KOMMUTATIVE ALGEBRA

OLAF M. SCHNÜRER

Inhaltsverzeichnis

Date: 17. Dezember 2018.
Skript zur Vorlesung „Kommutative Algebra“ im Wintersemester 2016/17 an der Bergischen Universität Wuppertal.

1. Einleitung

1.1. **Gegenstand der Vorlesung.**

1.1.1. Gegenstand dieser Vorlesung ist die Theorie kommutativer Ringe und ihrer Ideale beziehungsweise allgemeiner der Moduln über ihnen.

1.1.2. Die Motivation kommt aus zwei Gebieten,

(a) der algebraischen Geometrie,
(b) der algebraischen Zahlentheorie.

Aber auch unabhängig von diesen Motivationen ist kommutative Algebra eine interessante eigenständige Disziplin.

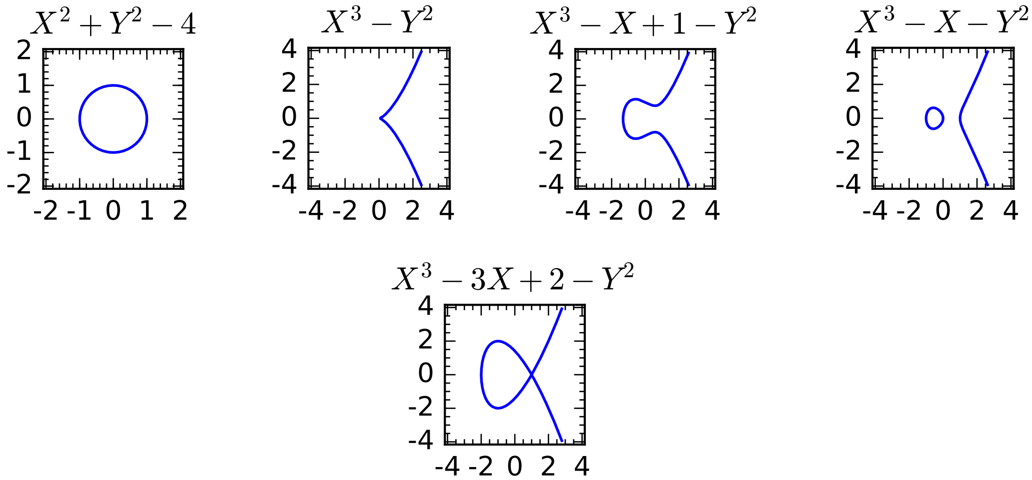
1.2. **Motivation aus der algebraischen Geometrie.**

Definition 1.2.1. Seien k ein Körper und $E \subset k[X_1, \dots, X_n]$ eine beliebige Teilmenge. Sei $\overline{k}$ ein algebraischer Abschluß von k. Betrachte die **gemeinsame Nullstellenmenge** (oder **Verschwindungsmenge**) von E,

$$\mathbf{V}(E) := \{x = (x_1, \dots, x_n) \in \overline{k}^n \mid f(x) = 0 \text{ für alle } f \in E\}. \tag{1.2.1}$$

Mengen dieser Form heißen **über k definierte algebraische Teilmengen** des affinen Raumes $\overline{k}^n$.

Beispiele 1.2.2. Reelle Bilder der durch die angegebenen Gleichungen $f \in \mathbb{R}[X, Y]$ definierten algebraischen Teilmengen $\mathbf{V}(f) := \mathbf{V}(\{f\})$ von $\mathbb{C}^2$, d. h. dargestellt ist $\mathbf{V}(f) \cap \mathbb{R}^2$.



1.2.3. Algebraische Geometrie ist die Theorie der geometrischen Gebilde, die lokal von dieser Form sind. Kommutative Algebra betrachtet die lokalen Aspekte dieser Gebilde. Typische Ringe sind Restklassenringe $k[X_1, \dots, X_n]/\mathfrak{a}$ von Polynomringen nach Idealen.

1.3. **Motivation aus der algebraischen Zahlentheorie.**

Definition 1.3.1. Sei $K/\mathbb{Q}$ eine endliche Körpererweiterung (= ein algebraischer Zahlkörper). Ein Element $a \in K$ heißt **ganz**, falls ein normiertes Polynom $f \in \mathbb{Z}[X]$ mit $f(a) = 0$ existiert.

1.3.2. Die ganzen Elemente bilden einen Teilring R von K, den Ring der **ganzen algebraischen Zahlen**, der in der algebraischen Zahlentheorie eingehend studiert wird (als Ersatz für die ganzen Zahlen $\mathbb{Z}$ in $\mathbb{Q}$).

Beispiele 1.3.3. (a) Für $K = \mathbb{Q}$ gilt $R = \mathbb{Z}$.
(b) (ohne Beweis) Für $K = \mathbb{Q}(\zeta)$ gilt $R = \mathbb{Z}[\zeta]$ wobei ζ eine Einheitswurzel ist. Ist ζ eine n-te Einheitswurzel, so ist ζ Nullstelle des normierten Polynoms $X^n - 1 \in \mathbb{Z}[X]$.
(c) Für $K = \mathbb{Q}(i)$ gilt $R = \mathbb{Z}[i]$.
(d) Für $K = \mathbb{Q}(\sqrt{3})$ gilt $R = \mathbb{Z}[\sqrt{3}]$.
(e) Für $K = \mathbb{Q}(\sqrt{5})$ gilt $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Das normierte Polynom $X^2-X-1 \in \mathbb{Z}[X]$ hat die zwei Nullstellen $\frac{1\pm\sqrt{5}}{2}$.
(f) Allgemeiner gilt (siehe Proposition 7.4.3): Sei $d \in \mathbb{Z}$ quadratfrei (also nicht Vielfaches einer Quadratzahl > 1; insbesondere ist d nicht durch 4 teilber). Für $K = \mathbb{Q}(\sqrt{d})$ gilt

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d = 2,3 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d = 1 \mod 4. \end{cases} \tag{1.3.1}$$

1.3.4. Das Bemerkenswerte dieser Ringe R (gegenüber $k[X_1, \dots, X_n]$ oder $\mathbb{Z}[X_1, \dots, X_n]$) ist, dass sie im Allgemeinen keine faktoriellen Ringe sind, z. B. $\mathbb{Z}(\sqrt{-5})$ (denn $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$).

1.4. **Literatur.**

1.4.1. Das Büchlein Atiyah-MacDonald, Introduction to Commutative Algebra, [AM69] ist wohl am nächsten an der Vorlesung. Es gibt eine große Auswahl anderer Texte, etwa von Matsumura [Mat89], Zariski-Samuel [ZS75a, ZS75b], Bourbaki (Algèbre commutative) [Bou98], Serre (Algèbre locale) [Ser65, Ser00], Grothendieck (EGA = Eléments de géométrie algébrique, chapitre 0), Eisenbud [Eis95], Kunz [Kun80], Peskine [Pes96], Reid [Rei95], Bosch [Bos13].

1.5. **Danksagung.** Ich danke Michael Rapoport für seine Unterlagen zur Kommutativen Algebra. Profitiert habe ich auch von Vorlesungsskripten von Wolfgang Soergel und Jakob Stix.

Für Korrekturen und Hinweise danke ich Julia Sudhoff, Artur Mildner, Annabelle Kahmann und Jürgen Müller.

1.6. **Konventionen.**

Konvention 1.6.1. Die Menge der natürlichen Zahlen ist $\mathbb{N} = \{0, 1, 2, \dots\}$.

Konvention 1.6.2. Die Notation $S \subset T$ meint, dass S Teilmenge von T ist. Die Notation $S \subsetneq T$ meint, dass S eine echte Teilmenge von T ist. Sind S und T Teilmengen einer gegebenen Menge, so schreiben wir $S - T$ für die Menge aller Elemente von S, die nicht in T liegen.

Konvention 1.6.3. Die Notation $\mathcal{P}(M)$ bezeichnet die Potenzmenge einer Menge M.

Konvention 1.6.4. Die Symbole $\hookrightarrow, \twoheadrightarrow, \xrightarrow{\sim}$ bezeichnen injektive, surjektive, bijektive Abbildungen von Mengen oder Ringen oder Moduln oder ähnlichen Strukturen.

2. Grundlegendes zu Ringen und Idealen

2.1. **Ringe.**

Definition 2.1.1. Ein **Ring** ist eine Menge R mit zwei Verknüpfungen **Addition** $+\colon R \times R \to R$ und **Multiplikation** $\cdot\colon R \times R \to R$, $(r, s) \mapsto rs := r \cdot s$, so dass gelten:

(a) $(R, +)$ ist eine abelsche (= kommutative) Gruppe;
(b) $(R, \cdot)$ ist ein Monoid d. h. Multiplikation ist assoziativ (für alle $r, s, t \in R$ gilt $r(st) = (rs)t$) und hat ein neutrales Element (es gibt ein Element $1 \in R$ mit der Eigenschaft $1r = r1 = r$ für alle $r \in R$);
(c) es gelten die Distributivgesetze, d. h. für alle $r, s, t \in R$ gelten:

$$\begin{aligned} r(s+t) &= rs + rt, \\ (r+s)t &= rt + st. \end{aligned}$$

Hier verwenden wir die Punkt-vor-Strich Regel.

Ein Ring R ist **kommutativ** falls $rs = sr$ für alle $r, s \in R$.

Konvention 2.1.2. Das Wort „Ring“ bezeichne im Folgenden einen kommutativen Ring, falls nicht explizit anderweitig betont. Wir verwenden meist lateinische Großbuchstaben $R, S, A, B, C, \dots$, um Ringe zu bezeichnen. (Das französische Wort für Ring ist anneau.)

2.1.3. Das neutrale Element der abelschen Gruppe $(R, +)$ ist eindeutig, wird als Null(element) bezeichnet und als $0 = 0_R$ notiert. Das neutrale Element des Monoids $(R, \cdot)$ ist eindeutig, wird als Eins(element) bezeichnet und als $1 = 1_R$ notiert.

2.1.4. Wir erlauben den Fall $0 = 1$. In diesem Fall besteht unser Ring R aus genau einem Element und wird als Nullring bezeichnet. Statt $R = \{0\}$ schreiben wir normalerweise $R = 0$.

Beispiele 2.1.5. Beispiele für Ringe sind:

(a) die ganzen Zahlen $\mathbb{Z}$ (die natürlichen Zahlen $\mathbb{N}$ sind kein Ring);
(b) jeder Körper, etwa die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$, jeder endliche Körper $\mathbb{F}_q$ (wobei q eine Primzahlpotenz ist);
(c) ist R ein Ring, so ist der Polynomring $R[X]$ in einer Variablen ein Ring; allgemeiner ist $R[X_1, \dots, X_n]$ ein Ring;
(d) ist R ein Ring und M eine beliebige Menge, so ist die Menge der Abbildungen $M \to R$ mit punktweiser Mulitplikation ein Ring. Ein Beispiel ist der Ring der reellwertigen Funktionen auf $\mathbb{R}^n$.

Beispiele für nicht notwendig kommutative Ringe sind:

(e) ist A eine abelsche Gruppe, so ist die Menge $\mathrm{End}(A)$ der Gruppenendomorphismen $A \to A$ in natürlicher Weise ein Ring: Addition ist punktweise definiert per $(f+g)(a) := f(a) + g(a)$, Multiplikation ist Verknüpfung, also $f \cdot g := f \circ g$. Er ist „meist“ nicht kommutativ, etwa für $A = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$;
(f) der Ring $\mathrm{Mat}(n, \mathbb{R})$ der $n \times n$-Matrizen mit reellen Einträgen ist für $n \geq 2$ nicht kommutativ;
(g) allgemeiner ist $\mathrm{End}_k(V)$ nicht kommutativ, falls V ein Vektorraum über einem Körper k ist mit $\dim_k V \geq 2$.

2.2. **Ringmorphismen.**

Definition 2.2.1. Seien A und B Ringe. Ein **Ringmorphismus** oder **Morphismus von Ringen** ist eine Abbildung $f\colon A \to B$ von Mengen, die mit den jeweiligen Additionen, Multiplikationen und Einselementen in der folgenden Weise verträglich ist:

(a) $f(a + a') = f(a) + f(a')$ für alle $a, a' \in A$;
(b) $f(aa') = f(a)f(a')$ für alle $a, a' \in A$;
(c) $f(1) = 1$.

Andere gängige Bezeichnungen sind **Ringhomomorphismus** oder **Homomorphismus von Ringen**. (Morphismen zwischen nicht notwendig kommutativen Ringen sind in derselben Weise definiert.)

Beispiele 2.2.2. (a) Für jeden Ring R (kommutativ oder nicht) gibt es genau einen Ringmorphismus $\mathbb{Z} \to R$. Er bildet ab $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 1 + 1$, etc., $-1 \mapsto -1$, $-2 \mapsto -(1 + 1)$ etc. Jede ganze Zahl kann man so kanonisch als Element von R auffassen. Da $\mathbb{Z} \to R$ im allgemeinen nicht injektiv ist (etwa für $R = \mathbb{Z}/n\mathbb{Z}$) können verschiede ganze Zahlen in R dasselbe Element bezeichnen.

(b) Die offensichtlichen Abbildungen $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ sind injektive Ringmorphismen.

(c) Zu diesen drei Abbildungen gibt es keine Ringmorphismen in die andere Richtung, z. B. gibt es keinen Ringmorphismus $\mathbb{Q} \to \mathbb{Z}$.

(d) (Universelle Eigenschaft des Polynomrings) Sei R ein Ring und $R[X]$ der Polynomring in der Variablen X. Die Abbildung $\mathrm{can}\colon R \to R[X]$, $r \mapsto r$, ist ein Ringmorphismus. Er hat die folgende universelle Eigenschaft: Gegeben ein beliebiger Ringmorphismus $f\colon R \to S$ und ein Element $s \in S$ gibt es genau einen Ringmorphismus $\tilde{f}\colon R[X] \to S$, der X auf s abbildet und das Diagramm

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\mathrm{can}"'] & S \\ R[X] \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

kommutativ macht, d. h. $\tilde{f} \circ \mathrm{can} = f$. Die Abbildung $\tilde{f}$ ist gegeben durch „Auswertung“ $p = p(X) = \sum_{i=0}^{n} p_i X^i \mapsto p(s) = \sum_{i=0}^{n} f(p_i)s^i$ eines Polynoms bei s (samt Anwenden von f auf die Koeffizienten).

(e) Die Abbildung $\mathbb{R}[X] \to \mathbb{C}$, $p(X) \mapsto p(i)$, ist ein surjektiver Ringmorphismus.

2.2.3. Ist A ein Ring, so ist $\mathrm{id}_A\colon A \to A$ ein Morphismus von Ringen. Sind $f\colon A \to B$ und $g\colon B \to C$ Ringmorphismen, so ist auch $gf := g \circ f\colon A \to C$ ein Ringmorphismus.

Definition 2.2.4. Ein Ringmorphismus $f\colon A \to B$ heißt **Ringisomorphismus**, falls es einen Ringmorphismus $g\colon B \to A$ gibt mit $gf = \mathrm{id}_A$ und $fg = \mathrm{id}_B$. Eine offensichtlich äquivalente Bedingung ist, dass f bijektiv ist.

Notation 2.2.5. Um anzudeuten, dass ein Ringmorphismus $A \to B$ surjektiv (bzw. injektiv, bijektiv) ist als Abbildung von Mengen, verwenden wir oft die Notation $f\colon A \twoheadrightarrow B$ (bzw. $f\colon A \hookrightarrow B$, $f\colon A \xrightarrow{\sim} B$).

Definition 2.2.6. Sei R ein Ring. Ein **Unterring** von R ist eine Teilmenge U von R, die unter Addition und Multiplikation abgeschlossen ist, mit jedem Element r auch sein additives Inverses $-r$ enthält, und die Eins 1_R enthält.

2.2.7. Es ist klar, dass ein Unterring mit der induzierten Addition und Multiplikation selbst ein Ring ist. Dies rechtfertigt die Terminologie. Die Inklusionsabbildung $U \hookrightarrow R$ ist ein injektiver Ringmorphismus.

Beispiele 2.2.8. Jeder der Ringe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{C}[X]$ ist ein Unterring seiner Nachfolger.

Beispiel 2.2.9. Ist $f\colon A \to B$ ein Ringmorphismus, so ist sein **Bild**

$$\mathrm{im}(f) := f(A)$$

ein Unterring von B und die induzierte Abbildung $A \twoheadrightarrow \mathrm{im} f$ ist ein surjektiver Ringmorphismus. Insbesondere faktorisiert $f\colon A \to B$ als

$$A \twoheadrightarrow \mathrm{im}(f) \hookrightarrow B.$$

2.3. **Ideale und Restklassenringe.**

Definition 2.3.1. Ein **Ideal** in einem Ring R ist eine additive Untergruppe $\mathfrak{a} \subset R$ so dass $rx \in \mathfrak{a}$ gilt für alle $r \in R$ und $x \in \mathfrak{a}$.

2.3.2. Gegeben ein Element $x \in R$ bilden seine Vielfachen rx, für $r \in R$, ein Ideal in R. Wir notieren dieses Ideal als (x) oder Rx oder xR.

Definition 2.3.3. Ein Ideal $\mathfrak{a}$ heißt **Hauptideal** falls es ein Element $x \in R$ gibt mit $\mathfrak{a} = (x)$. Gegeben $x \in R$ nennen wir (x) das **von x erzeugte Hauptideal**.

Beispiele 2.3.4. (a) In jedem Ring R gibt es das Ideal $R = (1)$ und das Nullideal $0 := \{0\} = (0)$. Diese beiden Ideale stimmen genau im Nullring überein.
(b) Alle Ideale im Ring $\mathbb{Z}$ sind von der Form $n\mathbb{Z}$ für $n \in \mathbb{Z}$.

Sei $f\colon A \to B$ ein Ringmorphismus
(c) Sein **Kern** $\ker(f) = \{a \in A \mid f(a) = 0\} = f^{-1}(0)$ ist ein Ideal.
(d) Allgemeiner sind Urbilder von Idealen Ideale: Ist $\mathfrak{b}$ ein Ideal in B, so ist $f^{-1}(\mathfrak{b})$ ein Ideal in A.
(e) Bilder von Idealen unter surjektiven Ringmorphismen sind Ideale: Ist f surjektiv und $\mathfrak{a}$ ein Ideal in A, so ist $f(\mathfrak{a})$ ein Ideal in B. (Surjektivität ist nötig: Betrachte das Bild von $2\mathbb{Z}$ unter $\mathbb{Z} \hookrightarrow \mathbb{Q}$.)

Proposition 2.3.5 (Restklassenring und universelle Eigenschaft)**.** *Sei $\mathfrak{a}$ ein Ideal in einem Ring A. Dann gelten:*
(a) Es gibt genau eine Verknüpfung „Multiplikation“ auf der Restklassengruppe $A/\mathfrak{a}$ derart, dass die kanonische Abbildung
$$\mathrm{can}\colon A \to A/\mathfrak{a}$$
mit den Multiplikationen verträglich ist, d. h. $\mathrm{can}(ab) = \mathrm{can}(a)\mathrm{can}(b)$.
*(b) Mit dieser Multiplikation wird $A/\mathfrak{a}$ ein Ring und $\mathrm{can}\colon A \to A/\mathfrak{a}$ ein surjektiver Ringmorphismus mit Kern $\mathfrak{a}$. Er heißt der **Restklassenring** oder **Faktorring** oder **Quotient(enring)** von A nach $\mathfrak{a}$.*
(c) (Universelle Eigenschaft) Jeder Ringmorphismus $f\colon A \to B$ mit $f(\mathfrak{a}) = \{0\}$ faktorisiert eindeutig über $\mathrm{can}\colon A \to A/\mathfrak{a}$, es gibt also genau einen Ringmorphismus $\overline{f}\colon A/\mathfrak{a} \to B$ so dass $f = \overline{f} \circ \mathrm{can}$ gilt, d. h. so dass das Diagramm
$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\mathrm{can}"'] & & B \\ & A/\mathfrak{a} \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$
kommutativ ist.

Erinnerung 2.3.6. Bevor wir dies beweisen, erinnern wir an die Definition der Restklassengruppe (oder Quotientengruppe) $A/\mathfrak{a}$ einer abelschen Gruppe A nach einer Untergruppe $\mathfrak{a}$ (die automatisch Normalteiler ist). Die Elemente von $A/\mathfrak{a}$ sind die Nebenklassen von $\mathfrak{a}$ in A. Sei $\overline{x} := x + \mathfrak{a} := \{x + a \mid a \in \mathfrak{a}\}$ die Nebenklasse von x. Es gilt $\overline{x} = \overline{y}$ genau dann, wenn $x - y \in \mathfrak{a}$. Die Addition auf $A/\mathfrak{a}$ ist gegeben durch $\overline{x} + \overline{y} = \overline{x + y}$ und die offensichtliche Abbildung $\mathrm{can}\colon A \to A/\mathfrak{a}$, $x \mapsto \mathrm{can}(x) = \overline{x}$, ist ein surjektiver Morphismus abelscher Gruppen mit Kern $\mathfrak{a}$. Ist $f\colon A \to B$ ein beliebiger Morphismus abelscher Gruppen mit $\mathfrak{a} \subset \ker(f)$, so gibt es genau einen Morphismus $\overline{f}\colon A/\mathfrak{a} \to B$ abelscher Gruppen mit $f = \overline{f} \circ \mathrm{can}$.

Beweis. (a) Gegeben zwei Teilmengen S, T von A definieren wir
$$S \odot T := ST + \mathfrak{a} := \{st + a \mid s \in S, t \in T, a \in \mathfrak{a}\}.$$
Dies definiert eine Verknüpfung auf der Potenzmenge von A. Da $\mathfrak{a}$ ein Ideal ist, gilt
$$\overline{x} \odot \overline{y} = (x + \mathfrak{a}) \odot (y + \mathfrak{a}) = \{(x + a)(y + a') + a'' \mid a, a', a'' \in \mathfrak{a}\} = xy + \mathfrak{a} = \overline{xy}.$$
Wir erhalten so die gesuchte Verknüpfung auf der Menge $A/\mathfrak{a}$ der Nebenklassen. Eindeutigkeit ist offensichtlich.

(b) Wir wissen bereits, dass $\mathrm{can}\colon A \to A/\mathfrak{a}$ ein surjektiver Morphismus abelscher Gruppen ist mit Kern $\mathfrak{a}$ und verträglich mit den Multiplikationen. Daraus folgen sofort alle Behauptungen.

(c) Nach der obigen Erinnerung wissen wir, dass es genau einen Morphismus $\overline{f}\colon A/\mathfrak{a} \to B$ abelscher Gruppen gibt mit $\overline{f} \circ \mathrm{can} = f$. Dieser ist kompatibel mit Multiplikationen und Einselementen, da can ein surjektiver Ringmorphismus ist. □

2.3.7. Insbesondere ist jedes Ideal Kern eines Ringmorphismus.

2.3.8. Im Folgenden verwenden wir natürlich nicht die komische Notation $\odot$ für die Multiplikation auf $A/\mathfrak{a}$, sondern schreiben schlicht ab oder $a \cdot b$ statt $a \odot b$ für $a, b \in A/\mathfrak{a}$. Beachte, dass jedes Element $a \in A/\mathfrak{a}$ die Form $a = \overline{x}$ hat für ein $x \in A$. Es gilt $\overline{x} \cdot \overline{y} = \overline{xy}$ für $x, y \in A$.

Notation 2.3.9. Gegeben Elemente $x, y \in A$ schreibt man manchml $x = y \pmod{\mathfrak{a}}$ für die Aussage $x - y \in \mathfrak{a}$. Äquivalent ist die Aussage $\overline{x} = \overline{y}$ in $A/\mathfrak{a}$. Manchmal schreibt man stattdessen einfach $x = y$ in $A/\mathfrak{a}$; es ist dann jedoch wichtig zu sagen, wo die Gleichheit stattfindet.

Beispiel 2.3.10. Betrachte das Ideal $12\mathbb{Z}$ im Ring $\mathbb{Z}$. Dann ist der Restklassenring $\mathbb{Z}/12\mathbb{Z}$ der „Ring der Uhrzeiten". Er hat die zwölf Elemente $\overline{0}, \overline{1}, \ldots, \overline{11}$. Es gilt $\overline{9} + \overline{5} = \overline{14} = \overline{2}$, d. h. 5 Stunden nach 9 ist es 2 ("clockwise arithmetic"). Natürlich kann man auch multiplizieren, es gilt etwa $\overline{3} \cdot \overline{8} = \overline{24} = \overline{0}$ in $\mathbb{Z}/12\mathbb{Z}$ (nach drei 8-Stunden-Schichten ist ein Tag vorbei).

Beispiel 2.3.11 (Homomorphiesatz)**.** Sei $f\colon A \to B$ ein Ringmorphismus. Wegen $f(\ker(f)) = \{0\}$ faktorisiert f eindeutig als

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\mathrm{can}"', two heads] & & B \\
& A/\ker(f) \arrow[ur, hook, "\overline{f}"'] &
\end{tikzcd}$$

Es ist klar, dass $\overline{f}$ injektiv ist (wie bereits im Diagramm angedeutet): Sei $x \in A$ mit $\overline{x} \in \ker(\overline{f})$. Aus $0 = \overline{f}(\overline{x}) = f(x)$ folgt $x \in \ker(f)$ und somit $\overline{x} = x + \ker(f) = 0 + \ker(f) = \overline{0} = 0$.

Wegen $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$ erhalten wir nach Beispiel 2.2.9 genauer ein kommutatives Diagramm

$$\begin{tikzcd}
A \arrow[r, "f", two heads] \arrow[d, "\mathrm{can}"', two heads] & B \\
A/\ker(f) \arrow[r, "\sim", two heads] & \mathrm{im}(f) \arrow[u, hook]
\end{tikzcd}$$

Die untere horizontale Abbildung ist ein Ringisomorphismus. Diese Aussage wird als Homomorphiesatz bezeichnet.

Proposition 2.3.12. *Sei $\mathfrak{a}$ ein Ideal in einem Ring A und* $\mathrm{can}\colon A \to A/\mathfrak{a}$ *die kanonische Surjektion. Dann ist*

$$\begin{aligned}
\{\textit{Ideale in } A, \textit{ die } \mathfrak{a} \textit{ enthalten}\} &\xrightarrow{\sim} \{\textit{Ideale in } A/\mathfrak{a}\}, \\
\mathfrak{b} &\mapsto \overline{\mathfrak{b}} := \mathrm{can}(\mathfrak{b}) = \{\overline{b} = b + \mathfrak{a} \mid b \in \mathfrak{b}\}, \\
\mathrm{can}^{-1}(\mathfrak{c}) &\leftarrow\!\shortmid \mathfrak{c},
\end{aligned}$$

eine Bijektion[1] *von Mengen.*

2.3.13. Gegeben Untergruppen $\mathfrak{a} \subset \mathfrak{b} \subset A$ einer abelschen Gruppe A ist die natürliche Abbildung $\mathfrak{b}/\mathfrak{a} \to A/\mathfrak{a}$ injektiv und hat als Bild gerade $\mathrm{can}(\mathfrak{b})$. Insofern ist $\mathfrak{b}/\mathfrak{a}$ auch eine gute Notation für $\mathrm{can}(\mathfrak{b})$.

Beweis. Die beiden Abbildungen sind wohldefiniert nach Beispiele 2.3.4 (da can surjektiv ist). Wir zeigen, dass sie zueinander inverse Bijektionen sind.

Sei $\mathfrak{b}$ ein Ideal in A mit $\mathfrak{a} \subset \mathfrak{b}$. Es ist zu zeigen, dass $\mathfrak{b} = \mathrm{can}^{-1}(\mathrm{can}(\mathfrak{b}))$. Die Inklusion $\subset$ ist trivial und gilt für jede Abbildung von Mengen. Sei nun $x \in \mathrm{can}^{-1}(\mathrm{can}(\mathfrak{b}))$. Dann folgt $\overline{x} \in \mathrm{can}(\mathfrak{b})$, d. h. es gibt ein $b \in \mathfrak{b}$ mit $\overline{x} = \overline{b}$ in $A/\mathfrak{a}$. Dies bedeutet $x - b \in \mathfrak{a} \subset \mathfrak{b}$ und somit $x = (x - b) + b \in \mathfrak{b}$.

[1] Genauer meinen wir hier und in ähnlichen Situationen im Folgenden, dass die beiden auf Elementen angegebenen Abbildungen invers zueinander sind.

Sei nun $\mathfrak{c}$ ein Ideal in $A/\mathfrak{a}$. Zu zeigen ist $\operatorname{can}(\operatorname{can}^{-1}(\mathfrak{c})) = \mathfrak{c}$. Dies gilt, da can eine surjektive Abbildung von Mengen ist.

Dies zeigt, dass die beiden Abbildungen invers zueinander sind. □

2.4. **Nullteiler, nilpotente Elemente, Einheiten.** Sei R ein Ring.

2.4.1. Für jedes Element $x \in R$ gilt natürlich $x0 = 0$ und somit ist x ein Teiler von Null. Ein Nullteiler im Sinne der folgenden Definition ist ein Element, dass Null in nichttrivialer Weise teilt.

Definition 2.4.2. Ein Element $x \in R$ heißt **Nullteiler**, falls es ein Element $y \neq 0$ in R mit $xy = 0$ gibt.

Beispiele 2.4.3. (a) Ist R nicht der Nullring, so ist 0 ein Nullteiler.
(b) Das Einselement 1 eines Ringes ist nie ein Nullteiler.
(c) Jedes Vielfache eines Nullteilers ist ein Nullteiler.
(d) Die Nullteiler in $\mathbb{Z}/12\mathbb{Z}$ sind $0, 2, 3, 4, 6, 8, 9, 10$ (wir haben hier den Überstrich weggelassen). (Insbesondere bilden die Nullteiler kein Ideal: $9 + 4 = 1$ ist kein Nullteiler.)
(e) Null ist der einzige Nullteiler in einem Körper.
(f) Null ist der einzige Nullteiler in $\mathbb{Z}$.

2.4.4 (Kürzen in Ringen)**.** Ist R ein Ring und $a \in R$ kein Nullteiler, so folgt aus $ax = ay$ schon $x = y$. In der Tat gilt $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.

Definition 2.4.5. (a) Ein Ring heißt **nullteilerfrei**, wenn er außer der Null keinen Nullteiler enthält: Aus $xy = 0$ folgt $x = 0$ oder $y = 0$.
(b) Ein Ring heißt **Integritätsbereich**, wenn er nullteilerfrei ist und nicht der Nullring ist.

Beispiele 2.4.6. (a) Ein Ring R ist nullteilerfrei genau dann, wenn für alle $x, y \in R$ gilt: Ist $xy = 0$, so ist $x = 0$ oder $y = 0$.
(b) Der Nullring ist nullteilerfrei, aber kein Integritätsbereich.
(c) Körper sind Integritätsbereiche.
(d) $\mathbb{Z}$ ist ein Integritätsbereich (aber kein Körper).
(e) Ist R ein Integritätsbereich, so ist $R[X]$ ein Integritätsbereich (betrachte die Leitkoeffizienten).

Erinnerung 2.4.7. Ein **Hauptidealring** ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Definition 2.4.8. Ein Element x eines Ringes R ist **nilpotent** falls $x^n = 0$ für ein $n \in \mathbb{N}$.

2.4.9. Das Nullelement 0 ist nilpotent.

2.4.10. Ist R nicht der Nullring, so ist jedes nilpotente Element ein Nullteiler.

Beweis. Sei $x \in R$ nilpotent. Sei $n \in \mathbb{N}$ minimal mit $x^n = 0$. Dann gilt $n \geq 1$, da $x^0 = 1 \neq 0$. Es folgt $x^{n-1} \neq 0$ und $x^{n-1} \cdot x = x^n = 0$. Also ist x Nullteiler. □

Proposition 2.4.11. *Die Menge* $\operatorname{Nil}(R)$ *der nilpotenten Elemente eines Ringes R ist ein Ideal. Im Faktorring* $R/\operatorname{Nil}(R)$ *gibt es keine nilpotenten Elemente* $\neq 0$.

Beweis. Für $r \in R$ und nilpotentes $x \in R$ ist offensichtlich rx nilpotent. Insbesondere ist $-x = (-1)x$ nilpotent. Seien $x, y \in \operatorname{Nil}(R)$. Gelte $x^m = 0$ und $y^n = 0$ für $m, n > 0$. Dann gilt $(x + y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i} = 0$, also $x + y \in \operatorname{Nil}(R)$.

Sei nun $\overline{x} \in R/\operatorname{Nil}(R)$ nilpotent. Gelte $0 = \overline{x}^n = \overline{x^n}$ für ein $n \in \mathbb{N}$. Dies bedeutet $x^n \in \operatorname{Nil}(R)$, also gibt es ein $m \in \mathbb{N}$ mit $0 = (x^n)^m = x^{nm}$. Es folgt $x \in \operatorname{Nil}(R)$ und $\overline{x} = 0$. □

Definition 2.4.12. Das Ideal der nilpotenten Elemente eines Ringes R heißt das **Nilradikal** von R.

Definition 2.4.13. Eine Element $x \in R$ ist eine **Einheit**, falls es ein Teiler von 1 ist: Es gibt ein $y \in R$ mit $xy = 1$. Ein Element ist **invertierbar**, falls es eine Einheit ist.

2.4.14. Ein Element y wie oben ist eindeutig bestimmt (aus $xy' = 1$ folgt $y = y1 = yxy' = 1y' = y'$), wird x^{-1} notiert und als Inverses von x bezeichnet.

Notation 2.4.15. Sei $R^\times$ die Menge der Einheiten in R. Es ist klar, dass $R^\times$ eine (multiplikative) abelsche Gruppe ist.

2.4.16. Es gilt $x \in R^\times$ genau dann, wenn $(x) = R$.

Lemma 2.4.17. *Ist x eine Einheit und y nilpotent, so ist $x + y$ eine Einheit.*

Beweis. Wir zeigen äquivalent, dass $1 + x^{-1}y$ eine Einheit ist. Da $x^{-1}y$ nilpotent ist, genügt es zu zeigen, dass für jedes nilpotente Element z das Element $1 + z$ eine Einheit ist. Da z nilpotent ist, ist die Summe $u := 1 - z + z^2 - z^3 \pm \dots$ endlich. Es folgt $(1 + z)u = u + z - z^2 + z^3 \mp \dots = 1$. □

2.4.18. Ist $f: A \to B$ ein Ringmorphismus, so gilt $f(A^\times) \subset B^\times$.

Erinnerung 2.4.19. Ein **Körper** ist ein Ring R mit $1 \neq 0$, in dem jedes Element ungleich Null eine Einheit ist: $R - \{0\} = R^\times$.

2.4.20. Jeder Körper ist ein Integritätsbereich, aber nicht umgekehrt.

Proposition 2.4.21. *Sei R ein Ring $\neq 0$. Dann sind äquivalent:*

(a) R ist ein Körper;
(b) die einzigen Ideale in R sind 0 und R;
(c) jeder Ringmorphismus von R in einen Ring $B \neq 0$ ist injektiv.

Beweis. (a) $\Rightarrow$ (b) Sei $\mathfrak{a}$ ein Ideal in R. Ist $\mathfrak{a} \neq 0$, so gibt es ein Element $a \in \mathfrak{a}$ mit $a \neq 0$. Dann ist a invertierbar und somit $1 = a^{-1}a \in (a) \subset \mathfrak{a}$, also $\mathfrak{a} = R$.

