \mathfrak{m}$ haben, dann kann das Ideal erzeugt von allen $s_{\mathfrak{m}}$ kein echtes Ideal sein (da es in keinem Maximalideal enthalten ist), also ist die 1 endliche Linearkombination der $s_{\mathfrak{m}}$, wir finden darunter also endlich viele $s_1, \dots, s_n$ die ebenfalls das Einsideal erzeugen. □

**Bemerkung 2.5.5.** Also ist damit Teil 2 von 2.5.2 äquivalent zu:

*Wenn wir für jedes $\mathfrak{m} \subseteq R$ ein $s_{\mathfrak{m}} \notin \mathfrak{m}$ finden, sodass die Eigenschaft für den $R[s_{\mathfrak{m}}^{-1}]$-Modul $M[s_{\mathfrak{m}}^{-1}]$ gilt, dann gilt sie für $M$.*

Insbesondere sind lokale Eigenschaften auch Zariski-lokal: Da $M_{\mathfrak{m}}$ eine weitere Lokalisierung von $M[s_{\mathfrak{m}}^{-1}]$ ist, haben wir:

Eigenschaft gilt für alle $M[s_{\mathfrak{m}}^{-1}] \Rightarrow$ Eigenschaft gilt für alle $M_{\mathfrak{m}} \Rightarrow$ Eigenschaft gilt für $M$.

**Lemma 2.5.6.** *Endlich erzeugt zu sein ist eine Zariski-lokale Eigenschaft.*

*Beweis.* Wenn $M$ endlich erzeugter $R$-Modul ist, dann ist $M[S^{-1}]$ endlich erzeugter $R[S^{-1}]$-Modul (mit demselben Erzeugendensystem).

Für den interessanten Teil müssen wir also zeigen: Haben wir $s_1, \ldots, s_n \in R$ die das Einsideal erzeugen, sodass $M[s_i^{-1}]$ endlich erzeugter $R[s_i^{-1}]$-Modul für jedes $i$ ist, dann ist $M$ endlich erzeugter $R$-Modul. Sei $i$ zunächst fix, und $\frac{m_1}{s_i^{k_1}}, \ldots \frac{m_{d_i}}{s_i^{k_{d_i}}}$ ein Erzeugendensystem. Dann ist auch $m_1, \ldots, m_{d_i}$ ein Erzeugendensystem, also die Abbildung $R^{d_i} \to M$ nach Lokalisierung zu $R[s_i^{-1}]^{d_i} \to M[s_i^{-1}]$ surjektiv.

Indem wir diese Abbildungen zu einer Abbildung

$$R^{\sum d_i} \to M$$

kombinieren, erhalten wir eine Abbildung die nach jeder der Lokalisierungen an $s_i$ surjektiv ist. Also ist sie surjektiv (da nach Bemerkung 2.5.5 Surjektivität von Modulabbildungen Zariski-lokal ist.), und $M$ endlich erzeugt. □

Im folgenden benötigen wir eine stärkere Form von endlich-Erzeugtheit:

**Definition 2.5.7.** *Ein $R$-Modul $M$ heißt* endlich präsentiert *wenn es eine surjektive Abbildung $R^n \to M$ gibt, die endlich erzeugten Kern hat.*

Wenn ein Modul $M$ endlich präsentiert ist, dann ist ja $M$ Kokern einer Abbildung $R^m \to R^n$ wo $R^m$ surjektiv auf den Kern von $R^n \to M$ abbildet. Also besitzt $M$ eine Präsentation mit $n$ Erzeugern und $m$ Relationen, was den Namen rechtfertigt.

**Beispiel 2.5.8.** Über einem Noetherschen Ring $R$ ist ein Modul $M$ genau dann endlich erzeugt wenn er endlich präsentiert ist: Sei $M$ endlich erzeugt, $R^n \to M$ surjektiv, und $K \subseteq R^n$ der Kern. Dann ist $R^n$ Noethersch, also $K$ ebenfalls Noethersch, also ist $K$ endlich erzeugt. (Unter allen endlich erzeugten Untermoduln $K' \subseteq K$ gibt es nämlich einen maximalen, wenn $K' \neq K$ dann gibt es $x \in K$ mit $x \notin K'$, und dann ist $K' + Rx$ ebenfalls endlich erzeugt aber größer, Widerspruch.)

**Lemma 2.5.9.** *1. Sei $M$ endlich präsentiert und $R^n \to M$ irgendeine surjektive Abbildung. Dann ist der Kern von $R^n \to M$ endlich erzeugt.*

*2. Endlich präsentiert zu sein ist eine Zariski-lokale Eigenschaft von Moduln.*

*Beweis.* Sei $K$ der Kern von $f : R^n \to M$, wir wollen zeigen dass $K$ endlich erzeugt ist. Da $M$ endlich präsentiert ist gibt es nach Definition eine surjektive Abbildung $f' : R^{n'} \to M$ mit endlich erzeugtem Kern $K'$. Sei $N$ der Kern von

$(f, f') : R^n \oplus R^{n'} \to M$. Wir haben eine Projektionsabbildung $N \to R^n$ mit Kern $N \cap R^{n'} = K'$, und diese ist surjektiv: Für jedes $x \in R^n$ finden wir ein $x'$ in $R^{n'}$ mit $f(x) + f'(x') = 0$ dank Surjektivität von $f'$. Also haben wir eine kurze exakte Folge

$$0 \to K' \to N \to R^n \to 0,$$

die spaltet (weil $R^n$ frei ist). Somit ist $N \cong K' \oplus R^n$ endlich erzeugt. Allerdings erhalten wir komplett analog $N \cong K \oplus R^{n'}$, und somit ist auch $K$ endlich erzeugt.

Für die zweite Aussage sei $M$ ein Modul und $s_1, \ldots, s_n$ eine Familie die das Einsideal erzeugt und so dass $M[s_i^{-1}]$ endlich präsentiert sind. Insbesondere ist $M$ endlich erzeugt (weil endlich erzeugt eine Zariski-lokale Eigenschaft ist), wir finden also surjektives $R^n \to M$. Sei $K$ der Kern. Da die $M[s_i^{-1}]$ endlich präsentiert sind sind die Kerne $K[s_i^{-1}]$ der Abbildungen $R[s_i^{-1}]^n \to M[s_i^{-1}]$ endlich erzeugt, also ist auch $K$ endlich erzeugt und $M$ somit endlich präsentiert. □

Wenn also für irgendeine Wahl von Erzeugern $R^n \to M$ der Kern endlich erzeugt ist (also wir endlich viele Relationen brauchen), dann ist das für *jede* Wahl von endlich vielen Erzeugern so.

Nun sind wir in der Lage, ein erstes überraschendes Resultat zu beweisen: Eine lokale Charakterisierung von endlich präsentierten flachen Moduln. Dazu benötigen wir noch folgendes Lemma über flache Moduln:

**Lemma 2.5.10.** *Sei $0 \to A \to B \to C \to 0$ eine exakte Folge von $R$-Moduln, wo $C$ flach ist, und $I \subseteq R$ ein Ideal. Dann ist auch*

$$0 \to A/IA \to B/IB \to C/IC \to 0$$

*exakt.*

*Beweis.* Die Abbildung $I \otimes_R A \to A$, $i \otimes a \mapsto ia$ hat Bild $IA \subseteq A$, analog für $B$ und $C$. Wir können also $A/IA$ etc. mit dem Kokern der Abbildung $I \otimes_R A \to R \otimes_R A \cong A$ identifizieren. Da Tensorprodukte rechtsexakt sind, haben wir auch

$$I \otimes_R A \to R \otimes_R A \to (R/I) \otimes_R A \to 0,$$

also $A/IA \cong (R/I) \otimes_R A$.

Für $C$ ist die linke Abbildung sogar injektiv, da $I \to R$ injektiv ist, und wir durch Tensorieren mit dem flachen Modul $C$ die Abbildung

$$I \otimes_R C \to R \otimes_R C \cong C$$

erhalten. Nun betrachten wir das folgende Diagramm:

$$\begin{array}{ccccccccc}
 & & I \otimes_R A & \longrightarrow & I \otimes_R B & \longrightarrow & I \otimes_R C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & A/IA & \longrightarrow & B/IB & \longrightarrow & C/IC & \longrightarrow & 0
\end{array}$$

Gegeben ein Element $[a] \in A/IA$ was in $B/IB$ auf 0 geht, sei $b \in B$ das Bild unter $A \mapsto B$ von $a$. Nun gibt es ein $\widetilde{b} \in I \otimes_R B$ mit $\widetilde{b} \mapsto b$, und $\widetilde{b} \mapsto 0$ in $I \otimes_R C$ aufgrund der Injektivität von $I \otimes_R C \to C$. Wir finden also ein $\widetilde{a} \in I \otimes_R A$ mit $\widetilde{a} \mapsto \widetilde{b}$, und aufgrund der Injektivität von $A \to B$ ist $\widetilde{a} \mapsto a$. Folglich ist $[a] = 0$ in $A/IA$. □

**Proposition 2.5.11.** *Sei $M$ ein endlich präsentierter $R$-Modul. Dann sind äquivalent:*

1. *$M$ ist flach.*
2. *$M_{\mathfrak{m}}$ ist freier $R_{\mathfrak{m}}$-Modul für jedes Maximalideal $\mathfrak{m} \subseteq R$.*
3. *Für jedes Maximalideal $\mathfrak{m} \subseteq R$ existiert $s \notin \mathfrak{m}$ sodass $M[s^{-1}]$ freier $R[s^{-1}]$-Modul ist.*

*Beweis.* Wir zeigen zunächst $1 \Rightarrow 3$. Sei also $M$ endlich präsentierter flacher $R$-Modul und $\mathfrak{m} \subseteq R$ ein Maximalideal.

Seien $m_1, \dots, m_n \in M$ Elemente, die in dem endlich erzeugten $R/\mathfrak{m}$-Vektorraum $M/\mathfrak{m}M$ auf eine Basis abgebildet werden. Die Abbildung

$$\bigoplus_{i=1}^{n} R \to M$$

die die Standardbasis links auf die $m_1, \dots, m_n$ schickt, ist surjektiv modulo $\mathfrak{m}$, also nach Nakayama-Lemma existiert $s \notin \mathfrak{m}$ sodass

$$\bigoplus_{i=1}^{n} R[s^{-1}] \to M[s^{-1}]$$

surjektiv ist. Sei $K$ der Kern, also

$$0 \to K \to \bigoplus_{i=1}^{n} R[s^{-1}] \to M[s^{-1}] \to 0$$

exakt. Insbesondere ist $K$ endlich erzeugt über $R[s^{-1}]$ da $M[s^{-1}]$ endlich präsentiert ist. Aufgrund der Flachheit von $M[s^{-1}]$ und des vorherigen Lemmas ist

$$0 \to K/\mathfrak{m}K \to \bigoplus_{i=1}^{n} R/\mathfrak{m} \to M/\mathfrak{m}M \to 0$$

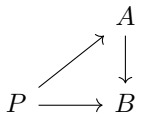
ebenfalls exakt (hier ist $M[s^{-1}]/\mathfrak{m}M[s^{-1}] = (M/\mathfrak{m}M)[s^{-1}] = M/\mathfrak{m}M$, da $s \notin \mathfrak{m}$, also $s$ in $R/\mathfrak{m}$ bereits invertierbar ist). Da die rechte Abbildung aber Isomorphismus ist, folgt $K/\mathfrak{m}K = 0$, und damit existiert aufgrund von Nakayama ein $s' \notin \mathfrak{m}$ mit $K[(s')^{-1}] = 0$. Insgesamt folgt also, dass

$$\bigoplus_{i=1}^{n} R[(ss')^{-1}] \to M[(ss')^{-1}]$$

Isomorphismus ist.

