Kommutative Algebra

Goethe–Universität Frankfurt — Sommersemester 2015

für Bachelor

JAKOB STIX

Zusammenfassung. — Die Vorlesung Kommutative Algebra behandelt die Strukturtheorie kommutativer Ringe mit 1 und ihrer Moduln.

Dieses Skript wird fortlaufend aktualisiert. Es muß davon ausgegangen werden, daß es noch einige Zeit dauern wird, bis eine stabile Version entstanden ist und die gröbsten Fehler korrigiert sind. Sie lesen das Skript **auf eigene Gefahr!**

Bitte teilen Sie mir Korrekturvorschläge per Email oder persönlich nach der Vorlesung mit.

Inhaltsverzeichnis

1. Einführung 3
Literatur 3

Teil 1. Das Spektrum eines Rings 4
2. Ringe 4
2.1. Ringe und Homomorphismen 4
2.2. Produkte 5
2.3. Ideale, Faktorringe und Quotienten 6
2.4. Algebren 8
3. Primideale und Radikale 9
3.1. Maximale Ideale und Primideale 9
3.2. Das Jacobsonradikal 12
3.3. Das Nilradikal 12
3.4. Radikale und reduzierte Ringe 14
4. Moduln 16
4.1. Moduln und Homomorphismen 16
4.2. Quotienten und Isomorphiesätze 18
4.3. Produkte und Summen von Moduln 20
4.4. Kerne, Kokerne und Hom 22
4.5. Das Tensorprodukt von Moduln 23
4.6. Basiswechsel 27
4.7. Determinanten und allgemeiner Cayley–Hamilton 29
5. Grundkonstruktionen der homologischen Algebra 32
5.1. Komplexe und exakte Sequenzen 32
5.2. Kern, Kokern, Bild und Kobild 35
5.3. Das Schlangenlemma 37
5.4. Projektive Moduln 43
5.5. Flache Moduln und Algebren 46
6. Lokalisieren und lokale Eigenschaften 47
6.1. Lokalisierung von Ringen 47
6.2. Der Lokalisierungsfunktor für Moduln 51
6.3. Lokalisierung von Idealen und Algebren 54
6.4. Lokale Ringe 55
6.5. Lokale Eigenschaften 56

6.6. Das Tensorprodukt von Algebren 60
7. Das Spektrum 63
7.1. Das Spektrum als Funktor 63
7.2. Der Support 65
7.3. Die Krull–Dimension 67

Teil 2. Kettenbedingungen 68
8. Noethersch 68
8.1. Noethersche Moduln und Ringe 68
8.2. Etwas affine algebraische Geometrie 74
8.3. Vorbereitungen zum Hilbertschen Nullstellensatz 77
8.4. Das Maximalspektrum 78
9. Artinsch 81
9.1. Moduln endlicher Länge 81
9.2. Artinsche Moduln und Ringe 86
9.3. Der Krullsche Hauptidealsatz 89
10. Primärzerlegung und Assoziierte Primideale 92
10.1. Assoziierte Primideale 93
10.2. Die Primärzerlegung 97
11. Moduln über Hauptidealringen 100
11.1. Die Primärzerlegung von Torsionsmoduln über Hauptidealringen 100
11.2. Der Elementarteilersatz 105
11.3. Fitting-Ideale 109

1. Einführung

Die Vorlesung hat das Ziel, das Studium von algebraischer Geometrie und algebraischer Zahlentheorie vorzubereiten.

Literatur

[AM69] Sir Michael Francis Atiyah, Ian Grant Macdonald, *Introduction to commutative algebra*, Adison-Wesley, 1969.

[Bou89] Nicolas Bourbaki, *Éléments de mathématique. Algèbre commutative. Chapitre 1–7*, Hermann, Paris, 1961–1965; oder *Commutative algebra. Chapters 1–7*, Springer, 1989.

[Eis95] David Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts In Mathematics **150**, Springer, 1995.

[La02] Serge Lang, *Algebra*, revidierte dritte Auflage, Graduate Texts in Mathematics **211**, Springer, 2002.

[Mat89] Hideyuki Matsumura, *Commutative Ring Theory*, übersetzt von Miles Reid, Cambridge University Press, 1989.

Teil 1. Das Spektrum eines Rings

Bemerkung 1.1. Alle Ringe, die hier behandelt werden, sind kommutativ mit 1, sofern nichts Gegenteiliges explizit erwähnt wird.

2. Ringe

2.1. **Ringe und Homomorphismen.** Wir erinnern an die grundlegenden Definitionen und Beispiele.

Definition 2.1. Ein **Ring (mit Eins)** ist eine Menge R zusammen mit einer **Addition** $+$, so daß $(R,+)$ eine abelsche Gruppe ist, und einer assoziativen und distributiven **Multiplikation** (zu der es ein Einselement $1 \in R$ gibt). Ein **kommutativer Ring** ist ein Ring, dessen Multiplikation kommutativ ist.

Notation 2.2. Wir benutzen die üblichen Abkürzungen. Die Multiplikation kürzen wir ab durch $ab := a \cdot b$. Außerdem gilt 'Punkt vor Strich'. Das neutrale Element der Addition wird mit 0 bezeichnet, das additive Inverse zu $a \in R$ hat die Notation $-a$. Statt $a + (-b)$ schreiben wir wie gewöhnlich $a - b$.

Definition 2.3. Ein **Körper** ist ein Ring R mit $0 \neq 1$ und jedes $0 \neq x \in R$ ist **invertierbar**: es gibt $y \in R$ mit $xy = 1$.

Proposition 2.4. *Gilt* $0 = 1$ *in einem Ring* R*, dann ist* R *der Nullring* $R = \{0\}$ *(mit den einzig möglichen Additions- und Multiplikationsverknüpfungen).*

Beweis. Sei $a \in R$ ein beliebiges Element. Dann gilt

$$a = a \cdot 1 = a \cdot 0 = 0$$

und R enthält nur ein einziges Element. Weiter hat $R = \{0\}$ eine (einzige) Ringstruktur. □

Beispiel 2.5. (1) Die ganzen Zahlen $\mathbb{Z}$. Jeder Körper ist ein Ring: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_p$, $\mathbb{C}$, ...,

(2) Sei R ein Ring. Der Polynomring $R[X]$ und der Potenzreihenring

$$R[[X]] = \{\sum_{i=0}^{\infty} a_i X^i \ ; \ a_i \in R \text{ für alle } i\}$$

mit Koeffizienten aus R sind Ringe. Das geht auch mit mehreren Variablen: $R[X_1, \ldots, X_n]$ und $R[[X_1, \ldots, X_n]]$.

(3) Sei X eine Menge und R ein Ring. Dann ist die Menge

$$\mathrm{Abb}(X, R) := \{f \ ; \ f : X \to R\}$$

der Abbildungen von X nach R ein Ring, der **Ring der Funktionen** von X nach R, und zwar mit punktweiser Addition und Multiplikation: für $f_1, f_2 \in \mathrm{Abb}(X, R)$ und $x \in X$ gilt

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 \cdot f_2)(x) = f_1(x) \cdot f_2(x).$$

Die Ringaxiome sind erfüllt, weil sie in R erfüllt sind.

Bemerkung 2.6. Jeder Ring ist ein Ring von geeigneten Funktionen auf einer Menge. Das Beispiel $\mathrm{Abb}(X, R)$ ist also gut für die Intuition, aber trotzdem noch eine grobe Approximation, denn man muß akzeptieren, daß der Wertebereich der Funktionen von $x \in X$ abhängt. So ist beispielsweise $\mathbb{Z}$ der Ring der algebraischen Funktionen auf $\mathrm{Spec}(\mathbb{Z})$, einer Menge, die im Wesentlichen aus den Primzahlen besteht. Der Wert von $n \in \mathbb{Z}$ an der Primzahl p ist die Restklasse $n \mod p$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Man kann zumindest sehen, daß diese Funktionswerte die ganzen Zahlen als Funktionen eindeutig festlegen. Denn falls für $n, m \in \mathbb{Z}$ und alle Primzahlen p gilt $n \equiv m$

mod p, so wählen wir einfach eine Primzahl p, die größer als $2\max\{|n|,|m|\}$ ist, und finden wegen

$$-p < n - m < p$$

und $p \mid n-m$, daß $n = m$ sein muß. Entscheidend geht hier ein, daß es unendlich viele Primzahlen in $\mathbb{Z}$ gibt und damit die gewünschte Wahl von p auch durchgeführt werden kann.

Zu einer algebraischen Struktur gehört stets ein passender Begriff von Homomorphismen, also strukturerhaltender Abbildungen.

Definition 2.7. Ein **Ringhomomorphismus** ist eine Abbildung $f : R \to S$ zwischen Ringen R und S, so daß für alle $a, b \in R$ gilt:

(i) $f(a+b) = f(a) + f(b)$,
(ii) $f(ab) = f(a)f(b)$,
(iii) $f(1) = 1$.

Ein **Ringisomorphismus** ist ein bijektiver Ringhomomorphismus. Die Menge der Ringhomomorphismen $f : R \to S$ bezeichnen wir mit $\mathrm{Hom}_{\mathsf{rings}}(R, S)$ (oder mit $\mathrm{Hom}(R, S)$, wenn klar ist, daß Ringhomomorphismen gemeint sind).

Ringhomomorphismen kann man komponieren. Die Identität $\mathrm{id}_R : R \to R$ ist ein Ringhomomorphismus. Ein Ringisomorphismus ist ein Ringhomomorphismus $f : R \to S$, zu dem es einen inversen Ringhomomorphismus $g : S \to R$ mit $fg = \mathrm{id}_S$ und $gf = \mathrm{id}_R$ gibt.

Beispiel 2.8. So wie man bei Ringen an Ringe von Funktionen denken soll, soll man bei Ringhomomorphismen an das folgende Beispiel denken. Sei R ein Ring und $\varphi : Y \to X$ eine Abbildung von Mengen. Dann definiert das Folgende einen Ringhomomorphismus:

$$\begin{aligned} \varphi^* : \mathrm{Abb}(X, R) &\to \mathrm{Abb}(Y, R) \\ (f : X \to R) &\mapsto \varphi^* f = (f \circ \varphi : Y \to R), \end{aligned}$$

also $(\varphi^* f)(y) = f(\varphi(y))$ für alle $y \in Y$.

2.2. **Produkte.** Das **direkte Produkt** zweier Ringe R_1 und R_2 ist der Ring

$$R_1 \times R_2 = \{(a_1, a_2) \ ; \ a_i \in R_i\}$$

mit komponentenweiser Addition und Multiplikation. Allgemeiner ist das direkte Produkt einer Familie von Ringen R_i für $i \in I$ der Ring

$$\prod_{i \in I} R_i = \{(a_i)_{i \in I} \ ; \ a_i \in R_i \text{ für alle } i \in I\}$$

wieder mit komponentenweiser Addition und Multiplikation.

Bemerkung 2.9. (1) Für jedes $j \in I$ ist die Projektion $\mathrm{pr}_j : \prod_{i \in I} R_i \to R_j$ mit $\mathrm{pr}_j((a_i)) = a_j$ ein Ringhomomorphismus. Allgemeiner ist auch für eine Teilmenge $J \subseteq I$ die Projektion $\mathrm{pr}_J : \prod_{i \in I} R_i \to \prod_{j \in J} R_j$ mit $\mathrm{pr}_J((a_i)_{i \in I}) = (a_j)_{j \in J}$ ein Ringhomomorphismus.

(2) Wenn R_i für unendlich viele $i \in I$ nicht der Nullring ist, dann ist

$$\{(a_i) \in \prod_{i \in I} R_i \ ; \ a_i = 0 \text{ für fast alle } i\}$$

kein Unterring. Es fehlt die 1.

(3) Die Inklusion $R_j \to \prod_{i \in I} R_i$, welche alle Koordinaten mit Index $i \neq j$ mit 0 belegt, ist im Allgemeinen kein Ringhomomorphismus. Wohl ist die Inklusion additiv und multiplikativ, aber es geht nicht 1 auf 1.

Definition 2.10. Sei I eine Menge und für jedes $i \in I$ ein Ring R_i gegeben. Ein **Produkt** der Ringe R_i für alle $i \in I$ ist ein Ring P zusammen mit Ringhomomorphismen

$$p_i : P \to R_i,$$

so daß die **universelle Eigenschaft für Produkte** gilt: für jeden Ring A und Ringhomomorphismen $f_i : A \to R_i$ für alle $i \in I$ gibt es einen eindeutigen Ringhomomorphismus

$$f : A \to P$$

mit $p_i \circ f = f_i$. Mit andern Worten ist die natürliche Abbildung $f \mapsto (p_i \circ f)$

$$\mathrm{Hom}(A, P) \to \prod_{i \in I} \mathrm{Hom}(A, R_i)$$

bijektiv.

Satz 2.11 (Existenz von Produkten)**.** *Produkte von Ringen existieren und sind eindeutig bis auf eindeutigen Isomorphismus: sei I eine Menge und R_i ein Ring für alle $i \in I$. Dann ist das direkte Produkt $P = \prod_{i \in I} R_i$ zusammen mit den Projektionen $\mathrm{pr}_j : P \to R_j$ ein Produkt.*

Beweis. Übung. □

Bemerkung 2.12. Wir haben schon gewarnt, daß es mit der direkten Summe von Ringen nicht so einfach ist. Die Inklusionsabbildungen der Faktoren sind keine Ringhomomorphismen, und so gilt auch nicht die universelle Eigenschaft der direkten Summe! Diese Rolle übernimmt das Tensorprodukt. Dazu später mehr.

2.3. **Ideale, Faktorringe und Quotienten.** Das Bild eines Ringhomomorphismus $f : R \to S$ ist ein Unterring. Da wir Ringe mit 1 betrachten, gilt dasselbe **nicht** für den **Kern** von f

$$\ker(f) = \{a \in R \ ; \ f(a) = 0\}.$$

Definition 2.13. Ein **Ideal** ist eine Teilmenge $\mathfrak{a}$ eines Rings R, die

(i) eine Untergruppe bezüglich Addition ist,
(ii) und für alle $x \in \mathfrak{a}$ und $a \in R$ gilt $ax \in \mathfrak{a}$.

Definition 2.14. Sei R ein Ring und $M \subseteq R$ eine Teilmenge. Das von M **erzeugte Ideal** ist

$$(M) = \{a_1 x_1 + \ldots + a_n x_n \ ; \ n \in \mathbb{N}_0, a_i \in R, x_i \in M \text{ für } 1 \leq i \leq n\}.$$

Man überlegt sich leicht, daß (M) ein Ideal ist, und zwar das kleinste Ideal, das die Menge M enthält.

Bemerkung 2.15. Für eine endliche Menge $M = \{x_1, \ldots, x_n\}$ schreiben wir $(M) = (x_1, \ldots, x_n)$. In jedem Ring R sind $(0) = \{0\}$ und $(1) = R$ Ideale. Alle anderen Ideale von R heißen **echte Ideale** von R.

Bemerkung 2.16. In $\mathbb{Z}$ ist jedes Ideal von der From $\mathfrak{a} = (n)$ für ein $n \in \mathbb{N}_0$. Ideale sind in diesem Beispiel sehr nahe an den Zahlen, also den Elementen. Historisch entstanden Ideale aus dem Versuch, für Erweiterungen von $\mathbb{Z}$ zu Zahlbereichen in $\mathbb{C}$ die guten Eigenschaften von $\mathbb{Z}$ zu erhalten (eindeutige Faktorisierung in Primfaktoren). Das Wort 'Ideal' erinnert dabei an 'ideale Zahl'.

Die Vorstellung, Ideale seien 'ideale Zahlen', ist allerdings im allgemeinen Fall irreführend.

Definition 2.17. Sei $\mathfrak{a} \subseteq R$ ein Ideal im Ring R. Dann existiert auf der Faktorgruppe $R/\mathfrak{a}$ eine eindeutige Ringstruktur, **Faktorring** von R nach $\mathfrak{a}$, so daß die **kanonische Projektion**

$$p : R \to R/\mathfrak{a}$$

ein Ringhomomorphismus ist. Man definiert Multiplikation auf Vertretern als

$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) := ab + \mathfrak{a}.$$

Es ist nur zu zeigen, daß diese Multiplikation wohldefiniert ist (hier braucht man die Idealaxiome). Alle anderen Ringaxiome gelten automatisch: sie werden via p von R geerbt. Das überlege man sich!

Bemerkung 2.18. Sei R ein Ring. Die Ideale von R sind genau die Kerne von Ringhomomorphismen $f : R \to S$. Das ist nun klar, denn $\mathfrak{a} = \ker(R \to R/\mathfrak{a})$.

Satz 2.19 (Quotienten)**.** *Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist $p : R \to R/\mathfrak{a}$ eine Quotientenabbildung, d.h., es gilt die universelle Eigenschaft:*

(i) $p(\mathfrak{a}) = 0$*, und*

(ii) für jeden Ringhomomorphismus $f : R \to S$ mit $f(\mathfrak{a}) = 0$ gibt es ein eindeutiges

$$\varphi : R/\mathfrak{a} \to S$$

mit $f = \varphi \circ p$.

Bemerkung 2.20. Wegen der universellen Eigenschaft ist der Quotient nach einem Ideal $\mathfrak{a} \subseteq R$ eindeutig bis auf eindeutigen Isomorphismus, sofern er existiert. Von der Existenz haben wir uns durch die Konstruktion des Faktorrings überzeugt.

Satz 2.21 (Homomorphiesatz)**.** *Sei $f : R \to S$ ein Ringhomomorphismus. Dann induziert f einen Isomorphismus*

$$\begin{aligned} \bar{f} : R/\ker(f) &\to \operatorname{im}(f) \\ a + \ker(f) &\mapsto f(a) \end{aligned}$$

Beweis. Der Beweis folgt sofort aus der Quotienteneigenschaft des Faktorrings $R/\ker(f)$. □

Aus dem Homomorphiesatz, also im Wesentlichen aus der Quotienteneigenschaft der Faktorringe, folgen die Isomorphiesätze.

Satz 2.22 (Erster Isomorphiesatz)**.** *Sei $U \subseteq R$ ein Unterring und $\mathfrak{a} \subseteq R$ ein Ideal.*
Dann ist $U \cap \mathfrak{a}$ ein Ideal in U und $U + \mathfrak{a}$ ein Unterring von R mit Ideal $\mathfrak{a}$, und

$$\begin{aligned} U/(U \cap \mathfrak{a}) &\xrightarrow{\sim} (U + \mathfrak{a})/\mathfrak{a} \\ u + (U \cap \mathfrak{a}) &\mapsto u + \mathfrak{a} \end{aligned}$$

ist ein Isomorphismus.

Beweis. Das ist der Homomorphiesatz angewandt auf $U \to R \to R/\mathfrak{a}$. □

Satz 2.23 (Zweiter Isomorphiesatz)**.** *Sei R ein Ring und seien $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$ Ideale.*
Dann ist $\mathfrak{b}/\mathfrak{a}$ ein Ideal in $R/\mathfrak{a}$ und die durch den Ringhomomorphismus $R/\mathfrak{a} \to R/\mathfrak{b}$, definiert durch $a + \mathfrak{a} \mapsto a + \mathfrak{b}$ für alle $a \in R$, induzierte Abbildung

$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \xrightarrow{\sim} R/\mathfrak{b}$$

ist ein Isomorphismus.

Beweis. Die Quotienteneigenschaft für $R \to R/\mathfrak{a}$ führt, da $\mathfrak{a}$ in $R \to R/\mathfrak{b}$ auf 0 abgebildet wird, zum Ringhomomorphismus $R/\mathfrak{a} \to R/\mathfrak{b}$. Der Isomorphismus kommt dann aus dem Homomorphiesatz für $R/\mathfrak{a} \to R/\mathfrak{b}$. □

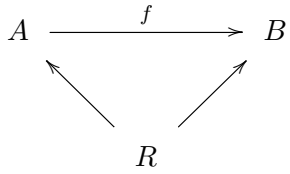
Proposition 2.24. *Sei $f : R \twoheadrightarrow S$ ein surjektiver Ringhomomorphismus. Dann ist $\mathfrak{b} \mapsto f^{-1}(\mathfrak{b})$ eine Bijektion*

$$\{\mathfrak{b} \ ; \ \textit{Ideal in } S\} \to \{\mathfrak{a} \ ; \ \textit{Ideal in } R, \ \textit{mit } \ker(f) \subseteq \mathfrak{a}\}$$

Beweis. Für ein Ideal $\mathfrak{b}$ von S ist $f^{-1}(\mathfrak{b})$ der Kern von $R \to S \to S/\mathfrak{b}$ und damit ein Ideal, das $\ker(f)$ enthält. Die Umkehrabbildung ist $\mathfrak{a} \mapsto \mathfrak{b} = \mathfrak{a}/\ker(f)$. □

2.4. **Algebren.** Algebren sind Ringe mit bekannten Konstanten. Genauer:

Definition 2.25. Eine R-**Algebra** über einem Ring R ist ein Ring A zusammen mit einem Homomorphismus $R \to A$, genannt **Strukturabbildung**. Ein R-**Algebrenhomomorphismus** zwischen R-Algebren $R \to A$ und $R \to B$ ist ein Ringhomomorphismus $f : A \to B$, der mit den Strukturabbildungen verträglich ist: es kommutiert



Die Menge aller R-Algebrahomomorphismen bezeichnen wir mit

$$\mathrm{Hom}_R(A, B) = \mathrm{Hom}_{R-\mathsf{alg}}(A, B).$$

Beispiel 2.26. (1) Das wichtigste Beispiel ist sicher der Polynomring $R[X_1, \ldots, X_n]$ über einem Ring R. Dies ist mit der Inklusion der konstanten Polynome eine R-Algebra.
(2) Genauso kann man den Potenzreihenring $R[[X_1, \ldots, X_n]]$ als R-Algebra auffasssen.
(3) Da $R[X_1, \ldots, X_n] \subseteq R[[X_1, \ldots, X_n]]$ ist der Potenzreihenring auch eine Algebra über dem Polynomring.
(4) Sei a ein Ideal in R. Dann ist $R/\mathfrak{a}$ vermöge der Quotientenabbildung $R \to R/\mathfrak{a}$ eine R-Algebra.
(5) Sei $\mathfrak{p}$ ein Primideal von R. Dann ist der Restklassenkörper $\kappa(\mathfrak{p})$ eine R-Algebra.
(6) Jeder Ring erlaubt einen eindeutigen Ringhomomorphismus $\mathbb{Z} \to R$. Jeder Ringhomomorphismus repsektiert diese Struktur als $\mathbb{Z}$-Algbera (wegen der Eindeutigkeit). Daher sind Ringe dasselbe wie $\mathbb{Z}$-Algebren.

Satz 2.27 (Universelle Eigenschaft des Polynomrings)**.** *Sei R ein Ring und $n \in \mathbb{N}$. Der Polynomring $R[X_1, \ldots, X_n]$ als R-Algebra und die Elemente $X_1, \ldots, X_n$ sind universell mit der folgenden Eigenschaft: für jede R-Algebra $\iota : R \to A$ gibt es zu jedem Tupel $a_1, \ldots, a_n$ von Elementen aus A genau einen R-Algebrenhomomorphismus*

$$R[X_1, \ldots, X_n] \to A,$$

der dadurch charakterisiert ist, daß X_i auf a_i für alle $i = 1, \ldots, n$ abgebildet wird. Also

$$\mathrm{Hom}_R(R[X_1, \ldots, X_n], A) = A^n$$

via $f \mapsto f(X_1), \ldots, f(X_n)$.

Beweis. Wir verwenden die Multiindexschreibweise $I = (i_1, \ldots, i_n)$ und

$$X^I = \prod_{\nu=1}^{n} X_\nu^{i_\nu}.$$

Zu einem Tupel $a_1, \ldots, a_n$ gehört die Auswertung $P \mapsto P(a_1, \ldots, a_n)$ definiert durch

$$P = \sum_I c_I X^I \mapsto P(a_1, \ldots, a_n) = \sum_I c_I \prod_{\nu=1}^{n} a_\nu^{i_\nu}.$$

Der Rest ist klar. □

Definition 2.28. Eine **endlich erzeugte** R-Algebra ist eine R-Algebra A, die als Ring von den Bildern von $R \to A$ und endlich vielen weiteren Erzeugern erzeugt werden kann.

Bemerkung 2.29. Endlich erzeugte R-Algebren sind dasselbe wie (isomorph zu einem) Quotienten eines Polynomrings über R. Sei A eine endlich erzeugte R-Algebra und $a_1, \ldots, a_n \in A$ Erzeuger als R-Algebra. Erzeuger zu sein bedeutet genau, daß die nach Satz 2.27 zu diesem Tupel gehörende Abbildung

$$R[X_1, \ldots, X_n] \to A$$

surjektiv ist. Nach dem Homomorphiesatz sind Quotienten dasselbe wie homomorphe Bilder, also zum Beispiel A.

Umgekehrt, wenn A Quotient von $R[X_1, \ldots, X_n]$ ist, dann erzeugen die endlich vielen Bilder der Variablen A als R-Algebra.

Die Struktur endlich erzeugter Algebren (über einem Körper) ist ein natürliches Ziel, denn allgemeine Ringe sind ein bizarrer Zoo. Die obige Überlegung reduziert dieses Unterfangen auf das Studium der Quotienten des Polynomrings in mehreren Variablen.

3. Primideale und Radikale

3.1. **Maximale Ideale und Primideale.** Sei $\mathfrak{m}$ ein Ideal des Rings R. Nach Proposition 2.24 hat der Quotient $R/\mathfrak{m}$ nur triviale Ideale, wenn entweder $\mathfrak{m} = R$ und damit $R/\mathfrak{m} = 0$, oder $\mathfrak{m}$ maximal bezüglich Inklusion unter den von R verschiedenen Idealen von R ist.

Lemma 3.1. *Ein Ring $R \neq 0$ ist ein Körper genau dann, wenn R nur die trivialen Ideale* (0) *und* (1) *hat.*

Beweis. Für jedes $0 \neq x \in R$ gilt dann $(x) = R$, also gibt es $y \in R$ mit $xy = 1$. Damit ist R ein Körper, denn jedes von 0 verschiedene Element ist invertierbar. Die Umkehrung ist trivial. □

Die folgende Definition klammert den trivialen Fall $R/\mathfrak{m} = 0$ aus:

Definition 3.2. Ein Ideal $\mathfrak{m}$ eines Rings R ist ein **maximales Ideal**, wenn der Quotient $R/\mathfrak{m}$ ein Körper ist.

Definition 3.3. Ein **Nullteiler** in einem Ring R ist ein Element $x \in R$, für das es ein $0 \neq y \in R$ gibt mit $xy = 0$.

Definition 3.4. Ein **Integritätsring** ist ein **nullteilerfreier** Ring R mit $1 \neq 0$, d.h. in dem 0 der einzige Nullteiler ist: für alle $x, y \in R$ gilt

$$xy = 0 \quad \Longrightarrow \quad x = 0 \text{ oder } y = 0.$$

Definition 3.5. Ein **Primideal** in einem Ring R ist ein Ideal $\mathfrak{p}$ von R, so daß der Faktorring $R/\mathfrak{p}$ ein Integritätsring ist. Das ist offensichtlich äquivalent zu: für alle $x, y \in R$ mit $xy \in \mathfrak{p}$ gilt $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.

Der **Restklassenkörper** eines Primideals $\mathfrak{p}$ in R ist $\kappa(\mathfrak{p}) = \mathrm{Quot}(R/\mathfrak{p})$.

Bemerkung 3.6. Körper sind Integritätsringe, also sind maximale Ideale Primideale (aber nicht umgekehrt, man suche ein Beispiel!).

Das Ideal (0) ist ein Primideal in R genau dann, wenn R ein Integritätsring ist.

Beispiel 3.7. Sei k ein Körper. Dann ist $(Y^2 - X^3)$ ein Primideal von $k[X, Y]$. Das sehe ich am besten so ein: Der k-Algebrahomomorphismus

$$k[X, Y] \to k[T],$$

der $X \mapsto T^2$ und $Y \mapsto T^3$ abbildet, schickt $Y^2 - X^3$ auf 0 und faktorisiert daher über

$$\varphi : k[X, Y]/(Y^2 - X^3) \to k[T].$$

Da $k[T]$ ein Integritätsring ist, ist auch das Bild nullteilerfrei. Es reicht zu zeigen, daß φ injektiv ist.

Jedes Polynom P in X, Y hat modulo $Y^2 - X^3$ einen Vertreter der Form

$$P(X,Y) \equiv f(X) + Yg(X) \mod (Y^2 - X^3).$$

Angenomen $P(T^2, T^3) = 0$, dann ist

$$f(T^2) + T^3 g(T^2) = 0 \in k[T].$$

Koeffizientenvergleich zeigt $f = g = 0$. Somit ist φ injektiv und $(Y^2 - X^3)$ prim.

Zur Existenz von Primidealen und maximalen Idealen verallgemeinern wir das übliche Argument.

Definition 3.8. Eine **multiplikative** (oder genauer eine **multiplikativ abgeschlossene** Teilmenge eines Rings R ist eine Teilmenge $S \subseteq R$ mit

(i) $1 \in S$,
(ii) für alle $s, t \in S$ ist $st \in S$.

Synonym verwenden wir auch die Bezeichnung **multiplikatives System** für eine multiplikative Teilmenge.

Beispiel 3.9. Ein Ideal $\mathfrak{a} \subseteq R$ ist ein Primideal genau dann, wenn $R \setminus \mathfrak{a}$ multiplikativ abgeschlossen ist.

Proposition 3.10. *Sei $\mathfrak{a} \subseteq R$ ein Ideal und $S \subseteq R$ eine multiplikative Teilmenge. Wenn $\mathfrak{a} \cap S = \emptyset$, dann gibt es ein Primideal $\mathfrak{p}$ von R mit*

$$\mathfrak{a} \subseteq \mathfrak{p} \subseteq R \setminus S.$$

Genauer: die bezüglich Inklusion maximalen Ideale, welche $\mathfrak{a}$ enthalten und S vermeiden, sind Primideale und solche gibt es.

Beweis. Die Menge

$$\Sigma = \{\mathfrak{b} \ ; \ \text{ Ideal von } R, \ \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus S\}$$

ist bezüglich Inklusion partiell geordnet, sogar induktiv geordnet mit der Vereinigung als obere Schranke. Außerdem ist $\mathfrak{a} \in \Sigma$, also ist Σ nicht leer. Nach dem Lemma von Zorn enthält Σ maximale Elemente. Es bleibt zu zeigen, daß ein maximales $\mathfrak{p} \in \Sigma$ ein Primideal ist.

Sei $\mathfrak{p}$ so ein maximales Element von Σ. Angenommen es gibt $x, y \in R$ mit $xy \in \mathfrak{p}$, aber $x, y \notin \mathfrak{p}$. Dann sind die Ideale $(\mathfrak{p}, x)$ und $(\mathfrak{p}, y)$ echt größer als $\mathfrak{p}$ und wegen der Maximalität von $\mathfrak{p}$ nicht in Σ. Es gibt also $s, t \in S$ und $a, b \in \mathfrak{p}$ und $f, g \in R$ mit

$$s = a + fx \quad t = b + gy.$$

Das ist aber wegen

$$st = (a + fx)(b + gy) = ab + fxb + gya + fg(xy) \in \mathfrak{p} \cap S = \emptyset$$

ein Widerspruch. □

Korollar 3.11 (Existenz maximaler Ideale)**.** *Jedes Ideal $\mathfrak{a} \neq R$ ist in einem maximalen Ideal $\mathfrak{m}$ von R enthalten. Insbesondere hat jeder Ring $R \neq 0$ ein maximales Ideal.*

Beweis. Proposition 3.10 für $S = \{1\}$. Da $\mathfrak{a} \neq R$, gilt $1 \notin \mathfrak{a}$.

Wenn R nicht der Nullring ist, dann ist $(0) \neq R$, und das Argument findet Anwendung. □

Alternativ kann man auch zuerst zeigen, daß jeder Ring $R \neq 0$ ein maximales Ideal hat. Dann zeigt man die Existenz von maximalen Idealen, die $\mathfrak{a}$ enthalten, durch das Urbild eines maximalen Ideals von $R/\mathfrak{a}$ unter $p : R \to R/\mathfrak{a}$. Das ist nämlich wieder ein maximales Ideal, denn $R/p^{-1}(\mathfrak{m}) = (R/\mathfrak{a})/\mathfrak{m}$ ist Körper.

Notation 3.12. Wir vereinbaren für ein Element $f \in R$ und ein Primideal $\mathfrak{p}$ von R die Notation

$$f(\mathfrak{p}) := \ (f + \mathfrak{p}) \in R/\mathfrak{p} \subseteq \kappa(\mathfrak{p}).$$

Beispiel 3.13. Sei k ein Körper. Der Kern der Auswertung $k[X] \to k$ in $a \in k$ wird erzeugt von $X - a$, denn (Taylorentwicklung) für alle Polynome $f \in k[X]$ gilt

$$f(X) = f(a) + (X - a) \cdot g(X)$$

für ein geeignetes Polynom $g \in k[X]$. Die Auswertung ist surjektiv, also $(X - a)$ ein maximales Ideal $\mathfrak{m}_a$ von $k[X]$.

Nach dem Homomorphiesatz induziert die Auswertung einen Isomorphismus

$$\kappa(\mathfrak{m}_a) = k[X]/(X - a) \simeq k.$$

Unter diesem Isomorphismus entsprechen sich

$$f(\mathfrak{m}_a) = f(a).$$

Gewisse maximale Ideale parametrisieren also die Punkte in der affinen Geraden $\mathbb{A}^1(k) = k$ und die Auswertung der Polynome im maximalen Ideal bzw. dem Punkt entspricht sich.

Bemerkung 3.14. Das Beispiel 3.13 legt nahe, den Ring mittels des Ringhomomorphismus

$$\begin{aligned} R &\to \prod_{\mathfrak{p}} \kappa(\mathfrak{p}) \\ f &\mapsto f(\mathfrak{p}) \end{aligned} \tag{3.1}$$

als Ring von Funktionen auf der Menge seiner Primideale anzusehen. Die erste psychologische Hürde, die man hier nehmen muß, besteht darin, die von Punkt (Primideal) zu Punkt variierenden Wertebereiche $\kappa(\mathfrak{p})$ zu akzeptieren.

Satz 3.15 (Primvermeidung)**.** *Sei $\mathfrak{a} \subseteq R$ ein Ideal und seien $\mathfrak{p}_i \in \operatorname{Spec}(R)$ für $i = 1, \ldots, n$ eine endliche Menge von Primidealen. Dann gilt genau eine der beiden Eigenschaften:*

(a) Die Elemente von $\mathfrak{a}$ haben auf $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ eine gemeinsame Nullstelle: es gibt ein i mit

$$\mathfrak{a} \subseteq \mathfrak{p}_i.$$

(b) (Primvermeidung) Es gibt $f \in \mathfrak{a}$, das keine Nullstelle in einem der $\mathfrak{p}_i$ für $i = 1, \ldots, n$ hat:

$$\mathfrak{a} \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Beweis. Die beiden Bedingungen widersprechen sich offensichtlich. Wir führen den Beweis per Induktion nach n. Der Fall $n = 1$ ist trivial ($n = 0$ auch). Sei daher der Satz für Mengen mit $< n$ Primidealen bewiesen.

Angenommen (a) und (b) gelten beide nicht. In Bezug auf die Mengen $\{\mathfrak{p}_i \,;\, 1 \leq i \leq n, i \neq j\}$ folgt dann per Induktion (b). Dafür gibt es Zeugen

$$x_j \in \mathfrak{a} \setminus \bigcup_{i \neq j} \mathfrak{p}_i$$

für jedes $1 \leq j \leq n$. Weil (b) in Bezug auf die Menge $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ auch nicht gilt, folgt

$$x_j \in \mathfrak{p}_j.$$

Per Konstruktion hat die 'Funktion' x_j nur in $\mathfrak{p}_j$ eine Nullstelle. Wir betrachten nun

$$f_i = \prod_{j \neq i} x_j \in \mathfrak{a}.$$

Dann gilt

$$f_i(\mathfrak{p}) = \prod_{j \neq i} x_j(\mathfrak{p}) = \begin{cases} 0 & \mathfrak{p} = \mathfrak{p}_j, j \neq i, \\ \neq 0 & \mathfrak{p} = \mathfrak{p}_i. \end{cases}$$

Die Summe
$$f = \sum_i f_i$$
ist weiter in $\mathfrak{a}$, aber hat keine Nullstelle in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, und das zeigt (b), Widerspruch. □

3.2. **Das Jacobsonradikal.** Das Beispiel 3.13 beschreibt Polynome bereits in der Regel gut (endliche Körper sind ein Problem) durch ihre Polynomfunktion und hier die Auswertung in maximalen Idealen. Der Kern des Ringhomomorphismus
$$\begin{aligned} R &\to \prod_{\mathfrak{m}} \kappa(\mathfrak{m}) \\ f &\mapsto f(\mathfrak{m}) \end{aligned}$$
der Auswertungen in maximalen Idealen hat auch einen Namen.

Definition 3.16. Das **Jacobsonradikal** eines Rings R ist das Ideal
$$\operatorname{Rad}(R) = \bigcap_{\mathfrak{m}} \mathfrak{m}.$$

Definition 3.17. Eine **Einheit** im Ring R ist ein Ringelement $a \in R$ mit multiplikativem Inversen in R: es gibt ein $b \in R$ mit $ab = ba = 1$. Die Menge der Einheiten
$$R^\times = \{a \in R\ ;\ \ a \text{ ist Einheit}\}$$
ist eine Gruppe bezüglich Multiplikation aus R. Diese Gruppe heißt **Einheitengruppe** von R.

Beispiel 3.18. (1) Ein Körper ist ein Ring R mit $R^\times = R \setminus \{0\}$ und $0 \neq 1$.
(2) Die Einheiten von $\mathbb{Z}$ sind $\mathbb{Z}^\times = \{1, -1\}$ und als Gruppe isomorph zu $\mathbb{Z}/2\mathbb{Z}$.
(3) Sei R ein Integritätsring. Dann ist $R[X]^\times = R^\times$ und $f \in R[[X]]$ ist Einheit genau dann, wenn $f(0) \in R^\times$. (Die Auswertung der Potenzreihe in 0 ist der konstante Term!)

Proposition 3.19. *Das Jacobsonradikal hat die folgende alternative Beschreibung*
$$\operatorname{Rad}(R) = \{f \in R\ ;\ \ \textit{für alle } a \in R \textit{ gilt } 1 - af \in R^\times\}.$$

Beweis. Sei f in allen maximalen Idealen enthalten. Falls $1 - af$ keine Einheit ist, dann gibt es ein maximales Ideal $(1 - af) \subseteq \mathfrak{m}$ und $1 = (1 - af) + af \in \mathfrak{m}$, Widerspruch. Dies zeigt: $\operatorname{Rad}(R)$ ist in der rechten Seite enthalten.

Sei nun f in der rechten Seite und $\mathfrak{m}$ maximal. Wenn $f \notin \mathfrak{m}$, dann ist $f(\mathfrak{m}) \neq 0 \in R/\mathfrak{m}$ und es gibt ein Inverses $\bar{a} = f(\mathfrak{m})^{-1}$. Wähle $a \in R$ im Urbild von $\bar{a}$. Dann ist $1 - af \in \mathfrak{m}$, somit keine Einheit in R, Widerspruch. Dies zeigt die andere Inklusion. □

3.3. **Das Nilradikal.** Wir wenden uns nun dem Kern des Ringhomomorphismus (3.1) zu, also den Ringelementen, die man als Funktionen nicht *sehen* kann.

Definition 3.20. Ein **nilpotentes Element** eines Rings ist ein Element $f \in R$ mit $f^n = 0$ für alle $n \gg 0$.

Lemma–Definition 3.21. *Das **Nilradikal** eines Rings R ist das Ideal*
$$\mathscr{N}(R) = \{f \in R\ ;\ f \textit{ nilpotent}\}.$$

Beweis. Wir müssen zeigen, daß $\mathscr{N}(R)$ ein Ideal ist. Wenn $a \in R$ und $f \in \mathscr{N}(R)$ mit $f^n = 0$, dann ist auch $(af)^n = a^n f^n = 0$ und $af \in \mathscr{N}(R)$.

Wenn $f, g \in \mathscr{N}(R)$ mit $f^n = g^n = 0$, dann ist
$$(f + g)^{2n} = \sum_{i=-n}^{n} \binom{2n}{n+i} f^{n+i} g^{n-i} = 0,$$
denn stets ein Exponent ist $\geq n$. □

Satz 3.22. *Es gilt*

$$\mathcal{N}(R) = \bigcap_{\mathfrak{p}\ prim} \mathfrak{p}.$$

Insbesondere besteht der Kern des Homomorphismus (3.1) *genau aus den nilpotenten Elementen.*

Beweis. Sei $\mathfrak{p}$ ein Primideal und $f \in R$ nilpotent. Aus $f^n = 0 \in \mathfrak{p}$ folgt (per Induktion über die Anzahl der Faktoren), daß bereits einer der Faktoren von f^n aus $\mathfrak{p}$ sein muß, also $f \in \mathfrak{p}$. Dies zeigt $\mathcal{N}(R) \subseteq \mathfrak{p}$, also auch im Schnitt aller $\mathfrak{p}$.

Sei $f \in R$ nicht nilpotent. Dann ist $S_f = \{1, f, f^2, \ldots, f^n, \ldots\}$ ein multiplikatives System, das (0) nicht trifft. Nach Proposition 3.10 gibt es dann ein Primideal $\mathfrak{p}$ von R mit $\mathfrak{p} \subseteq R \setminus S_f$. Insbesondere gilt $f \notin \mathfrak{p}$. Dies zeigt den Satz. □

Korollar 3.23. *Es gilt* $\mathcal{N}(R) \subseteq \mathrm{Rad}(R)$.

Im Kapitel über lokale Ringe sehen wir, daß die Umkehrung von Korollar 3.23 nicht gilt.

Definition 3.24. Ein **nilpotentes Ideal** in einem Ring R ist ein Ideal $\mathfrak{a}$ von R mit $\mathfrak{a}^n = (0)$ für alle $n \gg 0$.

Beispiel 3.25. Sei k ein Körper. Im Ring

$$R = k[X_i; i \in \mathbb{N}]/(X_i^i; i \in \mathbb{N})$$

sind alle X_i nilpotent. Das Nilradikal enthält daher alle X_i und ist genauer

$$\mathcal{N}(R) = (X_i; i \in \mathbb{N}),$$

denn der Quotient ist k, ein Körper, also ist $(X_i; i \in \mathbb{N})$ schon ein maximales Ideal, damit das einzige Primideal in R. Dieses $\mathcal{N}(R)$ besteht nur aus nilpotenten Elementen, aber für kein $n \geq 0$ ist $\mathcal{N}(R)^n = (0)$. Es gibt einfach keine uniforme Potenz, die alle nilpotenten Elemente annulliert: man überlege sich

$$X_i^n = 0 \in R$$

genau dann, wenn $n \geq i$ (das braucht in eine Richtung noch ein Argument!).

Bemerkung 3.26. Ein nilpotentes Ideal besteht ausschließlich aus nilpotenten Elementen. Die Umkehrung gilt nicht. Wir haben in Beispiel 3.25 gesehen: jedes nilpotente Ideal von R ist in $\mathcal{N}(R)$ enthalten, aber $\mathcal{N}(R)$ braucht selbst nicht nilpotent zu sein.

Ein von endlich vielen nilpotenten Elementen erzeugtes Ideal ist jedoch nilpotent. Sei $\mathfrak{a} = (f_1, \ldots, f_r) \subseteq R$ mit f_i nilpotent für alle $1 \leq i \leq r$. Da es nur endlich viele sind, reicht ein $n \gg 0$ für $f_i^n = 0$ für alle i. Ein beliebiges Element in $\mathfrak{a}$ hat nun die Form

$$g = x_1 f_1 + \ldots + x_r f_r$$

mit $x_i \in R$. Multipliziert man rn-viele von diesen und sortiert um in Linearkombinationen von Monomen in den f_i, dann hat jedes der Monome den Grad nr. Mindestens einer der Erzeuger f_i kommt dann mit Vielfachheit $\geq n$ vor. Das Monom verschwindet wegen $f_i^n = 0$. Also gilt $\mathfrak{a}^{rn} = (0)$ und $\mathfrak{a}$ ist nilpotent als Ideal.

Lemma 3.27 (geometrische Reihe)**.** *Sei $f \in R$ nilpotent. Dann ist $1 \pm f$ eine Einheit.*

Beweis. Mit f ist auch $-f$ nilpotent. Es reicht daher $1 - f$.

Sei $f^n = 0$. Dann ist

$$(1 - f)(1 + f + f^2 + \ldots + f^{n-1}) = 1 - f^n = 1.$$ □

Proposition 3.28. *Sei R ein Ring und $f \in R$. Dann sind äquivalent:*

(i) *f ist nilpotent.*

(ii) *$1 - fX \in R[X]$ ist eine Einheit.*

Beweis. Wenn $f \in R$ nilpotent ist, dann ist auch $fX \in R[X]$ nilpotent. Lemma 3.27 zeigt dann, daß $1 - fX$ eine Einheit ist.

Sei nun umgekehrt f nicht nilpotent. Dann gibt es nach Satz 3.22 ein Primideal $\mathfrak{p}$ von R mit $f \notin \mathfrak{p}$. Unter dem koeffizientenweisen Auswertungshomomorphismus

$$R[X] \to (R/\mathfrak{p})[X] \to \kappa(\mathfrak{p})[X]$$

geht $1 - fX$ damit auf das Polynom $1 - f(\mathfrak{p})X$ vom Grad 1 im Polynomring über dem Körper $\kappa(\mathfrak{p})$. Wäre $1 - fX$ Einheit in $R[X]$, so auch seine Auswertung $1 - f(\mathfrak{p})X$, ein Widerspruch dazu, daß in $\kappa(\mathfrak{p})[X]$ nur konstante Polynome Einheiten sein können. □

Wir schließen den Abschnitt mit einer Anwendung des Lemmas von Zorn.

Satz 3.29. *Sei R ein Ring.*

(1) *Es gibt in* $\operatorname{Spec}(R)$ *minimale Elemente bezüglich Inklusion.*
(2) *Genauer gibt es zu jedem* $\mathfrak{p} \in \operatorname{Spec}(R)$ *ein bezüglich Inklusion minimales Primideal* $\mathfrak{p}_0$ *mit* $\mathfrak{p}_0 \subseteq \mathfrak{p}$.
(3) *Insbesondere gilt*

$$\mathscr{N}(R) = \bigcap_{\mathfrak{p}_0 \text{ minimal}} \mathfrak{p}_0.$$

Beweis. (1) Die Menge $\operatorname{Spec}(R)$ ist nicht leer und bezüglich fallender Inklusion induktiv geordnet. Die obere (besser untere) Schranke einer totalgeordneten Teilmenge $(\mathfrak{p}_i)$ ist der Schnitt $\mathfrak{p} = \bigcap_i \mathfrak{p}_i$. Wenn es Elemente $a, b \in R$ gibt mit $ab \in \mathfrak{p}$, aber $a, b \notin \mathfrak{p}$, dann ist für einen hinreichend kleinen Index i auch schon $a, b \notin \mathfrak{p}_i$, aber trotzdem $ab \in \mathfrak{p}_i$, Widerspruch. Daher ist $\mathfrak{p}$ ein Primideal.

(2) folgt aus (1) angewandt auf $R_{\mathfrak{p}}$ und aus den natürlichen Identifikationen.

(3) ist unmittelbare Folge von (2) und Satz 3.22. □

3.4. **Radikale und reduzierte Ringe.** Ringe, in denen die Elemente f eindeutig durch die Funktion $f(\mathfrak{p})$ auf Primidealen $\mathfrak{p}$ festgelegt sind, haben einen Namen:

Definition 3.30. Ein **reduzierter** Ring ist ein Ring, in dem 0 das einzige nilpotente Element ist.

Beispiel 3.31. Integritätsringe sind reduziert.

Definition 3.32. Das **Radikal** eines Ideals $\mathfrak{a}$ im Ring R ist das Ideal

$$\sqrt{\mathfrak{a}} = \{f \in R \,;\; f^n \in \mathfrak{a} \text{ für } n \gg 0\}.$$

Proposition 3.33. *Für Ideale $\mathfrak{a}, \mathfrak{b}$ im Ring R gilt*

(1) $\sqrt{\mathfrak{a}}$ *ist das Urbild von* $\mathscr{N}(R/\mathfrak{a})$ *unter der Projektion* $R \to R/\mathfrak{a}$. *Insbesondere ist das Radikal von* $\mathfrak{a}$ *ein Ideal.*
(2) $\mathscr{N}(R) = \sqrt{(0)}$,
(3) *wenn* $\mathfrak{a} \subseteq \mathfrak{b}$, *dann* $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$,
(4) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$,
(5) $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$,
(6) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$,
(7) $\sqrt{\mathfrak{a}} = (1) \iff \mathfrak{a} = (1)$,
(8) *Wenn* $\mathfrak{p}$ *ein Primideal ist, dann gilt* $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ *für alle* $n \geq 1$.

Beweis. Bei (1), (2) und (3) muß man nur die Definition ausschreiben. Dann ist das klar.

Aus (3) folgt $\sqrt{\mathfrak{a}} \subseteq \sqrt{\sqrt{\mathfrak{a}}}$. Sei also $f \in \sqrt{\sqrt{\mathfrak{a}}}$. Dann gibt es $n \geq 0$ mit $f^n \in \sqrt{\mathfrak{a}}$. Also gibt es ein $m \geq 0$ mit $(f^n)^m \in \mathfrak{a}$. Daher ist $f^{nm} \in \mathfrak{a}$ und so $f \in \sqrt{\mathfrak{a}}$. Das zeigt (4).

Aus (3) folgt $\sqrt{\mathfrak{ab}} \subseteq \sqrt{\mathfrak{a}\cap\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}}\cap\sqrt{\mathfrak{b}}$. Sei also $f \in \sqrt{\mathfrak{a}}\cap\sqrt{\mathfrak{b}}$. Dann gibt es $n \geq 0$ mit $f^n \in \mathfrak{a}$ und $m \geq 0$ mit $f^m \in \mathfrak{b}$. Daraus folgt $f^{n+m} \in \mathfrak{ab}$. Dies zeigt

$$\sqrt{\mathfrak{a}}\cap\sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{ab}}$$

und (5) folgt.

Aus (3) folgt: $\sqrt{\mathfrak{a}}$ und $\sqrt{\mathfrak{b}}$ sind in $\sqrt{\mathfrak{a}+\mathfrak{b}}$ enthalten, also $\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}+\mathfrak{b}}$ und dann wieder mit (3) und (4)

$$\sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}} \subseteq \sqrt{\sqrt{\mathfrak{a}+\mathfrak{b}}} = \sqrt{\mathfrak{a}+\mathfrak{b}}.$$

Andererseits ist $\mathfrak{a}+\mathfrak{b} \subseteq \sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}$ und wieder (3) zeigt die andere Inklusion, somit (6).

(7) $\sqrt{\mathfrak{a}} = (1) \iff$ es gibt $n \geq 0$ mit $1^n \in \mathfrak{a} \iff 1 \in \mathfrak{a} \iff \mathfrak{a} = (1)$.

(8) Nach Definition und (3) gilt $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}^n} \subseteq \sqrt{\mathfrak{p}}$. Sei daher $f \in \sqrt{\mathfrak{p}}$. Dann gibt es $m \geq 1$ mit $f^m \in \mathfrak{p}$. Weil $\mathfrak{p}$ prim ist, muß einer der Faktoren von f^m bereits in $\mathfrak{p}$ liegen. Alle Faktoren sind gleich, also $f \in \mathfrak{p}$ und das zeigt (8). □

Beispiel 3.34. Im Allgemeinen gilt

$$\sqrt{\mathfrak{a}+\mathfrak{b}} \neq \sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}.$$

Hier ist ein Beispiel. Sei k ein Körper. Im Polynomring $k[X,Y]$ sind die Ideale $\mathfrak{a}_f = (Y - f(X))$ Primideale, denn das ist offensichtlich der Kern von

$$k[X,Y] \to k[X]$$

definiert durch $X \mapsto X$ und $Y \mapsto f(X)$. Details wie in Beispiel 3.7, nur einfacher. Speziell sind

$$\mathfrak{p} = (Y - X^2) \text{ und } \mathfrak{q} = (Y - X^2 + X^3)$$

Primideale. Damit ist

$$\mathfrak{a} := \sqrt{\mathfrak{p}} + \sqrt{\mathfrak{q}} = \mathfrak{p} + \mathfrak{q} = (Y - X^2, Y - X^2 + X^3) = (Y - X^2, X^3)$$

und

$$k[X,Y]/\mathfrak{a} = k[X,Y]/(Y - X^2, X^3) = k[X]/X^3$$

ein k-Vektorraum der Dimension 3.

Andererseits ist $\mathfrak{p} + \mathfrak{q} = (Y - X^2, X^3)$ und daher $X \in \sqrt{\mathfrak{p}+\mathfrak{q}}$, woraus

$$\mathfrak{b} := \sqrt{\mathfrak{p}+\mathfrak{q}} = (X, Y)$$

folgt. Dann ist aber $k[X,Y]/\mathfrak{b} = k$ ein k-Vektorraum von Dimension 1. (Warum darf man mit der k-Dimension argumentieren? Weil alles k-Algebren sind und die k-Vektorraumstruktur damit vorgegeben.) Es folgt $\mathfrak{a} \neq \mathfrak{b}$ wie gewünscht.

Definition 3.35. Ein Primideal $\mathfrak{p}$, das ein Ideal $\mathfrak{a}$ enthält, heißt **Primoberideal** von $\mathfrak{a}$.

Aus dem zweiten Isomorphiesatz folgt

$$(R/\mathfrak{a})/(\mathfrak{p}/\mathfrak{a}) = R/\mathfrak{p},$$

somit ist ein Ideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$ genau dann ein Primideal, wenn das Bild $\mathfrak{p}/\mathfrak{a}$ in $R/\mathfrak{a}$ ein Primideal ist.