(b) $\Rightarrow$ (c) Sei $\varphi: R \to B$ ein Ringmorphismus mit $B \neq 0$. Der Kern $\ker(\varphi)$ ist ein Ideal in R und somit entweder R oder 0. Im Fall $\ker(\varphi) = R$ ist $1 = \varphi(1) \in \varphi(R) = 0$ und damit $B = 0$ im Widerspruch zur Annahme. Also gilt $\ker(\varphi) = 0$ und φ ist injektiv.

(c) $\Rightarrow$ (a) Wir wissen bereits, dass $R \neq 0$. Sei $a \in R - \{0\}$. Wir müssen zeigen, dass a eine Einheit ist. Betrachte den kanonischen Ringmorphismus $R \to R/(a)$. Er ist nicht injektiv (das Element $a \neq 0$ liegt im Kern), und somit folgt $R/(a) = 0$. Also $\overline{1} = \overline{0}$ und somit $1 = 1 - 0 \in (a)$. Also ist a eine Einheit. □

2.5. **Schnitt, Summe, Produkt von Idealen, erzeugtes Ideal.**

2.5.1. Gegeben Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in einem Ring, ist $\mathfrak{a} \cap \mathfrak{b}$ wieder ein Ideal. Es ist das größte Ideal (bezüglich Inklusion), dass in $\mathfrak{a}$ und $\mathfrak{b}$ enthalten ist. Allgemeiner ist $\bigcap_{i \in I} \mathfrak{a}_i$ das größte Ideal, das in gegebenen Idealen $\mathfrak{a}_i$ enthalten ist (dabei ist I nicht notwendig endlich).

Definition 2.5.2. Gegeben eine beliebige Teilmenge T eines Ringes A definiert man das **von T erzeugte Ideal** $\langle T \rangle$ als Menge aller endlichen A-Linearkombinationen von Elementen aus T, in Formeln

$$\langle T \rangle = \{\sum_{i=1}^{n} a_i t_i \mid n \in \mathbb{N}, a_i \in A, t_i \in T\}.$$

2.5.3. Die Menge $\langle T \rangle$ ist offensichtlich ein Ideal. Das Ideal $\langle T \rangle$ kann alternativ beschrieben werden als das kleinste Ideal, das T enthält, oder als Schnitt aller Ideale, die T enthalten, in Formeln

$$\langle T \rangle := \bigcap_{\mathfrak{a} \subset A \text{ Ideal mit } T \subset \mathfrak{a}} \mathfrak{a}. \tag{2.5.1}$$

Beispiel 2.5.4. Gegeben $x \in A$ gilt $(x) = \langle \{x\} \rangle$.

2.5.5. Gegeben Ideale $\mathfrak{a}$ und $\mathfrak{b}$ ist $\mathfrak{a} \cup \mathfrak{b}$ im Allgemeinen kein Ideal, zum Beispiel ist $2\mathbb{Z} \cup 3\mathbb{Z}$ kein Ideal in $\mathbb{Z}$. Wir definieren die **Summe** $\mathfrak{a} + \mathfrak{b}$ durch

$$\mathfrak{a} + \mathfrak{b} := \langle \mathfrak{a} \cup \mathfrak{b} \rangle = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}. \tag{2.5.2}$$

Allgemeiner ist die **Summe** $\sum_{i \in I} \mathfrak{a}_i$ definiert als $\langle \bigcup_{i \in I} \mathfrak{a}_i \rangle$ oder explizit als Menge aller Summen $\sum_{i \in I_0} a_i$, wobei $I_0 \subset I$ eine endliche Teilmenge ist und $a_i \in \mathfrak{a}_i$ für alle $i \in I_0$.

Notation 2.5.6. Gegeben Elemente $x_1, \dots, x_n$ nennen wir $(x_1, \dots, x_n) := (x_1) + \dots + (x_n) = \langle \{x_1, \dots, x_n\} \rangle$ das **von $x_1, \dots, x_n$ erzeugte Ideal**.

2.5.7. Allgemeiner gilt $\sum_{t \in T} (t) = \langle T \rangle$.

2.5.8. Gegeben Ideale $\mathfrak{a}$ und $\mathfrak{b}$ ist die Menge aller Produkte $\{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ im Allgemeinen kein Ideal. Wir definieren **das Produkt** $\mathfrak{ab} = \mathfrak{a} \cdot \mathfrak{b}$ als das von dieser Menge erzeugte Ideal. Es gilt offenbar $\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$. Gegeben endlich viele Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ definiert man $\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \dots \cdot \mathfrak{a}_n$ analog. Notation: $\mathfrak{a}^n = \mathfrak{a} \cdot \mathfrak{a} \cdot \dots \cdot \mathfrak{a}$. Spezialfälle sind $\mathfrak{a}^0 = R$, $\mathfrak{a}^1 = \mathfrak{a}$.

2.5.9. Es gilt $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ und $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$ für Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$.

2.6. **Primideale und maximale Ideale.** Die beiden folgenden Definitionen sind äußerst wichtig, insbesondere in der algebraischen Geometrie. Sei R ein Ring.

Definition 2.6.1. Ein Ideal $\mathfrak{p}$ in R ist ein **Primideal**, falls $\mathfrak{p} \neq R$ und für alle $x, y \in R$ gilt: $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Ein Ideal ist **prim**, falls es ein Primideal ist.

2.6.2. Ein echtes Ideal $\mathfrak{p} \subsetneq R$ ist prim genau dann, wenn sein Komplement $R - \mathfrak{p}$ abgeschlossen unter Multiplikation ist.

Definition 2.6.3. Ein Ideal $\mathfrak{m}$ in R ist **maximal**, falls es maximal unter den Idealen $\mathfrak{b} \neq R$ ist: es gilt $\mathfrak{m} \neq R$ und gegeben eine Inklusion von Idealen $\mathfrak{m} \subset \mathfrak{a}$ folgt entweder $\mathfrak{m} = \mathfrak{a}$ oder $\mathfrak{a} = R$.

Beispiel 2.6.4. Sei R ein faktorieller Ring und $f \in R$. Dann ist f genau dann irreduzibel, wenn (f) ein Primideal ist (wegen Eindeutigkeit der Faktorisierung in irreduzible Faktoren). Ist R sogar ein Hauptidealring und ist f irreduzibel, so ist (f) maximal. Insbesondere gelten:

(a) Ist p eine Primzahl, so ist (p) ein maximales Ideal von $\mathbb{Z}$ (da $\mathbb{Z}$ ein Hauptidealring ist).
(b) Ist k ein Körper und $f \in k[X_1, \dots, X_n]$ irreduzibel, so ist (f) ein Primideal.
(c) Ist k ein Körper und $f \in k[X]$ irreduzibel, so ist (f) ein maximales Ideal (da $k[X]$ ein Hauptidealring ist).

Proposition 2.6.5. *Sei R ein Ring.*

(a) Ein Ideal $\mathfrak{p}$ ist prim genau dann, wenn $R/\mathfrak{p}$ ein Integritätsbereich ist.

Insbesondere ist das Nullideal prim genau dann, wenn R ein Integritätsbereich ist (da $R \xrightarrow{\sim} R/0$).

(b) Ein Ideal $\mathfrak{m}$ ist maximal genau dann, wenn $R/\mathfrak{m}$ ein Körper ist.

Insbesondere ist jedes maximale Ideal prim, und das Nullideal ist maximal genau dann, wenn R ein Körper ist.

Beweis. (a) Die Bedingung $\mathfrak{p} \subsetneq R$ ist äquivalent zu $R/\mathfrak{p} \neq 0$. Gelte $\mathfrak{p} \subsetneq R$. Dann ist $\mathfrak{p}$ ein Primideal genau dann, wenn für alle $x, y \in R$ aus $xy \in \mathfrak{p}$ folgt, dass $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Der Ring $R/\mathfrak{p}$ ist nullteilerfrei genau dann, wenn für alle $x, y \in R$ aus $\overline{xy} = 0$ folgt, dass $\overline{x} = 0$ oder $\overline{y} = 0$. Die Behauptung folgt.

(b) Sei $\mathfrak{m}$ ein maximales Ideal. Wegen $\mathfrak{m} \subsetneq R$ folgt $R/\mathfrak{m} \neq 0$. Sei $x \in R$ mit $\overline{x} \neq 0$, also $x \notin \mathfrak{m}$. Wegen $\mathfrak{m} \subsetneq \mathfrak{m} + (x)$ und Maximalität von $\mathfrak{m}$ folgt $R = \mathfrak{m} + (x)$. Also gibt es ein $m \in \mathfrak{m}$ und ein $y \in R$ mit $1 = m + yx$. Es folgt $\overline{1} = \overline{m} + \overline{yx} = \overline{yx}$. Also ist $\overline{x}$ invertierbar und $R/\mathfrak{m}$ ein Körper.

Sei $R/\mathfrak{m}$ ein Körper. Da ein Körper genau zwei Ideale hat (das Nullideal und den ganzen Körper), gibt es nach Proposition 2.3.12 genau zwei Ideale in R, die $\mathfrak{m}$ enthalten, nämlich $\mathfrak{m}$ und R. Also ist $\mathfrak{m}$ ein maximales Ideal. □

Bemerkung 2.6.6. Sei $\varphi\colon A \to B$ ein Ringmorphismus und $I \subset B$ ein Ideal. Der Kern von $A \xrightarrow{\varphi} B \to B/I$ ist $\varphi^{-1}(I)$, und wir erhalten ein kommutatives Diagramm

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, two heads] & B \arrow[d, two heads] \\ A/\varphi^{-1}(I) \arrow[r, hook] & B/I \end{tikzcd}$$

mit injektiver unterer Horizontale (siehe Beispiel 2.3.11). Wir können also $A/\varphi^{-1}(I)$ als Unterring von R/I auffassen. Ist φ surjektiv, so ist die untere Horizontale ebenfalls surjektiv und damit ein Ringisomorphismus.

Proposition 2.6.7. *Urbilder von Primidealen unter Ringmorphismen sind Primideale.*

Ist insbesondere $\varphi\colon A \to B$ ein Ringmorphismus in einen Integritätsbereich, so ist $\ker(\varphi)$ ein Primideal.

Beweis. Sei $\varphi\colon A \to B$ ein Ringmorphismus und sei $I \subset B$ ein Primideal. Nach Bemerkung 2.6.6 ist $A/\varphi^{-1}(I) \hookrightarrow B/I$ ein injektiver Ringmorphismus. Wir verwenden Proposition 2.6.5.(a) zweimal: Zunächst ist B/I ein Integritätsbereich. Da Unterringe von Integritätsbereichen Integritätsbereiche sind, ist $A/\varphi^{-1}(I)$ ein Integritätsbereich. Also ist $\varphi^{-1}(I)$ prim. Alternativ kann man diese Behauptung auch einfach nachrechnen. Schließlich ist nach Proposition 2.6.5.(a) in jedem Integritätsbereich das Nullideal prim. □

Proposition 2.6.8. *Seien $\varphi\colon A \twoheadrightarrow B$ ein surjektiver Ringmorphismus und $I \subset R$ ein Ideal. Dann ist das Ideal I prim bzw. maximal genau dann, wenn $\varphi^{-1}(I)$ prim bzw. maximal ist.*

Ist insbesondere $\varphi\colon R \to k$ ein surjektiver Ringmorphismus in einen Körper k, so ist $\ker(f)$ *ein maximales Ideal in R.*

Beweis. Nach Bemerkung 2.6.6 erhalten wir einen Ringisomorphismus $A/\varphi^{-1}(I) \xrightarrow{\sim} R/I$. Nun verwende Proposition 2.6.5. □

Beispiel 2.6.9. Seien $a_1, \dots, a_n$ Elemente eines Körpers k. Dann ist der Kern der Auswertungsabbildung $\mathrm{ev}_a\colon k[X_1, \dots, X_n] \to k$, $f \mapsto f(a) := f(a_1, \dots, a_n)$, ein maximales Ideal in $k[X_1, \dots, X_n]$ (nach Proposition 2.6.8.

Man überlegt sich leicht, dass $\ker(\mathrm{ev}_a) = (X_1 - a_1, \dots, X_n - a_n)$ gilt (dies gilt für einen beliebigen Ring k).

Beweis. Die Inklusion $(X_1 - a_1, \dots, X_n - a_n) \subset \ker(\mathrm{ev}_a)$ ist offensichtlich. Sei $f = \sum_\alpha f_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$ ein Polynom mit Koeffizienten $f_\alpha \in k$. In $k[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n)$ gilt offenbar $\overline{f} = \sum_\alpha \overline{f_\alpha}\, \overline{X}_1^{\alpha_1} \dots \overline{X}_n^{\alpha_n} = \sum_\alpha \overline{f_\alpha} \overline{a}_1^{\alpha_1} \dots \overline{a}_n^{\alpha_n} = \overline{f(a)}$, also $f - f(a) \in (X_1 - a_1, \dots, X_n - a_n)$. Die Bedingung $f \in \ker(\mathrm{ev}_a)$ besagt schlicht $f(a) = 0$ und impliziert $f = f - f(a) \in (X_1 - a_1, \dots, X_n - a_n)$. □

Korollar 2.6.10. *Unter der Bijektion aus Proposition 2.3.12 ist ein Ideal $\mathfrak{b}$ mit $\mathfrak{a} \subset \mathfrak{b} \subset A$ prim bzw. maximal in A genau dann, wenn $\overline{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}$ prim bzw. maximal in $A/\mathfrak{a}$ ist.*

Beweis. Das folgt sofort aus Proposition 2.6.8. □

2.6.11. Der Vollständigkeit halber (und da sie einen prominenten Namen hat) geben wir die folgende einfache Folgerung aus Bemerkung 2.6.6.

Satz 2.6.12 ((Zweiter) Isomorphiesatz)**.** *Seien $\mathfrak{a} \subset \mathfrak{b}$ Ideale in einem Ring A. Dann ist $\mathfrak{b}/\mathfrak{a}$ ein Ideal in $A/\mathfrak{a}$, und die Abbildung*

$$A/\mathfrak{b} \xrightarrow{\sim} (A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}),$$
$$\overline{r} = r + \mathfrak{b} \mapsto \overline{\overline{r}} = (r + \mathfrak{a}) + \mathfrak{b}/\mathfrak{a},$$

ist ein Ringisomorphismus.

Beweis. Wende Bemerkung 2.6.6 an auf $\mathrm{can}\colon A \to A/\mathfrak{a}$ und das Ideal $\mathfrak{b}/\mathfrak{a}$ von $A/\mathfrak{a}$. Sein Urbild in A ist $\mathfrak{b}$. Da can surjektiv ist, erhalten wir den behaupteten Ringisomorphismus. □

Satz 2.6.13. *In jedem Ring $R \neq 0$ gibt es ein maximales Ideal.*

Erinnerung 2.6.14. Wir erinnern an das Lemma von Zorn. Sei S eine **partiell geordnete** Menge (partially ordered set oder poset im Englischen), d. h. S ist eine Menge zusammen mit einer Relation $\leq$, so dass gelten: $\forall x \in S : x \leq x$ (reflexiv), $\forall x, y, z \in S : x \leq y$ und $y \leq z \Rightarrow x \leq z$ (transitiv), $\forall x, y \in S : x \leq y$ und $y \leq x \Rightarrow x = y$ (antisymmetrisch). Eine **Kette** in S ist eine total geordnete Teilmenge $T \subset S$ (d. h. für alle $x, y \in T$ gilt $x \leq y$ oder $y \leq x$). Eine **obere Schranke** einer Teilmenge $T \subset S$ ist ein Element $s \in S$ mit $t \leq s$ für alle $t \in T$. Ein **maximales Element** von S ist ein Element $s \in S$, so dass für jedes beliebige Element $x \in S$ gilt: $s \leq x \Rightarrow s = x$.

Lemma 2.6.15. *[Lemma von (Kuratowski-)Zorn] Sei S eine nichtleere partiell geordnete Menge mit der Eigenschaft, dass jede nichtleere Kette in S (= jede total geordnete Teilmenge von S) eine obere Schranke in S hat. Dann besitzt S ein maximales Element.*

Das Lemma von Zorn ist äquivalent zum Auswahlaxiom (siehe Wikipedia) und hat somit axiomatischen Charakter.

Beweis. Sei S die Menge aller echten Ideale $\mathfrak{b}$ in R. Sie enthält das Nullideal (da $R \neq 0$) und ist damit nichtleer. Die Inklusionsrelation macht S zu einer partiell geordneten Menge. Sei $T \subset S$ eine nichtleere Kette. Man sieht leicht, dass $\mathfrak{a} := \bigcup_{\mathfrak{b} \in T} \mathfrak{b}$ ein echtes Ideal und eine obere Schranke von T ist. Nach Zorns Lemma gibt es ein maximales Element in S, also ein maximales Ideal in R. □

Korollar 2.6.16. *Jedes echte Ideal $\mathfrak{a} \subsetneq R$ ist in einem maximalen Ideal enthalten.*

Beweis. Das zeigt man genauso, indem man die Menge aller Ideale betrachtet, die $\mathfrak{a}$ enthalten. Alternativ hat $R/\mathfrak{a}$ nach Proposition 2.3.12 ein maximales Ideal, das nach Satz 2.6.13 einem maximalen Ideal in R entspricht, das $\mathfrak{a}$ enthält. □

Aufgabe 2.6.17. Es ist nicht richtig, dass es in jeder (abelschen) Gruppe eine maximale echte Untergruppe gibt, obwohl man nach dem Beweis von Satz 2.6.13 auf diese Idee kommen könnte.

Zeigen Sie, dass $\mathbb{Q}$ keine maximale echte Untergruppe enthält.

2.7. **Radikal eines Ideals, Radikalideale, reduzierte Ringe.**

Definition 2.7.1. Sei $\mathfrak{a}$ ein Ideal in R. Das **Radikal** von $\mathfrak{a}$ ist

$$\sqrt{\mathfrak{a}} = \{x \in R \mid \text{es gibt ein } n \in \mathbb{N} \text{ mit } x^n \in \mathfrak{a}\}.$$

2.7.2. Offensichtlich gilt $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$. Es ist leicht zu sehen, dass $\sqrt{\mathfrak{a}}$ ein Ideal ist (aus $x, y \in \sqrt{a}$, also $x^m, y^n \in \mathfrak{a}$, folgt $(x+y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i} \in \mathfrak{a}$, also $x + y \in \sqrt{\mathfrak{a}}$).

Beispiel 2.7.3. Das Radikal des Nullideals ist das Nilradikal, $\operatorname{Nil}(R) = \sqrt{(0)}$.

Beispiel 2.7.4. Ist $\mathfrak{p}$ ein Primideal, so gilt $\mathfrak{p} = \sqrt{\mathfrak{p}}$.

Aufgabe 2.7.5. Ist $\mathfrak{p}$ ein Primideal, so gilt $\mathfrak{p} = \sqrt{\mathfrak{p}^n}$ für alle $n \geq 1$.

Definition 2.7.6. Ein **Radikalideal** ist ein Ideal, das mit seinem Radikal übereinstimmt, also ein Ideal $\mathfrak{a}$ mit $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Beispiele 2.7.7. (a) Radikale von Idealen sind Radikalideale, $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.
(b) Primideale sind Radikalideale (vgl. Beispiel 2.7.4).
(c) Schnitte von Radikalidealen sind Radikalideale.

Definition 2.7.8. Ein Ring R heißt reduziert, falls 0 das einzige nilpotente Element ist.

Beispiele 2.7.9. (a) Der Faktorring $R/\operatorname{Nil}(R)$ ist reduziert (Proposition 2.4.11).
(b) Ist M eine Menge und R ein reduzierter Ring, so ist der Ring $\operatorname{Abb}(M, R)$ der R-wertigen Funktionen auf M reduziert, und alle seine Unterringe sind reduziert.
  (i) Ist k ein Körper, so ist der Ring der (polynomialen) Funktionen $k^n \to k$ reduziert.
  (ii) Der Ring aller bzw. der stetigen bzw. der glatten reellwertigen Funktionen auf einer Mannigfaltigkeit ist reduziert.

Proposition 2.7.10. *Der Faktorring $R/\sqrt{\mathfrak{a}}$ ist reduziert.*

Beweis. Der Beweis, $R/\operatorname{Nil}(R)$ keine nilpotenten Elemente außer der Null enthätl (siehe Proposition 2.4.11), verallgemeinert sich in der offensichtlichen Weise: Aus $0 = \overline{x}^n$ folgt $x^n \in \sqrt{\mathfrak{a}}$ und damit $(x^n)^m = x^{nm} \in \mathfrak{a}$, also $x \in \sqrt{\mathfrak{a}}$ und damit $\overline{x} = 0$. □

Proposition 2.7.11. *Sei $\mathfrak{a} \subset R$ ein Ideal. Dann gilt*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \subset R \text{ Primideal mit } \mathfrak{a} \subset \mathfrak{p}} \mathfrak{p}. \tag{2.7.1}$$

Insbesondere ist das Nilradikal $\operatorname{Nil}(R)$ *der Durchschnitt aller Primideale, in Formeln*

$$\operatorname{Nil}(R) = \bigcap_{\mathfrak{p} \subset R \text{ Primideal}} \mathfrak{p}. \tag{2.7.2}$$

Beweis. Sei $x \in \sqrt{\mathfrak{a}}$ und gelte $x^n \in \mathfrak{a}$. Also liegt x^n in jedem Primideal, das $\mathfrak{a}$ enthält, und somit in jedem solchen Primideal.

Sei nun $x \in R - \sqrt{\mathfrak{a}}$. Betrachte die Menge S aller Ideale, die $\mathfrak{a}$ enthalten, aber keines der Elemente $1, x, x^2, \dots$, also

$$S := \{\mathfrak{b} \subset R \text{ Ideal} \mid \mathfrak{a} \subset \mathfrak{b} \text{ und } \mathfrak{b} \cap \{1, x, x^2, \dots\} = \emptyset\}. \tag{2.7.3}$$

Diese Menge ist partiell geordnet (per Inklusion) und nicht leer, da sie das Ideal $\mathfrak{a}$ enthält (da $x \notin \sqrt{\mathfrak{a}}$). Sei T eine nichtleere Kette in S. Dann ist $\bigcup_{\mathfrak{b} \in T} \mathfrak{b}$ ein Element von S (diese Menge ist ein Ideal und enthält $\mathfrak{a}$; würde sie ein Element x^n enthalten, so gäbe es bereits ein $\mathfrak{b} \in T$ mit $x^n \in \mathfrak{b}$, Widerspruch) und eine obere Schranke für T. Nach Zorns Lemma gibt es also ein maximales Element $\mathfrak{p} \in S$. Wegen $x \notin \mathfrak{p}$ genügt es zu zeigen, dass $\mathfrak{p}$ ein Primideal ist.

Wegen $1 \notin \mathfrak{p}$ ist $\mathfrak{p}$ ein echtes Ideal. Seien $a, b \in R - \mathfrak{p}$. Weil die Ideale $\mathfrak{p} + (a)$ und $\mathfrak{p} + (b)$ echt größer als $\mathfrak{p}$ sind, sind sie nicht in S. Also gibt es $m, n \in \mathbb{N}$ mit $x^m \in \mathfrak{p} + (a)$ und $x^n \in \mathfrak{p} + (b)$. Es folgt $x^{m+n} \in \mathfrak{p} + (ab)$. Wäre $ab \in \mathfrak{p}$, so folgte $x^{m+n} \in \mathfrak{p} + (ab) = \mathfrak{p}$ im Widerspruch zu $\mathfrak{p} \in S$. Also folgt $ab \notin \mathfrak{p}$. □

2.7.12. Sobald wir den Begriff der Lokalisierung kennen, ist der Beweis von $\operatorname{Nil}(R) \supset \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$ leicht zu merken: Sei $x \notin \operatorname{Nil}(R)$. Dann ist die Lokalisierung R_x nicht der Nullring. Also gibt es in R_x ein maximales Ideal. Sein Urbild in R ist ein Primideal $\mathfrak{q}$, das x nicht enthält. Es gilt also $x \notin \mathfrak{q}$ und damit $x \notin \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$.

2.8. Das Jacobsonradikal.

Definition 2.8.1. Das **Jacobsonradikal** $\operatorname{Jac}(R)$ eines Ringes R ist der Durchschnitt aller maximalen Ideale, in Formeln

$$\operatorname{Jac}(R) = \bigcap_{\mathfrak{m} \subset R \text{ maximal}} \mathfrak{m}.$$

2.8.2. Offensichtlich ist $\operatorname{Jac}(R)$ ein Ideal.

2.8.3. Das Nilradikal ist im Jacobsonradikal enthalten, d. h. $\operatorname{Nil}(R) \subset \operatorname{Jac}(R)$: Gilt $x^n = 0$, so ist x^n und damit x in jedem maximalen Ideal enthalten.

Proposition 2.8.4. *Es gilt $x \in \operatorname{Jac}(R)$ genau dann, wenn $1 + Rx \subset R^\times$ (vgl. Lemma 2.4.17). Insbesondere gilt $1 + \operatorname{Jac}(R) \subset R^\times$.*

Beweis. Wir zeigen $x \notin \operatorname{Jac}(R)$ genau dann, wenn $1 + Rx \not\subset R^\times$.

Gelte $x \notin \operatorname{Jac}(R)$. Dann gibt es ein maximales Ideal $\mathfrak{m} \subset R$ mit $x \notin \mathfrak{m}$. Wegen $\mathfrak{m} \subsetneq \mathfrak{m} + (x)$ und Maximalität von $\mathfrak{m}$ folgt $\mathfrak{m} + (x) = R$. Also existieren $m \in \mathfrak{m}$ und $r \in R$ mit $m + rx = 1$. Dann ist $1 + (-r)x = 1 - rx = m \in \mathfrak{m}$ keine Einheit.

Gelte $1 + Rx \not\subset R^\times$. Dann gibt es ein $r \in R$, so dass $1 + rx$ keine Einheit ist. Also ist $(1 + rx) \subsetneq R$. Nach Korollar 2.6.16 gibt es ein maximales Ideal $\mathfrak{m} \subset R$ mit $1 + rx \subset \mathfrak{m}$. Die Annahme $x \in \mathfrak{m}$ führt zum Widerspruch $1 \in \mathfrak{m}$. Es folgt $x \notin \mathfrak{m}$, also $x \notin \operatorname{Jac}(R)$. □

2.9. Produkte von Ringen.

Proposition 2.9.1. *Seien R_1 und R_2 Ringe.*

(a) Die Menge $R_1 \times R_2$ wird ein Ring, indem man Addition und Multiplikation komponentenweise definiert: $(r_1, r_2) + (s_1, s_2) := (r_1 + s_1, r_2 + s_2)$, $(r_1, r_2) \cdot (s_1, s_2) := (r_1 s_1, r_2 s_2)$. Dieser Ring heißt das ***Produkt*** *von R_1 und R_2. Die Projektionen $R_1 \times R_2 \to R_1$ und $R_1 \times R_2 \to R_2$ sind Ringmorphismen.*

(b) (Universelle Eigenschaft des Produkts) Gegeben eine beliebigen Ring A und Ringmorphismen $\varphi_1 \colon A \to R_1$ und $\varphi_2 \colon A \to R_2$ definiert

$$\begin{aligned} A &\to R_1 \times R_2, \\ a &\mapsto (\varphi_1(a), \varphi_2(a)), \end{aligned}$$

einen Ringmorphismus. Er ist eindeutig dadurch bestimmt, dass seine Verknüpfung mit der ersten bzw. zweiten Projektion φ_1 bzw. φ_2 ist: Das Diagramm

$$\begin{tikzcd}
A \arrow[dr, dotted] \arrow[drr, "\varphi_2"] \arrow[ddr, "\varphi_1"'] & & \\
& R_1 \times R_2 \arrow[r] \arrow[d] & R_2 \\
& R_1 &
\end{tikzcd}$$

ist kommutativ.

Analog existiert das Produkt $\prod_{i\in I} R_i$ beliebig vieler Ringe $(R_i)_{i\in I}$.

Beweis. Alle Aussagen sind offensichtlich. □

Warnung 2.9.2. Die Abbildung $R_1 \to R_1 \times R_2$, $r_1 \mapsto (r_1, 0)$, ist kein Ringmorphismus, falls $R_2 \neq 0$, da $1 \mapsto (1, 0)$.

2.10. **Chinesischer Restsatz.**

Definition 2.10.1. Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen **relativ prim** (oder **koprim**), falls $\mathfrak{a} + \mathfrak{b} = (1)$.

Warnung 2.10.2. Dieser Begriff hat im Allgemeinen nichts mit Primidealen zu tun. Der Begriff kommt wohl daher, dass in $\mathbb{Z}$ zwei Ideale (n) und (m) genau dann relativ prim sind, wenn n und m keinen gemeinsamen Primfaktor haben.

Aufgabe 2.10.3. Sind $\mathfrak{a}, \mathfrak{b}$ relativ prim, so sind auch $\mathfrak{a}^m, \mathfrak{b}^n$ relativ prim für alle $m, n \in \mathbb{N}$.

Proposition 2.10.4. *Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ Ideale, die paarweise relativ prim sind. Dann gilt*

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \dots \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n.$$

Beweis. Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale. Dann gilt $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Sind $\mathfrak{a}$ und $\mathfrak{b}$ relativ prim, so gilt

$$\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b}) \cdot (1) = (\mathfrak{a} \cap \mathfrak{b}) \cdot (\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b}) \cdot \mathfrak{a} + (\mathfrak{a} \cap \mathfrak{b}) \cdot \mathfrak{b} \subset \mathfrak{a} \cdot \mathfrak{b}.$$

Dies zeigt den Fall $n = 2$. (Der Fall $n = 1$ ist trivial.)

Sei $n \geq 3$. Für $i > 2$ sind $\mathfrak{a}_1$, $\mathfrak{a}_i$ relativ prim und $\mathfrak{a}_2$, $\mathfrak{a}_i$ sind relativ prim. Wegen

$$(1) = (1) \cdot (1) = (\mathfrak{a}_1 + \mathfrak{a}_i) \cdot (\mathfrak{a}_2 + \mathfrak{a}_i) \subset \mathfrak{a}_1\mathfrak{a}_2 + \mathfrak{a}_i, \tag{2.10.1}$$

sind $\mathfrak{a}_1\mathfrak{a}_2$ und $\mathfrak{a}_i$ relativ prim. Induktion liefert

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \mathfrak{a}_3 \cdot \dots \cdot \mathfrak{a}_n = (\mathfrak{a}_1 \cdot \mathfrak{a}_2) \cdot \mathfrak{a}_3 \cdot \dots \cdot \mathfrak{a}_n = (\mathfrak{a}_1 \cdot \mathfrak{a}_2) \cap \mathfrak{a}_3 \cap \dots \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cap \mathfrak{a}_2) \cap \mathfrak{a}_3 \cap \dots \cap \mathfrak{a}_n.$$

□

Satz 2.10.5 (Chinesischer Restsatz)**.** *Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ Ideale in R, die paarweise relativ prim sind. Dann induzieren die kanonischen Abbildungen $R \to R/\mathfrak{a}_i$ einen Ringisomorphismus*

$$R/\mathfrak{a}_1\mathfrak{a}_2 \dots \mathfrak{a}_n \xrightarrow{\sim} R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_n,$$
$$\overline{r} \mapsto (\overline{r}, \dots, \overline{r}).$$

Beweis. Wir betrachten zunächst den Fall $n = 2$ (der Fall $n = 1$ ist trivial). Seien also $\mathfrak{a}$ und $\mathfrak{b}$ relativ prime Ideale. Die kanonischen Projektionen $R \to R/\mathfrak{a}$ und $R \to R/\mathfrak{b}$ definieren einen Ringmorphismus $R \to R/\mathfrak{a} \times R/\mathfrak{b}$. Sein Kern ist offensichtlich $\mathfrak{a} \cap \mathfrak{b}$ und stimmt nach Proposition 2.10.4 mit $\mathfrak{a}\mathfrak{b}$ überein. Also erhalten wir einen injektiven Ringmorphismus

$$\psi\colon R/\mathfrak{a}\mathfrak{b} \hookrightarrow R/\mathfrak{a} \times R/\mathfrak{b}.$$

Surjektivität: Sei $1 = a + b$ mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$. Dann gilt

$$\psi(\overline{a}) = (\overline{a}, \overline{a}) = (0, \overline{1 - b}) = (0, 1)$$

und analog $\psi(\overline{b}) = (1,0)$. Für beliebige $x, y \in R$ folgt daraus

$$\psi(xb + ya) = \psi(x)\psi(b) + \psi(y)\psi(a) = (\overline{x}, \overline{x})(1,0) + (\overline{y}, \overline{y})(0,1) = (\overline{x}, 0) + (0, \overline{y}) = (\overline{x}, \overline{y}).$$

Also ist ψ surjektiv.

Nun betrachten wir den Fall $n \geq 3$. Nach (2.10.1) sind die Ideale $(\mathfrak{a}_1\mathfrak{a}_2), \mathfrak{a}_3, \ldots, \mathfrak{a}_n$ paarweise relativ prim. Induktion und das obige Argument im Fall $n = 2$ liefert Ringisomorphismen

$$R/\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n \xrightarrow{\sim} R/\mathfrak{a}_1\mathfrak{a}_2 \times R/\mathfrak{a}_3 \times \cdots \times R/\mathfrak{a}_n \xrightarrow{\sim} R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times R/\mathfrak{a}_3 \times \cdots \times R/\mathfrak{a}_n.$$

Die Verknüpfung ist nach Konstruktion die angegebene Abbildung. □

Beispiele 2.10.6. (a) $\mathbb{Z}/6\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

(b) $\mathbb{Z}/300\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$

(c) Die Ideale $(X + i)$ und $(X - i)$ in $\mathbb{C}[X]$ sind relativ prim. Also gilt

$$\mathbb{C}[X]/(X^2 + 1) \xrightarrow{\sim} \mathbb{C}[X]/(X + i) \times \mathbb{C}[X]/(X - i) \xrightarrow[\sim]{\mathrm{ev}(-i)\times\mathrm{ev}(i)} \mathbb{C} \times \mathbb{C}.$$

Aufgabe 2.10.7. Finde alle ganzzahligen Lösungen der drei Kongruenzen

$$\begin{aligned} x &= 0 \mod 3, \\ x &= 1 \mod 4, \\ x &= 17 \mod 25. \end{aligned}$$

Proposition 2.10.8 (Primvermeidung)**.** *Sei R ein Ring. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ Primideale und $\mathfrak{a}$ ein Ideal. Gilt $\mathfrak{a} \not\subset \mathfrak{p}_i$ für alle $i = 1, \ldots, n$, so folgt $\mathfrak{a} \not\subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$.*

Mit anderen Worten: Gibt es für jedes i ein Element $a_i \in \mathfrak{a} - \mathfrak{p}_i$ (also ein Element von $\mathfrak{a}$, das $\mathfrak{p}_i$ vermeidet), so gibt es bereits ein Element $a \in \mathfrak{a} - (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n)$ (also ein Element von $\mathfrak{a}$, dass alle $\mathfrak{p}_i$ vermeidet).

Beweis. (Wir können sogar annehmen, dass höchstens zwei der $\mathfrak{p}_i$ keine Primideale sind.)