Die Richtungen $3 \Rightarrow 2 \Rightarrow 1$ sind klar. □

**Definition 2.5.12.** *Sei $R$ ein Ring und $P$ ein Modul. $P$ heißt projektiv, wenn für $A \to B$ surjektiv auch $\mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B)$ surjektiv ist, oder äquivalent jeder Homomorphismus $P \to B$ durch einen $P \to A$ faktorisiert.*




**Lemma 2.5.13.** *Ein Modul ist projektiv genau wenn er direkter Summand eines freien Moduls ist. Er ist endlich erzeugt und projektiv genau dann wenn er direkter Summand eines endlich erzeugten freien Moduls ist.*

*Beweis.* Sei $P$ projektiv. Wir können $f : F \to P$ surjektiv wählen, mit $F$ frei. Wenn $P$ endlich erzeugt ist, können wir $F$ zusätzlich endlich erzeugt wählen. Nun existiert wegen surjektivität von $\mathrm{Hom}_R(P, F) \to \mathrm{Hom}_R(P, P)$ ein $i : P \to F$ mit $f \circ i = \mathrm{id}_P$, also ist $i$ injektiv und $F \cong P \oplus \ker(f)$.

Umgekehrt ist für $F \cong P \oplus Q$ ja $\mathrm{Hom}_R(F, U) \cong \mathrm{Hom}_R(P, U) \times \mathrm{Hom}_R(Q, U)$. Also ist für surjektives $A \to B$ $\mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B)$ surjektiv weil $\mathrm{Hom}_R(F, A) \to \mathrm{Hom}_R(F, B)$ surjektiv ist. □

**Lemma 2.5.14.** *Wenn $P$ projektiver $R$-Modul ist, dann ist $P[S^{-1}]$ projektiver $R[S^{-1}]$-Modul.*

*Beweis.* Das folgt aus dem natürlichen Isomorphismus $\mathrm{Hom}_{R[S^{-1}]}(P[S^{-1}], U) \cong \mathrm{Hom}_R(P, U)$. □

Wir wollen nun zeigen dass endlich erzeugt und projektiv zu sein eine lokale Eigenschaft ist, also gewissermaßen für endlich erzeugte Moduln die Umkehrung gilt. Dafür benötigen wir ein Lemma über Lokalisierungen und Hom:

**Bemerkung 2.5.15.** Wenn $P$ projektiv ist, dann ist $P$ endlich erzeugt genau dann wenn $P$ endlich präsentiert ist. Ist nämlich $f : R^n \to P$ eine surjektive Abbildung, so spaltet sie, und $R^n \cong P \oplus \ker(f)$. Also ist $\ker(f)$ automatisch endlich erzeugt.

**Lemma 2.5.16.** *Sei $R$ ein kommutativer Ring, $M$ ein endlich präsentierter $R$-Modul, und $N$ ein beliebiger $R$-Modul. Dann ist*

$$\mathrm{Hom}_R(M, N)[S^{-1}] \cong \mathrm{Hom}_R(M, N[S^{-1}]) \cong \mathrm{Hom}_{R[S^{-1}]}(M[S^{-1}], N[S^{-1}]).$$

*Beweis.* Den zweiten Isomorphismus haben wir ganz allgemein gesehen, als universelle Eigenschaft der Lokalisierung. Für den ersten gibt es eine offensichtliche natürliche Transformation von links nach rechts, sie schickt ein $\frac{f}{s}$ auf die Abbildung $m \mapsto \frac{f(m)}{s}$. Im Fall $M = R$ ist diese klar ein Isomorphismus, weil dann beide Seiten einfach $N[S^{-1}]$ sind. Falls $M = M' \oplus M''$, und sie ein Isomorphismus für $M'$ und $M''$ ist, dann ist sie ebenfalls ein Isomorphismus für $M$, da $\mathrm{Hom}_R(M, N)[S^{-1}] \cong \mathrm{Hom}_R(M', N)[S^{-1}] \oplus \mathrm{Hom}_R(M'', N)[S^{-1}]$ und

analog für die andere Seite. Insgesamt ist sie also für $M = R^n$ ein Isomorphismus. Für allgemeines endlich präsentiertes $M$ schreiben wir das als Kokern $R^m \to R^n \to M \to 0$, somit haben wir exakte Folgen

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(M,N)[S^{-1}] & \longrightarrow & \mathrm{Hom}_R(R^n,N)[S^{-1}] & \longrightarrow & \mathrm{Hom}_R(R^m,N)[S^{-1}] \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_R(M,N[S^{-1}]) & \longrightarrow & \mathrm{Hom}_R(R^n,N[S^{-1}]) & \longrightarrow & \mathrm{Hom}_R(R^m,N[S^{-1}]) \end{array}$$

und die mittlere und rechte vertikale Abbildung sind Isomorphismen, also auch die linke. □

Nun zeigen wir:

**Proposition 2.5.17.** *Sei $R$ ein kommutativer Ring und $M$ ein $R$-Modul. Die folgenden Aussagen sind äquivalent:*

1. *$M$ ist projektiv und endlich erzeugt.*
2. *$M$ ist flach und endlich präsentiert.*
3. *Für jedes Maximalideal $\mathfrak{m}$ existiert $s \in R$ sodass $M[s^{-1}]$ als $R[s^{-1}]$-Modul frei und endlich erzeugt ist.*

*Beweis.* (1) ⇒ (2) ist einfach: Für projektive Moduln ist endlich erzeugt äquivalent zu endlich präsentiert, und projektive Moduln sind immer flach. (2) ⇒ (3) ist Teil der Aussage von Proposition 2.5.11. Es bleibt (3) ⇒ (1) zu zeigen.

Da endlich präsentiert zu sein eine Zariski-lokale Eigenschaft ist, ist $M$ endlich präsentiert. Es folgt also dass $\mathrm{Hom}_R(M,U)[S^{-1}] \cong \mathrm{Hom}_R(M,U[S^{-1}]) \cong \mathrm{Hom}_{R[S^{-1}]}(M[S^{-1}],U[S^{-1}])$ mit Lemma 2.5.16. Wenn nun $A \to B$ surjektiv ist, dann auch $A[s^{-1}] \to B[s^{-1}]$ für jedes $s$, und wenn $M[s^{-1}]$ frei (insbesondere projektiv) ist, dann ist also $\mathrm{Hom}_{R[s^{-1}]}(M[s^{-1}],A[s^{-1}]) \to \mathrm{Hom}_{R[s^{-1}]}(M[s^{-1}],B[s^{-1}])$ surjektiv. Also ist

$$\mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B)$$

lokal surjektiv, also surjektiv, und $M$ ist projektiv. □

**Beispiel 2.5.18.**

1. Der Modul $M = (2, 1+\sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$ ist projektiv: Nach Übungsaufgabe ist nämlich sowohl $M[2^{-1}]$ als auch $M[3^{-1}]$ frei auf einem Erzeuger, und $2, 3$ erzeugen das Einsideal.
2. $R$ als $R \times S$-Modul ist projektiv, da $R \oplus S$ freier $R \times S$-Modul ist. (Wie im Beweis dass produkte halbeinfacher Ringe halbeinfach sind). Alternativ sei $e = (1,0) \in R \times S$ die Idempotente die zum Summanden $R$ gehört, dann ist $R[e^{-1}] = R$ frei als $(R \times S)[e^{-1}] = R$-Modul auf einem Erzeuger, und $R[(1-e)^{-1}] = 0$ frei als $(R \times S)[(1-e)^{-1}] = S$-Modul auf null Erzeugern, und $e, (1-e)$ erzeugen das Einsideal.

**Definition 2.5.19.** *Für einen endlich erzeugten projektiven (bzw. endlich präsentierten flachen) $R$-Modul $P$ sei*

$$\mathrm{rk}(P) : \mathrm{Spec}(R) \to \mathbb{N}$$

*die Abbildung, die jedem Primideal $\mathfrak{p} \subseteq R$*

$$\mathrm{rk}_{\mathfrak{p}}(P) = \dim_{\mathrm{Quot}(R/\mathfrak{p})}(\mathrm{Quot}(R/\mathfrak{p}) \otimes_{R/\mathfrak{p}} P/\mathfrak{p}P)$$

*zuordnet.*

**Lemma 2.5.20.** *Wenn $P$ endlich erzeugt projektiv ist, und $\mathfrak{p} \subseteq \mathfrak{q}$ zwei ineinander enthaltene Primideale sind, dann ist $\mathrm{rk}_{\mathfrak{p}}(P) = \mathrm{rk}_{\mathfrak{q}}(P)$.*

*Beweis.* Sei $\mathfrak{m}$ ein Maximalideal mit $\mathfrak{p} \subseteq \mathfrak{q} \subseteq \mathfrak{m}$. Wir finden ein $s \notin \mathfrak{m}$ sodass $P[s^{-1}]$ freier $R[s^{-1}]$-Modul auf $n$ Erzeugern ist, für irgendein $n$. Also sind auch die weiteren Lokalisierungen $P_{\mathfrak{p}}$ und $P_{\mathfrak{q}}$ frei über $R_{\mathfrak{p}}$ bzw. $R_{\mathfrak{q}}$ auf $n$ Erzeugern. Indem wir die Folge

$$\mathfrak{p}P \to P \to P/\mathfrak{p}P \to 0$$

an $R \setminus \mathfrak{p}$ lokalisieren, sehen wir dass

$$\mathfrak{p}P_{\mathfrak{p}} \to P_{\mathfrak{p}} \to \mathrm{Quot}(R/\mathfrak{p}) \otimes_{R/\mathfrak{p}} (P/\mathfrak{p}) \to 0$$

exakt ist, also die rechte Seite übereinstimmt mit $P_{\mathfrak{p}}/\mathfrak{p}P_{\mathfrak{p}}$. Diese ist also auch frei von Rang $n$ (über $\mathrm{Quot}(R/\mathfrak{p})$), und entsprechend für $\mathfrak{q}$. □

**Korollar 2.5.21.** Sei $R$ nullteilerfrei. Dann ist $\mathrm{rk}_{\mathfrak{p}}(P)$ für alle $\mathfrak{p}$ gleich, und stimmt überein mit $\dim_{\mathrm{Quot}(R)}(\mathrm{Quot}(R) \otimes_R P)$.