Korollar 3.36. *Es gilt*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a}\subseteq\mathfrak{p}} \mathfrak{p},$$

wobei der Schnitt über alle Primoberideale von $\mathfrak{a}$ *zu nehmen ist.*

Beweis. Nach eben Gesagtem müssen wir über die Urbilder der Primideale in $R/\mathfrak{a}$ schneiden. Da alles $\mathfrak{a}$ enthält, ändert sich der Schnitt nicht, wenn wir zuerst nach $R/\mathfrak{a}$ gehen, dort schneiden und dann wieder das Urbild in R nehmen. Dann folgt alles aus dem entsprechenden Satz für $R/\mathfrak{a}$ und das Ideal (0). Das ist Satz 3.22. □

Definition 3.37. Ein **Radikalideal** ist ein Ideal $\mathfrak{a}$ in einem Ring R, das mit seinem Radikal übereinstimmt: $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Bemerkung 3.38. Aus Proposition 3.33 folgt sofort, daß der Quotient $R/\mathfrak{a}$ genau dann reduziert ist, wenn $\sqrt{\mathfrak{a}} = \mathfrak{a}$ ein Radikalideal ist.

Übungsaufgaben zu §3

Übungsaufgabe 3.1. Sei $R \neq 0$. Zeigen Sie die Existenz bezüglich Inklusion minimaler Primideale in R.

Übungsaufgabe 3.2. Sei k ein Körper. Bestimmen Sie Nilradikal und Jacobsonradikal der folgenden Ringe.

(1) $\mathbb{Z}$,
(2) $k[X]$,
(3) ein Hauptidealring mit unendlich vielen maximalen Idealen,
(4) $\mathbb{Z}/p^n\mathbb{Z}$ für eine Primzahl p, oder allgemeiner $\mathbb{Z}/n\mathbb{Z}$,
(5) $k[X,Y]/(X^2 - Y^2, Y^3)$.

4. Moduln

4.1. **Moduln und Homomorphismen.** Wenn man die Theorie der Ringe als eine nichtlineare Theorie betrachten will, dann muß man die Theorie der zugehörigen Moduln als eine Linearisierung ansehen.

Definition 4.1. Ein **Modul**, genau ein R-Modul zu einem Ring R, ist eine abelsche Gruppe M zusammen mit einer Multiplikation

$$R \times M \to M,$$

so daß für alle $a, b \in R$ und $x, y \in M$ gilt:

$$\begin{aligned} a(x+y) &= ax + ay \\ (a+b)x &= ax + bx \\ (ab)x &= a(bx) \\ 1x &= x. \end{aligned}$$

Ein **Untermodul**, genauer ein **R-Untermodul** eines R-Moduls M, ist eine Untergruppe $M' \subseteq M$, so daß für alle $a \in R$ und $x \in M'$ wieder $ax \in M'$.

Beispiel 4.2. Beispiele für Moduln in bekanntem Kontext.

(1) Ist R ein Körper k, so entspricht ein R-Modul einem k-Vektorraum.
(2) Abelsche Gruppen sind nichts anderes als $\mathbb{Z}$-Moduln.
(3) Sei $R = k[X]$. Dann ist ein R-Modul M erst mal ein k-Vektorraum über die Wirkung der konstanten Polynome. Sodann gibt es einen Endomorphismus $\varphi : M \to M$, der zur Multiplikation mit X gehört. Da X und die Konstanten k kommutieren, muß φ eine k-lineare Abbildung sein. Ein Polynom $P(X) \in k[X]$ operiert dann durch $P(\varphi)$ auf M. Ein $k[X]$-Modul ist somit nichts anderes als ein Vektorraum zusammen mit einem Endomorphismus.

Beispiel 4.3. Beispiele für Untermoduln.

(1) Der Ring R selbst ist ein R-Modul vermöge der Ringmultiplikation. Die Untermoduln von R sind nichts anderes als die Ideale von R.
(2) Jeder Modul M enthält die beiden trivialen Untermoduln $0 = \{0\} \subseteq M$ und $M \subseteq M$.

Beispiel 4.4. Sei $M' \subseteq M$ ein Untermodul des R-Moduls M. Dann ist die Faktorgruppe $M'' = M/M'$ auf eindeutige Art und Weise ein R-Modul derart, daß die Quotientenabbildung $M \to M''$ ein R-Modulhomomorphismus ist. Das ist das übliche Verfahren: zu $x \in M$ und $a \in R$ definieren wir die Modulmultiplikation einfach auf Repräsentanten als

$$a(x + M') = ax + M' \in M''.$$

Weil M' ein Untermodul ist, folgt die Wohldefiniertheit dieser R-Modulmultiplikation. Übung!

Definition 4.5. Ein R-**Modulhomomorphismus** von einem R-Modul M in einen R-Modul N ist eine Abbildung $f : M \to N$, die ein R-linearer (für $a \in R$ und $x \in M$ gilt $\varphi(ax) = a\varphi(x)$) Gruppenhomomorphismus ist (für alle $x, y \in M$ gilt $\varphi(x + y) = \varphi(x) + \varphi(y)$).

Die Menge aller R-Modulhomomorphismen $M \to N$ bezeichnen wir mit

$$\mathrm{Hom}_R(M, N)$$

oder auch nur mit $\mathrm{Hom}(M, N)$, wenn der Ring R sich aus dem Kontext erschließt.

Wie üblich ist ein R-**Modulisomorphismus** (oder **Isomorphismus von** R-**Moduln**) ein bijektiver R-Modulhomomorphismus (oder äquivalent ein solcher mit einem inversen R-Modulhomomorphismus).

Beispiel 4.6. In den Fällen von Beispiel 4.2 sind Modulhomomorphismen bekannt: für Körper sind es lineare Abbildungen, für $R = \mathbb{Z}$ sind es Gruppenhomomorphismen und für $k[X]$ sind es k-lineare Abbildungen, die mit dem gegebenen Endomorphismus vertauschen. So ist ein Untermodul von V mit $\varphi : V \to V$ nichts anderes als ein φ-stabiler Unterraum.

Beispiel 4.7. Das n-fache Produkt $M = R^n$ ist ein R-Modul durch komponentenweise Addition und diagonale skalare Multiplikation: für $a \in R$ und $(x_1, \ldots, x_n) \in R^n$ gilt

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n).$$

Dieser Modul wird **freier Modul vom Rang** n genannt. Wir sehen später, daß der Rang wohldefiniert ist, also aus $R^n \simeq R^m$ schon $n = m$ folgt. (Das gilt nicht in jedem Fall für Moduln über nichtkommutativen Ringen.)

Der Modul R^n zusammen mit den Elementen $e_i = (0, \ldots, 1, \ldots, 0)$ für $i = 1, \ldots, n$ mit einer 1 genau an der i-ten Stelle ist universell für diese Daten. Genauer, zu jedem R-Modul M und Elementen $x_1, \ldots, x_n$ gehört genau ein R-Modulhomomorphismus $\xi : R^n \to M$ mit $\xi(e_i) = x_i$ für $i = 1, \ldots, n$. Das ist nichts anderes als die Abbildung

$$\varphi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i x_i,$$

von der man sofort nachrechnet, daß sie ein R-Modulhomomorphismus ist und dadurch eindeutig festgelegt ist. Wir haben also eine Bijektion

$$\mathrm{Hom}_R(R^n, M) = M^n$$

durch $\varphi \mapsto (\varphi(e_1), \ldots, \varphi(e_n))$.

Definition 4.8. Sei $X \subseteq M$ eine Teilmenge eines R-Moduls M. Dann ist der **von** X **erzeugte Untermodul** $\langle X \rangle_R \subseteq M$ der kleinste R-Untermodul von M, der X enthält. Dieser wird offensichtlich durch

$$\langle X \rangle_R = \{ \sum_{i=1}^{r} a_i x_i \ ; \ a_i \in R \text{ und } x_i \in X \}$$

gegeben.

Wenn $\langle X \rangle_R = M$, so nennt man X eine Menge von **Erzeugern** von M als R-Modul. Ein **endlich erzeugter** R-**Modul** ist eine R-Modul M, der von endlich vielen Elementen erzeugt werden kann.

Bemerkung 4.9. Sei M ein R-Modul und gehöre $f : R^n \to M$ zu den Elementen $x_1, \ldots, x_n \in M$. Dann ist f surjektiv genau dann, wenn die $x_1, \ldots, x_n$ Erzeuger von M sind. Somit ist M endlich erzeugt genau dann, wenn es ein n und einen surjektiven R-Modulhomomorphismus $R^n \twoheadrightarrow M$ gibt.

Beispiel 4.10. Sei k ein Körper.

(1) Sei $R = k[X, Y]$. Das Ideal $(X, Y) \subseteq R$ ist von 2 Elementen erzeugt und kann auch nicht mit weniger als 2 Elementen erzeugt werden, obwohl $M = (X, Y)$ ein Untermodul im freien Modul vom Rang 1 ist. Moduln verhalten sich im Allgemeinen anders als Vektorräume.

Dies sieht man wie folgt. Der Untermodul $M' = (X^2, XY, Y^2) \subseteq M$ führt zu einem Quotienten $M \to V = M/M'$, der als k-Vektorraum von den Bildern von X und Y erzeugt wird. Wäre M von weniger als 2 Elementen als R-Modul erzeugbar, so auch V. Aber $P \in R$ wirkt auf V via der Auswertung bei $X = 0$ und $Y = 0$, also durch $P(0, 0) \in k$. Somit ist das R-Modulerzeugnis von Elementen in V nichts anderes als das k-Vektorraumerzeugnis. Wegen $\dim_k(V) = 2$ braucht man mindestens 2 Erzeuger.

(2) Sei $R = k[X]$. Der Modul R wird von 1 erzeugt, aber auch von X und $1 - X$:

$$R = (1) = (X, 1 - X).$$

Auch das längere Erzeugersystem ist nicht redundant: kein Erzeuger kann weggelassen werden. Somit ist selbst bei freien Moduln nicht in jedem Erzeugersystem eine Basis enthalten.

Definition 4.11. Das **Annullatorideal** (oder kurz der **Annullator**) eines R-Moduls M ist das Ideal

$$\mathrm{Ann}_R(M) = \{f \in R \,;\; fM = (0)\}$$

von R. (Ist wirklich Ideal: triviale Übung.)

Beispiel 4.12. Wir berechnen ein paar Annullatoren.

(1) $\mathrm{Ann}_R(R/\mathfrak{a}) = \mathfrak{a}$
(2) $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Q}) = (0)$
(3) $\mathrm{Ann}_{k[X]}\big(\bigoplus_{i\geq 1} k[X]/(X^i)\big) = (0)$.

Proposition 4.13. *Sei R ein Ring und $\mathfrak{a}$ ein Ideal in R. Dann sind Moduln M mit $\mathfrak{a} \subseteq \mathrm{Ann}_R(M)$ nichts anderes als $R/\mathfrak{a}$-Moduln. Das gilt inklusive Homomorphismen: sind M und N solche R-Moduln, dann gilt*

$$\mathrm{Hom}_R(M, N) = \mathrm{Hom}_{R/\mathfrak{a}}(M, N).$$

Beweis. Definiert $R/\mathfrak{a} \times M \to M$ eine $R/\mathfrak{a}$-Modulstruktur auf M, so definiert $ax := (a + \mathfrak{a})x$ für $a \in R$ und $x \in M$ eine R-Modulstruktur auf M mit $\mathfrak{a} \subseteq \mathrm{Ann}_R(M)$.

Umgekehrt, wenn M ein R-Modul ist mit $\mathfrak{a} \subseteq \mathrm{Ann}_R(M)$, dann faktorisiert die Modulmultiplikation $R \times M \to M$ zu einer Modulmultiplikation $R/\mathfrak{a} \times M \to M$. Diese beiden Konstruktionen sind offensichtlich zueinander invers.

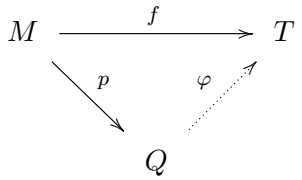
Die Aussage zu Modulhomomorphismen ist trivial. □

4.2. **Quotienten und Isomorphiesätze.** Für Moduln gelten Homomorphiesatz und Isomorphiesätze wie für Gruppen. Auch hier folgen sie formal aus der Existenz von Quotienten.

Proposition 4.14. *Sei R ein Ring, M ein R-Modul und M' ein Untermodul von M. Dann gibt es einen **Quotientenmodul** $p : M \to Q$ mit der universellen Eigenschaft:*

(i) $p(M') = 0$,

(ii) *für alle R-Moduln T und R-Modulhomomorphismen $f : M \to T$ mit $f(M') = 0$ faktorisiert f eindeutig durch einen R-Modulhomomorphismus $\varphi : Q \to T$, d.h. $f = \varphi \circ p$ bzw. das Diagramm*



kommutiert.

Beweis. Wir zeigen zuerst die Eindeutigkeit bis auf eindeutigen Isomorphismus. Angenommen $p' : M \to Q'$ ist auch ein Quotientenmodul. Dann gilt $p'(M') = 0$ und somit gibt es eindeutig $\varphi : Q \to Q'$ mit $p' = \varphi \circ p$. Umgekehrt können wir genauso argumentieren und erhalten $\psi : Q' \to Q$ mit $p = \psi \circ p'$. Die Komposition $\psi \circ \varphi : Q \to Q$ erfüllt dann die geforderte Faktorisierungseigenschaft für $p : M \to Q$ bezüglich p. Da dies auch die Identität $\mathrm{id}_Q : Q \to Q$ erfüllt, folgt aus der Eindeutigkeit der Faktorisierung bereits $\psi \circ \varphi = \mathrm{id}_Q$. Umgekehrt schließt man genauso auf $\varphi \circ \psi = \mathrm{id}_{Q'}$, so daß φ und ψ zueinander inverse R-Modulhomomorphismen sind. Außerdem sind diese eindeutig, wenn man Verträglichkeit mit den Quotientenabbildungen fordert. Das war rein formal!

Zur Existenz eines Quotientenmoduls überlegen wir uns nur, daß die Projektion $p : M \to Q := M/M'$ ein Quotient ist. Das ist einfach: (1) Die Bedingung $p(M') = 0$ folgt aus der Konstruktion sofort, und ein $f : M \to T$ mit $f(M') = 0$ läßt die Definition von $\varphi : Q \to T$ mittels

$$\varphi(x + M') := f(x)$$

zu. Dies ist wohldefiniert, da $f(M') = 0$. Weiter ist φ ein R-Modulhomomorphismus, wie man leicht durch Wahl geeigneter Vertreter und der Homomorphie von f nachrechnet. Die Faktorisierungseigenschaft folgt sofort aus der Definition und ist gewissermaßen die Leitidee für die Definition. Auch die Eindeutigkeit ist offensichtlich. □

Bemerkung 4.15. Wir nutzen die Notation von Proposition 4.14. Die funktionale Eigenschaft des Quotienten beinhaltet nicht die Forderung, daß die Quotientenabbildung $M \to Q$ surjektiv ist. Dies folgt erst aus der Konstruktion als Faktormodul und wegen der Eindeutigkeit dann allgemein.

Beispiel 4.16. Sei $f : M \to N$ ein R-Modulhomomorphismus.

(1) Der **Kern** von f ist der Untermodul $\ker(f) = f^{-1}(0) = \{x \in M \,;\, f(x) = 0\}$ von M. Im Gegensatz zu allgemeinen Gruppen, wo nur ausgezeichnete Untergruppen, nämlich Normalteiler, Kerne sind, gibt es diese Unterscheidung bei Moduln nicht: Kerne sind Untermoduln und jeder Untermodul $M' \subseteq M$ ist der Kern eines geeigneten R-Modulhomomorphismus, etwa der Quotientenabbildung $M \to M/M'$.

(2) Das **Bild** von f ist der Untermodul $\mathrm{im}(f) = f(M)$ von N.

Satz 4.17 (Homomorphiesatz)**.** *Sei $f : M \to N$ ein R-Modulhomomorphismus. Dann definiert*

$$\begin{aligned} \varphi : M/\ker(f) &\to \mathrm{im}(f) \\ x + \ker(f) &\mapsto f(x) \end{aligned}$$

einen Isomorphismus von R-Moduln.

Beweis. Die Quotienteneigenschaft von $M \to M/\ker(f)$ nach Proposition 4.14 führt bezüglich $f : M \to N$ zu einem R-Modulhomomorphismus $M/\ker(f) \to N$, dessen Bild weiter $f(M)$ ist. Schränken wir das Ziel auf $\mathrm{im}(f)$ ein, so erhalten wir den behaupteten R-Modulhomomorphismus φ. Dieser ist offensichtlich surjektiv. Sei x ein Vertreter im Urbild von $\bar{x} \in M/\ker(f)$. Dann ist

$\varphi(\bar{x}) = 0$ genau dann, wenn $x \in \ker(f)$, also wenn $\bar{x} = 0$. Damit ist φ auch injektiv. Als bijektiver R-Modulhomomorphismus ist φ ein Isomorphismus. □

Bemerkung 4.18. Sei M ein R-Modul und seien M_1' und M_2' Untermoduln von M.

(1) Schnitt $M_1' \cap M_2'$, und
(2) Summe $M_1' + M_2' = \{x_1 + x_2 \ ; \ x_i \in M_i' \text{ für } i = 1, 2\}$

sind ebenfalls R-Untermoduln von M. Schnitt und Summe lassen sich auch für beliebige Familien von Untermoduln $M_i' \subseteq M$ mit $i \in I$ definieren.

Korollar 4.19 (Erster Isomorphiesatz)**.** *Sei M ein R-Modul mit Untermoduln $K, L \subseteq M$. Dann induziert die Identität einen R-Modulisomorphismus*

$$K/K \cap L \xrightarrow{\sim} K + L/L$$

Beweis. Das ist der Homomorphiesatz für Moduln angewandt auf $K \to M \to M/L$. □

Korollar 4.20 (Zweiter Isomorphiesatz)**.** *Sei M ein R-Modul mit Untermoduln $K \subseteq L \subseteq M$. Dann induziert die Identität einen R-Modulisomorphismus*

$$(M/K)/(L/K) \xrightarrow{\sim} M/L.$$

Beweis. Die Quotienteneigenschaft von $M \to M/K$ nach Proposition 4.14 führt bezüglich $M \to M/L$ zu einem R-Modulhomomorphismus $M/K \to M/L$. Der behauptete Isomorphismus folgt aus dem Homomorphiesatz angewandt auf $M/K \to M/L$. □

4.3. **Produkte und Summen von Moduln.** Wir diskutieren nun Produkte und Summen für Moduln.

Definition 4.21. Sei R ein Ring. Das **direkte Produkt** einer Familie von R-Moduln M_i für $i \in I$ ist der R-Modul

$$\prod_{i \in I} M_i = \{(x_i)_{i \in I} \ ; \ x_i \in M_i \text{ für alle } i \in I\}$$

mit komponentenweiser Addition und R-Multiplikation. Für jedes $j \in I$ ist die Projektion

$$\mathrm{pr}_j : \prod_{i \in I} M_i \to M_j$$

mit $\mathrm{pr}_j((x_i)) = x_j$ ein R-Modulhomomorphismus. Allgemeiner ist auch für eine Teilmenge $J \subseteq I$ die Projektion

$$\mathrm{pr}_J : \prod_{i \in I} M_i \to \prod_{j \in J} M_j$$

mit $\mathrm{pr}_J((x_i)_{i \in I}) = (x_j)_{j \in J}$ ein R-Modulhomomorphismus.

Das Produkt zweier Moduln M und N schreiben wir als $M \times N$.

Satz 4.22 (Existenz von Produkten bei Moduln)**.** *Sei R ein Ring. Das direkte Produkt von R-Moduln M_i mit $i \in I$ zusammen mit den Projektionen $\mathrm{pr}_j : \prod_{i \in I} M_i \to M_j$ erfüllt die universelle Eigenschaft des **Produkts** von R-Moduln:*

Zu jedem R-Modul T und R-Modulhomomorphismen $f_i : T \to M_i$ für alle $i \in I$ gibt es genau einen R-Modulhomomorphismus $f : T \to \prod_{i \in I} M_i$ mit $f_i = \mathrm{pr}_i \circ f$ für alle $i \in I$.

Beweis. Übung. Wie bei Ringen. □

Definition 4.23. Sei R ein Ring. Die **direkte Summe** einer Familie von R-Moduln M_i für $i \in I$ ist der R-Modul

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \ ; \ x_i \in M_i \text{ für alle } i \in I \text{ und } x_i = 0 \text{ für fast alle } i\}$$

mit komponentenweiser Addition und R-Multiplikation. Für jedes $j \in I$ ist die Inklusion

$$\iota_j : M_j \to \bigoplus_{i \in I} M_i$$

mit $\iota_j(x) = (0, \ldots, x, \ldots, 0)$, wobei x in der j-ten Koordinate sitzt, ein R-Modulhomomorphismus. Allgemeiner ist auch für eine Teilmenge $J \subseteq I$ die Inklusion

$$\iota_J : \bigoplus_{j \in J} M_j \to \bigoplus_{i \in I} M_i$$

mit der naheliegenden Definition der Fortsetzung eines Tupels durch 0 auf $I \setminus J$ ein R-Modulhomomorphismus.

Die direkte Summe von zwei R-Moduln M und N schreibt man auch $M \oplus N$.

Satz 4.24 (Existenz von Summen bei Moduln)**.** *Sei R ein Ring. Die direkte Summe von R-Moduln M_i mit $i \in I$ zusammen mit den Inklusionen $\iota_j : M_j \to \bigoplus_{i \in I} M_i$ erfüllt die universelle Eigenschaft der **Summe** von R-Moduln:*

Zu jedem R-Modul T und R-Modulhomomorphismen $f_i : M_i \to T$ für alle $i \in I$ gibt es genau einen R-Modulhomomorphismus $f : \bigoplus_{i \in I} M_i \to T$ mit $f_i = f \circ \iota_i$ für alle $i \in I$.

Beweis. Übung: $f((x_i)_{i \in I}) = \sum_i f_i(x_i)$ definert f, denn die Summe ist endlich. □

Beispiel 4.25. Seien R ein Ring und X eine Menge. Die direkte Summe der R-Moduln $M_x = R$ für alle $x \in X$ bezeichne ich gerne mit

$$R^{(X)} := \bigoplus_{x \in X} R \cdot x$$

und identifiziere $1 \cdot x$ mit x. Dadurch wird $X \subseteq R^{(X)}$ eine Teilmenge und $R^{(X)}$ besteht genau aus allen R-Linearkombinationen der Elemente von X. Damit ist X offenbar ein Erzeugendensystem von $R^{(X)}$ als R-Modul und genau hat jedes $y \in R^{(X)}$ eine eindeutige Darstellung

$$y = \sum_{x \in X} a_x \cdot x$$

mit $a_x \in R$ und fast alle $= 0$.

Definition 4.26. Ein **freier R-Modul** ist ein R-Modul M, der für eine Menge X isomorph zu $R^{(X)}$ ist. Das Bild von $X \subseteq R^{(X)}$ unter dem Isomorphismus in M heißt **Basis** (oder **R-Basis**) von M.

Bemerkung 4.27. (1) Offenbar hat in einem freien Modul jedes Element eine eindeutige Darstellung als R-Linearkombination bezüglich einer Basis.

(2) Natürlich kann ein freier Modul auf mehrere Arten isomorph zu einem $R^{(X)}$ sein und dementsprechend verschiedene Basen haben.

(3) Als Beispiel haben wir bereits R^n gesehen, das frei auf der Menge der $\{1, \ldots, n\}$ ist mit Basis gegeben durch die Elemente e_i für $i = 1, \ldots, n$.

(4) Die universelle Eigenschaft der direkten Summe nach Proposition 4.24 führt sofort zu folgender universeller Eigenschaft für freie Moduln bezüglich einer Basis, also ohne Einschränkung für $R^{(X)}$: für jeden R-Modul M gilt

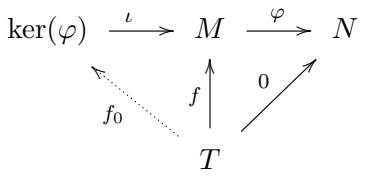
$$\mathrm{Hom}_R(R^{(X)}, M) = \mathrm{Abb}(X, M)$$

via $(\varphi : R^{(X)} \to M) \mapsto (\varphi|_X : X \to M)$.

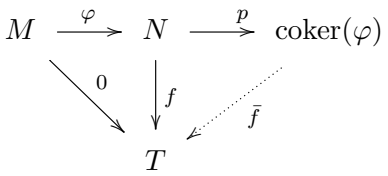
4.4. **Kerne, Kokerne und Hom.**

Definition 4.28. Sei $\varphi : M \to N$ ein R-Modulhomomorphismus.

(1) Ein **Kern** von φ ist ein R-Modulhomomorphismus $\iota : \ker(\varphi) \to M$, so daß:
   (i) $\varphi \circ \iota = 0$
   (ii) für alle R-Modulhomomorphismen $f : T \to M$ mit $\varphi \circ f = 0$ gibt es eine eindeutige Faktorisierung $f_0 : T \to \ker(\varphi)$, also mit $\iota \circ f_0 = f$.



(2) Ein **Kokern** von φ ist ein R-Modulhomomorphismus $p : N \to \operatorname{coker}(\varphi)$, so daß:
   (i) $p \circ \varphi = 0$
   (ii) für alle R-Modulhomomorphismen $f : N \to T$ mit $f \circ \varphi = 0$ gibt es eine eindeutige Faktorisierung $\bar{f} : \operatorname{coker}(\varphi) \to T$, also mit $\bar{f} \circ p = f$.



Lemma 4.29. *Kerne und Kokerne von Modulhomomorphismen sind eindeutig bis auf eindeutige Isomorphie.*

Beweis. Die Eindeutigkeitsaussage wird mit den üblichen Argumenten bewiesen. Übung! □

Satz 4.30. *Kerne und Kokerne von Modulhomomorphismen existieren.*

Beweis. Zu $f : M \to N$ ist der Kern gegeben durch die Inklusion $\ker(f) \hookrightarrow M$, und der Kokern durch $p : N \to N/f(M)$. Die universelle Eigenschaft des Kerns ist trivial. Diejenige des Kokerns folgt, weil die Projektion auf den Faktormodul eine Quotientenabbildung ist. □

Beispiel 4.31. Sei R ein Ring und seien M, N zwei R-Moduln. Die Menge

$$\operatorname{Hom}_R(M, N)$$

ist natürlich ein R-Modul durch Addition

$$(f + g)(x) = f(x) + g(x)$$

und Multiplikation mit $a \in R$

$$(af)(x) = af(x).$$

Man überzeugt sich sofort, daß für alle $f, g \in \operatorname{Hom}_R(M, N)$ und alle $a \in R$ die so definierten Abbildungen $f + g$ und af wieder R-Modulhomomorphismen sind.

Seien $\varphi : M_1 \to M_2$ und $\psi : N_1 \to N_2$ Homomorphismen von R-Moduln. Dann liefert Komposition Abbildungen

$$\psi\circ : \operatorname{Hom}_R(M, N_1) \to \operatorname{Hom}_R(M, N_2)$$
$$\circ\varphi : \operatorname{Hom}_R(M_2, N) \to \operatorname{Hom}_R(M_1, N),$$

die offensichtlich R-Modulhomomorphismen sind.

Der Kern von $\psi\circ$ ist mit $\iota : \ker(\psi) \to N_1$ gegeben durch

$$\iota\circ : \operatorname{Hom}_R(M, \ker(\psi)) \to \operatorname{Hom}_R(M, N_1).$$

Der Kern von $\circ\varphi$ ist mit $p : M_2 \to \operatorname{coker}(\varphi)$ gegeben durch

$$\circ p : \operatorname{Hom}_R(\operatorname{coker}(\varphi), N) \to \operatorname{Hom}_R(M_2, N).$$

Das sieht auf den ersten Blick kompliziert aus, stellt sich aber verbalisiert als nichts anderes dar als die Definition von Kern und Kokern!

Beispiel 4.32. Sei M ein R-Modul und $n \in \mathbb{N}$. Die natürliche Bijektion

$$\operatorname{Hom}_R(R^n, M) = M^n$$

durch Auswerten in der Standardbasis von R^n ist ein Isomorphismus von R-Moduln.

Sei speziell $M = R^m$ für ein $m \in \mathbb{N}$. Dann ist

$$\operatorname{Hom}_R(R^n, R^m) = (R^m)^n = \mathrm{M}_{m\times n}(R)$$

wie in linearer Algebra durch den freien R-Modul der Matrizen gegeben. Zur Matrix A gehört die R-lineare Abbildung $x \mapsto Ax$ der Matrizenmultiplikation von Spalten mit Einträgen aus R mit der Matrix A.

Beispiel 4.33. Sei R ein Ring und sei M ein R-Modul. Das **Transporterideal** für zwei Untermoduln $N_1, N_2 \subseteq M$ ist das Ideal

$$(N_1 : N_2) = \{f \in R \,;\; fN_2 \subseteq N_1\} \subseteq R.$$

Anders ausgedrückt ist $(N_1 : N_2)$ der Kern der Abbildung

$$\begin{aligned} R &\to \operatorname{Hom}_R(N_2, M/N_1) \\ f &\mapsto \big(x \mapsto fx + N_1\big), \end{aligned}$$

oder aber $(N_1 : N_2) = \operatorname{Ann}_R(N_1 + N_2/N_1)$.

Beispiel 4.34. Seien $f_i : M_i \to N$ zwei R-Modulhomomorphismen. Das Faserprodukt $M_1 \times_N M_2$ ist ein R-Modul zusammen mit Projektionen $\mathrm{pr}_i : M_1 \times_N M_2 \to M_i$ für $i = 1, 2$ so daß

(i) $f_1 \circ \mathrm{pr}_1 = f_2 \circ \mathrm{pr}_2$, und

(ii) für alle R-Moduln T und R-Modulhomomorphismen $\varphi_i : T \to M_i$ für $i = 1, 2$, gibt es einen eindeutigen R-Modulhomomorphismus $\varphi : T \to M_1 \times_N M_2$, so daß $\varphi_i = \mathrm{pr}_i \circ \varphi$ für $i = 1, 2$.

Das übliche Argument zeigt, daß ein Faserprodukt, wenn es existiert eindeutig ist bis auf eindeutigen Isomorphismus. Die Existenz des Faserprodukts folgt aus der Konstruktion als

$$M_1 \times_N M_2 = \{(x_1, x_2) \in M_1 \times M_2 \,;\; f_1(x_1) = f_2(x_2)\}$$

als Untermodul des Produkts $M_1 \times M_2$. Die benötigten Projektionen bekommt man als Einschränkung der Projektionen $\mathrm{pr}_i : M_1 \times M_2 \to M_i$. Alternativ kann man das Faserprodukt auch als **Differenzkern** konstruieren:

$$M_1 \times_N M_2 = \ker\big(f_1 - f_2 : M_1 \oplus M_2 \to N\big).$$

4.5. **Das Tensorprodukt von Moduln.** Multilineare Algebra verlangt nach dem Tensorprodukt.

Definition 4.35. Sei R ein Ring.

(1) Eine R-**bilineare** Abbildung von zwei R-Moduln M und N in einen R-Modul T ist eine Abbildung

$$f : M \times N \to T,$$

so daß für alle $x \in M$ und alle $y \in N$ die Abbildungen

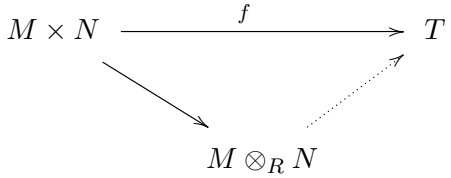
$$\begin{aligned} f_x : N &\to T \\ z &\mapsto f(x, z) \end{aligned}$$

und

$$\begin{aligned} f_y : M &\to T \\ z &\mapsto f(z, y) \end{aligned}$$

R-Modulhomomorphismen sind.

(2) Das **Tensorprodukt** der R-Moduln M und N ist ein R-Modul $M \otimes_R N$ zusammen mit einer R-bilinearen Abbildung $M \times N \to M \otimes_R N$ mit der folgenden universellen Eigenschaft:
für alle R-Moduln T und R-bilinearen Abbildungen $f : M \times N \to T$ gibt es genau eine R-lineare Abbildung $M \otimes_R N \to T$, so daß das folgende Diagramm kommutiert:



Satz 4.36. *Tensorprodukte von Moduln existieren und sind eindeutig bis auf eindeutigen Isomorphismus.*

Beweis. Die Eindeutigkeit folgt mit den üblichen Überlegungen aus der universellen Eigenschaft. Details dazu sind eine Übungsaufgabe.

Wir zeigen nun die Existenz durch eine *universelle* Konstruktion. Seien R-Moduln M und N gegeben und sei $F_{M\times N} = R^{(M\times N)}$ zunächst der freie R-Modul auf der Menge $M \times N$, zusammen mit einer Abbildung von Mengen

$$M \times N \to F_{M\times N},$$

deren Bild eine R-Basis von $F_{M\times N}$ ist. Sodann betrachten wir den Untermodul

$$R_{M\times N} \subseteq F_{M\times N}$$

der R-bilinearen Relationen, der von den folgenden Elementen in $F_{M\times N}$ als R-Modul erzeugt wird:

$$\begin{aligned} &a(x, y) - (ax, y), \\ &a(x, y) - (x, ay), \\ &(x_1 + x_2, y) - (x_1, y) - (x_2, y), \\ &(x, y_1 + y_2) - (x, y_1) - (x, y_2), \end{aligned}$$

für alle $a \in R$ und $x, x_1, x_2 \in M$ und $y, y_1, y_2 \in N$. Dann setzen wir

$$M \otimes_R N := F_{M\times N}/R_{M\times N}.$$

Die Restklasse von (x, y) bezeichnen wir mit $x \otimes y$. Die Konstruktion erzwingt die R-Bilinearität der Abbildung

$$\begin{aligned} M \times N &\to M \otimes_R N \\ (x, y) &\mapsto x \otimes y. \end{aligned}$$

Sei nun $f : M \times N \to T$ eine bilineare Abbildung von R-Moduln. Dann definiert die universelle Eigenschaft der freien Moduln einen R-Modulhomomorphismus

$$\begin{aligned} F : F_{M\times N} &\to T \\ (x, y) &\mapsto f(x, y) \end{aligned}$$

der, weil f bilinear ist, $F(R_{M\times N}) = 0$ erfüllt und daher wegen der universellen Eigenschaft des Quotienten zu einem R-Modulhomomorphismus

$$M \otimes_R N \to T$$

gehört. Dieser ist eindeutig, denn auf dem Erzeugendensystem der $x \otimes y$ für alle $(x, y) \in M \times N$ ist der Wert vorgegeben. □

Bemerkung 4.37. Als Bonus aus Konstruktion des Tensorprodukts erhalten wir die besonderen Elemente (atomare Tensoren) $x \otimes y \in M \otimes_R N$, von denen $M \otimes_R N$ erzeugt wird. Das ist nicht aus der universellen Eigenschaft klar.

Korollar 4.38. *Sind M und N endlich erzeugte R-Moduln, dann ist auch $M \otimes_R N$ ein endlich erzeugter R-Modul.*

Beweis. Das folgt aus der Konstruktion: wird M von $x_1, \ldots, x_m$ erzeugt und N von $y_1, \ldots, y_n$, dann erzeugen die $x_i \otimes y_j$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ das Tensorprodukt. □

Beispiel 4.39. (1) Das Tensorprodukt hat eine Eins: Es gilt für alle R-Moduln M natürlich

$$R \otimes_R M = M.$$

Die R-bilineare Abbildung $(a, x) \mapsto ax$ induziert einen R-Modulhomomorphismus, dessen Inverses durch $x \mapsto 1 \otimes x$ gegeben ist. Analog gilt natürlich auch $M = M \otimes_R R$.

(2) Das Tensorprodukt ist kommutativ: Für zwei R-Moduln M und N gilt natürlich

$$M \otimes_R N = N \otimes_R M.$$

Die R-bilineare Abbildung $(x, y) \mapsto y \otimes x$ induziert einen R-Modulhomomorphismus, dessen Inverses per Symmetrie auf die gleiche Art und Weise konstruiert wird.

(3) Das Tensorprodukt ist assoziativ: Für drei R-Moduln M, N und L gilt natürlich

$$(M \otimes_R N) \otimes_R L = M \otimes_R (N \otimes_R L).$$

Man sieht leicht, daß beide Seiten universell sind bezüglich R-multilinearer Abbildungen auf $M \times N \times L$.

Bemerkung 4.40. Das Tensorprodukt kann auch mit R-Modulhomomorphismen umgehen. Seien $\varphi : M_1 \to M_2$ und $\psi : N_1 \to N_2$ Homomorphismen von R-Moduln. Dann induziert die R-bilineare Abbildung $M_1 \times N_1 \to M_2 \otimes_R N_2$ gegeben durch

$$(x, y) \mapsto \varphi(x) \otimes \psi(y)$$

einen eindeutigen R-Modulhomomorphismus

$$\varphi \otimes \psi : M_1 \otimes_R N_1 \to M_2 \otimes_R N_2.$$

Hat man weiter R-Modulhomomorphismen $\varphi' : M_2 \to M_3$ und $\psi' : N_2 \to N_3$, dann gilt

$$(\varphi'\varphi) \otimes (\psi'\psi) = (\varphi' \otimes \psi') \circ (\varphi \otimes \psi) : M_1 \otimes_R N_1 \to M_3 \otimes_R N_3$$

unmittelbar aus der Definition.

Hat man hingegen einen R-Modulhomomorphismus $\vartheta : M_1 \to M_2$ und $a, b \in R$, dann gilt weiter

$$(a\varphi + b\vartheta) \otimes \psi = a(\varphi \otimes \psi) + b(\vartheta \otimes \psi) : M_1 \otimes_R N_1 \to M_2 \otimes_R N_2$$

und natürlich analog im zweiten Faktor.

Proposition 4.41 (Adjungiertheit von Hom und Tensor)**.** *Für R-Moduln M, N und L gibt es einen natürlichen Isomorphismus von R-Moduln*

$$\mathrm{Hom}_R(M \otimes_R N, L) = \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L)).$$

Beweis. Ein $\varphi : M \otimes_R N \to L$ gehört zu einer R-bilinearen Abbildung $M \times N \to L$, die man als Abbildung $M \to \mathrm{Hom}_R(N, L)$

$$x \mapsto \varphi_x = \big(y \mapsto \varphi(x \otimes y)\big)$$

mit $x \in M$ und $y \in N$ auffassen kann. R-linear in $y \in N$ führt dazu, daß φ_x auch R-linear ist. Und R-linear in $x \in M$ bedeutet, daß die Zuordnung $x \mapsto \varphi_x$ ein R-Modulhomomorphismus ist.

Hat man umgekehrt einen R-Modulhomomorphismus $\psi : M \to \mathrm{Hom}_R(N, L)$, so definiert

$$(x, y) \mapsto \psi(x)(y)$$

eine R-bilineare Abbildung $M \times N \to L$, somit einen R-Modulhomomorphismus $M \otimes_R N \to L$.

Die beiden Konstruktionen sind offensichtlich invers zueinander und auch R-linear. □

Proposition 4.42 (Tensorprodukt und Kokern)**.** *Sei $\varphi : M_1 \to M_2$ ein R-Modulhomomorphismus und N ein R-Modul. Dann gibt es einen natürlichen Isomorphismus*

$$\mathrm{coker}(\varphi \otimes \mathrm{id} : M_1 \otimes_R N \to M_2 \otimes_R N) = \mathrm{coker}(\varphi : M_1 \to M_2) \otimes_R N$$

von R-Moduln.

Beweis. Sei $p : M_2 \to \mathrm{coker}(\varphi)$ der Kokern im eigentlichen Sinn. Wir haben zu zeigen, daß

$$p \otimes \mathrm{id} : M_2 \otimes_R N \to \mathrm{coker}(\varphi) \otimes_R N$$

ein Kokern von $\varphi \otimes \mathrm{id}$ ist. Dazu gehört zunächst

$$(p \otimes \mathrm{id}) \circ (\varphi \otimes \mathrm{id}) = (p\varphi \otimes \mathrm{id}) = 0 \otimes \mathrm{id} = 0.$$

Sodann sei $f : M_2 \otimes_R N \to L$ gegeben mit $f(\varphi \otimes \mathrm{id}) = 0$. Zu f gehört nach Proposition 4.41 der R-Modulhomomorphismus

$$F : M_2 \to \mathrm{Hom}_R(N, L).$$

Die Voraussetzung $f(\varphi \otimes \mathrm{id}) = 0$ ist äquivalent zu $F\varphi = 0$. Nach der universellen Eigenschaft des Kokerns zu φ gibt es eine eindeutige Faktorisierug über p:

$$\bar{F} : \mathrm{coker}(\varphi) \to \mathrm{Hom}_R(N, L).$$

Wenden wir Proposition 4.41 diesmal in die andere Richtung an, so gehört zu $\bar{F}$ eindeutig ein R-Modulhomomorphismus

$$\bar{f} : \mathrm{coker}(\varphi) \otimes_R N \to L.$$

Per Konstruktion gilt

$$\bar{f}(\varphi \otimes \mathrm{id}) = f$$

und $\bar{f}$ ist auch eindeutig mit dieser Eigenschaft. Dies zeigt die Behauptung. □

Beispiel 4.43. Zu einem R-Modul M und einem Ideal $\mathfrak{a} \subseteq R$ können wir den Untermodul

$$\mathfrak{a}M = \Big\{ \sum_i a_i x_i \ ; \ a_i \in \mathfrak{a}, x_i \in M \Big\} \subseteq M$$

betrachten. Dies ist genau das Bild der Komposition

$$\mathfrak{a} \otimes_R M \to R \otimes_R M = M.$$

Nach Proposition 4.42 gilt dann

$$M \otimes_R R/\mathfrak{a} = M \otimes_R \mathrm{coker}(\mathfrak{a} \to R) = \mathrm{coker}(\mathfrak{a} \otimes_R M \to R \otimes_R M) = M/\mathfrak{a}M.$$

Proposition 4.44. *Sei R ein Ring, M und N_i für alle $i \in I$ seien R-Moduln. Dann gibt es einen natürlichen R-Modulhomomorphismus*

$$M \otimes_R \Big(\bigoplus_{i \in I} N_i\Big) = \bigoplus_{i \in I} M \otimes_R N_i.$$

Beweis. Das ist eine Übungsaufgabe. □

Bemerkung 4.45. Man sagt, das Tensorprodukt vertauscht mit direkten Summen. Im Fall einer endlichen Indexmenge I ist das direkte Produkt eine direkte Summe und vertauscht somit mit dem Tensorprodukt. Die zu Proposition 4.44 analoge Aussage mit direkten Produkten gilt aber im Allgemeinen nicht!

$$\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{n \in \mathbb{N}} \mathbb{Z} = \{(a_n) \in \prod_{n \in \mathbb{N}} \mathbb{Q} \ ; \ \text{ es gibt } N \in \mathbb{N}\colon Na_i \in \mathbb{Z} \text{ für alle } n\} \subsetneq \prod_{n \in \mathbb{N}} \mathbb{Q} = \prod_{n \in \mathbb{N}} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}$$

4.6. **Basiswechsel.** Sei $f : A \to B$ ein Ringhomomorphismus. Zu einem B-Modul N gehört der A-Modul

$$f_*N,$$

der als abelsche Gruppe mit N übereinstimmt und auf dem ein $a \in A$ durch $ay = f(a)y$ für alle $y \in N$ operiert. Wir vergessen quasi die Operation von B und merken uns nur die Operation von A via $f : A \to B$. Wenn $\varphi : M \to N$ ein B-Modulhomomorphismus ist, dann ist $\varphi : f_*M \to f_*N$ offensichtlich auch ein A-Modulhomomorphismus.

Beispiel 4.46. Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist B ein B-Modul über sich selbst und demnach B auch als f_*B ein A-Modul. Wir betrachten stets eine A-Algebra B als A-Modul in diesem Sinne.

Definition 4.47. Der **Basiswechsel** (oder die **Erweiterung der Skalare**) eines A-Moduls M entlang des Ringhomomorphismus $f : A \to B$ (oder von A nach B) ist der B-Modul

$$f^*M = M \otimes_A B$$

als B-Modul vermöge der B-Operation auf dem zweiten Faktor durch

$$b(x \otimes \beta) := x \otimes (b\beta).$$

Beweis. Diese Definition erfordert ein kurzes Nachdenken über die Wohldefiniertheit der B-Operation. Für alle $b \in B$ ist die Multiplikation mit b ein A-Modulhomomorphismus, den wir mit $[b] : B \to B$ bezeichnen. Dann ist $\mathrm{id} \otimes [b]$ auf $M \otimes_A B$ wohldefiniert und die gewünschte B-Operation auf f^*M. Dies macht aus f^*M einen B-Modul:

(i) $[1] = \mathrm{id}$, also operiert $1 \in B$ wie die Identität.
(ii) $[bb'] = [b][b']$ für alle $b, b' \in B$, also ist die Operation assoziativ.
(iii) $[b + b'] = [b] + [b']$ für alle $b, b' \in B$, also ist die Operation distributiv (die andere Relation der Distributivität ist klar. □

Bemerkung 4.48. Mit der Notation wie oben haben wir $f_*(f^*M) = M \otimes_A B$ als A-Moduln, denn für $a \in A$, $x \in M$ und $b \in B$ folgt

$$a(x \otimes b) = (\mathrm{id} \otimes [f(a)])(x \otimes b) = x \otimes f(a)b = a(x \otimes b).$$

Hierbei ist die linke Version von $a(x \otimes b)$ als Operation im Sinne von $f_*(f^*M)$ zu verstehen und die rechte Version im Sinne des Tensorprodukts als A-Moduln.

Die B-Modulstruktur auf f^*M setzt also in gewissem Sinne die A-Modulstruktur fort.

Bemerkung 4.49. Sei $\varphi : M \to N$ ein A-Modulhomomorphismus. Dann ist $\varphi \otimes \mathrm{id} : f^*M \to f^*N$ offensichtlich ein B-Modulhomomorphismus. Die induzierte Abbildung

$$\begin{aligned} \mathrm{Hom}_A(M, N) &\to \mathrm{Hom}_B(f^*M, f^*N) \\ \varphi &\mapsto \varphi \otimes \mathrm{id} \end{aligned}$$

ist ein Gruppenhomomorphismus und auch A-linear als Modulhomomorphismus

$$\mathrm{Hom}_A(M, N) \to f_* \mathrm{Hom}_B(f^*M, f^*N). \tag{4.1}$$

Proposition 4.50 (Adjungiertheit von Basiswechsel und Vergessen)**.** *Sei $f : A \to B$ ein Ringhomomorphismus, M ein A-Modul und N ein B-Modul. Dann gibt es einen natürlichen Isomorphismus von A-Moduln:*

$$\begin{aligned} f_* \mathrm{Hom}_B(f^*M, N) &= \mathrm{Hom}_A(M, f_*N) \\ (\varphi : M \otimes_A B \to N) &\mapsto \big(x \mapsto \varphi(x \otimes 1)\big). \end{aligned}$$

Mit andern Worten ist $M \to f^*M$ gegeben durch $x \mapsto x \otimes 1$ universell für A-Modulhomomorphismen von M in B-Moduln N, die entlang f als A-Moduln aufgefaßt werden.

Beweis. Der A-Modulhomomorphismus $M \to f^*M$ ist $id \otimes f : M = M \otimes_A A \to M \otimes_A B$. Die angegebene Abbildung ist damit

$$\varphi \mapsto \varphi \circ (\mathrm{id} \otimes f),$$

somit wohldefiniert. Die dazu inverse Abbildung ordnet $\psi : M \to f_*N$ den Homomorphismus $f^*M \to N$ gegeben durch

$$x \otimes b \mapsto b\psi(x)$$

für $x \in M$ und $b \in B$ zu. Dies ist wohldefiniert, da $b\psi(x)$ eine A-bilineare Abbildung $M \times B \to N$ definiert. Offensichtlich sind die beiden Abbildungen invers zueinander und A-linear. □

Bemerkung 4.51. Sei $f : A \to B$ ein Ringhomomorphismus, M ein A-Modul und N ein B-Modul. Durch

$$\mathrm{Hom}_f(M, N) = \{\varphi : M \to N \ ; \ \varphi \text{ ist linear und } \varphi(ax) = f(a)\varphi(x) \text{ für alle } x \in M, a \in A\}$$

wird eine symmetrischere Definition der Menge von mit f verträglichen Modulhomomorphismen (mit Ringwechsel entlang f) definiert. Man sieht hoffentlich sofort, daß

$$\mathrm{Hom}_B(f^*M, N) = \mathrm{Hom}_f(M, N) = \mathrm{Hom}_A(M, f_*N).$$

Bemerkung 4.52. Proposition 4.50 übersetzt (4.1) in einen B-Modulhomomorphismus

$$\mathrm{Hom}_A(M, N) \otimes_A B \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B), \tag{4.2}$$

den man studieren muß, wenn man über die Erweiterung der Skalare für Homomorphismen Bescheid wissen möchte.

Beispiel 4.53. Sei $M = A^m$ und $N = A^n$ für $m, n \in \mathbb{N}$. Dann haben wir nach Beispiel 4.32 und (4.1) ein kommutatives Diagramm:

$$\begin{array}{ccc} \mathrm{Hom}_A(A^m, A^n) & \xrightarrow{-\otimes \mathrm{id}_B} & \mathrm{Hom}_B(B^m, B^n) \\ \| & & \| \\ \mathrm{M}_{n\times m}(A) & \xrightarrow{\quad f \quad} & \mathrm{M}_{n\times m}(B). \end{array}$$

Der Basiswechsel ändert somit nur die Koordinaten (nun aus B), nicht aber die Matrixeinträge der Homomorphismen: die Matrix von $f \otimes \mathrm{id}$ ist gleich (dem Bild unter f) der Matrix von f.

Wir sehen auch, daß in diesem Beispiel der Morphismus (4.2) zum Isomorphismus

$$\mathrm{M}_{n\times m}(A) \otimes_A B = \mathrm{M}_{n\times m}(B)$$

wird. Im Allgemeinen ist (4.2) aber weder injektiv noch surjektiv, siehe Aufgabe 4.2.

Proposition 4.54. *Sei $R \neq 0$ ein Ring, $n, m \in \mathbb{N}$ und $R^n \simeq R^m$ als R-Moduln. Dann ist $n = m$.*

Beweis. Allgemein gilt für einen Ringhomomorphismus $f : A \to B$ und $r \in \mathbb{N}$

$$A^r \otimes_A B = (A \otimes_A B)^r = B^r,$$

da Tensorprodukt und direkte Summe vertauschen, Proposition 4.44.

Sei $\mathfrak{m} \subseteq R$ ein maximales Ideal. Wir setzen $k = R/\mathfrak{m}$, das ist ein Körper. Wenn $R^n \simeq R^m$, dann ist auch der Basiswechsel entlang $R \to k$ ein Isomorphismus

$$k^n = R^n \otimes_R k \simeq R^m \otimes_R k = k^m,$$

also

$$n = \dim_k R^n \otimes_R k = \dim_k R^m \otimes_R k = m.$$ □

4.7. **Determinanten und allgemeiner Cayley–Hamilton.** Nicht nur über Körpern gibt es Determinanten. Zunächst bemerken wir, daß zu einem Ringhomomorphismus $f : A \to B$ und $n \in \mathbb{N}$ die koeffizientenweise Anwendung von f einen Homomorphismus (nichtkommutativer, falls $n \geq 2$,) Ringe

$$f : \mathrm{M}_n(A) \to \mathrm{M}_n(B)$$

liefert.

Proposition 4.55 (Existenz und Eindeutigkeit von Determinanten)**.** *Es gibt für alle Ringe R und $n \in \mathbb{N}$ eine Determinante*

$$\det : \mathrm{M}_n(R) \to R,$$

die durch die folgenden Eigenschaften eindeutig definiert ist:

(i) *Für alle Ringhomomorphismen $f : A \to B$ und alle $S \in \mathrm{M}_n(A)$ gilt*

$$f(\det(S)) = \det(f(S)),$$

d.h. das folgende Diagramm kommutiert:

$$\begin{array}{ccc} \mathrm{M}_n(A) & \xrightarrow{f} & \mathrm{M}_n(B) \\ \downarrow{\scriptstyle \det} & & \downarrow{\scriptstyle \det} \\ A & \xrightarrow{f} & B. \end{array}$$

(ii) *Für einen Körper k ist* det *die bekannte Determinante für quadratische Matrizen mit Einträgen in k.*

Beweis. Sei $\mathbb{Z}[\underline{X}] := \mathbb{Z}[X_{ij}; 1 \leq i, j \leq n]$ der Polynomring in Variablen X_{ij}. Dies ist ein Integritätsring mit Quotientenkörper $\mathbb{Q}(\underline{X}) := \mathbb{Q}(X_{ij}; 1 \leq i, j \leq n)$. Die universelle Matrix ist

$$\mathbb{X} = (X_{ij}) \in \mathrm{M}_n(\mathbb{Z}[\underline{X}]).$$

Jede andere Matrix $S = (s_{ij}) \in \mathrm{M}_n(R)$ gehört eindeutig zu einem Ringhomomorphismus

$$\begin{aligned} \varphi_S : \mathbb{Z}[\underline{X}] &\to R \\ X_{ij} &\mapsto \varphi_S(X_{ij}) = s_{ij} \end{aligned}$$

mit $\varphi_S(\mathbb{X}) = S$. Wegen

$$\det(S) = \det(\varphi_S(\mathbb{X})) = \varphi_S(\det(\mathbb{X}))$$

reicht es aus, $\det(\mathbb{X})$ zu definieren. Die Inklusion $i : \mathbb{Z}[\underline{X}] \subseteq \mathbb{Q}(\underline{X})$ zusammen mit der bekannten Theorie der Determinante über Körpern, speziell der Leibniz-Formel, erfordert

$$i(\det(\mathbb{X})) = \det(i(\mathbb{X})) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{\alpha=1}^{n} X_{\alpha\sigma(\alpha)} \in \mathbb{Q}(\underline{X}).$$

Da i injektiv ist, zeigt dies bereits die Eindeutigkeit. Die Existenz folgt nun, da die angegebene Formel polynomial in den X_{ij} ist und daher bereits in $\mathbb{Z}[\underline{X}]$ liegt. Dies definiert $\det(\mathbb{X})$ und dann durch

$$\det(S) := \varphi_S(\det(\mathbb{X}))$$

auch alle Determinanten. Es bleibt zu zeigen, daß Bedinungen (i) und (ii) gelten. Es folgt sofort Korollar 4.56

$$\det(S) = \varphi_S(\det(\mathbb{X})) = \varphi_S\left(\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{\alpha=1}^{n} X_{\alpha\sigma(\alpha)}\right) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{\alpha=1}^{n} s_{\alpha\sigma(\alpha)}.$$

Da diese Formel über jedem Körper die bekannte Determinante definiert, folgt (ii). Für Eigenschaft (i) rechnet man

$$f(\det(S)) = f(\varphi_S(\det(\mathbb{X})) = \varphi_{f(S)}(\det(\mathbb{X})) = \det(f(S)).$$ □

Die so definierte Determinante hat die gewohnten Eigenschaften.