Für $n = 1$ ist die Behauptung trivial (und $\mathfrak{p}_1$ muss nicht einmal ein Primideal sein).

Wir zeigen die Behauptung für $n = 2$ (dabei dürfen $\mathfrak{p}_1$ und $\mathfrak{p}_2$ beliebige Ideale sein): Seien $a_1 \in \mathfrak{a} - \mathfrak{p}_1$ und $a_2 \in \mathfrak{a} - \mathfrak{p}_2$. Gilt $a_1 \notin \mathfrak{p}_2$ oder $a_2 \notin \mathfrak{p}_1$, so sind wir fertig. Sonst gilt $a_1 \in \mathfrak{p}_2$ und $a_2 \in \mathfrak{p}_1$. Betrachte $a_1 + a_2 \in \mathfrak{a}$. Aus der Annahme $a_1 + a_2 \in \mathfrak{p}_1$ folgt der Widerspruch $a_1 \in \mathfrak{p}_1$. Aus der Annahme $a_1 + a_2 \in \mathfrak{p}_2$ folgt der Widerspruch $a_2 \in \mathfrak{p}_2$. Also ist $a_1 + a_2$ in $\mathfrak{a} - (\mathfrak{p}_1 \cup \mathfrak{p}_2)$.

Sei nun $n > 2$. (Wir können oBdA annehmen, dass $\mathfrak{p}_n$ ein Primideal ist.) Per Induktion wissen wir bereits $\mathfrak{a} \not\subset \bigcup_{j\neq\ell} \mathfrak{p}_j$ für jedes $\ell = 1, \ldots, n$. Also gibt es $a_\ell \in \mathfrak{a} - \bigcup_{j\neq\ell} \mathfrak{p}_j$. Gilt $a_\ell \notin \mathfrak{p}_\ell$ für ein ℓ, so sind wir fertig. Andernfalls gilt $a_\ell \in \mathfrak{p}_\ell$ für alle $\ell = 1, \ldots, n$.

Betrachte das Element $a_1a_2 \cdots a_{n-1} + a_n \in \mathfrak{a}$. Wir behaupten, dass es in keinem der $\mathfrak{p}_i$, für $i = 1, \ldots, n$, liegt.

- Angenommen, es gilt $a_1a_2 \cdots a_{n-1} + a_n \in \mathfrak{p}_i$ für ein $i = 1, \ldots, n-1$. Wegen $a_i \in \mathfrak{p}_i$ folgt $a_n \in \mathfrak{p}_i$. Dies ist ein Widerspruch zu $a_n \in \mathfrak{a} - \bigcup_{j\neq n} \mathfrak{p}_j$.
- Angenommen, es gilt $a_1a_2 \cdots a_{n-1} + a_n \in \mathfrak{p}_n$. Wegen $a_n \in \mathfrak{p}_n$ folgt $a_1a_2 \cdot a_{n-1} \in \mathfrak{p}_n$. Weil $\mathfrak{p}_n$ ein Primideal ist, liegt einer der Faktoren a_ℓ für $\ell = 1, \ldots, n-1$ in $\mathfrak{p}_n$. Dies ist ein Widerspruch zu $a_\ell \in \mathfrak{a} - \bigcup_{j\neq\ell} \mathfrak{p}_j$.

Dies zeigt die Behauptung. □

Zusatzbemerkung 2.10.9. Proposition 2.10.8 ist äquivalent zu seiner Kontraposition: Gilt $\mathfrak{a} \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, so gibt es bereits ein i mit $\mathfrak{a} \subset \mathfrak{p}_i$. Äquivalent ist: Gilt $\mathfrak{a} = (\mathfrak{p}_1 \cap \mathfrak{a}) \cup \cdots \cup (\mathfrak{p}_n \cap \mathfrak{a})$, so gibt es bereits ein i mit $\mathfrak{a} = \mathfrak{p}_i \cap \mathfrak{a}$.

Enthält nun R einen unendlichen Körper, so sind $\mathfrak{a}$ und alle $\mathfrak{p}_i \cap \mathfrak{a}$ Vektorräume über diesem Körper, und obige Implikation folgt aus der Aussage, dass ein Vektorraum über einem unendlichen Körper nicht von endlich vielen echten Untervektorräumen überdeckt werden kann.

2.11. **Das Spektrum eines Ringes.** Sei R ein Ring.

Definition 2.11.1. Das **Spektrum** $\operatorname{Spec} R$ eines Ringes R ist die Menge aller seiner Primideale, d. h.

$$\operatorname{Spec} R = \{\mathfrak{p} \mid \mathfrak{p} \subset R \text{ Primideal}\}.$$

Diese Menge wird auch **Zariski-Spektrum** oder **Primspektrum** oder **Primidealspektrum** genannt.

Beispiele 2.11.2. (a) Ist k ein Körper, so gilt $\operatorname{Spec} k = \{(0)\}$.
(b) Es gilt $\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \{p\mathbb{Z} \mid p \text{ prim}\}$.
(c) Ist k ein algebraisch abgeschlossener Körper (etwa $\mathbb{C}$), so gilt $\operatorname{Spec} k[X] = \{(0)\} \cup \{(x-a) \mid a \in k\}$.
(d) Es gilt

$$\operatorname{Spec} \mathbb{R}[X] = \{(0)\} \cup \{(X-r) \mid r \in \mathbb{R}\} \cup \{((X-z)(X-\overline{z})) \mid z \in \mathbb{C} - \mathbb{R}\}. \tag{2.11.1}$$

Wenn wir zusätzlich $\operatorname{Re}(z) > 0$ verlangen, so sind die angegebenen Ideale alle verschieden.

Notation 2.11.3. Gegeben eine Teilmenge $E \subset R$ schreiben wir

$$\mathcal{V}(E) := \{\mathfrak{p} \in \operatorname{Spec} R \mid E \subset \mathfrak{p}\}$$

für die Menge der Primideale, die E enthalten (die also „oberhalb von E liegen"). Gegeben Elemente $f_1, \dots, f_n$ schreiben wir $\mathcal{V}(f_1, \dots, f_n) := \mathcal{V}(\{f_1, \dots, f_n\})$.

2.11.4. Offensichtlich gilt $\mathcal{V}(E) = \mathcal{V}(\langle E \rangle)$. Jede Menge der Form $\mathcal{V}(E)$ ist also durch ein Ideal definiert.

2.11.5. Aus $E \subset E'$ folgt $\mathcal{V}(E) \supset \mathcal{V}(E')$. Die Abbildung $\mathcal{V} \colon \mathcal{P}(R) \to \mathcal{P}(\operatorname{Spec} R)$ zwischen den Potenzmengen ist also inklusionsumkehrend.

Proposition 2.11.6. *Sei $X = \operatorname{Spec} R$. Dann gelten*

$$\mathcal{V}(0) = X, \qquad \mathcal{V}(1) = \emptyset,$$
$$\bigcap_{i \in I} \mathcal{V}(E_i) = \mathcal{V}(\bigcup_{i \in I} E_i), \qquad \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b}) = \mathcal{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathcal{V}(\mathfrak{a}\mathfrak{b})$$

für beliebige Familien $(E_i)_{i \in I}$ von Teilmengen von R und Ideale $\mathfrak{a}, \mathfrak{b} \subset R$.

Beweis. Die ersten drei Gleichheiten sind offensichtlich. Wegen $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$ und $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$ folgt

$$\mathcal{V}(\mathfrak{a} \cdot \mathfrak{b}) \supset \mathcal{V}(\mathfrak{a} \cap \mathfrak{b}) \supset \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b}).$$

Es bleibt zu zeigen, dass $\mathcal{V}(\mathfrak{a} \cdot \mathfrak{b}) \subset \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b})$ gilt.

Sei $\mathfrak{p} \in \mathcal{V}(\mathfrak{a} \cdot \mathfrak{b})$, also $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{p}$. Gilt $\mathfrak{a} \subset \mathfrak{p}$, so folgt $\mathfrak{p} \in \mathcal{V}(\mathfrak{a})$ und wir sind fertig. Sonst gibt es ein $a \in \mathfrak{a} - \mathfrak{p}$. Für beliebiges $b \in \mathfrak{b}$ gilt dann $ab \in \mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist und $a \notin \mathfrak{p}$ folgt $b \in \mathfrak{p}$. Da b beliebig war, folgt $\mathfrak{b} \subset \mathfrak{p}$, also $\mathfrak{p} \in \mathcal{V}(\mathfrak{b})$. ☐

Erinnerung 2.11.7. Sei X eine Menge. Eine **Topologie** auf X ist eine Teilmenge $\mathcal{T} \subset \mathcal{P}(X)$ der Potenzmenge mit folgenden Eigenschaften:

(a) $\emptyset, X \in \mathcal{T}$;
(b) $\mathcal{T}$ ist abgeschlossen unter beliebigen Schnitten: Für alle Familien $(A_i)_{i \in I}$ in $\mathcal{T}$ gilt $\bigcap_{i \in I} A_i \in \mathcal{T}$;
(c) $\mathcal{T}$ ist abgeschlossen unter endlichen Vereinigungen: Gegeben $A, B \in \mathcal{T}$ gilt $A \cup B \in \mathcal{T}$.

Man nennt dann $(X, \mathcal{T})$ einen **topologischen Raum**. Die Elemente von $\mathcal{T}$ nennt man **abgeschlossene** Teilmengen von X. Eine Teilmenge von X heißt **offen** genau dann, wenn ihr Komplement abgeschlossen ist.

Zusatzbemerkung 2.11.8. Proposition 2.11.6 besagt, dass wir $X = \operatorname{Spec} R$ als topologischen Raum auffassen können: Seine **abgeschlossenen** Teilmengen sind per definitionem genau die Teilmengen der Form $\mathcal{V}(E)$, für Teilmengen $E \subset R$. Diese Topologie auf X heißt **Zariski-Topologie** und macht X zu einem topologischen Raum.[2]

Es ist oft psychologisch sinnvoll, Elemente von $X = \operatorname{Spec} R$ mit Symbolen wie x, y, z zu bezeichnen, auch wenn sie natürlich Primideale sind. Wenn man von $x \in X$ als Primideal denkt, ist es sinnvoll, die Notation $\mathfrak{p}_x := x$ zu verwenden.

[2] In der Algebraischen Geometrie definiert man zusätzlich eine Garbe von Ringen $\mathcal{O}_X$ auf X, deren Halme lokale Ringe sind. Damit wird X zu einem lokal geringten Raum.

Lemma 2.11.9. *Ist $\mathfrak{a} \subset R$ ein Ideal, so gilt $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\sqrt{\mathfrak{a}})$. Insbesondere ist also jede Menge der Form $\mathcal{V}(E)$ durch ein Radikalideal definiert.*

Beweis. In der Tat, die Inklusion $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ impliziert $\mathcal{V}(\mathfrak{a}) \supset \mathcal{V}(\sqrt{\mathfrak{a}})$. Um die umgekehrte Inklusion zu zeigen, sei $\mathfrak{p} \in \mathcal{V}(\mathfrak{a})$, also $\mathfrak{a} \subset \mathfrak{p}$. Da das Nehmen $\sqrt{?}$ des Radikals inklusionserhaltend ist und Primideale Radikalideale sind, folgt $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$, also $\mathfrak{p} \in \mathcal{V}(\sqrt{\mathfrak{a}})$. □

Bemerkung 2.11.10. Sei $\mathfrak{a} \subset R$ ein Ideal. Wegen $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\sqrt{\mathfrak{a}})$ ist klar, dass man aus $\mathcal{V}(\mathfrak{a})$ im Allgemeinen nicht das Ideal $\mathfrak{a}$ zurückerhalten kann. Proposition 2.7.11 besagt jedoch, dass man aus $\mathcal{V}(\mathfrak{a})$ das Radikal $\sqrt{\mathfrak{a}}$ zurückerhalten kann: Es gilt

$$\sqrt{a} = \bigcap_{\mathfrak{p} \in \mathcal{V}(\mathfrak{a})} \mathfrak{p}. \tag{2.11.2}$$

Insbesondere gelten die folgenden Aussagen für Ideale $\mathfrak{a}, \mathfrak{b}$ von R:

(a) $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{b}}$ genau dann, wenn $\mathcal{V}(\mathfrak{a}) \supset \mathcal{V}(\mathfrak{b})$ (verwende Lemma 2.11.9 und Gleichung (2.11.2));
(b) $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{b})$ genau dann, wenn $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$.

2.11.11. Nach Proposition 2.6.7 sind Urbilder von Primidealen unter Ringmorphismen prim. Also induziert jeder Ringmorphismus $\varphi\colon A \to B$ eine Abbildung

$$\begin{aligned} \varphi^{-1}\colon \operatorname{Spec} B &\to \operatorname{Spec} A, \\ \mathfrak{q} &\mapsto \varphi^{-1}(\mathfrak{q}). \end{aligned}$$

Aufgabe 2.11.12. Beschreibe die durch $\mathbb{R}[X] \to \mathbb{C}[X]$ induzierte Abbildung

$$\operatorname{Spec} \mathbb{C}[X] \to \operatorname{Spec} \mathbb{R}[X].$$

Aufgabe 2.11.13. Beschreibe die durch $\mathbb{Q}[X] \to \mathbb{C}[X]$ induzierte Abbildung $\operatorname{Spec} \mathbb{C}[X] \to \operatorname{Spec} \mathbb{Q}[X]$. Ist sie surjektiv? Wie sehen die Fasern aus?

Aufgabe 2.11.14. Beschreibe die durch $\mathbb{Z} \to \mathbb{C}[X]$ induzierte Abbildung $\operatorname{Spec} \mathbb{C}[X] \to \operatorname{Spec} \mathbb{Z}[X]$.

Beispiel 2.11.15. Es ist nicht richtig, dass man $\varphi\colon A \to B$ aus der Abbildung $\varphi^{-1}\colon \operatorname{Spec} B \to \operatorname{Spec} A$ von Mengen zurückgewinnen kann. Ist beispielsweise $\sigma\colon k \to k$ ein Automorphismus eines Körpers k, so ist $\varphi^{-1}\colon \operatorname{Spec} k = \{(0)\} \to \operatorname{Spec} k = \{(0)\}$ die einzig mögliche Abbildung, nämlich die Identität. Expliziter liefern komplexe Konjugation $\mathbb{C} \to \mathbb{C}$ und die Identität $\mathbb{C} \to \mathbb{C}$ denselben Morphismus auf den Spektren.

Geometriebemerkung 2.11.16. In der algebraischen Geometrie macht man die Menge $\operatorname{Spec} A$ zu einem lokal geringten Raum $(\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$ und zeigt, dass jeder Morphismus $A \to B$ von Ringen einen Morphismus $(\operatorname{Spec} B, \mathcal{O}_{\operatorname{Spec} B}) \to (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$ von lokal geringten Räumen induziert. Diese Zuordnung ist dann bijektiv: Jeder Morphismus $(\operatorname{Spec} B, \mathcal{O}_{\operatorname{Spec} B}) \to (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$ von lokal geringten Räumen kommt von genau einem Ringmorphismus $A \to B$.

Proposition 2.11.17. *Sei $\mathfrak{a} \subset A$ ein Ideal und $\operatorname{can}\colon A \to A/\mathfrak{a}$. Dann ist $i := \operatorname{can}^{-1}\colon \operatorname{Spec}(A/\mathfrak{a}) \to \operatorname{Spec} A$ injektiv mit Bild $\mathcal{V}(\mathfrak{a})$, d. h. i induziert eine Bijektion*

$$\operatorname{Spec}(A/\mathfrak{a}) \xrightarrow{\sim} \mathcal{V}(\mathfrak{a}). \tag{2.11.3}$$

Beweis. Es ist klar, dass i injektiv ist und sein Bild in $\mathcal{V}(\mathfrak{a})$ enthalten ist (nach Proposition 2.3.12). Sei $\mathfrak{p} \in \mathcal{V}(\mathfrak{a})$. Nach Korollar 2.6.10 ist $\mathfrak{p}/\mathfrak{a}$ prim, also in $\operatorname{Spec}(A/\mathfrak{a})$. Es gilt $i(\mathfrak{p}/\mathfrak{a}) = \operatorname{can}^{-1}(\mathfrak{p}/\mathfrak{a}) = \mathfrak{p}$. □

Zusatzbemerkung 2.11.18 (Spektrum als Funktor). Gegeben $\varphi\colon A \to B$ definiere $\operatorname{Spec} \varphi := \varphi^{-1}\colon \operatorname{Spec} B \to \operatorname{Spec} A$. Dann gelten $\operatorname{Spec} \mathrm{id}_A = \mathrm{id}_{\operatorname{Spec} A}$ und $\operatorname{Spec}(\varphi \circ \psi) = \operatorname{Spec}(\psi) \circ \operatorname{Spec}(\varphi)$. Dies bedeutet, dass das Spektrum einen Funktor

$$\operatorname{Spec}\colon \mathrm{Ring}^{\mathrm{op}} \to \mathrm{Set}$$

definiert. Hier ist Ring die Kategorie der (kommutativen) Ringe (und Ringmorphismen), $\mathrm{Ring}^{\mathrm{op}}$ ist ihre opponierte Kategorie, und Set ist die Kategorie der Mengen (und Abbildungen von Mengen).

2.12. **Das Maximalspektrum.**

Definition 2.12.1. Das **Maximalspektrum** eines Ringes R ist

$$\operatorname{MaxSpec} R := \{\mathfrak{m} \mid \mathfrak{m} \subset R \text{ maximales Ideal}\}.$$

2.12.2. Offensichtlich gilt $\operatorname{MaxSpec} R \subset \operatorname{Spec} R$.

Ausblick 2.12.3. Oft ist das Maximalspektrum anschaulicher als das Primspektrum. Hilberts Nullstellensatz 8.2.4 (oder genauer sein Korollar 8.2.16) zeigt nämlich: Sei k ein algebraisch abgeschlossener Körper. Dann ist die Abbildung

$$\begin{gathered} k^n \xrightarrow{\sim} \operatorname{MaxSpec} k[T_1, \dots, T_n], \\ x = (x_1, \dots, x_n) \mapsto \mathfrak{m}_x := (T_1 - x_1, \dots, T_n - x_n) = \ker(\mathrm{ev}_x), \end{gathered} \tag{2.12.1}$$

eine Bijektion von Mengen (siehe Beispiel 2.6.9). Allgemeiner gilt: Seien $\mathfrak{a} \subset k[T_1, \dots, T_n]$ ein Ideal und $\mathbf{V}(\mathfrak{a}) = \{x = (x_1, \dots, x_n) \in k^n \mid f(x) = 0 \text{ für alle } f \in \mathfrak{a}\}$ die gemeinsame Nullstellenmenge von $\mathfrak{a}$ (siehe (1.2.1)). Unter der Bijektion (2.12.1) entsprechen die Punkte von $\mathbf{V}(\mathfrak{a})$ genau den maximalen Idealen, die $\mathfrak{a}$ enthalten (denn $x \in \mathbf{V}(\mathfrak{a})$ genau dann, wenn $f(x) = 0$ für alle $f \in \mathfrak{a}$, genau dann, wenn $\mathfrak{a} \subset \ker(\mathrm{ev}_x) = \mathfrak{m}_x$). Wir erhalten das folgende kommutative Diagramm. (Beachte $\mathbf{V}$ und $\mathcal{V}$.)

$$\begin{tikzcd}
k^n \arrow[r, "\sim"] & \operatorname{MaxSpec} k[T_1, \dots, T_n] \arrow[r, phantom, "\subset"] & \operatorname{Spec} k[T_1, \dots, T_n] \\
\cup & \cup & \cup \\
\mathbf{V}(\mathfrak{a}) \arrow[r, "\sim"] & (\operatorname{MaxSpec} k[T_1, \dots, T_n]) \cap \mathcal{V}(\mathfrak{a}) \arrow[r, phantom, "\subset"] & \mathcal{V}(\mathfrak{a}) \\
& \operatorname{MaxSpec}(k[T_1, \dots, T_n]/\mathfrak{a}) \arrow[u, "\sim"'] \arrow[r, phantom, "\subset"] & \operatorname{Spec}(k[T_1, \dots, T_n]/\mathfrak{a}) \arrow[u, "\sim"', "(2.11.3)"]
\end{tikzcd}$$

Wie angedeutet, ist der rechte vertikale Pfeil die Bijektion aus Proposition 2.11.17. Unter dieser Bijektion entsprechen sich die maximalen Ideale nach Korollar 2.6.10. Dies erklärt, dass der linke vertikale Pfeil eine Bijektion ist.

2.12.4. Urbilder von maximalen Idealen unter Ringmorphismen sind im Allgemeinen nicht maximal (für surjektive Ringmorphismen ist dies der Fall, siehe Proposition 2.6.8). Betrachte etwa

(a) $\mathbb{Z} \hookrightarrow \mathbb{Q}$ und das maximale Ideal $(0) \subset \mathbb{Q}$, oder
(b) $k[X] \hookrightarrow k(X)$, wobei k ein Körper ist, und das maximale Ideal $(0) \subset k(X)$, oder
(c) allgemeiner die Inklusion $R \hookrightarrow \mathrm{Q}(R)$ eines Integritätsbereichs in seinen Quotientenkörper und das maximale Ideal $(0) \subset \mathrm{Q}(R)$.

Im Gegensatz zum Primspektrum ist das Maximalspektrum also nicht funktoriell. Deswegen arbeitet man in der (modernen) Algebraischen Geometrie meist mit Primspektren.

Wie wir in Korollar 8.2.10 sehen werden, gilt aber: Ist $A \to B$ ein Morphismus von Algebren über einem Körper k, wobei B eine endlich erzeugte k-Algebra ist, so ist das Urbild eines maximalen Ideals in B ein maximales Ideal in A Wir erhalten also eine Abbildung

$$\varphi^{-1} \colon \operatorname{MaxSpec} B \to \operatorname{MaxSpec} A.$$

Nehmen wir nun zusätzlich an, dass k algebraisch abgeschlossen ist und dass A als k-Algebra endlich erzeugt ist. Fixieren wir isomorphismen $A \cong k[T_1, \dots, T_m]/\mathfrak{a}$ und $B \cong k[S_1, \dots, S_n]/\mathfrak{b}$, so wissen wir nach obigen Erklärungen, dass $\mathbf{V}(\mathfrak{a}) \cong \operatorname{MaxSpec} A$ und $\mathbf{V}(\mathfrak{b}) \cong \operatorname{MaxSpec} B$, und somit können wir φ^{-1} anschaulich auffassen als Abbildung

$$\mathbf{V}(\mathfrak{b}) \to \mathbf{V}(\mathfrak{a}).$$

Aufgabe 2.12.5. Sei R ein Ring und $X = \operatorname{Spec} R$. Eine Teilmenge U von X heißt **offene Teilmenge von** X falls es eine Teilmenge $E \subset R$ gibt mit $U = X - \mathcal{V}(E)$. Für $f \in R$ ist also insbesondere $X_f := X - \mathcal{V}(f)$ eine offene Teilmenge von X. Zeige:

(a) $X_f \cap X_g = X_{fg}$ für alle $g, f \in R$;
(b) $X_f = \emptyset$ genau dann, wenn f nilpotent ist;

(c) $X_f = X$ genau dann, wenn f eine Einheit ist;

(d) Sei U eine offene Teilmenge von X und $u = \mathfrak{p}_u \in U$. Zeigen Sie, dass es ein $f \in R$ gibt mit $u \in X_f \subset U$.

(Dies bedeutet, dass die Mengen der Form X_f eine Basis der Zariski-Topologie auf X bilden.)

(e) Gegeben offene Teilmengen U_i von X, für $i \in I$, mit $X = \bigcup_{i \in I} U_i$, gibt es bereits endlich viele $i_1, \dots, i_n \in I$ mit $X = U_{i_1} \cup \dots \cup U_{i_n}$.

(Dies bedeutet, dass $X = \operatorname{Spec} R$ mit der Zariski-Topologie quasi-kompakt ist.)

Aufgabe 2.12.6. Betrachte den Polynomring $k[X_1, \dots, X_n]$ über einem Körper k und die Abbildung

$$F\colon k[X_1, \dots, X_n] \to \operatorname{Abb}(k^n, k),$$

die einem Polynom $p \in k[X_1, \dots, X_n]$ die Abbildung $F(p)\colon k^n \to k$, $x = (x_1, \dots, x_n) \mapsto p(x)$ zuordnet.

(a) Die Abbildung F ist ein Morphismus von Ringen.

(b) Ist k unendlich (beispielsweise algebraisch abgeschlossen), so ist F injektiv.
(Beginne mit dem Fall $n = 1$ und verwende Induktion.)

(c) Ist k endlich, so ist F nicht injektiv. Was ist der Kern von F?

Aufgabe 2.12.7. Das Maximalspektrum $\operatorname{MaxSpec} A$ ist genau dann dicht in $\operatorname{Spec} A$, wenn $\operatorname{Nil}(A) = \operatorname{Jac}(A)$.

Nach Aufgabe 2.4 auf Übungsblatt 2 gilt dies insbesondere für Polynomringe in endlich vielen Variablen (mindestens eine).

Für den lokalen Ring $\mathbb{C}[[X]]$ etwa gilt dies nicht.

3. Moduln

3.1. Moduln und Morphismen von Moduln.

Sei R ein Ring.

Definition 3.1.1. Ein ***R*-Modul** oder **Modul über** R ist eine abelsche Gruppe M zusammen mit einer Abbildung

$$\begin{aligned} .\colon R \times M &\to M, \\ (r, m) &\mapsto rm := r.m, \end{aligned}$$

genannt **Skalarmultiplikation**, so dass

$$\begin{aligned} r(m + m') &= rm + r'm, \\ (r + r')m &= rm + r'm, \\ (rr')m &= r(r'm), \\ 1m &= m \end{aligned}$$

für alle $r, r' \in R$ und $m, m' \in M$ gelten.

Beispiele 3.1.2. (a) Jedes Ideal $\mathfrak{a}$ in R ist ein R-Modul: Die Multiplikation $R \times R \to R$ restringiert zu $R \times \mathfrak{a} \to \mathfrak{a}$ und erfüllt die an einen Modul gestellten Bedingungen.

(b) Insbesondere ist R selbst ein R-Modul.

(c) Ist k ein Körper, so ist ein k-Modul dasselbe wie ein k-Vektorraum.

(d) Abelsche Gruppen sind dasselbe wie $\mathbb{Z}$-Moduln. Demit meinen wir, dass jede abelsche Gruppe kanonisch als $\mathbb{Z}$-Modul aufgefasst werden kann (gegeben eine abelsche Gruppe A gibt es nach Beispiel 2.2.2.(a) genau einen Ringmorphismus $\mathbb{Z} \to \operatorname{End}(A)$, und dieser definiert nach Aufgabe 3.1.3 eine $\mathbb{Z}$-Modulstruktur auf A).

(e) Sei k ein Körper. Dann ist ein $k[X]$-Modul M dasselbe wie ein k-Vektorraum V zusammen mit einem k-linearen Endomorphismus $\varphi\colon V \to V$.

Aufgabe 3.1.3. Sei R ein Ring und A eine abelsche Gruppe. Sei $\operatorname{End}(A)$ der Endomorphismenring der abelschen Gruppe A, ein im Allgemeinen nichtkommutativer Ring.

(a) Sei μ eine ***R*-Modulstruktur** auf A, also eine Abbildung $\mu\colon R \times A \to A$, so dass (A, μ) ein R-Modul ist. Dann definiert $\rho\colon R \to \operatorname{End}(A)$, $r \mapsto \mu(r, -) = (a \mapsto ra = \mu(r, a))$, einen Ringmorphismus.

(b) Ist $\rho\colon R \to \operatorname{End}(A)$ ein Ringmorphismus, so definiert $\mu\colon R \times A \to A$, $(r, a) \mapsto \rho(r)(a)$, eine R-Modulstruktur auf A.

(c) Diese beiden Zuordnungen $\mu \mapsto \rho$ und $\rho \mapsto \mu$ sind invers zueinander.

Definition 3.1.4. Seien R-Moduln M und N gegeben. Ein **Morphismus von R-Moduln** von M nach N ist eine Abbildung $f\colon M \to N$ abelscher Gruppen, die verträglich ist mit den Skalarmultiplikationen, d. h. es gelten

$$\begin{aligned} f(m+m') &= f(m) + f(m'), \\ f(rm) &= rf(m) \end{aligned}$$

für alle $m, m' \in M$ und $r \in R$. Andere gängige Bezeichnungen sind **R-lineare Abbildung** oder **Homomorphismus von R-Moduln**, auch **R-Modulmorphismus** oder **R-Modulhomomorphismus**.

Notation 3.1.5. Die Menge aller Morphismen $M \to N$ von R-Moduln wird als $\mathrm{Hom}_R(M, N)$ notiert. Wir schreiben $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ und bezeichnen die Elemente dieser Menge als **Endomorphismen** de R-Moduls M.

Beispiele 3.1.6. (a) Ist k ein Körper, so ist ein Morphismus von k-Moduln dasselbe wie eine k-lineare Abbildung von k-Vektorräumen.

(b) (Homo-)Morphismen abelscher Gruppen sind Morphismen von $\mathbb{Z}$-Moduln.

Aufgabe 3.1.7. Sei R ein Ring. Dann ist ein $R[X]$-Modul M in kanonischer Weise dasselbe wie ein R-Modul M zusammen mit einem Endomorphismus $\varphi\colon M \to M$ von R-Moduln.

3.1.8. Die Menge $\mathrm{Hom}_R(M, N)$ ist selbst ein R-Modul: Gegeben $f, g \in \mathrm{Hom}_R(M, N)$ und $r \in R$ ist $f + g$ definiert per $(f + g)(m) := f(m) + g(m)$ und $r.f$ per

$$(r.f)(m) := rf(m) = f(rm),$$

für $m \in M$. Hier nutzen wir, dass R kommutativ ist (damit $r.f$ wieder R-linear ist).

Lemma 3.1.9. *Sei M ein R-Modul. Die Auswertung bei $1 \in R$ definiert einen Isomorphismus von R-Moduln*

$$\begin{aligned} \mathrm{ev}_1 \colon \mathrm{Hom}_R(R, M) &\xrightarrow{\sim} M, \\ f &\mapsto f(1). \end{aligned}$$

Die Umkehrabbildung bildet $m \in M$ auf die Abbildung $R \to M$, $r \mapsto rm$, ab.

Beweis. Nachrechnen. Für $f \in \mathrm{Hom}_R(R, M)$ gilt beispielsweise $f(r) = f(r1) = rf(1)$. $\square$

3.1.10. Die Komposition von Morphismen von R-Moduln ist ein Morphismus von R-Moduln: Wir erhalten eine Abbildung

$$\begin{aligned} \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(L, M) &\to \mathrm{Hom}_R(L, N), \\ (g, f) &\mapsto gf := g \circ f. \end{aligned}$$

Diese Abbildung R-bilinear (genaue Definition später): Es gelten $(g + g') \circ f = g \circ f + g' \circ f$, $g \circ (f + f') = g \circ f + g \circ f'$, $(rg) \circ f = r(g \circ f) = g \circ (rf)$.

Insbesondere wird $\mathrm{End}_R(M)$ ein im Allgemeinen nichtkommutativer Ring. Die Abbildung $R \to \mathrm{End}_R(M)$, $r \mapsto r.\mathrm{id}_M$, ist ein Morphismus nicht notwendig kommutativer Ringe. Beachte, dass $r.\mathrm{id}_M$ mit allen Elementen von $\mathrm{End}_R(M)$ kommutiert[3]: $(r.\mathrm{id}_M) \circ f = r.(\mathrm{id}_M \circ f) = r.f = r.(f \circ \mathrm{id}_M) = f \circ (r.\mathrm{id}_M)$. Oft schreibt man einfach r statt $r.\mathrm{id}_M$, wenn aus dem Kontext klar ist, was gemeint ist.

Definition 3.1.11. Ein **Epimorphismus** bzw. **Monomorphismus** bzw. **Isomorphismus**) von R-Moduln ist ein surjektiver bzw. injektiver bzw. bijektiver Morphismus von R-Moduln. Ein **Automorphismus** ist ein bijektiver Endomorphismus. Zwei R-Moduln M und N heißen **isomorph** genau dann, wenn es einen Isomorphismus $M \xrightarrow{\sim} N$ von R-Moduln gibt.

Notation 3.1.12. Die Symbole $\twoheadrightarrow, \hookrightarrow, \xrightarrow{\sim}$ bezeichnen gemäß unserer Konvention 1.6.4 Epimorphismen, Monomorphismen und Isomorphismen von R-Moduln. Die Menge der Automorphismen eines R-Moduls M wird als $\mathrm{Aut}_R(M)$ notiert.

[3] Also ist $\mathrm{End}_R(M)$ eine R-Algebra.

3.2. **Untermoduln und Quotienten.**

Definition 3.2.1. Sei M ein R-Modul. Ein **(R-)Untermodul** von M ist eine abelsche Untergruppe $U \subset M$, die unter Skalarmultiplikation abgeschlossen ist: aus $r \in R$ und $u \in U$ folgt $ru \in U$.

3.2.2. Ein Untermodul U von M ist offensichtlich selbst ein R-Modul. Die Inklusion $U \to M$ ist ein Monomorphismus von R-Moduln.

Beispiel 3.2.3. Jeder Modul hat sich selbst und den Nullmodul $0 := \{0\}$ als Untermoduln.

Beispiel 3.2.4. Fassen wir R als R-Modul auf, so sind die Untermoduln von R genau die Ideale von R.

Beispiel 3.2.5. Ist $f\colon M \to N$ ein Morphismus von R-Moduln, so ist sein **Bild** $\operatorname{im}(f) := f(M)$ ein Untermodul von N und f faktorisiert als

$$M \twoheadrightarrow \operatorname{im}(f) \hookrightarrow N.$$

Sein **Kern** $\ker(f) := f^{-1}(0)$ ist ein Untermodul von M.

Beispiel 3.2.6. Urbilder und Bilder von Untermoduln unter Morphismen von R-Moduln sind Untermoduln.

3.2.7. Gegeben Untermoduln U und V eines R-Moduls M sind der Schnitt $U \cap V$ und die Summe $U + V := \{u + v \mid u \in U, v \in V\}$ Untermoduln von M. Sind allgemeiner Untermoduln U_i, für $i \in I$, gegeben, so sind $\bigcap_{i \in I} U_i$ und

$$\sum_{i \in I} U_i := \{\sum_{i \in I_0} u_i \mid I_0 \subset I \text{ endlich}, u_i \in U_i \text{ für alle } i \in I_0\}$$

Untermoduln.

Definition 3.2.8. Sei E eine Teilmenge eines R-Moduls M. Die Teilmenge

$$RE := \{\sum_{i=1}^{n} r_i e_i \mid n \in \mathbb{N}, r_i \in R, e_i \in E\}$$

ist offenbar ein Untermodul von M und heißt der **von E erzeugte Untermodul**. Wir nennen E ein **Erzeugendensystem** von M, falls $RE = M$ gilt. Gegeben $m \in M$ schreiben wir $Rm := R\{m\}$. Wir nennen gegebene Elemente m_i von M, für $i \in I$, **Erzeuger** von M, falls $\{m_i \mid i \in I\}$ ein Erzeugendensystem von M ist.