*Beweis.* In einem nullteilerfreien Ring ist (0) ein Primideal, das in allen Primidealen enthalten ist. □

Eine besonders wichtige Klasse von endlich erzeugten projektiven Moduln sind diejenigen von Rang 1. Diese besitzen eine andere Charakterisierung, als sogenannte *invertierbare Moduln*:

**Definition 2.5.22.** *Ein $R$-Modul $L$ heißt* invertierbar*, wenn es einen $R$-Modul $L'$ gibt sodass $L \otimes_R L' \cong R$.*

**Theorem 2.5.23.** *Die folgenden Aussagen sind äquivalent:*

1. *$L$ ist invertierbar.*
2. *$L$ ist endlich erzeugt und projektiv von konstantem Rang 1.*
3. *$L$ ist lokal frei von Rang 1, d.h. für jedes Maximalideal $\mathfrak{m}$ gibt es ein $s \notin \mathfrak{m}$ sodass $L[s^{-1}]$ freier $R[s^{-1}]$-Modul von Rang 1 ist.*

*Beweis.* (1) $\Rightarrow$ (2): Sei $L$ invertierbar mit $L \otimes L' \cong R$. Der Funktor $L \otimes_R (-)$ liefert eine Abbildung $\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(L \otimes_R M, L \otimes_R N)$, tensorieren mit $L'$ analog eine Abbildung

$$\mathrm{Hom}_R(L \otimes_R M, L \otimes_R N) \to \mathrm{Hom}_R(L' \otimes_R L \otimes_R M, L' \otimes_R L \otimes_R N) \cong \mathrm{Hom}_R(M,N),$$

und die Komposition ist die Identität, da das Diagramm

$$\begin{array}{ccc} L \otimes_R L' \otimes_R M & \xrightarrow{\cong} & M \\ \downarrow{\scriptstyle \mathrm{id}_L \otimes \mathrm{id}_{L'} \otimes f} & & \downarrow{\scriptstyle f} \\ L \otimes_R L' \otimes_R N & \xrightarrow{\cong} & N \end{array}$$

kommutiert. Also ist $\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(L \otimes_R M, L \otimes_R N)$ injektiv für alle $M, N$. Analog ist auch Tensorieren mit $L'$, also die zweite Abbildung, injektiv, und da es sich um ein linksinverses zur ersten Abbildung handelt, ist diese bijektiv. Insbesondere haben wir eine natürliche Bijektion

$$\mathrm{Hom}_R(L,A) \cong \mathrm{Hom}_R(L' \otimes_R L, L' \otimes_R A) \cong \mathrm{Hom}_R(R, L' \otimes_R A) \cong L' \otimes_R A.$$

Für eine surjektive Abbildung $A \to B$ ist also auch $\mathrm{Hom}_R(L,A) \to \mathrm{Hom}_R(L,B)$ surjektiv, und $L$ ist projektiv. Weiterhin lässt sich das Bild von 1 unter dem Isomorphismus $R \to L \otimes_R L'$ als endliche Summe $\sum_{i=1}^n x_i \otimes y_i$ schreiben, und der inverse Isomorphismus schickt $\sum x_i \otimes y_i \mapsto 1$. Wir behaupten $(x_i) : R^n \to L$ ist surjektiv. Es genügt dies nach Tensorieren mit $L'$ zu zeigen (da wir durch Tensorieren mit $L$ wieder zurück kommen), und

$$(R \otimes_R L')^n \to L \otimes_R L' \cong R$$

schickt den Vektor $(y_1, \ldots, y_n)$ auf 1 nach Konstruktion, ist also surjektiv. Damit ist $L$ auch endlich erzeugt. Schließlich ist $\mathrm{rk}_{\mathfrak{p}}(L \otimes_R L') = \mathrm{rk}_{\mathfrak{p}}(L) \cdot \mathrm{rk}_{\mathfrak{p}}(L')$ und damit $\mathrm{rk}_{\mathfrak{p}}(L) = 1$.

(2) $\Rightarrow$ (3) ist die lokale Charakterisierung von endlich erzeugten projektiven Moduln. Für (3) $\Rightarrow$ (2) sei $L$ lokal frei vom Rang 1. Dann ist $L$ insbesondere endlich präsentiert, und $\mathrm{Hom}_R(L,R)[S^{-1}] = \mathrm{Hom}_{R[S^{-1}]}(L[S^{-1}], R[S^{-1}])$. Die kanonische Abbildung

$$L \otimes_R \mathrm{Hom}_R(L,R) \to R, x \otimes f \mapsto f(x)$$

ist lokal ein Isomorphismus, also auch global, und $L$ ist invertierbar mit $L' = \mathrm{Hom}_R(L,R)$. □

**Beispiel 2.5.24.** $M = (2, 1+\sqrt{-5})$ ist ein invertierbarer $\mathbb{Z}[\sqrt{-5}]$-Modul.

## 2.6 Ganzheit

Wie im Fall von Körpern nennen wir ein Paar von ineinander enthaltenen Ringen $R \subseteq S$ eine Ringerweiterung. Wir wollen nun ein Analogon zu algebraischen Elementen und algebraischen Erweiterungen betrachten.

**Definition 2.6.1.** *1. Eine Ringerweiterung $A \subseteq B$ heißt* endlich*, wenn $B$ als $A$-Modul endlich erzeugt ist.*

*2. Für eine Ringerweiterung $A \subseteq B$ heißt ein Element $b \in B$* ganz über $A$ *wenn der von $A$ und $b$ erzeugte Unterring $A[b] \subseteq B$ endlich über $A$ ist.*

*3. Eine Ringerweiterung $A \subseteq B$ heißt ganz, wenn alle Elemente $b \in B$ ganz über $A$ sind.*

**Lemma 2.6.2.** *Sei $A \subseteq B$ und $b \in B$. Dann sind äquivalent:*

1. *Das Element $b$ ist ganz über $A$.*
2. *Das Element $b$ erfüllt eine Gleichung*
$$b^n + c_{n-1}b^{n-1} + \ldots + c_0 = 0$$
*mit $c_i \in A$.*
3. *Es gibt einen endlich erzeugten $A$-Untermodul $M \subseteq B$ mit $\operatorname{ann}_A(M) = 0$, und $bM \subseteq M$.*

*Beweis.* $1 \Rightarrow 3$ per Definition. Für $3 \Rightarrow 2$ sei $A^n \to M$ eine surjektive $A$-Modulabbildung. Aufgrund der Projektivität von $A^n$ finden wir ein $f : A^n \to A^n$ sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} A^n & \xrightarrow{f} & A^n \\ \downarrow & & \downarrow \\ M & \xrightarrow{\cdot b} & M. \end{array}$$

Dieses $f$ ist nun durch eine $n \times n$-Matrix gegeben. Wir erhalten mit $\det(t \cdot \mathrm{id}_{A^n} - f)$ ein Polynom der Form

$$\chi_f(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_0,$$

wo die $c_i$ Polynome in den Einträgen der $n \times n$-Matrix zu $f$ gegeben sind, also in $A$ liegen. Der Satz von Cayley-Hamilton impliziert nun

$$f^n + c_{n-1}f^{n-1} + \ldots + c_0.$$

(Auch wenn dieser in LA nur für Körper bewiesen wurde, gilt er für beliebige kommutative Ringe: Die Terme des charakteristischen Polynoms sind Polynome in den Einträgen der Matrix, machen also Sinn über abstrakten Ringen, und die Einträge von $\chi_f(f)$ sind ebenfalls Polynome in den Einträgen der Matrix. Da

Cayley-Hamilton z.B. über $\mathbb{C}$ gilt, folgt dass diese Polynome schon identisch 0 sein müssen, also Cayley-Hamilton über jedem kommutativen Ring gilt.)

Also kommutiert das Diagramm

$$\begin{array}{ccc} A^n & \xrightarrow{\chi_f(f)=0} & A^n \\ \downarrow & & \downarrow \\ M & \xrightarrow{\cdot\chi_f(b)} & M, \end{array}$$

und da $\operatorname{ann}_A(M) = 0$ nach Annahme, ist $\chi_f(b) = 0$.

Für $2 \Rightarrow 1$ beobachten wir dass $A[b]$ als $A$-Modul von $1, \ldots, b^{n-1}$ erzeugt wird, da wir $b^n$ und induktiv alle höheren Potenzen als Linearkombination schreiben können. □

Insbesondere sind mit 3. endliche Ringerweiterungen immer ganz. Für $b \in B$ ganz ist also $A \subseteq A[b] \subseteq B$ eine ganze Ringerweiterung.

**Beispiel 2.6.3.**

1. Für eine Körpererweiterung $K \subseteq L$ ist $b \in L$ ganz über $K$ genau wenn $b$ algebraisch über $K$ ist, da wir Polynome dort normieren können.
2. $b = \frac{1+\sqrt{5}}{2} \in \mathbb{Q}[\sqrt{5}]$ ist ganz über $\mathbb{Z}$, da
$$b^2 - b - 1 = 0$$
3. $\frac{1}{2} \in \mathbb{Q}$ ist nicht ganz über $\mathbb{Z}$, da der von $\frac{1}{2}$ erzeugte Unterring $\mathbb{Z}[\frac{1}{2}]$ nicht als $\mathbb{Z}$-Modul von endlich vielen Elementen erzeugt wird (er ist z.B. torsionsfrei, aber nicht frei, da seine mod 2 Reduktion trivial ist.)

**Lemma 2.6.4.** *Sei $A \subseteq B \subseteq C$ eine Folge von Ringerweiterungen. Dann gilt:*

1. *Wenn $C$ ganz über $A$ ist, dann ist $C$ auch ganz über $B$.*
2. *Wenn $C$ ganz über $B$ ist und $B$ ganz über $A$ ist, dann ist $C$ ganz über $A$.*

*Beweis.* Für 1. beobachten wir: Wenn wir für $c \in C$ ein Polynom $c^n + a_{n-1}c^{n-1} + \ldots + a_0 = 0$ mit Koeffizienten $a_i \in A$, dann haben wir insbesondere ein solches Polynom mit Koeffizienten in $B$.

Für 2. sei $c \in C$ mit Polynom $c^n + b_{n-1}c^{n-1} + \ldots + b_0 = 0$ mit $b_i \in B$. Nach Annahme ist jeder der Ringe $A[b_i] \subseteq B$ endlich über $A$, also auch der von ihnen erzeugte Ring $A[c_0, \ldots, c_{n-1}]$ (mit Erzeugendensystem gegeben durch alle Produkte von Erzeugern von $A[c_i]$). Aufgrund der Polynomgleichung für $c$ ist $A[b_0, \ldots, b_{n-1}, c]$ endlich über $A[b_0, \ldots, b_{n-1}]$, und es folgt dass $A[b_0, \ldots, b_{n-1}, c]$ endlich über $A$ ist. Also ist $c$ ganz über $A$. □

**Korollar 2.6.5.** Sei $A \subseteq B$. Dann bilden die Elemente von $B$, die ganz über $A$ sind, einen Unterring.

*Beweis.* Wenn $b, b' \in B$ ganz über $A$ sind, dann ist insbesondere $b'$ ganz über $A[b]$. Also ist mit $A \subseteq A[b] \subseteq A[b, b']$ auch $A \subseteq A[b, b']$ eine ganze Ringerweiterung, und damit sind auch $b' \cdot b$ und $b' \pm b$ ganz über $R$. □

**Definition 2.6.6.** *Sei $A \subseteq B$ eine Ringerweiterung. Der Unterring der Elemente von $B$, die ganz über $A$ sind, heißt* Ganzabschluss von $A$ in $B$, *und wir schreiben $\overline{A}^B$.*

Der Ganzabschluss kann charakterisiert werden als eindeutige maximale ganze Ringerweiterung von $A$ in $B$. $A \subseteq \overline{A}^B$ ist nämlich ganz, enthält alle anderen ganzen Ringerweiterungen von $A$ in $B$, und ist maximal: $\overline{A}^B \subseteq B'$ ganz, so ist auch $A \subseteq B'$ ganz, also auch $B' \subseteq \overline{A}^B$ und es herrscht Gleichheit.

**Beispiel 2.6.7.** Für einen faktoriellen Ring $R$ (also ein Ring mit eindeutiger Primfaktorzerlegung) ist der Ganzabschluss von $R$ in $\mathrm{Quot}(R)$ wieder $R$. Sei nämlich $\frac{a}{b} \notin R$. Dann gibt es einen Primfaktor $p$, der in der Primfaktorzerlegung von $b$ aber nicht von $a$ vorkommt. Wäre $R[\frac{a}{b}]$ endlich erzeugt als Modul, dann gäbe es ein $r \in R$ sodass $r \cdot R[\frac{a}{b}] \subseteq R$ (Wähle $r$ als ein gemeinsames Vielfaches der Nenner eines Erzeugendensystems). Aber $r \cdot \frac{a^k}{b^k}$ hat für großes $k$ den Primfaktor $p$ öfter im Nenner als im Zähler.