Korollar 4.56. *Es gilt für alle* $S = (s_{ij}) \in \mathrm{M}_n(R)$

$$\det(S) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{\alpha=1}^{n} s_{\alpha\sigma(\alpha)}.$$

Proposition 4.57. *Die Determinante hat die folgenden Eigenschaften. Sei* R *ein Ring und* $n \in \mathbb{N}$ *und* $S \in \mathrm{M}_n(R)$.

(1) $\det : \mathrm{M}_n(R) \to R$ *ist multiplikativ.*
(2) $\det(S) = \det(S^t)$.
(3) det *ist alternierend multilinear in den Zeilen (oder Spalten).*
(4) Laplace-Entwicklung: sei $S^\#$ *die adjunkte Matrix mit*

$$(S^\#)_{ij} = (-1)^{i+j} \det(S_{ji}),$$

wobei $S_{ji} \in \mathrm{M}_{n-1}(R)$ *die Matrix ist, die aus* S *durch streichen der* j*-ten Zeile und* i*-ten Spalte entsteht. Dann gilt*

$$SS^\# = S^\# S = \det(S) \cdot I$$

mit der Einheitsmatrix $I \in \mathrm{M}_n(R)$.

Beweis. Die behaupteten Identitäten (2) - (4) sind polynomialer Natur. Es reicht daher, sie für die universelle Matrix $\mathbb{X}$ zu verifizieren. Da diese Koeffizienten in einem Integritätsring hat, reicht es, die Gleichheiten im Matrizenring über dem Quotientenkörper $\mathbb{Q}(\underline{X})$ zu kontrollieren. Dort gelten die Aussagen aus der bekannten Theorie der Determinante über einem Körper.

Mit Aussage (1) verfährt man genauso, nur daß man diesmal zwei Matrizen $S = (s_{ij}), T = (t_{ij}) \in \mathrm{M}_n(R)$ wählen können muß. Das gelingt mit

$$\begin{aligned} \varphi_{S,T} : \mathbb{Z}[X_{ij}, Y_{ij}; 1 \le i, j \le n] &\to R \\ X_{ij} &\mapsto s_{ij} \\ Y_{ij} &\mapsto t_{ij}. \end{aligned}$$

und den Matrizen $\mathbb{X} = (X_{ij})$ und $\mathbb{Y} = (Y_{ij})$. Der Koeffizientenring von $\mathbb{X}$ und $\mathbb{Y}$ ist wieder ein Integritätsring also in einem Körper enthalten. Damit gilt

$$\det(\mathbb{X}) \cdot \det(\mathbb{Y}) = \det(\mathbb{X}\mathbb{Y})$$

und weiter

$$\begin{aligned} \det(S) \cdot \det(T) &= \varphi_{S,T}(\det(\mathbb{X})) \cdot \varphi_{S,T}(\det(\mathbb{Y})) = \varphi_{S,T}(\det(\mathbb{X})\det(\mathbb{Y})) = \varphi_{S,T}(\det(\mathbb{X}\mathbb{Y})) \\ &= \det(\varphi_{S,T}(\mathbb{X}\mathbb{Y})) = \det(\varphi_{S,T}(\mathbb{X})\varphi_{S,T}(\mathbb{Y})) = \det(ST). \end{aligned}$$

□

Der folgende Determinantentrick ist eine Version des Cayley-Hamilton-Theorems.

Satz 4.58 (Determinantentrick)**.** *Sei* M *ein endlich erzeugter* R*-Modul und* $\mathfrak{a}$ *ein Ideal. Sei* $\varphi : M \to M$ *ein Endomorphismus mit* $\varphi(M) \subseteq \mathfrak{a}M$*. Dann gibt es* $n \in \mathbb{N}$ *und* $a_i \in \mathfrak{a}^i$ *für* $i = 1 \ldots, n$*, so daß*

$$\varphi^n + a_1\varphi^{n-1} + \ldots + a_{n-1}\varphi + a_n = 0$$

in $\mathrm{Hom}_R(M, M)$.

Beweis. Wir machen aus M einen $R[X]$-Modul, indem wir X durch φ operieren lassen. Ein Polynom $P \in R[X]$ wirkt dann auf $y \in M$ durch

$$P(X)y = P(\varphi)(y).$$

Sei $y_1, \ldots, y_n$ ein Erzeugendensystem von M als R-Modul, insbesondere ist

$$\mathfrak{a}M = \{\sum_{i=1}^{n} \alpha_i y_i \ ; \ \alpha_i \in \mathfrak{a}\}.$$

Dann gibt es nach Voraussetzung $a_{ij} \in \mathfrak{a}$ mit

$$\varphi(y_i) = \sum_{j=1}^{n} a_{ij} y_j.$$

Wir betrachten die Matrix

$$S = X \cdot I - (a_{ij}) \in \mathrm{M}_n(R[X]),$$

wobei I die Einheitsmatrix ist. Es gilt wegen der Leibniz-Formel für die Determinante und, weil $a_{ij} \in \mathfrak{a}$ gilt,

$$\det(S) = X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n \in R[X]$$

mit $a_i \in \mathfrak{a}^i$.

Nun folgt aus Laplace-Entwicklung in komprimierter Form:

$$\det(S) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = S^{\#} S \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = S^{\#}(S \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}) = S^{\#} 0 = 0,$$

da ja X wie φ wirkt. Es gilt also $\det(S) y_i = 0$ für alle $1 \leq i \leq n$. Da die $y_1, \ldots, y_n$ den Modul M erzeugen, folgt $\det(S) \in \mathrm{Ann}_{R[X]}(M)$. Also folgt für alle $y \in M$

$$0 = (X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n)(y) = (\varphi^n + a_1 \varphi^{n-1} + \ldots + a_{n-1}\varphi + a_n \,\mathrm{id})(y)$$

und $\det(S)$ ist das gesuchte Polynom. □

Korollar 4.59. *Sei M ein endlich erzeugter R-Modul, und sei $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a}M = M$. Dann gibt es $f \in \mathfrak{a}$ mit $(1 + f) \in \mathrm{Ann}_R(M)$.*

Beweis. Wir wenden Satz 4.58 auf $\varphi = \mathrm{id}_M$ an. Wir finden $a_i \in \mathfrak{a}^i \subseteq \mathfrak{a}$ für $1 \leq i \leq n$ mit

$$0 = (\varphi^n + a_1 \varphi^{n-1} + \ldots + a_{n-1}\varphi + a_n)(x) = (1 + \sum_{i=1}^{n} a_i)x$$

für alle $x \in M$. Es folgt, daß $f = \sum_{i=1}^{n} a_i \in \mathfrak{a}$ das Gewünschte leistet. □

Korollar 4.60 (Allgemeines Nakayama–Lemma)**.** *Sei M ein endlich erzeugter R-Modul und sei $\mathfrak{a} \subseteq \mathrm{Rad}(R)$ ein Ideal von R. Aus $\mathfrak{a}M = M$ folgt dann bereits $M = 0$.*

Beweis. Nach Korollar 4.59 gibt es ein $f \in \mathfrak{a}$ mit $1 + f \in \mathrm{Ann}_R(M)$. Da $\mathfrak{a} \subseteq \mathrm{Rad}(R)$, folgt $1 + f \in R^\times$ nach Proposition 3.19. Also enthält das Annullatorideal eine Einheit und damit die 1, ergo $M = 0$. □

Korollar 4.61. *Sei M ein endlich erzeugter R-Modul, $N \subseteq M$ ein Untermodul und $\mathfrak{a} \subseteq \mathrm{Rad}\, R$ ein Ideal von R mit*

$$M = N + \mathfrak{a}M.$$

Dann gilt bereits $M = N$.

Beweis. Mit M ist auch das homomorphe Bild M/N endlich erzeugt als R-Modul. Nach Voraussetzung ist $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N = M/N$. Damit findet Korollar 4.60 Anwendung und $M/N = 0$. Das bedeutet $M = N$. □

Beispiel 4.62. Auf die Voraussetzung, daß M endlich erzeugt ist als R-Modul, kann nicht verzichtet werden. Betrachten wir einen Körper k und $R = k[[X]]$. Dann ist $\mathfrak{m} = (X)$ das einzige maximale Ideal, also $\mathfrak{m} = \mathrm{Rad}(R)$. Für den Quotientenkörper $k((X))$ gilt dann als Modul über $k[[X]]$, daß $(X)k((X)) = k((X))$, aber trotzdem ist $k((X)) \neq 0$.

Übungsaufgaben zu §4

Übungsaufgabe 4.1. Sei K ein Körper und $R \subseteq K$ ein Ring. Sei M ein R-Modul, so daß es für alle $0 \neq x \in M$ ein $0 \neq f \in R$ gibt mit $fx = 0$. Zeigen Sie, daß dann

$$M \otimes_R K = 0.$$

Übungsaufgabe 4.2. Sei k ein Körper, sei $A = k[X,Y]/(XY, Y^2)$ und $f : A \to k$ die Auswertung in $X = Y = 0$. Sei $M = f_*k = k$ als A-Modul via f, und sei $N = A$ als A-Modul. Dann ist

$$\mathrm{Hom}_A(k, A) \otimes_A k \to \mathrm{Hom}_k(k \otimes_A k, A \otimes_A k)$$

die Nullabbildung, obwohl beide Hom-Mengen $\neq 0$ sind.

5. Grundkonstruktionen der homologischen Algebra

5.1. **Komplexe und exakte Sequenzen.**

Definition 5.1. Ein **Komplex** von R-Moduln ist ein Diagramm $M^\bullet$ der Form

$$M^a \to \ldots \to M^i \xrightarrow{d_i} M^{i+1} \to \ldots \to M^b$$

für ein Intervall $a \leq i \leq b$, so daß für alle $i = a, \ldots, b-2$ gilt:

$$d_{i+1} \circ d_i = 0.$$

Wir erlauben auch $a = -\infty$ und/oder $b = \infty$. In diesem Falle heißt der Komplex **nach unten/oben unbeschränkt**. Die R-Modulhomomorphismen des Komplexes heißen **Differentiale** des Komplexes.

Bemerkung 5.2. (1) Die Bedingung an die Differentiale des Komplexes bedeuten, daß an jeder Stelle im Innern des Komplexes gilt

$$\mathrm{im}(d_i) \subseteq \ker(d_{i+1}).$$

(2) Manchmal spielt die genaue Indizierung keine Rolle!

Definition 5.3. Die **(Ko-)homologie** eines Komplexes $M^\bullet$ von R-Moduln an der (inneren) Stelle i, also beim Ausschnitt des Diagramms

$$\ldots M^{i-1} \xrightarrow{d_{i-1}} M^i \xrightarrow{d_i} M^{i+1} \ldots,$$

ist der R-Modul

$$\mathrm{H}^i(M^\bullet) = \ker(d_i)/\,\mathrm{im}(d_{i-1}).$$

Der Komplex $M^\bullet$ heißt **exakt** an der Stelle i, wenn

$$\mathrm{im}(d_{i-1}) = \ker(d_i).$$

Eine **kurze exakte Sequenz** von R-Moduln ist ein exakter Komplex der Form

$$0 \to M' \to M \to M'' \to 0.$$

Bemerkung 5.4. Ein Komplex $M^\bullet$ ist offensichtlich genau dann exakt an der Stelle i, wenn $\mathrm{H}^i(M^\bullet) = 0$ ist.

Beispiel 5.5. Sei M ein R-Modul und $f \in R$. Sei $f\cdot : M \to M$ die Multiplikation mit f. Dann ist

$$0 \to M \xrightarrow{f\cdot} M \to 0$$

ein Komplex. Platzieren wir diesen in die Grade $[-1, 2]$, dann gilt

$$\mathrm{H}^0 = \ker(f\cdot : M \to M) = \{x \in M \;;\; fx = 0\}$$
$$\mathrm{H}^1 = \mathrm{coker}(f\cdot : M \to M) = M/fM.$$

Beispiel 5.6. Sei k ein Körper und $R = k[\varepsilon]$ also $k[X]/(X^2)$ mit ε dem Bild von X. Dann ist

$$\ldots \to R \xrightarrow{\varepsilon\cdot} R \xrightarrow{\varepsilon\cdot} R \xrightarrow{\varepsilon\cdot} R \to \ldots$$

ein nach oben und unten unbeschränkter exakter Komplex.

Lemma 5.7. *Sei R ein Ring und seien $i : M' \to M$ und $p : M \to M''$ Homomorphismen von R-Moduln.*

(1) $0 \to M' \xrightarrow{i} M$ *ist exakt* $\iff$ i *ist injektiv.*

(2) $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ *ist exakt* $\iff$ $i : M' \to M$ *ist Kern von p (kurz: $M' = \ker(p)$).*

(3) $M \xrightarrow{p} M'' \to 0$ *ist exakt* $\iff$ p *ist surjektiv.*

(4) $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *ist exakt* $\iff$ $p : M \to M''$ *ist Kokern von i (kurz $M'' = \operatorname{coker}(i)$).*

(5) $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *ist kurz exakt* $\iff$ i *ist injektiv, p ist surjektiv und eins der beiden: M' ist Kern von p oder M'' ist Kokern von i.*

Beweis. Das folgt sofort aus der Definition. □

Korollar 5.8. *Sei $\varphi : M \to N$ ein R-Modulhomomorphismus. Der Komplex*

$$0 \to M \xrightarrow{\varphi} N \to 0$$

ist exakt genau dann, wenn φ ein Isomorphismus ist.

Beweis. Klar. □

Korollar 5.9. *Sei M ein R-Modul. Der Komplex*

$$0 \to M \to 0$$

ist exakt genau dann, wenn $M = 0$ ist.

Beweis. Wenn exakt, dann ist $M = \ker(0) = \operatorname{im}(0) = 0$. □

Definition 5.10. Ein **Homomorphismus** zwischen Komplexen $M^\bullet$ und $N^\bullet$ von R-Moduln im Intervall $[a, b]$ besteht aus R-Modulhomomorphismen $f_i : M^i \to N^i$, so daß das Diagramm

$$\begin{array}{ccccccccccc}
M^a & \longrightarrow & \ldots & \longrightarrow & M^i & \xrightarrow{d_i} & M^{i+1} & \longrightarrow & \ldots & \longrightarrow & M^b \\
\downarrow{\scriptstyle f_a} & & & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i+1}} & & & & \downarrow{\scriptstyle f_b} \\
N^a & \longrightarrow & \ldots & \longrightarrow & N^i & \xrightarrow{d_i} & N^{i+1} & \longrightarrow & \ldots & \longrightarrow & N^b
\end{array}$$

kommutiert.

Bemerkung 5.11. Homomorphismen von Komplexen kann man hintereinanderausführen (komponieren), und es gibt die Identität, die an jeder Stelle die Identität ist. Ein Isomorphismus von Komplexen ist ein Homomorphismus von Komplexen, der ein Inverses besitzt. Die Menge

$$\operatorname{Hom}_R(M^\bullet, N^\bullet)$$

aller Homomorphismen der Komplexe als R-Moduln ist ein R-Modul bezüglich der gradweisen R-Modulstruktur der $\operatorname{Hom}_R(M^i, N^i)$.

Kurze exakte Sequenzen dienen der Technik des *dévissage*. Eigenschaften eines R-Moduls M sind oft Konsequenz derselben Eigenschaften von Untermodul $N \subseteq M$ und Quotient M/N. Wir geben zwei Beispiele.

Proposition 5.12 (5-er Lemma für kurze exakte Sequenzen)**.** *Sei*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N' & \xrightarrow{j} & N & \xrightarrow{q} & N'' & \longrightarrow & 0 \end{array} \tag{5.1}$$

ein Homomorphismus kurzer exakter Sequenzen.

Wenn α und γ Isomorphismen sind, dann auch β.

Beweis. Diagrammjagd.

β ist injektiv: Sei $x \in M$ mit $\beta(x) = 0$. Dann ist auch $\gamma(p(x)) = q(\beta(x)) = 0$. Weil γ ein Isomorphismus ist, folgt $p(x) = 0$. Es gibt also ein eindeutiges $x' \in M'$ mit $i(x') = x$. Dann ist $j(\alpha(x')) = \beta(i(x')) = \beta(x) = 0$. Weil α und j injektiv sind, folgt $x' = 0$ und damit $x = i(x') = 0$.

β ist surjektiv: Sei $y \in N$. Weil γ surjektiv ist, gibt es ein $x'' \in M''$ mit $\gamma(x'') = q(y)$. Weil p surjektiv ist, gibt es ein $x_1 \in M$ mit $p(x_1) = x''$. Dann ist

$$q(y - \beta(x_1)) = q(y) - q(\beta(x_1)) = q(y) - \gamma(p(x_1)) = 0.$$

Also gibt es ein $y_2' \in N'$ mit $j(y_2') = y - \beta(x_1)$. Weil α surjektiv ist, gibt es $x_2' \in M'$ mit $\alpha(x_2') = y_2'$. Wir setzen $x_2 = i(x_2')$ und $x = x_1 + x_2$. Dann ist

$$\beta(x) = \beta(x_1) + \beta(x_2) = y - j(y_2') + \beta(i(x_2')) = y - j(\alpha(x_2') + \beta(i(x_2') = y. \qquad \square$$

Bemerkung 5.13. Kurze exakte Sequenzen $0 \to M' \to M \to M'' \to 0$ und $0 \to N' \to N \to N'' \to 0$ mit $M' \simeq N'$ und $M'' \simeq N''$ führen nicht notwendig zu isomorphen R-Moduln M und N. Die a priori existierende Abbildung β und deren Kompatibilität mit α und γ wie in Proposition 5.12 ist keine leere Voraussetzung. Als Beispiel betrachte man die zwei kurzen exakten Sequenzen von $\mathbb{Z}$-Moduln

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{p\cdot} \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

und

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{i_1} \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \xrightarrow{\mathrm{pr}_2} \mathbb{Z}/p\mathbb{Z} \to 0.$$

Es gilt aber sicher $\mathbb{Z}/p^2\mathbb{Z} \not\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, denn die eine Gruppe ist zyklisch und die andere nicht.

Proposition 5.14. *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Dann gilt:*

$$M' \text{ und } M'' \text{endlich erzeugt} \implies M \text{endlich erzeugt} \implies M'' \text{endlich erzeugt.}$$

Beweis. Wir bezeichnen die Abbildungen mit $i : M' \to M$ und $p : M \to M''$. Seien $x_1', \dots, x_r'$ Erzeuger von M' und $x_{r+1}'', \dots, x_{r+s}''$ Erzeuger von M'' als R-Modul. Seien

$$x_n = \begin{cases} i(x_n') & 1 \le n \le r \\ \text{Wahl in } p^{-1}(x_n'') & r+1 \le n \le r+s. \end{cases}$$

Dann erzeugen die $x_1, \dots, x_{r+s}$ den R-Modul M. Sei $x \in M$ beliebig. Dann gibt es in R Elemente $a_{r+1}, \dots, a_{r+s}$ mit

$$p(x) = \sum_{n=r+1}^{r+s} a_n x_n''.$$

Dann ist $x - \sum_{n=r+1}^{r+s} a_n x_n \in \ker(p) = \mathrm{im}(i)$, also von der Form $i(\sum_{n=1}^{r} a_n x_n')$ für geeignete $a_n \in R$. Daher ist $x = \sum_{n=1}^{r+s} a_n x_n$. Das zeigt die erste Aussage.

Die zweite Aussage folgt sofort aus der offensichtlichen Tatsache, daß die Bilder der Erzeuger von M das Bild M'' unter $M \to M''$ erzeugen. $\square$

5.2. **Kern, Kokern, Bild und Kobild.** Wir kennen schon die Definition von Kern und Kokern.

Definition 5.15. Das Bild eines R-Modulhomomorphismus $\varphi : M \to N$ ist

$$\operatorname{im}(\varphi) = \ker(N \to \operatorname{coker}(\varphi)).$$

Das Kobild eines R-Modulhomomorphismus $\varphi : M \to N$ ist

$$\operatorname{coim}(\varphi) = \operatorname{coker}(\ker(\varphi) \to M).$$

Bemerkung 5.16. (1) Nach unserer Konstruktion des Kokerns ist $N \to \operatorname{coker}(\varphi)$ nichts anderes als die Quotientenabbildung $N \to N/\varphi(M)$, deren Kern gerade die Inklusion $\varphi(M) \hookrightarrow N$ ist. Die neue Definition des Bildes stimmt also mit der alten überein.

(2) Das Kobild konstruieren wir gewöhnlich als $M \to M/\ker(\varphi)$.

(3) Kern, Kokern, Bild und Kobild passen in das folgende Diagramm mit exakten Zeilen.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\varphi) & \xrightarrow{i} & M & \longrightarrow & \operatorname{coim}(\varphi) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \varphi} & \swarrow & & & \\ 0 & \longrightarrow & \operatorname{im}(\varphi) & \longrightarrow & N & \xrightarrow{p} & \operatorname{coker}(\varphi) & \longrightarrow & 0. \end{array}$$

Weil $\varphi \circ i = 0$, induziert φ einen R-Modulhomomorphismus $\operatorname{coim}(\varphi) \to N$. Da $p \circ \varphi = 0$, landet dieser R-Modulhomomorphismus als

$$\operatorname{coim}(\varphi) \to \operatorname{im}(\varphi)$$

mit seinem Bild im Bild von φ. Man kann die Reihenfolge ändern und zunächst wegen $p \circ \varphi = 0$ den Homomorphismus φ über $M \to \operatorname{im}(\varphi)$ faktorisieren lassen, und dann wegen $\varphi \circ i = 0$ weiter als $\operatorname{coim}(\varphi) \to \operatorname{im}(\varphi)$. Beide Homomorphismen stimmen überein, denn auf Vertretern ist das nichts anderes als φ selbst:

$$M/\ker(\varphi) \to \varphi(M)$$
$$x + \ker(\varphi) \mapsto \varphi(x).$$

Proposition 5.17. *Der natürliche R-Modulhomomorphismus*

$$\operatorname{coim}(\varphi) \to \operatorname{im}(\varphi)$$

ist ein Isomorphismus.

Beweis. Das ist nichts anderes als der Homomorphiesatz. □

Proposition 5.18. *Seien $i : M' \to M$ und $p : M \to M''$ zwei R-Modulhomomorphismen.*

(1) $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ *ist exakt genau dann, wenn für alle R-Moduln T die induzierte Sequenz*

$$0 \to \operatorname{Hom}_R(T, M') \xrightarrow{i\circ} \operatorname{Hom}_R(T, M) \xrightarrow{p\circ} \operatorname{Hom}_R(T, M'')$$

exakt ist.

(2) $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *ist exakt genau dann, wenn für alle R-Moduln T die induzierte Sequenz*

$$0 \to \operatorname{Hom}_R(M'', T) \xrightarrow{\circ p} \operatorname{Hom}_R(M, T) \xrightarrow{\circ i} \operatorname{Hom}_R(M', T)$$

exakt ist.

Beweis. (1) Es ist $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ exakt $\iff$ $M' = \ker(p)$, und das ist per Definition genau dann der Fall, wenn für alle R-Moduln T und $f : T \to M$ mit $p \circ f = 0$ eine eindeutige Faktorisierung $T \to M'$ über i existiert. Genau das besagt die Exaktheit der Hom-Sequenz.

(2) Es ist $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ exakt $\iff$ $M'' = \operatorname{coker}(i)$, und das ist per Definition genau dann der Fall, wenn für alle R-Moduln T und $f : M \to T$ mit $f \circ i = 0$ eine eindeutige Faktorisierung $M'' \to T$ über p existiert. Genau das besagt die Exaktheit der Hom-Sequenz. □

Korollar 5.19 (Tensorprodukt ist rechtsexakt)**.** *Sei* $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *eine exakte Sequenz von* R*-Moduln und* N *ein* R*-Modul. Dann ist*

$$M' \otimes_R N \xrightarrow{i\otimes\mathrm{id}} M \otimes_R N \xrightarrow{p\otimes\mathrm{id}} M'' \otimes_R N \to 0$$

exakt.

Beweis. Das wissen wir bereits, denn nach Proposition 4.42 ist

$$M'' \otimes_R N = \operatorname{coker}(p) \otimes_R N = \operatorname{coker}(p \otimes \mathrm{id}).$$

Proposition 5.18 erlaubt aber den folgenden formalen Beweis. Da $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ exakt ist, gilt für alle R-Moduln T mit dem R-Modul $\operatorname{Hom}_R(N,T)$, daß

$$0 \to \operatorname{Hom}_R(M'', \operatorname{Hom}_R(N,T)) \xrightarrow{\circ p} \operatorname{Hom}_R(M, \operatorname{Hom}_R(N,T)) \xrightarrow{\circ i} \operatorname{Hom}_R(M', \operatorname{Hom}_R(N,T))$$

exakt ist. Adjungiertheit von Hom und $\otimes$ nach Proposition 4.41 übersetzt dies in die Exaktheit von

$$0 \to \operatorname{Hom}_R(M'' \otimes_R N, T) \xrightarrow{\circ p} \operatorname{Hom}_R(M \otimes_R N, T) \xrightarrow{\circ i} \operatorname{Hom}_R(M' \otimes_R N, T).$$

Laut Proposition 5.18 beweist dies die behauptete Exaktheit.[1] □

Bemerkung 5.20. Seien $\varphi : M_1 \to M_2$ und $\psi : N_1 \to N_2$ Homomorphismen von R-Moduln, und sei $f = (f_1, f_2)$ ein Homomorphismus von φ nach ψ als Komplexe:

$$\begin{array}{ccc} M_1 & \xrightarrow{\varphi} & M_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ N_1 & \xrightarrow{\psi} & N_2 \end{array} .$$

Dann gibt es eindeutig R-Modulhomomorphismen $\ker(f)$ und $\operatorname{coker}(f)$, so daß das folgende Diagramm kommutiert:

$$\begin{array}{ccccccc} \ker(\varphi) & \xrightarrow{i} & M_1 & \xrightarrow{\varphi} & M_2 & \longrightarrow & \operatorname{coker}(\varphi) \\ \vdots{\scriptstyle \ker(f)} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \vdots{\scriptstyle \operatorname{coker} f} \\ \ker(\psi) & \longrightarrow & N_1 & \xrightarrow{\psi} & N_2 & \xrightarrow{p} & \operatorname{coker}(\psi) \end{array} .$$

Das folgt sofort aus $\psi \circ (f_1 \circ i) = f_2 \circ (\varphi \circ i) = 0$ und $(p \circ f_2) \circ \varphi = (p \circ \psi) \circ f_1 = 0$.

Hat man einen dritten R-Modulhomomorphismus $\vartheta : L_1 \to L_2$ und einen Homomorphismus $g = (g_1, g_2)$ im Sinne von Komplexen von ψ nach ϑ, dann gilt

$$\ker(gf) = \ker(g) \circ \ker(f)$$
$$\operatorname{coker}(gf) = \operatorname{coker}(g) \circ \operatorname{coker}(f).$$

Das folgt sofort aus der Eindeutigkeit der Faktorisierungen über Kern und Kokern.

Proposition 5.21 (Kern ist linksexakt)**.** *Zu einem kommutativen Diagramm mit exakten Zeilen*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' \end{array}$$

[1] Man mache sich klar, daß die vorgenommenen Übersetzungen die richtigen Abbildungen in den exakten Sequenzen ergeben!

gehört eine exakte Sequenz

$$0 \to \ker(f') \to \ker(f) \to \ker(f''),$$

in dem die Abbildungen die vom Diagramm induzierten sind.

Beweis. Wir müssen zeigen, daß mit den natürlichen Abbildungen gilt

$$\ker(f') = \ker(\ker(f) \to \ker(f'')).$$

Das folgt sofort aus Diagrammjagd:

$$\begin{aligned}\ker(\ker(f) \to \ker(f'')) &= \{x \in M \ ; \ \text{ in } M'' \text{ und } N \text{ auf } 0\} \\ &= \{x \in M' \ ; \ \text{ in } N \text{ auf } 0\} = \{x \in M' \ ; \ \text{ in } N' \text{ auf } 0\} = \ker(f').\end{aligned}$$ □

Proposition 5.22 (Kokern ist rechtsexakt)**.** *Zu einem kommutativen Diagramm mit exakten Zeilen*

$$\begin{array}{ccccccc} M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ N' & \xrightarrow{i} & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

gehört eine exakte Sequenz

$$\operatorname{coker}(f') \to \operatorname{coker}(f) \to \operatorname{coker}(f'') \to 0,$$

in dem die Abbildungen die vom Diagramm induzierten sind.

Beweis. Wir müssen zeigen, daß mit den natürlichen Abbildungen gilt

$$\operatorname{coker}(f'') = \operatorname{coker}(\operatorname{coker}(f') \to \operatorname{coker}(f)).$$

Das folgt sofort aus Diagrammjagd:

$$\begin{aligned}\operatorname{coker}(\operatorname{coker}(f') \to \operatorname{coker}(f)) &= \operatorname{coker}(N'/f'(M') \to N/f(M)) = N/(i(N') + f(M)) \\ &= N''/\operatorname{im}(M \to N'') = N''/f''(M'') = \operatorname{coker}(f'').\end{aligned}$$ □

5.3. **Das Schlangenlemma.** Sicherlich eines der wichtigsten Werkzeuge der homologischen Algebra ist das Schlangenlemma. Die Namensgebung ist wegen (5.3) hoffentlich selbstredend.

Satz 5.23 (Schlangenlemma)**.** *Sei R ein Ring und sei*

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{j} & N & \xrightarrow{q} & N'' & & \end{array} \tag{5.2}$$

ein kommutatives Diagramm von R-Moduln mit exakten Zeilen.

(1) Die Zuordnung für alle $x \in p^{-1}(\ker(f''))$

$$\delta(p(x)) = f(x) + f'(M') \in N/f'(M')$$

definiert einen natürlichen R-Modulhomomorphismus

$$\delta : \ker(f'') \to \operatorname{coker}(f').$$

(2) Die Sequenz von R-Moduln

$$\begin{array}{ccccccc} \ker(f') & \xrightarrow{i} & \ker(f) & \xrightarrow{p} & \ker(f'') & & \\ & & & \overset{\delta}{\searrow} & & & \\ & & \operatorname{coker}(f') & \xrightarrow{j} & \operatorname{coker}(f) & \xrightarrow{q} & \operatorname{coker}(f'') \end{array} \tag{5.3}$$

ist exakt. Die R-Modulhomomorphismen sind induziert von den jeweiligen mit denselben Buchstaben bezeichneten R-Modulhomomorphismen.

Beweis. Vorab das zum Beweis von (1) gehörende Diagramm:

$$\begin{array}{ccccccc} p^{-1}(\ker(f'')) & \longrightarrow & M & \xrightarrow{f} & N & \longrightarrow & N/f'(M') \\ \downarrow & & & & & & \uparrow \\ \ker(f'') & & \xrightarrow{\quad\delta\quad} & & & & \operatorname{coker}(f') \end{array}$$

Weil p surjektiv ist, ist auch die Einschränkung $p : p^{-1}(\ker(f'')) \to \ker(f'')$ surjektiv. Die angegebene Formel definiert also δ für alle Elemente von $\ker(f'')$. Wir müssen zeigen, daß die Werte von Wahlen unabhängig und tatsächlich in $\operatorname{coker}(f')$ sind. Den Kokern identifizieren wir mittels der von j induzierten Abbildung

$$\operatorname{coker}(f') = N'/f'(M') \xrightarrow{j} N/f'(M')$$

als Untermodul von $N/f'(M')$. Das machen wir zunächst mit Elementen. Es gilt wegen $p(x) \in \ker(f'')$

$$q(f(x)) = f''(p(x)) = 0,$$

und damit $f(x) \in \ker(q) = \operatorname{im}(j)$. Die Formel für δ nimmt daher Werte in $\operatorname{coker}(f')$ an.

Wenn $p(x_1) = p(x_2)$ für $x_1, x_2 \in p^{-1}(\ker(f''))$, dann ist $y' = x_1 - x_2 \in M'$, welches wir vermöge i mit einem Untermodul von M identifiziert haben, weil $\operatorname{im}(i) = \ker(p)$ und $p(y) = p(x_1) - p(x_2) = 0$. Dann ist aber modulo $f'(M')$

$$\delta(p(x_1)) \equiv f(x_1) = f(y' + x_2) = f(y') + f(x_2) \equiv f(x_2) \equiv \delta(p(x_2))$$

und δ ist unabhängig von den Wahlen.

Zum Beweis von (2) bemerken wir, daß die Exaktheit bei $\ker(f)$ und $\operatorname{coker}(f)$ als Variation (nicht genau das gleiche) von Proposition 5.21 und Proposition 5.22 folgt. Wir beweisen also nur die Exaktheit bei $\ker(f'')$ und $\operatorname{coker}(f')$. Wir zeigen zunächst, daß (5.3) ein Komplex ist. Dazu betrachten wir

$$\begin{array}{ccccccc} & & p^{-1}(\ker(f'')) & \longrightarrow & M & \xrightarrow{f} & N & \longrightarrow & N/f'(M') \\ & \nearrow & \downarrow & & & & \uparrow & \searrow & \\ \ker(f) & \xrightarrow{p} & \ker(f'') & & \xrightarrow{\qquad\delta\qquad} & & \operatorname{coker}(f') & \xrightarrow{j} & \operatorname{coker}(f) \end{array}$$

mit den punktierten Modulhomomorphismen induziert von Inklusion und Projektion

$$N/f'(M') \twoheadrightarrow N/f(M) = \operatorname{coker}(f),$$

weil $f'(M') \subseteq f(M)$ in N. Dann kann man $\delta \circ p = 0$ durch Komposition mit der Injektion $\operatorname{coker}(f') \hookrightarrow N/f'(M')$ berechnen und findet 0, weil letztlich f auf $\ker(f)$ angewandt wird. Dual dazu sieht man $j \circ \delta = 0$ durch Komposition mit der Surjektion $p^{-1}(\ker(f'')) \to \ker(f'')$, weil letztlich nach f die Projektion auf $N/f(M)$ folgt.

Exakt bei $\ker(f'')$*:* Sei $x'' \in \ker(f'')$ mit $\delta(x'') = 0$. Dann gibt es ein Urbild $x \in p^{-1}(x'') \subseteq M$ mit $f(x) \in f'(M')$. Sei $x' \in M'$ mit $f(x) = f(x')$. Dann ist auch $p(x - x') = p(x) = x''$ und $f(x - x') = f(x) - f(x') = 0$, also ist x'' im Bild von $p : \ker(f) \to \ker(f'')$.

Exakt bei $\operatorname{coker}(f')$*:* Sei $y' \in N'$ ein Repräsentant für ein Element in $\ker(j : \operatorname{coker}(f') \to \operatorname{coker}(f))$. Das bedeutet, daß es ein $x \in M$ gibt mit

$$j(y') = f(x).$$

Dann ist $f''(p(x)) = q(f(x)) = q(j(y')) = 0$, also $x \in \ker(f'')$ und per Definition von δ sofort

$$\delta(x) = y' \in \operatorname{coker}(f'). \qquad \square$$

Korollar 5.24 (Schlangenlemma mit 0)**.** *Sei R ein Ring und sei*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{j} & N & \xrightarrow{q} & N'' & \longrightarrow & 0 \end{array} \tag{5.4}$$

ein kommutatives Diagramm von R-Moduln mit exakten Zeilen. Dann hat man die folgende exakte Sequenz von R-Moduln:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f') & \xrightarrow{i} & \ker(f) & \xrightarrow{p} & \ker(f'') & & \\ & & & & & \overset{\delta}{\searrow} & & & \\ & & \operatorname{coker}(f') & \xrightarrow{j} & \operatorname{coker}(f) & \xrightarrow{q} & \operatorname{coker}(f'') & \longrightarrow & 0 \end{array} \tag{5.5}$$

Genauer sind die beiden im Vergleich zu Satz 5.23 zusätzlichen Voraussetzungen 'i injektiv' und 'q surjektiv' und die resultierenden Folgerungen mit der identischen Bezeichnung unabhängig voneinander.

Beweis. Das ist eine Kombination aus Satz 5.23 und jeweils Proposition 5.21 und/oder Proposition 5.22. $\square$

Beispiel 5.25. Das 5-er Lemma für kurze exakte Sequenzen, Proposition 5.12, ist ein Spezialfall von Satz 5.23. In der Tat folgt aus (5.1) eine exakte Sequenz

$$\begin{array}{ccccccc} 0 & \xrightarrow{i} & \ker(\beta) & \xrightarrow{p} & 0 & & \\ & & & \overset{\delta}{\searrow} & & & \\ 0 & \xrightarrow{j} & \operatorname{coker}(\beta) & \xrightarrow{q} & 0. & & \end{array}$$

Aus Korollar 5.9 folgt sofort $\ker(\beta) = 0 = \operatorname{coker}(\beta)$ und damit ist β ein Isomorphismus.

Lemma 5.26. *Sei $M_1 \to M_2 \to M_3 \to M_4 \to M_5$ ein exakter Komplex. Dann gibt es natürlich eine kurze exakte Sequenz*

$$0 \to \operatorname{coker}(M_1 \to M_2) \to M_3 \to \ker(M_4 \to M_5) \to 0.$$

Beweis. Die universelle Eigenschaft von Kern und Kokern führen zu den fehlenden Abbildungen i und p im kommutativen Diagramm

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow & & \downarrow & & \| & & \uparrow & & \\ 0 & \longrightarrow & \operatorname{coker}(M_1 \to M_2) & \xrightarrow{i} & M_3 & \xrightarrow{p} & \ker(M_4 \to M_5) & \xrightarrow{\psi_4} & 0 \end{array}$$

Exaktheit bei M_4 besagt, daß p surjektiv ist. Exaktheit bei M_2 besagt, daß i injektiv ist, denn

$$\ker(i) = \ker(M_2 \to M_3)/\operatorname{im}(M_1 \to M_2) = 0.$$

Und die Exaktheit in der unteren Zeile bei M_3 folgt aus der in der oberen Zeile:

$$\ker(p) = \ker(M_3 \to M_4) = \operatorname{im}(M_2 \to M_3) = \operatorname{im}(i).$$ □

Proposition 5.27 (5-er Lemma)**.** *Sei R ein Ring und sei*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{\varphi_1} & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \xrightarrow{\varphi_4} & M_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ N_1 & \xrightarrow{\psi_1} & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \xrightarrow{\psi_4} & N_5 \end{array} \tag{5.6}$$

ein kommutatives Diagramm von R-Moduln mit exakten Zeilen.

(1) Wenn f_2 und f_4 injektiv und f_1 surjektiv sind, dann ist f_3 injektiv.
(2) Wenn f_2 und f_4 surjektiv und f_5 injektiv sind, dann ist f_3 surjektiv.
(3) Wenn f_1, f_2, f_4 und f_5 Isomorphismen sind, dann auch f_3.

Beweis. Die R-Modulhomomorphismen f_2 und f_4 induzieren

$$f' : M' := \operatorname{coker}(M_1 \to M_2) \to \operatorname{coker}(N_1 \to N_2) =: N'$$

und

$$f'' : M'' := \ker(M_4 \to M_5) \to \ker(N_4 \to N_5) =: N''.$$

Wir wenden Lemma 5.26 auf obere und untere Zeile an und erhalten das folgende kommutative Diagramm mit exakten Zeilen:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M_3 & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N_3 & \longrightarrow & N'' & \longrightarrow & 0 \end{array} \tag{5.7}$$

Das Schlangenlemma angewandt auf (5.7) reduziert die Behauptungen auf die folgenden Aussagen:

(a) Wenn f_2 und f_4 injektiv und f_1 surjektiv sind, dann sind f' und f'' injektiv.
(b) Wenn f_2 und f_4 surjektiv und f_5 injektiv sind, dann sind f' und f'' surjektiv.

Wir zeigen nur (a), denn (b) geht genauso (dual). Wenn f_4 injektiv ist, dann ist offensichtlich f'' als Einschränkung von f_4 auf Untermoduln auch injektiv. Der Homomorphismus f' sitzt in einem kommutativen Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{im}(M_1 \to M_2) & \longrightarrow & M_2 & \longrightarrow & M' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_{12}} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f'} & & \\ 0 & \longrightarrow & \operatorname{im}(N_1 \to N_2) & \longrightarrow & N_2 & \longrightarrow & N' & \longrightarrow & 0 \end{array}$$

mit exakten Zeilen, wobei f_{12} induziert von wahlweise f_1 oder f_2 injektiv und surjektiv ist. Aus dem Schlangenlemma folgt die exakte Sequenz

$$0 = \ker(f_2) \to \ker(f') \xrightarrow{\delta} \operatorname{coker}(f_{12}) = 0$$

und damit $\ker(f') = 0$. □

Bemerkung 5.28. Man kann das 5-er Lemma auch per Diagrammjagd beweisen. Hier aber sollte die Nützlichkeit des allgegenwärtigen Schlangenlemmas verdeutlicht werden.

Bemerkung 5.29. Sei $M^\bullet$ ein Komplex von R-Moduln. Dann ist die Kohomologie im Grad i per Definition

$$\mathrm{H}^i(M^\bullet) = \ker(M^i \to M^{i+1}) / \operatorname{im}(M^{i-1} \to M^i).$$

Es gibt noch eine zweite Art, die Kohomologie zu beschreiben. Das Differential $d : M^i \to M^{i+1}$ faktorisiert zu einem R-Modulhomomorphismus $d : M^i / \operatorname{im}(M^{i-1} \to M^i) \to M^{i+1}$. Dabei muß hier und im Folgenden stets bei Differentialen dasjenige mit dem richtigen Index gewählt werden. Wir spezifizieren den Index nur, wenn es nötig ist. Wir erhalten ein Schlangenlemmadiagramm

$$\begin{array}{ccccccccc}
 & & M^{i-1} & \xrightarrow{d} & M^i & \longrightarrow & M^i/(\operatorname{im}(d)) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d} & & \| & & \downarrow{\scriptstyle d} & & \\
0 & \longrightarrow & \ker(d) & \longrightarrow & M^i & \xrightarrow{d} & M^{i+1}. & &
\end{array}$$

Nach dem Schlangenlemma und weil in der Mitte der Isomorphismus $\mathrm{id} : M^i \to M^i$ steht, ist der zugehörige δ-Morphismus ein Isomorphismus

$$\ker\left(M^i / \operatorname{im}(M^{i-1} \to M^i) \to M^{i+1}\right) \xrightarrow{\simeq,\ \delta} \ker(d)/d(M^{i-1}) =: \mathrm{H}^i(M^\bullet).$$

Bemerkung 5.30. Sei $f : M^\bullet \to N^\bullet$ ein Homomorphismus von Komplexen. Wir bezeichnen die Differentiale in $M^\bullet$ mit d_M und die in $N^\bullet$ mit d_N. Dann induziert f auf kompatible Art und Weise R-Modulhomomorphismen

$$\begin{array}{ccccccc}
M^{i-1} & \xrightarrow{d} & \ker(d_{M,i}) & \longrightarrow & \mathrm{H}^i(M^\bullet) & \longrightarrow & 0 \\
\downarrow{\scriptstyle f^{i-1}} & & \downarrow{\scriptstyle f^i} & & \vdots{\scriptstyle \mathrm{H}^i(f)} & & \\
N^{i-1} & \xrightarrow{d} & \ker(d_{N,i}) & \longrightarrow & \mathrm{H}^i(N^\bullet) & \longrightarrow & 0
\end{array}$$

Der so definierte R-Modulhomomorphismus

$$\mathrm{H}^i(f) : \mathrm{H}^i(M^\bullet) \to \mathrm{H}^i(N^\bullet)$$

hat die folgenden Eigenschaften.

(1) Wenn $f = \mathrm{id}$ gradweise die Identität auf dem Komplex $M^\bullet$ ist, dann gilt

$$\mathrm{H}^i(\mathrm{id}) = \mathrm{id}_{\mathrm{H}^i(M^\bullet)}.$$

(2) Wenn $g : N^\bullet \to L^\bullet$ ein weiterer Homomorphismus von Komplexen ist, dann gilt

$$\mathrm{H}^i(gf) = \mathrm{H}^i(g) \circ \mathrm{H}^i(f).$$

(3) Wenn wir $\mathrm{H}^i(M^\bullet)$ gemäß Bemerkung 5.29 als Kern berechnen, dann erhalten wir eine zweite Abbildung aus dem Diagramm

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^i(M^\bullet) & \longrightarrow & M^i/\operatorname{im}(d_M^i) & \xrightarrow{d} & M^{i+1} \\
 & & \vdots{\scriptstyle \mathrm{h}^i(f)} & & \downarrow{\scriptstyle f^i} & & \downarrow{\scriptstyle f^{i+1}} \\
0 & \longrightarrow & \mathrm{H}^i(N^\bullet) & \longrightarrow & N^i/\operatorname{im}(d_N^i) & \xrightarrow{d} & N^{i+1}
\end{array}$$

Dann gilt $\mathrm{h}^i(f) = \mathrm{H}^i(f)$.

Dies folgt alles sofort, wenn man bedenkt, daß Elemente von $\mathrm{H}^i(M^\bullet)$ durch geeignete Repräsentanten in M^i gegeben sind, auf denen die jeweiligen Abbildungen durch f^i berechnet werden.

Definition 5.31. Eine Folge von Abbildungen von Komplexen auf dem gleichen Bereich $[a, b]$

$$0 \to M'^\bullet \to M^\bullet \to M''^\bullet \to 0$$

ist eine **kurze exakte Sequenz von Komplexen**, wenn für alle $i \in [a, b]$

$$0 \to M'^i \to M^i \to M''^i \to 0$$

eine kurze exakte Sequenz von R-Moduln ist.

Kommen wir nun zu einem fundamentalen Ergebnis über Komplexe und ihre Kohomologie. Es sollte nicht überraschen, daß das Schlangenlemma die zentrale Rolle im Beweis übernimmt.

Satz 5.32. *Zu einer kurzen exakten Sequenz von Komplexen*

$$0 \to M'^\bullet \xrightarrow{f} M^\bullet \xrightarrow{g} M''^\bullet \to 0$$

gehört eine natürliche lange exakte Sequenz, lange Kohomologiesequenz genannt, der Kohomologiemoduln

$$\cdots \longrightarrow \mathrm{H}^i(M'^\bullet) \xrightarrow{\mathrm{H}^i(f)} \mathrm{H}^i(M^\bullet) \xrightarrow{\mathrm{H}^i(g)} \mathrm{H}^i(M''^\bullet) \xrightarrow{\delta} \mathrm{H}^{i+1}(M'^\bullet) \xrightarrow{\mathrm{H}^{i+1}(f)} \mathrm{H}^{i+1}(M^\bullet) \xrightarrow{\mathrm{H}^{i+1}(g)} \mathrm{H}^{i+1}(M''^\bullet) \longrightarrow \cdots$$

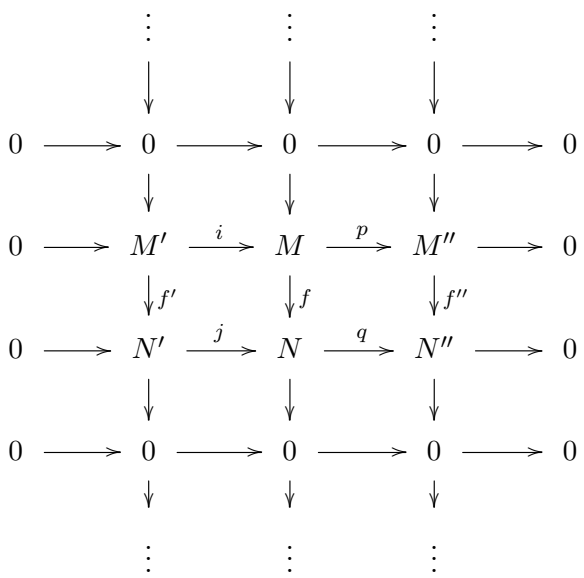
Beweis. Wir bezeichnen die Differentiale in $M'^\bullet$ mit d' und in $M''^\bullet$ mit d''. Weil Kern linksexakt ist nach Proposition 5.21 und weil Kokern rechtsexakt ist nach Proposition 5.22, extrahieren wir aus der kurzen exakten Sequenz der Komplexe das folgende Schlangenlemmadiagramm mit exakten Zeilen

$$\begin{array}{ccccccccc}
 & & M'^i/(\mathrm{im}(d')) & \xrightarrow{f} & M^i/(\mathrm{im}(d)) & \xrightarrow{g} & M''^i/(\mathrm{im}(d'')) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\
0 & \longrightarrow & \ker(d'_i) & \xrightarrow{f} & \ker(d_i) & \xrightarrow{g} & \ker(d''_i). & &
\end{array}$$

Ein Fragment der langen Kohomologiesequenz entsteht aus der Sequenz des Schlangenlemmas, Satz 5.23, und dem Vergleich der beiden Definitionen von Kohomologie aus Bemerkung 5.29. Durch Verschieben des Index und Anstückeln dieser Fragmente entsteht die ganze lange Kohomologiesequenz. □

Beispiel 5.33. Der Beweis von Satz 5.32 besteht im Kern aus dem Schlangenlemma. Das Schlangenlemma selbst ist aber auch ein Beispiel! Wir betrachten Diagramm (5.4) als kurze exakte

Sequenz von Komplexen (der Index der Komplexe verläuft hier in vertikaler Richtung)



und erhalten als lange exakte Kohomologiesequenz genau

$$0 \to \ker(f') \to \ker(f) \to \ker(f'') \xrightarrow{\delta} \operatorname{coker}(f') \to \operatorname{coker}(f) \to \operatorname{coker}(f'') \to 0.$$

5.4. **Projektive Moduln.**

Definition 5.34. Ein **projektiver** R-Modul ist ein R-Modul P, so daß $\operatorname{Hom}_R(P, -)$ kurze exakte Sequenzen in kurze exakte Sequenzen überführt.

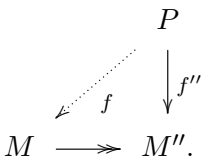
Bemerkung 5.35. Ein R-Modul P ist also projektiv, wenn für alle kurzen exakten Sequenzen von R-Moduln $0 \to M' \to M \to M'' \to 0$ die Sequenz

$$0 \to \operatorname{Hom}_R(P, M') \to \operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, M'') \to 0$$

eine kurze exakte Sequenz von R-Moduln ist. Da nach Proposition 5.18 $\operatorname{Hom}_R(P, -)$ sowieso immer linksexakt ist, bleibt nur zu testen, ob

$$\operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, M'')$$

surjektiv ist. Da jede Surjektion $p : M \to M''$ via $M' = \ker(p)$ in einer kurzen exakten Sequenz von R-Moduln auftritt, erhalten wir das folgende Liftungskriterium für projektiv: Ein R-Modul P ist projektiv, wenn es zu jedem surjektiven R-Modulhomomorphismus $p : M \twoheadrightarrow M''$ und jedem $f'' : P \to M''$ ein $f : P \to M$ gibt, so daß das Diagram



kommutiert.

Satz 5.36. *Sei R ein Ring und M ein R-Modul.*

(1) Freie R-Moduln sind projektiv.
(2) Ein direkter Summand eines projektiven R-Moduls ist projektiv.
(3) Sei $P = \bigoplus_{i \in I} P_i$. Dann ist P projektiv $\iff$ alle P_i sind projektiv.
(4) M projektiv $\iff$ M ist direkter Summand eines freien R-Modul.

Beweis. (1) Sei $p : M \twoheadrightarrow M''$ surjektiv. Jeder freie R-Modul ist von der Form $R^{(X)}$ für eine Menge X. Es gilt

$$\prod_{x\in X} M = \mathrm{Hom}_R(R^{(X)}, M) \xrightarrow{p\circ} \mathrm{Hom}_R(R^{(X)}, M'') = \prod_{x\in X} M''$$

und die Abbildung ist komponentenweise die surjektive Abbildung p. Daher ist $p\circ$ auch surjektiv.

(2) folgt sofort aus (3). Für (3) sei $p : M \twoheadrightarrow M''$ ein surjektiver R-Modulhomomorphismus. Dann ist der obere Pfeil im kommutativen Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_R(P, M) & \xrightarrow{\quad p\circ \quad} & \mathrm{Hom}_R(P, M'') \\ \| & & \| \\ \prod_{i\in I} \mathrm{Hom}_R(P_i, M) & \xrightarrow{(p\circ)_{i\in I}} & \prod_{i\in I} \mathrm{Hom}_R(P_i, M'') \end{array}$$

surjektiv genau dann, wenn die Komponenten des unteren Pfeils surjektiv sind.

(4) Wenn M direkter Summand eines freien Moduls ist, dann folgt aus (1) und (2) sofort, daß M ein projektiver Modul ist.