Proposition 3.2.9. *(Quotientenmodul und universelle Eigenschaft) Sei U ein Untermodul eines R-Moduls M. Dann gelten:*

(a) Auf dem Quotient M/U als abelsche Gruppe gibt es genau eine Verknüpfung "Skalarmultiplikation" $R \times M/U \to M/U$, so dass die kanonische Abbildung $\mathrm{can}\colon M \twoheadrightarrow M/U$ *mit Skalarmultiplikation verträglich ist. Diese Verknüpfung ist gegeben durch $(r, \overline{m} := m + U) \mapsto \overline{rm}$.*

(b) Mit dieser Skalarmultiplikation werden M/U ein R-Modul und $\mathrm{can}\colon M \to M/U$ *ein Morphismus von R-Moduln mit Kern U. Er heißt der* ***Quotient(enmodul)*** *von M nach U.*

(c) (Universelle Eigenschaft) Jeder Morphismus $f\colon M \to N$ mit $f(U) = \{0\}$ faktorisiert eindeutig über $\mathrm{can}\colon M \to M/U$, *d. h. es gibt genau einen Morphismus $\overline{f}\colon M/U \to N$ von R-Moduln mit $\overline{f} \circ \mathrm{can} = f$, der also das Diagramm*

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\mathrm{can}"'] & & N \\ & M/U \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

kommutativ macht. Es gilt also $\overline{f}(\overline{m}) = f(m)$.

Beweis. Die Skalarmultiplikation $R \times M/U \to M/U$ ist definiert per $(r, \overline{m} = m + U) \mapsto \overline{rm} = rm + U$. Dies ist wohldefiniert wegen $\overline{m} = \overline{m'}$ genau dann, wenn $m - m' \in U$, was $rm - rm' \in U$ impliziert, also $\overline{rm} = \overline{rm'}$. Die restlichen Behauptungen folgen direkt aus den analogen Aussagen für Quotienten abelscher Gruppen. $\square$

Proposition 3.2.10. *Sei U ein Untermodul eines R-Moduls M und* $\mathrm{can}\colon M \to M/U$ *die kanonische Abbildung. Dann ist*

$$\begin{aligned}\{\textit{Untermoduln von } M\textit{, die } U \textit{ enthalten}\} &\xrightarrow{\sim} \{\textit{Untermoduln von } M/U\},\\ V &\mapsto \mathrm{can}(V) = V/U,\\ \mathrm{can}^{-1}(W) &\leftarrow\!\shortmid W,\end{aligned}$$

eine Bijektion von Mengen.

Beweis. Das ist offensichtlich (vgl. Proposition 2.3.12). ☐

Satz 3.2.11 (Homomorphiesatz)**.** *Jeder Morphismus $f\colon M \to N$ von R-Modulen faktorisiert als*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\mathrm{can}"'] & N \\ M/\ker(f) \arrow[r, "\sim"] & \mathrm{im}(f), \arrow[u, hook] \end{tikzcd}$$

wobei die untere Horizontale ein Isomorphismus ist.

Beweis. Das ist offensichtlich (vgl. Beispiel 2.3.11). ☐

Satz 3.2.12. *(a) (Erster Isomorphiesatz) Seien U und N Untermoduln eines R-Moduls M. Dann ist die Abbildung*

$$\begin{aligned} N/(U \cap N) &\xrightarrow{\sim} (N+U)/U,\\ \overline{n} &\mapsto \overline{n},\end{aligned}$$

ein Isomorphismus von R-Moduln.

(b) (Zweiter Isomorphiesatz) Seien $U \subset N \subset M$ Untermoduln eines R-Moduls M. Dann ist die Abbildung

$$\begin{aligned} M/N &\xrightarrow{\sim} (M/U)/(N/U),\\ \overline{m} &\mapsto \overline{\overline{m}},\end{aligned}$$

ein Isomorphismus von R-Moduln.

Beweis. (a) Wende den Homomorphiesatz 3.2.11 auf die Verknpfung $N \to M \to M/U$ an: ihr Kern ist $U \cap N$ und ihr Bild ist $\mathrm{can}(N) = (N+U)/U$ (denn $\mathrm{can}^{-1}(\mathrm{can}(N)) = N + U$).

(b) Wende den Homomorphiesatz 3.2.11 auf die Verknüpfung $M \to M/U \to (M/U)/(N/U)$ an: Sie ist surjektiv und hat N als Kern. ☐

Notation 3.2.13. Gegeben ein R-Modul M und ein Ideal $\mathfrak{a} \subset R$, definieren wir

$$\mathfrak{a}M := \{\sum_{i=1}^{n} a_i m_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, m_i \in M\}.$$

Dies ist offenbar ein Untermodul von M.

Lemma 3.2.14. *Ist M ein R-Modul und $\mathfrak{a} \subset R$ ein Ideal, so gibt es auf der abelschen Gruppe $M/\mathfrak{a}M$ genau eine $R/\mathfrak{a}$-Modulstruktur, so dass $\overline{r}.\overline{m} = \overline{rm}$ für alle $r \in R$ und $m \in M$ gilt.*

Beweis. Dies ist offensichtlich. ☐

3.3. **Produkte und direkte Summen.**

Proposition 3.3.1. *Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln.*

(a) *Die abelsche Gruppe $\prod_{i\in I} M_i$ wird ein R-Modul per $r.(m_i)_{i\in I} := (rm_i)_{i\in I}$. Er heißt das **Produkt** der R-Moduln $(M_i)_{i\in I}$. Die **Projektionen***

$$\begin{aligned}\mathrm{pr}_j\colon \prod_{i\in I} M_i &\to M_j,\\ (m_i)_{i\in I} &\mapsto m_j,\end{aligned}$$

sind Morphismen von R-Moduln, für alle $j \in I$.

(b) *(Universelle Eigenschaft des Produkt) Gegeben einen beliebigen R-Modul N und Morphismen $(\varphi_i\colon N \to M_i)_{i\in I}$ von R-Moduln, definiert*

$$\begin{aligned}\langle\varphi_i\rangle\colon N &\to \prod_{i\in I} M_i,\\ n &\mapsto (\varphi_i(n))_{i\in I},\end{aligned}$$

einen Morphismus von R-Moduln. Er ist eindeutig dadurch bestimmt, dass für alle $j \in I$ das Diagramm

$$\begin{tikzcd} & \prod_{i\in I} M_i \arrow[d, "\mathrm{pr}_j"] \\ N \arrow[ur, "\langle\varphi_i\rangle"] \arrow[r, "\varphi_j"] & M_j, \end{tikzcd}$$

kommutativ ist.

Beweis. Das ist offensichtlich. □

Bemerkung 3.3.2. Die universelle Eigenschaft des Produkts bedeutet schlicht, dass für alle R-Moduln N die Abbildung

$$\begin{aligned}\mathrm{Hom}_R(N, \prod_{i\in I} M_i) &\xrightarrow{\sim} \prod_{j\in J} \mathrm{Hom}_R(N, M_j),\\ \varphi &\mapsto (\mathrm{pr}_j \circ \varphi)_{j\in I},\end{aligned}$$

bijektiv ist. Sie ist sogar ein Isomorphismus von R-Moduln.

Notation 3.3.3. Endliche Produkte $\prod_{i=1}^n M_i$ schreiben wir als $M_1 \times \cdots \times M_n$. Gegeben ein R-Modul M schreiben wir $M^{\times n} = M \times \cdots \times M$ (mit m Faktoren M). Ist I eine beliebige Menge, so schreiben wir $M^{\times I} := \prod_{i\in I} M$. Oft wird dieser Modul schlicht als M^I notiert.

Proposition 3.3.4. *Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln.*

(a) *Die Teilmenge*

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \in \prod_{i\in I} M_i \mid m_i = 0 \text{ für alle bis auf endlich viele } i \in I\}$$

*ist ein Untermodul von $\prod_{i\in I} M_i$. Er heißt die **direkte Summe** (oder das **Koprodukt**) der R-Moduln $(M_i)_{i\in I}$. Die **Inklusionen***

$$\begin{aligned}\iota_j\colon M_j &\to \bigoplus_{i\in I} M_i,\\ m &\mapsto \iota_j(m) = (0,\dots,0,m,0,\dots,0) \quad \text{(mit } m \text{ als } j\text{-te Koordinate)},\end{aligned}$$

sind Morphismen von R-Moduln, für alle $j \in I$.

(b) (Universelle Eigenschaft der direkten Summe) Gegeben ein beliebiger R-Modul N und Morphismen $(\varphi_i\colon M_i \to N)_{i\in I}$ von R-Moduln, definiert

$$\begin{aligned}(\varphi_i)\colon \bigoplus_{i\in I} M_i &\to N,\\ (m_i)_{i\in I} &\mapsto \sum_{i\in I} \varphi_i(m_i),\end{aligned}$$

einen Morphismus von R-Moduln (dieser ist wohldefiniert, da nur endlich viele Summanden ungleich Null sind). Er ist eindeutig dadurch bestimmt, dass für alle $j \in I$ das Diagramm

$$\begin{tikzcd} M_j \arrow[r, "\varphi_j"] \arrow[d, "\iota_j"] & N \\ \bigoplus_{i\in I} M_i \arrow[ur, "(\varphi_i)"'] & \end{tikzcd}$$

kommutativ ist.

Beweis. Das ist offensichtlich. □

Bemerkung 3.3.5. Die universelle Eigenschaft der direkten Summe bedeutet schlicht, dass für alle R-Moduln N die Abbildung

$$\begin{aligned}\mathrm{Hom}_R(\bigoplus_{i\in I} M_i, N) &\to \prod_{j\in J} \mathrm{Hom}_R(M_j, N),\\ \varphi &\mapsto (\varphi \circ \iota_j)_{j\in I},\end{aligned}$$

bijektiv ist. Sie ist sogar ein Isomorphismus von R-Moduln.

3.3.6. Endliche direkte Summen $\bigoplus_{i=1}^n M_i$ schreiben wir als $M_1 \oplus \cdots \oplus M_n$. Gegeben ein R-Modul M schreiben wir $M^{\oplus n} = M \oplus \cdots \oplus M$ (mit m Summanden M). Ist I eine beliebige Menge, so schreiben wir $M^{\oplus I} := \bigoplus_{i\in I} M$. In der Literatur wird dieser Modul oft als $M^{(I)}$ notiert.

3.3.7. Die direkte Summe ist definiert als Untermodul des Produkt. Die Inklusion definiert also einen Morphismus

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

von R-Moduln (man kann diesen auch mit Hilfe der universellen Eigenschaften konstruieren). Ist die Indexmenge endlich, so ist er ein Isomorphismus.[4] Insbesondere gilt

$$M_1 \oplus \cdots \oplus M_m = M_1 \times \cdots \times M_m.$$

Notation 3.3.8. Ist M ein R-Modul, so schreiben wir

$$M^n := M^{\oplus n} = M^{\times n}.$$

3.3.9. Speziell erhalten wir $R^n = R^{\oplus n} = R^{\times n}$.

3.3.10 (Morphismen als Matrizen)**.** Seien R-Moduln $M_1, \ldots, M_m, N_1, \ldots N_n$ gegeben. Nach den universellen Eigenschaften von direkter Summe und Produkt gilt

$$\mathrm{Hom}_R(N_1 \oplus \cdots \oplus N_n, M_1 \oplus \cdots \oplus M_m) \xrightarrow{\sim} \prod_{i,j=1}^{m,n} \mathrm{Hom}_R(N_j, M_i).$$

Wir können Morphismen also als $(m \times n)$-Matrizen mit (i,j)-Eintrag in $\mathrm{Hom}_R(N_j, M_i)$ auffassen. Schreiben wir Elemente der direkten Summen als Spaltenvektoren, so entspricht das Anwenden eines Morphismus der Multiplikation der entsprechenden Matrix mit dem Spaltenvektor.

[4] Genauer ist er ein Isomorphismus genau dann, wenn höchstens endlich viele der M_i nicht Null sind.

Beispielsweise entspricht ein Morphismus $\varphi\colon N_1 \oplus N_2 \oplus N_3 \to M_1 \oplus M_2$ einer (2×3)-Matrix

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} & \varphi_{13} \\ \varphi_{21} & \varphi_{22} & \varphi_{23} \end{pmatrix}$$

mit Einträgen $\varphi_{ij} \in \operatorname{Hom}_R(N_j, M_i)$. Schreiben wir ein Element $n = (n_1, n_2, n_3) \in N_1 \oplus N_2 \oplus N_3$ als Spaltenvektor

$$\begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix}$$

und „multiplizieren" unsere obige Matrix in offensichtlicher Weise von links mit diesem Zeilenvektor, so ist das Ergebnis

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} & \varphi_{13} \\ \varphi_{21} & \varphi_{22} & \varphi_{23} \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} = \begin{pmatrix} \varphi_{11}(n_1) + \varphi_{12}(n_2) + \varphi_{13}(n_3) \\ \varphi_{21}(n_1) + \varphi_{22}(n_2) + \varphi_{23}(n_3) \end{pmatrix}$$

das Element $\varphi(n)$ als Zeilenvektor geschrieben. Man beachte etwa, dass man $\varphi_{12} \in \operatorname{Hom}_R(N_2, M_1)$ auf das Element $n_2 \in N_3$ anwenden darf und ein Element $\varphi_{12}(n_2)$ von M_1 erhält.

Analog entspricht das Verknüpfen von Morphismen zwischen direkten Summen von Moduln der Multiplikation der entsprechenden Matrizen.

3.3.11. Nach 3.3.10 und Lemma 3.1.9 können Elemente von $\operatorname{Hom}_R(R^n, R^m)$ als $(m \times n)$-Matrizen mit Einträgen in $\operatorname{Hom}_R(R, R) \xrightarrow{\sim} R$ beschrieben werden, d. h.

$$\operatorname{Hom}_R(R^n, R^m) \xrightarrow{\sim} \operatorname{Mat}_{m \times n}(R).$$

Wir erhalten einen Matrizenkalkül, der den aus der Linearen Algebra bekannten Kalkül von Körpern zu Ringen verallgemeinert.

Definition 3.3.12. Ist $(M_i)_{i \in I}$ eine Familie von Untermoduln eines R-Moduls M, so liefern die Inklusionen $M_i \to M$ einen Morphismus $\bigoplus_{i \in I} M_i \to M$. Sein Bild ist genau $\sum_{i \in I} M_i$. Ist dieser Morphismus injektiv, so sagen wir, dass die **Summe der Untermoduln** M_i **direkt** ist und schreiben statt $\sum_{i \in I} M_i$ auch $\bigoplus_{i \in I} M_i$.

Zwei Untermoduln M_1, M_2 von M heißen **komplementär**, falls $M_1 \oplus M_2 = M$ gilt, falls also die durch die Einbettungen induzierte Abbildung $M_1 \oplus M_2 \to M$ ein Isomorphismus ist. Man nennt dann M_2 ein **Komplement** von M_1. Ein Untermodul heißt **Summand**, falls er ein Komplement besitzt.

Beispiel 3.3.13. Seien M_1 und M_2 Untermoduln eines R-Moduls M. Dann ist der von den Inklusionen $M_1 \hookrightarrow M$ und $M_2 \hookrightarrow M$ induzierte Morphismus $M_1 \oplus M_2 \to M$ injektiv genau dann, wenn $M_1 \cap M_2 = 0$ gilt.

Proposition 3.3.14 (Kriterium für Direktheit einer Summe)**.** *Sei $(M_i)_{i \in I}$ eine Familie von Untermoduln eines R-Moduls M. Dann ist der von den Inklusionen $M_i \hookrightarrow M$ induzierte Morphismus $\bigoplus_{i \in I} M_i \to M$ injektiv genau dann, wenn*

$$M_k \cap \big(\sum_{j \in J} M_j\big) = 0$$

für jede endliche Teilmenge $J \subset I$ und jedes $k \in I - J$ gilt.

Beweis. Sei $\varphi\colon \bigoplus_{i \in I} M_i \to M$ der betrachtete Morphismus.

Sei φ injektiv. Seien $J \subset I$ endlich, $k \in I - J$ und $m \in M_k \cap \big(\sum_{j \in J} M_j\big)$. Dann gilt $m = \sum_{j \in J} m_j$ für geeignete $m_j \in M_j$, für $j \in J$. Wir berechnen

$$\varphi(\iota_k(m)) = m = \sum_{j \in J} m_j = \sum_{j \in J} \varphi(\iota_j(m_j)) = \varphi(\sum_{j \in J} \iota_j(m_j)).$$

Da φ injektiv ist, folgt $\iota_k(m) = \sum_{j \in J} \iota_j(m_j)$. Da insbesondere die k-ten Koordinaten übereinstimmen, folgt $m = 0$.

Seien umgekehrt alle angegebenen Schnitte Null. Sei $z = (z_i)_{i\in I} \in \bigoplus M_i$ mit $0 = \varphi(z) = \sum_{i\in I} z_i$. Nach Definition der direkten Summe sind nur endlich viele der z_i ungleich Null. Also gibt es eine endliche Teilmenge $L \subset I$ mit $z_i = 0$ für alle $i \in I - L$. Falls $L = \emptyset$ so ist $z = 0$. Sonst sei $l_0 \in L$ beliebig. Dann gilt

$$z_{l_0} = -\sum_{l\in L-\{l_0\}} z_l \in M_{l_0} \cap \Big(\sum_{l\in L-\{l_0\}} M_l\Big).$$

Der Schnitt ist nach Annahme Null. Also erhalten wir $z_{l_0} = 0$. Da $l_0 \in L$ beliebig war, folgt $z = 0$, und φ ist injektiv. □

3.4. **Freie Moduln und Basen.**

Definition 3.4.1. Ein R-Modul M heißt **frei** genau dann, wenn er isomorph zu einem R-Modul der Form $\bigoplus_{i\in I} R$ ist, für eine Menge I.

Notation 3.4.2. Ist I eine Menge und $j \in I$, so definieren wir

$$e_j := \iota_j(1) = (0, \dots, 0, 1, 0, \dots, 0) \in \bigoplus_{i\in I} R$$

mit der 1 als j-ter Koordinate und allen anderen Koordinaten Null.

Lemma 3.4.3 (Universelle Eigenschaft des freien Moduls über einer Menge)**.** *Ist I eine Menge und M ein R-Modul, so ist die Abbildung*

$$\begin{aligned} \mathrm{Hom}_R\Big(\bigoplus_{i\in I} R, M\Big) &\xrightarrow{\sim} \mathrm{Abb}(I, M), \\ \varphi &\mapsto (i \mapsto \varphi(e_i)), \end{aligned}$$

ein Isomorphismus von R-Moduln.

Beweis. Bemerkung 3.3.5 und Lemma 3.1.9 liefern Bijektionen

$$\mathrm{Hom}_R\Big(\bigoplus_{i\in I} R, M\Big) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_R(R, M) \xrightarrow{\sim} \prod_{i\in I} M.$$

Die Verknüpfung ist gegeben durch $\varphi \mapsto ((\varphi \circ \iota_i)(1))_{i\in I} = (\varphi(e_i))_{i\in I}$. Nun verwende die offensichtliche Gleichheit $\prod_{i\in I} M = \mathrm{Abb}(I, M)$. □

Definition 3.4.4. Sei M ein R-Modul. Eine Teilmenge $B \subset M$ heißt **linear unabhängig** (oder genauer **R-linear unabhängig**), falls für paarweise verschiedene Elemente $b_1, \dots, b_n$ von B und beliebige Skalare $r_1, \dots, r_n \in R$ aus $r_1 b_1 + \dots + r_n b_n = 0$ bereits $r_1 = r_2 = \dots = r_n = 0$ folgt. Eine **Basis** (oder genauer **R-Basis**) von M ist ein R-linear unabhängiges Erzeugendensystem.

Beispiele 3.4.5. (a) Die Teilmenge $\{e_1, \dots, e_n\}$ ist eine Basis von R^n.
(b) Allgemeiner ist die Teilmenge $\{e_i \mid i \in I\}$ eine Basis von $\bigoplus_{i\in I} R$.

Lemma 3.4.6. *Sei E eine Teilmenge eines R-Moduls M. Betrachte den Morphismus*

$$\begin{aligned} \bigoplus_{e\in E} R &\to M, \\ (r_e)_{e\in E} &\mapsto \sum_{e\in E} r_e e, \end{aligned}$$

von R-Moduln (unter der Bijektion von Lemma 3.4.3 kommt er von der Abbildung $I = E \to M$, $e \mapsto e$). Diese Abbildung ist surjektiv genau dann, wenn E ein Erzeugendensystem ist, und injektiv genau dann, wenn E linear unabhängig ist. Also ist sie bijektiv genau dann, wenn E eine Basis ist.

Beweis. Das ist nur eine Umformulierung der Definitionen. □

3.4.7. Ist B eine Basis von M, so ist M die direkte Summe der Untermoduln Rb, für $b \in B$, im Sinne der Definition 3.3.12. Man beachte, dass jeder der Untermoduln Rb frei ist (vom Rang eins): Die Abbildung $R \xrightarrow{\sim} Rb$, $r \mapsto rb$, ist ein Isomorphismus.

Lemma 3.4.8. *Ein R-Modul ist frei genau dann, wenn er eine Basis hat.*

Beweis. Das Bild einer Basis unter einem Isomorphismus von R-Moduln ist offensichtlich wieder eine Basis. Da $\{e_i \mid i \in I\}$ eine Basis von $\bigoplus_{i\in I} R$ ist, hat also jeder freie R-Modul eine Basis.

Ist umgekehrt B eine Basis von M, so ist M frei nach Lemma 3.4.6. □

Definition 3.4.9. Gegeben R-Moduln M und N sagen wir, dass M ein **Quotient** von N ist, falls M isomorph zu einem Quotientenmodul N/U von N ist. Eine offensichtlich äquivalente Bedingung ist (nach dem Homomorphiesatz 3.2.11), dass es einen Epimorphismus $N \twoheadrightarrow M$ gibt.

Lemma 3.4.10. *Jeder Modul ist Quotient eines freien Moduls.*

Beweis. Die Menge $E := M$ ist ein Erzeugendensystem von M. Also liefert Lemma 3.4.6 einen Epimorphismus $p\colon F := \bigoplus_{m\in M} R \twoheadrightarrow M$. □

Aufgabe 3.4.11. Ein Epimorphismus $f\colon M \twoheadrightarrow N$ von R-Moduln **spaltet**, falls es einen Morphismus $s\colon N \to M$ von R-Moduln gibt, so dass $f \circ s = \mathrm{id}_N$. Ein solcher Morphismus s heißt **Spaltung** von f.

(a) Zeigen Sie: Ist s eine Spaltung von $f\colon M \twoheadrightarrow N$, so ist die Abbildung

$$\begin{aligned} \ker(f) \oplus N &\to M, \\ (u, n) &\mapsto u + s(n), \end{aligned}$$

ein Isomorphismus von R-Moduln.

(b) Zeigen Sie: Jeder Epimorphismus $f\colon M \twoheadrightarrow \bigoplus_{i\in I} R$ von R-Moduln spaltet. Folgern Sie: Über einem Körper k spaltet jeder Epimorphismus von k-Vektorräumen.

(c) Geben Sie für die beiden Ringe $\mathbb{Z}$ und $k[X]$, wobei k ein Körper ist, Beispiele von nicht spaltenden Epimorphismen.

3.5. **Endlich erzeugte Moduln.**

Definition 3.5.1. Ein R-Modul M heißt **endlich erzeugt**, falls er ein endliches Erzeugendensystem besitzt.

Beispiel 3.5.2. Der freie R-Modul $R^{\oplus n}$ ist endlich erzeugt, für jedes $n \in \mathbb{N}$.

3.5.3. Die Bezeichnung „endlich erzeugbar“ ist möglicherweise ein besserer Begriff; wir folgen aber dem allgemeinen Sprachgebrauch.

3.5.4. Quotienten endlich erzeugter Moduln sind endlich erzeugt: Sei $f\colon M \twoheadrightarrow N$ ein Epimorphismus von R-Moduln. Ist M endlich erzeugt, so ist N ebenfalls endlich erzeugt.

Lemma 3.5.5. *Ein R-Modul M ist endlich erzeugt von n Elementen genau dann, wenn es einen Epimorphismus $R^n \twoheadrightarrow M$ von R-Moduln gibt.*

Beweis. Ist $\varphi\colon R^n \twoheadrightarrow M$ ein Epimorphismus von R-Moduln, so sind die Elemente $\varphi(e_1), \dots, \varphi(e_n)$ Erzeuger von M. Sind $m_1, \dots, m_n$ Erzeuger von M, so wende man Lemma 3.4.6 an auf die Menge $\{m_1, \dots, m_n\}$ (und addiere Summanden R, falls die m_i nicht paarweise verschieden sind). □

Aufgabe 3.5.6 (Rang eines endlich erzeugten freien Moduls)**.** Zeigen Sie:

(a) Ist ein R-Modul endlich erzeugt und frei, so ist er bereits isomorph zu R^n für ein $n \in \mathbb{N}$. (Die Umkehrung dieser Aussage ist offensichtlich ebenfalls richtig.)

(b) Gelte $R \neq 0$. Gibt es einen Isomorphismus $R^n \xrightarrow{\sim} R^m$ von R-Moduln, so gilt $m = n$.
Hinweis: Ziehen Sie sich mit Lemma 3.2.14 auf den aus der linearen Algebra bekannten Fall zurück, dass die entsprechende Aussage für Körper gilt.

Insbesondere haben je zwei Basen eines endlich erzeugten freien R-Moduls M gleich viele Elemente. Wir nennen diese Kardinalität den **Rang** von M.

Aufgabe 3.5.7 (Untermoduln endlich erzeugter Moduln sind im Allgemeinen nicht endlich erzeugt)**.** Betrachten Sie den Polynomring $R = k[X_1, X_2, \dots]$ in abzählbar vielen Variablen über einem Körper k als Modul über sich selbst. Dieser ist offensichtlich endlich erzeugt durch das Element 1. Zeigen Sie, dass der Untermodul $\mathfrak{m} := (X_1, X_2, \dots) := \sum_{i\in\mathbb{N}} Rx_i$ nicht endlich erzeugt ist als R-Modul.

Hinweis: Verwenden Sie Lemma 3.2.14 und betrachten Sie $\mathfrak{m}/\mathfrak{m}^2$ als Vektorraum über dem Körper $k \xrightarrow{\sim} R/\mathfrak{m}$.

3.6. **Determinanten.** Sei R ein Ring und $\mathrm{Mat}_n(R)$ der nichtkommutative (falls $R \neq 0$ und $n \geq 2$) Ring der $n \times n$-Matrizen mit Einträgen aus R.

Definition 3.6.1. Die **Determinante** $\det(S)$ von $S \in \mathrm{Mat}_n(R)$ ist definiert durch die **Leibniz-Formel**

$$\det(S) := \sum_{\sigma \in \mathrm{S}_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} S_{i,\sigma(i)}.$$

Dies definiert eine Abbildung $\det\colon \mathrm{Mat}_n(R) \to R$.

Bemerkung 3.6.2. Die Determinante determiniert, ob gewisse Gleichungen lösbar sind. Dies erklärt vermutlich den Namen.

3.6.3. Ist $\varphi\colon A \to B$ ein Ringmorphismus, so definiert komponentenweises Anwenden einen Morphismus

$$\tilde{\varphi}\colon \mathrm{Mat}_n(A) \to \mathrm{Mat}_n(B),$$

nicht notwendig kommutativer Ringe; per definitionem gilt $\tilde{\varphi}(S)_{ij} = \varphi(S_{ij})$ für $S \in \mathrm{Mat}_n(A)$. Aus der Definition der Determinante folgt sofort

$$\varphi(\det(S)) = \det(\tilde{\varphi}(S)) \tag{3.6.1}$$

für $S \in \mathrm{Mat}_n(A)$. Das folgende Diagramm ist also kommutativ.

$$\begin{tikzcd} \mathrm{Mat}_n(A) \arrow[r, "\tilde{\varphi}"] \arrow[d, "\det"] & \mathrm{Mat}_n(A) \arrow[d, "\det"] \\ A \arrow[r, "\varphi"] & B \end{tikzcd}$$

Definition 3.6.4. Sei $S \in \mathrm{Mat}_n(R)$. Die **adjunkte Matrix** $S^\# \in \mathrm{Mat}_n(R)$ von S ist definiert durch

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

wobei $S(j,i) \in \mathrm{Mat}_{n-1}(R)$ die Matrix ist, die man aus S durch Streichen der j-ten Zeile und der i-ten Spalte erhält.

3.6.5. Ist $\varphi\colon A \to B$ ein Ringmorphismus, so gilt

$$\tilde{\varphi}(S^\#) = (\tilde{\varphi}(S))^\# \tag{3.6.2}$$

für $S \in \mathrm{Mat}_n(A)$. Dies folgt aus der Definition der adjunkten Matrix und (3.6.1). Das folgende Diagramm ist also kommutativ.

$$\begin{tikzcd} \mathrm{Mat}_n(A) \arrow[r, "\tilde{\varphi}"] \arrow[d, "(-)^\#"] & \mathrm{Mat}_n(B) \arrow[d, "(-)^\#"] \\ \mathrm{Mat}_n(A) \arrow[r, "\tilde{\varphi}"] & \mathrm{Mat}_n(B) \end{tikzcd}$$

Notation 3.6.6. Wir notieren die $n \times n$-Einheitsmatrix als $I = I_n$.

3.6.7. Aus der Linearen Algebra ist bekannt: Ist k ein Körper, so gilt $S^\# S = S S^\# = \det(S) I$ für jedes $S \in \mathrm{Mat}_n(k)$. Wir benötigen dieselbe Formel für beliebige Ringe.

Proposition 3.6.8 (Laplace-Entwicklung oder Cramersche Regel)**.** *Sei R ein Ring und $S \in \mathrm{Mat}_n(R)$. Dann gilt*

$$S^\# S = S S^\# = \det(S) I.$$

Bemerkung 3.6.9. Man kann sich leicht überzeugen, dass viele in der Linearen Algebra gegebene Beweise dieser Aussage auch für beliebige kommutative Ringe gelten (etwa der Beweis per stupidem Nachrechnen). Wir geben stattdessen einen Beweis, der die Aussage auf den Körperfall reduziert. Die Idee dieses Beweises erlaubt auch den Beweis ähnlicher polynomialer Identitäten, etwa der Multiplikativität der Determinante, $\det(ST) = \det(S)\det(T)$, aus dem Körperfall zu folgern. Man folgert, dass eine Matrix $S \in \mathrm{Mat}_n(R)$ genau dann invertierbar ist, wenn $\det(S) \in R^\times$.

Beweis. Wir beweisen nur die Aussage $S^\# S = \det(S)I$. Der Beweis von $SS^\# = \det(S)I$ geht vollkommen analog.

Reduktionsschritt: Betrachte den Polynomring

$$\mathbb{Z}[X_{ij}] = \mathbb{Z}[X_{ij} \mid 1 \leq i, j \leq n]$$

in n^2 Variablen. Sei $U \in \mathrm{Mat}_n(\mathbb{Z}[X_{ij}])$ definiert durch

$$U_{ij} := X_{ij}.$$

Für $n = 2$ gilt also beispielsweise

$$U = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix} \in \mathbb{Z}[X_{11}, X_{12}, X_{21}, X_{22}].$$

Wir behaupten, dass es genügt, $U^\# U = \det(U)I$ für diese Matrix zu zeigen.

Seien R ein beliebiger Ring und $S \in \mathrm{Mat}_n(R)$. Betrachte den Ringmorphismus

$$\begin{aligned} \varphi\colon \mathbb{Z}[X_{ij}] &\to R, \\ X_{ij} &\mapsto S_{ij} \end{aligned}$$

Dieser ist so konstruiert, dass

$$\tilde{\varphi}(U) = S$$

gilt. Aus (3.6.2) erhalten wir demnach

$$\tilde{\varphi}(U^\#) = (\tilde{\varphi}(U))^\# = S^\#$$

Die Gleichheit $U^\# U = \det(U)I$ bereits als bekannt angenommen, schließen wir wie folgt.

$$\begin{aligned} S^\# S &= \tilde{\varphi}(U^\#)\tilde{\varphi}(U) \\ &= \tilde{\varphi}(U^\# U) && (\tilde{\varphi} \text{ Ringmorphismus}) \\ &= \tilde{\varphi}(\det(U)I) \\ &= \varphi(\det(U))I \\ &= \det(\tilde{\varphi}(U))I && (\text{nach } (3.6.1)) \\ &= \det(S)I. \end{aligned}$$

Beweis von $U^\# U = \det(U)I$: Der Ring $\mathbb{Z}[X_{ij}]$ ist ein Integritätsbereich, und

$$\mathbb{Q}(X_{ij}) = \mathbb{Q}(X_{ij} \mid 1 \leq i, j \leq n)$$

ist sein Quotientenkörper. Also ist $\mathbb{Z}[X_{ij}] \subset \mathbb{Q}(X_{ij})$ ein Unterring. Auf Matrizenebene ist damit

$$\mathrm{Mat}_n(\mathbb{Z}[X_{ij}]) \subset \mathrm{Mat}_n(\mathbb{Q}(X_{ij}))$$

ein Unterring (beide Ringe sind im Allgemeinen nichtkommutativ). Fassen wir U als Element von $\mathrm{Mat}_n(\mathbb{Q}(X_{ij}))$ auf, so ist die Gleichheit $U^\# U = \det(U)I$ in $\mathrm{Mat}_n(\mathbb{Q}(X_{ij}))$ bekannt aus der Linearen Algebra, da $\mathbb{Q}(X_{ij})$ ein Körper ist. Daraus folgt aber bereits die Gleichheit $U^\# U = \det(U)I$ in $\mathrm{Mat}_n(\mathbb{Z}(X_{ij}))$, da die Inklusion der Matrizenringe kompatibel ist mit Multiplikation, dem Übergang zur adjunkten Matrix (siehe (3.6.2)) und dem Nehmen der Determinante (siehe (3.6.1)).

(Falls die zitierte Aussage in der Linearen Algebra nur für algebraisch abgeschlossene Körper bewiesen wurde, kann man in dem obigen Argument $\mathbb{Q}(X_{ij})$ durch einen algebraischen Abschluss ersetzen. Es genügt sogar, die Aussage nur für die komplexen Zahlen (oder die reellen Zahlen) zu kennen: man bette $\mathbb{Q}(X_{ij})$ in $\mathbb{C}$ (oder in $\mathbb{R}$) als Unterring ein, indem nan n^2 algebraisch unabhängige Elemente wählt.) ☐

3.7. **Verallgemeinerter Cayley-Hamilton.**

Satz 3.7.1 (Determinantentrick)**.** *Sei $\varphi\colon M \to M$ ein Endomorphismus eines endlich erzeugten Moduls über einem Ring R. Ist $\mathfrak{a} \subset R$ ein Ideal mit $\varphi(M) \subset \mathfrak{a}M$, so gibt es ein $n \in \mathbb{N}$ und Elemente $a_i \in \mathfrak{a}^i$, für $i = 1, \dots, n$, so dass*

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

in $\mathrm{End}_R(M)$ *gilt.*

3.7.2. Wissen wir, dass M von d Elementen erzeugt wird, so zeigt der folgende Beweis, dass wir $n = d$ annehmen können.

Beweis. Seien $x_1, \dots, x_n$ Erzeuger von M als R-Modul, also $M = Rx_1 + \dots + Rx_n$. Es folgt

$$\mathfrak{a}M = \{\alpha_1 x_1 + \dots \alpha_n x_n \mid \alpha_i \in \mathfrak{a}\}.$$

Wegen $\varphi(M) \subset \mathfrak{a}M$ gibt es also Elemente $a_{ij} \in \mathfrak{a}$ mit

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ij}x_j \quad \text{für alle } i = 1, \dots, n. \tag{3.7.1}$$

Setze $A := (a_{ij}) \in \mathrm{Mat}_n(R)$.