**Beispiel 2.6.8.** Der Ganzabschluss von $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$ ist $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Sei nämlich $a + b\sqrt{5}$ ganz.

Dann ist auch $a - b\sqrt{5}$ ganz, da wir einen Automorphismus $\mathbb{Q}[\sqrt{5}]$ haben, der $\sqrt{5}$ und $-\sqrt{5}$ vertauscht. Somit ist auch deren Summe $2a$ ganz. Diese liegt aber in $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$, und damit ist $2a \in \mathbb{Z}$.

Wir wissen bereits dass $\frac{1+\sqrt{5}}{2}$ ganz ist, und somit ist auch

$$a + b\sqrt{5} - 2a \cdot \frac{1+\sqrt{5}}{2} = (b-a)\sqrt{5}$$

ganz, also auch das Quadrat $5(b-a)^2$, das somit in $\mathbb{Z}$ liegt. Aus $5(b-a)^2 \in \mathbb{Z}$ folgt $(b-a) \in \mathbb{Z}$, da jeder Primfaktor die im Nenner von $b-a$ vorkommt auch mindestens einmal im Nenner von $5(b-a)^2$ vorkommt. Mit $2a \in \mathbb{Z}$ und $b-a \in \mathbb{Z}$ ist $a + b\sqrt{5}$ eine Linearkombination von 1 und $\frac{1+\sqrt{5}}{2}$, liegt also in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Allgemein ist der Ganzabschluss von $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{d}]$ für quadratfreies $d$ (kein $p^2$ teilt $d$) gegeben durch $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ wenn $d = 1 \bmod 4$, und $\mathbb{Z}[\sqrt{d}]$ sonst.

Nun analysieren wir das Verhalten von Ganzheit unter Lokalisierung:

**Lemma 2.6.9.** *1. Sei $A \subseteq B$ eine ganze Ringerweiterung, und $S \subseteq A$ eine Teilmenge. Dann ist auch $A[S^{-1}] \to B[S^{-1}]$ eine ganze Ringerweiterung.*

*2. Sei $A \subseteq B$ eine Ringerweiterung, und $S \subseteq A$ eine Teilmenge. Dann stimmen $\overline{A}^B[S^{-1}]$ und $\overline{A[S^{-1}]}^{B[S^{-1}]}$ überein.*

*Beweis.* Für 1. sei $\frac{b}{s} \in B[S^{-1}]$. Dann haben wir eine Gleichung

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

mit Koeffizienten in $A$. Dann ist

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \ldots \frac{a_0}{s^n} = 0$$

eine Gleichung für $\frac{b}{s}$ mit Koeffizienten in $A[S^{-1}]$.

Für 2. beobachten wir zunächst dass nach 1. jedes Element von $\overline{A}^B[S^{-1}]$ ganz über $A[S^{-1}]$ ist, also in $\overline{A[S^{-1}]}^{B[S^{-1}]}$ liegt. Zu zeigen ist die Umkehrung, also dass jedes Element von $B[S^{-1}]$ was ganz über $A[S^{-1}]$ ist, von der Form $\frac{b}{s}$ ist wo $b \in B$ ganz über $A$ ist.

Sei also $\beta \in B[S^{-1}]$ mit Polynomgleichung

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \ldots + \alpha_0 = 0$$

mit $\alpha_i \in A[S^{-1}]$. Für ein $s \in \overline{S}$ erhalten wir durch Multiplikation mit $s^n$:

$$(s\beta)^n + s\alpha_{n-1}(s\beta)^{n-1} + \ldots + (s^n\alpha_0) = 0.$$

Indem wir $s$ als Produkt der Nenner von $\beta$ und aller $\alpha_i$ wählen, finden wir also ein $b \in B$ und $a_i \in A$ sodass

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

in $B[S^{-1}]$. Also existiert $t \in \overline{S}$ mit

$$t(b^n + a_{n-1}b^{n-1} + \ldots + a_0) = 0$$

in $B$, insbesondere

$$(tb)^n + ta_{n-1}(tb)^{n-1} + \ldots t^n a_0 = 0.$$

Somit ist $tb$ ganz über $A$, und $\beta = \frac{tb}{ts}$. □

**Korollar 2.6.10.** 1. Für eine Ringerweiterung $A \subseteq B$ ist die Eigenschaft, dass $A \subseteq B$ ganz ist, lokal (in $A$, also ist $A \subseteq B$ ganz genau dann wenn $A_\mathfrak{m} \subseteq B_\mathfrak{m}$ ganz für alle Maximalideale $\mathfrak{m} \subseteq A$.)

2. Für eine Ringerweiterung $A \subseteq B$ ist die Eigenschaft, dass $A$ in $B$ ganzabgeschlossen ist, lokal (ebenfalls in $A$).

*Beweis.* Wir haben $A \subseteq \overline{A}^B \subseteq B$, und für jedes Maximalideal ist $A_\mathfrak{m} \subseteq (\overline{A}^B)_\mathfrak{m} \subseteq B_\mathfrak{m}$ ebenfalls der Ganzabschluss von $A_\mathfrak{m}$ in $B_\mathfrak{m}$. Ganzheit von $A \subseteq B$ korrespondiert dazu dass die zweite Inklusion ein Isomorphismus ist, Ganzabgeschlossenheit von $A$ in $B$ dazu dass die erste Inklusion ein Isomorphismus ist. Beides können wir lokal testen. □

**Definition 2.6.11.** *Ein nullteilerfreier Ring $R$ heißt* normal*, wenn $R$ in* $\mathrm{Quot}(R)$ *ganzabgeschlossen ist.*

**Beispiel 2.6.12.** 1. Nach Beispiel 2.6.7 ist jeder faktorielle Ring normal.

2. Für einen nullteilerfreien Ring $R$ ist $\overline{R}^{\mathrm{Quot}(R)}$ normal, da $\overline{R}^{\mathrm{Quot}(R)}$ den gleichen Quotientenkörper wie $R$ hat.

3. $\mathbb{Z}[\sqrt{5}]$ ist nicht normal.

## 2.7 Dimension

Für einen Körper $K$ besteht $\mathrm{Spec}(K)$ aus einem einzelnen Element, ist also in gewisser Weise 0-dimensional. Wir wollen nun einen allgemeinen Begriff von *Dimension* von Ringen entwickeln, sodass Körper 0-dimensional sind. Hierbei sollte $\dim K[x_1, \ldots, x_n] = n$ sein. Der Polynomring hat die Eigenschaft, dass wenn wir $(x_n)$ herausteilen, einen Polynomring in $x_1, \ldots, x_{n-1}$ erhalten. Wir haben also eine Kette von Quotienten

$$K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_{n-1}] \to \ldots \to K[x_1] \to K$$

der Länge $n+1$. Die Kerne bilden eine aufsteigende Kette von Primidealen

$$(0) \subseteq (x_n) \subseteq \ldots \subseteq (x_2, \ldots, x_n) \subseteq (x_1, \ldots, x_n).$$

**Definition 2.7.1.** *Für einen kommutativen Ring $R$ definieren wir*

1. *Für jedes Primideal $\mathfrak{p} \subseteq R$ die* Höhe $\mathrm{ht}(\mathfrak{p})$ *als Supremum über alle $n$ sodass eine Primidealkette*
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$
*existiert.*

2. $\dim(R)$ *als* $\sup_{\mathfrak{p} \subseteq R} \mathrm{ht}(\mathfrak{p})$.

Insgesamt ist $\dim(R)$ also die Länge einer längsten Primidealkette in $R$, oder $\infty$ wenn es beliebig lange Primidealketten gibt.

**Beispiel 2.7.2.** 1. Die Überlegung oben zeigt $\dim(K[x_1, \ldots, x_n]) \geq n$. (Gleichheit gilt, ist aber schwierig zu zeigen!)

2. Für einen Körper $K$ ist $\dim(K) = 0$, da $(0)$ das einzige Primideal ist. Umgekehrt ist in einem nullteilerfreien Ring mit $\dim(R) = 0$ ja bereits $(0)$ maximal, also $R$ ein Körper.

3. Für einen Hauptidealring $R$ (z.B. $K[x]$ oder $\mathbb{Z}$) ist $\dim(R) = 1$: Primideale sind entweder $(0)$ oder $(p)$ für ein Primelement $p$, wir haben nie $(p) \subseteq (q)$ für verschiedene Primelemente, also sind maximale Primidealketten von der Form $(0) \subsetneq (p)$.

Wie interagiert Dimension mit Lokalisierungen?

**Proposition 2.7.3.** *1. Für einen Ring $R$ und eine Teilmenge $S \subseteq R$ ist* $\dim R[S^{-1}] \leq \dim R$.

*2. Für einen Ring $R$ ist* $\dim R = \sup_{\mathfrak{m}} \mathrm{ht}(\mathfrak{m}) = \sup_{\mathfrak{m}} \dim R_{\mathfrak{m}}$.

*Beweis.* Da die Primideale von $R[S^{-1}]$ genau zu den Primidealen von $R$ korrespondieren, die disjunkt zu $S$ sind, liefert jede Primidealkette in $R[S^{-1}]$ eine in $R$ derselben Länge. Also ist $\dim R[S^{-1}] \leq \dim R$.

Insbesondere gilt $\dim R \geq \sup_{\mathfrak{m}} \dim R_{\mathfrak{m}}$. Sei umgekehrt $n \leq \dim R$ beliebig und $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_n$ eine Primidealkette in $R$. Dann gibt es ein Maximalideal $\mathfrak{m}$ was $\mathfrak{p}_n$ enthält, somit ist $n \leq \sup_{\mathfrak{m}} \dim R_{\mathfrak{m}}$. Da $n$ hier beliebig war, ist $\dim R \leq \sup_{\mathfrak{m}} \dim R_{\mathfrak{m}}$. □

**Bemerkung 2.7.4.** Dieses Resultat lässt sich auch formulieren als: Für jedes $n \in \mathbb{N}$ ist die Eigenschaft "$R$ hat $\dim R \leq n$" eine lokale Eigenschaft. Die erste Eigenschaft drückt aus dass diese Eigenschaft stabil unter Lokalisierungen ist, die zweite drückt aus dass sie lokal getestet werden kann, also $\dim R \leq n$ genau wenn $\dim R_{\mathfrak{m}} \leq n$ für alle $\mathfrak{m}$.

Wir fragen uns nun zunächst allgemeiner: Wie sehen Ringe mit $\dim(R) = 0$ aus? Zumindest für $R$ Noethersch gibt es hier eine schöne Antwort. Da wir im folgenden oft mit Noetherschen Ringen arbeiten werden, beginnen wir mit einigen grundlegenden Beobachtungen:

**Lemma 2.7.5.** *Sei $R$ Noethersch. Dann ist $\bigcap_{\mathfrak{p} \subseteq R} \mathfrak{p}$ bereits Schnitt endlich vieler Primideale.*

*Beweis.* Angenommen, $R$ ist ein Noetherscher Ring für den die Behauptung nicht gilt. Unter allen Idealen $\mathfrak{a}$, für die $R/\mathfrak{a}$ die Behauptung ebenfalls verletzt, können wir ein maximales wählen. Wenn $R/\mathfrak{a}$ nullteilerfrei ist, erfüllt er die Behauptung (da dann (0) Primideal ist). Seien also $xy = 0$ Nullteiler. Sowohl $R/(\mathfrak{a} + (x))$ als auch $R/(\mathfrak{a} + (y))$ erfüllen die Behauptung, also sind

$$\bigcap_{x \in \mathfrak{p} \subseteq R/\mathfrak{a}} \mathfrak{p}, \quad \bigcap_{y \in \mathfrak{p} \subseteq R/\mathfrak{a}} \mathfrak{p}$$

endliche Schnitte von Primidealen. Da jedes Primideal $x$ oder $y$ enthält, ist aber nun auch $\bigcap_{\mathfrak{p} \subseteq R/\mathfrak{a}} \mathfrak{p}$ endlicher Schnitt von Primidealen. □

**Bemerkung 2.7.6.** $\bigcap_{\mathfrak{p} \subseteq R} \mathfrak{p}$ besteht aus allen nilpotenten Elementen von $R$: Wenn $x$ in allen Primidealen liegt, ist $\mathrm{Spec}(R[x^{-1}])$ leer, also muss $R[x^{-1}]$ der Nullring sein. Das ist aber gleichbedeutend damit dass $x^n = 0$ für ein $n$.