Für die Umkehrung nutzen wir Korollar 5.38, das jetzt schon zur Verfügung steht. Es gibt also einen freien R-Modul F und ein surjektives $p : F \twoheadrightarrow M$. Weil M projektiv ist, liftet $\mathrm{id} : M \to M$ zu einem R-Modulhomomorphismus $s : M \to F$ mit $p \circ s = \mathrm{id}$. Das folgende Lemma 5.37 zeigt dann

$$F \simeq \ker(p) \oplus M. \qquad \square$$

Lemma 5.37. *Sei $p : M \to M''$ ein R-Modulhomomorphismus mit Spaltung $s : M'' \to M$, d.h. $p \circ s = \mathrm{id}_{M''}$. Dann gilt mit $M' = \ker(p)$*

$$M \simeq M' \oplus M.$$

Beweis. Aus den R-Modulhomomorphismen p und s bauen wir einen Homomorphismus von kurzen exakten Sequenzen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i_1} & M' \oplus M'' & \xrightarrow{\mathrm{pr}_2} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle (i,s)} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0. \end{array}$$

Nach dem 5-er Lemma, Proposition 5.12, ist deshalb (i, s) ein Isomorphismus. $\square$

Korollar 5.38. *Sei R ein Ring. Es gibt **genügend projektive** R-Moduln: zu jedem R-Modul M gibt es einen projektiven (sogar einen freien) R-modul P und einen surjektiven R-Modulhomomorphismus*

$$P \twoheadrightarrow M.$$

Beweis. Nach Satz 5.36 (1) reicht es, eine Surjektion von einem freien R-Modul zu konstruieren. Dies gelingt auf brutale Art und Weise durch den freien Modul auf der Menge M, indem wir jeden Erzeuger des freien Moduls quasi auf sich selbst, nun als Element von M, abbilden:

$$R^{(M)} \to M$$
$$\sum_{x\in M} a_x \cdot x \mapsto \sum_{x\in M} a_x x.$$

Dieser R-Modulhomomorphismus ist offensichtlich surjektiv. $\square$

Beispiel 5.39. (1) Der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ ist für $n \neq 0$ nicht projektiv, denn sonst hätte die Surjektion $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ eine Spaltung.

(2) Sei $R = R_1 \times R_2$. Die Projektionen $\mathrm{pr}_i : R \to R_i$ machen aus den Faktoren R_i Moduln unter R, die wir der Deutlichkeit halber mit M_i bezeichnen. Dann ist $R \simeq M_1 \oplus M_2$ über die Identität, und beide M_i sind projektiv. Wenn $R_i \neq 0$ für $i = 1, 2$, dann sind die M_i nicht frei, denn R wirkt auf den M_i mit nichttrivialem Annullator.

Beispiel 5.40. Es gibt projektive Moduln, die nicht frei sind. Als Beispiel betrachten wir $R = \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$ und als Modul das Ideal $\mathfrak{a} = (2, 1+\sqrt{-5})$. Der arithmetische Grund für das Bespiel besteht in der Gleichung

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Die Surjektion

$$\begin{aligned} p : R^2 &\twoheadrightarrow \mathfrak{a} \\ \begin{pmatrix} x \\ y \end{pmatrix} &\mapsto 2x + (1 + \sqrt{-5})y \end{aligned}$$

erlaubt eine Spaltung $s : \mathfrak{a} \to R^2$ wie folgt. Die Matrix

$$A = \begin{pmatrix} -2 & -1 - \sqrt{-5} \\ 1 - \sqrt{-5} & 3 \end{pmatrix} \in \mathrm{M}_2(R)$$

definiert durch Matrixmultiplikation

$$A : R^2 \to R^2.$$

Es gilt (gerechnet mit Nennern in $\mathfrak{a} \subseteq R \subseteq \mathbb{C}$) für $\begin{pmatrix} x \\ y \end{pmatrix} \in \ker(p)$

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2x - (1+\sqrt{-5})y \\ (1-\sqrt{-5})x + 3y \end{pmatrix} = (2x + (1+\sqrt{-5})y) \cdot \begin{pmatrix} -1 \\ (1-\sqrt{-5})/2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Also faktorisiert A als $s : R^2/\ker(p) = \mathfrak{a} \to R^2$. Dies ist eine Spaltung, weil p surjektiv ist und

$$\begin{aligned} p \circ s(p(\begin{pmatrix} x \\ y \end{pmatrix})) = p(A \begin{pmatrix} x \\ y \end{pmatrix}) &= p(\begin{pmatrix} -2x - (1+\sqrt{-5})y \\ (1-\sqrt{-5})x + 3y \end{pmatrix}) \\ &= 2\big(-2x - (1+\sqrt{-5})y\big) + (1+\sqrt{-5})\big((1-\sqrt{-5})x + 3y\big) \\ &= 2x + (1+\sqrt{-5})y = p(\begin{pmatrix} x \\ y \end{pmatrix}). \end{aligned}$$

Damit wissen wir nun, daß $\mathfrak{a}$ ein direkter Summand von R^2 und als solcher projektiv ist.

Jetzt müssen wir noch zeigen, daß $\mathfrak{a}$ nicht frei ist. Man überlegt sich leicht, daß der Rang von $\mathfrak{a}$ gleich 1 sein müßte. Wir müssen also zeigen, daß $\mathfrak{a}$ kein Hauptideal ist. Angenommen $\mathfrak{a} = (f)$ für ein $f = x + \sqrt{-5}y \in R$ und $x, y \in \mathbb{Z}$. Dann gibt es $a, b, c, d \in \mathbb{Z}$ mit

$$\begin{aligned} 2 &= (a + b\sqrt{-5})f, \\ 1 + \sqrt{-5} &= (c + d\sqrt{-5})f. \end{aligned}$$

Anwendung der Norm $N : \mathbb{Q}(\sqrt{-5}) \to \mathbb{Q}$ liefert

$$\begin{aligned} 4 &= (a^2 + 5b^2)(x^2 + 5y^2), \\ 6 &= (c^2 + 5d^2)(x^2 + 5y^2). \end{aligned}$$

Dies geht nur für $x^2 + 5y^2 \mid (4, 6) = 2$ und das bedeutet $f = \pm 1$. Dann wäre $\mathfrak{a} = (1) = R$. Aber

$$R/\mathfrak{a} = \mathbb{Z}[X]/(X^2 + 5, 2, 1 + X) = \mathbb{Z}/(2, 6) = \mathbb{F}_2$$

zeigt $\mathfrak{a} \neq R$. Damit ist gezeigt, daß $\mathfrak{a}$ projektiv, aber nicht frei als R-Modul ist.

5.5. **Flache Moduln und Algebren.** Die Begriff *flach* geht auf Jean-Pierre Serre zurück. Neben seiner technischen Nützlichkeit hat er eine tiefere algebraisch geometrische Bedeutung als die richtige grundsätzliche Annahme, die eine kontinuierliche algebraische Familie von ... (was auch immer) ... garantiert.

Definition 5.41. Ein **flacher** R-Modul ist eine R-Modul N, so daß $- \otimes_R N$ kurze exakte Sequenzen von R-Moduln in kurze exakte Sequenzen von R-Moduln überführt.

Bemerkung 5.42. Wir wissen bereits aus Korollar 5.19, daß $- \otimes_R N$ rechtsexakt ist: jede exakte Sequenz

$$M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

von R-Moduln führt zu einer exakten Sequenz von R-Moduln

$$M' \otimes_R N \xrightarrow{i\otimes\mathrm{id}} M \otimes_R N \xrightarrow{p\otimes\mathrm{id}} M'' \otimes_R N \to 0.$$

Da jeder injektive R-Modulhomomorphismus $i : M' \to M$ via $M'' = \operatorname{coker}(i)$ in einer kurzen exakten Sequenz enthalten ist, erhalten wir das folgende Kriterium für flach: Ein R-Modul N ist flach, wenn zu jedem injektiven R-Modulhomomorphismus $i : M' \to M$ der R-Modulhomomorphismus

$$i \otimes \mathrm{id} : M' \otimes_R N \to M \otimes_R N$$

injektiv ist.

Satz 5.43. *Sei R ein Ring.*

(1) R ist flacher R-Modul.
(2) Sei $N = \bigoplus_{i\in I} N_i$. Dann ist N flach $\iff$ alle N_i sind flach.
(3) Projektive R-Moduln sind flach.

Beweis. (1) Sei $i : M' \hookrightarrow M$ ein beliebiger injektiver R-Modulhomomorphismus. Dann ist

$$M' = M' \otimes_R R \xrightarrow{i\otimes\mathrm{id}} M \otimes_R R = M$$

nichts anderes als i und daher immer noch injektiv. Daher ist R ein flacher R-Modul.

(2) Sei $j : M' \hookrightarrow M$ ein beliebiger injektiver R-Modulhomomorphismus. Dann ist der obere Pfeil im kommutativen Diagramm

$$\begin{array}{ccc} M' \otimes_R N & \xrightarrow{\quad j\otimes\mathrm{id} \quad} & M \otimes_R N \\ \| & & \| \\ \bigoplus_{i\in I}(M' \otimes_R N_i) & \xrightarrow{(j\otimes\mathrm{id})_{i\in I}} & \bigoplus_{i\in I}(M \otimes_R N_i) \end{array}$$

injektiv genau dann, wenn die Komponenten des unteren Pfeils injektiv sind.

(3) Nach (2) und Satz 5.36 (4) reicht es zu zeigen, daß freie Moduln flach sind. Jeder freie R-Modul ist direkte Summe von Kopien von R. Dieser Modul ist flach nach (1) und (2) beendet den Beweis. □

Definition 5.44. Eine **flache** A-Algebra ist eine A-Algebra $A \to B$, so daß B aufgefaßt als A-Modul ein flacher A-Modul ist.

Bemerkung 5.45. Flache A-Algebren B haben einen besonders angenehmen, nämlich einen exakten Basiswechsel von A-Moduln zu B-Moduln.

Übungsaufgaben zu §5

Übungsaufgabe 5.1. Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Zeigen Sie, daß zu $f \in R$ eine exakte Sequenz

$$0 \to M'[f] \to M[f] \to M''[f] \xrightarrow{\delta} M'/fM' \to M/fM \to M''/fM'' \to 0$$

existiert. Beschreiben Sie den Homomorphismus δ.

Notation: Wir bezeichnen die f-Torsion in M mit $M[f] = \{x \in M \ ; \ fx = 0\}$.

Übungsaufgabe 5.2. Zeigen Sie, daß $\mathbb{Q}$ kein projektiver $\mathbb{Z}$-Modul ist.

Übungsaufgabe 5.3. Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Zeigen Sie die Äquivalenz der beiden folgenden Aussagen.

(a) $R/\mathfrak{a}$ ist projektiver R-Modul.
(b) Es gibt ein Ideal $\mathfrak{b} \subseteq R$ und die kanonische Abbildung

$$R \to R/\mathfrak{a} \times R/\mathfrak{b}$$

ist ein Isomorphismus.

Einführung in Kategorien: im Appendix, wird nachgeliefert

6. Lokalisieren und lokale Eigenschaften

6.1. **Lokalisierung von Ringen.** Der allgemeinen Vorstellung folgend, daß Ringe Funktionenringe sind, muß man einen Ring lokal in der Umgebung eines Punktes anschauen können. Dies erfordert die Technik des Lokalisierens.

Sei R ein Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Wir studieren nun R-Algebren, in denen das Bild von S invertierbar wird. Als Notation vereinbaren wir, daß $*$ eine einelementige Teilmenge ist. Die Zuordnung

$$F_S : R\text{-Algebren} \to \mathsf{sets}$$
$$(\iota : R \to A) \mapsto F_S(A) := \begin{cases} * & \text{falls } \iota(S) \subseteq A^\times \\ \emptyset & \text{sonst} \end{cases}$$

ist ein zugegebenermaßen nicht sehr aufschlußreicher Funktor. Aber es ist ein Funktor, denn wenn $f : A \to B$ ein R-Algebrenhomomorphismus ist und S in A invertierbar wird, dann wird S auch in B invertierbar. Dadurch ist der Effekt von $F_S(f)$ festgelegt. Man hat sowieso keine Wahl und muß nur verhindern, daß $F_S(f) : * \to \emptyset$ sein soll. Das haben wir gerade ausgeschlossen.

Dieser Funktor F_S ist nun von der Form $\mathrm{Hom}_R(S^{-1}R, -)$ für eine geeignete R-Algebra $\iota_S : R \to S^{-1}R$. Durch Auswerten bei $S^{-1}R$ verrät uns

$$\mathrm{id} \in \mathrm{Hom}_R(S^{-1}R, S^{-1}R) = F_S(S^{-1}R) \neq \emptyset,$$

daß S in $S^{-1}R$ invertierbar wird. Die genaue Übersetzung von $\mathrm{Hom}_R(S^{-1}R, -) = F_S(-)$ liefert der folgende Satz. (Das Blabla über F_S kann man auch wieder vergessen.)

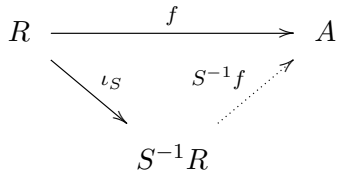
Satz 6.1 (Existenz und Eindeutigkeit der Lokalisierung)**.** *Sei R ein Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann gibt es eine R-Algebra*

$$\iota_S : R \to S^{-1}R$$

mit den folgenden Eigenschaften.

(i) $\iota_S(S) \subseteq (S^{-1}R)^\times$,

(ii) *für jede R-Algebra $f : R \to A$ mit $f(S) \subseteq A^\times$ gibt es genau eine Faktorisierung $S^{-1}f$ wie im kommutativen Diagramm*



Die R-Algebra $S^{-1}R$ ist eindeutig bis auf eindeutigen Isomorphismus.

Beweis. Die Eindeutigkeitsaussage beweist sich rein formal aus den geforderten Eigenschaften von selbst. Nach der Vorrede über den Funktor F_S können wir auch einfach das Yoneda–Lemma zitieren. Aber eigentlich ist das dasselbe Argument.

Der Gehalt des Satzes steckt in der Konstruktion eines solchen $\iota_S : R \to S^{-1}R$. Die Idee zur Konstruktion ist das formale *Bruchrechnen*. Wir definieren

$$S^{-1}R := R \times S/\sim$$

nach der Äquivalenzrelation

$$(a, s) \sim (b, t) \iff \text{es gibt } u \in S \text{ mit } u(at - bs) = 0.$$

Dies ist trivialerweise symmetrisch und reflexiv ist auch klar (mit $u = 1$). Transitiv sieht man wie folgt. Sei $(a, s) \sim (b, t)$, bezeugt durch $u \in S$ und $u(at - bs) = 0$, und sei $(b, t) \sim (c, r)$, bezeugt durch $v \in S$ und $v(br - ct) = 0$, dann ist $(a, s) \sim (c, r)$, weil $uvt \in S$ und

$$uvt(ar - cs) = vr(uat) - us(vct) = vr(ubs) - us(vbr) = 0.$$

Wir schreiben suggestiv

$$\frac{a}{s}$$

für die Äquivalenzklasse mit Vertreter (a, s). Die Definition der Relation liest sich dann

$$\frac{a}{s} = \frac{uat}{ust} = \frac{ubs}{ust} = \frac{b}{t}$$

als bekannte Gleichung durch Erweitern und Kürzen von Brüchen.

Addition und Multiplikation auf $S^{-1}R$ definiert man wie für Brüche:

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Es ist eine Übungsaufgabe zu zeigen, daß dies aus $S^{-1}R$ einen Ring mit $1 = \frac{1}{1}$ und $0 = \frac{0}{1}$ macht. Die Abbildung $\iota_S : R \to S^{-1}R$

$$\iota_S(a) = \frac{a}{1}$$

ist offensichtlich ein Ringhomomorphismus. Sei $s \in S$. Wegen

$$\iota_S(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1$$

schickt ι_S die Elemente von S auf Einheiten von $S^{-1}R$.

Sei $f : R \to A$ ein Ringhomomorphimus wie in (ii). Da S in $S^{-1}R$ auf Einheiten geht, kann $F = S^{-1}f$ höchstens dann existieren, wenn auch $f(S) \subseteq A^\times$ gilt. Dann definieren wir $F : S^{-1}R \to A$ durch

$$F(\frac{a}{s}) := f(a)f(s)^{-1}.$$

Dies ist eine wohldefinierte Abbildung, denn aus $a/s = b/t$ folgt mit $u \in S$ und $u(at - bs)$

$$f(a)f(s)^{-1} = f(uat)f(ust)^{-1} = f(ubs)f(ust)^{-1} = f(b)f(t)^{-1}.$$

Außerdem ist F ein Ringhomomorphismus: die Eins wird bewahrt

$$F(1) = F(1/1) = f(1)f(1)^{-1} = 1,$$

F ist additiv

$$\begin{aligned} F(a/s + b/t) &= F((at + bs)/st) = f(at + bs)f(st)^{-1} \\ &= f(at)f(st)^{-1} + f(bs)f(st)^{-1} = F(a/s) + F(b/t), \end{aligned}$$

und multiplikativ

$$\begin{aligned} F(a/s \cdot b/t) &= F(ab/st) = f(ab)f(st)^{-1} \\ &= f(a)f(s)^{-1} \cdot f(b)f(t)^{-1} = F(a/s) \cdot F(b/t), \end{aligned}$$

Die in (ii) geforderte Faktorisierungseigenschaft gilt, da für alle $a \in R$

$$F(a/1) = f(a)f(1)^{-1} = f(a).$$

Die Definition von F ist zudem die einzig mögliche, da

$$F(\frac{a}{s}) = F(\frac{a}{1} \cdot \frac{1}{s}) = F(\iota_S(a)\iota_S(s)^{-1}) = F(\iota_S(a)) \cdot F(\iota_S(s))^{-1} = f(a)f(s)^{-1}.$$

Die verbleibenden Details der Beweise, insbesondere das Assoziativgesetz und das Distributivgesetz in $S^{-1}R$, bleiben der geneigten Leserschaft zur Übung überlassen. □

Bemerkung 6.2. Die Bedingung (i) in Satz 6.1 zu fordern ist notwendig, weil sonst $\mathrm{id} : R \to R$ selbst auch (ii) löst und $S^{-1}R$ nicht mehr eindeutig ist.

Beispiel 6.3. (1) Sei R ein Integritätsring. Dann ist $S = R \setminus \{0\}$ multiplikativ und

$$\mathrm{Quot}(R) = (R \setminus \{0\})^{-1}R$$

der Quotientenkörper. Aus der universellen Eigenschaft von Satz 6.1 folgt, daß insbesondere $R \to \mathrm{Quot}(R)$ den universellen injektiven Homomorphismus in einen Körper darstellt. Jede Einbettung $R \hookrightarrow K$ in einen Körper K faktorisiert eindeutig zu $\mathrm{Quot}(R) \hookrightarrow K$. Der Quotientenkörper ist der kleinste Körper, der R enthält.

(2) Seien S und T multiplikative Teilmengen des Rings R. Dann ist auch

$$ST = \{st \ ; \ s \in S, \ t \in T\}$$

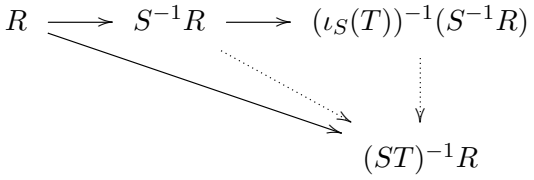
multiplikativ, und es gilt

$$(ST)^{-1}R = (\iota_S(T))^{-1}S^{-1}R$$

als R-Algebren. Das folgt sofort aus der universellen Eigenschaft: ST ist in $(\iota_S(T))^{-1}S^{-1}R$ invertierbar, da st invertierbar ist, wenn nur s und t invertierbar sind. Also gibt es

$$\begin{aligned} (ST)^{-1}R &\to (\iota_S(T))^{-1}S^{-1}R \\ \frac{a}{st} &\mapsto \frac{\frac{a}{s}}{t}. \end{aligned}$$

Umgekehrt sind S und $\iota_S(T)$ in $(ST)^{-1}R$ invertierbar, somit existieren eindeutig die punktierten Pfeile im Diagramm



Die nun konstruierte Abbildung ist die inverse Abbildung zur ersten.

Proposition 6.4. *Sei S eine multiplikative Teilmenge im Ring R. Dann ist*

$$\ker(R \to S^{-1}R) = \{a \in R\ ;\quad \text{es gibt } s \in S \text{ mit } sa = 0\}.$$

Beweis. $\iota_S(a) = 0$ bedeutet $\frac{a}{1} = \frac{0}{1}$, und das sagt, es gibt $s \in S$ mit $s(a \cdot 1 - 0 \cdot 1) = 0$. □

Bemerkung 6.5. Für eine multiplikative Teilmenge S ist $0 \in S$ nicht ausgeschlossen. Aber aus Erfahrung sind wir skeptisch, wenn 0 im Nenner auftritt. Zwar sind die Elemente von $S^{-1}R$ nur formal Brüche (aber das sind die echten Brüche auch!), dennoch wollen wir gerne eine solche katastrophale Division durch 0 kontrollieren.

Proposition 6.6. *Sei S eine multiplikative Teilmenge im Ring R. Dann ist*

$$S^{-1}R = 0 \iff 0 \in S.$$

Beweis. $S^{-1}R = 0 \iff 0 = 1 \in S^{-1}R \iff 1 \in \ker(\iota_S)$. Dies gilt nach Proposition 6.4 genau dann, wenn 1 von einem $s \in S$ annulliert wird, also wenn $0 = s \cdot 1 = s$ für ein $s \in S$. □

Korollar 6.7. *Sei R ein Integritätsring und $S \subseteq R$ multiplikativ mit $0 \notin S$. Dann ist*

$$R \hookrightarrow S^{-1}R \hookrightarrow \mathrm{Quot}(R)$$

injektiv.

Beweis. Aus der universellen Eigenschaft folgen Homomorphismen

$$R \to S^{-1}R \to \mathrm{Quot}(R),$$

die nach Proposition 6.4 injektiv sind, da in einem Integritätsring keine Nullteiler existieren. □

Beispiel 6.8. Sei $f \in R$ ein beliebiges Element. Dann ist

$$S_f := \{1, f, f^2, \ldots, f^n, \ldots\}$$

multiplikativ. Die Lokalisierung bezeichnen wir mit

$$R_f := R[\frac{1}{f}] := S_f^{-1}R.$$

In diesem Ring werden als Nenner nur Potenzen von f zugelassen.

Proposition 6.9. *Sei R ein Ring und $f \in R$ beliebig. Dann gibt es eindeutige R-Algebraisomorphismen*

$$R_f = R[X]/(1 - fX).$$

Beweis. Das Element f hat in $R[X]/(1 - fX)$ das Bild x von X als Inverses. Dies legt den R-Algebrahomomorphismus

$$R_f \to R[X]/(1 - fX)$$

fest. Den inversen Homomorphismus konstruieren wir mit der universellen Eigenschaft des Polynomrings und der Faktorringe: wir brauchen ein Bild für X und dies muß die Gleichung $1 - fX = 0$ erfüllen. Da kommt nur $\frac{1}{f}$ in Frage. □

Satz 6.10. *Sei $f \in R$ ein Element. Dann sind äquivalent:*

(a) f *ist nilpotent.*
(b) $S_f = \{1, f, f^2, \ldots, f^n, \ldots\}$ *enthält die* 0.
(c) $R_f = 0$.
(d) $1 - fX$ *ist Einheit in* $R[X]$.

Beweis. (a) $\iff$ (b) ist trivial, (b) $\iff$ (c) folgt sofort aus Proposition 6.6, und (c) $\iff$ (d) folgt aus Proposition 6.9. □

6.2. **Der Lokalisierungsfunktor für Moduln.** Auch Moduln möchte man lokal in der Nähe eines Punktes des Spektrums anschauen können.

Satz 6.11 (Lokalisierung von Moduln)**.** *Sei R ein Ring und $S \subseteq R$ ein multiplikatives System. Zu einem R-Modul M gibt es einen R-Modulhomomorphismus $R \to S^{-1}R$ mit der Eigenschaft:*

(i) für alle $t \in S$ ist die Multiplikation mit t auf $S^{-1}M$ bijektiv,

(ii) für alle R-Modulhomomorphismen $\varphi : M \to N$, so daß alle $t \in S$ auf N durch Multiplikation bijektiv operieren, gibt es eine eindeutige Fortsetzung $S^{-1}\varphi : S^{-1}M \to N$, also ein kommutatives Diagramm

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ & \searrow \quad \nearrow_{S^{-1}\varphi} & \\ & S^{-1}M. & \end{array}$$

Der Modulhomomorphismus $M \to S^{-1}M$ ist mit den angegebenen Eigenschaften eindeutig bis auf eindeutigen Isomorphismus.

Beweis. Die Eindeutigkeit ist formal. Die Existenz wird durch die folgende Konstruktion gewährleistet. Es ist

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

bezüglich der Äquivalenzrelation

$$(x,s) \sim (y,t) \iff \text{es gibt } u \in S : u(tx - sy) = 0.$$

Der Rest des Beweises verläuft parallel zum Beweis von Satz 6.1 und bringt keine neuen Erkenntnisse. □

Bemerkung 6.12. (1) Auf dem Modul $S^{-1}M$ operieren alle $t \in S$ bijektiv durch Multiplikation. Daher ist $S^{-1}M$ auf eindeutige Weise durch

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}$$

mit $a \in R$, $s,t \in S$ und $x \in M$ ein $S^{-1}R$-Modul.

(2) Die Lokalisierung an S ist sogar ein Funktor. Auf Objekten haben wir $M \rightsquigarrow S^{-1}M$ konstruiert. Zu einem R-Modulhomomorphismus $\varphi : M \to N$ gehört wegen der universellen Eigenschaft von $S^{-1}M$ im Diagramm

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \downarrow & & \downarrow \\ S^{-1}M & \overset{S^{-1}\varphi}{\dashrightarrow} & S^{-1}N \end{array}$$

der Pfeil $S^{-1}\varphi$ der Form

$$S^{-1}\varphi(\frac{x}{s}) = \frac{\varphi(x)}{s}.$$

Dieser ist eindeutig, sogar ein $S^{-1}R$-Modulhomomorphismus und offensichtlich funktoriell. Wir erhalten den Lokalisierungsfunktor auf Moduln

$$S^{-1} : \mathrm{Mod}(R) \to \mathrm{Mod}(S^{-1}R)$$
$$M \mapsto S^{-1}M.$$

(3) Auch für Moduln ist das Lokalisieren transitiv. Seien $S,T \subseteq R$ multiplikativ. Dann ist natürlich

$$(ST)^{-1}M = T^{-1}(S^{-1}M).$$

Satz 6.13. *Sei S ein multiplikatives System in einem Ring R. Dann gibt es für alle $M \in \mathrm{Mod}(R)$ einen natürlichen Isomorphismus*

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

Beweis. Da S in $S^{-1}R$ auf Einheiten abgebildet wird, ist $M = M \otimes_R R \to M \otimes_R S^{-1}R$ ein R-Modulhomomorphismus in einen R-Modul, auf dem die Multiplikation mit allen $s \in S$ bijektiv ist. Aus der universellen Eigenschaft ergibt sich ein eindeutiger R- sogar $S^{-1}R$-Modulhomomorphismus

$$\begin{aligned} S^{-1}M &\to M \otimes_R S^{-1}R \\ \frac{x}{s} &\mapsto x \otimes \frac{1}{s}. \end{aligned}$$

In die umgekehrte Richtung betrachten wir die R-bilineare Abbildung

$$\begin{aligned} M \times S^{-1}R &\to S^{-1}M \\ (x, \frac{a}{s}) &\mapsto \frac{ax}{s}. \end{aligned}$$

Diese induziert nach der universellen Eigenschaft einen R- sogar $S^{-1}R$-Modulhomomorphismus

$$\begin{aligned} M \otimes_R S^{-1}R &\to S^{-1}M \\ x \otimes \frac{a}{s} &\mapsto \frac{ax}{s}. \end{aligned}$$

Diese beiden Homomorphismen sind offensichtlich natürlich und invers zueinander. □

Satz 6.14. *Lokalisieren von Moduln ist ein exakter Funktor.*

Beweis. Sei S ein multiplikatives System in einem Ring R und sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Wir müssen zeigen, daß auch die induzierte Sequenz

$$0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$$

exakt ist. Da Lokalisieren ein Tensorprodukt $- \otimes_R S^{-1}R$ ist, folgt aus allgemeinen Gründen (Korollar 5.19), daß Lokalisieren rechtsexakt ist. Wir müssen also nur zeigen, daß ein injektiver R-Modulhomomorphismus $i : M' \hookrightarrow M$ nach Lokalisieren immer noch injektiv ist.

Sei $y \in S^{-1}M'$ und $S^{-1}i(y) = 0 \in S^{-1}M$. Dann gibt es $x \in M'$ und $s \in S$ mit $y = \frac{x}{s}$, und

$$0 = S^{-1}i(y) = \frac{i(x)}{s}.$$

Weiter gibt es dann $u \in S$ mit $u(1 \cdot i(x) - s \cdot 0) = 0$, also $0 = ui(x) = i(ux)$. Da i injektiv ist, folgt $0 = ux = u(1 \cdot x - s \cdot 0)$. Das bedeutet rückwärts, daß $y = \frac{x}{s} = 0 \in S^{-1}M'$. Damit ist $S^{-1}i$ injektiv. □

Korollar 6.15. *Sei S ein multiplikatives System in einem Ring R. Dann ist $S^{-1}R$ eine flache R-Algebra.*

Beweis. Das folgt sofort aus der Kombination von Satz 6.13 und Satz 6.14. □

Beispiel 6.16. $\mathbb{Q}$ ist als Lokalisierung von $\mathbb{Z}$ eine flache $\mathbb{Z}$-Algebra. Da der $\mathbb{Z}$-Modul $\mathbb{Q}$ nicht projektiv ist, haben wir ein Beispiel, daß flach nicht projektiv impliziert.

Definition 6.17. Ein **endlich präsentierter R-Modul** ist ein R-Modul M, für den es $n_1, n_0 \in \mathbb{N}_0$ und eine exakte R-Modulsequenz

$$R^{n_1} \xrightarrow{A} R^{n_0} \xrightarrow{p} M \to 0$$

gibt. Eine solche Sequenz nennt man eine **endliche Präsentation** von M.

Bemerkung 6.18. Eine endliche Präsentation wie in der Definition besagt, daß M von n_0-vielen Elementen, den Bildern $x_i = p(e_i)$ für $i = 1, \dots, n_0$ mit der Standardbasis e_i von R^{n_0} erzeugt werden kann. Weiter besagt die Präsentation, daß die R-linearen Relationen, die zwischen den x_i in M gelten, durch die n_1-vielen Relationen $A(e_j)$ mit $j = 1, \dots, n_1$ erzeugt werden können. Wenn man A durch eine Matrix beschreibt, dann sind die Koeffizienten der erzeugenden Relationen in den Spalten der Matrix abzulesen.

Satz 6.19. *Sei $A \to B$ eine flache A-Algebra und M ein endlich präsentierter A-Modul. Dann ist für alle A-Moduln N die Basiswechselabbildung*

$$\beta_M : \operatorname{Hom}_A(M, N) \otimes_A B \to \operatorname{Hom}_B(M \otimes_A B, N \otimes_A B)$$
$$\varphi \otimes b \mapsto b(\varphi \otimes \mathrm{id})$$

ein natürlicher Isomorphismus.

Beweis. Schritt 1: Die Aussage ist trivialerweise wahr für $M = A$. Dann ist nämlich

$$\operatorname{Hom}_A(A, N) = N$$

durch Auswertung bei 1 und $A \otimes_A B = B$. Somit betrachten wir

$$\operatorname{Hom}_A(A, N) \otimes_A B = N \otimes_A B = \operatorname{Hom}_B(B, N \otimes_A B).$$

Schritt 2: Wenn die Aussage für R-Moduln M_1 und M_2 anstelle von M gilt, dann auch für $M = M_1 \oplus M_2$. In der Tat ist

$$\operatorname{Hom}_A(M_1 \oplus M_2, N) \otimes_A B = \big(\operatorname{Hom}_A(M_1, N) \otimes_A B\big) \oplus \big(\operatorname{Hom}_A(M_2, N) \otimes_A B\big)$$

und

$$\operatorname{Hom}_B((M_1 \oplus M_2) \otimes_A B, N \otimes_A B) = \operatorname{Hom}_B(M_1 \otimes_A B, N \otimes_A B) \oplus \operatorname{Hom}_B(M_2 \otimes_A B, N \otimes_A B)$$

und die Basiswechselabbildung ist aufgrund ihrer Natürlichkeit mit der Aufspaltung als direkter Summe verträglich. Damit ist sie ein Isomorphismus genau dann, wenn sie komponentenweise ein Isomorphismus ist.

Schritt 3: Aus Schritt 1 und 2 folgt per Induktion die Aussage für $M = R^n$ und beliebige $n \in \mathbb{N}_0$.

Schritt 4: Wir wählen nun eine endliche Präsentation $R^{n_1} \to R^{n_0} \to M \to 0$. Auf diese Sequenz wenden wir zum einen die Funktoren $\operatorname{Hom}_A(-, N)$ und dann $- \otimes_A B$ und zum andern die Funktoren $- \otimes_A B$ und $\operatorname{Hom}_B(-, N \otimes_A B)$ an. Aus den jeweiligen Exaktheitseigenschaften folgt das kommutative Diagramm

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Hom}_A(M, N) \otimes_A B & \longrightarrow & \operatorname{Hom}_A(R^{n_0}, N) \otimes_A B & \longrightarrow & \operatorname{Hom}_A(R^{n_1}, N) \otimes_A B \\
 & & \downarrow{\scriptstyle \beta_M} & & \downarrow{\scriptstyle \beta_{R^{n_0}}} & & \downarrow{\scriptstyle \beta_{R^{n_1}}} \\
0 & \to & \operatorname{Hom}_B(M \otimes_A B, N \otimes_A B) & \to & \operatorname{Hom}_B(R^{n_0} \otimes_A B, N \otimes_A B) & \to & \operatorname{Hom}_B(R^{n_1} \otimes_A B, N \otimes_A B)
\end{array}$$

mit exakten Zeilen. Die beiden rechten vertikalen Abbildungen sind nach Schritt 3 Isomorphismen. Damit ist es auch β_M nach dem 5-er Lemma, Proposition 5.27 (man denke sich das Diagramm nach links durch Nullen fortgesetzt, um auf die 5 Spalten zu kommen).

□

Korollar 6.20. *Sei M ein endlich präsentierter R-Modul und $S \subseteq R$ multiplikativ. Dann ist für alle R-Moduln N die natürliche Abbildung*

$$S^{-1} \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

ein Isomorphismus von $S^{-1}R$-Moduln.

Beweis. Das folgt sofort aus der Kombination von Satz 6.19, Korollar 6.15 und Satz 6.13. □

Beispiel 6.21. Wir geben ein Beispiel an, das zeigt, daß im allgemeinen nicht darauf verzichtet werden kann, daß im rechten Argument ein endlich präsentierter Modul steht. Sei $R = \mathbb{Z}$ und $S^{-1}R = \mathbb{Q}$. Weiter sei $M = \bigoplus_{n\geq 1} \mathbb{Z}$ und $N = \mathbb{Z}$. Dann ist

$$\mathrm{Hom}_{\mathbb{Z}}(\bigoplus_{n\geq 1} \mathbb{Z}, \mathbb{Z}) \otimes \mathbb{Q} = \mathbb{Q} \otimes \prod_{n\geq 1} \mathbb{Z} = \{(x_n) \in \prod_{n\geq 1} \mathbb{Q} \ ; \ \text{ es gibt } N \in \mathbb{N} : Nx_n \in \mathbb{Z} \text{ für alle n}\},$$

während

$$\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q} \otimes \bigoplus_{n\geq 1} \mathbb{Z}, \mathbb{Q} \otimes \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Q}}(\bigoplus_{n\geq 1} \mathbb{Q}, \mathbb{Q}) = \prod_{n\geq 1} \mathbb{Q}$$

mit der offensichtlichen Inklusion als Basiswechselabbildung. Diese ist injektiv, aber nicht bijektiv.

6.3. **Lokalisierung von Idealen und Algebren.**

Lemma 6.22. *Sei R ein Ring, $S \subseteq R$ ein multiplikatives System und $\iota : R \to A$ eine R-Algebra. Dann ist auch $\iota(S) \subseteq A$ ein multiplikatives System und*

$$S^{-1}A = \iota(S)^{-1}A.$$

Das heißt, die Lokalisierung als R-Modul an S und als Ring an $\iota(S)$ stimmen als $S^{-1}R$-Moduln überein. Insbesondere ist $S^{-1}A$ durch $S^{-1}\iota : S^{-1}R \to S^{-1}A$ eine $S^{-1}R$-Algebra.

Beweis. Trivial durch Ausnutzen der jeweiligen universellen Eigenschaften, oder durch Vergleich der Konstruktion. □

Proposition 6.23. *Sei R ein Ring und S eine multiplikative Teilmenge.*

(1) Sei $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist $S^{-1}\mathfrak{a} \subseteq S^{-1}R$ ein Ideal.
(2) Sei $\mathfrak{a} \subseteq R$ ein Ideal. Dann haben wir einen Isomorphismus von $S^{-1}R$-Algebren

$$S^{-1}R/S^{-1}\mathfrak{a} = S^{-1}(R/\mathfrak{a}).$$

(3) Jedes Ideal $\mathfrak{b} \subseteq S^{-1}R$ ist von der Form $S^{-1}\mathfrak{a}$ für ein Ideal $\mathfrak{a} \subseteq R$.
(4) Seien $\mathfrak{a}_1, \mathfrak{a}_2$ Ideale von R. Dann gilt

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \implies S^{-1}\mathfrak{a}_1 \subseteq S^{-1}\mathfrak{a}_2.$$

Beweis. (1) Da Lokalisieren exakt ist, bleibt $S^{-1}\mathfrak{a} \hookrightarrow S^{-1}R$ injektiv. Außerdem sind Untermoduln von $S^{-1}R$ dasselbe wie Ideale.

Die Aussage (2) folgt aus der Exaktheit des Lokalisierens und Lemma 6.22 für die Interpretation als $S^{-1}R$-Algebren.

(3) Zum Ideal $\mathfrak{b} \subseteq S^{-1}R$ betrachten wir

$$\mathfrak{a} = \{x \in R \ ; \ \frac{x}{1} \in \mathfrak{b}\} = \iota_S^{-1}(\mathfrak{b}).$$

Als Urbild eines Ideals ist $\mathfrak{a} \subseteq R$ ein Ideal. Außerdem gilt offensichtlich

$$S^{-1}\mathfrak{a} \subseteq \mathfrak{b}.$$

Wenn $\frac{x}{s} \in \mathfrak{b}$, dann ist $\frac{x}{1} = s \cdot \frac{x}{s} \in \mathfrak{b}$ und damit $x \in \mathfrak{a}$, oder $\frac{x}{s} \in S^{-1}\mathfrak{a}$. Es folgt $S^{-1}\mathfrak{a} = \mathfrak{b}$.

(4) ist klar. □

Satz 6.24. *Sei R ein Ring und S eine multiplikative Teilmenge. Die Lokalisierung an S ist eine bijektive, inklusionserhaltende Abbildung*

$$\begin{aligned} S^{-1} : \{\mathfrak{p} \in \mathrm{Spec}(R) \ ; \ \mathfrak{p} \cap S = \emptyset\} &\xrightarrow{\sim} \mathrm{Spec}(S^{-1}R) \\ \mathfrak{p} &\mapsto S^{-1}\mathfrak{p}. \end{aligned}$$

Die Umkehrabbildung wird durch $\mathfrak{q} \mapsto \iota_S^{-1}(\mathfrak{q})$ beschrieben.

Beweis. Wenn $\mathfrak{p} \subseteq R$ ein Primideal ist, dann ist der Faktorring zum Ideal $S^{-1}\mathfrak{p}$

$$S^{-1}R/S^{-1}\mathfrak{p} = S^{-1}(R/\mathfrak{p})$$

die Lokalisierung am Bild $\bar{S}$ von S in $R/\mathfrak{p}$. Da $R/\mathfrak{p}$ ein Integritätsring ist, gilt dasselbe für die Lokalisierung, sofern $0 \notin \bar{S} \subseteq R/\mathfrak{p}$. Äquivalent dazu ist $S \cap \mathfrak{p} = \emptyset$. In diesem Fall ist $S^{-1}R$ ein Primideal und die Abbildung wohldefiniert.

Die Umkehrabbildung führt zu einem Ideal $\mathfrak{p} = \iota_S^{-1}(\mathfrak{q})$, so daß per Definition die induzierte Abbildung

$$R/\mathfrak{p} \hookrightarrow S^{-1}R/\mathfrak{q}$$

injektiv ist. Daher ist auch $R/\mathfrak{p}$ ein Integritätsring, und $\mathfrak{p}$ ist ein Primideal. Wenn $S \cap \mathfrak{p} \neq 0$, dann wäre auch $S \cap \mathfrak{q} \neq 0$ und $\mathfrak{q} = S^{-1}R$, Widerspruch. Die Umkehrabbildung ist also auch wohldefiniert.

Offensichtlich gilt $\mathfrak{p} \subseteq \iota_S^{-1}(S^{-1}\mathfrak{p})$. Wenn $x \in \iota_S^{-1}(S^{-1}\mathfrak{p})$, dann gibt es $y \in \mathfrak{p}$ und $s \in S$ mit $\frac{x}{1} = \iota_S(x) = \frac{y}{s}$. Dann gibt es $u \in S$ mit $u(xs - y) = 0$, also

$$x(us) = uy \in \mathfrak{p}.$$

Da $us \in S \subseteq R \setminus \mathfrak{p}$, muß der andere Faktor $x \in \mathfrak{p}$ sein, denn $\mathfrak{p}$ ist ein Primideal. Daher gilt

$$\mathfrak{p} = \iota_S^{-1}(S^{-1}\mathfrak{p}).$$

Betrachten wir nun ein Primideal $\mathfrak{q} \subseteq S^{-1}R$ und setzen $\mathfrak{p} = \iota_S^{-1}(\mathfrak{q})$. Dann gilt nach dem Beweis von Proposition 6.23

$$S^{-1}\mathfrak{p} = \mathfrak{q},$$

und die Bijektion ist bewiesen. Die Behauptung über die Inklusionsrelation folgt aus Proposition 6.23 (4). □

6.4. **Lokale Ringe.** Extremes Lokalisieren führt zu lokalen Ringen, die wir nun betrachten wollen.

Definition 6.25. Ein **lokaler Ring** ist ein Ring R der nur ein einziges maximales Ideal $\mathfrak{m}$ besitzt. Wir schreiben dann kurz: sei $(R, \mathfrak{m})$ ein lokaler Ring ... und bezeichnen damit implizit mit $\mathfrak{m}$ das eindeutige maximale Ideal von R.

Proposition 6.26. *Sei R ein Ring. Dann: R ist lokal $\iff$ $R \setminus R^\times$ ist ein Ideal von R.*
In diesem Fall ist $\mathfrak{m} = R \setminus R^\times$ das eindeutige maximale Ideal von R.

Beweis. Jedes echte Ideal $\mathfrak{a} \subseteq R$ enthält keine Einheit, also gilt $\mathfrak{a} \subseteq R \setminus R^\times$. Wenn Letzteres ein Ideal ist, dann ist es offensichtlich das einzige maximale Ideal.

Sei umgekehrt R lokal und $\mathfrak{m}$ das einzige maximale Ideal. Dann ist für jedes $f \in R \setminus \mathfrak{m}$, das Ideal (f) nicht in $\mathfrak{m}$ enthalten, also $(f) = R$. Damit ist f eine Einheit. Wir sehen $R \setminus \mathfrak{m} \subseteq R^\times$. Aber $R^\times \cap \mathfrak{m} = \emptyset$, weil $\mathfrak{m}$ ein echtes Ideal ist. Daher gilt Gleichheit und auch $\mathfrak{m} = R \setminus R^\times$. □

Proposition 6.27. *Sei $(R, \mathfrak{m})$ ein lokaler Ring.*

(1) $f \in R$ *ist Einheit* $\iff$ $f \notin \mathfrak{m}$ $\iff$ $f(\mathfrak{m}) \neq 0$.
(2) $\mathrm{Rad}(R) = \mathfrak{m}$.

Beweis. (1) haben wir bereits in Proposition 6.26 bewiesen, und (2) ist trivial. □

Beispiel 6.28. Beispiele für lokale Ringe sind:

(1) Körper,
(2) $k[[X]]$ für einen Körper k,
(3) $\mathbb{Z}/p^n\mathbb{Z}$,

(4) $\mathbb{C}\{X\}$ = Ring der bei 0 holomorphen Funktionen in $\mathbb{C}$, auch holomorphe Funktionskeime bei 0 genannt. In der Funktionentheorie wird bewiesen, daß für jede in einer Umgebung $0 \in U \subseteq \mathbb{C}$ holomorphe Funktion $f : U \to \mathbb{C}$ mit $f(0) \neq 0$ in einer eventuell kleineren offenen Umgebung der 0 die Funktion $1/f$ auch holomorph ist. Damit sind alle Funktionen außerhalb des Ideals $\mathfrak{m} = \{f \ ; \ f(0) = 0\}$ invertierbar und $\mathfrak{m}$ somit ein maximales Ideal.

Satz 6.29 (Nakayamas Lemma)**.** *Sei $(R, \mathfrak{m})$ ein lokaler Ring, sei $k = R/\mathfrak{m}$ der Restklassenkörper und sei M ein endlich erzeugter R-Modul. Dann sind äquivalent:*

(a) $M = 0$,
(b) $M \otimes_R k = 0$,
(c) $M/\mathfrak{m}M = 0$,
(d) $\mathfrak{m}M = M$.

Beweis. Die Implikationen (a) $\implies$ (b) $\implies$ (c) $\implies$ (d) sind trivial. Und (d) $\implies$ (a) folgt aus Korollar 4.60, weil $\mathrm{Rad}(R) = \mathfrak{m}$. □

Korollar 6.30. *Sei $(R, \mathfrak{m})$ ein lokaler Ring, sei $k = R/\mathfrak{m}$ der Restklassenkörper und sei M ein endlich erzeugter R-Modul.*

(1) Sei $N \subseteq M$ ein Untermodul. Dann gilt

$$N = M \iff M = N + \mathfrak{m}M.$$

(2) Elemente $x_1, \ldots, x_n \in M$ erzeugen M als R-Modul genau dann, wenn die Bilder $\bar{x}_i = x_i + \mathfrak{m}M$ den k-Vektorraum $M/\mathfrak{m}M = M \otimes_R k$ erzeugen.

Beweis. (1) folgt sofort aus Satz 6.29 angewandt auf den endlich erzeugten R-Modul M/N.
(2) folgt aus (1) angewandt auf $N = \langle x_1, \ldots, x_n \rangle_R \subseteq M$. □

Beispiel 6.31. Es ist nicht richtig, daß aus $\dim_k M/\mathfrak{m}M < \infty$ folgt, daß M endlich erzeugt ist als R-Modul. So hat beispielsweise der $k[[X]]$-Modul $M = k((X))$ die Eigenschaft $M/\mathfrak{m}M = 0$, aber $M \neq 0$.

6.5. **Lokale Eigenschaften.** Jetzt endlich wollen wir das Lokalisieren in einem Punkt des Spektrums betrachten. Sei $\mathfrak{p} \in \mathrm{Spec}(R)$ ein Primideal des Rings R. Dann sollen in der Nähe von $\mathfrak{p}$ alle Funktionen $f \in R$, die einen von 0 verschiedenen Wert haben, invertierbar sein. Da $f(\mathfrak{p}) \neq 0$ äquivalent zu $f \notin \mathfrak{p}$ ist, führt uns das auf die Menge

$$R \setminus \mathfrak{p},$$

die wir gerne invertieren möchten. In der Tat ist $R \setminus \mathfrak{p}$ multiplikativ. Das ist unmittelbar äquivalent zur Definition eines Primideals.

Definition 6.32. Der **lokale Ring** bei $\mathfrak{p} \in \mathrm{Spec}(R)$ ist die R-Algebra

$$R \to R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} R.$$

Die **Lokalisierung eines R-Moduls M in $\mathfrak{p}$** ist die Lokalisierung an $R \setminus \mathfrak{p}$ mit der Notation

$$M_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} M = M \otimes_R R_{\mathfrak{p}}.$$

Proposition 6.33. *Der Ring $R_{\mathfrak{p}}$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ und Restklassenkörper*

$$R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = (R/\mathfrak{p})_{\mathfrak{p}} = \mathrm{Quot}(R/\mathfrak{p}) = \kappa(\mathfrak{p}).$$

Beweis. Die Lokalisierungsabbildung $\iota : R \to R_{\mathfrak{p}}$ identifiziert $\mathrm{Spec}(R_{\mathfrak{p}})$ nach Satz 6.24 als Menge mit partieller Ordnung durch Inklusion mit

$$\{\mathfrak{q} \in \mathrm{Spec}(R) \ ; \ \mathfrak{q} \cap (R \setminus \mathfrak{p}) = \emptyset\} = \{\mathfrak{q} \in \mathrm{Spec}(R) \ ; \ \mathfrak{q} \subseteq \mathfrak{p}\}.$$

Daher ist $\mathfrak{p}$, entsprechend $\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Spec}(R_{\mathfrak{p}})$, das einzige maximale Element bezüglich Inklusion. Die Aussage zum Restklassenkörper folgt aus der Exaktheit des Lokalisierens und Lemma 6.22. □

Viele Eigenschaften erhalten sich beim Lokalisieren. Die besseren unter diesen lassen sich sogar dadurch nachweisen, dass man die Eigenschaft nach Lokalisieren an allen Primidealen verifiziert.

Proposition 6.34. *Sei R ein Ring und M ein R-Modul. Dann sind äquivalent:*

(a) $M = 0$.
(b) $M_\mathfrak{p} = 0$ *für alle Primideale* $\mathfrak{p}$ *von* R.
(c) $M_\mathfrak{m} = 0$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* R.

Beweis. (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) ist trivial. Sei also (c) erfüllt und sei $x \in M$ beliebig. Dann ist

$$\mathrm{Ann}_R(x) = \{a \in R \ ; \ ax = 0\}$$

das Annullatorideal von $x \in M$. Angenommen, $\mathrm{Ann}_R(x)$ ist ein echtes Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$ von R mit $\mathrm{Ann}_R(x) \subseteq \mathfrak{m}$. Das heißt andersherum $\mathrm{Ann}_R(x) \cap (R \setminus \mathfrak{m}) = \emptyset$. Daher ist

$$x \notin \ker(M \to M_\mathfrak{m}) = \{y \in M \ ; \ \text{ es gibt } s \in R \setminus \mathfrak{m} \text{ mit } sy = 0\}.$$

Aber dann ist das Bild von x in $M_\mathfrak{m} = 0$ nichttrivial, ein Widerspruch. Also muß $\mathrm{Ann}_R(x) = R$ sein, woraus $0 = 1 \cdot x = x$ folgt. Alle Elemente von M sind somit 0, und $M = 0$ folgt. □

Korollar 6.35. *Sei $f : M \to N$ ein R-Modulhomomorphismus. Die Eigenschaften*

$$\mathscr{P} = \textit{injektiv, surjektiv, bijektiv, Nullabbildung}$$

sind lokal, d.h. es sind äquivalent:

(a) f *hat* $\mathscr{P}$.
(b) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ *hat* $\mathscr{P}$ *für alle Primideale* $\mathfrak{p}$ *von* R.
(c) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ *hat* $\mathscr{P}$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* R.

Beweis. Da Lokalisieren exakt ist, gilt

$$\begin{aligned} \ker(f_\mathfrak{p}) &= \ker(f)_\mathfrak{p}, \\ \mathrm{coker}(f_\mathfrak{p}) &= \mathrm{coker}(f)_\mathfrak{p}, \\ \mathrm{im}(f_\mathfrak{p}) &= \mathrm{im}(f)_\mathfrak{p}. \end{aligned}$$

Das Korollar folgt nun aus Proposition 6.34 angewandt auf $\ker(f)$, $\mathrm{coker}(f)$, $\ker(f)$ und $\mathrm{coker}(f)$, oder $\mathrm{im}(f)$. □

Korollar 6.36. *Seien N_1, N_2 Untermoduln des R-Moduls M.*

(1) Es sind äquivalent:
  (a) $N_1 = N_2$.
  (b) $N_{1,\mathfrak{p}} = N_{2,\mathfrak{p}}$ *für alle Primideale* $\mathfrak{p}$ *von* R.
  (c) $N_{1,\mathfrak{m}} = N_{2,\mathfrak{m}}$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* R.
(2) Es sind äquivalent:
  (a) $N_1 \subseteq N_2$.
  (b) $N_{1,\mathfrak{p}} \subseteq N_{2,\mathfrak{p}}$ *für alle Primideale* $\mathfrak{p}$ *von* R.
  (c) $N_{1,\mathfrak{m}} \subseteq N_{2,\mathfrak{m}}$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* R.

Beweis. (1) folgt aus (2) angewandt auf $N_1 \subseteq N_2$ und $N_2 \subseteq N_1$.

Aussage (2) folgt aus Korollar 6.35 angewandt auf das Nullsein der Komposition der Modulhomomorphismen

$$N_1 \hookrightarrow M \twoheadrightarrow M/N_2.$$ □

Korollar 6.37. *Sei $M^\bullet$ ein Komplex von R-Moduln. Dann ist für alle Primideale $\mathfrak{p}$*

$$\mathrm{H}^i(M^\bullet)_\mathfrak{p} = \mathrm{H}^i(M^\bullet_\mathfrak{p})$$

und insbesondere sind äquivalent:

(a) $M^\bullet$ *ist exakt im Grad i.*

(b) $M^\bullet_\mathfrak{p}$ *ist exakt im Grad* i *für alle Primideale* $\mathfrak{p}$ *von* R.
(c) $M^\bullet_\mathfrak{m}$ *ist exakt im Grad* i *für alle maximalen Ideale* $\mathfrak{m}$ *von* R.