Wir setzen den Morphismus $R \to \mathrm{End}_R(M)$, $r \mapsto r\mathrm{id}_M$, von Ringen (wobei $\mathrm{End}_R(M)$ im Allgemeinen nicht kommutativ ist) per $T \mapsto \varphi$ zu dem Ringmorphismus "Auswerten bei φ"

$$\begin{aligned} R[T] &\to \mathrm{End}_R(M), \\ p(T) &\mapsto p(\varphi), \end{aligned}$$

fort. Wir erhalten einen induzierten Morphismus "komponentenweise Auswerten bei φ"

$$\begin{aligned} \mathrm{Mat}_n(R[T]) &\to \mathrm{Mat}_n(\mathrm{End}_R(M)), \\ B = (b_{ij}) &\mapsto B(\varphi) \text{ mit } B(\varphi)_{ij} := B_{ij}(\varphi), \end{aligned}$$

von im Allgemeinen nichtkommutativen Ringen.

Betrachte die Matrix

$$S := TI - A \in \mathrm{Mat}_n(R[T]).$$

Ihre Auswertung $S(\varphi) \in \mathrm{Mat}_n(\mathrm{End}_R(M))$ hat den (i,j)-Eintrag

$$S(\varphi)_{ij} = S_{ij}(\varphi) = (\delta_{ij}T - a_{ij})(\varphi) = \delta_{ij}\varphi - a_{ij}\mathrm{id}_M \in \mathrm{End}_R(M).$$

Werten wir dies auf x_j aus und summieren über alle $j \in \{1, \dots, n\}$, so ergibt sich mit Hilfe von (3.7.1)

$$\sum_j S(\varphi)_{ij}(x_j) = \varphi(x_i) - \sum_j a_{ij}x_j = 0 \quad \text{in } M \text{ für alle } i = 1, \dots, n. \tag{3.7.2}$$

Um Summenzeichen und Indizes zu vermeiden, verwenden nun den in 3.3.10 erklärten Matrizenkalkül (siehe Bemerkung 3.7.3 für die Rechnungen mit Indizes). Dieser Kalkül erlaubt es, die n Gleichheiten (3.7.2) in der Gleichheit

$$S(\varphi)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \quad \text{in } M^n \tag{3.7.3}$$

zusammenzufassen; wir verwenden $S(\varphi) \in \mathrm{Mat}_n(\mathrm{End}_R(M)) \xrightarrow{\sim} \mathrm{End}_R(M^n)$ und haben $(x_1, \dots, x_n) \in M^n$ als Spaltenvektor geschrieben.

Aus Proposition 3.6.8 und der Tatsache, dass komponentenweises Auswerten bei φ ein Morphismus von (Matrizen-)Ringen ist, folgt

$$S^{\#}(\varphi)S(\varphi) = (S^{\#}S)(\varphi) = (\det(S)I)(\varphi) = (\det(S)(\varphi))I. \tag{3.7.4}$$

Multiplizieren wir (3.7.3) von links mit der Matrix $S^{\#}(\varphi)$, so ergibt sich damit

$$0 = S(\varphi)^{\#} S(\varphi) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\det(S)(\varphi)) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} (\det(S)(\varphi))(x_1) \\ \vdots \\ (\det(S)(\varphi))(x_n) \end{pmatrix}$$

Also verschwindet $\det(S)(\varphi) \in \mathrm{End}_R(M)$ auf allen Erzeugern $x_1, \dots, x_n$, und es folgt

$$\det(S)(\varphi) = 0. \tag{3.7.5}$$

Die Leibniz-Formel zusammen mit der Tatsache, dass alle a_{ij} in $\mathfrak{a}$ liegen, zeigt

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

für geeignete $a_i \in \mathfrak{a}^i$. Werten wir dies bei φ aus, so erhalten wir nach (3.7.5) die Behauptung. □

Bemerkung 3.7.3. Hier ist der Beweis mit Summenzeichen und Indizes. Für beliebiges $l \in \{1, \dots, n\}$ wenden wir $S^{\#}(\varphi)_{li}$ auf (3.7.2) an und summieren über i. Dies erklärt die zweite Gleichheit (die erste ist offensichtlich) in

$$\sum_j \Big(\sum_i S^{\#}(\varphi)_{li} S(\varphi)_{ij} \Big)(x_j) = \sum_i S^{\#}(\varphi)_{li} \big(\sum_j S(\varphi)_{ij}(x_j) \big) = 0 \quad \text{in } M. \tag{3.7.6}$$

In der (l, i)-Koordinate bedeutet Gleichung (3.7.4) schlicht

$$\sum_i S^{\#}(\varphi)_{li} S(\varphi)_{ij} = \delta_{lj} \det(S)(\varphi).$$

Dies vereinfacht (3.7.6) zu $\det(S)(\varphi)(x_l) = 0$ und wir erhalten $\det(S)(\varphi) = 0$, da x_l beliebig war. Nun fahre man wie im obigen Beweis fort.

Korollar 3.7.4 (Cayley-Hamilton für kommutative Ringe)**.** *Jede Matrix ist Nullstelle ihres charakteristischen Polynoms: Ist $A \in \mathrm{Mat}_n(R)$ eine Matrix und $\chi_A := \det(TI - A) \in R[T]$ ihr **charakteristisches Polynom**, so gilt $\chi_A(A) = 0$ in $\mathrm{Mat}_n(R)$.*

Beweis. Setze $\mathfrak{a} = R$ und $M = R^n$ und fasse $A \in \mathrm{Mat}_n(R) \xleftarrow{\sim} \mathrm{End}_R(R^n)$ als Endomorphismus $\varphi\colon M \to M$ auf. Nun wähle im Beweis von Satz 3.7.1 als Erzeuger von M die Standardbasis $e_1, \dots, e_n$ von R^n. Die a_{ij} aus dem Beweis sind dann genau die Einträge A_{ij} der Matrix A. Mit der dortigen Notation gilt dann $\chi_A = \det(TI - A) = \det(S) \in R[T]$, und $\chi_A(A) \in \mathrm{Mat}_n(R)$ entspricht $\det(S)(\varphi) \in \mathrm{End}_R(R^n)$ unter dem kanonischen Isomorphismus $\mathrm{Mat}_n(R) \xleftarrow{\sim} \mathrm{End}_R(R^n)$. Das folgende Diagramm illustriert die Situation.

$$\begin{tikzcd} & R[T] \arrow[dl] \arrow[dr] & \\ \mathrm{End}_R(R^n) \arrow[rr, "\sim"] & & \mathrm{Mat}_n(R), \end{tikzcd} \qquad \begin{tikzcd} & \det(S) = \chi_A \arrow[dl, mapsto] \arrow[dr, mapsto] & \\ \det(S)(\varphi) \arrow[rr, mapsto] & & \chi_A(A) \end{tikzcd}$$

Nach (3.7.5) wissen wir $\det(S)(\varphi) = 0$ und erhalten also $\chi_A(A) = 0$. □

3.8. **Nakayamas Lemma.**

Satz 3.8.1. *Seien R ein Ring und M ein endlich erzeugter R-Modul. Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a}M = M$, so existiert ein $a \in \mathfrak{a}$ mit $(1 + a)M = 0$.*

3.8.2. Mit anderen Worten bedeutet dies, dass es ein Element $b \in \mathfrak{a}$ (nämlich $-a$) gibt, dass auf M genauso operiert wie die Identität: $\mathrm{id}_M = b\mathrm{id}_M = b.?$.

Beweis. Wir wenden Satz 3.7.1 an auf $\varphi = \mathrm{id}_M$ (was erlaubt ist wegen $\varphi(M) = M \subset \mathfrak{a}M$) und erhalten ein $n \in \mathbb{N}$ und Elemente $a_i \in \mathfrak{a}^i$, für $i = 1, \dots, n$, mit

$$\mathrm{id}_M + a_1 \mathrm{id}_M + \dots a_{n-1} \mathrm{id}_M + a_n \mathrm{id}_M = 0$$

in $\mathrm{End}_R(M)$. Das Element $a := a_1 + \dots + a_n$ liegt somit in $\mathfrak{a}$ und erfüllt $(1 + a)M = 0$. □

Korollar 3.8.3. *Sei $\varphi\colon M \to M$ ein surjektiver Endomorphismus eines endlich erzeugten R-Moduls M. Dann ist φ bereits injektiv und somit ein Automorphismus.*

3.8.4. Korollar 3.8.3 wird falsch, wenn man injektiv und surjektiv vertauscht, betrachte etwa $(2\cdot)\colon \mathbb{Z} \to \mathbb{Z}$.

3.8.5. Korollar 3.8.3 ist wohlbekannt für Vektorräume.

Beweis. Wir fassen M als $R[X]$-Modul auf, indem wir X per φ auf M operieren lassen (siehe Aufgabe 3.1.7). Setze $\mathfrak{a} = (X) \subset R[X]$. Dann gilt nach Voraussetzung $\mathfrak{a}M = M$. Nach Satz 3.8.1 existiert ein $a \in \mathfrak{a}$ mit $(1+a)M = 0$. Für $m \in \ker(\varphi)$ gilt $0 = \varphi(m) = Xm$ und damit $am = 0$, da a ein Vielfaches von X ist. Es folgt $0 = (1+a)m = m + am = m$. Also ist φ injektiv. □

Korollar 3.8.6 (Nakayamas Lemma)**.** *Ist R ein Ring und M ein endlich erzeugter R-Modul mit $\mathrm{Jac}(R)M = M$, so folgt $M = 0$.*

3.8.7. Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a} \subset \mathrm{Jac}(R)$ und $\mathfrak{a}M = M$, so gilt trivialerweise $\mathrm{Jac}(R)M = M$ und Nakayamas Lemma zeigt $M = 0$.

Erster Beweis. Nach Satz 3.8.1) existiert ein $a \in \mathrm{Jac}(R)$ mit $(1+a)M = 0$. Nach Proposition 2.8.4 gilt $1 + \mathrm{Jac}(R) \in R^\times$. Also ist $1+a$ eine Einheit, und es folgt $M = 1M = (1+a)^{-1}(1+a)M = 0$. □

Zweiter Beweis. Sei n die minimale Kardinalität eines Erzeugendensystems von M. Seien $m_1, \dots, m_n$ Erzeuger von M. Ist $n = 0$, so sind wir fertig. Sonst hat $m_n \in M = \mathrm{Jac}(R)M$ eine Darstellung

$$m_n = r_1 m_1 + \cdots + r_n m_n$$

mit $r_i \in \mathrm{Jac}(R)$ für alle $i = 1, \dots, n$. Es folgt

$$(1 - r_n)m_n = r_1 m_1 + \cdots + r_{n-1} m_{n-1}.$$

Nach Proposition 2.8.4 ist $1 - r_n$ eine Einheit. Es folgt $m_n \in Rm_1 + \dots Rm_{n-1}$ im Widerspruch zur Wahl von n. □

Korollar 3.8.8. *Sei M ein endlich erzeugter R-Modul und $U \subset M$ ein Untermodul. Gilt $M = U + \mathrm{Jac}(R)M$ (äquivalent: ist die Verknüpfung $U \hookrightarrow M \twoheadrightarrow M/\mathrm{Jac}(R)M$ surjektiv), so gilt bereits $U = M$.*

Beweis. Der R-Modul M/U ist auch endlich erzeugt, und es gilt $\mathrm{Jac}(R).(M/U) = (\mathrm{Jac}(R)M + U)/U = M/U$. Nach Korollar 3.8.6 folgt daraus $M/U = 0$, also $U = M$. □

3.9. **Lokale Ringe.**

Definition 3.9.1. Ein Ring heißt **lokal**, wenn er genau ein maximales Ideal besitzt. Ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, so bezeichnet man den Körper $R/\mathfrak{m}$ als seinen **Restklassenkörper**.

Notation 3.9.2. Die Aussage, dass $(R, \mathfrak{m})$ ein lokaler Ring ist, bedeutet, dass R ein lokaler Ring ist und $\mathfrak{m}$ sein maximales Ideal.

3.9.3. Ist $(R, \mathfrak{m})$ ein lokaler Ring, so gilt $\mathrm{Jac}(R) = \mathfrak{m}$.

3.9.4. Ist R ein Ring, dessen Nichteinheiten $R - R^\times$ ein Ideal bilden, so ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m} := R - R^\times$ (denn $R - R^\times$ ist ein echtes Ideal und jedes echte Ideal ist darin enthalten).

Lemma 3.9.5. *Ist $(R, \mathfrak{m})$ ein lokaler Ring, so gilt $R = \mathfrak{m} \sqcup R^\times$ (disjunkte Vereinigung). Insbesondere bilden die Nichteinheiten von R ein Ideal.*

Beweis. Sei $x \in R - \mathfrak{m}$. Ist x keine Einheit, so ist Rx ein echtes Ideal von R. Nach Korollar 2.6.16 ist es in einem maximalen Ideal enthalten. Da es nur ein maximales Ideal gibt, folgt $Rx \subset \mathfrak{m}$ im Widerspruch zur Annahme. □

Beispiele 3.9.6. Beispiele lokaler Ringe sind:

(a) Körper;
(b) Formale Potenzreihenringe $k[[X_1, \dots, X_n]]$ über einem Körper k;
(c) $\mathbb{Z}/p$ und allgemeiner $\mathbb{Z}/p^n$ für eine Primzahl p;
(d) Später: Die Lokalisierung $R_\mathfrak{p}$ eines Rings R an einem Primideal $\mathfrak{p}$.

(e) Der Ring der Keime stetiger (reellwertiger) Funktionen bei $x \in M$ wobei M ein topologischer Raum ist. Betrachte Paare (U, f) wobei U eine offene Umgebung von x in M ist und $f \colon U \to \mathbb{R}$ eine stetige Funktion. Schreibe $(U, f) \sim (V, g)$ genau dann, wenn es eine offene Umgebung $W \subset U \cap V$ von x in M gibt mit $f|_W = g|_w$. Dies definiert eine Äquivalenzrelation auf der Menge K der Paare (U, f). Die Äquivalenzklassen heißen Keime stetiger Funktionen bei x. Wir überlassen es dem Leser, sich zu überlegen, dass K eine natürliche Ringstruktur besitzt, und dass man jeden Keim bei x auswerten kann. Dann ist K ein lokaler Ring und der Kern der Auswertungsabbildung $\mathrm{ev}_x \colon K \to \mathbb{R}$ ist sein maximales Ideal.

3.9.7. Ein Funktionskeim ist eine „lokal definierte Funktion“. Daher kommt vermutlich die Terminologie „lokaler Ring“.

3.9.8. Im Allgemeinen haben **minimale** Erzeugendensysteme (bezüglich Inklusion) eines (endlich erzeugten) R-Moduls M verschieden viele Elemente. Gilt etwa $1 = x + y$ für Elemente $x, y \in R - R^\times$, so sind $\{1\}$ und $\{x, y\}$ minimale Erzeugendensysteme des R-Moduls $M = R$. Als konkretes Beispiel nehme man etwa $x = T$ und $y = 1 - T$ in $\mathbb{C}[T]$.

Korollar 3.9.9 (Nakayamas Lemma für lokale Ringe)**.** *Sei $(R, \mathfrak{m})$ ein lokaler Ring und $k = R/\mathfrak{m}$ sein Restklassenkörper. Sei M ein endlich erzeugter R-Modul und $\overline{M} := M/\mathfrak{m}M$ (dies ist ein endlichdimensionaler k-Vektorraum, vgl. Lemma 3.2.14). Sei $\dim_k \overline{M} = n$. Seien $m_1, \ldots, m_n$ Elemente von M, deren Bilder $\{\overline{m}_1, \ldots, \overline{m}_n\}$ eine k-Basis von $\overline{M}$ bilden. Dann ist $\{m_1, \ldots, m_n\}$ ein minimales Erzeugendensystem von M. Jedes minimale Erzeugendensystem entsteht auf diese Weise.*

Insbesondere folgt aus $\mathfrak{m}M = M$ bereits $M = 0$.

Beweis. Sei $U = Rm_1 + \cdots + Rm_n$. Weil die Verknüpfung $U \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}M$ surjektiv ist, gilt $U = M$ nach Korollar 3.8.8. Also ist $\{m_1, \ldots, m_n\}$ ein Erzeugendensystem von M. Es ist offensichtlich minimal, denn jedes Erzeugendensystem geht auf ein Erzeugendensystemm von $\overline{M}$ als k-Vektorraum und muss somit mindestens n Elemente haben. Wir folgern sofort, dass jedes minimale Erzeugendensystem auf diese Weise entsteht. □

Beispiel 3.9.10. Sei k ein Körper und $R = k[[X]]$ der lokale Ring der formalen Potenzreihen in einer Variablen, und $\mathfrak{m} = (X)$ sein maximales Ideal. Fassen wir seinen Quotientenkörper $k((X))$ als R-Modul auf, so gilt $\mathfrak{m}M = M$. Dies zeigt, dass die Voraussetzung, dass M endlich erzeugt ist, in den Korollar 3.9.9 (und auch in Korollar 3.8.6) unabdingbar ist.

3.10. **Scholion: Kategorien und Funktoren.**

3.10.1. Der Begriff der Kategorie ist ein abstraktes Konzept, das die elementare Struktur vieler mathematischer Theorien beschreibt.

Definition 3.10.2. Eine **Kategorie** $\mathcal{C}$ ist ein Datum bestehend aus

(a) einer Klasse $\mathrm{Obj}(\mathcal{C})$ von **Objekten**;
(b) einer Menge $\mathcal{C}(X, Y)$ von **Morphismen** für je zwei Objekte $X, Y \in \mathrm{Obj}(\mathcal{C})$;
(c) einer Abbildung

$$\circ \colon \mathcal{C}(Y, Z) \times \mathcal{C}(X, Y) \to \mathcal{C}(X, Z),$$
$$(g, f) \mapsto g \circ f,$$

für je drei Objekte $X, Y, Z \in \mathrm{Obj}(\mathcal{C})$, genannt **Verknüpfung** von Morphismen,

so dass die folgenden Bedingungen gelten:

(a) Die Verknüpfung ist **assoziativ**, d. h. es gilt $(f \circ g) \circ h = f \circ (g \circ h)$ für alle Morphismen f, g, h, für die diese Verknüpfungen sinnvoll sind.
(b) Für jedes Objekt X gibt es einen Morphismus $\mathrm{id}_X \in \mathcal{C}(X, X)$, die **Identität** von X, so dass $\mathrm{id}_X \circ f = f$ und $g \circ \mathrm{id}_X = g$ für alle Morphismen f und g, für die diese Verknüpfungen sinnvoll sind.
(c) Die Morphismenmengen sind paarweise disjunkt.

3.10.3. Die Identität von X ist eindeutig bestimmt (sind id_X und id'_X Identitäten von X, so gilt $\mathrm{id}_X = \mathrm{id}_X \circ \mathrm{id}'_X = \mathrm{id}'_X$).

Notation 3.10.4. Wir schreiben oft $X \in \mathcal{C}$ für $X \in \mathrm{Obj}(\mathcal{C})$. Seien $X, Y \in \mathcal{C}$. Statt $f \in \mathcal{C}(X, Y)$ sagen wir auch, dass f ein **Morphismus von** X **nach** Y ist und schreiben kurz $f\colon X \to Y$. Man nennt Morphismen deswegen manchmal **Pfeile**. Man schreibt of $g \circ f$ statt gf und id_X statt id.

Definition 3.10.5. Ein Morphismus $f\colon X \to Y$ in einer Kategorie $\mathcal{C}$ heißt **Isomorphismus**, falls es einen Morphismus $g\colon Y \to X$ gibt mit $fg = \mathrm{id}_Y$ und $gf = \mathrm{id}_X$.

Notation 3.10.6. Ist $f\colon X \to Y$ ein Isomorphismus, so gibt es genau einen Morphismus g wie in der Definition (der natürlich selbst ein Isomorphismus ist). Ein Isomorphismus $X \to Y$ wird als $X \xrightarrow{\sim} Y$ notiert.

Beispiele 3.10.7. (a) Ist R ein Ring, so ist die Kategorie $\mathrm{Mod}(R)$ der R-Moduln wie folgt definiert:
 (i) Die Objekte sind die R-Moduln.
 (ii) Gegeben Objekte M, N setze $\mathrm{Mod}(R)(M, N) := \mathrm{Hom}_R(M, N)$.
 (iii) Die Verknüpfung ist die offensichtliche Verknüpfung von Morphismen von R-Moduln.

 Es ist klar, dass dieses Datum die Axiome einer Kategorie erfüllt.

(b) Ein Spezialfall ist die Kategorie $\mathrm{Mod}(k)$ der Vektorräume über einem Körper.

(c) Analog definiert man viele andere Kategorien:
 (i) Die Kategorie Set der Mengen hat die Mengen als Objekte und Abbildungen zwischen Mengen als Morphismen.
 (ii) Die Kategorie Ring der Ringe hat die Ringe als Objekte und Ringmorphismen als Morphismen.
 (iii) Die Kategorie Top der topologischen Räume hat als Objekte topologische Räume und als Morphismen stetige Abbildungen. Hier ist es nicht richtig, dass ein Morphismus invertierbar ist (also ein Isomorphismus ist) genau dann, wenn er eine Bijektion auf den unterliegenden Mengen induziert. Isomorphismen in Top werden klassisch als Homöomorphismen bezeichnet.

(d) Es gibt auch Kategorien mit wenigen Objekten:
 (i) Die leere Kategorie, die kein Objekt hat.
 (ii) Einen multiplikativ geschriebenen Monoid M kann man auffassen als eine Kategorie $\underline{M}$ mit genau einem Objekt, notieren wir es $*$, und mit Morphismenmenge $\underline{M}(*, *) = M$ und Multiplikation als Verknüpfung. Es gilt $\mathrm{id}_* = 1$.
 (iii) Die im folgenden Diagramm angedeutete Kategorie $\mathcal{P}$ hat genau zwei Objekte, die wir 0 und 1 nennen, und genau drei Morphismen, nämlich die Identitäten id_0 und id_1 und einen weiteren Morphismus $f\colon 0 \to 1$; ihre Verknüpfung ist die einzig mögliche.

$$\mathcal{P}\colon \qquad \begin{tikzcd} 0 \arrow[loop left, "\mathrm{id}_0"] \arrow[r, "f"] & 1 \arrow[loop right, "\mathrm{id}_1"] \end{tikzcd}$$

 Es gilt also $\mathrm{Obj}(\mathcal{P}) = \{0, 1\}$. Die Mengen von Morphismen sind wie folgt gegeben: $\mathcal{P}(1, 0) := \emptyset$, $\mathcal{P}(0, 0) := \{\mathrm{id}_X\}$, $\mathcal{P}(0, 1) := \{f\}$, $\mathcal{P}(1, 1) := \{\mathrm{id}_Y\}$.
 (iv) Allgemeiner kann man jede partiell geordnete Menge $(A, \leq)$ als Kategorie $\mathcal{A}$ auffassen: Die Objekte sind die Elemente $a, b, \ldots$ von A, und $\mathcal{A}(a, b)$ besteht aus genau einem Element, falls $a \leq b$, und ist sonst leer. Die Verknüpfung ist die einzig mögliche.

(e) Ist $\mathcal{C}$ eine Kategorie, so dass $\mathcal{C}(X, X) = \{\mathrm{id}_X\}$ und $\mathcal{C}(X, Y) = \emptyset$ für alle Objekte $X \neq Y$ in $\mathcal{C}$, so sagt man, dass $\mathcal{C}$ eine **diskrete** Kategorie ist. Insbesondere kann man jede Menge als diskrete Kategorie auffassen.

Definition 3.10.8. Ein **Funktor** $F\colon \mathcal{C} \to \mathcal{D}$ von einer Kategorie $\mathcal{C}$ in eine andere Kategorie $\mathcal{D}$ ist ein Datum bestehend aus

(a) einer Abbildung $F = F_{\mathrm{Obj}}\colon \mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{D})$ und
(b) Abbildungen $F = F_{X,Y}\colon \mathcal{C}(X, Y) \to \mathcal{D}(FX, FY)$, für je zwei Objekte $X, Y \in \mathcal{C}$,

so dass gelten:

(a) $F(f \circ g) = F(f) \circ F(g)$ für alle verknüpfbaren Morphismen f und g in $\mathcal{C}$;
(b) $F(\mathrm{id}_X) = \mathrm{id}_{FX}$ für alle Objekte $X \in \mathcal{C}$.

Beispiel 3.10.9. Ist $\mathcal{C}$ eine Kategorie, so ist der **Identitätsfunktor** $\mathrm{id}_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$ die Identität auf Objekten und Morphismen.

Beispiel 3.10.10. Der Vergiß-Funktor $\mathrm{Mod}(R) \to \mathrm{Set}$ bildet einen R-Modul auf die zugrundeliegende Menge ab. Es gibt viele andere Vergiß-Funktoren, etwa der Funktor $\mathrm{Ring} \to \mathrm{Ab}$, der einen Ring auf die zugrundeliegende abelsche Gruppe abbildet.

3.10.11. Sei R ein Ring und M ein R-Modul. Wir definieren einen Funktor

$$\mathrm{Hom}_R(M, -)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$$

wie folgt: Ein Objekt N von $\mathrm{Mod}(R)$ wird auf $\mathrm{Hom}_R(M, N)$ geschickt, und ein Morphismus $f\colon N \to N'$ in $\mathrm{Mod}(R)$ auf

$$\begin{aligned} \mathrm{Hom}_R(M, f) := f_* := (f \circ ?)\colon \mathrm{Hom}_R(M, N) &\to \mathrm{Hom}_R(M, N'), \\ a &\mapsto fa = f \circ a. \end{aligned}$$

(Dies ist nicht nur ein Morphismus von Mengen, sondern sogar ein Morphismus von R-Moduln.) Wir vermeiden normalerweise die sperrige Notation $\mathrm{Hom}_R(M, f)$.

Ist $g\colon N' \to N''$ ein weiterer Morphismus in $\mathrm{Mod}(R)$, so gilt $(gf)_* = g_* f_*$, und offensichtlich gilt $(\mathrm{id}_N)_* = \mathrm{id}_{\mathrm{Hom}_R(N,N)}$ oder kurz $\mathrm{id}_* = \mathrm{id}$. Also ist $\mathrm{Hom}_R(M, -)$ wirklich ein Funktor.

Beispiel 3.10.12. Ist $\mathcal{C}$ eine beliebige Kategorie und $X \in \mathcal{C}$ ein Objekt, so definiert man analog einen Funktor

$$F := \mathcal{C}(X, -)\colon \mathcal{C} \to \mathrm{Set}.$$

Definition 3.10.13. Ist $\mathcal{C}$ eine Kategorie, so bezeichnen wir mit $\mathcal{C}^{\mathrm{op}}$ ihre **opponierte Kategorie**. Sie entsteht, indem man die Richtung aller Pfeile in $\mathcal{C}$ umdreht. Genauer hat $\mathcal{C}^{\mathrm{op}}$ dieselben Objekte wie $\mathcal{C}$, aber ihre Morphismenmengen sind definiert als

$$\mathcal{C}^{\mathrm{op}}(Y, X) := \mathcal{C}(X, Y).$$

Die Verknüpfung ist definiert per $f \circ_{\mathcal{C}^{\mathrm{op}}} g := g \circ_{\mathcal{C}} f$ für Morphismen $X \xleftarrow{f} Y \xleftarrow{g} Z$ in $\mathcal{C}^{\mathrm{op}}$ alias Morphismen $X \xrightarrow{f} Y \xrightarrow{g} Z$ in $\mathcal{C}$.

3.10.14. Sei $F\colon \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ ein Funktor. Dann dreht F die Richtung der Pfeile in folgendem Sinne um: Ist $X \xrightarrow{f} Y$ ein Morphismus in $\mathcal{C}$, also ein Morphismus $X \xleftarrow{f} Y$ in $\mathcal{C}^{\mathrm{op}}$, so liefert F einen Morphismus $F(X) \xleftarrow{F(f)} F(Y)$ in $\mathcal{D}$.

Sind

$$X \xrightarrow{f} Y \xrightarrow{g} Z \quad \text{Morphismen in } \mathcal{C},$$

so erhalten wir Morphismen

$$F(X) \xleftarrow{F(f)} F(Y) \xleftarrow{F(g)} F(Z) \quad \text{in } \mathcal{D},$$

und es gilt

$$F(g \circ_{\mathcal{C}} f) = F(f \circ_{\mathcal{C}^{\mathrm{op}}} g) = F(f) \circ_{\mathcal{D}} F(g)$$

oder kurz $F(gf) = F(f)F(g)$.

3.10.15. Ist R ein Ring und M ein R-Modul, so definieren wir wie folgt einen Funktor

$$\mathrm{Hom}_R(-, M)\colon \mathrm{Mod}(R)^{\mathrm{op}} \to \mathrm{Mod}(R).$$

Auf Objekten ist er in der offensichtlichen Weise gegeben, und einen Morphismus $f\colon N \to N'$ bildet er auf den Morphimsmus

$$\begin{aligned} \mathrm{Hom}_R(-, M)\colon f^* := (? \circ f)\colon \mathrm{Hom}_R(N', M) &\to \mathrm{Hom}_R(N, M), \\ a &\mapsto af = a \circ f, \end{aligned}$$

ab. Es gelten $\mathrm{id}^* = \mathrm{id}$ und $(gf)^* = f^* g^*$ (wobei die Verknüpfung gf in $\mathrm{Mod}(R)$ und nicht in $\mathrm{Mod}(R)^{\mathrm{op}}$ gebildet wurde).

Beispiel 3.10.16. Ist $\mathcal{C}$ eine beliebige Kategorie und $X \in \mathcal{C}$ ein Objekt, so erhält man Funktoren

$$F := \mathcal{C}(X, -) \colon \mathcal{C} \to \mathrm{Set}$$

und

$$F := \mathcal{C}(-, X) \colon \mathcal{C}^{\mathrm{op}} \to \mathrm{Set}.$$

3.10.17 (Verknüpfung von Funktoren)**.** Sind $F \colon \mathcal{C} \to \mathcal{D}$ und $G \colon \mathcal{D} \to \mathcal{E}$ Funktoren, so definiert man die **Verknüpfung** in der offensichtlichen Weise.

to be explained

Wenn man mengentheoretische Probleme ignoriert, erhalten wir die Kategorie der Kategorien.

3.11. **Exakte Sequenzen.** Sei R ein Ring.

Definition 3.11.1. Eine **Sequenz** oder **Folge** (von R-Moduln) ist eine Familie $(f_i \colon M_i \to M_{i+1})_{i \in I}$ von Morphismen von R-Moduln, für ein Intervall I in $\mathbb{Z}$. Eine solche Folge wird meist durch

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

illustriert (falls I nach unten bzw. nach oben beschränkt ist, so ergänzt man links den Modul $M_{\min(I)}$ bzw. rechts den Modul $M_{\max(I)} + 1$). Eine solche Folge heißt **exakt bei** M_i, für ein $i \in I$, falls $i - 1 \in I$ und

$$\mathrm{im}(f_{i-1}) = \ker(f_i)$$

gelten (insbesondere muss also $f_i \circ f_{i-1} = 0$ gelten). Sie heißt **exakt**, falls sie exakt bei M_i ist für alle $i \in I$ mit $i - 1 \in I$.

Beispiele 3.11.2.
(a) Eine Folge $0 \to M' \xrightarrow{f} M$ ist exakt genau dann, wenn f injektiv ist. (Der nicht bezeichnete Morphismus $0 \to M'$ ist der einzig mögliche, nämlich die Nullabbildung.)
(b) Eine Folge $M \xrightarrow{g} M'' \to 0$ ist exakt genau dann, wenn g surjektiv ist.
(c) Ist $f \colon M \to N$ ein Morphismus von R-Moduln, so ist die Folge

$$0 \to \ker(f) \to M \xrightarrow{f} N \to N/\mathrm{im}(f) \to 0$$

exakt. Man bezeichnet $N/\mathrm{im}(f)$ als **Kokern** von f und notiert ihn $\mathrm{cok}(f)$.
(d) Die Folge $0 \to M \to M \oplus N \to N \to 0$ ist exakt.
(e) Die Folge

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

ist exakt. Hier ist $\mathbb{Z}/4 := \mathbb{Z}/4\mathbb{Z}$ und alle Abbildungen sind Mulitplikation mit $2 = \overline{2}$.
(f) Teilfolgen exakter Folgen sind exakt.
(g) Eine Folge von R-Moduln ist exakt genau dann, wenn sie als Folge von abelschen Gruppen exakt ist.
(h) könnte Koszulauflösung explizit angeben für $R = k[X, Y]$ und die Elemente X und Y.

Definition 3.11.3. Eine **kurze exakte Sequenz** oder **kurze exakte Folge** (von R-Moduln) ist eine exakte Sequenz von R-Moduln der Gestalt

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

Explizit bedeutet dies, das f injektiv ist (Exaktheit bei M'), dass $\mathrm{im}(f) = \ker(g)$ gilt (Exaktheit bei M), und dass g surjektiv ist (Exaktheit bei M'').

Beispiele 3.11.4.
(a) Ist $U \subset M$ ein Untermodul, so ist $0 \to U \to M \to M/U \to 0$ eine kurze exakte Sequenz. Jede kurze exakte Sequenz ist „bis auf eindeutigen Isomorphismus“ von dieser Form, siehe Beispiel 3.11.14.
(b) Die Folgen $0 \to \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z} \to \mathbb{Z}/2 \to 0$ und $0 \to \mathbb{Z}/2 \xrightarrow{2} \mathbb{Z}/4 \to \mathbb{Z}/2 \to 0$ sind kurze exakte Sequenzen.

Proposition 3.11.5.

(a) *Eine Sequenz*

$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$$

von R-Moduln ist exakt genau dann, wenn für alle R-Moduln T (die wir als „Testmoduln“ auffassen) die Sequenz

$$0 \to \mathrm{Hom}_R(T, N') \xrightarrow{f_*} \mathrm{Hom}_R(T, N) \xrightarrow{g_*} \mathrm{Hom}_R(T, N'') \tag{3.11.1}$$

von R-Moduln exakt ist.

(b) *Eine Sequenz*

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

von R-Moduln ist exakt genau dann, wenn für alle R-Moduln T die Sequenz

$$\mathrm{Hom}_R(M', T) \xleftarrow{f^*} \mathrm{Hom}_R(M, T) \xleftarrow{g^*} \mathrm{Hom}_R(M'', T) \leftarrow 0 \tag{3.11.2}$$

von R-Moduln exakt ist.

Beweis. (a) $\Rightarrow$: Sei T ein R-Modul. Zu zeigen ist, dass die Sequenz (3.11.1) exakt ist.

(1) Exaktheit bei $\mathrm{Hom}_R(T, N')$: Zu zeigen ist, dass f_* injektiv ist. Sei $a \in \ker(f_*)$, also $0 = f_*(a) = f \circ a$. Da f injektiv ist, folgt $a = 0$.