**Theorem 2.7.7.** *Ein kommutativer Ring $R$ ist genau dann Artinsch wenn er Noethersch ist und* $\dim(R) = 0$.

*Beweis.* Die Bedingung $\dim(R) = 0$ bedeutet, dass jedes Primideal bereits maximal ist. Sei zunächst $R$ Artinsch. Dann ist $R$ auch Noethersch nach Korollar 1.4.25. Sei nun $\mathfrak{p} \subseteq R$ ein Primideal. Dann ist $R/\mathfrak{p}$ Artinsch und nullteilerfrei,

also ist aufgrund der Nilpotenz von $\mathrm{Jac}(R/\mathfrak{p})$ schon $\mathrm{Jac}(R/\mathfrak{p}) = 0$, und $R/\mathfrak{p}$ ist halbeinfach. Da $R/\mathfrak{p}$ nullteilerfrei und kommutativ ist, ist $R/\mathfrak{p}$ somit ein Körper, also war $\mathfrak{p}$ in $R$ maximal.

Für die Umkehrung sei $R$ Noethersch und nulldimensional, also alle Primideale maximal. Nach dem vorherigen Lemma ist $\mathrm{Jac}(R)$ Schnitt endlich vieler Maximalideale, also $R/\mathrm{Jac}(R) \to \prod R/\mathfrak{m}$ injektiv, für ein endliches Produkt. Insbesondere ist $R/\mathrm{Jac}(R)$ ein $R$-Modul endlicher Länge. Nun ist $\mathrm{Jac}(R)$ endlich erzeugt. Jede der Potenzen $\mathrm{Jac}(R)^k$ ist also auch endlich erzeugt, insbesondere sind die $\mathrm{Jac}(R)^k/\mathrm{Jac}(R)^{k+1}$ als endlich erzeugte $R/\mathrm{Jac}(R)$-Moduln ebenfalls von endlicher Länge. Da $\mathrm{Jac}(R)$ mit dem Schnitt aller Primideale übereinstimmt ist jeder der endlich vielen Erzeuger außerdem nilpotent, somit finden wir $n$ mit $\mathrm{Jac}(R)^n = 0$. Also ist $R$ eine endliche Erweiterung von Moduln endlicher Länge, hat also selbst endliche Länge, und $R$ ist Artinsch. □

Unser Ziel für den Rest der Vorlesung wird es sein, den 1-dimensionalen Fall zu verstehen. Dafür beweisen wir zunächst einen wichtigen Zusammenhang zwischen Dimension und ganzen Ringerweiterungen.

**Lemma 2.7.8.** *Sei $R \subseteq S$ eine ganze Ringerweiterung, und $I \subseteq S$ ein Ideal. Dann ist auch*

$$R/(I \cap R) \subseteq S/I$$

*eine ganze Ringerweiterung.*

*Beweis.* Gegeben ein Element von $S/I$ mit Repräsentant $s \in S$. Dann ist $R[s] \subseteq S$ endlich erzeugter $R$-Modul, also sein Bild $R/(I \cap R)[s] \subseteq S/I$ endlich erzeugt als $R/(I \cap R)$-Modul. □

**Theorem 2.7.9** ("Lying over")**.** *Sei $R \subseteq S$ eine ganze Ringerweiterung, und $\mathfrak{p} \subseteq R$ ein Primideal. Dann existiert ein Primideal $\mathfrak{q} \subseteq S$ mit $\mathfrak{p} = \mathfrak{q} \cap R$.*
*(also $\mathfrak{q} \mapsto \mathfrak{p}$ unter $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$, $\mathfrak{q}$ "liegt über" $\mathfrak{p}$)*

*Beweis.* Wir betrachten zunächst den Fall, wo $R$ lokaler Ring und $\mathfrak{p} = \mathfrak{m}$ das Maximalideal ist. Sei $\mathfrak{m}' \subseteq S$ ein *beliebiges* Maximalideal von $S$. Dann ist $R/(\mathfrak{m}' \cap R) \subseteq S/\mathfrak{m}'$ eine ganze Ringerweiterung und $S/\mathfrak{m}'$ ein Körper. Für $r \in R/(\mathfrak{m}' \cap R)$ mit $r \neq 0$ gibt es in $S/\mathfrak{m}'$ also ein Inverses $r^{-1}$. Nach Übungsaufgabe ist $r$ auch in $R/(\mathfrak{m}' \cap R)$ invertierbar, also ist $R/(\mathfrak{m}' \cap R)$ ebenfalls ein Körper, und $\mathfrak{m}' \cap R$ maximal, also $\mathfrak{m}' \cap R = \mathfrak{m}$ wie erwünscht.

Für beliebiges $R \subseteq S$ können wir nun an der Teilmenge $R \setminus \mathfrak{p} \subseteq R$ lokalisieren und erhalten eine ganze Ringerweiterung $R_\mathfrak{p} \subseteq S_\mathfrak{p}$. Wir finden ein $\mathfrak{q} \subseteq S_\mathfrak{p}$ dessen Urbild in $R_\mathfrak{p}$ das Maximalideal $R_\mathfrak{p}\mathfrak{p}$ ist, also dessen Urbild in $R$ $\mathfrak{p}$ ist. Das Urbild von $\mathfrak{q}$ in $S$ ist also das gesuchte Ideal. □

**Korollar 2.7.10** ("Going up")**.** Für eine ganze Ringerweiterung $R \subseteq S$ finden wir für jede Primidealkette $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ in $R$ eine Primidealkette $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n$ in $S$, mit $\mathfrak{p}_i = R \cap \mathfrak{q}_i$. Insbesondere ist $\dim(S) \geq \dim(R)$.

*Beweis.* Sei $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ eine Primidealkette in $\dim(R)$. "Lying over" liefert uns ein Primideal $\mathfrak{q}_0 \subseteq S$ mit $\mathfrak{p}_0 = S \cap \mathfrak{q}_0$. Dann ist auch $R/\mathfrak{p}_0 \subseteq S/\mathfrak{q}_0$ eine ganze Ringerweiterung, und indem wir "lying over" auf das Ideal $\mathfrak{p}_1/\mathfrak{p}_0 \subseteq R/\mathfrak{p}_0$ anwenden finden wir ein Primideal $\mathfrak{q}_1 \subseteq S$ mit $\mathfrak{p}_1 = R \cap \mathfrak{q}_1$. Induktiv erhalten wir so eine Primidealkette

$$\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n$$

in $S$, mit $\mathfrak{p}_i = R \cap \mathfrak{q}_i$. Da wir für jede Primidealkette von $R$ eine Primidealkette der gleichen Länge in $S$ finden, ist also $\dim(S) \geq \dim(R)$. □

Wir wollen nun Gleichheit zeigen. Dazu wollen wir sehen, dass Primidealketten in $S$ Primidealketten bleiben, wenn wir sie mit $R$ schneiden, also die Inklusionen echte Inklusionen bleiben.

**Theorem 2.7.11** ("Incomparability")**.** *Sei $R \subseteq S$ eine ganze Ringerweiterung. Wenn $\mathfrak{q} \subseteq \mathfrak{q}'$ Primideale in $S$ sind, mit $R \cap \mathfrak{q} = R \cap \mathfrak{q}'$, dann ist bereits $\mathfrak{q} = \mathfrak{q}'$.*

*Beweis.* $R/(\mathfrak{q} \cap R) \subseteq S/\mathfrak{q}$ ist ebenfalls eine ganze Ringerweiterung, aber hier ist das erste Ideal 0. Es genügt also folgenden Spezialfall zu zeigen: Sei $R \subseteq S$ eine ganze Ringerweiterung von nullteilerfreien Ringen, $\mathfrak{q} \subseteq S$ ein Primideal, und $0 = \mathfrak{q} \cap R$. Dann ist bereits $\mathfrak{q} = 0$.

Wenn $0 = \mathfrak{q} \cap R$, dann können wir weiter an allen Elementen aus $R \setminus \{0\}$ lokalisieren, dürfen also annehmen dass $R \subseteq S$ eine ganze Erweiterung von nullteilerfreien Ringen ist, wo $R$ ein Körper ist. Aber dann ist $S$ auch ein Körper: Für $s \in S$ ist $R[s] \subseteq S$ ein endlichdimensionaler $R$-Vektorraum auf dem Multiplikation mit $s$ injektiv, also auch surjektiv wirkt. Somit ist $\mathfrak{q} = (0)$ wie gewünscht. □

**Theorem 2.7.12.** *Sei $R \subseteq S$ eine ganze Ringerweiterung. Dann ist* $\dim(R) = \dim(S)$.

*Beweis.* Die Abschätzung $\dim(R) \leq \dim(S)$ ist Korollar 2.7.10. Für die andere sei $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n$ eine Primidealkette in $S$. Dann bilden die $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ eine Primidealkette in $R$, da $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$ mit Theorem 2.7.11. □

Dieser Satz liefert nun insbesondere viele weitere Beispiele von 1-dimensionalen Ringen, über die Hauptidealringe hinaus:

**Beispiel 2.7.13.** Sei $K$ eine endliche Körpererweiterung von $\mathbb{Q}$, und $R \subseteq K$ ein Unterring, der endlich erzeugt als $\mathbb{Z}$-Modul ist. Dann ist $R$ ganz über $\mathbb{Z}$, also $\dim(R) = \dim(\mathbb{Z}) = 1$. Zum Beispiel lässt sich das anwenden auf $R = \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{Q}$.

Wie in der Einleitung beobachtet, ist $\dim R[x] \geq \dim R + 1$. Was können wir noch über die Dimension von Polynomringen sagen?

**Lemma 2.7.14.** *Sei $R$ kommutativer Ring und $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \mathfrak{p}_2$ mit $\mathfrak{p}_0 \cap R = \mathfrak{p}_1 \cap R = \mathfrak{p}_2 \cap R$. Dann ist $\mathfrak{p}_0 = \mathfrak{p}_1$ oder $\mathfrak{p}_1 = \mathfrak{p}_2$.*

*Beweis.* Indem wir $R$ durch $R/\mathfrak{p}_0 \cap R$ ersetzen, dürfen wir annehmen dass $\mathfrak{p}_i \cap R = (0)$. Nun dürfen wir an $R \setminus \{0\}$ lokalisieren, und annehmen dass $R$ Körper ist. Dann ist $R[x]$ Hauptidealring, also $\dim R[x] = 1$, und somit können die Inklusionen $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \mathfrak{p}_2$ nicht alle echt sein. □

**Korollar 2.7.15.** $\dim R[x] \leq 2 \dim R + 1$.

*Beweis.* Sei $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_n$ eine Primidealkette in $R[x]$. Dann ist in $\mathfrak{p}_0 \cap R \subseteq \ldots \subseteq \mathfrak{p}_n \cap R$ von zwei aufeinanderfolgenden Inklusionen immer mindestens eine echt. Von den $n-1$ Inklusionen bleiben bei geradem $n-1$ also mindestens $\frac{n-1}{2}$ echt, bei ungeradem $n-1$ mindestens $\frac{n-2}{2}$. Also erhalten wir in $R$ eine Primidealkette der Länge mindestens $\left\lfloor \frac{n-1}{2} \right\rfloor + 1$, und es folgt

$$\dim R \geq \left\lfloor \frac{n-1}{2} \right\rfloor,$$

also $2 \dim R \geq n - 1 = \dim R[x] - 1$ wie gewünscht. □

**Korollar 2.7.16.** Sei $R \subseteq S$ eine Erweiterung von Ringen, wo $S$ endlich erzeugt als Ring über $R$ ist. Wenn $\dim(R)$ endlich ist, dann ist auch $\dim(S)$ endlich.