Beweis. Kern und Bild und Kokern lokalisieren sich. Das zeigt $\mathrm{H}^i(M^\bullet)_\mathfrak{p} = \mathrm{H}^i(M^\bullet_\mathfrak{p})$. Proposition 6.34 angewandt auf $\mathrm{H}^i(M^\bullet)$ zeigt nun den Rest. □

Wir studieren nun das Verhalten der Eigenschaft *flach* unter Lokalisierung (an allen Primidealen).

Lemma 6.38. *Sei* $f : A \to B$ *ein Ringhomomorphismus.*
(1) *Sei* M *ein* B*-Modul und* N *ein* A*-Modul. Dann gilt natürlich als* B*-Moduln*
$$M \otimes_B f^*N = f_*(M) \otimes_A N,$$
(2) *Seien nun* M *und* N *beides* A*-Moduln. Dann gibt es einen natürlichen Isomorphismus von* B*-Moduln*
$$f^*(M \otimes_A N) = f^*(M) \otimes_B f^*(N).$$

Beweis. (1) Wegen Assoziativität und Kommutativität des Tensorprodukts gilt
$$M \otimes_B (N \otimes_A B) = M \otimes_B (B \otimes_A N) = (M \otimes_B B) \otimes_A N = M \otimes_A N,$$
und das ist die Behauptung, weil M ganz rechts via f als A-Modul f_*M aufgefaßt wird.

Aussage (2) folgt aus (1) und der Assoziativität und Kommutativität des Tensorprodukts mittels
$$\begin{aligned} f^*(M) \otimes_B f^*(N) &= f_*f^*(M) \otimes_A N \\ &= (M \otimes_A B) \otimes_A N = (M \otimes_A N) \otimes_A B = f^*(M \otimes_A N). \end{aligned}$$ □

Lemma 6.39 (Basiswechsel von flach)**.** *Sei* $f : A \to B$ *ein Ringhomomorphismus, und sei* N *ein flacher* A*-Modul. Dann ist* $f^*(N) = N \otimes_A B$ *ein flacher* B*-Modul.*

Beweis. Sei $i : M' \hookrightarrow M$ ein injektiver Homomorphismus von B-Moduln. Dann kommutiert
$$\begin{array}{ccc} M' \otimes_B f^*(N) & \xrightarrow{i\otimes \mathrm{id}_{f^*N}} & M \otimes_B f^*(N) \\ \| & & \| \\ f_*(M') \otimes_A N & \xrightarrow{i\otimes \mathrm{id}_N} & f_*(M) \otimes_A N. \end{array}$$
Weil N flacher A-Modul ist, ist der untere Pfeil injektiv. Damit ist der obere Pfeil injektiv und $- \otimes_B f^*N$ erhält injektive B-Modulhomomorphismen. Somit ist f^*N flach. □

Satz 6.40 (flach ist lokale Eigenschaft)**.** *Sei* R *ein Ring und* N *ein* R*-Modul. Dann sind äquivalent.*
(a) N *ist flacher* R*-Modul.*
(b) $N_\mathfrak{p}$ *ist flacher* $R_\mathfrak{p}$*-Modul für alle Primideale* $\mathfrak{p}$ *von* R.
(c) $N_\mathfrak{m}$ *ist flacher* $R_\mathfrak{m}$*-Modul für alle maximalen Ideale* $\mathfrak{m}$ *von* R.

Beweis. Aus Lemma 6.39 folgt sofort (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c). Wir nehmen daher (c) an und zeigen (a). Sei dazu $i : M' \hookrightarrow M$ ein injektiver R-Modulhomomorphismus. Nun ist
$$\begin{array}{ccc} (M' \otimes_R N)_\mathfrak{m} & \xrightarrow{(i\otimes \mathrm{id}_N)_\mathfrak{m}} & (M \otimes_R N)_\mathfrak{m} \\ \| & & \downarrow \\ M'_\mathfrak{m} \otimes_{R_\mathfrak{m}} N_\mathfrak{m} & \xrightarrow{i_\mathfrak{m}\otimes \mathrm{id}_{N_\mathfrak{m}}} & M_\mathfrak{m} \otimes_{R_\mathfrak{m}} N_\mathfrak{m} \end{array}$$

kommutativ. Weil Lokalisieren exakt ist, ist $i_{\mathfrak{m}} : M'_{\mathfrak{m}} \hookrightarrow M_{\mathfrak{m}}$ immer noch injektiv. Weil $N_{\mathfrak{m}}$ flacher $R_{\mathfrak{m}}$-Modul ist, bleibt dies ebenso nach $- \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}}$. Proposition 6.34 angewandt auf

$$\ker(i \otimes \mathrm{id}_N)_{\mathfrak{m}} = \ker((i \otimes \mathrm{id}_N)_{\mathfrak{m}}) = \ker(i_{\mathfrak{m}} \otimes \mathrm{id}_{N_{\mathfrak{m}}}) = (0)$$

zeigt die Behauptung. □

Wir studieren nun das Verhalten der Eigenschaft *projektiv* für endlich erzeugte Moduln unter Lokalisierung (an allen Primidealen).

Lemma 6.41 (Basiswechsel von projektiv)**.** *Sei $f : A \to B$ ein Ringhomomorphismus und P ein projektiver A-Modul. Dann ist $P \otimes_A B$ ein projektiver B-Modul.*

Beweis. P ist projektiv, also direkter Summand eines freien A-Moduls. Das bleibt beim $- \otimes_A B$ erhalten. □

Lemma 6.42. *Sei R ein Ring und P ein projektiver R-Modul. Dann sind äquivalent:*

(a) *P ist endlich präsentiert.*
(b) *P ist endlich erzeugt.*

Beweis. Jeder endlich präsentierte Modul ist endlich erzeugt. Wir müssen also nur noch (b) $\Longrightarrow$ (a) zeigen. Sei dazu $n \in \mathbb{N}$ und $x_1, \ldots, x_n \in P$ Erzeuger. Dazu gehört eine Surjektion

$$f : R^n \to P$$

$$(a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i x_i$$

mit Kern $K = \ker(f)$. Weil P projektiv ist, ist die kurze exakte Sequenz

$$0 \to K \xrightarrow{i} R^n \xrightarrow{f} P \to 0$$

gespalten und

$$R^n \simeq P \oplus K.$$

Die Projektion ist ein surjektiver R-Modulhomomorphismus $p : R^n \twoheadrightarrow K$. Die Komposition mit der Inklusion ist ein Endomorphismus $e = i \circ p : R^n \to R^n$ mit $\mathrm{im}(e) = K$ und

$$R^n \xrightarrow{e} R^n \xrightarrow{f} P \to 0$$

ist exakt. Dies zeigt, daß P endlich präsentiert ist. □

Satz 6.43. *Sei $(R, \mathfrak{m})$ ein lokaler Ring. Dann ist jeder endlich erzeugte projektive R-Modul P frei.*

Beweis. Seien $x_1, \ldots, x_n \in P$ Elemente, deren Bilder in $P/\mathfrak{m}P$ eine Basis als $k = R/\mathfrak{m}$-Vektorraum sind. Nach Nakayamas Lemma, genauer Korollar 6.30, erzeugen dann $x_1, \ldots, x_n$ den Modul P. Zu diesen Erzeugern betrachten wir wie in Lemma 6.42 die kurze exakte Sequenz

$$0 \to K \to R^n \to P \to 0.$$

Weil P projektiv ist, gibt es eine Spaltung und $R^n \simeq P \oplus K$. Dann ist auch

$$k^n = R^n \otimes_R k = (P \oplus K) \otimes_R k = P/\mathfrak{m}P \oplus K/\mathfrak{m}K.$$

Da $n = \dim_k P/\mathfrak{m}P$, muß $\dim_k(K/\mathfrak{m}K) = 0$ sein. Also ist $K/\mathfrak{m}K = 0$. Nun ist K als direkter Summand von R^n insbesondere auch endlich erzeugt. Daher darf man Nakayamas Lemma, Satz 6.29, anwenden. Es folgt $K = 0$ und $R^n \to P$ ist ein Isomorphismus. □

Satz 6.44 (projektiv ist für endlich präsentierte Moduln lokal)**.** *Sei R ein Ring und P ein endlich präsentierter R-Modul. Dann sind äquivalent:*

(a) *P ist projektiver R-Modul.*
(b) *$P_{\mathfrak{p}}$ ist projektiver $R_{\mathfrak{p}}$-Modul für alle Primideale $\mathfrak{p}$ von R.*

(c) $P_{\mathfrak{m}}$ *ist projektiver* $R_{\mathfrak{m}}$*-Modul für alle maximalen Ideale* $\mathfrak{m}$ *von* R*.*

Beweis. Aus Lemma 6.41 folgt (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c). Wir nehmen daher (c) an und zeigen (a). Sei

$$0 \to M' \to M \to M'' \to 0$$

eine kurze exakte Sequenz von R-Moduln. Wir müssen zeigen, daß

$$0 \to \mathrm{Hom}_R(P, M') \to \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'') \to 0$$

exakt ist. Gemäß Korollar 6.37 ist dies äquivalent zur Exaktheit für alle maximalen Ideale $\mathfrak{m}$ von

$$0 \to \mathrm{Hom}_R(P, M')_{\mathfrak{m}} \to \mathrm{Hom}_R(P, M)_{\mathfrak{m}} \to \mathrm{Hom}_R(P, M'')_{\mathfrak{m}} \to 0. \tag{6.1}$$

Weil P endlich präsentiert ist, folgt aus Korollar 6.20 für alle R-Moduln N

$$\mathrm{Hom}_R(P, N)_{\mathfrak{m}} = \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, N_{\mathfrak{m}}).$$

Daher ist (6.1) nichts anderes als

$$0 \to \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, M'_{\mathfrak{m}}) \to \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, M_{\mathfrak{m}}) \to \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, M''_{\mathfrak{m}}) \to 0,$$

und das ist exakt, weil $P_{\mathfrak{m}}$ wegen (c) projektiv ist. □

Korollar 6.45. *Sei* R *ein Ring und* P *ein endlich präsentierter* R*-Modul. Dann ist* P *projektiv genau dann, wenn* P *lokal frei ist. Das heißt, wenn* $P_{\mathfrak{p}}$ *ein freier* $R_{\mathfrak{p}}$*-Modul ist für alle* $\mathfrak{p} \in \mathrm{Spec}(R)$ *(oder auch nur die maximalen Ideale von* R*).*

Beweis. Das folgt aus Satz 6.44 zusammen mit Satz 6.43. □

Bemerkung 6.46. Satz 6.44 illustriert die folgende Methode. Man codiert eine Eigenschaft durch exakte Sequenzen, zeigt, daß die Sequenz nach Lokalisieren die entsprechende lokale Eigenschaft codiert, und schließt daraus, daß die Eigenschaft eine lokale Eigenschaft ist.

6.6. **Das Tensorprodukt von Algebren.**

Definition 6.47. Das **Tensorprodukt von** R**-Algebren** ist die direkte Summe (sic!) in der Kategorie

$$R\text{-Algebren}.$$

Konkret heißt das das Folgende. Seien $R \to A$ und $R \to B$ zwei R-Algebren. Dann gibt es eine R-Algebra

$$R \to A \otimes_R B$$

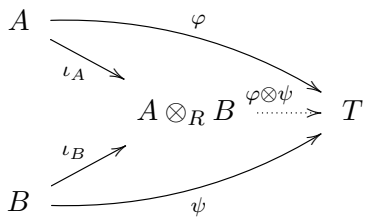
zusammen mit R-Algebramorphismen $\iota_A : A \to A \otimes_R B$ und $\iota_B : B \to A \otimes_R B$, so daß für alle R-Algebren $R \to T$ die natürliche Abbildung

$$\mathrm{Hom}_R(A \otimes_R B, T) \to \mathrm{Hom}_R(A, T) \times \mathrm{Hom}_R(B, T)$$
$$f \mapsto (f \circ \iota_A, f \circ \iota_B)$$

eine Bijektion von Mengen ist. Der zu $\varphi : A \to T$ und $\psi : B \to T$ gehörenden R-Algebrenhomomorphismus wird mit

$$\varphi \otimes \psi : A \otimes_R B \to T$$

bezeichnet. In Diagrammform bedeutet das:



Satz 6.48. *Das Tensorprodukt von Algebren existiert und ist eindeutig bis auf eindeutigen Isomorphismus.*

Beweis. Die Eindeutigkeit ist rein formal. Die Existenz folgt aus der folgenden Konstruktion. Wir betrachten zunächst A und B als R-Moduln. Dann liefert das Tensorprodukt von R-Moduln den R-Modul

$$A \otimes_R B.$$

Die Abbildungen $R \to A$ und $R \to B$ liefern R-Modulhomomorphismen

$$\begin{aligned} \iota_A : A &\to A \otimes_R B \\ a &\mapsto a \otimes 1, \\ \iota_B : B &\to A \otimes_R B \\ b &\mapsto 1 \otimes b. \end{aligned}$$

Die Multiplikation auf A ist R-bilinear und definiert einen R-Modulhomomorphismus $\mu_A : A \otimes_R A \to A$, dito die Multiplikation auf B ein $\mu_B : B \otimes_R B \to B$. Die Multiplikation auf $A \otimes_R B$ wird nun definiert durch

$$\mu : (A \otimes_R B) \otimes_R (A \otimes_R B) = (A \otimes_R A) \otimes_R (B \otimes_R B) \xrightarrow{\mu_A \otimes \mu_B} A \otimes_R B,$$

wobei Assoziativität und Kommutativität des Tensorprodukts von Moduln verwendet wurden. Man rechnet leicht nach, daß μ eine R-Algebrastruktur auf $A \otimes_R B$ definiert und ι_A und ι_B Algebrahomomorphismen sind.

Auf Erzeugern $a \otimes b$ von $A \otimes_R B$ hat die Multiplikation die folgende Form. Für $a_1, a_2 \in A$ und $b_1, b_2 \in B$ ist in $A \otimes_R B$

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2).$$

Die universelle Eigenschaft bekommt man wie folgt. Zu R-Algebrenhomomorphismen $\varphi : A \to T$ und $\psi : B \to T$ ist

$$\begin{aligned} A \times B &\to T \\ (a, b) &\mapsto \varphi(a)\psi(b) \end{aligned}$$

R-bilinear und induziert daher einen R-Modulhomomorphismus $\varphi \otimes \psi : A \otimes B \to T$. Dies ist in der Tat ein R-Algebrenhomomorphismus, also auch mit der Multiplikation verträglich, weil

$$\varphi \otimes \psi(1 \otimes 1) = \varphi(1)\psi(1) = 1$$

und für alle $a_1, a_2 \in A$ und alle $b_1, b_2 \in B$

$$\begin{aligned} \varphi \otimes \psi\big((a_1 \otimes b_1)(a_2 \otimes b_2)\big) &= \varphi \otimes \psi\big((a_1 a_2) \otimes (b_1 b_2)\big) = \varphi(a_1 a_2) \otimes \psi(b_1 b_2) \\ &= (\varphi(a_1)\varphi(a_2)) \otimes (\psi(b_1)\psi(b_2)) = \varphi \otimes \psi(a_1 \otimes b_1) \cdot \varphi \otimes \psi(a_2 \otimes b_2). \end{aligned}$$

Auf beliebige Elemente von $A \otimes_R B$ setzt sich dies R-linear fort, so daß für alle $x, y \in A \otimes_R B$ gilt

$$\varphi \otimes \psi(xy) = \varphi \otimes \psi(x) \cdot \varphi \otimes \psi(y).$$

Es gilt nun

$$\varphi \otimes \psi(a \otimes 1) = \varphi(a)\psi(1) = \varphi(a),$$

also $(\varphi \otimes \psi)\iota_A = \varphi$ und genauso $(\varphi \otimes \psi)\iota_B = \psi$. Außerdem stimmen $f : A \otimes_R B \to T$ und

$$(f \circ \iota_A) \otimes (f \circ \iota_B) : A \otimes_R B \to T$$

auf den R-Modulerzeugern $a \otimes b$ für alle $a \in A$ und $b \in B$ überein: $f = (f \circ \iota_A) \otimes (f \circ \iota_B)$. Damit ist $\varphi, \psi \mapsto \varphi \otimes \psi$ die zur Abbildung im Satz inverse Abbildung und natürlich

$$\mathrm{Hom}_R(A \otimes_R B, T) = \mathrm{Hom}_R(A, T) \times \mathrm{Hom}_R(B, T). \qquad \square$$

Beispiel 6.49. (1) Sei R ein Ring, $S \subseteq R$ ein multiplikatives System und $\iota : R \to A$ eine R-Algebra. Dann gilt
$$S^{-1}A = A \otimes_R S^{-1}R.$$
Das folgt sofort aus Lemma 6.22 und Satz 6.13.

(2) Es gilt $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/d\mathbb{Z}$ mit $d = \mathrm{ggT}(n, m)$. Insbesondere gilt für teilerfremde n, m
$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0.$$
Das liefert einen weiteren Grund dafür, daß es den Nullring geben muß!

(3) Für eine R-Algebra A und ein Ideal $I \subseteq R$ gilt
$$A \otimes_R R/I = A/IA.$$

(4) Sei R ein Ring und A eine R-Algebra. Dann ist
$$R[X] \otimes_R A = A[X]$$
und analog mit beliebig vielen Idealen.

(5) Sei R ein Ring und A eine R-Algebra. Dann ist die natürliche Abbildung
$$R[[X]] \otimes_R A \to A[[X]]$$
im Allgemeinen kein Isomorphismus. Die Elemente im Bild haben eine spezielle Eigenschaft: Das Bild von $\sum_{i=1}^r f_i(X)$ mit Potenzreihen $f_i(X) = \sum_{n\geq 0} b_{i,n}X^n \in R[[X]]$ hat die Form
$$F = \sum_{n\geq 0} \Big(\sum_{i=1}^r b_{i,n}a_i \Big) X^n$$
Das von allen Koeffizienten von F in A erzeugte Ideal liegt in dem von den $a_1, \ldots, a_r$ endlich erzeugten R-Untermodul. Das ist nicht für alle Elemente von $A[[X]]$ richtig. Als Beispiel betrachten wir $R = \mathbb{Z}$ und $A = \mathbb{Q}$. Dann ist
$$\sum_{n\geq 1} \frac{1}{n} X^n$$
nicht im Bild von $\mathbb{Z}[[X]] \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow \mathbb{Q}[[X]]$.

(6) Sei A eine R-Algebra. Die Multiplikation in A ist ein Morphismus von R-Algebren
$$A \otimes_R A \to A.$$

Übungsaufgaben zu §6

Übungsaufgabe 6.1. Sei R ein Ring und $S \subseteq R$ ein multiplikatives System. Ein Ideal $\mathfrak{a} \subseteq R$ heißt **S-saturiert**, wenn für alle $s \in S$ und $x \in R$ aus $sx \in \mathfrak{a}$ auch $x \in \mathfrak{a}$ folgt. Zeigen Sie:

(1) Ein Primideal $\mathfrak{p} \in \mathrm{Spec}(R)$ ist S-saturiert genau dann, wenn $\mathfrak{p} \cap S = \emptyset$.

(2) Jedes Ideal von $S^{-1}R$ ist von der Form $S^{-1}\mathfrak{a}$ für genau ein S-saturiertes Ideal $\mathfrak{a} \subseteq R$.

Übungsaufgabe 6.2. Sei R ein Ring und $S \subseteq R$ ein multiplikatives System. Zeigen Sie
$$S^{-1}(R[X]) = (S^{-1}R)[X],$$
aber
$$S^{-1}(R[[X]]) \neq (S^{-1}R)[[X]].$$

Übungsaufgabe 6.3. Betrachten Sie $M = \mathbb{Q}$ als $\mathbb{Z}$-Modul.

(a) Berechnen Sie für jedes Primideal $\mathfrak{p} \in \mathrm{Spec}(\mathbb{Z})$ die Lokalisierung $M_{\mathfrak{p}}$.

(b) Zeigen Sie, daß es Moduln gibt, die nicht projektiv sind, für die aber jede Lokalisierung an einem Primideal projektiv ist.

Übungsaufgabe 6.4. Sei R ein Ring und $S \subseteq R$ ein multiplikatives System. Sei M ein R-Modul und $N_1, N_2 \subseteq M$ Untermoduln. Zeigen Sie:

$$S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2.$$

Übungsaufgabe 6.5. Sei R ein Ring und $S \subseteq R$ ein multiplikatives System. Zeigen Sie, daß das Nilradikal sich wohl unter Lokalisieren verhält:

$$S^{-1}(\mathscr{N}(R)) = \mathscr{N}(S^{-1}R).$$

Übungsaufgabe 6.6. Sei R ein Ring. Zeigen Sie die Äquivalenz der folgenden Aussagen.

(1) R ist reduziert.
(2) $R_\mathfrak{p}$ ist reduziert für alle $\mathfrak{p} \in \operatorname{Spec}(R)$.
(3) $R_\mathfrak{m}$ ist reduziert für alle maximalen Ideale $\mathfrak{m}$.

Übungsaufgabe 6.7. Sei R ein reduzierter Ring und sei $\mathfrak{p} \in \operatorname{Spec}(R)$ ein minimales Primideal bezüglich Inklusion. Zeigen Sie, daß dann $R_\mathfrak{p}$ ein Körper ist.

Übungsaufgabe 6.8. Sei R ein Ring. Ein **Nullteiler** ist ein $x \in R$, so daß es $0 \neq y \in R$ gibt mit

$$xy = 0.$$

Zeigen Sie, daß ein minimales Primideal $\mathfrak{p} \in \operatorname{Spec}(R)$ nur aus Nullteilern besteht.

7. Das Spektrum

7.1. **Das Spektrum als Funktor.** Das Spektrum eines Rings ist zunächst ein kontravarianter Funktor

$$\begin{aligned} \mathsf{Rings} &\to \mathsf{sets} \\ R &\mapsto \operatorname{Spec}(R). \end{aligned}$$

Aus einem Ringhomomorphismus $f : A \to B$ macht $\operatorname{Spec}(-)$ die Abbildung

$$\begin{aligned} f^{-1} : \operatorname{Spec}(B) &\to \operatorname{Spec}(A) \\ \mathfrak{p} &\mapsto f^{-1}(\mathfrak{p}). \end{aligned}$$

Es gilt offensichtlich

$$f^{-1}(\mathfrak{p}) = \ker(A \to B/\mathfrak{p}),$$

so daß nach dem Homomorphiesatz $A/f^{-1}(\mathfrak{p})$ als Unterring des Integritätsrings $B/\mathfrak{p}$ selbst auch ein Integritätsring ist. Damit ist $f^{-1}(\mathfrak{p})$ ein Primideal. Die Verträglichkeit mit Komposition von Ringhomomorphismen ist klar.

Bemerkung 7.1. Später, das heißt in der Theorie der Schemata, wird $\operatorname{Spec}(R)$ mit mehr und mehr Struktur versehen, so daß $\operatorname{Spec}(-)$ sogar eine kontravariante Kategorienäquivalenz zur Kategorie der affinen Schemata[2] wird.

Wir begnügen uns hier damit, daß der Funktor $\operatorname{Spec}(-)$ die Inklusionsrelation erhält. Aus $\mathfrak{p} \subseteq \mathfrak{q}$ in $\operatorname{Spec}(B)$ folgt bei $f : A \to B$ sofort $f^{-1}(\mathfrak{p}) \subseteq f^{-1}(\mathfrak{q})$.

Beispiel 7.2. Wir betrachten drei typische Teilmengen von $\operatorname{Spec}(R)$ als Bilder induziert von Ringhomomorphismen.

[2] $\operatorname{Spec}(R)$ bekommt die Zariski–Topologie, in der die $V(\mathfrak{a})$ die abgeschlossenen Mengen sind und die $D(f)$ eine Basis der offenen Mengen. Außerdem bekommt $X = \operatorname{Spec}(R)$ eine Strukturgarbe $\mathcal{O}_X$, das ist ein lokaler Begriff von algebraischen Funktionen auf X.

(1) Das **Spektrum eines Faktorrings**. Sei $\mathfrak{a} \subseteq R$ ein Ideal und $p : R \twoheadrightarrow R/\mathfrak{a}$ die Quotientenabbildung. Dann sind Primideale von $R/\mathfrak{a}$ genau die Primideale von R zwischen $\mathfrak{a}$ und R. Wir definieren

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ \mathfrak{a} \subseteq \mathfrak{p} \subseteq R\} \subseteq \operatorname{Spec}(R).$$

und erhalten eine Bijektion

$$p^{-1} : \operatorname{Spec}(R/\mathfrak{a}) \xrightarrow{\sim} V(\mathfrak{a}).$$

Wenn man Aussagen über alle Primideale, die ein Primideal $\mathfrak{p}$ enthalten, machen möchte, dann betrachte man den Ring $R/\mathfrak{p}$.

(2) Das **Spektrum der Lokalisierung**. Sei $S \subseteq R$ eine multiplikative Teilmenge. Dann haben wir bereits in Satz 6.24 gesehen, daß die Lokalisierungsabbildung $\iota_S : R \to S^{-1}R$ eine Bijektion

$$\iota_S^{-1} : \operatorname{Spec}(S^{-1}R) \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ \mathfrak{p} \cap S = \emptyset\} =: D(S)$$

liefert.

Lokalisiert man an $\mathfrak{p}$, dann gilt speziell

$$\operatorname{Spec}(R_{\mathfrak{p}}) \simeq \{\mathfrak{q} \in \operatorname{Spec}(R) \ ; \ \mathfrak{q} \subseteq \mathfrak{p}\},$$

so daß man für Aussagen, die alle Primideale betreffen, die in $\mathfrak{p}$ enthalten sind, zum Ring $R_{\mathfrak{p}}$ übergehen soll.

(3) Eine **standardoffene Teilmenge** von $\operatorname{Spec}(R)$ erhält man zu einem $f \in R$ als

$$D(f) := \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ f(\mathfrak{p}) \neq 0\} \subseteq \operatorname{Spec}(R).$$

Es sind äquivalent

$$f(\mathfrak{p}) \neq 0 \iff f^n \notin \mathfrak{p} \text{ für alle } n \geq 0,$$

denn sowieso $f^0 = 1 \notin \mathfrak{p}$, und aus $f^n \in \mathfrak{p}$ folgt schon, daß ein Faktor, also f, in $\mathfrak{p}$ sein muß. Damit ist

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ \mathfrak{p} \cap \{1, f, f^2, \ldots\} = \emptyset\} \xrightarrow{\sim} \operatorname{Spec}(R_f)$$

unter der Lokalisierungsabbildung.

Bemerkung 7.3. Sei R ein Ring. Der Übergang zu Teilmengen des Spektrums beschrieben durch Faktorringe oder Lokalisierungen kann kombiniert werden.

(1) Aussagen über Primideale von R, die ein Ideal $\mathfrak{a}$ enthalten und außerhalb einer multiplikativen Teilmenge S liegen, handeln von

$$\operatorname{Spec}(S^{-1}R/S^{-1}\mathfrak{a}) = \operatorname{Spec}(S^{-1}(R/\mathfrak{a})) \xrightarrow{\sim} D(S) \cap V(\mathfrak{a}) \subseteq \operatorname{Spec}(R).$$

(2) Speziell handeln Aussagen von Primidealen, die zwischen $\mathfrak{q}$ und $\mathfrak{p} \subseteq \mathfrak{q}$ liegen von

$$\operatorname{Spec}(R_{\mathfrak{q}}/\mathfrak{p}_{\mathfrak{q}}) = \operatorname{Spec}((R/\mathfrak{p})_{\mathfrak{q}}) \xrightarrow{\sim} D(R \setminus \mathfrak{q}) \cap V(\mathfrak{p}) \subseteq \operatorname{Spec}(R).$$

Satz 7.4 (Vereinigung)**.** *Sei R ein Ring, sei $\mathfrak{p}$ ein Primideal von R und seien $\mathfrak{a}_i \subseteq R$ für $i = 1, \ldots, n$ Ideale. Dann sind äquivalent:*

(a) *Es gibt ein i mit $\mathfrak{a}_i \subseteq \mathfrak{p}$.*
(b) $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$.
(c) $\prod_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$.

Insbesondere gilt

$$\bigcup_{i=1}^n V(\mathfrak{a}_i) = V(\bigcap_{i=1}^n \mathfrak{a}_i) = V(\prod_{i=1}^n \mathfrak{a}_i).$$

Beweis. Die Implikation (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) gilt, weil für alle i

$$\prod_{i=1}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{a}_i.$$

Sie nun (c) gegeben, und nehmen wir an, daß (a) nicht gilt. Dann gibt es $f_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ für alle $i = 1, \ldots, n$. Da kein Faktor von $f = \prod_{i=1}^{n} f_i$ in $\mathfrak{p}$ liegt ist $f \notin \mathfrak{p}$. Andererseits gilt wegen (c)

$$f \in \prod_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p},$$

ein Widerspruch. Dies zeigt (c) $\Longrightarrow$ (a).

Der Zusatz folgt sofort aus der Definition von $V(-)$. □

7.2. **Der Support.**

Notation 7.5. Sei x ein Element eines R-Moduls M und sei $\mathfrak{p}$ ein Primideal von R. Wir vereinbaren die Notation

$$x_{\mathfrak{p}} = i_{\mathfrak{p}}(x)$$

für das Bild unter der Lokalisierungsabbildung $i_{\mathfrak{p}} : M \to M_{\mathfrak{p}}$.

Bemerkung 7.6. Der Ringhomomorphismus $R \to \prod_{\mathfrak{p}} \kappa(\mathfrak{p})$ der Auswertungen in den Primidealen hat das Nilradikal $\mathscr{N}(R) = \bigcap_{\mathfrak{p}} \mathfrak{p}$ zum Kern und liftet zum injektiven Ringhomomorphismus

$$\begin{aligned} R &\hookrightarrow \prod_{\mathfrak{p}} R_{\mathfrak{p}} \\ f &\mapsto (f_{\mathfrak{p}})_{\mathfrak{p} \in \operatorname{Spec}(R)} \end{aligned} \tag{7.1}$$

Dazu betrachten wir zu $f \in R$ das Ideal $\mathfrak{a} = (f)$. Wenn $f_{\mathfrak{p}} = 0$ ist für alle Primideale $\mathfrak{p}$, dann ist $\mathfrak{a}_{\mathfrak{p}} = 0$ für alle $\mathfrak{p}$ und nach Proposition 6.34 dann auch $\mathfrak{a} = (f) = 0$, somit $f = 0$.

Mit demselben Beweis hat ein R-Modul M einen injektiven R-Modulhomomorphismus

$$M \hookrightarrow \prod_{\mathfrak{p}} M_{\mathfrak{p}}.$$

Definition 7.7. Der **Halm** eines R-Moduls M in einem Primideal $\mathfrak{p} \in \operatorname{Spec}(R)$ ist der $R_{\mathfrak{p}}$-Modul

$$M_{\mathfrak{p}} = M \otimes_R R_{\mathfrak{p}}.$$

Die **Faser** von M in $\mathfrak{p}$ ist der $\kappa(\mathfrak{p})$-Vektorraum

$$M \otimes_R \kappa(\mathfrak{p}).$$

Vorsicht: die Terminologien Halm und Faser sind nicht gebräuchlich. Halm versteht man noch, Faser eventuell nicht mehr.

Proposition 7.8. *Sei M ein endlich erzeugter R-Modul. Dann ist sind äquivalent:*

(a) $M = 0$,
(b) $M \otimes_R \kappa(\mathfrak{p}) = 0$ *für alle* $\mathfrak{p} \in \operatorname{Spec}(R)$,
(c) $M \otimes_R \kappa(\mathfrak{m}) = 0$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* R.

Beweis. Die Implikationen (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) sind trivial. Wenn (c) gilt, so folgt aus dem Nakayama-Lemma, Satz 6.29, angewandt auf den endlich erzeugten $R_{\mathfrak{m}}$-Modul $M_{\mathfrak{m}}$ wegen

$$M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}} = (M/\mathfrak{m}M)_{\mathfrak{m}} = (M \otimes_R R/\mathfrak{m}) \otimes_R R_{\mathfrak{m}} = M \otimes_R (R/\mathfrak{m})_{\mathfrak{m}} = M \otimes_R \kappa(\mathfrak{m})$$

bereits $M_{\mathfrak{m}} = 0$. Dann schließen wir auf (a) mit Proposition 6.34. □

Definition 7.9. Der **Support (Träger)** eines Elements $x \in M$ in einem R-Modul M ist

$$\operatorname{supp}(x) := \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ x_{\mathfrak{p}} \neq 0\}.$$

Der **Support (Träger)** eines R-Moduls M ist

$$\operatorname{supp}(M) := \{\mathfrak{p} \in \operatorname{Spec}(R) \ : \ M_{\mathfrak{p}} \neq 0\}.$$

Korollar 7.10. *Sei M ein endlich erzeugter R-Modul. Der Support von M ist der Träger der Rangfunktion*

$$\begin{aligned} \operatorname{rk}_M : \operatorname{Spec}(R) &\to \mathbb{N}_0 \\ \mathfrak{p} &\mapsto \operatorname{rk}_M(\mathfrak{p}) = \dim_{\kappa(\mathfrak{p})} M \otimes_R \kappa(\mathfrak{p}), \end{aligned}$$

das heißt, es gilt

$$\operatorname{supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ M \otimes_R \kappa(\mathfrak{p}) \neq 0\}.$$

Beweis. Das ist ein Korollar zum Beweis von Proposition 7.8. □

Proposition 7.11. *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Dann gilt*

$$\operatorname{supp}(M) = \operatorname{supp}(M') \cup \operatorname{supp}(M'').$$

Beweis. Zu jedem $\mathfrak{p} \in \operatorname{Spec}(R)$ ist

$$0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$$

exakt und daher $M_{\mathfrak{p}} = 0 \iff M'_{\mathfrak{p}} = 0$ und $M''_{\mathfrak{p}} = 0$. □

Satz 7.12. *Sei M ein R-Modul und sei $x \in M$. Dann gilt*

$$\operatorname{supp}(x) = V(\operatorname{Ann}_R(x)).$$

Wenn M endlich erzeugt ist, dann gilt auch

$$\operatorname{supp}(M) = V(\operatorname{Ann}_R(M)).$$

Beweis. Sei $\mathfrak{p}$ ein Primideal von R. Wegen

$$\ker(M \to M_{\mathfrak{p}}) = \{y \in M \ ; \ \text{ es gibt } s \notin \mathfrak{p} : sy = 0\}$$

gilt

$$\begin{aligned} \mathfrak{p} \in \operatorname{supp}(x) &\iff x_{\mathfrak{p}} \neq 0 \\ &\iff \operatorname{Ann}_R(x) \cap (R \setminus \mathfrak{p}) = \emptyset \iff \operatorname{Ann}_R(x) \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\operatorname{Ann}_R(x)). \end{aligned}$$

Sei M erzeugt von $x_1, \ldots, x_n$. Dann ist $M_{\mathfrak{p}} \neq 0$ genau dann, wenn $x_{i,\mathfrak{p}} \neq 0$ für ein i, also

$$\begin{aligned} \operatorname{supp}(M) &= \bigcup_{i=1}^{n} \operatorname{supp}(x_i) = \bigcup_{i=1}^{n} V(\operatorname{Ann}_R(x_i)) && \text{(Satz 7.4)} \\ &= V(\bigcap_{i=1}^{n} \operatorname{Ann}_R(x_i)) = V(\operatorname{Ann}_R(M)). \end{aligned}$$

□

Beispiel 7.13. Der Support des R-Moduls $R/\mathfrak{a}$ ist $V(\mathfrak{a})$. Dies folgt sofort aus Satz 7.12, denn $\operatorname{Ann}_R(R/\mathfrak{a}) = \mathfrak{a}$.

7.3. **Die Krull–Dimension.**

Definition 7.14. Wir definieren die Dimension eines Rings.

(1) Eine **Kette von Primidealen** eines Rings R ist eine totalgeordnete Teilmenge von $\mathrm{Spec}(R)$. (Eine Kette hat keine Wiederholungen, weil es sich ja um eine Teilmenge handelt!)
(2) Die **Länge** der Kette
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$
von Primidealen $\mathfrak{p}_i \in \mathrm{Spec}(R)$ ist n.
(3) Die **(Krull-)Dimension** eines Rings R ist definiert als
$$\dim(R) := \max\{n \ ; \text{ es gibt in } \mathrm{Spec}(R) \text{ eine Kette von Primidealen der Länge } n\}.$$

Beispiel 7.15. (1) Körper haben nur ein Primideal, also Dimension 0.
(2) Ein Integritätsring hat genau dann Dimension 0, wenn es ein Körper ist.
(3) Sei p eine Primzahl. Der Ring $\mathbb{Z}/p^n$ hat nur das Primideal (p), hat also Dimension 0.
(4) Ein Hauptidealring hat Dimension 1.
(5) Sei R ein Ring und $R_0 = R/\mathcal{N}(R)$ der maximale reduzierte Quotient. Dann ist die induzierte Abbildung
$$\mathrm{Spec}(R_0) \xrightarrow{\sim} \mathrm{Spec}(R)$$
bijektiv und daher
$$\dim(R) = \dim(R_0).$$
(6) Wir sehen später, daß für einen Körper k gilt
$$\dim(k[X_1, \ldots, X_n]) = n,$$
so wie es für den Ring der algebraischen Funktionen auf $\mathbb{A}^n_k$ sein soll. Im Moment gibt uns die Kette von Primidealen
$$(0) \subseteq (X_1) \subseteq \ldots \subseteq (X_1, \ldots, X_i) \subseteq \ldots \subseteq (X_1, \ldots, X_n)$$
die Abschätzung $\dim(k[X_1, \ldots, X_n]) \geq n$.

Übungsaufgaben zu §7

Übungsaufgabe 7.1. Sei k ein algebraisch abgeschlossener Körper. Sei $f : V \to V$ ein endlichdimensionaler k-Vektorraum. Betrachten wir V als $k[X]$-Modul, indem wir X durch f wirken lassen. Dann ist
$$\mathrm{supp}(V) = \{(X - a) \ ; \ a \text{ ist Eigenwert von } f\}.$$
Tipp: Die Primideale von $k[X]$ sind (0) und die Ideale $(X - a)$ für $a \in k$.

Übungsaufgabe 7.2. Sei R ein Ring und $f \in R$. Zeigen Sie: $D(f) = \emptyset \iff f$ ist nilpotent.

Übungsaufgabe 7.3. Sei R ein Ring und $f, g \in R$ mit $D(f) \subseteq D(g)$. Zeigen Sie:
(1) Das Bild von g in R_f ist eine Einheit.
(2) Es gibt einen eindeutigen R-Algebrahomomorphismus $R_g \to R_f$.

Übungsaufgabe 7.4. Sei R ein Ring und $f, g \in R$. Zeigen Sie:
$$D(f) = D(g) \iff R_f = R_g \text{ als Lokalisierung von } R.$$

Teil 2. Kettenbedingungen

Die Welt allgemeiner Ringe ist ein Dschungel. Um ein wenig Licht und Ordnung zu schaffen, muß man zunächst Ringe mit gewissen Endlichkeitsbedingungen verstehen. Vor Emmy Noether betrieb man die Theorie der Ringe vornehmlich in zwei Fällen:

(1) **geometrischer Fall**: für endlich erzeugte Algebren über einem Körper k. Das sind die Faktorringe des Polynomrings $k[X_1, \ldots, X_n]$.
(2) **arithmetischer Fall**: für endlich erzeugte $\mathbb{Z}$-Algebren, die Unterringe von endlichen Körpererweiterungen $K/\mathbb{Q}$ sind.

Mit Emmy Noether hält die konzeptionelle begriffliche Denkweise Einzug in die Algebra. Bei manchen gilt daher Emmy Noether als Begründerin der modernen Algebra.

8. Noethersch

Anstelle der Endlichkeitsbedingungen im geometrischen/arithmetischen Fall treten nun Kettenbedingungen in den Vordergrund.

8.1. Noethersche Moduln und Ringe.

Definition 8.1. Ein **noetherscher** R-Modul ist ein R-Modul M, so daß die folgenden äquivalenten Bedingungen gelten

(a) Jeder R-Untermodul von M ist endlich erzeugt.
(b) Jede **aufsteigende Kette**
$$N_1 \subseteq N_2 \subseteq \ldots \subseteq N_i \subseteq N_{i+1} \subseteq \ldots$$
von R-Untermoduln von M wird stationär, d.h., es gibt $i_0 \in \mathbb{N}$, so daß für alle $i \geq i_0$ gilt $N_i = N_{i_0}$.
(c) Jede nichtleere Teilmenge von R-Untermoduln von M hat ein maximales Element bezüglich Inklusion.

Ein **noetherscher** Ring ist ein Ring R, der als Modul über R ein noetherscher R-Modul ist.

Bemerkung 8.2. (1) Die Ideale eines Rings sind genau die Untermoduln. Daher ist ein Ring R genau dann noethersch, wenn die folgenden äquivalenten Bedingungen gelten
   (a) Jedes Ideal von R ist endlich erzeugt.
   (b) Jede **aufsteigende Kette**
   $$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \ldots$$
   von Idealen von R wird stationär, d.h., es gibt $n_0 \in \mathbb{N}$, so daß für alle $n \geq n_0$ gilt $\mathfrak{a}_n = \mathfrak{a}_{n_0}$.
   (c) Jede nichtleere Teilmenge von Idealen von R hat ein maximales Element bezüglich Inklusion.
(2) Damit ein R-Modul noethersch ist, muß R kein noetherscher Ring sein.

Bemerkung 8.3. Definition 8.1 geht fahrlässig mit dem Begriff der Kette um. Korrekt müßte man unter (b) behaupten:

(b') Es gibt keine unendlich **aufsteigende Kette**
$$N_1 \subseteq N_2 \subseteq \ldots \subseteq N_i \subseteq N_{i+1} \subseteq \ldots$$
von R-Untermoduln von M.

Ketten sind nämlich mit echten Inklusionen definiert und können somit gar nicht stationär werden. In der Praxis hat man aber oft die Situtaion einer aufsteigenden Folge von Untermoduln, die dann nach (b) oder (b') stationär werden muß. Die Formulierung von (b) ist zwar unpräzise dafür aber näher an der Anwendung.

Definition 8.1 ist wohldefiniert. (a) $\Longrightarrow$ (b): Die Vereinigung $N = \bigcup_i N_i$ ist auch ein Untermodul von M. Somit ist N endlich erzeugt, sagen wir von $x_1, \ldots, x_r \in M$. Für $i_0 \gg 0$ gilt bereits $x_\alpha \in N_{i_0}$ für alle $1 \leq \alpha \leq r$. Dann ist aber für alle $j \geq i_0$

$$N_j \subseteq N = \langle x_1, \ldots, x_r \rangle_R \subseteq N_{i_0} \subseteq N_j.$$

Es gilt daher Gleichheit und die Kette ist ab i_0 stationär.

(b) $\Longrightarrow$ (c): Wegen (b) ist jede nichtleere Menge von Untermoduln bezüglich Inklusion induktiv geordnet. Die obere Schranke einer Kette (N_i) ist N_j für $j \gg 0$. Nach dem Lemma von Zorn gibt es daher maximale Elemente.

(c) $\Longrightarrow$ (a): Wir betrachten die Menge der endlich erzeugten Untermoduln von M:

$$\mathscr{U} = \{N \subseteq M \ ; \ N \text{ endlich erzeugter } R\text{-Modul}\}.$$

Nach (c) gibt es darin ein maximales Element. Dies sei $M_0 \subseteq M$. Wenn $x \in M \setminus M_0$, dann ist $M_1 := M_0 + Rx \subseteq M$ auch endlich erzeugt und enthält M_0. Weil M_0 maximal ist, folgt $M_0 = M_1$ und daher $x \in M_0$, Widerspruch. Es gibt deshalb kein solches x und $M = M_0$ ist endlich erzeugt. □

Beispiel 8.4. (1) Hauptidealringe sind noethersch, insbesondere sind $\mathbb{Z}$ und $k[X]$ für einen Körper k noethersch.

(2) Körper und allgemeiner endliche k-Algebren A, d.h., $\dim_k(A) < \infty$ als k-Vektorraum, sind noethersch. Ideale sind insbesondere auch Untervektorräume und da erlaubt die Dimension keine unendlichen aufsteigenden Ketten.

(3) Sei $k_0 \subseteq k$ ein Teilkörper. Wir betrachten den Ring

$$R = k_0 \oplus X \cdot k[X] = \{f \in k[X] \ ; \ f(0) \in k_0\}.$$

Wenn $[k : k_0] = \infty$, dann ist R nicht noethersch. Das Ideal $\mathfrak{a} = X \cdot k[X] \subseteq R$ ist dann nicht endlich erzeugt. Andernfalls wäre auch der Faktormodul

$$M = X \cdot k[X]/X^2 \cdot k[X] \simeq k$$

als R-Modul endlich erzeugt. Nun operiert R auf M vermöge der Auswertung $R \twoheadrightarrow k_0$ in 0 gegeben durch $f \mapsto f(0)$. Also ist M ein k_0-Vektorraum und Erzeuger als R-Modul sind genau Erzeuger als k_0-Vektorraum. Aber nach Voraussetzung ist $[k : k_0] = \dim_{k_0} k = \infty$ und damit M als R-Modul nicht endlich erzeugt.

Das Beispiel zeigt, daß für Unterring $A \subseteq B$ aus B noethersch nicht A noethersch folgt.

Proposition 8.5. *Sei* $0 \to M' \to M \to M'' \to 0$ *eine kurze exakte Sequenz von* R*-Moduln. Dann gilt*

$$M \text{ noethersch} \iff M' \text{ und } M'' \text{ noethersch.}$$

Beweis. Sei M noethersch. Jede aufsteigende Kette von Untermoduln von M' ist auch eine in M und wird damit stationär. Jede aufsteigende Kette von Untermoduln von M'' ist Bild einer Kette in M. Diese wird stationär, also wird auch ihr Bild stationär. Damit sind M' und M'' noethersch.

Seien nun M' und M'' noethersch. Sei (N_i) eine Kette von Untermoduln von M. Wir setzen $N_i' = N_i \cap M'$ und $N_i'' = \operatorname{im}(N_i \to M'')$. Dann ist $0 \to N_i' \to N_i \to N_i'' \to 0$ kurz exakt. Die Inklusionen $N_i \to N_{i+1}$ definieren Morphismen kurzer exakter Sequenzen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N_i' & \longrightarrow & N_i & \longrightarrow & N_i'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_{i+1}' & \longrightarrow & N_{i+1} & \longrightarrow & N_{i+1}'' & \longrightarrow & 0,
\end{array}$$

und zwar sind alle vertikalen Morphismen Inklusionen von Untermoduln von M' bzw. M bzw. M''. Die äußeren Inklusionen sind für $i \gg 0$ Isomorphismen, da die Ketten (N_i') und (N_i'') stationär werden. Nach dem 5er-Lemma wird dann auch die mittlere Inklusion ein Isomorphismus, also (N_i) wird stationär. □

Korollar 8.6. *Sei R ein Ring.*

(1) Für R-Moduln M_i, $1 \leq i \leq r$ gilt

$$\bigoplus_{i=1}^{r} M_i \text{ noethersch} \iff M_i \text{ noethersch für alle } 1 \leq i \leq r.$$

(2) Untermoduln noetherscher Moduln sind noethersch.
(3) Faktormoduln noetherscher Moduln sind noethersch.
(4) Sei R noetherscher Ring. Dann gilt

$$M \text{ noethersch} \iff M \text{ endlich erzeugt.}$$

Beweis. (1) Dies folgt per Induktion über die Anzahl der Summanden aus Proposition 8.5 angewandt auf die kurze exakte Sequenz $0 \to M' \to M' \oplus M'' \to M'' \to 0$.

(2) (bzw. (3)): Jeder Untermodul $M' \subseteq M$ (bzw. jeder Faktormodul $M \twoheadrightarrow M''$) sitzt in einer kurzen exakten Sequenz

$$0 \to M' \to M \to M'' \to 0.$$

Die Aussage folgt damit sofort aus Proposition 8.5.

(4) Wenn M noethersch ist, so auch endlich erzeugt per Definition. Sei also M endlich erzeugt. Zunächst ist nach (1) für jedes $n \in \mathbb{N}$ der R-Modul R^n noethersch. Endlich erzeugt bedeutet, daß es eine Surjektion $R^n \twoheadrightarrow M$ gibt. Damit ist M noethersch nach (3). □

Satz 8.7. *Sei R ein noetherscher Ring.*

(1) Für jedes Ideal $\mathfrak{a} \subseteq R$ ist $R/\mathfrak{a}$ noethersch.
(2) Für jedes multiplikative System $S \subseteq R$ ist $S^{-1}R$ noethersch.

Beweis. Aussage (1) folgt sofort aus Korollar 8.6: der Ring $R/\mathfrak{a}$ ist als R-Modul noethersch. Somit ist jeder Untermodul als R-Modul endlich erzeugt, und dann auch als $R/\mathfrak{a}$-Modul.

(2) Nach Proposition 6.23 ist jedes Ideal $\mathfrak{b} \subseteq S^{-1}R$ von der Form $\mathfrak{b} = S^{-1}\mathfrak{a}$ für ein Ideal $\mathfrak{a} \subseteq R$. Erzeugen $x_1, \ldots, x_r \in \mathfrak{a}$ das Ideal R, dann erzeugen $\frac{x_i}{1}$ mit $1 \leq i \leq r$ das Ideal $S^{-1}\mathfrak{a}$. □

Bemerkung 8.8. Warnung: noethersch ist keine lokale Eigenschaft. Zwar sind die lokalen Ringe $R_\mathfrak{p}$ eines noetherschen Rings R wieder noethersch nach Satz 8.7, aber die Umkehrung gilt nicht. Ein Beispiel hierfür ist mit einem beliebigen Körper k der Ring

$$R = \prod_{n \in \mathbb{Z}} k.$$

Theorem 8.9 (Hilbertscher Basissatz)**.** *R noethersch $\implies R[X]$ noethersch.*

Beweis. Sei $\mathfrak{a} \subseteq R[X]$ ein Ideal. Wir setzen für alle $n \geq 0$

$$\mathfrak{a}_n := \{a \in R \,;\ \text{es gibt } f \in \mathfrak{a} \text{ mit } f = aX^n + \text{ kleinere Grade}\}.$$

Dann ist offensichtlich $\mathfrak{a}_n \subseteq R$ ein Ideal. Weil man ein $f = aX^n + \ldots \in \mathfrak{a}$ mit X multiplizieren kann, bilden die $\mathfrak{a}_i$ eine Kette

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \ldots$$

von Idealen in R. Weil R noethersch ist, wird diese Kette stationär, etwa ab $\mathfrak{a}_d$, und es gibt $a_i \in R$ mit

$$\mathfrak{a}_d = \bigcup_{n \geq 0} \mathfrak{a}_n = \langle a_1, \ldots, a_r \rangle_R.$$

Zeugen für $a_i \in \mathfrak{a}_d$ seien gegeben durch $f_i \in \mathfrak{a}$ mit

$$f_i = a_i X^d + \text{ kleinere Grade.}$$

Der R-Modul

$$\mathfrak{b} = \{f \in \mathfrak{a} \ ; \ \deg(f) < d\} \subseteq \bigoplus_{\alpha=0}^{d} R \cdot X^\alpha \simeq R^d$$

ist als Untermodul eines noetherschen Moduls isomorph zu R^d als R-Modul endlich erzeugt. Damit ist

$$\mathfrak{a}' = \mathfrak{b} \cdot R[X] + \langle f_1, \ldots, f_r \rangle_{R[X]} \subseteq \mathfrak{a}$$

als $R[X]$-Modul endlich erzeugt. Es bleibt $\mathfrak{a}' = \mathfrak{a}$ zu zeigen.

Sei $f \in \mathfrak{a}$ beliebig. Wir zeigen per Induktion über $e = \deg(f)$, daß $f \in \mathfrak{a}'$. Wenn $\deg(f) < d$, ist nichts zu zeigen. Andernfalls schreiben wir

$$f = aX^e + \text{ kleinere Grade}$$

mit $a \in \mathfrak{a}_e = \mathfrak{a}_d$. Dann gibt es $\lambda_i \in R$ mit $a = \sum_{i=1}^r \lambda_i a_i$. Sei

$$g = f - \sum_{i=1}^{r} \lambda_i X^{e-d} f_i \in \mathfrak{a}.$$

Die Terme vom höchsten Grad X^e heben sich weg und

$$\deg(g) = \deg(aX^e - \sum_{i=1}^{r} \lambda_i a_i X^e + \text{ kleinere Grade}) < \deg(f) = e.$$

Per Induktion ist $g \in \mathfrak{a}'$ und damit auch $f \in \mathfrak{a}'$. □

Korollar 8.10. *Sei R noethersch und A eine endlich erzeugte R-Algebra. Dann ist A auch noethersch und endlich präsentierte R-Algebra. Für jeden surjektiven R-Algebrahomomorphismus*

$$\varphi : R[X_1, \ldots, X_n] \twoheadrightarrow A$$

ist $\ker(\varphi)$ *endlich erzeugt als Ideal in* $R[X_1, \ldots, X_n]$.

Beweis. Per Induktion nach der Anzahl der Variablen ist nach Theorem 8.9 auch $R[X_1, \ldots, X_n]$ noethersch. Satz 8.7 zeigt, daß Faktorringe von $R[X_1, \ldots, X_n]$ dann auch noethersch sind. Dies sind genau die endlich erzeugten R-Algebren.