(2) Exaktheit bei $\mathrm{Hom}_R(T, N)$:

(i) $\mathrm{im}(f_*) \subset \ker(g_*)$: Aus $\mathrm{im}(f) \subset \ker(g)$ folgt $gf = 0$, also $0 = 0_* = (gf)_* = g_* f_*$, also $\mathrm{im}(f_*) \subset \ker(g_*)$.

Da $f\colon N' \to N$ injektiv ist und $\mathrm{im}(f) = \ker(g)$ gilt, faktorisiert f nach dem Homomorphiesatz 3.2.11 als

$$N' \xrightarrow{\sim} \mathrm{im}(f) = \ker(g) \hookrightarrow N.$$

(ii) $\mathrm{im}(f_*) \supset \ker(g_*)$: Sei $b \in \ker(g_*)$, es gilt also $0 = g_*(b) = gb$. Also landet b in $\ker(g)$, und wir erhalten den im folgenden Diagramm angedeuteten Morphismen b', und dann offensichtlich auch den Morphismus a, so dass das Diagramm kommutativ ist.

$$\begin{tikzcd}
 & & & T \arrow[dlll, dotted, "\exists! a"'] \arrow[dl, dotted, "\exists! b'"'] \arrow[d, "b"] \\
N' \arrow[r, "\sim"] \arrow[rrr, hook, bend right, "f"'] & \mathrm{im}(f) \arrow[r, phantom, "="] & \ker(g) \arrow[r, hook] & N
\end{tikzcd}$$

Es folgt $b = fa = f_*(a)$, also $\ker(g_*) \subset \mathrm{im}(f_*)$.

$\Leftarrow$: Die vertikalen Isomorphismen in dem Diagramm

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(R, N') \arrow[r, "f_*"] \arrow[d, "\sim"] & \mathrm{Hom}_R(R, N) \arrow[r, "g_*"] \arrow[d, "\sim"] & \mathrm{Hom}_R(R, N'') \arrow[d, "\sim"] \\
0 \arrow[r] & N' \arrow[r, "f"] & N \arrow[r, "g"] & N''
\end{tikzcd}$$

sind die durch Auswerten bei 1 gegebenen Isomorphismen von R-Moduln (Lemma 3.1.9). Man überprüft leicht, dass das Diagramm kommutativ ist.[5] Die obere Zeile ist die exakte Sequenz (3.11.1) für $T = R$. Also ist auch die untere Zeile exakt.

(b) $\Rightarrow$: Sei T ein R-Modul.

(1) Exaktheit bei $\mathrm{Hom}_R(M'', T)$: Zu zeigen ist, dass g^* injektiv ist. Ist $a \in \ker(g^*)$, also $0 = g^*(a) = ag$, so folgt aus der Surjektivität von g, dass $a = 0$.

(2) Exaktheit bei $\mathrm{Hom}_R(M, T)$:

(i) $\mathrm{im}(g^*) \subset \ker(f^*)$: Aus $0 = gf$ folgt $0 = 0^* = (gf)^* = f^* g^*$ und damit $\mathrm{im}(g^*) \subset \ker(f^*)$.

[5] In kategorieller Sprache liegt das daran, dass Auswerten bei 1 ein Isomorphismus (= eine natürliche Isotransformation) $\mathrm{Hom}_R(R, -) \overset{\sim}{\Rightarrow} \mathrm{id}$ von Funktoren $\mathrm{Mod}(R) \to \mathrm{Mod}(R)$ ist.

Da g surjektiv ist und $\ker(g) = \mathrm{im}(f)$, faktorisiert g nach dem Homomorphiesatz 3.2.11 als

$$M \twoheadrightarrow M/\ker(g = M/\mathrm{im}(f) \xrightarrow{\sim} M''.$$

(ii) $\mathrm{im}(g^*) \supset \ker(f^*)$: Sei $b \in \ker(f^*)$, also $0 = f^*(b) = bf$. Dies bedeutet $b(\mathrm{im}(f)) = 0$, und somit faktorisiert $b\colon M \to T$ eindeutig über $M \twoheadrightarrow M/\mathrm{im}(f)$, es existiert also der im folgenden Diagramm angedeutete Morphismus b', und dann auch der Morphismus c, so dass das Diagramm kommutativ ist.

$$\begin{tikzcd}
M \arrow[r, two heads] \arrow[rrr, bend left, "g"] \arrow[d, "b"'] & M/\ker(g) \arrow[r, phantom, "="] & M/\mathrm{im}(f) \arrow[r, "\sim"] \arrow[dll, dotted, "\exists! b'"'] & M'' \arrow[dlll, dotted, "\exists! c"] \\
T
\end{tikzcd}$$

Es folgt $b = ag = g^*(a)$ und damit $\ker(f^*) \subset \mathrm{im}(g^*)$.

$\Leftarrow$: Wir zeigen, dass $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ exakt ist.

(a) Exaktheit bei M'': Betrachte die exakte Sequenz (3.11.2) für $T = M''/\mathrm{im}(g)$. Der Morphismus $\mathrm{can}\colon M'' \to M''/\mathrm{im}(g)$ erfüllt $g^*(\mathrm{can}) = \mathrm{can} \circ g = 0$. Da g^* injektiv ist, folgt $\mathrm{can} = 0$. Da can surjektiv ist, folgt $M''/\mathrm{im}(g) = 0$ und somit $M'' = \mathrm{im}(g)$. Damit ist g surjektiv.

(b) Exaktheit bei M:

(i) $\mathrm{im}(f) \subset \ker(g)$: Betrachte die exakte Sequenz (3.11.2) für $T = M''$. Wegen $Kern(f^*) \subset \mathrm{im}(g^*)$ gilt $f^*g^* = 0$ und somit $0 = f^*(g^*(\mathrm{id}_{M''})) = gf$ und es folgt $\mathrm{im}(f) \subset \ker(g)$.

Wie unten erklärt erhalten wir damit das kommutative Diagramm

(3.11.3)
$$\begin{tikzcd}
M \arrow[rr, two heads, "g"] \arrow[d, two heads, "q"] \arrow[drr, "p"] & & M'' \\
M/\mathrm{im}(f) \arrow[rr, two heads, "\overline{p}"] & & M/\ker(g). \arrow[u, "\overline{g}"', "\sim"]
\end{tikzcd}$$

Wir wissen bereits, dass g ein Epimorphismus ist. Nach dem Homomorphiesatz 3.2.11 faktorisiert er als $g = \overline{g} \circ p$, wobei $\overline{g}$ ein Isomorphismus ist. Aus $\mathrm{im}(f) \subset \ker(g)$ folgt $p(\mathrm{im}(f)) \subset p(\ker(g)) = 0$, und damit faktorisiert p nach der universellen Eigenschaft des Quotienten $q\colon M \to M/\mathrm{im}(f)$ (eindeutig) als $p = \overline{p} \circ q$, und mit p ist auch $\overline{p}$ surjektiv.

(ii) $\mathrm{im}(f) \supset \ker(g)$: Nun betrachte die exakte Sequenz (3.11.2) für $T = M/\mathrm{im}(f)$. Wegen $f^*(q) = qf = 0$ gibt es (genau) einen Morphismus $c\colon M'' \to M/\mathrm{im}(f)$ mit $q = g^*(c) = cg$. Aus dem kommutativen Diagramm (3.11.3) folgt somit $q = cg = c\overline{g}\,\overline{p}q$. Weil q surjektiv ist, folgt daraus $\mathrm{id}_{M/\mathrm{im}(f)} = c\overline{g}\,\overline{p}$. Insbesondere ist $\overline{p}$ injektiv. Damit ist $\overline{p}$ bijektiv, und es folgt $0 = \ker(\overline{p}) = \ker(g)/\mathrm{im}(f)$ und somit $\ker(g) = \mathrm{im}(f)$.

□

Korollar 3.11.6.

(a) Eine Sequenz

$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$$

in $\mathrm{Mod}(R)$ *ist exakt genau dann, wenn* $gf = 0$ *gilt und für alle Morphismen* $t\colon T \to N$ *(die wir als „Testmorphismen“ auffassen) mit* $gt = 0$ *genau ein Morphismus* $t'\colon T \to N'$ *existiert mit* $ft' = t$*. Wir illustrieren dies so:*

$$\begin{tikzcd}
& T \arrow[dl, dotted, "\exists! t'"'] \arrow[d, "\forall t"] \arrow[dr, "\text{falls } gt = 0"] & \\
N' \arrow[r, "f"] & N \arrow[r, "g"] & N''
\end{tikzcd}$$

(b) Eine Sequenz

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

in $\mathrm{Mod}(R)$ *ist exakt genau dann, wenn* $gf = 0$ *gilt und für alle Morphismen* $t\colon M \to T$ *mit* $tf = 0$ *genau ein Morphismus* $t'\colon M'' \to T$ *mit* $t'g = t$ *existiert. Wir illustrieren dies so:*

$$\begin{tikzcd} M' \arrow[r, "f"] \arrow[dr, "\text{falls } tf=0"'] & M \arrow[r, "g"] \arrow[d, "\forall t"] & M'' \arrow[dl, "\exists! t'"] \\ & T & \end{tikzcd}$$

Beweis. (a) Dies ist nur eine Umformulierung von Proposition 3.11.5.(a): Die Bedingung $gf = 0$ ist äquivalent zu $\mathrm{im}(f_*) \subset \ker(g_*)$. Die Bedingung, dass t' unter den gegebenen Voraussetzungen existiert, ist äquivalent zu $\mathrm{im}(f_*) \supset \ker(g_*)$. Die Bedingung, dass t' eindeutig ist, ist äquivalent zur Injektivität von f_* (gegeben $a, b\colon T \to N'$ mit $fa = f_*(a) = f_*(b) = fb$ setze man $t = fa = fb$).

(b) Dies ist ebenso nur eine Umformulierung von Proposition 3.11.5.(b). □

Definition 3.11.7. Sei $f\colon M \to N$ ein Morphismus von R-Moduln. Ein Morphismus $\kappa\colon K \to M$ von R-Moduln heißt **Kern** von f, falls $0 \to K \xrightarrow{\kappa} M \xrightarrow{f} N$ exakt ist. Ein Morphismus $\gamma\colon N \to C$ von R-Moduln heißt **Kokern** von f, falls $M \xrightarrow{f} N \xrightarrow{\gamma} C \to 0$ exakt ist.

3.11.8. Kern und Kokern eines Morphismus erfüllen die in Korollar 3.11.6 beschriebenen universellen Eigenschaften. Diese Eigenschaften liefern äquivalente Definitionen von Kern und Kokern.[6]

3.11.9. Ist der Morphismus $\kappa\colon K \to M$ offensichtlich, sagt man abkürzend, dass K ein Kern von f ist. In diesem Sinne ist der in Beispiel 3.2.5 eingeführte Kern $\ker(f) = f^{-1}(0)$ (zusammen mit der Inklusionsabbildung $\ker(f) \hookrightarrow M$) ein Kern von f im Sinne der Definition 3.11.7 (nach Beispiel 3.11.2.(c)). Insbesondere hat jeder Morphismus einen Kern. Ist K ein Kern von f, so schreibt man auch $\ker(f)$ statt K. Analoges gilt für den Kokern.

3.11.10. Bei der Definition 3.11.1 der Exaktheit haben wir verlangt, dass $\mathrm{im}(f_{i-1}) = \ker(f_i)$. Hier fassen wir der Einfachheit halber $\ker(f_i)$ weiterhin als Untermodul von M_i aus, wir verlangen also, dass $f_{i-1}(M_{i-1}) = (f_i)^{-1}(0_{M_{i+1}})$.

Lemma 3.11.11. *Sei* $f\colon M \to N$ *ein Morphismus von* R*-Moduln.*

(a) *(Eindeutigkeit des Kerns bis auf eindeutigen Isomorphismus) Seien* $\kappa_1\colon K_1 \to M$ *und* $\kappa_2\colon K_2 \to M$ *Kerne von* f*. Dann gibt es genau einen Isomorphismus* $\alpha\colon K_1 \to K_2$ *mit* $\kappa_2\alpha = \kappa_1$*.*

$$\begin{tikzcd} K_1 \arrow[dr, "\kappa_1"] \arrow[dd, "\exists!\alpha"', "\sim"] & \\ & M \\ K_2 \arrow[ur, "\kappa_2"'] & \end{tikzcd}$$

(b) *(Eindeutigkeit des Kokerns bis auf eindeutigen Isomorphismus) Seien* $\gamma_1\colon N \to C_1$ *und* $\gamma_2\colon N \to C_2$ *Kokerne von* f*. Dann gibt es genau einen Isomorphismus* $\alpha\colon C_1 \to C_2$ *mit* $\alpha\gamma = \gamma'$*.*

$$\begin{tikzcd} & C_1 \arrow[dd, "\alpha"', "\sim"] \\ N \arrow[ur, "\gamma_1"] \arrow[dr, "\gamma_2"'] & \\ & C_2 \end{tikzcd}$$

3.11.12. Wir dürfen also den bestimmten Artikel verwenden und von dem Kern (bzw. dem Kokern) eines Morphismus verwenden.

Beweis. (a) Wir verwenden die in Korollar 3.11.6.(a) beschriebenen universellen Eigenschaft eines Kerns. Seien $i, j \in \{1, 2\}$. Wegen $f\kappa_i = 0$ und Exaktheit von $0 \to K_j \xrightarrow{\kappa_j} M \xrightarrow{f} N$ gibt es genau einen Morphismus $\alpha_{ij}\colon K_i \to K_j$ mit $\kappa_j\alpha_{ij} = \kappa_i$. Auf diese Weise erhalten wir vier Morphismen $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$.

Aus $\kappa_1 \mathrm{id}_{K_1} = \kappa_1$ und $\kappa_1\alpha_{21}\alpha_{12} = \kappa_2\alpha_{12} = \kappa_1$ folgt $\mathrm{id}_{K_1} = \alpha_{11} = \alpha_{21}\alpha_{12}$ wegen der Eindeutigkeit von α_{11}. Analog folgt $\mathrm{id}_{K_2} = \alpha_{22} = alpha_{12}\alpha_{21}$.

[6] Dies sind die üblichen Definitionen von Kern und Kokern in einer beliebigen Kategorie mit Nullobjekt (= ein Objekt, das zugleich initial und final ist).

Also sind α_{12} und $\alpha 21$ zueinander inverse Isomorphismen. Setze $\alpha = \alpha_{12}$.
(b) Dies folgt analog aus Korollar 3.11.6.(b). $\square$

Aufgabe 3.11.13. Betrachten Sie das Diagramm

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, dotted, "a"'] & B \arrow[r, "p"] \arrow[d, "b"'] & C \arrow[r] \arrow[d, dotted, "c"'] & 0 \\
0 \arrow[r] & A' \arrow[r, "i'"] & B' \arrow[r, "p'"] & C' \arrow[r] & 0
\end{tikzcd}$$

in $\mathrm{Mod}(R)$ und nehmen Sie an, dass die beiden Zeilen kurze exakte Sequenzen sind. Gelte $p' \circ b \circ i = 0$.

(a) Zeigen Sie, dass es eindeutige gepunktete Pfeile a und c wie in dem obigen Diagramm angedeutet gibt, so dass die beiden Quadrate kommutativ sind.
(b) (Spezialfall des Fünferlemmas) Zeigen Sie: Sind die beiden Morphismen a und c Isomorphismen, so ist auch c ein Isomorphismus.

Beispiel 3.11.14. Sei $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ eine kurze exakte Sequenz und $U := \mathrm{im}(f) = \ker(g)$. Nach Aufgabe 3.11.13 gibt es wegen $pf = 0$ eindeutige gepunktete Morphismen, so dass das Diagramm

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, dotted] & M \arrow[r, "g"] \arrow[d, equal] & M'' \arrow[r] \arrow[d, dotted] & 0 \\
0 \arrow[r] & U \arrow[r, "i"] & M \arrow[r, "p"] & M/U \arrow[r] & 0
\end{tikzcd}$$

kommutativ ist. Dasselbe Argument liefert wegen $gi = 0$ eindeutige Morphismen $U \to M'$ und $M/U \to M''$ in der anderen Richtung, so dass das offensichtliche Diagramm kommutativ ist. Es folgt dann wie im Beweis von Lemma 3.11.11.(a), dass die gepunkteten Morphismen Isomorphismen sind. In diesem Sinne ist jede kurze exakte Sequenz eindeutig isomorph zu einer kurzen exakten Sequenz $0 \to U \to M \to M/U \to 0$ in Standardform.

Aufgabe 3.11.15. Sei $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ eine kurze exakte Sequenz in $\mathrm{Mod}(R)$. Zeigen Sie die Äquivalenz der beiden folgenden Aussagen:

(a) Der Epimorphismus p spaltet (siehe Aufgabe 3.4.11): Es gibt einen Morphismus $s\colon C \to B$ mit $ps = \mathrm{id}_C$.
(b) Der Monomorphismus i **spaltet**: Es gibt einem Morphismus $t\colon B \to A$ mit $ti = \mathrm{id}_A$. (Ein solches t nennt man eine **Spaltung** des Monomorphimus i.)

Sind diese Bedingungen erfüllt, so sagt man, dass die kurze exakte Sequenz spaltet (oder besser: eine Spaltung erlaubt).

(c) Nehmen Sie an, dass unsere kurze exakte Sequenz spaltet. Zeigen Sie, dass es eine Isomorphismus β gibt, so das das Diagramm (mit exakten Zeilen)

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota_A"] \arrow[d, "\mathrm{id}_A"'] & A \oplus C \arrow[r, "\mathrm{pr}_C"] \arrow[d, "\beta"', "\sim"] & C \arrow[r] \arrow[d, "\mathrm{id}_C"'] & 0 \\
0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r, "p"] & C \arrow[r] & 0
\end{tikzcd}$$

kommutativ ist.
(d) Geben Sie ein Beispiel einer nicht spaltenden exakten Folge für einen geeigneten Ring.

Definition 3.11.16. Seien A und B Ringe. Ein Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ oder $F\colon \mathrm{Mod}(A)^{\mathrm{op}} \to \mathrm{Mod}(B)$ heißt **additiv**, falls $F(f + f') = F(f) + F(f')$ für alle Morphismen $f, f'\colon M \to N$ in $\mathrm{Mod}(A)$ gilt.

3.11.17. Ein solcher Funktor F bildet den Nullmodul auf den Nullmodul ab: Sei N ein A-Modul. Da F ein Funktor ist, gilt $F(\mathrm{id}_N) = \mathrm{id}_{F(N)}$. Da die Abbildung $F\colon \mathrm{Hom}_A(N, N) \to \mathrm{Hom}_B(F(N), F(N))$ ein Morphismus abelscher Gruppen ist, gilt $F(0_N) = 0_{F(N)}$, wobei hier 0_N und $0_{F(N)}$ die jeweiligen Nullendomorphismen bezeichnen. Nehmen wir nun an, dass $N = 0$ der Nullmodul ist. Dann gilt $\mathrm{id}_N = 0_N$, und es folgt $\mathrm{id}_{F(N)} = F(\mathrm{id}_N) = F(0_N) = 0_{F(N)}$. Daraus folgt $F(N) = 0$.

Definition 3.11.18. Seien A und B Ringe. Ein Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ heißt

(a) **linksexakt**, falls er additiv ist und falls für jede exakte Sequenz

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

in $\mathrm{Mod}(A)$ die Sequenz

$$0 \to F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'')$$

in $\mathrm{Mod}(B)$ exakt ist.

(b) **rechtsexakt**, falls er additiv ist und falls für jede exakte Sequenz

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

in $\mathrm{Mod}(A)$ die Sequenz

$$F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'') \to 0$$

in $\mathrm{Mod}(B)$ exakt ist.

(c) **exakt** ist, falls er links- und rechtsexakt ist.

Beispiel 3.11.19. Der Funktor $\mathrm{Hom}_R(T, -)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$ ist linksexakt (siehe Proposition 3.11.5.(a)).

Frage 3.11.20. Ich wüßte gerne ein Beispiel eines Funktors $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$, der nicht additiv ist, aber die andere definierende Eigenschaft eines linksexakten Funktors erfüllt.

3.11.21. Ein additiver Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ ist linksexakt genau dann, wenn er Kerne auf Kerne abbildet: Ist $\kappa\colon K \to M$ ein Kern von $f\colon M \to N$, so ist $F(\kappa)\colon F(K) \to F(M)$ ein Kern von $F(f)\colon F(M) \to F(N)$. Dies ist nur eine Umformulierung mit Hilfe der Definitionen.

Analog ist F rechtsexakt genau dann, wenn er Kokerne auf Kokerne abbildet.

3.11.22. Jeder linksexakte (bzw. rechtsexakte) Funktor $\mathrm{Mod}(A) \to \mathrm{Mod}(B)$ erhält Monomorphismen (bzw. Epimorphismen).

Aufgabe 3.11.23. Seien A und B Ringe.

(a) Ein additiver Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ ist genau dann linksexakt, wenn für jede kurze exakte Sequenz $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ die Folge $0 \to F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'')$ exakt ist.

(b) Die analoge Aussage für rechtsexakte Funktoren gilt ebenfalls.

(c) Folgern Sie, dass ein additiver Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ exakt ist genau dann, wenn er kurze exakte Sequenzen auf kurze exakte Sequenzen abbildet.

(d) Folgern Sie, dass ein linksexakter Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ Epimorphismen erhält genau dann, wenn er exakt ist.

(e) Folgern Sie, dass ein rechtsexakter Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ Monomorphismen erhält genau dann, wenn er exakt ist.

Aufgabe 3.11.24. Ein additiver Funktor $F\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ ist exakt genau dann, wenn für jede exakte Folge $M_1 \to M_2 \to M_3$ (Exaktheit wird also nur bei M_2 verlangt) die Folge $F(M_1) \to F(M_2) \to F(M_3)$ exakt ist.

Definition 3.11.25. Seien A und B Ringe. Ein Funktor $F\colon \mathrm{Mod}(A)^{\mathrm{op}} \to \mathrm{Mod}(B)$ heißt

(a) **linksexakt**, falls er additiv ist und falls für jede exakte Sequenz

$$0 \leftarrow M' \xleftarrow{f} M \xleftarrow{g} M''$$

in $\mathrm{Mod}(A)$ die Sequenz

$$0 \to F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'')$$

in $\mathrm{Mod}(B)$ exakt ist.

(b) **rechtsexakt**, falls er additiv ist und falls für jede exakte Sequenz

$$M' \xleftarrow{f} M \xleftarrow{g} M'' \leftarrow 0$$

in $\mathrm{Mod}(A)$ die Sequenz

$$F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'') \to 0$$

in $\mathrm{Mod}(B)$ exakt ist.

(c) **exakt** ist, falls er links- und rechtsexakt ist.

Beispiel 3.11.26. Der Funktor $\mathrm{Hom}_R(-, T)\colon \mathrm{Mod}(R)^{\mathrm{op}} \to \mathrm{Mod}(R)$ ist ein linksexakter Funktor (siehe Proposition 3.11.5.(b)).

Aufgabe 3.11.27. Sei R ein Ring.

(a) Sei $\mathfrak{a}$ ein Ideal in R und N ein R-Modul. Finden Sie einen kanonischen Isomorphismus

$$\mathrm{Hom}_R(R/\mathfrak{a}, N) \xrightarrow{\sim} \{n \in N \mid an = 0 \text{ für alle } a \in \mathfrak{a}\}.$$

(b) Geben Sie ein Beispiel dafür, dass der Funktor $\mathrm{Hom}_R(T, -)$ im Allgemeinen nicht exakt ist. (Sie können zum Beispiel $R = \mathbb{Z}$ wählen).

(c) Geben Sie ein Beispiel dafür, dass der Funktor $\mathrm{Hom}_R(-, T)$ im Allgemeinen nicht exakt ist. (Sie können zum Beispiel $R = \mathbb{Z}$ wählen).

(d) Sei $\mathfrak{a}$ ein Ideal in R. Zeigen Sie, dass der Funktor $\mathrm{Mod}(R) \to \mathrm{Mod}(R)$, $M \mapsto M/\mathfrak{a}M$, rechtsexakt ist.

(e) Verifizieren Sie, dass der Funktor $\mathrm{Mod}(\mathbb{Z}) \to \mathrm{Mod}(\mathbb{Z})$, $M \mapsto \mathfrak{a}M$, für $\mathfrak{a} = 2\mathbb{Z}$ weder links- noch rechtsexakt ist.

Lemma 3.11.28. *Sei $0 \to K \xrightarrow{i} L \xrightarrow{p} M \to 0$ eine kurze exakte Sequenz von R-Moduln. Sind K und M endlich erzeugt, so ist auch L endlich erzeugt.*

3.11.29. Die Umkehrung gilt nicht: Untermoduln endlich erzeugter Moduln sind im Allgemeinen nicht endlich erzeugt (siehe Aufgabe 3.5.7 für das Standardbeispiel).

Beweis. Die Bilder von Erzeugern von K samt Urbildern von Erzeugern von M liefern Erzeuger von L. Genauer seien $k_1, \dots, k_s$ Erzeuger von K und $m_1, \dots, m_t$ Erzeuger von M. Da p surjektiv ist, gibt es $l_1, \dots, l_t \in L$ mit $p(l_i) = m_i$. Wir behaupten, dass $i(k_1), \dots, i(k_s), l_1, \dots, l_t$ Erzeuger von L sind. Sei $x \in L$. Dann gilt $p(x) = \sum_{i=1}^t r_i m_i$ für geeignete $r_i \in R$. Wegen

$$p(x - \sum r_i l_i) = p(x) - \sum r_i p(l_i) = p(x) = \sum r_i m_i = 0$$

gilt $x - \sum r_i l_i \in \ker(p) = \mathrm{im}(i)$. Also existieren $a_j \in R$ mit $i(\sum_{j=1}^s a_j k_j) = x - \sum r_i l_i$ und es folgt $x = \sum a_j i(k_j) + \sum r_i l_i$. Also ist L endlich erzeugt. □

Aufgabe 3.11.30. Sei C der Kokern von $\bigoplus_{\mathbb{N}} \mathbb{Z} \to \prod_{\mathbb{N}} \mathbb{Z}$. Zeigen Sie, dass die kurze exakte Sequenz

$$0 \to \bigoplus_{\mathbb{N}} \mathbb{Z} \to \prod_{\mathbb{N}} \to C \to 0$$

abelscher Gruppen nicht spaltet.

Hinweise:

(a) Jeder Morphismus $f\colon \prod_{\mathbb{N}} \mathbb{Z} \to \mathbb{Z}$ abelscher Gruppen, dessen Einschränkung auf $\bigoplus_{\mathbb{N}}$ verschwindet, ist bereits Null, d. h.

$$\mathrm{Hom}_{\mathbb{Z}}(\prod_{\mathbb{N}} \mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\bigoplus_{\mathbb{N}} \mathbb{Z}, \mathbb{Z})$$

ist injektiv ist.

(b) Es folgt $\mathrm{Hom}_{\mathbb{Z}}(C, \mathbb{Z}) = 0$.

Man kann zeigen, dass $\mathrm{Hom}_{\mathbb{Z}}(\prod_{\mathbb{N}} \mathbb{Z}, \mathbb{Z}) = \bigoplus_{\mathbb{N}} \mathbb{Z}$ gilt. [7]

[7] Das Stichwort zum Suchen lautet Baer-Specker group.

3.12. **Projektive Moduln.**

Definition 3.12.1. Ein R-Modul P heißt **projektiv**, falls der Funktor $\mathrm{Hom}_R(P,-)$ exakt ist.

3.12.2. Da $\mathrm{Hom}_R(P,-)$ stets linksexakt ist, folgern wir aus Aufgabe 3.11.23.(d): Der R-Modul P ist genau dann projektiv, wenn für jeden Epimorphismus $\pi\colon M \twoheadrightarrow M''$ die Abbildung

$$\pi_*\colon \mathrm{Hom}_R(P,M) \to \mathrm{Hom}_R(P,M'')$$

surjektiv ist. Dies bedeutet, dass P die folgende Liftungseigenschaft besitzt: Gegeben ein beliebiger Morphismus $a\colon P \to M''$, existiert ein Morphismus $\hat{a}\colon P \to M$ (ein Lift von a), so dass das Diagramm

$$\begin{tikzcd} & P \arrow[dl, dotted, "\exists\hat{a}"'] \arrow[d, "a"] \\ M \arrow[r, two heads, "\pi"] & M'' \end{tikzcd}$$

kommutativ ist.

3.12.3. Insbesondere gilt: Ist P projektiv, so spaltet jeder Epimorphismus $\pi\colon M \twoheadrightarrow P$. (Wende 3.12.2 auf $a = \mathrm{id}_P$ an.)

Zusatzbemerkung 3.12.4. In der homologischen Algebra sind projektive Moduln das wichtigste Hilfsmittel, um linksderivierte Funktoren auszurechnen.

Zusatzbemerkung 3.12.5. Endlich erzeugte projektive R-Moduln entsprechen in der algebraischen Geometrie den Vektorbündeln auf $\mathrm{Spec}\, R$.

Zusatzbemerkung 3.12.6. Ein R-Modul I heißt **injektiv** genau dann, wenn der Funktor $\mathrm{Hom}_R(-,I)$ exakt ist. Dieser Begriff ist dual zu dem Begriff eines projektiven Moduls. Wir studieren ihn vorerst nicht.

Proposition 3.12.7. *Ein R-Modul P ist projektiv genau dann, wenn er Summand eines freien Moduls ist. Insbesondere sind freie R-Moduln projektiv.*

Beweis. $\Rightarrow$: Nach Lemma 3.4.10 gibt es einen freien R-Modul F und einen Epimorphismus $\pi\colon F \twoheadrightarrow P$. Da P projektiv ist, spaltet dieser, und wir erhalten $P \oplus \ker(\pi) \cong F$ (siehe Aufgabe 3.4.11).

$\Leftarrow$: Wir werden dies aus drei Behauptungen folgern:

(a) R ist projektiv: Sei $\pi\colon M \to M''$ ein Morphismus in $\mathrm{Mod}(R)$. Lemma 3.1.9 liefert die vertikalen Isomorphismen in dem offensichtlich kommutativen Diagramm

(3.12.1)
$$\begin{tikzcd} \mathrm{Hom}_R(R,M) \arrow[r, "\pi_*"] \arrow[d, "\mathrm{ev}_1", "\sim"'] & \mathrm{Hom}_R(R,M'') \arrow[d, "\mathrm{ev}_1", "\sim"'] \\ M \arrow[r, "\pi"] & M''. \end{tikzcd}$$

Ist π ein surjektiv, so ist also auch π_* surjektiv.

(b) Ist $P \xrightarrow{\sim} Q$ ein Isomorphismus von R-Moduln, so ist P projektiv genau dann, wenn Q projektiv ist. Das ist offensichtlich.

(c) Sei $(P_i)_{i\in I}$ eine Familie von R-Moduln. Dann ist $\bigoplus_{i\in I} P_i$ projektiv genau dann, wenn jedes P_j projektiv ist, für $j \in I$.

$\Rightarrow$: Sei $\bigoplus_{i\in I} P_i$ projektiv. Sei $j \in I$ beliebig. Seien $a\colon P_j \to M''$ ein Morphismus und $\pi\colon M \twoheadrightarrow M''$ ein Epimorphismus. Wir erklären das Diagramm

$$\begin{tikzcd} \bigoplus_{i\in I} P_i \arrow[d, dotted, "\hat{b}"] \arrow[dr, dashed, "b"] & P_j \arrow[l, "\iota_j"'] \arrow[d, "a"] \\ M \arrow[r, two heads, "\pi"] & M''. \end{tikzcd}$$

Der Morphismus a und die Nullmorphismen $P_l \to M''$ für $l \in I - \{j\}$ liefern einen eindeutigen gestrichelten Morphismus $b\colon \bigoplus_{i\in I} P_i \to M''$ mit $b\iota_j = a$ und $b\iota_l = 0$ für alle $l \in I - \{j\}$. Laut

Annahme hat b den gepunkteten Lift $\hat{b}$ mit $\pi\hat{b} = b$. Wegen $\pi\hat{b}\iota_j = b\iota_j = a$ ist $\hat{b}\iota_j$ der gesuchte Lift von a.

$\Leftarrow$: Seien alle P_j projektiv. Seien $a\colon \bigoplus_{i\in I} P_i \to M''$ ein Morphismus und $\pi\colon M \twoheadrightarrow M''$ ein Epimorphismus. Wir erklären das Diagramm

$$\begin{tikzcd}
& P_j \arrow[d, "\iota_j"] \arrow[ddl, dotted, "a_j"'] \\
& \bigoplus_{i\in I} P_i \arrow[d, "a"] \arrow[dl, dashed, "b"'] \\
M \arrow[r, two heads, "\pi"] & M''.
\end{tikzcd}$$

Weil P_j für jedes $j \in I$ projektiv ist, liftet $a\iota_j$ entlang der Surjektion π zu dem gepunkteten Morphismus a_j mit $\pi a_j = a\iota_j$. Die Morphismen $(a_j)_{j\in I}$ liefern einen eindeutigen gestrichelten Morphismus $b\colon \bigoplus P_i \to M$ mit $b\iota_j = a_j$ für alle $j \in I$. Wir behaupten, dass dies der gesuchte Lift ist. Zu zeigen ist also $\pi b = a$. Wegen $\pi b\iota_j = \pi a_j = a\iota_j$ für beliebiges $j \in I$ folgt dies aber aus der universellen Eigenschaft der direkten Summe.

Diese drei Behauptungen implizieren, dass R, jeder direkte Summe $\bigoplus_{i\in I} R$ von Kopien von R, und jeder freie R-Modul projektiv sind. Sei nun P ein Summand eines freien R-Moduls, d. h. es gibt einen R-Modul Q, so dass $P \oplus Q$ frei ist. Projektivität von $P \oplus Q$ impliziert dann Projektivität von P (und Q) nach der dritten Behauptung. □

Beispiele 3.12.8. (a) Alle Vektorräume sind frei und damit projektiv.

(b) Alle Ideale von $\mathbb{Z}$ sind frei (vom Rang 1) als $\mathbb{Z}$-Moduln und somit projektiv.

(c) Analog sind Ideale in Hauptidealringen frei und projektiv.

(d) Der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ ist für $n \neq 0$ nicht projektiv. In der Tat, der Epimorphismus $\mathbb{Z} \to \mathbb{Z}/n$ spaltet nicht, denn in $\mathbb{Z}$ ist Null das einzige Element a, dass $na = 0$ erfüllt.

(e) Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist nicht projektiv (siehe Lemma 3.12.10).

3.12.9. Falls es nicht aus dem Kontext klar ist, ist es wichtig zu sagen, über welchem Ring man arbeitet: Beispielsweise ist $\mathbb{Q}$ projektiv als $\mathbb{Q}$-Modul, aber nicht als $\mathbb{Z}$-Modul.