*Beweis.* Wenn $s_1, \ldots, s_n \in S$ Erzeuger von $S$ über $R$ sind, dann ist die Abbildung $R[x_1, \ldots, x_n] \to S$, die $x_i \mapsto s_i$ schickt, surjektiv. Nun ist

$$\dim(S) \leq \dim(R[x_1, \ldots, x_n]),$$

da jede Primidealkette in $S$ über Urbild nehmen eine Primidealkette derselben Länge in $R[x_1, \ldots, x_n]$ liefert. Indem wir das vorherige Korollar induktiv anwenden ist $\dim R[x_1, \ldots, x_n]$ endlich. □

**Bemerkung 2.7.17.** Wenn $R$ Noethersch ist, dann ist $\dim R[x] = \dim R + 1$. Der Beweis erfordert andere Charakterisierungen der Dimension, die wir hier nicht betrachten werden, speziell kann man zeigen

$$\begin{aligned}
&\mathrm{ht}(\mathfrak{m}) = 0 \text{ genau wenn } \mathfrak{m} \text{ nilpotent, sonst} \\
&\mathrm{ht}(\mathfrak{m}) = 1 + \lim_{n \to \infty} \frac{\log(\dim_{R/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1}))}{\log(n)} \\
&\qquad = 1 + \text{Grad eines Polynoms in } n, \text{ das } \dim_{R/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \text{ beschreibt}
\end{aligned}$$

für ein Maximalideal $\mathfrak{m}$ in einem Noetherschen Ring.

**Lemma 2.7.18** (Hilbertscher Basissatz)**.** *Wenn $R$ Noethersch ist, ist auch $R[x]$ Noethersch. Insbesondere ist $\mathbb{Z}[x_1, \ldots, x_n]$ Noethersch für jedes $n$, und jeder endlich erzeugte Ring ist ebenfalls Noethersch.*

*Beweis.* Wir schreiben $R[x]_{\leq n}$ für den $R$-Untermodul von $R[x]$ bestehend aus Polynomen von Grad $n$. Für ein Ideal $I \subseteq R[x]$ sei nun $I_n \subseteq R$ das Bild von $I \cap R[x]_{\leq n}$ unter dem Homomorphismus

$$R[x]_{\leq n} \to R$$

der ein Polynom von Grad $n$ auf den Koeffizienten von $x^n$ schickt. Wir haben $I_n \subseteq I_{n+1}$ (da der $x^n$-Koeffizient von $f \in I \cap R[x]_{\leq n}$ auch der $x^{n+1}$-Koeffizient von $xf \in I \cap R[x]_{\leq n+1}$ ist), und ab irgendeinem $n$ wird die Folge der $I_n$ stabil.

Seien für solches $n$ $f_1, \ldots, f_k$ Elemente von $I \cap R[x]_{\leq n}$, deren $x^n$-Koeffizienten $I_n$ erzeugen. Dann erzeugen auch die Leitkoeffizienten von $x^m f_i$ das Ideal $I_{n+m}$. Wir können also durch "Polynomdivision" jedes Element von $I$ als Summe von Vielfachen der $f_i$, und einem Restterm in $I \cap R[x]_{\leq n-1}$ schreiben. Letzterer $R$-Modul ist Noethersch (als Untermodul von $R[x]_{\leq n}$), also endlich erzeugt, und Erzeuger als $R$-Modul zusammen mit den $f_i$ bilden ein endliches Erzeugendensystem von $I$. □

Wenn $R$ Noethersch ist, sind also induktiv auch $R[x_1, \ldots, x_n]$ Noethersch, und mit Bemerkung 2.7.17 gilt $\dim(R[x_1, \ldots, x_n]) = \dim(R) + n$. Zum Beispiel gilt tatsächlich $\dim(K[x_1, \ldots, x_n]) = n$ für einen Körper $K$.

## 2.8 Diskrete Bewertungsringe und Dedekindringe

Wie wollen nun Ringe mit $\dim(R) = 1$ genauer betrachten. Da sich die Dimension eines nullteilerfreien Rings unter Ganzabschluss nicht ändert, ist es naheliegend zunächst normale, also in ihrem Quotientenkörper ganzabgeschlossene Ringe von Dimension 1 zu studieren.

**Definition 2.8.1.** *Ein* Dedekindring *ist ein nullteilerfreier, normaler, Noetherscher Ring $R$ von Dimension $\leq 1$.*

**Beispiel 2.8.2.**

1. Körper sind Dedekindringe, nämlich genau die mit $\dim R = 1$.
2. Der Ganzabschluss von $\mathbb{Z}$ in einer endlichen Körpererweiterung $K$ von $\mathbb{Q}$ ist ein Dedekindring.
3. Hauptidealringe sind Dedekindringe. Da Hauptidealringe faktoriell sind sind sie normal. Außerdem sind sie Noethersch (jedes Ideal ist endlich erzeugt) und haben Dimension 1.

**Lemma 2.8.3.** *1. Wenn $R$ Dedekindring ist, dann auch $R[S^{-1}]$ für eine Teilmenge $S \subseteq R$.*

*2. Wenn $R$ Noethersch und nullteilerfrei ist und $R_{\mathfrak{m}}$ Dedekindring ist für jedes Maximalideal $\mathfrak{m} \subseteq R$, dann ist $R$ auch Dedekindring.*

*Beweis.* Wenn $R$ Noethersch ist dann ist auch $R[S^{-1}]$ Noethersch: Wenn nämlich $f : R \to R[S^{-1}]$ die kanonische Abbildung ist, und

$$\ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

eine Kette von Idealen in $R[S^{-1}]$, dann ist

$$f^{-1}(I_n) = \{r \in R \mid \exists s \in \overline{S} : \frac{r}{s} \in I_n\},$$

und somit $I_n = f^{-1}(I_n)[S^{-1}]$. Da die Kette der $f^{-1}(I_n)$ stabil wird, gilt das auch für die Kette der $I_n$.

Der Rest folgt direkt aus den lokalen Charakterisierungen von Ganzabschluss und Dimension. □

Wir betrachten jetzt also *lokale* Dedekindringe.

**Lemma 2.8.4.** *Sei $R$ ein lokaler Dedekindring der kein Körper ist, mit Maximalideal $\mathfrak{m}$. Dann gilt:*

1. *$\mathfrak{m}$ ist Hauptideal, also $\mathfrak{m} = (a)$ für ein $a \in R$.*
2. *Jedes Ideal ist von der Form $(0)$ oder $\mathfrak{m}^n = (a^n)$ für ein $n$.*

*Insbesondere ist $R$ Hauptidealring.*

*Beweis.* Da $R$ Noethersch ist ist $\mathfrak{m}$ endlich erzeugter $R$-Modul. Wenn also $\mathfrak{m}/\mathfrak{m}^2 = 0$ wäre, dann wäre aufgrund von Nakayama auch $\mathfrak{m} = 0$ und $R$ Körper. Wir können also ein $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ wählen. $R/(a)$ ist nulldimensional und Noethersch, also auch Artinsch. Es gibt also ein $n$ mit $\mathfrak{m}^n \subseteq (a)$. Wir wählen ein minimales solches $n$. Sei also $b \in \mathfrak{m}^{n-1} \setminus (a)$, dann ist $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$. Also gilt

$$\frac{b}{a} \cdot \mathfrak{m} \subseteq R$$

in $\mathrm{Quot}(R)$, und nun gibt es zwei Möglichkeiten:

Wenn $\frac{b}{a} \cdot \mathfrak{m} = R$, dann ist $\mathfrak{m} = \frac{a}{b} \cdot R$. Insbesondere ist $\frac{a}{b} \in R$ und $\mathfrak{m}$ Hauptideal.

Ansonsten ist $\frac{b}{a} \cdot \mathfrak{m} \subseteq \mathfrak{m}$, aber dann ist $\frac{b}{a}$ ganz, da $\mathfrak{m}$ endlich erzeugter Untermodul mit $\mathrm{ann}_R(\mathfrak{m}) = 0$ ist. Da $R$ ganzabgeschlossen in $\mathrm{Quot}(R)$ ist bedeutet das $\frac{b}{a} \in R$ im Widerspruch zur Wahl von $b$.

Insgesamt haben wir gesehen dass $\mathfrak{m}$ von einem Element erzeugt wird, also ist $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$ und nach Nakayama ist jedes Element von $\mathfrak{m} \setminus \mathfrak{m}^2$ ein Erzeuger von $\mathfrak{m}$, insbesondere unser $a$. Wir sehen auch, dass $\mathfrak{m}^n$ von $a^n$ erzeugt wird, und $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ eindimensional ist (ansonsten wäre $a^n = ua^{n+1}$, und damit $a^n(1 - ua) = 0$ im Widerspruch zu Nullteilerfreiheit).

Sei nun $I \subseteq R$ ein Ideal mit $I \neq 0$. Dann ist wieder $R/I$ Artinsch. Die Ideale $\mathfrak{m}^n$ können nicht alle $I$ enthalten, da wir sonst eine unendliche absteigende Kette in $R/I$ hätten. Es gibt also ein maximales $n$ mit $I \subseteq \mathfrak{m}^n$. Insbesondere ist die Komposition $I \to \mathfrak{m}^n \to \mathfrak{m}^n/\mathfrak{m}^{n+1}$ nicht 0, also surjektiv (da $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ als eindimensionaler $R/\mathfrak{m}$-Vektorraum einfacher $R$-Modul ist). Nach Nakayama ist dann $I \to \mathfrak{m}^n$ surjektiv, also sind die Ideale gleich. □

**Definition 2.8.5.** *Ein lokaler Hauptidealring, der kein Körper ist, heißt* diskreter Bewertungsring.

**Definition 2.8.6.** *Sei $R$ ein diskreter Bewertungsring mit Maximalideal $\mathfrak{m} = (\pi)$. Wir definieren eine Abbildung*

$$v : \mathrm{Quot}(R) \to \mathbb{Z} \cup \{\infty\}$$

*(die* Bewertung*) durch*

$$v(x) = \begin{cases} \infty \text{ für } x = 0 \\ \max\{n \in \mathbb{Z} \mid \pi^{-n} x \in R\} \text{ für } x \neq 0 \end{cases}$$

**Lemma 2.8.7.** *Die Bewertung hat die folgenden Eigenschaften:*

1. $v(x) = \infty$ *genau wenn* $x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \geq \min(v(x), v(y))$ *mit Gleichheit dann wenn* $v(x) \neq v(y)$
4. $R = \{x \in \mathrm{Quot}(R) \mid v(x) \geq 0\}$
5. $\mathfrak{m} = \{x \in \mathrm{Quot}(R) \mid v(x) > 0\}$
6. $R^\times = \{x \in \mathrm{Quot}(R) \mid v(x) = 0\}$

*Beweis.* Aussage 1 ist klar.