Der Kern $\ker(\varphi)$ ist als Ideal im noetherschen Ring $R[X_1, \ldots, X_n]$ endlich erzeugt, damit A endlich präsentiert. □

Theorem 8.11 (Hilbertscher Basissatz für Potenzreihen)**.** *R noethersch $\Longrightarrow$ $R[[X]]$ noethersch.*

Beweis. Der Beweis ist ähnlich zum Beweis des Hilbertschen Basissatzes, Theorem 8.9. Für ein Ideal $\mathfrak{a} \subseteq R[[X]]$ betrachten wir zu $n \geq 0$ das Ideal

$$\mathfrak{a}_n = \{a \in R \ ; \ \text{ es gibt } f = aX^n + \text{höhere Grade} \in \mathfrak{a}\}$$

von R. Dann ist wieder

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \ldots$$

eine Kette von Idealen in R und wird demnach stationär, etwa ab $\mathfrak{a}_d$. Seien für $i = 1, \ldots, r$

$$f_i = a_i X^d + \text{höhere Grade} \in \mathfrak{a}$$

mit

$$\mathfrak{a}_d = \langle a_1, \ldots, a_r \rangle_R.$$

Der R-Modul

$$\mathfrak{b} = \mathrm{im}(\mathfrak{a} \subseteq R[[X]] \twoheadrightarrow R[[X]]/(X^d)) \subseteq R[[X]]/(X^d) \simeq \bigoplus_{i=0}^{d-1} R \cdot X^i \simeq R^d$$

ist endlich erzeugt. Seien $g_1, \dots g_s \in \mathfrak{a}$ Urbilder von Erzeugern. Dann ist

$$\mathfrak{a}' = \langle f_1, \dots, f_r, g_1, \dots, g_s \rangle_{R[X]} \subseteq \mathfrak{a}$$

ein endlich erzeugter $R[X]$-Modul, und es bleibt $\mathfrak{a} = \mathfrak{a}'$ zu zeigen.

Sei $f \in \mathfrak{a}$ beliebig. Es gibt eine R-Linearkombination der g_i, so daß $g = \sum_{i=1}^s \lambda_i g_i$ und f dasselbe Bild in $R[[X]]/(X^d)$ haben, also dieselben Koeffizienten in Graden $< d$. Es reicht zu zeigen, daß $f - g \in \mathfrak{a}'$. Wir dürfen also ohne Einschränkung annehmen, daß

$$f = \sum_{i=d}^{\infty} c_i \cdot X^i \in \mathfrak{a} \cap X^d R[[X]].$$

Wir konstruieren nun rekursiv $\mu_{ij} \in R$ für $i = 1, \dots r$ und $j \geq 0$, so daß für alle $e \geq 0$ gilt

$$f - \sum_{i=1}^{r} (\sum_{j=0}^{e} \mu_{ij} X^j) f_i \in X^{d+e+1} R[[X]],$$

Zu Anfang gilt dies für $e = -1$ und der leeren Summe in j. Wenn μ_{ij} bereits für $j < e$ konstruiert ist, so daß

$$f - \sum_{i=1}^{r} (\sum_{j=0}^{e-1} \mu_{ij} X^j) f_i = \gamma_{d+e} X^{d+e} + \text{höhere Ordnung } \in X^{d+e} R[[X]],$$

so ist $\gamma_{d+e} \in \mathfrak{a}_{d+e} = \mathfrak{a}_d$ und wir bestimmen $\mu_{ie} \in R$ passend durch

$$\gamma_{d+e} = \sum_{i=1}^{r} \mu_{ie} a_i,$$

denn dann gilt modulo $X^{d+e+1} R[[X]]$

$$f - \sum_{i=1}^{r} (\sum_{j=0}^{e} \mu_{ij} X^j) f_i \equiv \gamma_{d+e} X^{d+e} - \big(\sum_{i=1}^{r} \mu_{ie} X^e f_i \big) \equiv \big(\gamma_{d+e} - \sum_{i=1}^{r} \mu_{ie} a_i \big) X^{e+d} \equiv 0.$$

Wir setzen nun

$$h_i = \sum_{j \geq 0} \mu_{ij} X^j$$

und finden

$$f = \sum_{i=1}^{r} h_i f_i,$$

denn per Konstruktion ist

$$f - \sum_{i=1}^{r} h_i f_i \in \bigcap_{e \geq 0} X^{d+e} R[[X]] = \{0\}.$$

Dies zeigt $f \in \mathfrak{a}'$. □

Der folgende Satz illustriert, wie man von der Eigenschaft noethersch Gebrauch machen kann.

Satz 8.12 (reduzierte Primärzerlegung)**.** *Sei R ein noetherscher Ring.*

(1) R hat nur endlich viele minimale Primideale.

*(2) Jedes Ideal $\mathfrak{a} \subseteq R$ hat nur endlich viele **minimale Primoberideale**, d.h., es gibt nur endlich viele bezüglich Inklusion minimalen Elemente in $V(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) \ ; \ \mathfrak{a} \subseteq \mathfrak{p}\}$.*

Beweis. (1) ist der Spezialfall $\mathfrak{a} = (0)$ von (2). Aber (2) für das Ideal $\mathfrak{a}$ folgt aus (1) für den Ring $R/\mathfrak{a}$, der auch noethersch ist. Somit sind die Aussagen (1) und (2) auf formaler Ebene äquivalent. Der Beweis läuft nun wider Erwarten nicht über (1), sondern über die allgemeinere Aussage (2), weil man damit flexibler ist.

Der Beweis verwendet die wichtige Technik der **noetherschen Induktion**. Wir betrachten die Menge der Gegenbeispiele

$$\mathscr{B} = \{\mathfrak{a} \ ; \ \text{Ideal von } R \text{ mit unendlich vielen minimalen Primoberidealen}\}.$$

Angenommen $\mathscr{B}$ ist nicht leer. Weil R noethersch ist, gibt es dann ein maximales Gegenbeispiel $\mathfrak{a} \subseteq R$. Dann ist $\mathfrak{a}$ nicht Primideal, sonst wäre $\mathfrak{a}$ selbst das einzige minimale Primoberideal von $\mathfrak{a}$. Deshalb gibt es Zeugen $x, y \in R$ mit $x, y \notin \mathfrak{a}$ aber $xy \in \mathfrak{a}$. Betrachten wir $\mathfrak{b} = \mathfrak{a} + Rx$ und $\mathfrak{c} = \mathfrak{a} + Ry$. Dann ist für jedes Primideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$ auch $xy \in \mathfrak{p}$, also $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Daraus folgt $\mathfrak{b} \subseteq \mathfrak{p}$ oder $\mathfrak{c} \subseteq \mathfrak{p}$, kurz

$$V(\mathfrak{a}) \subseteq V(\mathfrak{b}) \cup V(\mathfrak{c}).$$

Die minimalen Primoberideale von $\mathfrak{a}$ sind also unter den minimalen Primoberidealen von $\mathfrak{b}$ oder von $\mathfrak{c}$ zu finden. Weil $\mathfrak{b}$ und $\mathfrak{c}$ echt größer sind als $\mathfrak{a}$, haben $\mathfrak{b}$ und $\mathfrak{c}$ jeweils nur endlich viele minimale Primoberideale, und damit dann auch $\mathfrak{a}$, Widerspruch. □

Abschließend geben wir noch eine verblüffende Charakterisierung noetherscher Ringe, die nur Primideale behandelt.

Satz 8.13 (Cohen)**.** *Ein Ring R ist genau dann noethersch, wenn alle $\mathfrak{p} \in \operatorname{Spec}(R)$ endlich erzeugt sind.*

Beweis. Wir müssen offensichtlich nur zeigen, daß alle Ideale von R endlich erzeugt sind, sobald alle Primideale endlich erzeugt sind. Dazu betrachten wir die Menge der Gegenbeispiele

$$\mathscr{M} = \{\mathfrak{a} \subseteq R \ ; \ \mathfrak{a} \text{ nicht endlich erzeugt}\},$$

die bezüglich Inklusion induktiv geordnet ist. Eine obere Schranke zu einer Kette $(\mathfrak{a}_i)$ ist die Vereinigung $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$. Zuerst ist $\mathfrak{a}$ wieder ein Ideal. Sodann ist $\mathfrak{a} \in \mathscr{M}$, also selbst nicht endlich erzeugt, weil sonst Erzeuger $x_1, \ldots, x_r$ von $\mathfrak{a}$ existieren, die dann für $i \gg 0$ bereits alle in $\mathfrak{a}_i$ liegen und dann $\mathfrak{a}_i = \mathfrak{a}$ gilt. Somit wäre auch $\mathfrak{a}_i$ endlich erzeugt, Widerspruch.

Wenn R nicht noethersch ist, dann ist $\mathscr{M}$ nicht leer und nach dem Lemma von Zorn gibt es maximale Elemente in $\mathscr{M}$. Sei $\mathfrak{a}$ ein solches maximales. Da Primideale alle endlich erzeugt sind, kann $\mathfrak{a}$ kein Primideal sein. Es gibt also $x, y \in R$ mit $xy \in \mathfrak{a}$ und $x, y \notin \mathfrak{a}$. Insbesondere ist $\mathfrak{b} = \mathfrak{a} + Rx$ echt größer als $\mathfrak{a}$ und damit endlich erzeugt. Durch Subtraktion geeigneter Vielfache von x findet man

$$\mathfrak{b} = \langle f_1, \ldots, f_n, x \rangle_R$$

mit Erzeugern $f_i \in \mathfrak{a}$. Betrachten wir nun das Ideal

$$\mathfrak{c} = (\mathfrak{a} : x) = \{c \in R \ ; \ cx \in \mathfrak{a}\}.$$

Es gilt $\mathfrak{a} + Ry \subseteq \mathfrak{c}$ und daher ist $\mathfrak{c}$ auch endlich erzeugt. Sei $\mathfrak{c} = \langle g_1, \ldots, g_m \rangle_R$. Dann ist $g_j x \in \mathfrak{a}$ für alle $1 \leq j \leq m$ und es gilt

$$\mathfrak{a}_0 := \langle f_1, \ldots, f_n, g_1 x, \ldots, g_m x \rangle_R \subseteq \mathfrak{a}.$$

Es gilt sogar $\mathfrak{a} = \mathfrak{a}_0$, denn zu $f \in \mathfrak{a}$ gibt es $a_i \in R$ und $g \in R$ mit

$$f = a_1 f_1 + \ldots + a_n f_n + gx.$$

Damit ist $g \in \mathfrak{c}$ und es gibt $b_j \in R$ mit $g = b_1 g_1 + \ldots + b_m g_m$. Zusammen macht das

$$f = a_1 f_1 + \ldots + a_n f_n + b_1(g_1 x) + \ldots + b_m(g_m x) \in \mathfrak{a}_0$$

wie behauptet.

Aber damit ist $\mathfrak{a}$ doch endlich erzeugt, Widerspruch. □

8.2. **Etwas affine algebraische Geometrie.** Der affine n-dimensionale Raum über dem Körper K ist die Menge

$$\mathbb{A}^n(K) := K^n.$$

Definition 8.14. Sei k ein Körper und K/k eine Körpererweiterung mit K algebraisch abgeschlossen. Eine **k-algebraische Menge in** $\mathbb{A}^n(K)$ ist eine Teilmenge der folgenden Form. Es gibt eine Menge I und eine Familie $f_i \in k[X_1, \ldots, X_n]$ von Polynomen für $i \in I$ mit

$$X = V(\{f_i \ ; \ i \in I\})(K) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n(K) \ ; \ f_i(a_1, \ldots, a_n) = 0 \text{ für alle } i \in I\} \subseteq \mathbb{A}^n(K).$$

Notation 8.15. Zur Vereinfachung der Notation schreiben wir auch

$$V(f_i \ ; \ i \in I) = V(\{f_i \ ; \ i \in I\})(K),$$

insbesondere, wenn wir die Körpererweiterung K/k implizit als gegeben ansehen und nicht in der Notation betonen wollen.

Bemerkung 8.16. Mit andern Worten ist eine k-algebraische Menge die gemeinsame Nullstellenmenge einer Familie von Polynomen.

Beispiel 8.17. (1) Die Gleichung $XY = 1$ führt zur k-algebraischen Teilmenge

$$V(XY - 1) \subseteq \mathbb{A}^2(K).$$

Lösungen (x, y) sind $x \in K^\times$ und $y = x^{-1}$. Die Projektion auf die erste (oder die zweite) Koordinate liefert eine Bijektion

$$V(XY - 1) \simeq K^\times.$$

(2) Sei $f \in k[X_1, \ldots, X_n]$ aufgefaßt als Polynom in den Variablen $X_1, \ldots, Y = X_{n+1}$. Die Gleichung $f(X_1, \ldots, X_n)Y = 1$ führt zur k-algebraischen Teilmenge

$$V(Yf(X_1, \ldots, X_n) - 1) \subseteq \mathbb{A}^{n+1}(K).$$

Lösungen $(x_1, \ldots, x_n, y)$ haben die Form $f(x_1, \ldots, x_n) \neq 0$ und $y = f(x_1, \ldots, x_n)^{-1}$. Die Projektion auf die ersten n Koordinaten liefert eine Bijektion

$$V(Yf(X_1, \ldots, X_n) - 1) \simeq \mathbb{A}^n(K) \setminus V(f).$$

(3) Bei den bisherigen Beispielen sieht man nicht ein, warum man die Lösungen nur in einem affinen Raum zu einem algebraisch abgeschlossenen Körper suchen soll. Seien nun konkret $k = \mathbb{R}$ und $K = \mathbb{C}$.

Die Gleichung $X^2 + Y^2 = 1$ führt zur $\mathbb{R}$-algebraischen Menge

$$V(X^2 + Y^2 - 1) \subseteq \mathbb{A}^2(\mathbb{C}).$$

Die reellen Lösungen bilden den Einheitskreis

$$\mathrm{S}^1 = \{(x, y) \in \mathbb{R}^2 \ ; \ x^2 + y^2 = 1\} \subseteq \mathbb{R}^2$$

Die komplexen Lösungen beschreibt man am besten durch die (invertierbare) Substitution $U = X + iY$ und $V = X - iY$, welche die Gleichung zu

$$UV = 1$$

transformiert. Somit ist die Abbildung

$$\begin{aligned} u : V(X^2 + Y^2 - 1) &\to \mathbb{C}^\times \\ (x, y) &\mapsto u(x, y) = x + iy \end{aligned}$$

eine Bijektion. Geometrisch ist dies die Riemannsche Zahlenkugel ohne Nord- und Südpol, in der die reellen Lösungen den Äquator bilden.

Im komplexen Bild sieht man, daß die Lösungsmenge einen freien Parameter hat (der nur 0 nicht annehmen darf). Das sieht man im reellen Bild nicht.

(4) Wir behalten $k = \mathbb{R}$ und $K = \mathbb{C}$. Die Gleichung $X^2 + Y^2 = 0$ führt zur $\mathbb{R}$-algebraischen Menge

$$V(X^2 + Y^2) \subseteq \mathbb{A}^2(\mathbb{C}).$$

Es gibt mit $(0,0)$ nur eine reelle Lösung. Trotzdem beschreibt die Gleichung etwas Eindimensionales, doch dies tritt nur komplex zum Vorschein. Die komplexen Lösungen beschreibt man am besten durch die (invertierbare) Substitution $U = X+iY$ und $V = X-iY$, welche die Gleichung zu

$$UV = 0$$

transformiert. Somit bestehen die komplexen Lösungen (in Koordinaten U, V) aus zwei Geraden $(u, 0)$ mit $u \in \mathbb{C}$ und $(0, v)$ mit $v \in \mathbb{C}$, die sich in $(0, 0)$ schneiden.

Proposition 8.18. *Die k-algebraischen Teilmengen von $\mathbb{A}^n(K)$ sind die abgeschlossenen Teilmengen einer Topologie auf $\mathbb{A}^n(K)$, genannt die **Zariski–Topologie**. Es gilt:*

(1) $\emptyset$ und $\mathbb{A}^n(K)$ sind k-algebraische Teilmengen.

(2) Sind $F_i \subseteq k[X_1, \ldots, X_n]$ für $i \in I$ Mengen von Polynomen, dann ist

$$\bigcap_i V(F_i)$$

auch k-algebraisch.

(3) Sind $F_1, \ldots, F_m \subseteq k[X_1, \ldots, X_n]$ endlich viele Teilmengen von Polynomen, dann ist

$$\bigcup_i V(F_i)$$

auch k-algebraisch.

Beweis. (1) Es gilt $V(1) = \emptyset$ und $V(0) = \mathbb{A}^n(K)$.

(2) Mit $F = \bigcup_i F_i$ gilt offensichtlich

$$V(F) = \bigcap_i V(F_i).$$

(3) Sei $F = \{\prod_{i=1}^m f_i \ ; \ f_i \in F_i \text{ für alle } i = 1, \ldots, m\}$. Dann ist

$$V(F) = \bigcup_{i=1}^m V(F_i).$$

Da

$$(\prod_{i=1}^m f_i)(a_1, \ldots, a_n) = \prod_{i=1}^m f_i(a_1, \ldots, a_n),$$

folgt sofort $V(F_i) \subseteq V(F)$. Zu zeigen ist also, daß jedes $(a_1, \ldots, a_n) \in V(F)$ in einem der $V(F_i)$ enthalten ist. Angenommen, dem ist nicht so. Dann gibt es für jeden Index i einen Zeugen $f_i \in F_i$ mit

$$f_i(a_1, \ldots, a_n) \neq 0.$$

Dann ist aber auch

$$(\prod_{i=1}^m f_i)(a_1, \ldots, a_n) \neq 0$$

im Widerspruch zu $(a_1, \ldots, a_n) \in V(F)$. □

Proposition 8.19. *Zur Beschreibung k-algebraischer Mengen reichen (Radikal-)Ideale.*

(1) Sei $f_i \in k[X_1, \ldots, X_n]$ für $i \in I$ eine Menge von Polynomen und $\mathfrak{a} = (f_i \ ; \ i \in I)$ das von ihnen erzeugte Ideal. Dann gilt

$$V(\mathfrak{a}) = V(f_i \ ; \ i \in I).$$

(2) Für jedes Ideal $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ gilt

$$V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}).$$

Beweis. (1) Offensichtlich gilt $V(\mathfrak{a}) \subseteq V(f_i \,;\, i \in I)$. Zu zeigen ist, daß eine gemeinsame Nullstelle $(a_1, \ldots, a_n)$ der f_i auch Nullstelle für jedes $f \in \mathfrak{a}$ ist. Aber f hat eine Darstellung als

$$f = \sum_i g_i f_i,$$

wobei alle bis auf endlich viele $g_i = 0$ sind, also eine endliche Summe vorliegt. Dann ist

$$f(a_1, \ldots, a_n) = \sum_i g_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) = 0.$$

(2) Offensichtlich gilt $V(\sqrt{\mathfrak{a}}) \subseteq V(\mathfrak{a})$. Zu zeigen ist, daß eine gemeinsame Nullstelle $(a_1, \ldots, a_n)$ aller Elemente von $\mathfrak{a}$ auch für $f \in \sqrt{\mathfrak{a}}$ eine Nullstelle ist. Nach Definition des Radikals gibt es $m \geq 1$ mit $f^m \in \mathfrak{a}$. Dann ist

$$f(a_1, \ldots, a_n)^m = (f^m)(a_1, \ldots, a_n) = 0,$$

und, weil K keine nilpotenten Elemente hat, folgt

$$f(a_1, \ldots, a_n) = 0$$

wie gewünscht. □

Korollar 8.20. *Jede k-algebraische Menge wird durch endlich viele Polynome beschrieben.*

Beweis. Jede k-algebraische Menge in $\mathbb{A}^n(K)$ ist für ein Ideal $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ von der Form $V(\mathfrak{a})$. Nach dem Hilbertschen Basissatz (Theorem 8.9) ist $\mathfrak{a}$ endlich erzeugt. Seien $f_1, \ldots, f_m$ Erzeuger von $\mathfrak{a}$. Dann ist $V(\mathfrak{a}) = V(f_1, \ldots, f_m)$. □

Definition 8.21. Das **Verschwindungsideal** einer k-algebraischen Menge $X \subseteq \mathbb{A}^n(K)$ ist das Ideal

$$I(X) = \{f \in k[X_1, \ldots, X_n] \,;\, f(a_1, \ldots, a_n) = 0 \text{ für alle } (a_1, \ldots, a_n) \in X\}.$$

Lemma 8.22. *Sei $X \subseteq \mathbb{A}^n(K)$ eine k-algebraische Menge.*

(1) $I(X)$ ist ein Ideal.
(2) $V(I(X)) = X$.
(3) $\sqrt{\mathfrak{a}} \subseteq I(V(\mathfrak{a}))$.

Beweis. (1) Seien $f_1, \ldots, f_m \in I(X)$ und $g_1, \ldots, g_m \in k[X_1, \ldots, X_n]$ beliebig. Dann verschwindet für alle $(a_1, \ldots, a_n) \in X$ auch

$$(\sum_i g_i f_i)(a_1, \ldots, a_n) = \sum_i g_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) = \sum_i g_i(a_1, \ldots, a_n) \cdot 0 = 0.$$

Also gehört auch $\sum_i g_i f_i$ zu $I(X)$.

(2) Per Definition ist $X \subseteq V(I(X))$. Sei $X = V(F)$ für eine Teilmenge $F \subseteq k[X_1, \ldots, X_n]$. Dann gilt offensichtlich $F \subseteq I(X)$ und

$$V(F) = X \subseteq V(I(X)) \subseteq V(F).$$

(3) Dies folgt aus $V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a})$: jedes $f \in \sqrt{\mathfrak{a}}$ verschwindet in den Punkten von $V(\mathfrak{a})$. □

8.3. **Vorbereitungen zum Hilbertschen Nullstellensatz.** Wir folgen der Strategie von Artin und Tate. Zuvor betrachten wir aber ein Beispiel, das auch im Beweis verwendet wird.

Lemma 8.23. *Sei k ein Körper. Der rationale Funktionenkörper $k(T)$ in einer Variablen T ist keine endlich erzeugte k-Algebra.*

Beweis. Angenommen die Elemente $f_1, \ldots, f_r \in k(T)$ erzeugen $k(T)$ als k-Algebra. Dann gibt es $g_i, h_i \in k[T]$ mit $f_i = g_i/h_i$. Die Nenner von Elementen im k-Algebraerzeugnis der f_i sind Teiler von f^n für $f = f_1 \cdot \ldots \cdot f_r$ und ein $n \geq 0$.

Sei $h \in K[T]$ ein irreduzibles Polynom, das kein Teiler von f ist, etwa ein irreduzibler Teiler von $f + 1$. Dann gibt es nach Annahme eine Darstellung

$$\frac{1}{h} = \frac{g}{f^n}$$

mit $n \in \mathbb{N}$ und $g \in k[T]$. Daraus folgt $f^n = hg$, und weil h irreduzibel (also prim) ist, sogar $h \mid f$ im Widerspruch zur Wahl von h. □

Definition 8.24. Eine **endliche** R-Algebra über dem Ring R ist eine R-Algebra A, die als R-Modul betrachtet endlich erzeugt ist.

Beispiel 8.25. Eine endliche R-Algebra ist automatisch eine endlich erzeugte R-Algebra, weil die R-Modulerzeuger auch R-Algebraerzeuger sind. Die Umkehrung gilt nicht, wie man an $R[X]$ sieht.

Wir haben bereits gesehen, daß ein Unterring eines noetherschen Rings selbst nicht noethersch zu sein braucht. Im Gegensatz dazu steht die folgende Proposition.

Proposition 8.26. *Sei A ein noetherscher Ring. Sei C eine endlich erzeugte A-Algebra und $B \subseteq C$ eine A-Unteralgebra, so daß C eine endliche B-Algebra ist.*

Dann ist B eine endlich erzeugte A-Algebra. Insbesondere ist B noethersch.

Beweis. Wir wählen $x_1, \ldots, x_n \in C$ Erzeuger als A-Algebra, d.h., der A-Algebrahomomorphismus

$$\begin{aligned} A[X_1, \ldots, X_n] &\twoheadrightarrow C \\ X_i &\mapsto x_i \end{aligned}$$

ist surjektiv. Wir wählen weiter $y_1, \ldots, y_m \in C$ Erzeuger als B-Modul, d.h.

$$C = By_1 + \ldots + By_m.$$

Dann gibt es Strukturkonstanten $b_{ij} \in B$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$ mit

$$x_i = \sum_{j=1}^{m} b_{ij} y_j$$

und $b_{ij}^k \in B$ für alle $1 \leq i, j, k \leq m$ mit

$$y_i y_j = \sum_{k=1}^{m} b_{ij}^k y_k. \tag{8.1}$$

Sei $B_0 \subseteq B$ die von allen b_{ij} und allen b_{ij}^k in B erzeugte A-Algebra. Nach Korollar 8.10 zum Hilbertschen Basissatz ist B_0 ein noetherscher Ring.

Wir dürfen nun A durch B_0 ersetzen, denn wenn B über B_0 als Algebra endlich erzeugt ist, dann auch als Algebra über A. Wir nehmen also nun an, daß $A \subseteq B \subseteq C$ und $b_{ij}, b_{ij}^k \in A$.

Da die A-Algebraerzeuger x_i von C nun A-Linearkombinationen der y_i sind, wird C auch von den $y_1, \ldots, y_m$ als A-Algebra erzeugt. Als A-Modul ist damit C von den Monomen

$$y^e = \prod_{i=1}^{m} y_i^{e_i}$$

mit dem Multiindex $e = (e_1, \ldots, e_m) \in \mathbb{N}_0^m$ erzeugt. Per Induktion über den Totalgrad

$$\deg(y^e) = \sum_{i=1}^{m} e_i$$

zeigt man mittels (8.1), daß schon die Monome vom Grad 1 als A-Modulerzeuger ausreichen. Damit ist C ein endlich erzeugter A-Modul. Weil A noethersch ist, ist C ein noetherscher A-Modul und der A-Untermodul B ist als A-Modul endlich erzeugt. Damit ist aber B erst recht als A-Algebra endlich erzeugt. □

Satz 8.27. *Sei K eine Körpererweiterung von k, die als k-Algebra endlich erzeugt ist. Dann ist K/k endlich algebraisch.*

Beweis. Seien $x_1, \ldots, x_n \in K$ Erzeuger als k-Algebra. Wir sortieren die x_i so, daß $x_1, \ldots, x_d$ algebraisch unabhängig über k sind, und die $x_{d+1}, \ldots, x_n$ algebraisch über dem Zwischenkörper

$$F = k(x_1, \ldots, x_d) \subseteq K.$$

Dabei ist F als Körper von den x_i mit $i \leq d$ erzeugt und ein rationaler Funktionenkörper in d Variablen.

Die Erweiterung K/F ist endlich erzeugt und algebraisch, also endlich. Nach Proposition 8.26 ist damit auch F als k-Algebra endlich erzeugt. Es reicht nun, K durch F zu ersetzen.

Wenn $d = 0$ und $F = k$ ist, sind wir fertig. Wir nehmen daher $d \geq 1$ an und setzen $k' = k(x_1, \ldots, x_{d-1}) \subseteq F$. Dann ist $F = k'(T)$ mit $T = x_d$ und erst recht als k'-Algebra endlich erzeugt. Dies widerspricht Lemma 8.23 und beendet so den Beweis. □

8.4. **Das Maximalspektrum.**

Notation 8.28. Die Menge der maximalen Ideale eines Rings R bezeichnen wir mit

$$\operatorname{Specmax}(R).$$

Ein surjektiver Ringhomomorphismus $i : A \twoheadrightarrow B$ induziert durch Urbildnehmen $\mathfrak{m} \mapsto i^{-1}(\mathfrak{m})$ eine Injektion

$$\operatorname{Specmax}(B) \hookrightarrow \operatorname{Specmax}(A).$$

Korollar 8.29. *Seien k ein Körper, A eine endlich erzeugte k-Algebra und $\mathfrak{m} \in \operatorname{Specmax}(A)$. Dann ist der Restklassenkörper $\kappa(\mathfrak{m}) = A/\mathfrak{m}$ eine endliche algebraische Erweiterung von k.*

Beweis. Als Quotient der endlich erzeugten k-Algebra ist $\kappa(\mathfrak{m})$ auch als k-Algebra endlich erzeugt. Damit folgt die Behauptung aus Satz 8.27. □

Theorem 8.30 (Hilbertscher Nullstellensatz, schwache Form)**.** *Sei K eine algebraisch abgeschlossene Erweiterung des Körpers k.*

(1) Die folgende Abbildung ist bijektiv:

$$\begin{aligned} \mathbb{A}^n(K) &\to \operatorname{Specmax}(K[X_1, \ldots, X_n]) \\ a = (a_1, \ldots, a_n) &\mapsto \mathfrak{m}_a := (X_1 - a_1, \ldots, X_n - a_n) \end{aligned}$$

(2) Sei $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ ein Ideal. Dann ist $\mathfrak{a} \otimes_k K$ ein Ideal von $K[X_1, \ldots, X_n]$ und es gibt ein kommutatives Diagramm mit natürlichen Abbildungen

$$\begin{array}{ccc} \operatorname{Specmax}(K[X_1, \ldots, X_n]/\mathfrak{a} \otimes_k K) & \xrightarrow{\subseteq} & \operatorname{Specmax}(K[X_1, \ldots, X_n]) \\ \downarrow \simeq & & \downarrow \simeq \\ V(\mathfrak{a}) & \xrightarrow{\subseteq} & \mathbb{A}^n(K) \end{array}$$

(3) (Existenz von Nullstellen) Sei $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ ein Ideal. Wenn $\mathfrak{a} \neq (1)$, dann ist

$$V(\mathfrak{a}) \neq \emptyset.$$

Beweis. (1) Sei $a = (a_1, \ldots, a_n) \in \mathbb{A}^n(K)$. Das Ideal $\mathfrak{m}_a = (X_1 - a_1, \ldots, X_n - a_n)$ ist in der Tat ein maximales Ideal, und zwar der Kern der Auswertung $P \mapsto P(a)$:

$$\begin{aligned} K[X_1, \ldots, X_n] &\twoheadrightarrow K \\ X_i &\mapsto a_i. \end{aligned}$$

Das sieht man wie folgt. Man ersetze in $P(X_1, \ldots, X_n)$ jeweils X_i durch $(X_i - a_i) + a_i$ und multipliziere aus. Dann wird P als Polynom in den $X_i - a_i$ geschrieben und einem konstanten Term $P(a)$, wie man durch Einsetzen bestätigt. Damit ist $P(a) = 0 \iff P \in \mathfrak{m}_a$.

Damit ist die Abbildung $a \mapsto \mathfrak{m}_a$ wohldefiniert. Wenn $\mathfrak{m}_a = \mathfrak{m}_b$, dann ist $(X - a_i)(b) = 0$ für alle i und somit $a_i = b_i$.

Sei nun $\mathfrak{m}$ ein beliebiges maximales Ideal von $K[X_1, \ldots, X_n]$. Dann ist $K[X_1, \ldots, X_n]/\mathfrak{m}$ eine endlich erzeugte K-Algebra, die ein Körper ist, somit nach Korollar 8.29 als K-Algebra eine endliche Körpererweierung von K. Weil K algebraisch abgeschlossen ist, folgt $K[X_1, \ldots, X_n]/\mathfrak{m} \simeq K$ als K-Algebra. Sei $a_i \in K$ das Bild von X_i unter diesem Isomorphismus. Dann ist $X - a_i \in \mathfrak{m}$ für alle $1 \leq i \leq n$, somit $\mathfrak{m}_a \subseteq \mathfrak{m}$ mit $a = (a_1, \ldots, a_n)$. Weil $\mathfrak{m}_a$ maximales Ideal ist, gilt sogar $\mathfrak{m} = \mathfrak{m}_a$. Dies zeigt (1).

(2) Jede Körpererweiterung ist flach, weil alle Moduln über Körpern frei sind und alle kurzen exakten Sequenzen spalten. Daher ist $- \otimes_k K$ exakt, und $\mathfrak{a} \otimes_k K$ ist ein Ideal von

$$K[X_1, \ldots, X_n] = k[X_1, \ldots, X_n] \otimes_k K.$$

Für das Diagramm ist nach (1) zu zeigen, daß ein maximales Ideal $\mathfrak{m}_a$ von $K[X_1, \ldots, X_n]$ das Ideal $\mathfrak{a} \otimes_k K$ enthält genau dann, wenn $a \in V(\mathfrak{a})$. Dies folgt sofort, weil $\mathfrak{m}_a$ der Kern der Auswertung in a ist.

(3) Nach (2) reicht es zu zeigen, daß $K[X_1, \ldots, X_n]/\mathfrak{a} \otimes_k K$ maximale Ideale hat. Aber jeder vom Nullring verschiedene Ring hat maximale Ideale. Da

$$A = K[X_1, \ldots, X_n]/\mathfrak{a} \otimes_k K = (k[X_1, \ldots, X_n]/\mathfrak{a}) \otimes_k K,$$

ist $A = 0$ genau dann, wenn $\mathfrak{a} = (1)$. □

Theorem 8.31 (Hilbertscher Nullstellensatz)**.** *Sei K eine algebraisch abgeschlossene Erweiterung des Körpers k. Die Abbildungen*

$$\{\mathfrak{a} \subseteq k[X_1, \ldots, X_n] \ ; \ \textit{Ideal}\} \underset{I(-)}{\overset{V(-)}{\rightleftarrows}} \{X \subseteq \mathbb{A}^n(K) \ ; \ \textit{k-algebraisch}\}$$

erfüllen für jedes Ideal $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ und jede k-algebraische Menge $X \subseteq \mathbb{A}^n(K)$

(1) $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$,
(2) $V(I(X)) = X$.

Beweis. (2) Die Aussage $V(I(X)) = X$ haben wir bereits in Lemma 8.22 bewiesen.

(1) Sei $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ ein beliebiges Ideal. Wir wissen bereits aus Lemma 8.22 (3) und Proposition 8.19

$$\sqrt{\mathfrak{a}} \subseteq I(V(\sqrt{\mathfrak{a}})) = I(V(\mathfrak{a})).$$

Zu zeigen ist also, daß jedes $f \in I(V(\mathfrak{a}))$ in $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ nilpotent ist. Dazu bemühen wir den Trick von Rabinovitch. Angenommen f ist nicht in A nilpotent. Dann ist $1 - fY \in A[Y]$ nach Satz 6.10 keine Einheit. Deshalb ist $(1 - fY) \subsetneq A[Y]$ ein echtes Ideal, genauso wie

$$\mathfrak{b} := \mathfrak{a} \cdot k[X_1, \ldots, X_n, Y] + (1 - fY) \cdot k[X_1, \ldots, X_n, Y] \subsetneq k[X_1, \ldots, X_n, Y].$$

Nach Theorem 8.30 (3) ist dann $V(\mathfrak{b}) \subseteq \mathbb{A}^{n+1}(K)$ nicht leer. Sei $P := (a_1, \ldots, a_n, b) \in V(\mathfrak{b})$. Weil für jedes $h \in \mathfrak{a} \subseteq \mathfrak{b}$ gilt

$$h(a_1, \ldots, a_n) = h(P) = 0,$$

folgt $(a_1, \ldots, a_n) \in V(\mathfrak{a})$. Damit verschwindet auch f in $(a_1, \ldots, a_n)$. Dann liefert

$$0 = (1 - fY)(P) = 1 - f(a_1, \ldots, a_n)b = 1 - 0 \cdot b = 1$$

einen Widerspruch. □

Korollar 8.32. *Seien k ein Körper, A eine endlich erzeugte k-Algebra und $\mathfrak{a} \subseteq A$ ein Ideal. Dann gilt*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m},\ \mathfrak{m} \in \operatorname{Specmax}(A)} \mathfrak{m}.$$

Insbesondere gilt $\operatorname{Rad}(A) = \mathscr{N}(A)$.

Beweis. Wir wählen eine Surjektion $\varphi : k[X_1, \ldots, X_n] \twoheadrightarrow A$ und setzen $\mathfrak{b} = \varphi^{-1}(\mathfrak{a})$. Die Aussage für $\mathfrak{a}$ folgt dann sofort aus der Aussage für $\mathfrak{b}$. Wir dürfen daher annehmen, daß $A = k[X_1, \ldots, X_n]$.

Weil Primideale Radikalideale sind und das Radikal mit Schnitten verträglich ist, gilt

$$\sqrt{\mathfrak{a}} \subseteq \sqrt{\bigcap_{\mathfrak{a} \subseteq \mathfrak{m},\ \mathfrak{m} \in \operatorname{Specmax}(A)} \mathfrak{m}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m},\ \mathfrak{m} \in \operatorname{Specmax}(A)} \sqrt{\mathfrak{m}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m},\ \mathfrak{m} \in \operatorname{Specmax}(A)} \mathfrak{m}.$$

Sei K ein algebraischer Abschluß von k. Die Auswertung in $P = (a_1, \ldots, a_n) \in V(\mathfrak{a})$ führt zu einem k-Algebrahomomorphismus

$$\operatorname{ev}_P : k[X_1, \ldots, X_n] \to K,$$

mit $\mathfrak{a} \subseteq \ker(\operatorname{ev}_P)$. Das Bild von ev_P ist eine endlich erzeugte k-Unteralgebra von K. Da K hier algebraisch über k ist, sind alle k-Unteralgebren selbst auch Körper. Damit ist $\ker(\operatorname{ev}_P)$ ein maximales Ideal von $k[X_1, \ldots, X_n]$, das $\mathfrak{a}$ enthält.

Sei nun $f \in \bigcap_{\mathfrak{a} \subseteq \mathfrak{m},\ \mathfrak{m} \in \operatorname{Specmax}(A)} \mathfrak{m}$. Dann folgt $f(P) = \operatorname{ev}_P(f) = 0$ für alle $P \in V(\mathfrak{a})$, also $f \in I(V(\mathfrak{a}))$. Nach Theorem 8.31 folgt $f \in \sqrt{\mathfrak{a}}$ und das war zu zeigen.

Die Behauptung über das Jacobsonradikal und das Nilradikal folgt als Spezialfall $\mathfrak{a} = (0)$. □

Definition 8.33. Ein **Jacobsonring** ist ein Ring R in dem für jedes Primideal $\mathfrak{p} \in \operatorname{Spec}(R)$ gilt

$$\mathfrak{p} = \bigcap_{\mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m},$$

wobei $\mathfrak{m}$ über maximale Ideale von R läuft.

Beispiel 8.34. (1) Für Jacobsonringe R kann man $\operatorname{Spec}(R)$ aus $\operatorname{Specmax}(R)$ zusammen mit der Zariski-Topologie rekonstruieren.

(2) Jedes Primideal ist sein eigenes Radikal. Daher sind nach Korollar 8.32 endlich erzeugte Algebren über einem Körper k Jacobsonringe. Solche Algebren beschreiben (affine) algebraische Geometrie über k. Daher reicht es oft, nur Punkte mit Werten in einer algebraisch abgeschlossenen Erweiterung K anzusehen, weil diese bereits alle maximalen Ideale der zugehörigen Algebren beschreiben.

(3) Der Potenzreihenring $k[[X]]$ ist kein Jacobsonring. Es gilt

$$\operatorname{Spec}(k[[X]]) = \{(0), (X)\},$$

und somit gibt es nur ein maximales Ideal. Das Primideal (0) ist nicht Schnitt von maximalen Idealen.

Bemerkung 8.35. Ein lokaler Ring $(R, \mathfrak{m})$ ist genau dann Jacobsonring, wenn $\operatorname{Spec}(R) = \{\mathfrak{m}\}$ nur aus einem Punkt besteht.

Übungsaufgaben zu §8

Übungsaufgabe 8.1. Man konstruiere ein Beispiel eines noetherschen R-Moduls für einen nichtnoetherschen Ring R.

Übungsaufgabe 8.2. Sei $(R, \mathfrak{m})$ ein lokaler Ring und $k = R/\mathfrak{m}$. Sei $k_0 \subseteq k$ ein Teilkörper. Wir setzen

$$R_0 = \{f \in R \; ; \; f(\mathfrak{m}) \in k_0\}.$$

Zeigen Sie die folgenden Aussagen.

(a) $\mathfrak{m} \subseteq R_0$ und $(R_0, \mathfrak{m})$ ist ein lokaler Ring mit Restklassenkörper k_0.
(b) R_0 ist nicht noethersch, wenn $[k : k_0] = \infty$.

Übungsaufgabe 8.3. Sei k ein Körper. Sei $R \subseteq k[X, Y]$ die k-Unteralgebra erzeugt von XY^i für alle $i \geq 0$. Zeigen Sie, daß R nicht noethersch ist.

Übungsaufgabe 8.4. (Ein nichtnoetherscher Ring mit noetherschen lokalen Ringen.) Es sei k ein Körper und

$$R = \prod_{n \in \mathbb{Z}} k$$

das direkte Produkt von mit $\mathbb{Z}$ indizierten identischen Faktoren k. Zeigen Sie entlang der folgenden Anleitung, daß R nicht noethersch ist, aber daß die Lokalisierung $R_\mathfrak{p}$ noethersch ist für jedes Primideal $\mathfrak{p}$ von R.

(a) Bestimmen Sie die Menge der Idempotenten in R, d.h. die Elemente $e \in R$ mit $e^2 = e$.
(b) Jedes Ideal von R wird durch die in ihm enthaltenen Idempotenten erzeugt.
(c) Jedes Primideal von R ist gleichzeitig maximal und minimal.
(d) $R_\mathfrak{p}$ ist reduziert.
(e) $R_\mathfrak{p}$ ist ein Körper, also noethersch.
(f) R ist nicht noethersch.

Bemerkung: Bei genauerem Hinsehen stellt man fest, daß Ideale gerade Filtern (siehe Bücher über Topologie) auf $\mathbb{Z}$ mit diskreter Topologie entsprechen. Dabei ist das Ideal genau dann ein Primideal, wenn es sich um einen maximalen Filter, einen Ultrafilter, handelt. $\mathrm{Spec}(R)$ entspricht also der Menge der Ultrafilter des diskreten topologischen Raums $\mathbb{Z}$. Dies ist ein kompakter topologischer Raum, die Stone-Čech-Kompaktifizierung von $\mathbb{Z}$, die $\mathbb{Z}$ enthält und damit kompaktifiziert.

Übungsaufgabe 8.5. Sei $R \neq 0$ ein noetherscher Ring. Dann ist $R[X_i; i \in \mathbb{N}]$ nicht noethersch.

Übungsaufgabe 8.6. Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale von $k[X_1, \ldots, X_n]$. Zeigen Sie

$$\mathfrak{a} \subseteq \mathfrak{b} \Longrightarrow V(\mathfrak{b}) \subseteq V(\mathfrak{a}) \Longrightarrow \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}.$$

Übungsaufgabe 8.7. Sei k ein Körper. Zeigen Sie, daß es im Polynomring $k[T]$ unendlich viele echt verschiedene (d.h. paarweise nicht-assoziierte) irreduzible Polynome gibt.

Übungsaufgabe 8.8. Zeigen Sie möglichst einfach die Aussage Theorem 8.30 (3) mittels Theorem 8.31.

9. Artinsch

9.1. **Moduln endlicher Länge.**

Definition 9.1. Ein **einfacher R-Modul** ist eine R-Modul $M \neq 0$, der keine echten R-Untermoduln hat: aus $M' \subseteq M$ folgt $M' = (0)$ oder $M' = M$.

Beispiel 9.2. Für jedes maximale Ideal $\mathfrak{m}$ eines Rings R ist $\kappa(\mathfrak{m}) = R/\mathfrak{m}$ als R-Modul einfach.

Proposition 9.3. *Sei R ein Ring und M ein R-Modul. Es sind äquivalent:*

(a) *M ist einfacher R-Modul.*
(b) *M wird von einem Element $0 \neq x \in M$ erzeugt und $\operatorname{Ann}_R(x) = \mathfrak{m}$ ist ein maximales Ideal.*

Ist M einfach, dann wird M wird von jedem $0 \neq x \in M$ erzeugt und es gilt

$$M \simeq R/\operatorname{Ann}_R(x).$$

Beweis. Für jedes $0 \neq x \in M$ ist $M' = \langle x \rangle_R \subseteq M$ ein Untermodul. Ist M einfach, dann gilt bereits $M' = M$. Der R-Modulhomomorphismus $f : R \to M$ gegeben durch

$$f(a) = ax$$

hat $\ker(f) = \operatorname{Ann}_R(x)$. Nach dem Homomorphiesatz gilt somit $M \simeq R/\operatorname{Ann}_R(x)$. Sei weiter $\mathfrak{m}$ ein maximales Ideal mit $\operatorname{Ann}_R(x) \subseteq \mathfrak{m}$. Dann gibt es eine Surjektion

$$p : M \simeq R/\operatorname{Ann}_R(x) \twoheadrightarrow R/\mathfrak{m}.$$

Der Kern ist als Untermodul des einfachen Moduls entweder $\ker(p) = (0)$ oder M. Letzteres geht nicht, weil $R/\mathfrak{m} \neq 0$. Also ist p ein Isomorphismus. Daraus folgt $\operatorname{Ann}_R(x) = \mathfrak{m}$.

Sei umgekehrt $M = \langle x \rangle_R \simeq R/\operatorname{Ann}_R(x) = R/\mathfrak{m}$ mit einem maximalen Ideal $\mathfrak{m}$. Dann entsprechen Untermoduln von M gerade den Moduln zwischen $\mathfrak{m} \subseteq R$. Davon gibt es nur $\mathfrak{m}$ und R, weil $\mathfrak{m}$ maximal ist. □

Proposition 9.4. *Der Support eines einfachen Moduls besteht aus einem einzigen maximalen Ideal.*

Beweis. Sei $\mathfrak{p} \in \operatorname{Spec}(R)$ und $M \simeq R/\mathfrak{m}$ ein einfacher R-Modul, also $\mathfrak{m}$ ein maximales Ideal. Es gilt

$$M_{\mathfrak{p}} \neq 0 \iff \mathfrak{p} \in V(\operatorname{Ann}_R(M)) = V(\mathfrak{m}) \iff \mathfrak{m} \subseteq \mathfrak{p} \iff \mathfrak{p} = \mathfrak{m}.$$ □

Definition 9.5. (1) Eine **Kette von Untermoduln** eines R-Moduls M ist eine bezüglich Inklusion totalgeordnete Teilmenge von Untermoduln von M (also echte Inklusion zwischen verschiedenen Gliedern der Kette).
(2) Die **Länge** der Kette von Untermoduln von M

$$(M_i) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots \subsetneq M_n$$

ist n.
(3) Eine **Kompositionsreihe** eines R-Moduls M ist eine endliche Kette

$$(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots \subsetneq M_n = M$$

von Untermoduln von M, so daß für alle $0 \leq i \leq n-1$

$$M_{i+1}/M_i$$

ein einfacher R-Modul ist. Man nennt M_{i+1}/M_i die **Kompositionsfaktoren** der Kompositionsreihe.
(4) Die Länge eines R-Moduls M ist

$$\ell_R(M) = \min\{n \ ; \ \text{ es gibt eine Kompositionsreihe für } M \text{ der Länge } n\},$$

falls eine Kompositionsreihe existiert. Ansonsten ist per Konvention

$$\ell_R(M) = \infty.$$

Man sagt, der Modul M hat **endliche Länge**, wenn M eine Kompositionsreihe besitzt.

Bemerkung 9.6. Kompositionsreihen sind genau die Ketten von Untermoduln, die nicht verfeinert werden können.

Beispiel 9.7. (1) Es gilt $\ell_R(M) = 0 \iff M = 0$.
(2) Ein Modul hat Länge 1 genau dann, wenn es ein einfacher R-Modul ist.

(3) Sei k ein Körper. Die k-Moduln sind Vektorräume und Kompositionsreihen von V sind **vollständige Fahnen** von Untervektorräumen

$$(0) = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_i \subsetneq \ldots \subsetneq V_n = V,$$

das heißt

$$\dim_k(V_i) = i.$$

Insbesondere gibt es eine Kompositionsreihe genau dann, wenn $\dim_k(V)$ endlich ist. Alle Kompositionsreihen sind dann gleich lang und

$$\ell_k(V) = \dim_k(V).$$

(4) Sei p eine Primzahl. Es gilt $\ell_{\mathbb{Z}}(\mathbb{Z}/p^2\mathbb{Z}) = 2$. Die Kette

$$(0) \subsetneq p\mathbb{Z}/p^2\mathbb{Z} \subsetneq \mathbb{Z}/p^2\mathbb{Z}$$

ist eine Kompositionsreihe und die Werte 0 und 1 scheiden für die Länge aus, weil der Modul weder 0 noch einfach ist.

(5) Nicht jeder Modul hat eine Kompositionsreihe. Zum Beispiel hat $\mathbb{Z}$ als $\mathbb{Z}$-Modul keine.

Satz 9.8. *Sei M eine R-Modul endlicher Länge und $M' \subsetneq M$ ein echter Untermodul. Dann hat M' endliche Länge und*

$$\ell_R(M') < \ell_R(M).$$

Beweis. Sei $(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots \subsetneq M_n = M$ eine Kompositionsreihe von M. Dann setzen wir $M'_i = M' \cap M$ und finden einen injektiven R-Modulhomomorphismus

$$M'_{i+1}/M'_i \hookrightarrow M_{i+1}/M_i.$$

Damit ist M'_{i+1}/M'_i entweder einfach und isomorph zu M_{i+1}/M_i oder $M'_{i+1}/M'_i = 0$ und $M'_i = M'_{i+1}$. Wenn wir aus

$$(0) = M'_0 \subseteq M'_1 \subseteq \ldots \subseteq M'_i \subseteq \ldots \subseteq M'_n = M'$$

die Wiederholungen streichen, erhalten wir also eine Kompositionsreihe von M'. Offenbar gilt dann

$$\ell_R(M') \leq \ell_R(M).$$

Wir führen nun die Annahme der Gleichheit zum Widerspruch. Wenn $\ell_R(M') = \ell_R(M)$ und wir mit einer Kompositionsreihe minimaler Länge für M begonnen haben, dann ergeben sich keine Wiederholungen. Es gilt also für alle i

$$M'_{i+1}/M'_i \simeq M_{i+1}/M_i$$

vermittels der durch die Inklusion induzierten Abbildung. Per Induktion über i zeigen wir $M'_i = M_i$. Der Anfang ist klar und der Induktionsschritt folgt aus dem Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M'_i & \longrightarrow & M'_{i+1} & \longrightarrow & M'_{i+1}/M'_i & \longrightarrow & 0 \\
 & & \downarrow \simeq & & \downarrow & & \downarrow \simeq & & \\
0 & \longrightarrow & M_i & \longrightarrow & M_{i+1} & \longrightarrow & M_{i+1}/M_i & \longrightarrow & 0
\end{array}$$

per 5er-Lemma, weil dann auch der mittlere Pfeil ein Isomorphismus sein muß. Für $i = \ell_R(M)$ folgt dann $M' = M$, ein Widerspruch. □

Theorem 9.9 (Jordan-Hölder-Theorem)**.** *Seien R ein Ring und M ein R-Modul endlicher Länge. Dann gilt:*

(1) Je zwei Kompositionsreihen sind gleich lang.

(2) Die Kompositionsfaktoren von M sind bis auf Permutation und Isomorphie unabhängig von der gewählten Kompositionsreihe.

(3) Jede Kette von Untermoduln von M läßt sich zu einer Kompositionsreihe verfeinern.

Beweis. (1) Das zeigen wir per Induktion nach $\ell_R(M)$. Für $\ell_R(M) \leq 1$ ist nichts zu tun, denn dann ist $M = (0)$ oder M ist einfacher R-Modul und die einzigen Ketten sind trivial oder $(0) \subsetneq M$.

Angenommen die Behauptung ist bewiesen für alle Moduln der Länge $< \ell_R(M)$. Sei $(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots \subsetneq M_n = M$ eine Kompositionsreihe von M minimaler Länge, also $n = \ell_R(M)$. Sei $(0) = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_i \subsetneq \ldots \subsetneq N_m = M$ eine weitere Kompositionsreihe. Dann gilt nach Satz 9.8

$$\ell_R(N_{m-1}) < \ell_R(M) = n \leq m.$$

Weil damit N_{m-1} kleinere Länge hat, gilt hier per Induktionsvoraussetzung, daß die Kompositionsreihe

$$(0) = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_i \subsetneq \ldots \subsetneq N_{m-1}$$

schon minimale Länge hat, also

$$m - 1 = \ell_R(N_{m-1}).$$

Zusammen ergibt dies $n = m$.

(2) Sei $\mathfrak{m}$ ein maximales Ideal. Lokalisieren wir eine Kompositionsreihe

$$(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots \subsetneq M_n = M$$

bei $\mathfrak{m}$, so erhalten wir eine Filtrierung (also Kette mit Wiederholungen)

$$(0) = (M_0)_\mathfrak{m} \subseteq (M_1)_\mathfrak{m} \subseteq \ldots \subseteq (M_i)_\mathfrak{m} \subseteq \ldots \subseteq (M_n)_\mathfrak{m} = M_\mathfrak{m},$$

wobei

$$(M_{i+1})_\mathfrak{m}/(M_i)_\mathfrak{m} \simeq (M_{i+1}/M_i)_\mathfrak{m} \simeq \begin{cases} (R/\mathfrak{m})_\mathfrak{m} = \kappa(\mathfrak{m}) & \text{wenn } \operatorname{supp}(M_{i+1}/M_i) = \{\mathfrak{m}\} \\ 0 & \text{sonst.} \end{cases}$$

Daraus folgt, daß nach Auslassung der Wiederholungen die lokalisierte Kompositionsreihe eine Kompositionsreihe des $R_\mathfrak{m}$-Moduls $M_\mathfrak{m}$ ist und genauer

$$\ell_{R_\mathfrak{m}}(M_\mathfrak{m}) = \#\{i \;;\; M_{i+1}/M_i \simeq R/\mathfrak{m}\}.$$

Weil die Länge (diesmal des $R_\mathfrak{m}$-Moduls $M_\mathfrak{m}$) nicht von der gewählten Kompositionsreihe abhängt, folgt Aussage (2).