Lemma 3.12.10. *Ist R ein Integritätsbereich, der kein Körper ist, so ist sein Quotientenkörper K nicht projektiv als R-Modul.*

Beweis. Wir nehmen an, dass K als R-Modul projektiv ist. Dann ist K ein Summand eines freien R-Moduls. Insbesondere gibt es also einen Monomorphismus

$$\iota\colon K \hookrightarrow F := \bigoplus_{i\in I} R$$

von R-Moduln. Sei $x = (x_i)_{i\in I} := \iota(1)$. Es gibt ein $j \in I$ mit $x_j \neq 0$. Sei $r \in R - \{0\}$ beliebig. Dann gilt $x_j r \neq 0$ und wir dürfen wie folgt rechnen:

$$x_j r\iota(\frac{1}{x_j r}) = \iota(\frac{x_j r}{x_j r}) = \iota(1) = x = (x_i)_{i\in I}.$$

Notieren wir die j-te Koordinate von $\iota(\frac{1}{x_j r})$ als a, so folgt $x_j r a = x_j$. Da R ein Integritätsbereich ist und $x_j \neq 0$, dürfen wir kürzen und erhalten $ra = 1$. Also ist jedes Element von $R - \{0\}$ invertierbar. Dies steht im Widerspruch zu der Annahme, dass R kein Körper ist. Also ist K nicht projektiv über R. □

Beispiele 3.12.11. Vielleicht später nicht in Vorlesung angeschrieben:

(a) Ist R ein Hauptidealring, so sind endlich erzeugte projektive R-Moduln frei, d. h. endlich erzeugt projektiv = endlich erzeugt frei.

(b) Ist $K/\mathbb{Q}$ eine endliche Körpererweiterung und $R = \mathcal{O}_K$, so ist jeder endlich erzeugte torsionsfreie R-Modul projektiv, d. h. projektiv endlich erzeugt = torsionsfrei endlich erzeugt. torsionsfrei zu definieren

Proposition 3.12.12. *Jeder endlich erzeugte projektive Modul über einem lokalen Ring ist frei.*

Zusatzbemerkung 3.12.13. Es ist sogar richtig, dass jeder projektive Modul über einem lokalen Ring frei ist, siehe [Sta16, 0593].

Beweis. Sei $(R, \mathfrak{m})$ ein lokaler Ring und M ein endlich erzeugter projektiver R-Modul. Seien $m_1, \dots, m_n$ Erzeuger von M, deren Bilder $\overline{m}_1, \dots, \overline{m}_n$ eine $R/\mathfrak{m}$-Basis von $M/\mathfrak{m}M$ bilden (solche Elemente gibt es nach Nakayamas Lemma 3.9.9). Betrachte den Epimorphismus

$$p \colon R^n \twoheadrightarrow M$$

mit $p(e_i) m_i$. Dieser spaltet, da M projektiv ist. Mit $K := \ker(p)$ folgt $K \oplus M \cong R^n$ und damit

$$K/\mathfrak{m}K \oplus M/\mathfrak{m}M \cong (K \oplus M)/\mathfrak{m}(K \oplus M) \cong R^n/(\mathfrak{m}R^n) \cong (R/\mathfrak{m})^n$$

als $R/\mathfrak{m}$-Vektorräume. Da $M/\mathfrak{m}M$ und $(R/\mathfrak{m})^n$ beide Dimension n haben, folgt $K/\mathfrak{m}K = 0$, also $K = \mathfrak{m}K$. Als Quotient von $K \oplus M \cong R^n$ ist K ein endlich erzeugter R-Modul. Nach Nakayamas Lemma 3.9.9 für lokale Ringe folgt $K = 0$ und somit ist p ein Isomorphismus $R^n \xrightarrow{\sim} M$. □

3.13. **Moduln von endlicher Darstellung.**

Definition 3.13.1. Ein R-Modul M heißt **von endlicher Darstellung** oder **endlich präsentierbar**, falls eine exakte Sequenz der Form

$$R^p \to R^q \to M \to 0$$

existiert. Eine solche exakte Sequenz heißt **endliche Darstellung** oder **endliche Präsentation** von M.

3.13.2. Äquivalent ist die Bedingung, dass es einen Epimorphismus $R^q \twoheadrightarrow M$ gibt, dessen Kern endlich erzeugt ist.

3.13.3. Jeder Modul von endlicher Darstellung ist endlich erzeugt.

3.13.4. Sei M ein endlich erzeugter R-Modul. Seien $m_1, \dots, m_q$ Erzeuger von M. Sie definieren einen Epimorphismus $\pi \colon R^q \twoheadrightarrow M$ per $\pi(e_i) = m_i$. Wir interpretieren die Elemente von

$$\ker(\pi) = \{(r_1, \dots, r_q) \mid r_1 m_1 + \dots + r_q m_q = 0\}$$

als **Relationen** (auch **Syzygien** genannt) zwischen den $m_1, \dots, m_q$ und nennen $\ker(\pi)$ den **Modul der Relationen** zwischen den $m_1, \dots, m_q$.

Ein Modul ist also von endlicher Darstellung genau dann, wenn es ein endliches Tupel von Erzeugern gibt, deren Modul der Relationen endlich erzeugt ist.

Satz 3.13.5. *(Unabhängigkeit von der Darstellung) Sei M ein R-Modul von endlicher Darstellung und*

$$0 \to K \to L \to M \to 0$$

eine kurze exakte Sequenz. Ist L endlich erzeugt, so ist auch K endlich erzeugt.

Bemerkung 3.13.6. Ist M von endlicher Darstellung, so zeigt Satz 3.13.5, dass der Modul der Relationen für jedes endliche Tupel von Erzeugern von M endlich erzeugt ist.

Ein Modul ist also von endlicher Darstellung genau dann, wenn er endlich erzeugt ist und für jedes endliche Tupel von Erzeugern der Modul der Relationen endlich erzeugt ist.

Beweis. Sei $R^p \to Q := R^q \xrightarrow{\rho} M \to 0$ eine endliche Darstellung von M. Sei $U := \ker(\rho)$ und sei $\sigma \colon U \hookrightarrow Q$ die Inklusion. Nach Voraussetzung ist U (als Bild von $R^p \to R^q$) endlich erzeugt. Wir konstruieren die gepunkteten Morphismen α und β im kommutativen Diagramm

$$\begin{tikzcd}
 & U \arrow[r, "\sigma"] \arrow[d, dotted, "\exists! \beta"'] & Q \arrow[d, dotted, "\exists \alpha"'] \arrow[dr, "\rho"] & & \\
0 \arrow[r] & K \arrow[r, "\kappa"] & L \arrow[r, "\lambda"] & M \arrow[r] & 0
\end{tikzcd}$$

wie folgt. Da λ surjektiv ist und Q projektiv, liftet ρ zu einem Morphismus α mit $\lambda\alpha = \rho$. Wegen $\lambda\alpha\sigma = \rho\sigma = 0$ faktorisiert $\alpha\sigma$ als $\kappa\beta$ für ein eindeutiges β.

Seien $l_1, \dots, l_s$ Erzeuger von L. Weil ρ surjektiv ist, gibt es Elemente $q_1, \dots, q_s \in Q$ mit $\rho(q_i) = \lambda(l_i)$. Wegen $\lambda(l_i - \alpha(q_i)) = \lambda(l_i) - \lambda(\alpha(q_i)) = \lambda(l_i) - \rho(q_i) = 0$ gibt es eindeutige $k_i \in K$ mit $\kappa(k_i) = l_i - \alpha(q_i)$.

Wir behaupten, dass die $k_1, \dots, k_s$ zusammen mit $\beta(U)$ ganz K erzeugen. Dies impliziert die Behauptung, denn U ist endlich erzeugt.

Sei $k \in K$. Schreibe $\kappa(k) = \sum r_i l_i$ für geeignete $r_i \in R$. Betrachte das Element $\sum r_i q_i \in Q$. Wegen

$$\rho(\sum r_i q_i) = \sum r_i \rho(q_i) = \sum r_i \lambda(l_i) = \lambda(\kappa(k)) = 0$$

gibt es (genau) ein $u \in U$ mit $\sigma(u) = \sum r_i q_i$. Es folgt

$$\kappa(\beta(u) + \sum r_i k_i) = \alpha(\sigma(u)) + \sum r_i \kappa(k_i) = \alpha(\sum r_i q_i) + \sum r_i (l_i - \alpha(q_i)) = \sum r_i l_i = \kappa(k).$$

Da κ injektiv ist, folgt $k = \beta(u) + \sum r_i k_i$. $\square$

Beispiel 3.13.7. Sei k ein Körper, $R = k[X_1, X_2, \dots]$ und $\mathfrak{m} = (X_1, X_2, \dots)$. Aufgabe 3.5.7 zeigt, dass der endlich erzeugte R-Modul $M := R/(X_1, X_2, \dots)$ nicht von endlicher Darstellung ist: Nimmt man $\overline{1}$ als Erzeuger, so ist der Modul der Relationen gerade $\mathfrak{m}$, was nicht endlich erzeugt ist. Also ist M nicht von endlicher Darstellung nach Bemerkung 3.13.6.

4. Noethersche Moduln und Ringe

4.1. Noethersche Moduln.

Definition 4.1.1. Ein R-Modul heißt **noethersch**, falls jeder Untermodul endlich erzeugt ist.

4.1.2. Insbesondere ist jeder noethersche Modul endlich erzeugt.

Beispiel 4.1.3. Sei k ein Körper und $R = k[X_1, X_2, \dots]$. Dann ist der R-Modul $M = R$ nicht noethersch, da sein Untermodul $\mathfrak{m} = (X_1, X_2, \dots)$ nicht endlich erzeugt ist (siehe Aufgabe 3.5.7).

Proposition 4.1.4. *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Folge von R-Moduln. Dann ist M noethersch genau dann, wenn M' und M'' noethersch sind.*

4.1.5. Die Eigenschaft, noethersch zu sein, verträgt sich also bestens mit kurzen exakten Sequenzen (was natürlich an der geschickten Definition liegt). Man vergleiche dies mit Lemma 3.11.28 und 3.11.29.

Beweis. Wir können annehmen, dass M' ein Untermodul von M ist und dass $M'' = M/M''$ (da die Eigenschaft von R-Moduln, noethersch zu sein, unter Isomorphismen von R-Moduln invariant ist).

Sei M noethersch. Ist U' ein Untermodul von M', so ist U' auch ein Untermodul von M und damit endlich erzeugt. Also ist M' noethersch. Ist U'' ein Untermodul von M'', so ist sein Urbild U in M ein Untermodul von M und nach Annahme endlich erzeugt. Weil $U \twoheadrightarrow U''$ surjektiv ist, ist auch U'' endlich erzeugt. Also ist M'' noethersch.

Seien M' und M'' noethersch. Sei U ein Untermodul von M. Dann ist $0 \to M' \cap U \to U \to U/(M' \cap U) \to 0$ eine kurze exakte Sequenz, und $U/(M' \cap U)$ ist isomorph zu dem Untermodul $(U + M')/M'$ von M/M' (nach dem Ersten Isomorphiesatz 3.2.12.(a)). Nach Annahme sind also $M' \cap U$ und $U/(M' \cap U)$ endlich erzeugt, und U ist endlich erzeugt nach Lemma 3.11.28. Also ist M noethersch. $\square$

Korollar 4.1.6. *Endliche direkte Summen von noetherschen Moduln sind noethersch. Summanden noetherscher Moduln sind noethersch.*

Beweis. Verwende kurze exakte Sequenzen der Form $0 \to M \to M \oplus N \to N \to 0$ und Proposition 4.1.4. $\square$

Beispiel 4.1.7. Seien M_1 und M_2 Untermoduln eines R-Moduls M. Dann sind M_1 und M_2 noethersch genau dann, wenn $M_1 \cap M_2$ und $M_1 + M_2$ noethersch sind: Offensichtlich ist

$$0 \to M_1 \cap M_2 \xrightarrow{i = \begin{pmatrix} 1 \\ -1 \end{pmatrix}} M_1 \oplus M_2 \xrightarrow{p = \begin{pmatrix} 1 & 1 \end{pmatrix}} M_1 + M_2 \to 0$$

eine kurze exakte Sequenz. Explizit ist p gegeben durch $p(m_1, m_2) = m_1 + m_2$ und i durch $i(m) = (m, -m)$. Nun wende man Proposition 4.1.4 (und Korollar 4.1.6) an.

Proposition 4.1.8. *Sei M ein R-Modul. Dann sind die beiden folgenden Bedingungen äquivalent.*

(a) M ist noethersch.
(b) (Aufsteigende-Ketten-Bedingung) Jede durch die natürlichen Zahlen indizierte aufsteigende Kette $U_0 \subset U_1 \subset U_2 \subset \dots$ von Untermoduln von M wird stationär, d. h. es gibt ein $n \in \mathbb{N}$ mit $U_n = U_{n+1} = \dots$.
(c) Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element.

Beweis. (a) $\Rightarrow$ (b): Sei $U_0 \subset U_1 \subset \dots$ eine aufsteigende Folge von Untermoduln von M. Dann ist $\bigcup_{n\in\mathbb{N}} U_n$ offensichtlich ein Untermodul von M und nach Annahme von endlich vielen Elementen $m_1, \dots, m_s$ erzeugt. Es gibt ein $N \in \mathbb{N}$ mit $m_1, \dots, m_s \in U_N$. Es folgt $\bigcup U_n = \sum Rm_i \subset U_N$ und somit $U_N = U_{N+1} = \dots$.

(b) $\Rightarrow$ (c): Sonst gibt es eine nichtleere Menge $\mathcal{T}$ von Untermoduln von M ohne maximales Element. Sei $U_0 \in \mathcal{T}$. Da U_0 nicht maximal in $\mathcal{T}$ ist, gibt es einen Untermodul U_1 mit $U_0 \subsetneq U_1$. Da U_1 nicht maximal in $\mathcal{T}$ ist können wir diesen Prozess iterieren, und wir erhalten eine echt aufsteigende Folge $U_0 \subsetneq U_1 \subsetneq U_2 \subsetneq \dots$ von Untermoduln von M, die also nicht stationär wird.

(c) $\Rightarrow$ (a): Betrachte die Menge $\mathcal{T}$ aller endlich erzeugten Untermoduln von U. Sie ist nichtleer, da sie den Nullmodul enthält. Da jeder Untermodul von U auch ein Untermodul von M ist und M noethersch ist, gibt es ein maximales Element $T \in \mathcal{T}$. Sei $u \in U$. Dann ist $T + Ru$ endlich erzeugter Untermodul von U und somit ein Element von $\mathcal{T}$. Wegen $T \subset T + Ru$ und Maximalität von T folgt $T = T + Ru \ni u$. Also gilt $T = U$ und U ist endlich erzeugt. □

4.2. **Noethersche Ringe.**

Definition 4.2.1. Ein Ring R heißt **noethersch**, wenn R als R-Modul noethersch ist, wenn also jedes Ideal von R endlich erzeugt ist.

Beispiele 4.2.2. (a) Körper sind noethersch.
(b) Hauptidealringe sind noethersch (z. B. $\mathbb{Z}$ oder $k[X]$ für einen Körper k).

Beispiel 4.2.3. Ist k ein Körper so ist $R = k[X_1, X_2, \dots]$ kein noetherscher Ring. Das Ideal $\mathfrak{m} = (X_1, X_2, \dots)$ ist nämlich nicht endlich erzeugt (siehe Aufgabe 3.5.7).

Bemerkung 4.2.4. Ein Satz von Cohen (den wir hier ohne Probleme beweisen könnten) besagt, dass ein Ring genau dann noethersch ist, wenn alle Primideale endlich erzeugt sind.

Proposition 4.2.5. *Quotienten noetherscher Ringe sind noethersch.*

Beweis. Sei R ein noetherscher Ring und $\mathfrak{a}$ ein Ideal in R. Dann ist $R/\mathfrak{a}$ ein noetherscher R-Modul nach Proposition 4.1.4. Die R-Untermoduln von $R/\mathfrak{a}$ sind aber genau die $R/\mathfrak{a}$-Untermoduln (oder Ideale) von $R/\mathfrak{a}$ (vgl. Lemma 3.2.14), und endliche Erzeugtheit über R und $R/\mathfrak{a}$ ist gleichbedeutend. Somit ist $R/\mathfrak{a}$ ein noetherscher Ring. □

Proposition 4.2.6. *Sei R ein noetherscher Ring. Dann sind für einen R-Modul die M folgenden Bedingungen äquivalent:*
(a) M ist endlich erzeugt;
(b) M ist noethersch;
(c) M ist von endlicher Darstellung.

Insbesondere sind also Untermoduln endlicher erzeugter Moduln über einem noetherschen Ring endlich erzeugt.

Beweis. Ist M noethersch oder von endlicher Darstellung, so ist M offensichtlich endlich erzeugt.

Sei M endlich erzeugt. Dann gibt es einen Epimorphismus $p\colon R^n \twoheadrightarrow M$ für geeignetes $n \in \mathbb{N}$. Nach Korollar 4.1.6 ist R^n ein noetherscher R-Modul. Proposition 4.1.4 zeigt nun einerseits, dass M noethersch ist. Andererseits zeigt sie, dass der Modul der Syzygien $\ker(p)$ noethersch und damit endlich erzeugt ist. Somit ist M von endlicher Darstellung. □

Korollar 4.2.7. *In Vorlesung weg(ge)lassen(?), da es eh aus Hilberts Basissatz folgt. Sei $\varphi\colon A \to B$ ein Ringmorphismus (zum Beispiel die Inklusion $A \subset B$ eines Unterrings). Ist A ein noetherscher Ring und B endlich erzeugt als A-Modul (wobei die Skalarmultiplikation von A auf B durch $a.b = \varphi(a)b$ gegeben ist, für $a \in A$ und $b \in B$), so ist B ein noetherscher Ring.*

Beispiel 4.2.8. Mit $\mathbb{Z}$ ist auch $\mathbb{Z}[i]$ noethersch.

4.2.9. Die Aussage von Korollar 4.2.7 folgt auch aus dem Hilbertschen Basissatz 4.2.10, den wir im Anschluss beweisen, und Proposition 4.2.5, denn sind $b_1, \dots, b_n$ Erzeuger von B als A-Modul, so setzt sich $\varphi\colon A \to B$ zu einem surjektiven Morphismus $A[X_1, \dots, X_n] \to B$, $X_i \mapsto b_i$, von Ringen fort, und somit ist B als Quotient eines noetherschen Ringes noethersch.

Beweis. Da B ein endlich erzeugter Modul über dem noetherschen Ring A ist, ist B als A-Modul noethersch (nach Proposition 4.2.6). Also erfüllt der A-Modul B die Aufsteigende-Ketten-Bedingung nach Proposition 4.1.8. Jede aufsteigende Kette von B-Untermoduln von B ist auch eine aufsteigende Kette von A-Untermoduln von B, und wird somit stationär. Proposition 4.1.8 zeigt nun, dass der B-Modul B noethersch ist. □

Satz 4.2.10 (Hilbertscher Basissatz (veraltete Terminologie), Hilbert (1888), [Hil90])**.** *Ist R ein noetherscher Ring, so ist auch $R[X]$ noethersch.*

4.2.11. Hilbert beweist in [Hil90], dass Polynomringe $k[X_1, \dots, X_n]$ über einem Körper noethersch sind, dass also jedes[8] Ideal endlich erzeugt ist. Diese Eigenschaft wurde zur definierenden Eigenschaft eines noetherscher Rings (benannt nach Emmy Noether).

Beweis. Sei $I \subset R[X]$ ein Ideal. Zu zeigen ist, dass I endlich erzeugt ist.

Sei $\mathfrak{a}$ das von den Leitkoeffizienten der Elemente von $I - \{0\}$ erzeugte Ideal von R (die Menge der Leitkoeffizienten zusammen mit dem Nullelement bildet übrigens bereits ein Ideal). Da R noethersch ist, ist $\mathfrak{a}$ endlich erzeugt. Seien $c_1, \dots, c_n$ Erzeuger von $\mathfrak{a}$. Wir können offensichtlich annehmen, dass jedes c_i Leitkoeffizient eines Polynoms $g_i \in I - \{0\}$ ist. Es gilt also

$$g_i = c_i X^{r_i} + (\text{Terme kleinerer Ordnung})$$

für geeignete $r_i \in \mathbb{N}$. Sei $J := R[X]g_1 + \dots R[X]g_n \subset I$.

Sei $r = \max(1, r_1, \dots, r_n) \geq 1$. Wir behaupten, dass jedes Element $f \in I$ die Form $f = g + h$ mit $g \in J$ und $h \in I$ mit $\deg(h) < r$ hat (der Grad des Nullpolynoms sei $-\infty$).

Wir zeigen dies per Induktion über $\deg(f)$. Falls $\deg(f) < r$, so ist $f = 0 + f$ die gesuchte Darstellung.

Sei nun $f \in I$ mit $m := \deg(f) \geq r$. Sei $c \in R$ der Leitkoeffizient von f, also

$$f = cX^m + (\text{Terme kleinerer Ordnung}).$$

Wegen $c \in \mathfrak{a}$ gilt $c = \sum u_i c_i$ für geeignete $u_i \in R$. Das Polynom $p := \sum u_i g_i X^{m-r_i} \in J$ hat ebenfalls Grad m und Leitkoeffizient c. Somit hat das Element $f - p$ von I Grad $< m$ und kann per Induktionsannahme als $f - p = g' + h$ mit $g' \in J$ und $h \in I$ mit $\deg(h) < r$ geschrieben werden. Es folgt $f = (p + g') + h$ wie gewünscht (beachte $p + g' \in J$).

Sei $M := R \oplus RX \oplus \dots \oplus RX^{r-1}$. Dies ist ein R-Untermodul von $R[X] = \bigoplus_{i \in \mathbb{Z}} RX^i$ (dies ist eine direkte Summe von R-Untermoduln im Sinne von Definition 3.3.12), und unsere Behauptung besagt

$$I = J + I \cap M$$

(Gleichheit von R-Moduln). Da M ein endlich erzeugter Modul über dem noetherscher Ring R ist, ist sein Untermodul $I \cap M$ ebenfalls endlich erzeugt als R-Modul. Nach obiger Gleichung ist also I endlich erzeugt als $R[X]$-Modul.[9] Dies zeigt, dass $R[X]$ noethersch ist. □

Korollar 4.2.12. *Ist R ein noetherscher Ring, so ist auch $R[X_1, \dots, X_n]$ ein noetherscher Ring.*

Als Spezialfälle erhalten wir:

(a) Polynomringe $k[X_1, \dots, X_n]$ in endlich vielen Variablen über einem Körper sind noethersche Ringe.
(b) Polynomringe $\mathbb{Z}[X_1, \dots, X_n]$ in endlich vielen Variablen über den ganzen Zahlen sind noethersche Ringe.

[8] Genauer betrachtet Hilbert nur von homogenen Elementen - sogenannten Formen - erzeugte Ideale. Soweit ich sehe, kommt in seinem Artikel der Begriff „Basis“ nicht vor.

[9] Genauer gilt: Wählen wir Erzeuger $h_1, \dots, h_s$ von $I \cap M$ als R-Modul, so läßt sich jedes Element von I als Summe einer $R[X]$-Linearkombination der $g_1, \dots, g_n$ und einer R-Linearkombintation der $h_1, \dots, h_s$ schreiben.

4.2.13. Quotienten der gerade angegebenen noetherschen Polynomringe sind ebenfalls noethersch nach Proposition 4.2.5.

Beweis. Dies folgt induktiv aus Satz 4.2.10 wegen $R[X_1, X_2, X_n] = (R[X_1, \dots, X_{n-1}])[X_n]$. Die Spezialfälle gelten, da k und $\mathbb{Z}$ als Hauptidealringe noethersch sind. $\square$

4.2.14. Sei k ein Körper und $E \subset k[X_1, \dots, X_n]$ eine (möglicherweise unendliche) Teilmenge. Wir behaupten, dass die gemeinsame Nullstellenmange $\mathbf{V}(E) \subset k^n$ aller Polynome in E (siehe Definition 1.2.1) bereits durch endlich viele Elemente von E definiert ist.

Das von E erzeugte Ideal $\langle E \rangle$ in $k[X_1, \dots, X_n]$ ist nach dem Hilbertschen Basissatz 4.2.10 (bzw. seinem Korollar 4.2.12) von endlich vielen Elementen erzeugt. Indem wir diese Elemente als Linearkombinationen von Elementen von E schreiben, sehen wir, dass $\langle E \rangle$ von endlich vielen Elementen von E erzeugt ist, sagen wir von $f_1, \dots, f_n \in E$. Es folgt

$$\mathbf{V}(E) = \mathbf{V}(\langle E \rangle) = \mathbf{V}(f_1, \dots, f_n).$$

Dies zeigt die Behauptung.

Aufgabe 4.2.15. Sei R ein noetherscher Ring. Zeigen Sie, dass der Ring $R[[X]]$ der formalen Potenzreihen noethersch ist.

Hinweis: Orientieren sie sich an der Beweisidee des Hilbertschen Basissatzes. Statt des Leitkoeffizienten betrachte man den niedrigsten nicht verschwindenden Koeffizienten. Außerdem verwende man $R[[X]] \twoheadrightarrow R[[X]]/(X^r) \xrightarrow{\sim} R[X]/(X^r) \cong R \oplus RX \oplus RX^{r-1}$ für geeignetes r. Bisher nur im Zug im Kopf überlegt.

5. Das Tensorprodukt

Sei R ein Ring.

5.1. **Bilineare Abbildungen.**

Definition 5.1.1. Gegeben R-Moduln M, N und P heißt eine Abbildung

$$\mu \colon M \times N \to P$$

von Mengen R-**bilinear**, falls sie in jedem Argument R-linear ist:

(a) Für alle $m \in M$ ist die Abbildung $\mu(m, -) \colon N \to P$ R-linear.
(b) Für alle $n \in N$ ist die Abbildung $\mu(-, n) \colon M \to P$ R-linear.

Notation 5.1.2. Die Menge der R-bilinearen Abbildung wird $\operatorname{Bil}_R(M \times N, P)$ notiert.

5.1.3. Da P ein R-Modul ist, wird $\operatorname{Bil}_R(M \times N, P)$ ebenfalls ein R-Modul: Definiere $\mu_1 + \mu_2$ per $(\mu_1 + \mu_2)(m, n) := \mu_1(m, n) + \mu_2(m, n)$ und $r\mu$ per $(r\mu)(m, n) := r\mu(m, n) = \mu(rm, n) = \mu(m, rn)$.

5.1.4. Die Abbildungen

$$\begin{aligned} \operatorname{Bil}(M \times N, P) &\xrightarrow{\sim} \operatorname{Hom}_R(M, \operatorname{Hom}_R(N, P)), \\ \mu &\mapsto (m \mapsto \mu(m, -)), \\ \Big((m, n) \mapsto (f(m))(n)\Big) &\leftarrow\!\shortmid f, \end{aligned} \tag{5.1.1}$$

und

$$\begin{aligned} \operatorname{Bil}(M \times N, P) &\xrightarrow{\sim} \operatorname{Hom}_R(N, \operatorname{Hom}_R(M, P)), \\ \mu &\mapsto (n \mapsto \mu(-, n)), \\ \Big((m, n) \mapsto (g(n))(m)\Big) &\leftarrow\!\shortmid g, \end{aligned}$$

sind kanonische Bijektionen von Mengen und sogar Isomorphismen von R-Moduln (wir überlassen den offensichtlichen Beweis dem Leser).

5.2. **Tensorprodukte.**

Definition 5.2.1. Seien M und N R-Moduln. Ein **Tensorprodukt** von M und N ist ein R-Modul T zusammen mit einer R-bilinearen Abbildung $\tau\colon M \times N \to T$, so dass gilt: Für jede R-bilineare Abbildung $f\colon M \times N \to P$ gibt es genau eine R-lineare Abbildung $f'\colon T \to P$ mit $f'\tau = f$.

$$\begin{tikzcd} M \times N \arrow[r, "\tau \text{ (bilinear)}"] \arrow[dr, "\forall f \text{ (bilinear)}"'] & T \arrow[d, dotted, "\exists! f' \text{ (linear)}"] \\ & P \end{tikzcd}$$

5.2.2. Dies bedeutet äquivalent, dass für alle R-Moduln P die Abbildung

$$\begin{aligned} \operatorname{Hom}_R(T, P) &\xrightarrow{\sim} \operatorname{Bil}_R(M \times N, P), \\ f' &\mapsto f' \circ \tau, \end{aligned} \tag{5.2.1}$$

bijektiv ist.

5.2.3. Wie üblich bei durch universelle Eigenschaften definierten Objekten, sind je zwei Tensorprodukte von M und N eindeutig isomorph: Sind (T, τ) und (T', τ') Tensorprodukte von M und N, so gibt es genau einen Isomorphismus $a\colon T \to T'$ von R-Moduln mit $a\tau = \tau'$. Dies zeigt man wie Lemma 3.11.11. Wir dürfen deshalb den bestimmten Artikel verwenden und von **dem** Tensorprodukt zweier Moduln sprechen.

Proposition 5.2.4 (Existenz des Tensorprodukts)**.** *Je zwei R-Moduln besitzen ein Tensorprodukt.*

Beweis. Seien R-Moduln M und N gegeben. Betrachte den freien R-Modul $\bigoplus_{(m,n) \in M \times N} R$. Er hat die Basis $\{e_{(m,n)} \mid (m, n) \in M \times N\}$ (vgl. 3.4.2 und 3.4.5). Wir kürzen ab $[m, n] := e_{(m,n)}$. Sei U der Untermodul, der von den folgenden Elementen erzeugt wird:

$$\begin{aligned} &[m_1 + m_2, n] - [m_1, n] - [m_2, n], && \text{für alle } m_1, m_2 \in M \text{ und } n \in N, \\ &[rm, n] - r[m, n], && \text{für alle } r \in R,\ m \in M \text{ und } n \in N, \\ &[m, n_1 + n_2] - [m, n_1] - [m, n_2], && \text{für alle } m \in M \text{ und } n_1, n_2 \in N, \\ &[m, rn] - r[m, n], && \text{für alle } r \in R,\ m \in M \text{ und } n \in N. \end{aligned}$$

Betrachte den R-Modul

$$T := \frac{\bigoplus_{M \times N} R}{U} := \left(\bigoplus_{M \times N} R \right) \Big/ U$$

und die Abbildung

$$\begin{aligned} \tau\colon M \times N &\to T, \\ (m, n) &\mapsto \overline{[m, n]} = \operatorname{can}([m, n]) = [m, n] + U, \end{aligned}$$

von Mengen. Dann ist τ nach Konstruktion R-bilinear: In der Tat ist τ R-linear im ersten Argument für fixiertes zweites Argument $n \in N$:

$$\begin{aligned} \tau(m_1 + m_2, n) &= \operatorname{can}([m_1 + m_2, n]) = \operatorname{can}([m_1, n]) + \operatorname{can}([m_2, n]) = \tau(m_1, n) + \tau(m_2, n), \\ \tau(rm, n) &= \operatorname{can}([rm, n]) = \operatorname{can}(r[m, n]) = r\operatorname{can}([m, n]) = r\tau(m, n), \end{aligned}$$

Analog sieht man R-Linearität im zweiten Argument für fixiertes erstes Argument.

Sei nun $f\colon M \times N \to P$ eine beliebige R-bilineare Abbildung. Nach Lemma 3.4.3 gibt es genau eine R-lineare Abbildung

$$\hat{f}\colon \bigoplus_{M \times N} R \to P$$

mit $\hat{f}([m, n]) = f(m, n)$. Da f bilinear ist, gilt $\hat{f}(U) = 0$. Also faktorisiert $\hat{f}$ eindeutig zu einer R-linearen Abbildung $f'\colon T \to P$ mit $f' \circ \operatorname{can} = \hat{f}$. Wir erhalten

$$f'(\tau(m, n)) = f'(\operatorname{can}([m, n])) = \hat{f}([m, n]) = f(m, n)$$

und somit $f' \circ \tau = f$.

Es ist klar, dass f' eindeutig ist: Sei $f''\colon T \to P$ eine weitere R-lineare Abbildung mit $f'' \circ \tau = f$. Dann gilt

$$\hat{f}([m,n]) = f(m,n) = f''(\tau(m,n)) = f''(\mathrm{can}([m,n]))$$

für alle $m \in M$ und $n \in N$. Es folgt $\hat{f} = f'' \circ \mathrm{can}$ und damit $f' = f''$. □

Notation 5.2.5. Der im Beweis von Proposition 5.2.4 konstruierte R-Modul T wird als $M \otimes_R N$ notiert. Gegeben $(m,n) \in M \times N$ schreiben wir

$$m \otimes n := \tau(m,n).$$

5.2.6. Damit ist das Tensorprodukt von M und N der R-Modul $M \otimes_R N$ zusammen mit der R-bilinearen Abbildung

$$\otimes\colon M \times N \to M \otimes_R N.$$

5.2.7. Bilinearität von τ bedeutet, dass $(m_1+m_2)\otimes n = m_1\otimes n + m_2 \otimes n$ und $m\otimes(n_1+n_2) = m\otimes n_1 + m\otimes n_2$ und $(rm)\otimes n = r(m\otimes n) = m \otimes (rn)$ gelten.

Der Index R am Tensorprodukt in der Notation $M \otimes_R N$ erinnert daran, dass man Skalare aus R am Tensorprodukt vorbeischieben darf: Es gilt $rm \otimes n = m \otimes rn$.

5.2.8. Jedes Element von $M \otimes_R N$ läßt sich als endliche Summe von Elementen der Form $m \otimes n$ schreiben, für $(m,n) \in M \times N$ (dies folgt sofort aus dem Beweis von Proposition 5.2.4). Ein Element der Form $m \otimes n$ nennt man einen **reinen Tensor**. Die reinen Tensoren bilden also ein Erzeugendensystem von $M \otimes_R N$.

Die Abbildung $\otimes\colon M \times N \to M \otimes_R N$ ist aber im Allgemeinen keineswegs surjektiv (siehe Beispiel 5.3.5 für ein Gegenbeispiel).

Ein Morphismus $\alpha\colon M \otimes_R N \to P$ von R-Moduln wird oft nur auf den reinen Tensoren angegeben, und es wird dem Leser überlassen, die Wohldefiniertheit zu überprüfen.

5.2.9. Sind M und N endlich erzeugt, so ist $M \otimes_R N$ ebenfalls endlich erzeugt. Dies folgt sofort aus der ersten Beobachtung in 5.2.8.

Proposition 5.2.10 (Tensor-Hom-Adjunktion $((- \otimes_R N, \mathrm{Hom}_R(N,-))$)**.** *Seien M, N, P R-Moduln. Dann ist die folgende Abbildung eine kanonische Bijektion*

$$\begin{aligned} \mathrm{Hom}_R(M \otimes_R N, P) &\xrightarrow{\sim} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P)), \\ f &\mapsto \Big(m \mapsto f(m \otimes -)\Big), \\ \Big(m \otimes n \mapsto (g(m)(n))\Big) &\leftarrow\!\shortmid g \end{aligned}$$

von R-Moduln.

Beweis. Wir haben nur die Bijektionen (5.1.1) und (5.2.1) kombiniert und das Tensorprodukt $M \otimes_R N$ verwendet. □

Beispiel 5.2.11. nicht in Vorlesung Wendet man diese Bijektion für gegebene R-Moduln N und P auf $M = \mathrm{Hom}_R(N,P)$ an, so entspricht der Identitätsabbildung $\mathrm{id}_M \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P))$ auf der rechten Seite auf der linken Seite die „Auswertungsabbildung“

$$\begin{aligned} \mathrm{Hom}_R(N,P) \otimes_R N &\to P, \\ f \otimes n &\mapsto f(n). \end{aligned}$$

5.2.12. Statt R-bilinearer Abbildungen kann man auch (in offensichtlicher Weise definierte) R-multilineare Abbildungen $M_1 \times \cdots \times M_n \to P$ betrachten und ein Tensorprodukt $\tau\colon M_1 \times \cdots \times M_n \to T$ per offensichtlicher universeller Eigenschaft definieren. Die Existenz eines solchen beweist man analog wie oben.