Nun zeigen wir zunächst Aussagen 4,5 und 6: Ein Element mit $v(x) \geq 0$ ist per Definition eines wo $\pi^0 \cdot x \in R$, also $x \in R$. Es erfüllt $v(x) > 0$ genau wenn $\pi^{-1}x \in R$, also $x \in (\pi) = \mathfrak{m}$. Es erfüllt $v(x) = 0$ demnach genau wenn $x \in R \backslash \mathfrak{m} = R^\times$, da in lokalen Ringen alle Elemente außerhalb des Maximalideals invertierbar sind. Wir sehen auch dass allgemeiner $v(x)$ die eindeutige Zahl mit $\pi^{-v(x)}x \in R \setminus (\pi) = R^\times$ ist.

Für 2 seien nun $v(x) = n$ und $v(y) = m$. Also ist $\pi^{-n}x \in R^\times$ und $\pi^{-m}y \in R^\times$, also $\pi^{-n-m}xy \in R^\times$, und somit $v(xy) = n + m$.

Für 3 können wir OBdA annehmen dass $v(x) \leq v(y)$, und indem wir $x, y$ durch $\pi^{-n}x$, $\pi^{-n}y$ ersetzen, wo $n = v(x)$, dürfen wir weiterhin annehmen dass $v(x) = 0$ und $v(y) \geq 0$. Dann sind $x, y \in R$, also $x + y \in R$ und $v(x + y) \geq 0$. Wenn $v(x) \neq v(y)$, also $v(y) > 0$, dann ist $y \in \mathfrak{m}$ und $x \notin \mathfrak{m}$, also $x + y \notin \mathfrak{m}$, also $v(x + y) = 0$. □

**Bemerkung 2.8.8.** Für ein beliebiges $\alpha \in \mathbb{R}$ mit $\alpha > 1$ definiert

$$\|x\| := \alpha^{-v(x)}$$

eine multiplikative Norm auf $\mathrm{Quot}(R)$: Es ist $\|x\| = 0$ genau wenn $x = 0$, $\|xy\| = \|x\| \cdot \|y\|$, und

$$\|x + y\| \leq \max(\|x\|, \|y\|),$$

mit Gleichheit wenn $\|x\| \neq \|y\|$. Das ist eine stärkere Form der Dreiecksungleichung, man nennt $\| - \|$ auch eine *Ultranorm*. $R$ liegt in $\mathrm{Quot}(R)$ als Elemente mit $\|x\| \leq 1$.

**Beispiel 2.8.9.** Ein Beispiel eines diskreten Bewertungsrings ist $\mathbb{Z}_{(p)}$. Die Bewertung misst, wie oft eine Zahl durch $p$ teilbar ist. Der Quotientenkörper von $\mathbb{Z}_{(p)}$ ist $\mathbb{Q}$, und die entsprechende Bewertung auf $\mathbb{Q}$ ist $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

Insbesondere erkennen wir in $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}$ unsere erste Beschreibung von $\mathbb{Z}_{(p)}$ ("Brüche, deren Nenner nicht durch $p$ teilbar ist") wieder.

Die $p$-adischen Zahlen $\mathbb{Z}_p$ sind ein weiteres Beispiel eines diskreten Bewertungsrings, wo die Bewertung wieder Teilbarkeit durch $p$ misst. Der Quotientenkörper heißt $\mathbb{Q}_p$, er ist überabzählbar und als Erweiterung von $\mathbb{Q}$ kompliziert: Zum Beispiel enthält er eine Wurzel von $-1$ wenn $p = 4k + 1$. $\mathbb{Q}$ und $\mathbb{Q}_p$ sind trotzdem eng verwandt: Für die Ultranorm aus Bemerkung 2.8.8 stellt sich $\mathbb{Q}_p$ als Vervollständigung (z.B. mittels Cauchyfolgen) von $\mathbb{Q}$ heraus. $\mathbb{Q}_p$ lässt sich also beschreiben als "Grenzwerte von Reihen $\sum_{n=0}^{\infty} a_n$ mit $v_p(a_n) \to \infty$".

**Proposition 2.8.10.** *Für einen lokalen Ring $R$, der kein Körper ist, sind äquivalent:*

1. *$R$ ist Dedekindring*
2. *$R$ ist diskreter Bewertungsring*

*Beweis.* Die Implikation $1 \Rightarrow 2$ ist Lemma 2.8.4. Für die Umkehrung beobachten wir zunächst dass ein diskreter Bewertungsring $R$ als Hauptidealring automatisch Noethersch ist. Somit müssen wir nur prüfen dass $R$ normal ist. Wenn $x \in \mathrm{Quot}(R)$ ganz ist, betrachten wir

$$x^n + c_{n-1}x^{n-1} + \ldots + c_0 = 0.$$

Wenn $v(x) < 0$, dann ist $v(c_{n-1}x^{n-1} + \ldots + c_0) \geq \min_{0 \leq i \leq n-1}(v(c_i) + iv(x)) \geq (n-1)v(x)$, aber $v(x^n) = nv(x) < (n-1)v(x)$, somit

$$v(x^n + c_{n-1}x^{n-1} + \ldots + c_0) = nv(x),$$

im Widerspruch zu $x^n + c_{n-1}x^{n-1} + \ldots + c_0 = 0$. Also gilt $v(x) \geq 0$ und somit $x \in R$. □

**Theorem 2.8.11.** *Sei $R$ ein nullteilerfreier, Noetherscher Ring, der kein Körper ist. Dann sind äquivalent:*

1. *$R$ ist Dedekindring.*
2. *$R_{\mathfrak{m}}$ ist diskreter Bewertungsring für jedes Maximalideal $\mathfrak{m}$.*
3. *Jedes Ideal in $R$ ist flacher $R$-Modul.*
4. *Jedes Ideal in $R$ ist projektiver $R$-Modul.*
5. *Jedes Ideal in $R$, was nicht null ist, ist invertierbarer $R$-Modul.*

*Beweis.* $1 \Leftrightarrow 2$: Lokale Ringe $R_{\mathfrak{m}}$ sind genau dann Dedekind wenn sie diskrete Bewertungsringe sind (nach Proposition 2.8.10), und für Noethersche, nullteilerfreie Ringe können wir lokal testen, ob sie Dedekindringe sind.

$2 \Rightarrow 3$: Wenn $R$ Noethersch ist und die $R_{\mathfrak{m}}$ diskrete Bewertungsringe sind, sind sie insbesondere Hauptidealringe. Für ein Ideal $I \subseteq R$ sind die $I_{\mathfrak{m}} \subseteq R_{\mathfrak{m}}$ insbesondere flach, also ist $I$ flach.

$3 \Rightarrow 4$: Da $I$ weil $R$ Noethersch ist automatisch endlich präsentiert ist, ist flaches $I$ außerdem projektiv.

$4 \Rightarrow 5$: Da $I$ weil $R$ Noethersch ist automatisch endlich erzeugt ist, ist projektives $I$ außerdem Zariski-lokal frei und endlich erzeugt. Weil $R$ nullteilerfrei ist ist $\mathrm{rk}_{\mathfrak{p}}(R) = \mathrm{rk}_{(0)}(R)$, und der Rang bei 0 ist 1: Weil $I \neq 0$ ist, ist $(R/I) \otimes_R \mathrm{Quot}(R) = (R/I)_{(0)} = 0$, und somit impliziert die kurze exakte Folge

$$0 \to I \to R \to R/I \to 0$$

einen Isomorphismus $I_{(0)} \cong R_{(0)}$, also $I \otimes_R \mathrm{Quot}(R) \cong \mathrm{Quot}(R)$. Also ist $I$ Zariski-lokal frei von Rang 1, somit invertierbar.

$5 \Rightarrow 2$: Sei $\mathfrak{m}$ ein Maximalideal und $I \subseteq R_{\mathfrak{m}}$ irgendein Ideal das nicht 0 ist. Sei $f : R \to R_{\mathfrak{m}}$ die kanonische Abbildung. Das Ideal $f^{-1}I$ ist invertierbar, also existiert $s \notin \mathfrak{m}$ sodass $f^{-1}(I)[s^{-1}]$ in $R[s^{-1}]$ frei auf einem Erzeuger ist. Insbesondere ist $(f^{-1}(I))_{\mathfrak{m}} = I$ frei auf einem Erzeuger, und $R_{\mathfrak{m}}$ ist Hauptidealring. Also ist $R_{\mathfrak{m}}$ diskreter Bewertungsring. □

**Korollar 2.8.12.** Ein Ring $R$ ist Dedekind genau dann wenn jedes Ideal ein invertierbarer Modul ist (d.h. Noethersch und nullteilerfrei sind automatisch!)

*Beweis.* Noethersch folgt, weil jeder invertierbare Modul automatisch endlich erzeugt ist. Nullteilerfrei sieht man wie folgt: Für $a \in R$ wollen wir zeigen dass die "Multiplikation mit $a$"-Abbildung $R \to R$ injektiv ist. Sei $I$ das Bild. Da wir Injektivität lokal checken dürfen, und invertierbare Moduln lokal frei auf einem Erzeuger sind, dürfen wir annehmen dass $I \cong R$, aber eine surjektive Abbildung $R \to R$ ist automatisch bijektiv. Also ist $R \twoheadrightarrow I$ bijektiv und somit $a : R \to R$ injektiv. □

Wir können nun eine schöne Charakterisierung von Hauptidealringen beweisen. Dazu erinnern wir daran dass für einen Ring $R$ die Isomorphieklassen der invertierbaren Moduln eine Gruppe (bzgl. $\otimes$) bilden, die *Picardgruppe* $\mathrm{Pic}(R)$ genannt wird.

**Theorem 2.8.13.** *Sei $R$ ein kommutativer Ring. Dann sind äquivalent:*

1. *$R$ ist Hauptidealring.*
2. *$R$ ist Dedekind und $\mathrm{Pic}(R) = 0$ (heißt: Jeder invertierbare Modul ist frei von Rang 1).*
3. *$R$ ist faktoriell, Noethersch und eindimensional.*

*Beweis.* $1 \Rightarrow 3$: Hauptidealringe sind faktoriell (Algebra 1, sehen wir aber gleich nochmal), Noethersch und eindimensional.

$3 \Rightarrow 2$: Faktorielle Ringe sind normal, also folgt Dedekind. Außerdem haben faktorielle Ringe immer $\mathrm{Pic}(R) = 0$ (Übungsblatt, Idee war wie folgt: Man findet eine injektive Abbildung $L \to R$. Für lokale Erzeuger $s_i$ von $L$ bildet man nun einen größten gemeinsamen Teiler, und prüft dass dieser auch in $L$ liegt, und dann ein globaler Erzeuger ist.)

$2 \Rightarrow 1$: Wenn $R$ Dedekind ist, ist jedes Ideal invertierbar, also wegen $\mathrm{Pic}(R) = 0$ Hauptideal. □

Hauptidealring zu sein ist keine lokale Eigenschaft, aber zerlegt sich hier in einen lokalen Teil (Dedekind lässt sich für Noethersche, nullteilerfreie Ringe lokal testen) und einen ausschließlich globalen Teil (für Dedekindringe sind die $R_{\mathfrak{m}}$ ja immer Hauptidealringe, also $\mathrm{Pic}(R_{\mathfrak{m}}) = 0$).