(3) Sei $(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots \subsetneq M_n = M$ eine Kompositionsreihe und

$$N_0 \subseteq N_1 \subseteq \ldots \subseteq N_m$$

eine Kette von Untermoduln. Wir verfeinern $N_i \subseteq N_{i+1}$ durch $N_{i,j} = N_i + M_j \cap N_{i+1}$. Dies ist offensichtlich aufsteigend in j und $N_{i,0} = N_i$ und $N_{i,n} = N_{i+1}$. Es gilt nun

$$(N_i + M_{j+1} \cap N_{i+1}) \cap (N_i + M_j) = (N_i + M_j \cap N_{i+1}).$$

Die rechte Seite ist offensichtlich in der linken enhalten. Umgekehrt, ein Element der linken Seite hat die Form

$$y + x = y' + x'$$

mit $y, y' \in N_i$ und $x \in M_{j+1} \cap N_{i+1}$ und $x' \in M_j$. Damit ist

$$x' = y - y' + x \in N_{i+1},$$

also $x' \in M_j \cap N_{i+1}$ und somit $y' + x'$ in der rechten Seite.

Deshalb befinden sich die Filtrationsquotienten in einem Diagramm

$$\begin{array}{ccc} & & M_{j+1}/M_j \\ & & \downarrow \\ N_{i,j+1}/N_{i,j} & \hookrightarrow & (N_i + M_{j+1})/(N_i + M_j) \end{array}$$

mit den angezeigten surjektiven bzw. injektiven Abbildungen. Damit ist $N_{i,j+1}/N_{i,j}$ ein einfacher R-Modul oder 0. Nach Auslassung von Wiederholungen haben wir eine Kompositionsreihe, welche die gegebene Kette verfeinert. □

Korollar 9.10. *Sei R ein Ring und $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Dann hat M endliche Länge genau dann, wenn M' und M'' endliche Länge haben und dann gilt*

$$\ell_R(M) = \ell_R(M') + \ell_R(M'').$$

Beweis. Haben zunächst M' und M'' endliche Länge. Dann verlängert das Urbild einer Kompositionsreihe von M'' unter $M \twoheadrightarrow M''$ eine Kompositionsreihe von M' zu einer Kompositionsreihe von M. Damit hat dann auch M endliche Länge.

Wir nehmen nun an, daß M endliche Länge hat. Wir betrachten die Kette $(0) \subseteq M' \subseteq M$ und verfeinern diese nach Theorem 9.9 (3) zu einer Kompositionsreihe von M. Das Anfangsstück bis M' wird zu einer Kompositionsreihe von M' und der Rest wird durch Projektion $M \twoheadrightarrow M''$ zu einer Kette in M'', die auch einfache Quotienten hat, also zu einer Kompositionsreihe. Damit haben auch M' und M'' endliche Länge.

Die Formel für die Längen folgt aus den skizzierten Konstruktionen von Kompositionsreihen und Theorem 9.9 (1). □

Satz 9.11. *Sei M ein R-Modul endlicher Länge. Dann ist* $\operatorname{supp}(M)$ *eine endliche Menge maximaler Ideale von R und die natürliche Lokalisierungsabbildung*

$$M \to \prod_{\mathfrak{m} \in \operatorname{supp}(M)} M_{\mathfrak{m}}$$

ist ein Isomorphismus.

Beweis. Der Support eines einfachen Moduls $\simeq R/\mathfrak{m}$ enthält genau $\mathfrak{m}$. Die Endlichkeit von $\operatorname{supp}(M)$ folgt nun per Induktioin über die Länge mittels Proposition 7.11.

Für eine kurze exakte Sequenz $0 \to M' \to M \to M'' \to 0$ erhält man, weil das Lokalisieren und das Bilden von Produkten exakt sind, einen Morphismus exakter Sequenzen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod M'_{\mathfrak{m}} & \longrightarrow & \prod M_{\mathfrak{m}} & \longrightarrow & \prod M''_{\mathfrak{m}} & \longrightarrow & 0. \end{array}$$

Dabei laufen die Produkte über alle $\mathfrak{m} \in \operatorname{supp}(M)$. Wegen

$$\prod_{\mathfrak{m} \in \operatorname{supp}(M)} M'_{\mathfrak{m}} = \prod_{\mathfrak{m} \in \operatorname{supp}(M')} M'_{\mathfrak{m}}$$

und genauso für M'', führt das 5-er Lemma und Induktion über $\ell_R(M)$ die Behauptung auf Moduln der Länge 1 zurück.

Sei also M ein Modul der Länge 1. Dann ist $M \simeq R/\mathfrak{m}$ sowie $\operatorname{supp}(M) = \{\mathfrak{m}\}$, und die Lokalisierung

$$R/\mathfrak{m} \to (R/\mathfrak{m})_{\mathfrak{m}}$$

ein Isomorphismus. □

9.2. **Artinsche Moduln und Ringe.**

Definition 9.12. Ein **artinscher R-Modul** ist ein R-Modul, für den die folgenden äquivalenten Bedingungen gelten:

(a) Jede **absteigende Kette**

$$N_1 \supseteq N_2 \supseteq \ldots \supseteq N_i \supseteq N_{i+1} \supseteq \ldots$$

von R-Untermoduln von M wird stationär, d.h., es gibt $i_0 \in \mathbb{N}$, so daß für alle $i \geq i_0$ gilt $N_i = N_{i_0}$.

(b) Jede nichtleere Teilmenge von R-Untermoduln von M hat ein minimales Element bezüglich Inklusion.

Ein **artinscher** Ring ist ein Ring R, der als Modul über R ein artinscher R-Modul ist.

Definition 9.12 ist wohldefiniert. (b) $\Longrightarrow$ (a): Sei $N_1 \supseteq N_2 \supseteq \ldots \supseteq N_i \supseteq N_{i+1} \supseteq \ldots$ eine absteigende Kette von Untermoduln. Dann hat die Menge bestehend aus den N_i ein minimales Element nach (b). Wenn dieses Minimum erreicht ist, wird die Kette stationär.

(a) $\Longrightarrow$ (b): Wenn es eine nichtleere Menge von Untermoduln gibt, die kein minimales Element besitzt, dann kann man rekursiv durch Auswahl eines echt kleineren Untermoduls eine unendlich absteigende Kette von Untermoduln bekommmen, im Widerspruch zu (a). □

Beispiel 9.13. (1) Körper sind artinsch (und noethersch).

(2) Endliche Ringe sind artinsch (und noethersch).

(3) Sei k ein Körper. Endliche k-Algebren sind artinsch (und noethersch).

(4) Hauptidealringe R sind nicht artinsch (aber noethersch). Für ein $0 \neq f \in R \setminus R^\times$ ist die Kette

$$(f) \supseteq (f^2) \supseteq (f^3) \supseteq \ldots$$

nicht stationär. Sonst wäre für $n \gg 0$ bereits $(f^n) = (f^{n+1})$ und damit f^n assoziiert zu f^{n+1}. Das widerspricht der eindeutigen Primfaktorzerlegung in R.

Bemerkung 9.14. Es herrscht nur eine scheinbare Symmetrie zwischen den Begriffen artinsch und noethersch.

Proposition 9.15. *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Dann gilt*

$$M \text{ artinsch} \iff M' \text{ und } M'' \text{ artinsch.}$$

Beweis. Das ist derselbe Beweis wie im noetherschen Fall von Proposition 8.5. □

Korollar 9.16. *Sei R ein Ring.*

(1) Für R-Moduln M_i, $1 \leq i \leq r$ gilt

$$\bigoplus_{i=1}^{r} M_i \text{ artinsch} \iff M_i \text{ artinsch für alle } 1 \leq i \leq r.$$

(2) Untermoduln artinscher Moduln sind artinsch.

(3) Faktormoduln artinscher Moduln sind artinsch.

(4) Sei R artinscher Ring. Dann sind endlich erzeugte R-Moduln artinsch.

Beweis. Das folgt alles wie in Korollar 8.6, wobei Proposition 8.5 durch Proposition 9.15 ersetzt wird. □

Beispiel 9.17. Sei p eine Primzahl. Wir schreiben

$$\mathbb{Z}[\frac{1}{p}] = \{\frac{a}{b} \in \mathbb{Q} \ ; \ a \in \mathbb{Z}, b = p^n \text{ für ein } n \in \mathbb{N}_0\}.$$

(Denn $\mathbb{Z}_p$ ist für die p-adischen ganzen Zahlen reserviert.) Dann ist der Quotient

$$\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$$

als $\mathbb{Z}$-Modul artinsch, aber nicht endlich erzeugt, also auch nicht noethersch. Dies sieht man so: sei

$$M \subseteq \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$$

eine Untergruppe. Sei $\frac{a}{p^n} \in M$ und $p \nmid a$. Nach dem Satz von Bézout gibt es $x, y \in \mathbb{Z}$ mit

$$1 = xa + yp^n.$$

Dann ist auch

$$\frac{1}{p^n} = \frac{xa + yp^n}{p^n} = x\frac{a}{p^n} + y \equiv x\frac{a}{p^n} \in M.$$

Somit wird M von allen Elementen der Form $\frac{1}{p^n}$, die in M liegen, erzeugt. Entweder ist der Nenner beschränkt, dann ist M endlich, oder $M = \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$. Dies ist eine vollständige Übersicht über die $\mathbb{Z}$-Untermoduln von $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$. Es folgt sofort, daß $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ artinsch ist.

Satz 9.18. *Sei R ein Ring. Die R-Moduln endlicher Länge sind genau die R-Moduln, die artinsch und noethersch sind.*

Beweis. Wenn M endliche Länge hat, dann beschränkt $\ell_R(M)$ die Länge jeder echt absteigenden/aufsteigenden Kette von Untermoduln. Deshalb ist M artinsch und noethersch.

Sei M nun artinsch und noethersch. Wir betrachten die Menge der schlechten Untermoduln

$$\mathscr{B} = \{N \subseteq M \ ; \ N \text{ hat nicht endliche Länge}\}.$$

Wenn $\mathscr{B}$ leer ist, dann hat M endliche Länge, und wir sind fertig. Ansonsten können wir in $\mathscr{B}$ ein minimales Element $N \in \mathscr{B}$ wählen, weil M artinsch ist. Aufgrund der Minimalität haben alle echten Untermoduln von N endliche Länge.

Als nächstes betrachten wir die echten R-Untermoduln

$$\mathscr{U} = \{L \subseteq N \ ; \ L \neq N\}.$$

Wenn $\mathscr{U}$ leer ist, dann ist $N = 0$ oder N ist ein einfacher R-Modul und hat endliche Länge im Widerspruch zur Wahl von N. Da M noethersch ist, hat $\mathscr{U}$ ein maximales Element N'. Dann hat N' endliche Länge, und aufgrund der Maximalität von N' ist $N'' = N/N'$ ein einfacher Modul, hat also endliche Länge. Nun folgt aus Proposition 9.15, daß auch N endliche Länge hat. Dies ist der gesuchte Widerspruch. □

Theorem 9.19 (Kriterium für artinsche Ringe)**.** *Sei R ein Ring. Es sind äquivalent:*

(a) *R ist artinsch.*
(b) *R ist noethersch und* $\dim(R) = 0$.
(c) *R hat endliche Länge als R-Modul.*

Beweis. (a) $\Longrightarrow$ (b): Wir betrachten die Menge der Produkte maximaler Ideale

$$\mathscr{P} = \left\{ \prod_{i=1}^{r} \mathfrak{m}_i \ ; \ \mathfrak{m}_i \text{ maximales Ideal für } i = 1, \ldots, r \right\}.$$

Weil $\mathscr{P} \neq \emptyset$ und R artinsch ist, gibt es minimale Elemente in $\mathscr{P}$. Sei $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{m}_i \in \mathscr{P}$ minimal. Dann gilt für jedes maximale Ideal $\mathfrak{m}$ von R

$$\mathfrak{m}\mathfrak{a} \subseteq \mathfrak{a}$$

und aufgrund der Minimalität bereits $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$. Iteriert angewandt für alle $\mathfrak{m}_i$ folgt

$$\mathfrak{a}^2 = \mathfrak{a}.$$

Außerdem folgt aus $\mathfrak{a} = \mathfrak{m}\mathfrak{a} \subseteq \mathfrak{m}$ auch $\mathfrak{a} \subseteq \mathrm{Rad}(R)$.

Wir wollen zeigen, daß $\mathfrak{a} = (0)$. Andernfalls ist

$$\mathscr{B} = \{\mathfrak{b} \subseteq R \,;\; \mathfrak{b}\mathfrak{a} \neq (0)\}$$

nicht leer, denn $\mathfrak{a} \in \mathscr{B}$. Sei $\mathfrak{b}$ ein minimales Element aus $\mathscr{B}$. Dann gibt es $x \in \mathfrak{b}$ mit $x\mathfrak{a} \neq (0)$ und dann schon $(x) = \mathfrak{b}$ aufgrund der Minimalität. Weiter gilt

$$\mathfrak{a}((x) \cdot \mathfrak{a}) = (x) \cdot \mathfrak{a}^2 = (x) \cdot \mathfrak{a} \neq (0).$$

Aufgrund der Minimalität gilt daher sogar $(x) \cdot \mathfrak{a} = (x)$, folglich

$$\mathfrak{a} \cdot (x) = (x).$$

Der Modul (x) ist endlich erzeugt (im Gegensatz zum Ideal $\mathfrak{a}$, von dem wir das a priori nicht wissen) und $\mathfrak{a}$ im Jacobsonradikal enthalten. Damit greift das allgemeine Nakayama–Lemma Korollar 4.60 und zeigt

$$(x) = (0).$$

Dies ist ein Widerspruch zu $x\mathfrak{a} \neq (0)$, folglich muß bereits $\mathfrak{a} = (0)$ verschwinden.

Sei nun $\mathfrak{p}$ ein Primideal von R. Weil

$$\prod_{i=1}^{r} \mathfrak{m}_i = \mathfrak{a} = (0) \subseteq \mathfrak{p},$$

folgt aus Satz 7.4, daß es ein i gibt mit $\mathfrak{m}_i \subseteq \mathfrak{p}$. Damit ist

$$\mathrm{Spec}(R) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$$

eine endliche Menge maximaler Ideale und $\dim(R) = 0$.

Die Ideale $\mathfrak{a}_j = \prod_{i=1}^{j} \mathfrak{m}_i$ filtrieren R mit Quotienten $M_{j-1} = \mathfrak{a}_{j-1}/\mathfrak{a}_j$. Jeder der M_{j-1} ist als Subquotient von R ein artinscher Modul. Wegen $\mathfrak{m}_j\mathfrak{a}_{j-1} = \mathfrak{a}_j$ wird M_{j-1} von $\mathfrak{m}_j$ annulliert und ist somit ein artinscher $R/\mathfrak{m}_j$-Modul. Artinsche Moduln über Körpern sind Moduln endlicher Dimension, insbesondere endlich erzeugte noethersche Moduln. Somit sind alle M_j noethersch und wegen Proposition 8.5 auch R noethersch.

(b) $\Longrightarrow$ (c): Wir betrachten die Menge

$$\mathscr{B} = \{\mathfrak{a} \subseteq R \,;\; R/\mathfrak{a} \text{ hat nicht endliche Länge}\}.$$

Wenn $\mathscr{B}$ leer ist, dann hat R endliche Länge. Ansonsten gibt es ein maximales Element $\mathfrak{a}$. Angenommen $\mathfrak{a}$ ist nicht Primideal. Dann gibt es $x, y \in R \setminus \mathfrak{a}$ mit $xy \in \mathfrak{a}$. Die folgende Sequenz ist dann exakt:

$$0 \to R/(\mathfrak{a} : x) \xrightarrow{x\cdot} R/\mathfrak{a} \to R/(\mathfrak{a}, x) \to 0.$$

Weil $y \in (\mathfrak{a} : x)$, ist $\mathfrak{a} \subsetneq (\mathfrak{a} : x)$ und auch $\mathfrak{a} \subsetneq (\mathfrak{a}, x)$. Daher haben die beiden äußeren R-Moduln in der Sequenz endliche Länge aufgrund der Maximalität von $\mathfrak{a}$. Nach Korollar 9.10 hat dann auch $R/\mathfrak{a}$ endliche Länge, Widerspruch.

Damit ist gezeigt, daß $\mathfrak{a}$ ein Primideal ist. Weil $\dim(R) = 0$, ist $\mathfrak{a}$ sogar ein maximales Ideal. Aber dann ist $R/\mathfrak{a}$ ein einfacher Modul und hat endliche Länge, Widerspruch.

(c) $\Longrightarrow$ (a): Das folgt sofort aus Satz 9.18. □

Theorem 9.20 (Struktursatz für artinsche Ringe)**.** *Sei R ein artinscher Ring.*

(1) Dann ist $\mathrm{Spec}(R) = \mathrm{Specmax}(R)$ *eine endliche Menge und die natürliche Lokalisierungsabbildung*

$$R \to \prod_{\mathfrak{p} \in \mathrm{Spec}(R)} R_{\mathfrak{p}}$$

ist ein Ringisomorphismus.

(2) Für jeden R-Modul M ist

$$\lambda_M : M \to \prod_{\mathfrak{p}\in \mathrm{Spec}(R)} M_{\mathfrak{p}}$$

ein Isomorphismus.

Beweis. (1) Die Aussage über $\mathrm{Spec}(R)$ wurde in Theorem 9.19 bereits bewiesen. Die Aussage über die Lokalisierungsabbildung ist der Spezialfall $M = R$ von (2).

(2) Der Ring R ist nach Theorem 9.19 artinsch und noethersch. Damit sind endlich erzeugte Moduln auch noethersch und artinsch, also nach Satz 9.18 Moduln endlicher Länge. Für solche Moduln ist (2) bereits in Satz 9.11 bewiesen worden.

Wir betrachten nun einen allgemeinen R-Modul M. Wenn $\lambda_M : M \to \prod_{\mathfrak{p}} M_{\mathfrak{p}}$ nicht injektiv ist, dann gibt es einen nichttrivialen endlich erzeugten Untermodul $K \subseteq \ker(\lambda_M) \subseteq M$. Die Natürlichkeit und Exaktheit der Lokalisierung führt zu einem kommutativen Diagramm

$$\begin{array}{ccc} K & \hookrightarrow & M \\ {\scriptstyle\lambda_K}\downarrow{\scriptstyle\simeq} & & \downarrow{\scriptstyle\lambda_M} \\ \prod_{\mathfrak{p}} K_{\mathfrak{p}} & \hookrightarrow & \prod_{\mathfrak{p}} M_{\mathfrak{p}}. \end{array}$$

Weil λ_K ein Isomorphismus ist, kann K kein nichttrivialer Untermodul von $\ker(\lambda_M)$ sein, Widerspruch.

Sei nun $(m_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} M_{\mathfrak{p}}$ und $x_{\mathfrak{p}} \in M$ und $s_{\mathfrak{p}} \in R \setminus \mathfrak{p}$ mit $m_{\mathfrak{p}} = \frac{x_{\mathfrak{p}}}{s_{\mathfrak{p}}}$. Der Untermodul $N = \langle x_{\mathfrak{p}} \ ; \ \mathfrak{p} \in \mathrm{Spec}(R)\rangle_R \subseteq M$ ist endlich erzeugt. Wir haben wieder ein kommutatives Diagramm

$$\begin{array}{ccc} N & \hookrightarrow & M \\ {\scriptstyle\lambda_N}\downarrow{\scriptstyle\simeq} & & \downarrow{\scriptstyle\lambda_M} \\ \prod_{\mathfrak{p}} N_{\mathfrak{p}} & \hookrightarrow & \prod_{\mathfrak{p}} M_{\mathfrak{p}}. \end{array}$$

Per Konstruktion ist $(m_{\mathfrak{p}}) \in \mathrm{im}(\lambda_N)$, also auch im Bild von λ_M. Damit ist λ_M auch surjektiv. □

Korollar 9.21. *Seien R ein artinscher Ring und M ein R-Modul. Dann ist*

$$M \text{ artinsch} \iff M \text{ endlich erzeugt.}$$

Beweis. Wir müssen nur noch zeigen, daß artinsche Moduln über artinschen Ringen endlich erzeugt sind. Nach Theorem 9.20 zerlegt sich M als endliches direktes Produkt, also endliche direkte Summe von $R_{\mathfrak{p}}$-Moduln $M_{\mathfrak{p}}$ zu den $\mathfrak{p} \in \mathrm{Spec}(R)$. Es reicht daher, $M = M_{\mathfrak{p}}$ zu betrachten und ohne Einschränkung R durch $R_{\mathfrak{p}}$ zu ersetzen. Nun ist $\mathfrak{p}$ nilpotent und daher

$$M \supseteq \mathfrak{p}M \supseteq \ldots \supseteq \mathfrak{p}^i M \supseteq \ldots \supseteq \mathfrak{p}^n M = (0)$$

für $n \gg 0$, also eine endliche Filtrierung. Die Filtrationsquotienten sind artinsche $\kappa(\mathfrak{p}) = R/\mathfrak{p}$-Moduln, also von endlicher $\kappa(\mathfrak{p})$-Dimension, oder besser ausgedrückt von endlicher Länge als R-Modul. Damit ist M ein Modul endlicher Länge und damit artinsch und noethersch. Dies zeigt, daß M endlich erzeugter Modul ist. □

9.3. **Der Krullsche Hauptidealsatz.**

Definition 9.22. Die **Höhe** eines Primideals $\mathfrak{p}$ eines Rings R ist

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}_R(\mathfrak{p}) = \sup\{n \ ; \ \text{ es gibt eine Kette } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

Bemerkung 9.23. (1) Sei $\mathfrak{p} \in \operatorname{Spec}(R)$ ein Primideal, das eine multiplikative Menge S vermeidet. Dann gilt
$$\operatorname{ht}_R(\mathfrak{p}) = \operatorname{ht}_{S^{-1}R}(S^{-1}\mathfrak{p}),$$
weil die Primidealketten unterhalb $\mathfrak{p}$ in $\operatorname{Spec}(R)$ mit denen unterhalb $S^{-1}\mathfrak{p}$ in $\operatorname{Spec}(S^{-1}R)$ übereinstimmen.

Diese Bemerkung betrifft insbesondere die Lokalisierungen $R_{\mathfrak{p}}$, worin die Höhe aller $\mathfrak{q} \subseteq \mathfrak{p}$ erhalten bleibt.

(2) Es folgt
$$\operatorname{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}).$$

(3) Es ist nicht ausgeschlossen, daß $\operatorname{ht}(\mathfrak{p}) = \infty$. Dies gilt zum Beispiel für das maximale Ideal $\mathfrak{m} = (X_1, X_2, \ldots)$ der Koordinatenfunktionen im unendlichen Polynomring $k[X_1, X_2, \ldots]$.

Der nächste Satz beschreibt die Intuition, daß durch eine einzige Gleichung die Dimension höchstens um 1 kleiner wird.

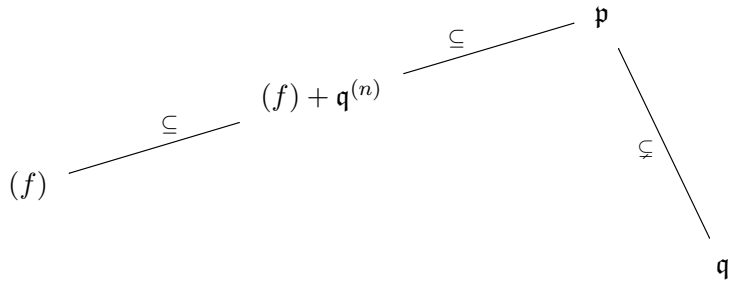
Theorem 9.24 (Krullscher Hauptidealsatz - 1. Form)**.** *Seien R ein noetherscher Ring und $f \in R$. Wenn das Primideal $\mathfrak{p} \in \operatorname{Spec}(R)$ ein minimales Primoberideal des Hauptideals (f) ist, dann gilt*
$$\operatorname{ht}(\mathfrak{p}) \leq 1.$$

Beweis. Schritt 1: Weil die Behauptung nur über Primideale enthalten in $\mathfrak{p}$ spricht, darf man R durch $R_{\mathfrak{p}}$ ersetzen. Wir nehmen also ohne Einschränkung an, daß R lokal mit maximalem Ideal $\mathfrak{p}$ ist. Der Quotient
$$R/(f)$$
ist dann lokal noethersch mit genau einem Primideal, also noethersch und von Dimension 0. Nach Theorem 9.19 ist $R/(f)$ artinsch.

Schritt 2: Wir müssen zeigen, daß für alle Primideale $\mathfrak{q}$ mit $\mathfrak{q} \subsetneq \mathfrak{p}$ gilt: $\dim(R_{\mathfrak{q}}) = 0$. Weil $R_{\mathfrak{q}}$ ein lokaler noetherscher Ring ist, haben wir zu zeigen, daß das maximale Ideal $\mathfrak{q}R_{\mathfrak{q}}$ von $R_{\mathfrak{q}}$ ein nilpotentes Ideal ist. Mittels des Lemmas von Nakayama folgt dies bereits daraus, daß die Folge der Ideale $(\mathfrak{q}R_{\mathfrak{q}})^n$ stationär in $R_{\mathfrak{q}}$ wird.

Schritt 3: Wir betrachten nun die Lokalisierung
$$j : R \to R_{\mathfrak{q}}$$
und die **symbolische Potenz**
$$\mathfrak{q}^{(n)} = j^{-1}((\mathfrak{q}R_{\mathfrak{q}})^n).$$
Der Beweis von Proposition 6.23 besagt, daß
$$\left(\mathfrak{q}^{(n)}\right)_{\mathfrak{q}} = (\mathfrak{q}R_{\mathfrak{q}})^n,$$
und es reicht zu zeigen, daß die absteigende Folge von Idealen $\mathfrak{q}^{(n)}$ stationär wird.

Schritt 4: Wir betrachten nun die Ideale



Weil $R/(f)$ artinsch ist, wird die absteigende Folge von Idealen $(f)+\mathfrak{q}^{(n)}$ stationär. Sei n so groß, daß

$$(f)+\mathfrak{q}^{(n)} = (f)+\mathfrak{q}^{(n+1)}$$

gilt. Dann gibt es für alle $x \in \mathfrak{q}^{(n)}$ ein $a \in R$ und $y \in \mathfrak{q}^{(n+1)}$ mit

$$x = fa + y.$$

Weil $f \in R \setminus \mathfrak{q}$, ist

$$j(a) = \frac{j(fa)}{f} = \frac{x-y}{f} \in (\mathfrak{q}R_{\mathfrak{q}})^n,$$

und damit

$$a \in \mathfrak{q}^{(n)}.$$

Wir schließen daraus auf

$$\mathfrak{q}^{(n)} = f \cdot \mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}.$$

Weil $f \in \mathfrak{p} = \mathrm{Rad}(R)$, folgt aus dem Nakayama-Lemma bereits

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}.$$

Damit ist gezeigt, daß, sobald die Folge der Ideale $(f)+\mathfrak{q}^{(n)}$ stationär wird, auch die Folge der $\mathfrak{q}^{(n)}$ stationär wird. Daraus folgt nun die Behauptung. □

Wir kommen nun zu einer nützlichen Anwendung, die als Pointe aus der Endlichkeitsannahme *noethersch* eine Unendlichkeitsaussage macht.

Satz 9.25. *Sei R ein noetherscher Ring.*

(1) *Sei* $\dim(R) \geq 2$. *Dann ist* $\mathrm{Spec}(R)$ *eine unendliche Menge.*

(2) *Seien $\mathfrak{p}_0 \subseteq \mathfrak{p}_2$ Primideale von R, so daß es ein Primideal $\mathfrak{p}_1$ mit $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ gibt. Dann ist die Menge*

$$\{\mathfrak{p} \in \mathrm{Spec}(R) \ ; \ \mathfrak{p}_0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_2\}$$

unendlich.

(3) *Sei $(R,\mathfrak{m})$ nun ein lokaler noetherscher Integritätsring der Dimension ≥ 2. Dann hat* $\mathrm{Spec}(R)$ *eine unendliche Menge von Primidealen der Höhe* 1. *Insbesondere ist* $\mathrm{Spec}(R)$ *eine unendliche Menge.*

Beweis. Aussage (1) folgt sofort aus Aussage (2), und Aussage (2) folgt aus Aussage (3) für

$$(R/\mathfrak{p}_0)_{\mathfrak{p}_2} = R_{\mathfrak{p}_2}/(\mathfrak{p}_0)_{\mathfrak{p}_2}.$$

(3) Angenommen, es gibt nur eine endliche Liste $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ von Primidealen der Höhe 1. Da $\mathfrak{m}$ maximal ist, gilt $\mathfrak{m} \not\subseteq \mathfrak{p}_i$ für alle $1 \leq i \leq n$. Nach Primvermeidung, Satz 3.15, gibt es daher ein

$$f \in \mathfrak{m} \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Wegen $(f) \subseteq \mathfrak{m}$ ist $R/(f)$ nicht der Nullring. Im Ring $R/(f) \neq 0$ gibt es nach Satz 3.29 minimale Primideale bezüglich Inklusion. Ein solches gehört zu einem Primideal $\mathfrak{q} \in \mathrm{Spec}(R)$, das minimales Primoberoideal $(f) \subseteq \mathfrak{q}$ von (f) ist. Nach dem Krullschen Hauptidealsatz, Theorem 9.24, und weil $(0) \neq \mathfrak{q}$ ist, gilt dann

$$\mathrm{ht}(\mathfrak{q}) = 1.$$

Dies steht im Widerspruch zur Wahl von f, das alle Primideale der Höhe 1 vermeidet. □

Satz 9.26 (Artin und Tate)**.** *Sei R ein noetherscher Integritätsring. Dann sind äquivalent:*

(a) $\mathrm{Spec}(R)$ *ist endliche Menge.*

(b) *Es gibt ein $f \in R$ und $R_f = \mathrm{Quot}(R)$.*

Wenn diese äquivalenten Bedingungen erfüllt sind, dann gilt $\dim(R) \leq 1$.

Beweis. (a) $\Longrightarrow$ (b): Sei $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ die Menge der von (0) verschiedenen Primideale von R. Sei $0 \neq f_i \in \mathfrak{p}_i$ jeweils ein Element. Das Produkt $f = f_1 \cdot \ldots \cdot f_n$ ist dann von 0 verschieden und in jedem der $\mathfrak{p}_i$ enthalten. Daher ist $\operatorname{Spec}(R_f) = \{(0)\}$ und R_f noethersch und von Dimension 0, also nach Theorem 9.19 artinsch. Als artinscher lokaler Integritätsring ist R_f somit ein Körper, notwendigerweise als Lokalisierung der Quotientenkörper von R.

(b) $\Longrightarrow$ (a): Sei $f \in R$ wie in (b). Dann ist f in jedem Primideal $\mathfrak{p} \neq (0)$ von R enthalten, weil $\operatorname{Spec}(R_f) = \{(0)\}$. Jedes Primideal $\mathfrak{p} \in \operatorname{Spec}(R)$ der Höhe 1 ist daher ein minimales Primoberideal von (f). Von diesen gibt es nur endlich viele nach Satz 8.12.

Angenommen es gibt in $\operatorname{Spec}(R)$ ein Primideal $\mathfrak{p}$ von Höhe ≥ 2. Dann zeigt Satz 9.25 angewandt auf $R_{\mathfrak{p}}$, daß es in R unendlich viele Primideale der Höhe 1 geben muß, Widerspruch. Wir schließen daraus, daß $\dim(R) \leq 1$, und $\operatorname{Spec}(R)$ enthält nur (0), das einzige Primideal der Höhe 0, und die endlich vielen Primideale der Höhe 1. Dies zeigt (a) und den Zusatz als Bonus obendrein. □

Übungsaufgaben zu §9

Übungsaufgabe 9.1. Sei R ein Hauptidealring. Zeigen Sie, daß R als R-Modul keine Kompositionsreihe besitzt.

Übungsaufgabe 9.2. Seien k ein Körper und V ein k-Vektorraum endlicher Dimension und $\varphi : V \to V$ ein k-linearer Endomorphismus. Wir machen aus V einen $k[X]$-Modul in der üblichen Weise, indem X durch φ wirkt.

(a) Zeigen Sie, daß V endliche Länge als $k[X]$-Modul hat.
(b) Bestimmen Sie die Länge in Abhängigkeit der Information der Jordannormalform von φ.

Übungsaufgabe 9.3. Seien k ein Körper und A eine endlich erzeugte k-Algebra. Zeigen Sie, daß $\dim_k(A) < \infty$ genau dann, wenn $\operatorname{Specmax}(A)$ eine endliche Menge ist.

Übungsaufgabe 9.4. Sei R ein unendlicher Integritätsring mit endlicher Einheitengruppe $R^\times$. Zeigen Sie, daß dann $\operatorname{Specmax}(R)$ unendlich viele Elemente hat.

Übungsaufgabe 9.5. Zeigen Sie, daß jeder Ring die Vereinigung noetherscher Unterringe ist.

10. Primärzerlegung und Assoziierte Primideale

Sei $n = \prod_{i=1}^r p_i^{e_i}$ die Faktorisierung von $n \in \mathbb{Z}$ als Produkt paarweise teilerfremder Primzahlpotenzen. Aufgrund der eindeutigen Primfaktorzerlegung gilt dann für das Ideal

$$(n) = \bigcap_{i=1}^{r} (p_i^{e_i}).$$

Der Untermodul $(n) \subseteq \mathbb{Z}$ wird hier durch einen Schnitt von Untermoduln beschrieben, deren Quotienten $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ hauptsächlich etwas mit dem Primideal (p_i) zu tun haben.

Die Primärzerlegung leistet Entsprechendes für noethersche Moduln über noetherschen Ringen. Dies wurde von Lasker für Ideale des Polynomrings über einem Körper bewiesen, ehe Emmy Noether einen Beweis basierend auf Kettenbedingungen für allgemeine noethersche Ringe fand und damit den Kettenbedingungen zum Durchbruch verhalf.

Beispiel 10.1. Das Ideal (XY, Y^2) in $k[X, Y]$ beschreibt als k-algebraische Menge in $\mathbb{A}^2$ die X-Achse $\{Y = 0\}$. Trotzdem ist das Bild von Y im Faktorring $k[X, Y]/(XY, Y^2)$ nicht 0. Dies findet sich in der Primärzerlegung wieder:

$$(XY, Y^2) = (Y) \cap (X, Y)^2.$$

Hier treten mit (Y) und (X, Y) zwei Primideale auf, die darüberhinaus noch ineinander enthalten sind: es gibt eine eingebettete Komponente.

10.1. **Assoziierte Primideale.**

Definition 10.2. Sei M ein R-Modul.

(1) Ein Element $a \in R$ ist ein **Nullteiler auf** M, wenn die Multiplikation mit a auf M

$$M \xrightarrow{a\cdot} M$$

nicht injektiv ist. Andernfalls ist a ein M**-reguläres** Element. Ein **Nullteiler** ist ein Nullteiler auf dem R-Modul R.

(2) Ein $\mathfrak{p} \in \operatorname{Spec}(R)$ heißt **zu** M **assoziiert**, falls die folgenden äquivalenten Bedingungen gelten:
   (a) Es gibt ein $0 \neq x \in M$ mit $\mathfrak{p} = \operatorname{Ann}_R(x)$.
   (b) Es gibt einen injektiven R-Modulhomomorphismus $R/\mathfrak{p} \hookrightarrow M$.
   Die Menge der zu M assoziierten Primideale wird mit

$$\operatorname{Ass}(M) = \operatorname{Ass}_R(M)$$

   bezeichnet. Es passiert leider, daß manchmal für ein Ideal $I \subseteq R$ mit $\operatorname{Ass}(I)$ eigentlich $\operatorname{Ass}(R/I)$ gemeint ist.

(3) Ein Primideal $\mathfrak{p}$ heißt **assoziiert**, wenn $\mathfrak{p} \in \operatorname{Ass}_R(R)$.

Beispiel 10.3. Sei $\mathfrak{p} \subseteq R$ ein Primideal. Dann ist

$$\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\},$$

denn für jedes $0 \neq x \in R/\mathfrak{p}$ ist $\mathfrak{p} = \operatorname{Ann}_R(x)$.

Bemerkung 10.4. Ist ein R-Modul M bereits ein R/I-Modul für ein Ideal $I \subseteq R$, d.h. $IM = (0)$, dann gilt

$$\operatorname{Ass}_R(M) = \operatorname{Ass}_{R/I}(M)$$

unter der Identifikation von $\operatorname{Spec}(R/I) \simeq V(I) \subseteq \operatorname{Spec}(R)$. In der Tat ist stets $I \subseteq \operatorname{Ann}_R(x)$ für alle $x \in M$.

Satz 10.5. *Seien R ein noetherscher Ring und $M \neq 0$ ein R-Modul.*

(1) Maximale Annullatorenideale, d.h. maximale Elemente der Menge

$$\{\operatorname{Ann}_R(x) \ ; \ 0 \neq x \in M\}$$

sind Primideale. Insbesondere ist $\operatorname{Ass}_R(M)$ nicht leer.

(2) Es gilt

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} \mathfrak{p} = \{f \in R \ ; \ f \text{ ist Nullteiler auf } M\}.$$

Beweis. (1) Sei $0 \neq x \in M$, so daß $\operatorname{Ann}_R(x)$ maximal unter allen solchen Annullatorenidealen ist. Angenommen $\operatorname{Ann}_R(x)$ ist nicht prim, dann gibt es $a, b \notin \operatorname{Ann}_R(x)$ mit $ab \in \operatorname{Ann}_R(x)$. Das bedeutet, daß $y = bx \neq 0$ und $ay = abx = 0$. Daher ist

$$\operatorname{Ann}_R(y) \supseteq \operatorname{Ann}_R(x) + Rb \supsetneq \operatorname{Ann}_R(x)$$

echt größer im Widerspruch zur Maximalität von $\operatorname{Ann}_R(x)$. Also ist ein $\operatorname{Ann}_R(x)$ ein Primideal.

Da R noethersch ist und die Menge der betrachteten Annullatorenideale nicht leer ist, gibt es maximale Annullatorenideale. Diese sind Primideale und zeigen, daß $\operatorname{Ass}_R(M) \neq \emptyset$.

(2) Wenn $\mathfrak{p} \in \operatorname{Ass}_R(M)$, dann ist $\mathfrak{p} = \operatorname{Ann}_R(x)$ für ein $0 \neq x \in M$. Dann zeigt $\mathfrak{p} \cdot x = 0$, daß $\mathfrak{p}$ nur aus Nullteilern auf M besteht.

Für die umgekehrte Richtung betrachten wir einen Nullteiler f auf M. Dazu gibt es ein $0 \neq x \in M$ mit $fx = 0$, d.h. es gilt $f \in \operatorname{Ann}_R(x)$. Da R noethersch ist, gibt es maxmiale Elemente in der nichtleeren Menge

$$\{\operatorname{Ann}_R(y) \ ; \ 0 \neq y \in M \text{ und } \operatorname{Ann}_R(x) \subseteq \operatorname{Ann}_R(y)\}.$$

Ein solches maximales Annullatorenideal ist auch unter allen Annullatorenidealen wie in (1) betrachtet maximal, daher ein Primideal und genauer ein assoziiertes Ideal, das f enhält. □

Korollar 10.6. *Sei R ein noetherscher Ring. Dann ist*

$$\bigcup_{\mathfrak{p}\in\mathrm{Ass}(R)} \mathfrak{p} = \{f \in R \;;\; f \text{ ist Nullteiler}\}.$$

Beweis. Das ist der Fall $M = R$ in Satz 10.5 (2). □

Proposition 10.7. *Seien R ein noetherscher Ring, $S \subseteq R$ eine multiplikative Teilmenge und M ein R-Modul. Dann ist*

$$\mathrm{Ass}_{S^{-1}R}(S^{-1}M) = \mathrm{Ass}_R(S^{-1}M) = \mathrm{Ass}_R(M) \cap \mathrm{Spec}(S^{-1}R)$$

vermöge der natürlichen Identifikation von $\mathrm{Spec}(S^{-1}R)$ *als Teilmenge von* $\mathrm{Spec}(R)$.

Beweis. Wir zeigen

$$\mathrm{Ass}_R(M) \cap \mathrm{Spec}(S^{-1}R) \subseteq \mathrm{Ass}_{S^{-1}R}(S^{-1}M) \subseteq \mathrm{Ass}_R(S^{-1}M) \subseteq \mathrm{Ass}_R(M) \cap \mathrm{Spec}(S^{-1}R).$$

Sei $\mathfrak{p} \in \mathrm{Ass}_R(M) \cap \mathrm{Spec}(S^{-1}R)$. Dann gibt es einen injektiven R-Modulhomomorphismus

$$R/\mathfrak{p} \hookrightarrow M.$$

Nach Lokalisieren an S wird daraus

$$0 \neq S^{-1}R/S^{-1}\mathfrak{p} \hookrightarrow S^{-1}M$$

zum einen, weil $\mathfrak{p} \cap S = \emptyset$, und zum andern, weil Lokalisieren exakt ist. Daraus lesen wir ab, daß $S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}R}(S^{-1}M)$.

Sei nun $\mathfrak{q} \in \mathrm{Ass}_{S^{-1}R}(S^{-1}M)$ bezeugt durch einen injektiven $S^{-1}R$-Modulhomomorphismus

$$S^{-1}R/\mathfrak{q} \hookrightarrow S^{-1}M.$$

Es gibt ein eindeutiges Primideal $\mathfrak{p}$ von R mit $\mathfrak{q} = S^{-1}\mathfrak{p}$ und einen injektiven R-Modulhomomorphismus $R/\mathfrak{p} \hookrightarrow S^{-1}(R/\mathfrak{p}) = S^{-1}R/\mathfrak{q}$. Die Komposition liefert

$$R/\mathfrak{p} \hookrightarrow S^{-1}R/\mathfrak{q} \hookrightarrow S^{-1}M$$

und zeigt $\mathfrak{p} \in \mathrm{Ass}_R(S^{-1}M)$.

Sei nun $\mathfrak{p} \in \mathrm{Ass}_R(S^{-1}M)$ bezeugt durch den injektiven R-Modulhomomorphismus

$$d : R/\mathfrak{p} \hookrightarrow S^{-1}M.$$

Nach der universellen Eigenschaft der Lokalisierung faktorisiert d über ein

$$f : S^{-1}(R/\mathfrak{p}) \to S^{-1}M.$$

Es folgt $S^{-1}(R/\mathfrak{p}) \neq 0$ und daher gehört $\mathfrak{p}$ zum Bild von $\mathrm{Spec}(S^{-1}R) \hookrightarrow \mathrm{Spec}(R)$. Weil R noethersch ist, ist $R/\mathfrak{p}$ ein endlich präsentierter R-Modul, und es gilt nach Korollar 6.20

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}(R/\mathfrak{p}), S^{-1}M) = S^{-1}\,\mathrm{Hom}_R(R/\mathfrak{p}, M).$$

Wenn wir also geeignet d und damit f durch ein Vielfaches mit $s \in S$ ersetzen, dann gibt es ein $F : R/\mathfrak{p} \to M$ in einem kommutativen Diagramm

$$\begin{array}{ccc} R/\mathfrak{p} & \xrightarrow{F} & M \\ \downarrow & \overset{sd}{\searrow} & \downarrow \\ S^{-1}(R/\mathfrak{p}) & \xrightarrow{sf} & S^{-1}M, \end{array}$$

wobei sd immer noch injektiv ist, weil Multiplikation mit s auf $S^{-1}M$ bijektiv ist. Damit ist auch F injektiv und $\mathfrak{p} \in \mathrm{Ass}_R(M)$. □

Korollar 10.8. *Seien R ein noetherscher Ring, $\mathfrak{p} \in \operatorname{Spec}(R)$ und M ein R-Modul. Dann gilt*

$$\mathfrak{p} \in \operatorname{Ass}_R(M) \iff \mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}).$$

Beweis. Sofort aus Proposition 10.7. □

Proposition 10.9. *Sei R ein Ring. Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von R-Moduln. Dann gilt*

$$\operatorname{Ass}_R(M') \subseteq \operatorname{Ass}_R(M) \subseteq \operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'').$$

Beweis. Sei $\mathfrak{p}$ ein Primideal. Ein injektives $R/\mathfrak{p} \hookrightarrow M'$ kann man mit $M' \to M$ zu einem injektiven $R/\mathfrak{p} \hookrightarrow M$ komponieren. Das zeigt $\operatorname{Ass}_R(M') \subseteq \operatorname{Ass}_R(M)$.

Sei nun $\mathfrak{p} \in \operatorname{Ass}_R(M)$ bezeugt durch das injektive $R/\mathfrak{p} \hookrightarrow M$. Entweder die Komposition $R/\mathfrak{p} \hookrightarrow M \to M''$ ist immer noch injektiv und $\mathfrak{p} \in \operatorname{Ass}_R(M'')$, oder der Schnitt $N' = M' \cap R/\mathfrak{p} \neq 0$ ist nichttrivial (nach Identifikation aller Injektionen als Untermoduln von M). Für jedes $0 \neq x \in N'$ ist die Multiplikation mit x auf $R/\mathfrak{p}$ injektiv mit Bild in $N' \subseteq R/\mathfrak{p}$. Daher ist die Komposition

$$R/\mathfrak{p} \xrightarrow{x\cdot} N' \hookrightarrow M'$$

injektiv, und es gilt $\mathfrak{p} \in \operatorname{Ass}_R(M')$. □

Satz 10.10 (Dévissage für noethersche Moduln)**.** *Sei R ein noetherscher Ring. Dann besitzt jeder endlich erzeugte R-Modul M eine endliche Kette von Untermoduln*

$$(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M,$$

so daß für alle $i = 1, \ldots, n$

$$M_i/M_{i-1} \simeq R/\mathfrak{p}_i$$

für ein Primideal $\mathfrak{p}_i$ von R.

Beweis. Nach Satz 10.5 (1) ist $\operatorname{Ass}(M) \neq \emptyset$. Wir wählen ein $\mathfrak{p}_1 \in \operatorname{Ass}(M)$ und einen bezeugenden injektiven R-Modulhomomorphismus $M_0 = R/\mathfrak{p}_1 \hookrightarrow M$. Wir ersetzen M durch $M'' = M/M_0$ und iterieren die Konstruktion. Das Urbild der gewählten Untermoduln $\simeq R/\mathfrak{p}_i$ beschreibt eine aufsteigende Kette von Untermoduln

$$(0) = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_i \subsetneq \ldots,$$

die stationär werden muß, weil M noethersch ist. Wenn die Kette bei M_n stationär wird, gilt $M = M_n$. □

Satz 10.11. *Seien R ein noetherscher Ring und M ein endlich erzeugter R-Modul.*

(1) $\operatorname{Ass}_R(M)$ *ist eine endliche Menge.*
(2) $\operatorname{Ass}_R(M) \subseteq \operatorname{supp}(M)$.
(3) Die minimalen Primideale in $\operatorname{supp}(M)$ *sind assoziierte Primideale von M.*

Beweis. (1) Das folgt sofort aus Satz 10.10, Satz 10.9 und Beispiel 10.3.

(2) Sei $\mathfrak{p} \in \operatorname{Ass}_R(M)$. Dann gibt es $R/\mathfrak{p} \hookrightarrow M$ und nach Lokalisieren $\kappa(\mathfrak{p}) \hookrightarrow M_\mathfrak{p}$. Also ist $M_\mathfrak{p} \neq 0$ und $\mathfrak{p} \in \operatorname{supp}(M)$.

(3) Sei $\mathfrak{p}$ ein minimales Primideal von $\operatorname{supp}(M)$. Dann ist $M_\mathfrak{p} \neq 0$ und $\operatorname{supp}(M_\mathfrak{p}) = \{\mathfrak{p}R_\mathfrak{p}\}$, wenn wir $M_\mathfrak{p}$ als $R_\mathfrak{p}$-Modul auffassen. Da $\operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p})$ nach Satz 10.5 nicht leer und nach (2) im Träger enthalten ist, folgt

$$\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}).$$

Da $\operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) \subseteq \operatorname{Ass}_R(M)$ nach Proposition 10.7, sind wir fertig. □

Korollar 10.12. *Sei R ein noetherscher Ring und sei M ein R-Modul. Für eine Teilmenge $V \subseteq \operatorname{Spec}(R)$ sind äquivalent:*

(1) Die Lokalisierungsabbildung

$$M \hookrightarrow \prod_{\mathfrak{p}\in V} M_{\mathfrak{p}}$$

ist injektiv.

(2) Zu jedem assoziierten Primideal $\mathfrak{p}_0 \in \operatorname{Ass}_R(M)$ gibt es ein $\mathfrak{p}_1 \in V$ mit $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$.

Beweis. (1) $\Longrightarrow$ (2): Sei $\mathfrak{p}_0 \in \operatorname{Ass}_R(M)$. Dann gibt es $0 \neq x \in M$ mit $\mathfrak{p}_0 = \operatorname{Ann}(x)$. Weil wir annehmen, daß die Lokalisierung $M \hookrightarrow \prod_{\mathfrak{p}\in V} M_{\mathfrak{p}}$ injektiv ist, gibt es ein $\mathfrak{p}_1 \in V$ mit $0 \neq \frac{x}{1} \in M_{\mathfrak{p}_1}$. Daraus folgt

$$\operatorname{Ann}(x) \cap (R \setminus \mathfrak{p}_1) = \emptyset.$$

Übersetzt bedeutet dies $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$.

(2) $\Longrightarrow$ (1): Wenn $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$, dann sind die Lokalisierungen $M \to M_{\mathfrak{p}_i}$ mit dem natürlichen R-Modulhomomorphismus $M_{\mathfrak{p}_1} \to M_{\mathfrak{p}_0}$ verträglich. Unter der Voraussetzung (2) gibt es eine Faktorisierung

$$\begin{array}{ccc} M & \longrightarrow & \prod_{\mathfrak{p}\in V} M_{\mathfrak{p}} \\ & \searrow & \downarrow \\ & & \prod_{\mathfrak{p}\in \operatorname{Ass}(M)} M_{\mathfrak{p}}. \end{array}$$

Damit reicht es aus, im Fall $V = \operatorname{Ass}_R(M)$ zu zeigen, daß $M \to \prod_{\mathfrak{p}\in \operatorname{Ass}(M)} M_{\mathfrak{p}}$ injektiv ist. Sei $0 \neq x \in M$ im Kern. Dann ist $\operatorname{Ann}_R(x) \cap (R \setminus \mathfrak{p}) \neq \emptyset$ für alle $\mathfrak{p} \in \operatorname{Ass}(M)$. Da aber

$$\operatorname{Ann}_R(x) \subseteq \bigcup_{\mathfrak{p}\in \operatorname{Ass}_R(M)} \mathfrak{p}$$

nach Satz 10.5, haben wir einen Widerspruch zur Primvermeidung, Satz 3.15, weil $\operatorname{Ass}_R(M)$ nach Satz 10.11 nur endlich viele Primideale enthält. □

Korollar 10.13 (Eingebettete Komponenten)**.** *Sei R ein noetherscher Ring. Wenn $\mathfrak{q} \in \operatorname{Ass}(R)$ kein minimales Primideal ist, dann gibt es ein nilpotentes $x \in \mathscr{N}(R)$ mit $\mathfrak{q} = \operatorname{Ann}_R(x)$.*

Beweis. Wir bezeichnen mit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die minimalen Primideale von R, von denen es nach Satz 8.12 nur endlich viele gibt. Weil $\mathfrak{q}$ nicht minimal ist nach Voraussetzung, können wir

$$f_i \in \mathfrak{q} \setminus \mathfrak{p}_i$$

wählen. Sei $\mathfrak{q} = \operatorname{Ann}_R(x)$ für ein $x \in R$. Dann folgt

$$f_i x = 0$$

und, weil $f_i \notin \mathfrak{p}_i$, bereits $x \in \mathfrak{p}_i$. Daher liegt x im Schnitt der minimalen Primideale, der wegen Satz 3.29 gleich dem Nilradikal ist:

$$x \in \bigcap_{i=1}^{r} \mathfrak{p}_i = \bigcap_{\mathfrak{p}\in \operatorname{Spec}(R)} \mathfrak{p} = \mathscr{N}(R).$$ □

Korollar 10.14. *Sei R noethersch. Dann sind äquivalent:*

(a) R ist reduziert.

(b) Es gibt Körper K_i mit $R \hookrightarrow \prod_{i=1}^{r} K_i$.

Beweis. (b) $\Longrightarrow$ (a): Ein Körper ist reduziert, ein Produkt reduzierter Ringe ist reduziert und ein Unterring eines reduzierten Rings ist reduziert.

(a) $\Longrightarrow$ (b): Nach Korollar 10.13 sind in einem reduzierten Ring alle $\mathfrak{p} \in \mathrm{Ass}(R)$ minimale Primideale. Dann ist $R_\mathfrak{p}$ ein lokaler reduzierter Ring von Dimension 0, also ein Körper. Die Injektion

$$R \hookrightarrow \prod_{\mathfrak{p}\in \mathrm{Ass}(R)} R_\mathfrak{p}$$

aus Korollar 10.12 zeigt dann (b). □

10.2. **Die Primärzerlegung.**

Definition 10.15. Sei R ein Ring. Ein R-Untermodul $N \subseteq M$ heißt **primär**, wenn jeder Nullteiler $a \in R$ auf M/N bereits nilpotent auf M/N operiert, d.h, wenn es ein $x \in M \setminus N$ gibt mit $ax \in N$, dann gibt es ein $n \geq 0$ mit $a^n M \subseteq N$.

Bemerkung 10.16. Ein primärer Untermodul $N \subseteq M$ zu sein ist keine Eigenschaft des Untermoduls N als Modul sondern eine Eigenschaft des Faktormoduls M/N. Es gilt

$$N \subseteq M \text{ primärer Untermodul } \iff (0) \subseteq M/N \text{ primärer Untermodul.}$$

Beispiel 10.17. Sei p eine Primzahl. Das Ideal (p^n) ist ein primärer Untermodul, denn auf dem Quotienten $\mathbb{Z}/p^n\mathbb{Z}$ operieren alle Nullteiler (durch p teilbar) sogar nilpotent.

Genauer ist $(n) \subseteq \mathbb{Z}$ genau dann primär, wenn n die Potenz einer Primzahl ist.