Wir lernen auch, dass in Dedekindringen die einzige Obstruktion, faktoriell zu sein, durch die Existenz von Idealen, die keine Hauptideale sind, gegeben ist. Eine sehr schöne Erklärung dafür liefert die Beobachtung, dass in Dedekindringen immer eine *Primfaktorzerlegung von Idealen* existiert:

**Lemma 2.8.14.** *Sei $R$ Dedekind und $I \subseteq R$ ein Ideal, das nicht 0 ist. Dann ist $I$ Produkt endlich vieler Primideale, also*

$$I = \prod_i \mathfrak{p}_i^{e_i}$$

*Diese Zerlegung ist eindeutig (im üblichen Sinne wie bei der Primfaktorzerlegung, also bis auf Umordnen).*

*Beweis.* Sei $I_0 = I$. Wenn $I_0 = R$, so können wir das leere Produkt nehmen (das per Definition $R$ ist). Andernfalls ist $I_0$ in einem maximalen Ideal $\mathfrak{p}_0$ enthalten, und wir haben eine injektive Abbildung $I_0 \to \mathfrak{p}_0$ (die Inklusion). Diese passt in ein kommutatives Diagramm mit

$$\begin{array}{ccc} I_0 \otimes \mathfrak{p}_0 & & \\ \downarrow & \searrow & \\ I_0 & \longrightarrow & \mathfrak{p}_0, \end{array}$$

wo die beiden Abbildungen aus dem Tensorprodukt jeweils einfach $a \otimes b \mapsto ab$ schicken, und injektiv sind da sie durch Tensorieren mit dem flachen Modul $I_0$ bzw. $\mathfrak{p}_0$ aus der Inklusion $\mathfrak{p}_0 \to R$ bzw. $I_0 \to R$ hervorgehen. Die vertikale Abbildung ist außerdem nicht surjektiv, da $\mathfrak{p}_0 \to R$ das nicht ist.

Da Ideale invertierbar sind, können wir mit $\mathfrak{p}_0^{-1}$ tensorieren um ein neues Diagramm von injektiven Abbildungen zu erhalten:

$$\begin{array}{ccc} I_0 & & \\ \downarrow & \searrow & \\ I_0 \otimes \mathfrak{p}_0^{-1} & \longrightarrow & R \end{array}$$

Das Bild der horizontalen Abbildung ist wieder ein Ideal $I_1$, das $I_0$ echt enthält weil die vertikale Abbildung injektiv, aber nicht surjektiv ist. Außerdem gilt $I_0 = \mathfrak{p}_0 I_1$. Diesen Prozess können wir nun iterieren, und da $I_0 \subsetneq I_1 \subsetneq \ldots$ und $R$ Noethersch ist, erreichen wir nach endlich vielen Schritten $I_n = R$. Somit haben wir $I_0$ als endliches Produkt von Primidealen geschrieben.

Für die Eindeutigkeit sei $\mathfrak{p}$ ein Primideal was nicht 0 ist (also maximal ist), und $I_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}$ die Lokalisierung. Da $R_{\mathfrak{p}}$ diskreter Bewertungsring ist, ist $I_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^k$ für ein eindeutiges $k$. Wenn $I = \mathfrak{p}$ selbst, dann ist $k = 1$. Wenn $I =$

$\mathfrak{q} \neq 0$ irgendein anderes Primideal ist, dann ist $\mathfrak{q} \not\subset \mathfrak{p}$, also $\mathfrak{q}_\mathfrak{p} = R_\mathfrak{p}$ und $k = 0$. Wenn $I$ also ein endliches Produkt von Primidealen ist, zählt $k$ wie oft $\mathfrak{p}$ vorkommt. Insbesondere sind die Exponenten in der Primfaktorzerlegung eindeutig festgelegt. □

**Bemerkung 2.8.15.** Wenn alle Ideale Hauptideale sind, sehen wir für $r \in R$

$$(r) = \prod \mathfrak{p}_i^{e_i} = \prod (p_i)^{e_i} = (\prod p_i^{e_i}),$$

also $r = u \prod p_i^{e_i}$ für ein invertierbares Element $u$ und Primelemente $p_i$. Hauptidealringe sind also faktoriell.

**Beispiel 2.8.16.** Sei $R = \mathbb{Z}[\sqrt{-5}]$, $\mathfrak{p} = (2, 1 + \sqrt{-5})$, $\mathfrak{q} = (3, 1 + \sqrt{-5})$, $\overline{\mathfrak{q}} = (3, 1 - \sqrt{-5})$. Dann sind $\mathfrak{p}, \mathfrak{q}, \overline{\mathfrak{q}}$ keine Hauptideale, aber wir haben

$$\begin{aligned}
\mathfrak{p}^2 &= (2) \\
\mathfrak{q}\overline{\mathfrak{q}} &= (3) \\
\mathfrak{p}\mathfrak{q} &= (1 + \sqrt{-5}) \\
\mathfrak{p}\overline{\mathfrak{q}} &= (1 - \sqrt{-5})
\end{aligned}$$

Es handelt sich bei $2, 3, 1 \pm \sqrt{-5}$ also jeweils um Elemente, die sich nicht weiter in Elemente faktorisieren lassen, aber in Ideale. Das Ideal (6) hat nun die Primfaktorzerlegung

$$(6) = \mathfrak{p}^2\mathfrak{q}\overline{\mathfrak{q}} = (\mathfrak{p}^2)(\mathfrak{q}\overline{\mathfrak{q}}) = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}\overline{\mathfrak{q}}),$$

die sich auf zwei Weisen zu Faktorisierungen in Hauptideale zusammenfassen lässt, was auf

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

führt. In Elementen sehen wir diesen beiden Faktorisierungen keine gemeinsamen Faktoren an, in Idealen schon.

Wir leiten nun noch die übliche Beschreibung der Picardgruppe her. Sei $R$ ein Dedekindring und $K = \mathrm{Quot}(R)$ der Quotientenkörper.

**Definition 2.8.17.** *Wir schreiben $\mathcal{I}_R$ für die Menge der endlich erzeugten $R$-Untermoduln $M \subseteq K$. (Sogenannte gebrochene Ideale)*

**Lemma 2.8.18.** *$\mathcal{I}_R$ ist eine Gruppe bezüglich $\cdot$, und die kanonische Abbildung $\mathcal{I}_R \to \mathrm{Pic}(R)$ ist ein surjektiver Homomorphismus deren Kern besteht aus denjenigen Untermoduln $M \subseteq \mathcal{I}_R$, die von einem Element erzeugt werden.*

*Beweis.* Für einen endlich erzeugten $R$-Untermodul $M \subseteq K$ existiert $x \in K$ mit $xM \subseteq R$. Insbesondere ist $M$ abstrakt invertierbar. Sei $M'$ ein inverser Modul. Nun ist $\mathrm{Hom}_R(M', K) \cong M \otimes_R K$. Die Abbildung $M \to K$ induziert einen Isomorphismus $M \otimes_R K \to K$, da $M$ lokal frei von Rang 1 ist, und die Abbildung

nicht 0 ist. Wir finden nun also ein eindeutiges Element von $\mathrm{Hom}_R(M', K)$, das unter dieser Abbildung auf 1 geht, also ein $f : M' \to K$ sodass

$$\begin{array}{ccc} M \otimes_R M' & & \\ \downarrow \cong & \searrow^{f \cdot i} & \\ R & \xrightarrow{1} & K \end{array}$$

kommutiert. Somit ist $f(M')$ ein Inverses zu $M$ in $\mathcal{I}_R$.

Dass es sich um einen Homomorphismus handelt, folgt direkt weil $M \otimes_R N \to K$ injektiv ist für invertierbare Moduln $M$ und $N$ (das können wir lokal checken, wo diese frei sind).

Die Beschreibung des Kerns ist klar. □

**Korollar 2.8.19.** Es gibt eine exakte Folge

$$1 \to R^\times \to K^\times \to \mathcal{I}_R \to \mathrm{Pic}(R) \to 1.$$

**Lemma 2.8.20.** *In $\mathcal{I}_R$ besitzt jedes Element $I$ eine eindeutige Primfaktorzerlegung mit $I = \prod \mathfrak{p}_i^{e_i}$ mit $e_i \in \mathbb{Z}$. Also ist $\mathcal{I}_R \cong \bigoplus_{\mathfrak{p}} \mathbb{Z}$.*

*Beweis.* Jedes $I$ ist endlich erzeugt, es gibt also $r \in R$ mit $rI \subseteq R$. Indem wir die Primfaktorzerlegung von $I$ durch die von $(r)$ teilen, erhalten wir die für $I$. Eindeutigkeit folgt auch aus der Eindeutigkeit von Primfaktorzerlegung in $R$. □

**Bemerkung 2.8.21.** Für ein gebrochenes Ideal $I \in \mathcal{I}_R$ können wir $v_\mathfrak{p}(I) \in \mathbb{Z}$ als Häufigkeit von $\mathfrak{p}$ in der Primfaktorzerlegung von $I$ definieren. Für ein Element $x \in K^\times$ definieren wir entsprechend $v_\mathfrak{p}(x) = v_\mathfrak{p}((x))$. Dann ist also

$$\mathcal{I}_R = \text{“Alle möglichen Kombinationen von Bewertungen”}$$
$$\mathrm{im}(K^\times \to \mathcal{I}_R) = \text{“Kombinationen von Bewertungen, die für Elemente auftreten”}$$

und $\mathrm{Pic}(R)$ misst somit, welche Kombinationen von Bewertungen tatsächlich $(v_\mathfrak{p}(x))_\mathfrak{p}$ für Elemente $x \in K^\times$ sind.

Weiterhin haben wir

$$R \setminus \{0\} = \text{“Elemente von } K^\times\text{, deren Bewertungen alle } \geq 0 \text{ sind”}$$
$$R^\times = \text{“Elemente von } K^\times\text{, deren Bewertungen alle } 0 \text{ sind”}$$

**Beispiel 2.8.22.** Sei $R = \mathbb{Z}[i] \subseteq \mathbb{C}$. Dann ist $\mathbb{Z}[i]$ Dedekindring, da $1, i$ ganz sind, und wenn $a + bi$ ganz für $|a| \leq \frac{1}{2}$ und $|b| \leq \frac{1}{2}$ ist, dann folgt

$$(a + bi)(a - bi) = a^2 + b^2 \leq \frac{1}{4}$$

also $a + bi = 0$. Für eine Primzahl $p \in \mathbb{Z}$ ist $(p) \subseteq \mathbb{Z}[i]$ Primideal genau wenn $\mathbb{F}_p[x]/(x^2 + 1)$ nullteilerfrei ist, also wenn $x^2 + 1 \in \mathbb{F}_p[x]$ irreduzibel ist. Das ist genau dann der Fall wenn $(-1)$ kein Quadrat in $\mathbb{F}_p$ ist, also (weil $\mathbb{F}_p^\times$ zyklisch

von Ordnung $p-1$ ist) wenn $p$ ungerade und $(-1)^{\frac{p-1}{2}} \neq 1$. Das Ideal $(p)$ ist also prim genau wenn $p = 4k+3$. Für $p = 4k+1$ finden wir also Primfaktoren, und indem man über die Ordnung von $R/\mathfrak{p}$ und die Galoiskonjugation $i \mapsto -i$ nachdenkt sieht man dass diese Primfaktorzerlegung immer von der Form

$$(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}}$$

ist. In algebraischer Zahlentheorie werden wir außerdem $\mathrm{Pic}(\mathbb{Z}[i]) = 0$ sehen, und damit folgt $\mathfrak{p} = (a+bi)$, $\overline{\mathfrak{p}} = (a-bi)$, und $p = (a+bi)\cdot(a-bi) = a^2+b^2$. Umgekehrt impliziert die Lösbarkeit von $p = a^2+b^2$ dass $(p) = (a+bi)(a-bi)$, also $(p)$ in $\mathbb{Z}[i]$ in zwei Hauptideale faktorisiert werden kann. Man sieht also die Rolle die $\mathrm{Pic}(R) = 0$ auch für ganz konkrete zahlentheoretische Fragen spielt.