Lemma 10.18. *Sei R ein noetherscher Ring und M ein endlich erzeugter R-Modul mit einem Untermodul $N \subseteq M$. Dann sind äquivalent:*

(a) *N ist primär.*
(b) *$\mathrm{Ass}_R(M/N)$ besteht nur aus einem Primideal.*
(c) *Es gibt ein Primideal $\mathfrak{p}$ von R mit $\mathfrak{p}^n(M/N) = 0$ für $n \gg 0$ und $\mathfrak{p}$ enthält alle Nullteiler auf M/N.*

Wenn (a)–(c) gelten, dann ist $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}\}$ und $\sqrt{\mathrm{Ann}_R(M/N)} = \mathfrak{p}$ für das Primideal aus (c). Das Primideal $\mathfrak{p}$ ist eindeutig durch M/N bestimmt.

Beweis. (a) $\Longrightarrow$ (b): Sei N primär. Die auf M/N nilpotenten Elemente sind $\sqrt{\mathrm{Ann}_R(M/N)}$. Jedes assoziierte $\mathfrak{p} \in \mathrm{Ass}_R(M/N)$ besteht nach Satz 10.5 aus Nullteilern auf M/N, und zusammen mit Satz 10.11 folgt

$$\mathrm{Ann}_R(M/N) \subseteq \mathfrak{p} \subseteq \sqrt{\mathrm{Ann}_R(M/N)}.$$

Da Primideale selbst Radikalideale sind, folgt

$$\mathfrak{p} = \sqrt{\mathrm{Ann}_R(M/N)}.$$

Da dies für jedes assoziierte Primideal von M/N gilt, kann es nur eines geben. Dies zeigt (b).

(b) $\Longrightarrow$ (c): Wenn $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}\}$ nur aus einem Primideal besteht, dann enthält $\mathfrak{p}$ nach Satz 10.5 alle Nullteiler auf M/N.

Nach Satz 10.11 enthält $\mathrm{Ass}_R(M/N)$ alle Urbilder in R der minimalen Primideale von

$$R/(\mathrm{Ann}_R(M/N)).$$

Da es nur ein assoziiertes Primideal gibt, hat $R/(\mathrm{Ann}_R(M/N))$ nur ein minimales Primideal, das damit mit dem Nilradikal von $R/(\mathrm{Ann}_R(M/N))$ übereinstimmt. Dessen Urbild ist dann

$$\sqrt{\mathrm{Ann}_R(M/N)} = \mathfrak{p}.$$

Weil $\mathfrak{p}$ endlich erzeugt ist, folgt, daß $\mathfrak{p}^n \subseteq \mathrm{Ann}_R(M/N)$ für $n \gg 0$. Dies zeigt (c).

(c) $\Longrightarrow$ (a): Sei $a \in R$ ein Nullteiler auf M/N. Nach Voraussetzung ist dann $a \in \mathfrak{p}$. Weil $\mathfrak{p}^n$ für $n \gg 0$ den Modul M/N annulliert, operiert a nilpotent auf M/N. Also ist N primärer Untermodul von M. Dies zeigt (a). □

Definition 10.19. Sei R ein Ring. Ein R-Untermodul $N \subseteq M$ heißt **$\mathfrak{p}$-primär** für das Primideal $\mathfrak{p} \in \mathrm{Spec}(R)$, wenn N primär und $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}\}$.

Bemerkung 10.20. Im für uns relevanten Fall endlich erzeugter Moduln über noetherschen Ringen sind primäre Untermoduln $\mathfrak{p}$-primär für ein eindeutiges $\mathfrak{p}$. Das ist der Inhalt von Lemma 10.18.

Beispiel 10.21. (1) Sei $(R, \mathfrak{m})$ ein lokaler noetherscher Ring. Ein Ideal $\mathfrak{a} \subseteq R$ ist $\mathfrak{m}$-primär genau dann, wenn es ein $r > 0$ gibt mit

$$\mathfrak{m}^r \subseteq \mathfrak{a} \subseteq \mathfrak{m}.$$

Das ist äquivalent dazu, daß $R/\mathfrak{a}$ artinsch ist.

(2) Ein Primideal $\mathfrak{p} \subseteq R$ ist $\mathfrak{p}$-primär, weil $\mathrm{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$ ist.

Lemma 10.22. *Seien R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann*

$$N_1, N_2 \subseteq M \quad \mathfrak{p}\text{-primär} \Longrightarrow N_1 \cap N_2 \subseteq M \quad \mathfrak{p}\text{-primär}.$$

Beweis. Die natürliche Abbildung

$$M/N_1 \cap N_2 \to M/N_1 \times M/N_2 \tag{10.1}$$

ist injektiv. Aus Satz 10.9 folgt

$$\mathrm{Ass}_R(M/N_1 \cap N_2) \subseteq \mathrm{Ass}_R(M/N_1 \times M/N_2) = \mathrm{Ass}_R(M/N_1) \cup \mathrm{Ass}_R(M/N_2) = \{\mathfrak{p}\}.$$

Da die Menge der assoziierten Primideale nicht leer ist, folgt $\mathrm{Ass}_R(M/N_1 \cap N_2) = \{\mathfrak{p}\}$. □

Definition 10.23. Ein Untermodul $N \subseteq M$ heißt **irreduzibel**, wenn es keine Untermoduln $N \subsetneq N', N'' \subseteq M$ gibt mit $N = N' \cap N''$.

Proposition 10.24. *Seien R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Jeder R-Untermodul $N \subseteq M$ ist ein endlicher Durchschnitt irreduzibler Untermoduln: es gibt (nicht eindeutig!) irreduzible $N_i \subseteq M$ für $i = 1, \ldots, r$ mit*

$$N = \bigcap_{i=1}^{r} N_i.$$

Beweis. Wir betrachten die Menge der Untermoduln von M, die Gegenbeispiele des Satzes sind. Wenn diese Menge leer ist, dann gilt der Satz. Ansonsten gibt es ein maximales Gegenbeispiel bezüglich Inklusion. Dies sei $N \subseteq M$. Dann ist N nicht irreduzibel, sonst wäre es als Durschnitt von nur N von der geforderten Form. Also gibt es $N \subsetneq N', N'' \subseteq M$ mit $N = N' \cap N''$. Weil N' und N'' echt größer sind als N, haben sie die Form als Schnitt über endlich viele irreduzible Untermoduln. Wenn man beide Mengen von irreduziblen zusammenfügt und über alle schneidet, kommt N heraus, ein Widerspruch. □

Theorem 10.25 (Primärzerlegung)**.** *Seien R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann gilt:*

(1) Jeder irreduzible Untermodul $N \subseteq M$ ist primär.

*(2) Jeder echte Untermodul $N \subsetneq M$ hat eine **Primärzerlegung**: Es gibt Untermoduln $N_i \subseteq M$ für $i = 1, \ldots, r$ und paarweise verschiedene Primideale $\mathfrak{p}_i$ für $i = 1, \ldots, r$, so daß N_i ein $\mathfrak{p}_i$-primärer Untermodul ist und*

$$N = \bigcap_{i=1}^{r} N_i$$

ein nicht redundanter Schnitt ist. Nicht redundant bezieht sich darauf, daß auf keinen der N_i verzichtet werden kann: sonst ist der Schnitt größer.

*Der Modul N_i wird $\mathfrak{p}_i$-**primäre Komponente** von N genannt.*

(3) Mit der Notation aus (b) gilt

$$\mathrm{Ass}_R(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

(4) *Die $\mathfrak{p}$-primäre Komponente zu einem minimalen assoziierten Primideal $\mathfrak{p}$ ist eindeutig bestimmt durch*

$$N(\mathfrak{p}) = j_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}}),$$

wobei $j_{\mathfrak{p}} : M \to M_{\mathfrak{p}}$ die Lokalisierungsabbildung ist.

Beweis. (1) Sei N irreduzibel. Angenommen N ist nicht primär, dann gibt es zwei verschiedene assoziierte Primideale $\mathfrak{p} \neq \mathfrak{q} \in \mathrm{Ass}_R(M/N)$. Entsprechend gibt es Untermoduln

$$R/\mathfrak{p} \simeq \bar{N}' \hookrightarrow M/N \quad \text{und} \quad R/\mathfrak{q} \simeq \bar{N}'' \hookrightarrow M/N.$$

Für jedes $0 \neq x \in R/\mathfrak{p}$ ist $\mathrm{Ann}_R(x) = \mathfrak{p}$ und entsprechend für $0 \neq x \in R/\mathfrak{q}$ ist $\mathrm{Ann}_R(x) = \mathfrak{q}$. Weil $\mathfrak{p} \neq \mathfrak{q}$ muß $\bar{N}' \cap \bar{N}'' = (0)$ sein. Wir setzen N' und N'' für die Urbilder unter $M \to M/N$ von $\bar{N}'$ und $\bar{N}''$. Dann ist $N' \cap N'' = N$ aber $N \subsetneq N', N''$. Dies ist ein Widerspruch, denn N ist irreduzibel. Folglich hat $\mathrm{Ass}_R(M/N)$ nur ein Element und N ist primär.

(2) Wir schreiben $N = \bigcap_{i=1}^r N_i$ mit N_i irreduzibel wie in Proposition 10.24. Dann sind alle N_i primär nach (1). Jetzt fassen wir für $\mathfrak{p} \in \mathrm{Spec}(R)$ alle N_i zusammen, die $\mathfrak{p}$-primär sind. Deren Schnitt ist nach Lemma 10.22 immer noch $\mathfrak{p}$-primär. Nach Umnummerierung erhalten wir die in (2) gesuchte Zerlegung als Schnitt primärer Moduln.

Durch sukzessives Weglassen redundanter Moduln N_i, die den Schnitt nicht verkleinern, kann man erreichen, daß der Schnitt nicht redundant ist.

(3) Aus

$$M/N \hookrightarrow \prod_{i=1}^r M/N_i \tag{10.2}$$

folgt mittels Satz 10.9

$$\mathrm{Ass}_R(M/N) \subseteq \bigcup_{i=1}^r \mathrm{Ass}_R(M/N_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

Weil der Schnitt in (2) nicht redundant ist, haben wir für alle $j = 1, \ldots, r$ mit

$$\bar{M}_j := (\bigcap_{i \neq j} N_i)/N \subseteq M/N$$

einen nicht-trivialen Untermodul. Nach dem Isomorphiesatz gilt

$$(\bigcap_{i \neq j} N_i)/N = (N_j + \bigcap_{i \neq j} N_i)/N_j \subseteq M/N_j.$$

Die assoziierten Primideale von $\bar{M}_j$ sind assoziierte Primideale von M/N_j, also nur $\mathfrak{p}_j$ nach Satz 10.9, aus dem auch folgt, daß dann wegen $\bar{M}_j \subseteq M/N$ das Primideal $\mathfrak{p}_j$ ein assoziiertes Primideal von M/N ist. Dies zeigt die andere Inklusion und damit (3).

(4) Sei $\mathfrak{p}$ ein minimales zu M/N assoziiertes Primideal und $N(\mathfrak{p})$ der $\mathfrak{p}$-primäre Untermodul in der Primärzerlegung aus (2). Für alle $\mathfrak{p}_i \neq \mathfrak{p}$ aus (2) trifft $R \setminus \mathfrak{p}$ das Primideal $\mathfrak{p}_i$, weil $\mathfrak{p}$ minimal ist. Daher enthält beim Lokalisieren an $\mathfrak{p}$ die Nennermenge Nullteiler auf M/N_i, damit nilpotente und schließlich folgt

$$(M/N_i)_{\mathfrak{p}} = 0.$$

Lokalisieren wir (10.2), so bleibt die Abbildung injektiv, aber nur die $\mathfrak{p}$-Komponente überlebt. Daher ist

$$M_{\mathfrak{p}}/N_{\mathfrak{p}} = (M/N)_{\mathfrak{p}} \hookrightarrow (M/N(\mathfrak{p}))_{\mathfrak{p}}$$

injektiv. Der Modulhomomorphismus

$$M/N(\mathfrak{p}) \to (M/N(\mathfrak{p}))_{\mathfrak{p}}$$

ist injektiv, weil $R \setminus \mathfrak{p}$ auf $M/N(\mathfrak{p})$ durch nicht-Nullteiler operiert. Damit ist

$$\begin{aligned} N(\mathfrak{p}) &= \ker(M \to M/N(\mathfrak{p}) \hookrightarrow (M/N(\mathfrak{p}))_{\mathfrak{p}}) \\ &= \ker(M \xrightarrow{j_{\mathfrak{p}}} M_{\mathfrak{p}} \twoheadrightarrow M_{\mathfrak{p}}/N_{\mathfrak{p}} \hookrightarrow (M_{\mathfrak{p}}/N(\mathfrak{p})_{\mathfrak{p}}) = j_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}}). \end{aligned}$$ □

Beispiel 10.26. Sei R ein reduzierter noetherscher Ring. Dann ist

$$(0) = \bigcap_{\mathrm{ht}(\mathfrak{p})=0} \mathfrak{p}$$

die Primärzerlegung von (0) entsprechend

$$R \hookrightarrow \prod_{\mathrm{ht}(\mathfrak{p})=0} R/\mathfrak{p}.$$

.

11. Moduln über Hauptidealringen

Ein Hauptidealring R ist offensichtlich ein noetherscher Integritätsring. Jedes von (0) verschiedene Primideal $\mathfrak{p}$ ist von einem Primelement p erzeugt, liegt damit minimal über einem $p \in R$. Damit ist $\mathrm{ht}(\mathfrak{p}) \leq 1$ nach dem Krullschen Hauptidealsatz, und wegen $(0) \subsetneq \mathfrak{p}$ genauer $\mathrm{ht}(\mathfrak{p}) = 1$. Ein Hauptidealring hat, sofern R kein Körper ist, also genau dann, wenn es von (0) verschiedene maximale Ideale gibt, die Krulldimension

$$\dim(R) = 1.$$

Hauptidealringe sind gewissermaßen die nach den Körpern am wenigsten komplizierten Ringe. Das zeigt sich unter anderem darin, daß man Moduln über Hauptidealringen sehr gut beschreiben kann.

11.1. Die Primärzerlegung von Torsionsmoduln über Hauptidealringen.

Definition 11.1. Seien R ein Ring und M ein R-Modul.

(1) Die **f-Torsion** von M zu einem $f \in R$ ist der Kern

$$M[f] = \{m \in M \mid fm = 0\} = \ker(M \xrightarrow{f\cdot} M)$$

der Multiplikation mit f auf M.

(2) Der Modul M heißt **Torsionsmodul**, falls

$$M = \bigcup_{0 \neq f \in R} M[f].$$

Lemma 11.2. *Sind $f, g \in R$ assoziierte Elemente, d.h. unterscheiden sie sich multiplikativ nur um eine Einheit, so gilt $M[f] = M[g]$.*

Beweis. Das ist klar. □

Definition 11.3. Seien R ein Integritätsring und M ein R-Modul. Die **Torsion von** M ist der R-Untermodul

$$M_{\mathrm{tors}} = \bigcup_{0 \neq f \in R} M[f]$$

von M. Dies ist der maximale Torsionsuntermodul von M.

Beweis. Jeder Torsionsuntermodul besteht nur aus Torsion und ist daher in M_{tors} enthalten.

In der Tat ist M_{tors} ein Untermodul, denn aus $f_i m_i = 0$ für $i = 1, 2$ mit $0 \neq f_i \in R$ und $m_i \in M$ folgt $f_1 f_2 (m_1 + m_2) = 0$, wobei immer noch $f_1 f_2 \neq 0$ gilt. □

Definition 11.4. Seien nun R ein Hauptidealring, M ein R-Modul und $p \in R$ ein Primelement. Die Elemente, welche von einer Potenz von p annulliert werden, nennt man **p-primär** und den R-Untermodul ihrer Vereinigung

$$M[p^\infty] := \bigcup_n M[p^n]$$

nennt man die **p-primäre Komponente** von M. Gilt $M = M[p^\infty]$, so nennt man M **p-primär**.

Bemerkung 11.5. Sei R ein Hauptidealring und $\mathfrak{p} = (p)$ ein Primideal mit einem Primelement $p \neq 0$. Sei M ein R-Modul. Man mache sich als Übungsaufgabe klar, daß $(0) \subseteq M$ ein $\mathfrak{p}$-primärer Untermodul ist genau dann, wenn M ein p-primärer Modul ist.

Vorsicht: Die p-primäre Komponente $M[p^\infty]$ ist in der Regel nicht der Untermodul von M, der in der Primärzerlegung von $(0) \subseteq M$ im Sinne von Theorem 10.25 zum Primideal (p) gehört!

Beispiel 11.6. Sei V ein endlich-dimensionaler K-Vektorraum mit Endomorphismus φ, den wir als $K[X]$-Modul auffassen, indem X durch φ operiert. Dann handelt es sich nach dem Satz von Cayley–Hamilton bei V um einen endlich erzeugten $K[X]$-Torsionsmodul, denn für das charakteristische Polynom

$$P_\varphi(X) = \det(X - \varphi) \in K[X]$$

gilt

$$V = V[P_\varphi].$$

Der Eigenraum V_λ zum Eigenwert $\lambda \in K$ ist nichts anderes als die $(X - \lambda)$-Torsion

$$V[X - \lambda].$$

Ist überdies φ diagonalisierbar, so ist sogar $V_\lambda = V[(X - \lambda)^\infty]$ die entsprechende Primärkomponente und es gilt $V = \bigoplus_\lambda V_\lambda$. Der Modul ist also die direkte Summe seiner Primärkomponenten. Dies ist kein Zufall.

Satz 11.7 (Primärzerlegung für Torsionsmoduln bei Hauptidealringen)**.** *Sei M ein endlich erzeugter Torsionsmodul über dem Hauptidealring R. Dann gilt:*

(1) Für alle bis auf endlich viele Primelemente p (bis auf assoziierte) gilt $M[p^\infty] = 0$ und

$$M = \bigoplus_{p \text{ prim}} M[p^\infty].$$

(2) Es gibt ein minimales $f \in R$ bezüglich Teilbarkeit mit $fM = 0$. Wenn $f = u \cdot \prod p^{\alpha(p)}$ seine Zerlegung in Primfaktoren p und eine Einheit u ist, so gilt genauer

$$M = \bigoplus_{p \mid f} M[p^{\alpha(p)}].$$

(3) Sei $f \in R$. Die Multiplikation mit f auf der p-Primärkomponente $M[p^\infty]$ ist

$$\begin{aligned} \text{ein Isomorphismus} &\iff p \text{ teilt } f \text{ nicht}, \\ \text{nilpotent} &\iff p \text{ teilt } f. \end{aligned}$$

(4) Mit $M[p'] := \bigoplus_{q \neq p} M[q^\infty]$ erhalten wir die eindeutige direkte Zerlegung von $M = M[p^\infty] \oplus M[p']$ in einen Summanden, auf dem die Multiplikation mit p nilpotent ist, und einen zweiten Summanden, auf dem die Multiplikation mit p ein Isomorphismus ist.

Beweis. Wir zeigen (2). Seien $m_1, \ldots, m_s$ Erzeuger von M und $0 \neq f_i \in R$ mit $f_i m_i = 0$ für $1 \leq i \leq s$. Dann annulliert $f_1 \cdot \ldots \cdot f_s \neq 0$ den Modul M. Somit ist $\operatorname{Ann}(M) \neq (0)$. Da R ein Hauptidealring ist, gilt $\operatorname{Ann}(M) = (f)$ für ein geeignetes $f \neq 0$. Dieses f ist minimal bezüglich Teilbarkeit mit der Eigenschaft $fM = 0$.

Sei nun $f = \prod_{i=1}^n p_i^{\alpha_i}$ die Zerlegung in Primfaktoren. Für $n = 0, 1$ ist nichts zu tun. Sei daher $n > 1$. Der größte gemeinsame Teiler der Elemente $p_i' = \prod_{j\neq i} p_j^{\alpha_j}$ für $1 \leq i \leq n$ ist 1. Gemäß des Satzes von Bézout wählen wir $a_i \in R$ mit

$$1 = \sum_{i=1}^n a_i p_i'.$$

Setzen wir $e_i = a_i p_i'$, so gilt in $\mathrm{End}_R(M)$ für die Multiplikationsabbildungen $e_i e_j = 0$ für $i \neq j$. In der Tat ist f ein Teiler von $e_i e_j$, ergo $e_i e_j \in \mathrm{Ann}_R(M)$. Des weiteren sind die e_i in $\mathrm{End}_R(M)$ Idempotente:

$$e_i = e_i(\sum_{j=1}^n e_j) = e_i^2.$$

Wir definieren die Untermoduln $e_i M = \{e_i m \,|\, m \in M\}$ von M. Die Inklusionen definieren eine Abbildung

$$\chi : \bigoplus_{i=1}^n e_i M \to M, \quad (m_1, \ldots, m_n) \mapsto \sum m_i,$$

welche die Abbildung $\psi : m \mapsto (e_1 m, \ldots, e_n m)$ als Inverses hat, denn

- $\chi(\psi(m)) = \sum_i e_i m = \big(\sum_i e_i\big)m = m$ und
- $\psi(\chi(m_1, \ldots, m_n)) = \big(\ldots, e_i(\sum_j m_j), \ldots\big) = (m_1, \ldots, m_n)$.

Es gilt nämlich für $x = e_j y \in e_j M$, daß $e_i x = e_i e_j y = 0$, falls $i \neq j$, oder $e_i x = e_i e_i y = e_i y = x$ für $i = j$. Daraus folgt die Rechnung für $\psi \circ \chi$.

Wir haben jetzt noch $e_i M = M[p_i^{\alpha_i}]$ nachzuweisen. Da f das Element $e_i p_i^{\alpha_i}$ teilt, gilt

$$e_i M \subseteq M[p_i^{\alpha_i}].$$

Um die umgekehrte Inklusion nachzuweisen, nehmen wir ein Element $m \in M[p_i^{\alpha_i}]$ und zerlegen es in Komponenten $e_j m$ bezüglich der Zerlegung $M = \bigoplus e_i M$. Für $j \neq i$ teilt $p_i^{\alpha_i}$ das Idempotent e_j und somit ist diese Komponente $e_j m =$ (anderer Faktor) $\cdot\, p_i^{\alpha_i} m = 0$. Somit gilt $m = e_i m$ und $m \in e_i M$.

Für (1) ist jetzt nur noch nachzuweisen, daß schon $M[p^\infty] = M[p^{\alpha(p)}]$ gilt und für Primelemente, die f nicht teilen, die entsprechende Primärkomponente von M verschwindet. Dies folgt beides aus (3) und dem Folgenden.

(3) Teilt p nicht f, so ist $(f, p^n) = 1$ für alle $n \in \mathbb{N}$, und es gibt nach dem Satz von Bézout

$$1 = \rho_n f + \pi_n p^n$$

mit $\rho_n, \pi_n \in R$. Somit operiert f auf $M[p^n]$ mit Inversem ρ_n. Damit ist auch in der Vereinigung $M[p^\infty]$ über alle n die Multiplikation mit f bijektiv (man beachte, daß $M[p^n] \subseteq M[p^{n+k}]$ für $k \geq 0$).

Ist hingegen p ein Teiler von f, so reicht es, sich mit dem Fall $f = p$ auseinanderzusetzen. Für jedes Element $m \in M[p^\infty]$ gibt es per Definition ein *a priori* von m abhängendes $N \in \mathbb{N}$, so daß $p^N m = 0$. Wir wollen aber die Multiplikation mit p als nilpotent erkennen und müssen so ein für alle $m \in M[p^\infty]$ uniform geltendes N finden.

Wir zerlegen ein Element $m \in M[p^\infty]$ gemäß (2) in Komponenten $e_i m \in M[p_i^{\alpha_i}]$. Sei $p_i \neq p$, so ist nach dem eben Bewiesenen die Multiplikation mit p ein Isomorphismus auf $M[p_i^{\alpha_i}]$. Damit verschwindet die entsprechende Komponente von $p^N m$, nämlich $e_i p^N m$, nur, wenn schon $e_i m = 0$. Somit liegt $M[p^\infty]$ schon in $M[p^{\alpha(p)}]$ und stimmt deswegen mit $M[p^{\alpha(p)}]$ überein. Dies zeigt (3) und damit auch (1).

Für (4) bemerken wir nur, daß in einer derartigen Zerlegung der nilpotente Teil in $M[p^\infty]$ enthalten sein muß. Der Anteil, auf dem p Isomorphismus ist, hingegen muß im Schnitt der Bilder der Multiplikation mit p^n über alle n liegen. Mit den Erkenntnissen aus (3) ist dieser

Schnitt gerade $M[p']$. Die Zerlegung $M = M[p^\infty] \oplus M[p']$ gilt nach (1). Die Summe eines p-nilpotenten und eines p-isomorphen Teils kann also nur dann ganz M sein, wenn es die in (4) beschriebene ist. □

Korollar 11.8. *Mit der Notation aus Satz 11.7 ist*

$$(0) = \bigcap_{p \text{ prim}} M[p']$$

die Primärzerlegung im Sinne von Theorem 10.25 von $(0) \subseteq M$.

Beweis. Es gilt nach Satz 11.7

$$M[p^\infty] \simeq M/M[p']$$

und $\mathrm{Ass}_R(M[p^\infty]) = \{(p)\}$. □

Die Struktur der Torsionsmoduln über Hauptidealringen ist noch genauer bekannt.

Definition 11.9. Ein **zyklischer** R-Modul ist ein R-Modul M, der von einem Element erzeugt werden kann.

Bemerkung 11.10. Sei $M = \langle x \rangle_R$ ein zyklischer R-Modul. Sei $\mathfrak{a} = \mathrm{Ann}_R(x) = \mathrm{Ann}_R(M)$ das Annullatorideal. Dann gibt es einen Isomorphismus $f : R/\mathfrak{a} \simeq M$ gegeben durch $f(a) = ax$. Zyklische Moduln sind also solche, die isomorph zu einem Faktormodul von R sind.

Für $R = \mathbb{Z}$ sind R-Moduln abelsche Gruppen und zyklische $\mathbb{Z}$-Moduln sind zyklische abelsche Gruppen.

Satz 11.11 (Struktursatz für endlich erzeugte Torsionsmoduln I)**.** *Seien R ein Haupidealring und M ein endlich erzeugter Torsions-R-Modul. Dann gilt:*

(1) M ist isomorph zu einer direkten Summe zyklischer R-Moduln.
(2) Es gibt nicht notwendig verschiedene Primelemente p_i und natürliche Zahlen e_i für $i = 1, \ldots, s$ und einen Isomorphismus von R-Moduln

$$M \simeq \bigoplus_{i=1}^{s} R/(p_i^{e_i}).$$

Beweis. Offenbar ist (1) eine Folge der präziseren Strukturaussage (2). Um (2) zu beweisen, dürfen wir nach der Primärzerlegung, Satz 11.7, den Modul M durch seine p-Primärkomponente $M[p^e]$ zu einer uniformen Potenz p^e mit einem Primelement p ersetzen. Da Hauptidealringe noethersch sind, ist auch $M[p^e]$ ein endlich erzeugter R-Modul.

Wir dürfen also nun annehmen, daß $\mathrm{Ann}(M) = (p^e)$. Es reicht dann, eine direkte Zerlegung

$$M = \bigoplus_i Rx_i$$

mit endlich vielen Elementen $x_i \in M$ zu finden, in der die Summanden von einem Element x_i erzeugt werden. In der Tat gilt $\mathrm{Ann}(x_i) \subseteq (p^e)$ und daher $\mathrm{Ann}(x_i) = (p^{e_i})$ für geeignete e_i und

$$Rx_i \simeq R/\mathrm{Ann}(x_i) \simeq R/(p_i^{e_i}).$$

Wir führen eine Induktion über die Anzahl der Erzeuger von M. Der Induktionsanfang mit einer leeren Erzeugermenge führt zum Modul $M = 0$, der die leere direkte Summe zyklischer Moduln ist. (Wem das suspekt ist, der analysiere den Fall mit nur einem Erzeuger.)

Behandeln wir nun den Induktionsschritt. Besitze M ein Erzeugendensystem aus n Elementen. Unter diesen gibt es ein Element $x_1 \in M$ mit $\mathrm{Ann}(x_1) = (p^e)$ und e maximal, denn sonst annullierte schon p^{e-1} den Modul M. Der Quotient

$$\mathrm{pr} : M \to \overline{M} = M/Rx_1$$

kann mit $n-1$ Elementen erzeugt werden, den Bildern der restlichen Erzeuger. Per Induktion ist $\overline{M} = \bigoplus_{i=2}^{s} R\overline{y}_i$. Wir werden versuchen, diese Zerlegung nach M zu liften, das heißt, wir suchen eine Spaltung σ (Rechtsinverses der Projektion $M \to \overline{M}$) der exakten Sequenz

$$0 \longrightarrow Rx_1 \longrightarrow M \overset{\sigma}{\underset{\longleftarrow}{\longrightarrow}} \bigoplus_{i=2}^{s} R\overline{y}_i \longrightarrow 0\,.$$

Dazu liften wir zunächst die $\overline{y}_i$ beliebig zu $y_i \in \mathrm{pr}^{-1}(\overline{y}_i)$ nach M. Es sei $\mathrm{Ann}(\overline{y}_i) = (p^{e_i})$. Dann gilt $e_i \leq e$ und $p^{e_i} y_i \in Rx_1$. Es gibt also $a_i \in R$ mit $p^{e_i} y_i = a_i x_1$. Jetzt verwenden wir die Extremalität von x_1. Da $p^{e-e_i} a_i x_1 = p^e y_i = 0$, muß p^{e_i} ein Teiler von a_i sein. Wir setzen $a_i = p^{e_i} b_i$ und modifizieren y_i ohne sein Bild in $\overline{M}$ zu ändern durch $x_i = y_i - b_i x_1$. Damit annulliert p^{e_i} den Lift x_i und $\sigma(\sum_{i=2}^{s} \lambda_i \overline{y}_i) = \sum_{i=2}^{s} \lambda_i x_i$ ist wohldefiniert und die gesuchte Spaltung. Aus Lemma 5.37 folgt dann die gewünschte Zerlegung

$$M \simeq Rx_1 \oplus \big(\bigoplus_{i=2}^{s} R\overline{y}_i\big),$$

und genauer mit der Wahl der Spaltung durch die x_i

$$M = \bigoplus_{i=1}^{s} Rx_i \simeq Rx_1 \oplus \big(\bigoplus_{i=2}^{s} R\overline{y}_i\big). \qquad \square$$

Satz 11.12 (Eindeutigkeit)**.** *Sei M ein p-primärer endlich erzeugter Torsionsmodul über dem Hauptidealring R. Sei*

$$M \simeq \bigoplus_{i} R/(p^{e_i})$$

mit $e_i > 0$ eine Zerlegung in eine direkte Summe zyklischer Moduln. Dann gilt:

(1) $\#\{i\} = \dim_{\kappa(p)}(M/pM)$,

(2) $\#\{i \,|\, e_i = e\} = \dim_{\kappa(p)}\big(M[p^e]/M[p^{e-1}]\big) - \dim_{\kappa(p)}\big(M[p^{e+1}]/M[p^e]\big)$,

(3) insbesondere sind die Anzahl der Summanden und genauer die Anzahl der Summanden mit Annulator (p^e) unabhängig von der gewählten Zerlegung.

Nach der Eindeutigkeit der Primärzerlegung gilt dies entsprechend auch für allgemeine endlich erzeugte Torsions-R-Moduln M.

Beweis. Aus $M = M' \oplus M''$ folgen

$$pM = pM' \oplus pM'',$$
$$M[p^e] = M'[p^e] \oplus M''[p^e],$$

also auch

$$M/pM = M'/pM' \oplus M''/pM'',$$
$$M[p^e]/M[p^{e-1}] = M'[p^e]/M'[p^{e-1}] \oplus M''[p^e]/M''[p^{e-1}].$$

Da die Dimension eines Vektorraums additiv auf direkten Summen ist, gelten die Formeln in (1) und (2) für M genau dann, wenn sie für M' und M'' gelten. Wir haben also nur den Fall $M = R/(p^\alpha), \alpha > 0$ zu analysieren. Dieser Fall jedoch ist klar. $\square$

Beispiel 11.13. Viel mehr an Eindeutigkeit läßt sich nicht erwarten. Wir betrachten zu $0 < e \in \mathbb{N}$ den R-Modul

$$M = R/(p^e) \oplus R/(p).$$

Für $e = 1$ handelt es sich um einen $\kappa(p)$-Vektorraum der Dimension 2. Eine Zerlegung wie im Struktursatz entspricht der Wahl einer Basis als $\kappa(p)$-Vektorraum. Die Mehrdeutigkeit einer Basiswahl wird parametrisiert durch ein Element in $\mathrm{GL}_2(\kappa(p))$, der Basiswechselmatrix.

Sei $e > 1$. Die Beweise des Struktursatzes lehren, daß jedes Element mit Annulator (p^e) ein direkter Summand von M ist. Diese sind gegeben durch

$$f \in \operatorname{Hom}\big(R/(p^e), R/(p)\big) \simeq \kappa(p)$$

als Graph

$$M_f := \{(x, f(x)) \,|\, x \in R/(p^e)\} \subset R/(p^e) \oplus R/(p).$$

Zu $M_f \simeq R/(p^e)$ kann man auf vielfache Weise ein Komplement finden. Der zweite Summand $R/(p)$ in der definierenden direkten Summenzerlegung von M tut es jedenfalls.

Satz 11.14 (Struktursatz für endlich erzeugte Torsionsmoduln II)**.** *Sei M ein endlich erzeugter Torsionsmodul über dem Hauptidealring R.*

(1) Es gibt eine Folge sich aufsteigend teilender Elemente $d_1|d_2|\ldots|d_s$ des Rings R, so daß

$$M \simeq \bigoplus_{i=1}^{s} R/(d_i).$$

(2) Die natürliche Zahl s und die Ideale (d_i) zu den Elementen d_i aus (1) sind eindeutig durch den R-Modul M bestimmt.

Beweis. Es folgt (1) aus dem ersten Struktursatz, Satz 11.11, und dem Chinesischen Restsatz. Die Eindeutigkeitsaussage (2) folgt aus Satz 11.12. □

11.2. **Der Elementarteilersatz.** Eine konstruktive Methode zur Bestimmung der Struktur eines endlich erzeugten Moduls über einem Hauptidealring basiert auf dem Elementarteilersatz.

Satz 11.15 (Elementarteilersatz)**.** *Seien R ein Hauptidealring und $A \in \mathrm{M}_{m\times n}(R)$.*

(1) Dann gibt es invertierbare Matrizen $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$, so daß

$$SAT = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_s \\ & & \end{pmatrix}$$

(alle restlichen Einträge der Matrix sind 0) mit $s \leq \min\{n, m\}$ und sich steigend teilenden Elementen $d_1|d_2|\ldots|d_s$ des Rings R.

(2) Die natürliche Zahl s und die d_i bis auf Multiplikation mit Einheiten hängen nicht von den Matrizen S, T ab.

Dies beweisen wir später.

Korollar 11.16. *Sei R ein Hauptidealring.*

(1) Untermoduln von freien R-Moduln sind frei.

(2) Ist $N \subseteq M \simeq R^m$ ein Untermodul eines freien Moduls über dem Hauptidealring R, so gibt es eine Basis $x_1, \ldots, x_m$ von M und sich aufsteigend teilende Elemente $d_1|d_2|\ldots|d_s$ für ein $s \leq m$, so daß N von den $d_1x_1, \ldots, d_sx_s$ frei erzeugt wird.

(3) Sei M ein freier R-Modul und $N \subseteq M$ ein Untermodul. Dann gilt

$$\mathrm{rk}_R(N) \leq \mathrm{rk}_R(M).$$

Beweis. Wir behandeln nur den Fall, daß der freie Modul endlichen Rang hat. Dann folgen (1) und (3) unmittelbar aus (2), worum wir uns also zu kümmern haben.

Ohne Einschränkung sei $M = R^m$. Da R noethersch ist, ist auch N endlich erzeugt. Sei $R^n \twoheadrightarrow N$ eine Surjektion, welche von der Wahl eines Erzeugendensystems von N der Kardinalität n herrührt. Dann entspricht der Verkettung $R^n \twoheadrightarrow N \subset R^m$ eine Matrix, auf die wir Satz 11.15 anwenden können. Das Komponieren mit S und T entspricht einer anderen Basiswahl von

R^m und R^n. Dies ändert am Bild N der Abbildung nichts, welches daher bezüglich der neuen Koordinaten die behauptete Form hat. □

Korollar 11.17 (Struktursatz für endlich erzeugte Moduln über Hauptidealringen)**.** *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul.*

(1) Es gibt eine kanonische exakte Sequenz

$$0 \to M_{\mathrm{tors}} \to M \to M/M_{\mathrm{tors}} \to 0 \tag{11.1}$$

mit dem maximalen Torsionsuntermodul $M_{\mathrm{tors}} \subseteq M$ und einem freien, endlich erzeugten Quotienten $M/M_{\mathrm{tors}} \simeq R^r$. Die Sequenz (11.1) spaltet unkanonisch. Somit gilt unkanonisch $M \simeq M_{\mathrm{tors}} \oplus M/M_{\mathrm{tors}}$ und M_{tors} ist auch endlich erzeugt.

(2) Es gibt eine nicht kanonische Zerlegung als direkte Summe

$$M \simeq R^r \oplus \bigoplus_{i=1}^{s} R/(d_i)$$

mit sich aufsteigend teilenden Elementen $d_1|d_2|\ldots|d_s$ des Rings R. Die Zahlen r und s sowie die Elemente d_i bis auf Assoziierung sind eindeutig.

Beweis. Wir beweisen zunächst die Existenzaussage von (2). Wir wählen Erzeuger $x_1, \ldots, x_m$ von M und damit eine Surjektion $\mathrm{pr} : R^m \to M$. Wir wenden Korollar 11.16 auf den Kern $\ker(\mathrm{pr}) \subset R^m$ dieser Abbildung an. Ohne Einschränkung sei $x_1, \ldots, x_m$ bereits die Basis von R^m, die das Korollar uns verspricht, so daß $\ker(\mathrm{pr})$ von $d_1x_1, \ldots, d_sx_s$ erzeugt wird. Es gilt nun nach dem Homomorphiesatz

$$M \simeq R^m/\ker(\mathrm{pr}) \simeq \left(\bigoplus_{i=1}^{m} Rx_i\right) / \left(\bigoplus_{i=1}^{s} Rd_ix_i\right) = (\bigoplus_{i=1}^{s} Rx_i/Rd_ix_i) \oplus R^{m-s}.$$

Damit ist $r = m - s$ und wegen

$$Rx_i/Rd_ix_i \simeq R/(d_i)$$

haben wir (2) bis auf die Eindeutigkeitsaussage bewiesen.

(1) Sei M_{tors} der Torsionsuntermodul. Dann ist M/M_{tors} torsionsfrei und endlich erzeugt. Denn wäre $\overline{m} \in M/M_{\mathrm{tors}}$ Torsion, etwa $f\overline{m} = 0$, so gilt für ein Urbild $m \mapsto \overline{m}$, daß $fm \in M_{\mathrm{tors}}$, und somit m selbst Torsion. Damit ist $\overline{m} = 0$ und

$$\big(M/M_{\mathrm{tors}}\big)_{\mathrm{tors}} = (0).$$

Wenden wir den bereits bewiesenen Teil von (2) auf M/M_{tors} an, so erkennen wir, daß alle Summanden $R/(d)$ verschwinden müssen, da sie aus R-Torsion bestehen. Ergo ist M/M_{tors} frei. Freie Moduln sind projektiv, somit gibt es eine Spaltung von (11.1) und

$$M \simeq M_{\mathrm{tors}} \oplus M/M_{\mathrm{tors}}.$$

Der Modul der Torsionselemente M_{tors} ist auch endlich erzeugt, weil R noethersch und M endlich erzeugt ist.

(2) Wir wenden uns nun der Eindeutigkeitsaussage von (2) zu. Sei K der Quotientenkörper von R. Die Zahl r ist charakterisiert als

$$r = \mathrm{rk}_R(M/M_{\mathrm{tors}}) = \dim_K M \otimes_R K,$$

und damit ist r eindeutig.

Zur Eindeutigkeit von s und der d_i bemerken wir, daß diese nicht aus der entsprechenden Eindeutigkeit der d_i aus dem Elementarteilersatz folgt, denn wir müssen über alle Matrizen A variieren, die zu einer endlichen **Präsentation**, also einer kurzen exakten Sequenz

$$R^n \xrightarrow{A} R^m \to M \to 0$$

gehören. Die Eindeutigkeit aus dem Elementarteilersatz garantiert nur für jede fixierte Matrix A die Eindeutigkeit der zu A äquivalenten diagonalen Form. Die Eindeutigkeit über alle Präsentationen wird durch die Theorie der Fittingideale geleistet, siehe [Eis95, Kap. 20]. Wir begnügen uns mit einem unnatürlichen Rückgriff auf Satz 11.14, den wir auf den Torsionsanteil $M_{\text{tors}} \subseteq M$ anwenden. □

Der Beweis des Elementarteilersatzes erfordert vorbereitende Lemmata.

Notation 11.18. Sei R ein Hauptidealring und $A \in \mathrm{M}_{n\times m}(R)$ eine Matrix. Den größten gemeinsamen Teiler der Einträge der Matrix A bezeichnen wir mit

$$\mathrm{ggT}(A).$$

Multiplikation mit invertierbaren Matrizen von links und rechts ändert den größten gemeinsamen Teiler nicht.

Lemma 11.19. *Sei R ein Hauptidealring und $A \in \mathrm{M}_{m\times n}(R)$, $S \in \mathrm{M}_m(R)$ und $T \in \mathrm{M}_n(R)$. Dann gilt:*

(1) $\mathrm{ggT}(A)$ *teilt* $\mathrm{ggT}(SA)$ *und* $\mathrm{ggT}(AT)$.
(2) Sind S, T invertierbar, so gilt $\mathrm{ggT}(A) = \mathrm{ggT}(SA) = \mathrm{ggT}(AT)$.

Beweis. Es folgt (2) sofort aus (1) und (1) ist auch klar. □

Lemma 11.20. *(1) Sei $w = (a_1, \ldots, a_n) \in R^n$ ein Zeilenvektor mit größtem gemeinsamen Teiler der Koordinaten $d = \mathrm{ggT}(w)$. Dann gibt es eine invertierbare Matrix $T \in \mathrm{GL}_n(R)$ mit $wT = (d, 0 \ldots, 0)$.*

(2) Analog gibt es für einen Spaltenvektor v der Länge m eine invertierbare Matrix $S \in \mathrm{GL}_m(R)$ so, daß in Sv die erste Zeile d ist und alle anderen Einträge verschwinden.

Beweis. Offenbar sind die Aussagen (1) und (2) äquivalent. Man hat nur alle Matrizen und Vektoren zu transponieren. Daher beweisen wir nur (2). Wir verwenden Induktion nach der Größe m des Vektors. Für $m = 1$ ist nichts zu zeigen. Des weiteren ist die Behauptung des Lemmas für Vektoren v und Bv äquivalent, wenn B eine invertierbare Matrix ist, denn nach Lemma 11.19 gilt $\mathrm{ggT}(v) = \mathrm{ggT}(Bv)$.

Sei $v = \binom{a_1}{v'}$ mit einem Spaltenvektor v' der Länge $m-1$. Per Induktionsvoraussetzung gibt es eine Matrix $S' \in \mathrm{GL}_{(m-1)}(R)$ so, daß $S'v'$ nur noch einen nichtverschwindenden Eintrag d' in der ersten Zeile hat. Dann ist die Blockmatrix

$$B = \begin{pmatrix} 1 & 0 \\ 0 & S' \end{pmatrix}$$

invertierbar, und es hat Bv nur noch nichtverschwindende Einträge in den ersten beiden Zeilen. Jetzt reicht es offenbar, den Fall $m = 2$ zu beherrschen.

Sei $m = 2$ und $v = \binom{a_1}{a_2}$. Nach dem Satz von Bézout gibt es in R eine Relation

$$\alpha_1 a_1 + \alpha_2 a_2 = d.$$

Damit erfüllt die Matrix

$$S = \begin{pmatrix} \alpha_1 & \alpha_2 \\ -a_2/d & a_1/d \end{pmatrix}$$

das Gewünschte:

$$Sv = \binom{d}{0}.$$

Es ist $d = \mathrm{ggT}(Sv) = \mathrm{ggT}(v)$ nach Lemma 11.19. □

Beweis des Elementarteilersatzes Satz 11.15 — Existenz. Wir beweisen zunächst die Existenzaussage. Wir werden versuchen, durch Multiplikation mit invertierbaren Matrizen von links und rechts die Matrix A auf die Blockform

$$\left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{11.2}$$

zu bringen, wobei $d_1 = \mathrm{ggT}(A)$ gelten soll. Somit teilt d_1 jeden Eintrag der Matrix A'. Wir schließen dann per Induktion nach $\min\{n, m\}$, indem wir den Induktionsschritt auf die Matrix

$$\frac{1}{d_1} A' \in \mathrm{M}_{(m-1)\times(n-1)}(R)$$

anwenden. Dabei ist wichtig, daß durch Multiplikation mit invertierbaren Matrizen von links und rechts sich der ggT nicht ändert, siehe Lemma 11.19.

Der Induktionsanfang $n = 1$ oder $m = 1$ wurde bereits in Lemma 11.20 behandelt.

Zum Induktionsschritt wenden wir Lemma 11.20 auf die erste Spalte von $A_0 = A$ an. Wir finden ein $S \in \mathrm{GL}_m(R)$, so daß

$$A_1 = SA_0 = \left(\begin{array}{c|ccc} a_1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & A'_1 & \\ 0 & & & \end{array}\right) \tag{11.3}$$

Dabei ist a_1 als ggT der ersten Spalte ein Teiler des Eintrags von A_0 an derselben Stelle. Nun wenden wir Lemma 11.20 auf die erste Zeile von A_1 an und finden $T \in \mathrm{GL}_n(R)$, so daß

$$A_2 = A_1T = \left(\begin{array}{c|ccc} a_2 & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & A'_2 & \\ * & & & \end{array}\right) \tag{11.4}$$

Diesmal ist a_2 der ggT der ersten Zeile und damit ein Teiler von a_1. Allerdings kontrollieren wir nicht, ob die Nullen in der ersten Spalte aus dem ersten Schritt erhalten bleiben.

Wir iterieren diese beiden Schritte alternierend und erhalten eine Folge von Matrizen A_i mit erstem Eintrag a_i oben links und

$$a_{i+1} \mid a_i.$$

Da in einem Hauptidealring kein Element beliebig oft Teiler mit weniger Primfaktoren haben kann, muß nach einer Weile a_{i+1} sich nur noch um eine Einheit von a_i unterscheiden. Das bedeutet, daß dann a_i schon der entsprechende ggT ist. In diesem Moment können wir die Nullen in der ersten Spalte und ersten Zeile durch elementare Spalten- (bzw. Zeilen-)transformationen erhalten (dies sind solche Multiplikationen mit invertierbaren Matrizen S und T!), nämlich durch Addition eines Vielfachen der ersten Spalte (bzw. Zeile), die dann die bereits vorhandenen Nullen nicht wieder zerstört. Wir erhalten so eine Matrix der Gestalt

$$\left(\begin{array}{c|ccc} \delta & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{11.5}$$

Damit sind wir fast am Ziel. Wir kontrollieren nur noch nicht, daß δ alle Einträge von A' teilt. Dieses Problem ignorieren wir zunächst und schließen per Induktion nach $\min\{n, m\}$ auf eine

Diagonalgestalt

$$\begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_s \\ & & \end{pmatrix} \tag{11.6}$$

Nun gehen wir einen Schritt rückwärts und addieren per Zeilenoperation die $2 \leq i \leq s$-te Zeile zur ersten Zeile dazu. In der Matrix

$$\begin{pmatrix} \delta_1 & \dots & \delta_s \\ & \ddots & \\ & & \delta_s \\ & & \end{pmatrix} \tag{11.7}$$

ist nun der ggT der ersten Zeile gleich $\mathrm{ggT}(A)$. Starten wir mit dieser Matrix das Verfahren erneut, wird die in (11.5) erreichte Matrix sogar die Eigenschaft haben, daß $\delta = \mathrm{ggT}(A)$ ein Teiler der Matrix A' ist, also das Ziel (11.2) erreicht ist. Wieder per Induktion nach $\min\{n, m\}$ folgt die Existenz der gewünschten Diagonalform.

Die Eindeutigkeitsaussage beweisen wir im nächsten Abschnitt mittels Fittingidealen. □

11.3. **Fitting-Ideale.** Die Eindeutigkeitsaussage im Elementarteilersatz folgt schnell aus der Theorie der Fittingideale, von der wir nur das Nötigste beweisen.

Definition 11.21. Sei $A \in \mathrm{M}_{n\times m}(R)$ eine Matrix mit Einträgen in einem beliebigen kommutativen Ring R. Für $\nu \geq 0$ ist das **ν-te Fittingideal** von A dasjenige Ideal

$$\mathrm{Fitt}_\nu(A) \subseteq R,$$

welches von den Minoren der Größe $n - \nu$ der Matrix A, also den Determinanten von quadratischen $(n - \nu) \times (n - \nu)$-Untermatrizen von A, erzeugt wird. Wir setzen

$$\mathrm{Fitt}_n(A) = R$$

(Minoren der Größe 0 sind per Konvention alle 1), und

$$\mathrm{Fitt}_\nu(A) = (0),$$

sobald $n - \nu > \min\{n, m\}$ und damit keine quadratischen Untermatrizen der Größe $n - \nu$ in A Platz finden.

Bemerkung 11.22. (1) Da ein $(r+1)$-Minor eine Linearkombination von r-Minoren ist, bilden die Fittingideale einer Matrix $A \in \mathrm{M}_{n\times m}(R)$ eine aufsteigende Kette von Idealen

$$(0) \subseteq \mathrm{Fitt}_0(A) \subseteq \mathrm{Fitt}_1(A) \subseteq \ldots \subseteq \mathrm{Fitt}_{n-1}(A) \subseteq \mathrm{Fitt}_n(A) = R$$

von R. Dabei ist $\mathrm{Fitt}_{n-1}(A)$ gerade das von den Einträgen von A erzeugte Ideal.

(2) Die Nummerierung der Fittingideale ist auf den ersten Blick merkwürdig, hat aber einen tieferen geometrischen Sinn. Es geht um die Struktur des Quotientenmoduls

$$M = R^n / A(R^m).$$

Der Quotient $R \twoheadrightarrow R/\mathrm{Fitt}_\nu(A)$ beschreibt den (schematheoretischen) Ort in $\mathrm{Spec}(R)$, an dem M einen Rang $> \nu$ hat.

Lemma 11.23 (Fittings Lemma)**.** *Sei R ein Ring, $A \in \mathrm{M}_{n\times m}(R)$ und $S \in \mathrm{GL}_n(R)$ und $T \in \mathrm{GL}_m(R)$. Dann gilt*

$$\mathrm{Fitt}_\nu(A) = \mathrm{Fitt}_\nu(SA) = \mathrm{Fitt}_\nu(AT).$$

Beweis. Man hat nur
$$\mathrm{Fitt}_\nu(SA) \subseteq \mathrm{Fitt}_\nu(A)$$
nachzuweisen, denn dann gilt
$$\mathrm{Fitt}_\nu(A) = \mathrm{Fitt}_\nu(S^{-1}SA) \subseteq \mathrm{Fitt}_\nu(SA) \subseteq \mathrm{Fitt}_\nu(A).$$
Die Aussage für AT erhält man analog durch Transposition.

Berechnen wir den Minor derjenigen Untermatrix $(SA)_{IJ}$ von SA, deren Zeilenindizes nur $i \in I$ und Spaltenindizes nur $j \in J$ durchlaufen ($\#I = \#J$). Wir stellen zunächst fest, daß die Zeilenvektoren von $(SA)_{IJ}$ Linearkombinationen der auf den Indexbereich $j \in J$ eingeschränkten Zeilenvektoren von A (alle Zeilen, nicht nur $i \in I$) sind. Dies folgt unmittelbar aus der Definition der Matrizenmultiplikation. Die Koeffizienten der Linearkombination stehen in der entsprechenden Zeile von S. Sodann berechnen wir die Determinate von $(SA)_{IJ}$ vermöge der Multilinearität in jeder Zeile als eine Linearkombination von Determinaten von auf den Bereich $j \in J$ eingeschränkten Zeilenvektoren von A, also entsprechende Minoren von A. Terme, in denen eine Zeile doppelt auftritt, verschwinden. Damit liegt $\det(SA)_{IJ}$ im entsprechenden Fittingideal von A. □

Beweis des Elementarteilersatzes Satz 11.15 — Eindeutigkeit. Jetzt kümmern wir uns um die Eindeutigkeit der Elemente
$$d_1 \mid d_2 \mid \ldots \mid d_s$$
und der Zahl s. Nach Lemma 11.23 sind die Fittingideale von A und der erreichten Diagonalform SAT die gleichen. Wir berechnen mittels der diagonalen Form (in der nur sehr wenige Minoren von 0 verschieden sind!)
$$\mathrm{Fitt}_\nu(A) = \begin{cases} (\prod_{i=1}^{n-\nu} d_i) & \text{falls } n-\nu \leq s, \\ (0) & \text{falls } n-\nu > s. \end{cases}$$
Da dies Invarianten der Matrix A und nicht nur der diagonalen Form SAT sind, schließen wir, daß sich s und die Elemente d_i bis auf Assoziiertheit eindeutig aus den Fittingidealen von A und damit der Matrix A rekonstruieren lassen. Dies zeigt die Eindeutigkeit der Parameter der diagonalen Form. □

Bemerkung 11.24. Es ist nicht schwer zu zeigen, daß die Fittingideale der Matrix A nur vom Faktormodul
$$\mathrm{coker}(A) = R^n/A(R^m)$$
abhängen. Dies zeigt die Eindeutigkeit im Struktursatz Korollar 11.17 erneut, und zwar mittels Fittingidealen auf konzeptionelle Weise.

Jakob Stix, Institut für Mathematik, Johann Wolfgang Goethe–Universität Frankfurt, Robert-Mayer-Strasse 6–8, 60325 Frankfurt am Main, Germany
E-mail address: stix@math.uni-frankfurt.de