5.3. **Tensorprodukt als Funktor.**

5.3.1. Seien $f\colon M \to M'$ und $g\colon N \to N'$ Morphismen in $\mathrm{Mod}(R)$. Betrachte das folgende Diagramm ohne den gepunkteten Pfeil.

$$\begin{tikzcd} M \times N \arrow[r, "\otimes"] \arrow[d, "f\times g"] & M \otimes_R N \arrow[d, dotted, "f\otimes g"] \\ M' \times N' \arrow[r, "\otimes"] & M' \otimes_R N'. \end{tikzcd}$$

(Die horizontalen Pfeile sind bilinear.) Da $\otimes \circ (f \times g)$ R-bilinear ist, existiert der gepunktete Morphismus in $\mathrm{Mod}(R)$ eindeutig, so dass das Diagramm kommutativ ist. Wie angedeutet, wird dieser Morphismus als $f \otimes g$ notiert. Explizit ist er (auf den reinen Tensoren) durch $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ gegeben.

Wie man leicht prüft, erhalten wir so einen Funktor[10]

$$\begin{aligned} \otimes_R\colon \mathrm{Mod}(R) \times \mathrm{Mod}(R) &\to \mathrm{Mod}(R), \\ (M, N) &\mapsto M \otimes_R N && \text{auf Objektebene,} \\ (f, g) &\mapsto f \otimes g && \text{auf Morphismenebene.} \end{aligned}$$

Fixieren wir eine R-Modul M, so erhalten wir einen Funktor

$$\begin{aligned} (M \otimes_R -)\colon \mathrm{Mod}(R) &\to \mathrm{Mod}(R), \\ N &\mapsto M \otimes_R N, \\ g &\mapsto \mathrm{id}_M \otimes g. \end{aligned}$$

Er ist offensichtlich additiv: Gegeben $f, f'\colon N \to N'$ stimmen die beiden Abbildungen $(\mathrm{id} \otimes f) + (\mathrm{id} \otimes f')$ und $\mathrm{id} \otimes (f + f')$ überein: Sie senden einen reinen Tensor $m \otimes n \in M \otimes N$ auf $m \otimes f(n) + m \otimes f'(n) = m \otimes (f(n) + f'(n)) = m \otimes ((f + f')(n))$.

Analog kann man das rechte Argument fixieren und erhält den additiven Funktor $(- \otimes_R N)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$.

Proposition 5.3.2. *Seien M, N, P R-Moduln. Dann sind die folgenden Abbildungen kanonische Isomorphismen von R-Moduln:*

$$R \otimes_R M \xrightarrow{\sim} M, \qquad r \otimes m \mapsto rm, \tag{5.3.1}$$

$$1 \otimes m \leftarrow\!\shortmid m, \tag{5.3.2}$$

$$(M \otimes_R N) \otimes_R P \xrightarrow{\sim} M \otimes_R (N \otimes_R P), \qquad (m \otimes n) \otimes p \mapsto m \otimes (n \otimes p), \tag{5.3.3}$$

$$(M \oplus P) \otimes_R N \xrightarrow{\sim} (M \otimes_R N) \oplus (P \otimes_R N), \qquad (m, p) \otimes n \mapsto ((m \otimes n), (p \otimes n)), \tag{5.3.4}$$

$$(m, 0) \otimes n_1 + (0, p) \otimes n_2 \leftarrow\!\shortmid (m \otimes n_1, p \otimes n_2) \tag{5.3.5}$$

$$M \otimes_R N \xrightarrow{\sim} N \otimes_R M, \qquad m \otimes n \xrightarrow{\sim} n \otimes m. \tag{5.3.6}$$

Das Tensorprodukt vertauscht allgemeiner mit beliebigen direkten Summen: Ist $(M_i)_{i \in I}$ eine Familie von R-Moduln, so ist die folgende Abbildung ein Isomorphismus von R-Moduln:

$$\begin{aligned} (\bigoplus_{i \in I} M_i) \otimes_R N &\xrightarrow{\sim} \bigoplus_{i \in I} (M_i \otimes_R N), \\ (m_i)_{i \in I} \otimes n &\mapsto (m_i \otimes n)_{i \in I}. \\ \sum_{i \in I} \iota_i(m_i) \otimes n_i &\leftarrow\!\shortmid (m_i \otimes n_i)_{i \in I}. \end{aligned} \tag{5.3.7}$$

Beweis. In Vorlesung wenig im Detail beweisen!

(5.3.1) Diese Abbildung kommt von der R-bilinearen Abbildung $R \times M \to M$, $(r, m) \mapsto m$, und ist deswegen wohldefiniert. Ihre Inverse ist offenbar durch $m \mapsto 1 \otimes m$ gegeben.

[10] Die Kategorie $\mathrm{Mod}(R) \times \mathrm{Mod}(R)$ ist ein Spezialfall der folgenden Konstruktion: Das Produkt $\mathcal{C} \times \mathcal{D}$ zweier Kategorien $\mathcal{C}$ und $\mathcal{D}$ ist wie folgt definiert: Seine Objekte sind Paare (C, D) von Objekten $C \in \mathcal{C}$ und $D \in \mathcal{D}$, seine Morphismenmengen sind per $\mathcal{C} \times \mathcal{D}((C, D), (C', D')) := \mathcal{C}(C, C') \times \mathcal{D}(D, D')$ definiert, und Verknüpfung ist komponentenweise Verknüpfung.

(5.3.3) Für fixiertes $p \in P$ ist die Abbildung $\alpha_p \colon M \times N \to M \otimes_R (N \otimes_R P)$, $(m, n) \mapsto m \otimes (n \otimes p)$, R-bilinear; wir erhalten eine R-lineare Abbildung $\alpha'_p \colon M \otimes_R N \to M \otimes_R (N \otimes_R P)$, $m \otimes n \mapsto m \otimes (n \otimes p)$. Nun ist die Abbildung $(M \otimes_R N) \times P \to M \otimes_R (N \otimes_R P)$, $(x, p) \mapsto \alpha'_p(x)$, R-bilinear; somit erhalten wir die R-lineare Abbildung (5.3.3). Ihre Inverse wird in analoger Weise konstruiert.

(5.3.4) ist Spezialfall des unten bewiesenen Isomorphismus (5.3.7).

(5.3.6) Die Abbildung $M \times N \to N \otimes_R M$, $(m, n) \mapsto n \otimes m$, ist R-bilinear und induziert die R-lineare Abbildung (5.3.6). Sie ist eine Involution, also zu sich selbst invers.

(5.3.7) Für fixiertes $n \in N$ haben wir für jedes $j \in I$ die folgende Verknüpfung von R-linearen Abbildungen

$$\begin{aligned} \alpha_n^j \colon M_j \to M_j \otimes_R N &\xrightarrow{\iota_j} \bigoplus_{i \in I} (M_i \otimes_R N), \\ x \mapsto m \otimes n. & \end{aligned}$$

Nach der universellen Eigenschaft der direkten Summe erhalten wir eine R-lineare Abbildung

$$\beta_n := (\alpha_n^j) \colon \bigoplus_{j \in J} M_j \to \bigoplus_{i \in I} (M_i \otimes_R N).$$

Nun ist die Abbildung

$$\begin{gathered} \Big(\bigoplus_{j \in J} M_j\Big) \times N \to \bigoplus_{i \in I} (M_i \otimes_R N), \\ (x, n) \mapsto \beta_n(x), \end{gathered}$$

R-bilinear, so dass wir die Abbildung (5.3.7) erhalten.

Um die Umkehrabbildung zu konstruieren, wende man auf die Inklusionen $\iota_i \colon M_i \to \bigoplus_{j \in I} M_j$ den Funktor $(- \otimes N)$ an. Man erhält R-lineare Abbildungen

$$\iota_i \otimes \mathrm{id}_N \colon M_i \otimes_R N \to \Big(\bigoplus_{j \in I} M_j\Big) \otimes_R N,$$

die nach der universellen Eigenschaft der direkten Summe eine R-lineare Abbildung

$$(\iota_i \otimes \mathrm{id}_N) \colon \bigoplus_{i \in I} (M_i \otimes_R N) \to \Big(\bigoplus_{j \in I} M_j\Big) \otimes_R N$$

liefern. Man überprüft, dass diese Abbildung invers zu (5.3.7) ist. □

5.3.3. Das für R-trilineare Abbildungen definierte Tensorprodukt im Sinne der Bemerkung 5.2.12 ist kanonisch sowohl zu $(M \otimes_R N) \otimes_R P$ isomorph als auch zu $M \otimes_R (N \otimes_R P)$ (und diese Isomorphismen sind verträglich mit (5.3.3)). Deswegen und auch schon allein wegen der Assoziativität (5.3.3) läßt man oft die Klammern weg und schreibt $M \otimes_R N \otimes_R P$. Analog schreibt man einfach $M_1 \otimes_R \cdots \otimes_R M_n$.

5.3.4. Sind M und N freie R-Moduln, so ist auch $M \otimes_R N$ frei. Dies folgt aus Proposition 5.3.2, die uns die folgenden Isomorphismen liefert (bis auf den letzten Isomorphismus, der wegen der universellen Eigenschaft der direkten Summe offensichtlich ist):

$$\Big(\bigoplus_{i \in I} R\Big) \otimes_R \Big(\bigoplus_{j \in J} R\Big) \xrightarrow{\sim} \bigoplus_{i \in I} \Big(R \otimes_R \Big(\bigoplus_{j \in J} R\Big)\Big) \xrightarrow{\sim} \bigoplus_{i \in I} \Big(\bigoplus_{j \in J} R\Big) \xrightarrow{\sim} \bigoplus_{(i,j) \in I \times J} R.$$

Insbesondere folgt: Ist B eine Basis von M und C eine Basis von N, so ist $\{b \otimes c \mid (b, c) \in B \times C\}$ eine Basis von $M \otimes_R N$. Für Vektorräume ist diese Aussage vermutlich wohlbekannt.

Ein Spezialfall der obigen Kette von Isomorphismen ist der Isomorphismus $R^m \otimes_R R^n \xrightarrow{\sim} R^{mn}$ für $m, n \in \mathbb{N}$.

Beispiel 5.3.5. Für einen Körper k und $V = k^2$ betrachte man die Abbildung $\otimes \colon V \times V \to V \otimes_k V$. Ist e_1, e_2 die (geordnete) Standard-k-Basis von V, so ist $e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2$ nach 5.3.4 eine k-Basis von

$V \otimes V$ und liefert einen Isomorphismus $V \otimes_k V \xrightarrow{\sim} k^4$. Unter dieser Identifikation ist die bilineare Abbildung $\otimes\colon V \times V \to V \otimes_k V$ wie folgt gegeben

$$k^2 \times k^2 \to k^4,$$
$$\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) \mapsto \begin{pmatrix} x_1 y_1 \\ x_1 y_2 \\ x_2 y_1 \\ x_2 y_2 \end{pmatrix}.$$

Man rechnet leicht nach, dass das Bild dieser Abbildung genau die Nullstellenmenge $\mathbf{V}(Z_1 Z_4 - Z_2 Z_3) \subset k^4$ ist, wobei $Z_i\colon k^4 \to k$ die i-te Koordinatenfunktion ist. Insbesondere ist $\otimes\colon V \times V \to V \otimes_k V$ alles andere als surjektiv.

5.3.6. Für einen schnellen Beweis von Proposition 5.3.16 ist es sinnvoll, den Begriff eines Morphismus von Funktoren einzuführen.

Definition 5.3.7. Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Seien $F, G\colon \mathcal{C} \to \mathcal{D}$ zwei Funktoren. Ein **Morphismus von Funktoren** (oder eine **natürliche Transformation**) von F nach G, geschrieben $\alpha\colon F \to G$, ist das Datum eines Morphismus

$$\alpha_X\colon F(X) \to G(X),$$

für alle Objekte $X \in \mathcal{C}$, so dass für alle Morphismen $f\colon X \to Y$ in $\mathcal{C}$ das Diagramm

$$\begin{tikzcd} F(X) \arrow[r, "\alpha_X"] \arrow[d, "F(f)"] & G(X) \arrow[d, "G(f)"] \\ F(Y) \arrow[r, "\alpha_Y"] & G(Y) \end{tikzcd}$$

in $\mathcal{D}$ kommutativ ist, dass also $G(f) \circ \alpha_X = \alpha_Y \circ F(f)$ gilt.

In Vorlesung ad hoc definiert: Wir sagen, dass α ein Isomorphismus von Funktoren ist, falls alle Morphismen α_X Isomorphismen sind, und schreibt $\alpha\colon F \xrightarrow{\sim} G$.

5.3.8 (Verknüpfung von Morphismen von Funktoren)**.** weggelassen in Vorlesung Ist $H\colon \mathcal{C} \to \mathcal{D}$ ein weiterer Funktor und $\beta\colon G \to H$ ein Morphismen von Funktoren, so definiert

$$(\beta \circ \alpha)_C := \beta_C \circ \alpha_C$$

für $C \in \mathcal{C}$, offensichtlich einen Morphismus $\beta \circ \alpha\colon F \to H$ von Funktoren.

5.3.9. weggelassen in Vorlesung Wir erhalten die Kategorie $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ der Funktoren von $\mathcal{C}$ nach $\mathcal{D}$. Ihre Objekte sind Funktoren von $\mathcal{C} \to \mathcal{D}$, Morphismen sind Morphismen solcher Funktoren, und die Verknüpfung haben wir gerade definiert. Es ist klar, dass dieses Datum die Axiome einer Kategorie erfüllt (wenn wir mengentheoretische Probleme ignorieren). Die Identiät id_F eines Objekts F, also eines Funktors $F\colon \mathcal{C} \to \mathcal{D}$, ist gegeben durch $(\mathrm{id}_F)_C := \mathrm{id}_{F(C)}$ für $C \in \mathcal{C}$.

5.3.10. weggelassen in Vorlesung Insbesondere wissen wir damit, was ein Isomorphismus von Funktoren ist. Es ist offensichtlich, dass ein Morphismus $\alpha\colon F \to G$ von Funktoren $F, G\colon \mathcal{C} \to \mathcal{D}$ genau dann ein Isomorphismus ist, wenn alle α_C Isomorphismen sind, für $C \in \mathcal{C}$.

Beispiel 5.3.11. Wir haben implizit bereits viele Morphismen und Isomorphismen von Funktoren gesehen und teils auch verwendet. Wir geben einige Beispiele:

(a) weggelassen in Vorlesung Auswerten bei Eins ist ein Isomorphismus

$$\mathrm{ev}_1\colon \mathrm{Hom}_R(R, -) \to \mathrm{id}_{\mathrm{Mod}(R)} \tag{5.3.8}$$

von Funktoren $\mathrm{Hom}_R(R, -), \mathrm{id}_{\mathrm{Mod}(R)}\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$, der wie folgt definiert ist: Ist $M \in \mathrm{Mod}(R)$, so sei

$$(\mathrm{ev}_1)_M\colon \mathrm{Hom}_R(R, M) \to M$$

durch $f \mapsto f(1)$ definiert (dies ist sogar ein Isomorphismus ist, siehe Lemma 3.1.9). Da für jeden Morphismus $\pi\colon M \to M''$ das Diagramm (3.12.1) kommutativ ist, ist dies wirklich ein Morphismus von Funktoren.

(b) weggelassen in Vorlesung Sei N ein fixierter R-Modul. Die Auswertungsabbildungen

$$\alpha_T\colon \mathrm{Hom}_R(N,T)\otimes_R N \to T,$$

aus Beispiel 5.2.11, für $T\in \mathrm{Mod}(R)$, definieren einen Morphismus

$$\alpha\colon \mathrm{Hom}_R(N,-)\otimes_R N \to \mathrm{id}_{\mathrm{Mod}(R)}$$

von Funktoren. Hier ist die linke Seite die offensichtliche Verknüpfung der beiden Funktoren $\mathrm{Hom}_R(N,-)$ und $(-\otimes_R N)$. Deren abstrakte Definition wir nachträglich in 3.10.17 aufgeschrieben haben.

Beispiel 5.3.12. Alle Isomorphismen in Proposition 5.3.2 kommen von Isomorphismen von Funktoren. Zum Beispiel definieren die Morphismen

$$\begin{aligned} M\otimes_R N &\xrightarrow{\sim} N\otimes_R M,\\ m\otimes n &\mapsto n\otimes m, \end{aligned}$$

einen Isomorphismus

$$(?\otimes_R -)\xrightarrow{\sim}(-\otimes_R ?)$$

von Funktoren $\mathrm{Mod}(R)\times\mathrm{Mod}(R)\to\mathrm{Mod}(R)$.

Fixieren wir den R-Modul M, so erhalten wir einen Isomorphismus

$$(M\otimes_R -)\xrightarrow{\sim}(-\otimes_R M) \tag{5.3.9}$$

von Funktoren $\mathrm{Mod}(R)\to\mathrm{Mod}(R)$.

Beispiel 5.3.13. weggelassen in Vorlesung Betrachte den Isomorphismus

$$\alpha_{(M,N,T)}\colon \mathrm{Hom}_R(M\otimes_R N,T)\xrightarrow{\sim}\mathrm{Hom}_R(M,\mathrm{Hom}_R(N,T))$$

aus Proposition 5.2.10. Lassen wir die R-Moduln M,N,T variieren, so definiert dies einen Isomorphismus

$$\alpha\colon \mathrm{Hom}_R(?\otimes_R -,*)\xrightarrow{\sim}\mathrm{Hom}_R(?,\mathrm{Hom}_R(-,*))$$

von Funktoren $\mathrm{Mod}(R)^{\mathrm{op}}\times\mathrm{Mod}(R)^{\mathrm{op}}\times\mathrm{Mod}(R)\to\mathrm{Mod}(R)$. Wir überlassen den Beweis dem Leser. Im Folgenden brauchen nur eine Restriktion dieses Beispiels, die wir im nächsten Beispiel explizit erläutern.

Beispiel 5.3.14. Seien M und T fixierte R-Moduln. Wir behaupten, dass die beiden Funktoren

$$\mathrm{Hom}_R(-\otimes_R M,T),\mathrm{Hom}_R(-,\mathrm{Hom}_R(M,T))\colon \mathrm{Mod}(R)^{\mathrm{op}}\to\mathrm{Mod}(R)$$

isomorph sind. Genauer ist ein Isomorphismus

$$\alpha\colon \mathrm{Hom}_R(-\otimes_R M,T)\xrightarrow{\sim}\mathrm{Hom}_R(-,\mathrm{Hom}_R(M,T))$$

durch

$$\begin{aligned} \alpha_X\colon \mathrm{Hom}_R(X\otimes_R M,T)&\xrightarrow{\sim}\mathrm{Hom}_R(X,\mathrm{Hom}_R(M,T)),\\ f&\mapsto \Big(x\mapsto f(x\otimes -)\Big), \end{aligned}$$

wie in Proposition 5.2.10 definiert. Das folgende Diagramm ist kommutativ, wie darunter nachgerechntet, und beweist, dass α wirklich ein Morphismus von Funktoren ist. Sei $g\colon Y\to X$ ein Morphismus in $\mathrm{Mod}(R)$ (also ein Morphismus $Y\xleftarrow{g}X$ in $\mathrm{Mod}(R)^{\mathrm{op}}$)

$$\begin{tikzcd} \mathrm{Hom}_R(X\otimes_R M,T) \arrow[r, "\alpha_X"] \arrow[d, "(g\otimes\mathrm{id}_M)^*"] & \mathrm{Hom}_R(X,\mathrm{Hom}_R(M,T)) \arrow[d, "g^*"] \\ \mathrm{Hom}_R(Y\otimes_R M,T) \arrow[r, "\alpha_Y"] & \mathrm{Hom}_R(Y,\mathrm{Hom}_R(M,T)), \end{tikzcd}$$

$$\begin{tikzcd} f \arrow[r, mapsto] \arrow[d, mapsto] & \alpha_X(f)\colon x\mapsto f(x\otimes -) \arrow[d, mapsto] \\ f\circ(g\otimes\mathrm{id}_M) \arrow[r, mapsto] & \alpha_Y(f\circ(g\otimes\mathrm{id}_M))=g^*(\alpha_X(f))\colon y\mapsto f(g(y)\otimes -). \end{tikzcd}$$

Lemma 5.3.15. *Ist $\alpha\colon F \xrightarrow{\sim} G$ ein Isomorphismus von Funktoren $F, G\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$, wobei A und B Ringe sind, so ist F genau dann additiv (linksexakt, rechtsexakt, exakt), wenn G diese Eigenschaft hat.*

Beweis. Sei F additiv, d. h. $F(f+f') = F(f) + F(f')$ für alle Morphismen $f, f'\colon M \to M'$ in $\mathrm{Mod}(A)$. Es folgt (wir lassen die Indizes bei α weg)

$$(G(f)+G(f'))\circ\alpha = G(f)\circ\alpha+G(f')\circ\alpha = \alpha\circ F(f)+\alpha\circ F(f') = \alpha\circ(F(f)+F(f')) = \alpha\circ F(f+f') = G(f+f')\circ\alpha.$$

Da α ein Isomorphismus ist, folgt $G(f) + G(f') = G(f+f')$. Also ist G additiv.

Die restlichen Aussagen sind offensichtlich. □

Proposition 5.3.16 (Rechtsexaktheit des Tensorprodukts)**.** *Sei M ein R-Modul. Dann ist der Funktor*

$$(- \otimes_R M)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$$

rechtsexakt. Analog ist der (isomorphe) Funktor $(M \otimes_R -)$ rechtsexakt.

Beweis. Siehe 5.3.1 für Additivität.

Die folgenden Aussagen sind äquivalent:

(a) $(- \otimes_R M)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$ ist rechtsexakt;

(b) für alle $T \in \mathrm{Mod}(R)$ ist der Funktor

$$\mathrm{Hom}_R(- \otimes_R M, T)\colon \mathrm{Mod}(R)^{\mathrm{op}} \to \mathrm{Mod}(R)$$

linksexakt (wegen Proposition 3.11.5.(b)).

(c) für alle $T \in \mathrm{Mod}(R)$ ist der Funktor

$$\mathrm{Hom}_R(-, \mathrm{Hom}_R(M,T))\colon \mathrm{Mod}(R)^{\mathrm{op}} \to \mathrm{Mod}(R)$$

linksexakt (da dieser Funktor und der vorige isomorph sind nach Beispiel 5.3.14 und Linksexaktheit invariant unter Isomorphismen von Funktoren ist (Lemma 5.3.15)).

Die letzte Aussage ist aber richtig, da für einen beliebigen R-Modul X der Funktor $\mathrm{Hom}_R(-, X)$ linksexakt ist nach Proposition 3.11.5.(b).

Die Aussage, dass $(M \otimes_R -)$ rechtsexakt ist, folgt aus dem Isomorphismus $(M \otimes_R -) \cong (- \otimes_R M)$ von Funktoren (Isomorphismus (5.3.9) in Beispiel 5.3.12) und Lemma 5.3.15. □

Derselbe Beweis noch einmal etwas expliziter. Sei

$$N' \to N \to N'' \to 0$$

eine exakte Sequenz in $\mathrm{Mod}(R)$. Zu zeigen ist, dass

$$N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$$

exakt ist. Nach Proposition 3.11.5.(b) ist dies der Fall genau dann, wenn für einen beliebigen Testmodul T die Sequenz

$$\mathrm{Hom}_R(N' \otimes_R M, T) \leftarrow \mathrm{Hom}_R(N \otimes_R M, T) \leftarrow \mathrm{Hom}_R(N'' \otimes_R M, T) \leftarrow 0$$

exakt ist. Proposition 5.2.10 liefert die vertikalen Isomorphismen im folgenden kommutativen Diagramm.

$$\begin{tikzcd}
\mathrm{Hom}_R(N' \otimes_R M, T) \arrow[d, "\sim"] & \mathrm{Hom}_R(N \otimes_R M, T) \arrow[l] \arrow[d, "\sim"] & \mathrm{Hom}_R(N'' \otimes_R M, T) \arrow[l] \arrow[d, "\sim"] & 0 \arrow[l] \\
\mathrm{Hom}_R(N', \mathrm{Hom}_R(M,T)) & \mathrm{Hom}_R(N, \mathrm{Hom}_R(M,T)) \arrow[l] & \mathrm{Hom}_R(N'', \mathrm{Hom}_R(M,T)) \arrow[l] & 0 \arrow[l]
\end{tikzcd}$$

Die untere Folge ist aber exakt, weil $\mathrm{Hom}_R(-, \mathrm{Hom}_R(M,T))$ linksexakt ist. □

5.3.17. Ist M ein R-Modul und $N' \hookrightarrow N$ ein Monomorphismus von R-Moduln, so ist

$$M \otimes_R N' \to M \otimes_R N$$

im Allgemeinen nicht injektiv.

Beispiel 5.3.18. Tensorieren wir die Inklusion $(2\cdot)\colon \mathbb{Z} \hookrightarrow \mathbb{Z}$ von $\mathbb{Z}$-Moduln mit $\mathbb{Z}/2$, so erhalten wir die obere Zeile des folgenden Diagramms

$$\begin{tikzcd} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2 \arrow[r, "(2\cdot)\otimes \mathrm{id}"] \arrow[d, "\sim"] & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2 \arrow[d, "\sim"] \\ \mathbb{Z}/2 \arrow[r, "\overline{2}\cdot"] & \mathbb{Z}/2. \end{tikzcd}$$

Seine Vertikalen sind die Isomorphismen $r \otimes m \mapsto rm$ aus Proposition 5.3.2 und man überprüft sofort, dass das Diagramm kommutativ ist (das ist Funktorialität von $R \otimes_R M \xrightarrow{\sim} M$ in M: $R \otimes_R - \xrightarrow{\sim} -$ ist ein Isomorphismus von Funktoren). Die untere horizontale Abbildung ist die Nullabbildung und nicht injektiv.

5.3.19. nicht in Vorlesung Das Element $2 \otimes \overline{1}$ von $(2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/2$ ist nicht Null (denn unter den Isomorphismen $(2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/2 \xleftarrow[\sim]{(2\cdot)\otimes\mathrm{id}} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2 \xrightarrow{\sim} \mathbb{Z}/2$ enspricht es dem Element $\overline{1}$) während das Element $2 \otimes \overline{1}$ von $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2$ Null ist (denn $2 \otimes \overline{1} = (1 \cdot 2) \otimes \overline{1} = 1 \otimes (2\overline{1}) = 1 \otimes 0 = 0$). Deswegen ist es wichtig anzugeben, in welchem Tensorprodukt ein Element der Form $x \otimes y$ lebt.

5.3.20. nicht in Vorlesung Seien M und N endlich erzeugte R-Moduln. Wir haben in 5.2.9 beobachtet, dass dann $M \otimes_R N$ endlich erzeugt ist. Mit der Linksexaktheit des Tensorprodukts kann man dies auch wie folgt sehen. Es gibt Epimorphismen $\mu\colon R^m \twoheadrightarrow M$ und $R^n \twoheadrightarrow N$ für geeignete $m, n \in \mathbb{N}$. Weil $(- \otimes_R R^n)$ und $(M \otimes_R -)$ als rechtsexakte Funktoren Epimorphismen erhalten, erhalten wir die beiden Epimorphismen

$$R^m \otimes_R R^n \overset{\mu\otimes\mathrm{id}}{\twoheadrightarrow} M \otimes_R R^n \overset{\mathrm{id}\otimes\nu}{\twoheadrightarrow} M \otimes_R N.$$

Wegen $R^m \otimes_R R^n \cong R^{mn}$ (siehe 5.3.4) zeigt dies, dass $M \otimes_R N$ endlich erzeugt ist.

5.4. **Flache Moduln.**

Definition 5.4.1. Ein R-Modul M heißt **flach** genau dann, wenn der Funktor

$$(M \otimes_R -)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$$

exakt ist.

5.4.2. Da $(M \otimes_R -)$ stets rechtsexakt ist, ist M flach genau dann, wenn für jeden injektiven Morphismus $i\colon U \hookrightarrow N$ von R-Moduln der Morphismus $\mathrm{id} \otimes i\colon M \otimes_R U \to M \otimes_R N$ injektiv ist (siehe Aufgabe 3.11.23.(e)).

Beispiel 5.4.3. Wir haben in Beispiel 5.3.18 gesehen, dass der $\mathbb{Z}$-Modul $\mathbb{Z}/2$ nicht flach ist.

Proposition 5.4.4. *Projektive R-Moduln sind flach. Insbesondere sind freie R-Moduln flach.*

Beweis. Wir verwenden mehrfach Lemma 5.3.15.

(a) Der R-Modul R ist flach wegen des in $N \in \mathrm{Mod}(R)$ funktoriellen Isomorphismus $R \otimes_R N \xrightarrow{\sim} N$: Genauer definieren diese Abbildungen für variables $N \in \mathrm{Mod}(R)$ einen Isomorphismus von Funktoren $R \otimes \mathrm{id}_{\mathrm{Mod}(R)} \xrightarrow{\sim} \mathrm{id}_{\mathrm{Mod}(R)}$, und der Identitätsfunktor ist offensichtlich exakt.

(b) Flachheit ist invariant unter Isomorphismen von R-Moduln: Ist genauer $\varphi\colon M \xrightarrow{\sim} M'$ ein Isomorphismus von R-Moduln, so ist $(M \otimes_R -) \xrightarrow[\sim]{\varphi\otimes -} (M' \otimes_R -)$ ein Isomorphismus von Funktoren.

(c) Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln. Dann ist $\bigoplus_{i\in I} M_i$ flach genau dann, wenn alle M_i flach sind.

Zunächst sind die Funktoren $\left(\bigoplus_{i\in I} M_i\right) \otimes_R -$ und $\bigoplus_{i\in I}(M_i \otimes_R -)$ isomorph (siehe Proposition 5.3.2 und Beispiel 5.3.12). Nun verwende man die folgende Beobachtung: Sei $(\Gamma_\alpha)_{\alpha\in A}$ eine Familie von (durch ein Intervall in $\mathbb{Z}$ indizierten) Folgen. Dann ist die (in offensichtlicher Weise definierte) komponentenweise direkte Summe $\bigoplus_{\alpha\in A} \Gamma_\alpha$ unsere Folgen exakt genau dann, wenn alle Folgen Γ_α exakt sind.

Die Behauptung folgt aus diesen drei Aussagen, da jeder projektive R-Modul Summand eines freien R-Moduls ist (Proposition 3.12.7). $\square$

Beispiel 5.4.5. Alle Vektorräume über einem Körper sind frei und damit flach.

Beispiele 5.4.6. Im Allgemeinen sind flache Moduln nicht projektiv. Beispielsweise ist der $\mathbb{Z}$-Modul $\mathbb{Q}$ flach, wie wir in Korollar 6.3.16 (und explizit im Beispiel 6.3.17.(a)) sehen werden (oder wie aus Aufgabe 5.4.12 folgt, da $\mathbb{Q}$ torsionsfrei ist), aber nicht projektiv (siehe Lemma 3.12.10).

Beispiel 5.4.7. Jedes Ideal in einem Hauptidealring (etwa in $\mathbb{Z}$ oder $k[X]$, für einen Körper k), ist frei und damit flach.

Beispielsweise ist für ein beliebiges Polynom $f \in k[X]$ das Ideal (f) flach als $k[X]$-Modul.

Zusatzbemerkung 5.4.8. Man kann zeigen, dass ein R-Modul M genau dann flach ist, wenn für jedes endlich erzeugte Ideal $I \subset R$ die induzierte Abbildung $I \otimes_R M \to R \otimes_R M = M$ injektiv ist (siehe [Sta16, 00HD]).

Aufgabe 5.4.9. Sei k ein Körper und $R = k[X, Y]$. Zeigen Sie, dass das maximale Ideal $\mathfrak{m} := (X, Y) \subset R$ kein flacher R-Modul ist.

Hinweis: Die Inklusion $\mathfrak{m} \to R \to R/\mathfrak{m} \to 0$ wird unter $(- \otimes_R \mathfrak{m})$ auf $\mathfrak{m} \otimes_R \mathfrak{m} \to R \otimes_R \mathfrak{m} \xrightarrow{\sim} \mathfrak{m}$ abgebildet. Man finde ein nichttriviales Element des Kerns dieser Abbildung. Um zu zeigen, dass dieses Element nichttrivial ist, verwende man den R-Modul $\mathfrak{m}/\mathfrak{m}^2 \otimes_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$.

Aufgabe 5.4.10. In Aufgabe 5.4.9 wurde gezeigt, dass die Multiplikationsabbildung $\mu\colon \mathfrak{m} \otimes_R \mathfrak{m} \twoheadrightarrow \mathfrak{m}^2$, $a \otimes b \mapsto ab$, nicht injektiv ist. Bestimmen Sie den Kern dieser Abbildung.

Hinweise:

(a) Zeigen Sie die Existenz eines kommutativen Diagramms

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m} \arrow[r, "\begin{pmatrix} y \\ -x \end{pmatrix}"] \arrow[d, hook] & \mathfrak{m} \oplus \mathfrak{m} \arrow[r] \arrow[d, "\mathrm{id}"] & \mathfrak{m} \otimes_R \mathfrak{m} \arrow[r] \arrow[d, two heads, "\mu"] & 0 \\
0 \arrow[r] & R \arrow[r, "\begin{pmatrix} y \\ -x \end{pmatrix}"'] & \mathfrak{m} \oplus \mathfrak{m} \arrow[r, "\begin{pmatrix} x & y \end{pmatrix}"] & \mathfrak{m}^2 \arrow[r] & 0
\end{tikzcd}$$

mit kurzen exakten Sequenzen als Zeilen, der Multiplikation als rechter Vertikale und der Inklusion als linker Vertikale. (Exaktheit der unteren Zeile ist nachzurechnen, für die obere Zeile wende man $(- \otimes_R \mathfrak{m})$ auf die kurze exakte (das ist zu checken) Sequenz

$$0 \to R \xrightarrow{\begin{pmatrix} y \\ -x \end{pmatrix}} R \oplus R \xrightarrow{\begin{pmatrix} x & y \end{pmatrix}} \mathfrak{m} \to 0$$

an.

(b) Folgern Sie eine kurze exakte Sequenz

$$0 \to R/\mathfrak{m} \to \mathfrak{m} \otimes_R \mathfrak{m} \xrightarrow{\mu} \mathfrak{m}^2 \to 0.$$

Insbesondere ist der Kern von μ eindimensional als k-Vektorraum. Geben Sie ein nichttriviales Element des Kerns an.

Zusatzbemerkung 5.4.11 (Zu Aufgabe 5.4.10)*.* Wendet man auf die kurze exakte Sequenz $0 \to \mathfrak{m} \to R \to R/\mathfrak{m} \to 0$ den Funktor $- \otimes_R \mathfrak{m}$ an, so erhält man eine lange exakte Sequenz

$$0 \to \operatorname{Tor}^1_R(R/\mathfrak{m}, \mathfrak{m}) \to \mathfrak{m} \otimes_R \mathfrak{m} \to R \otimes_R \mathfrak{m} \to (R/\mathfrak{m}) \otimes_R \mathfrak{m} \to 0.$$

(Mir fällt es leichter, deriviert zu denken.) Die mittlere Abbildung ist die Multiplikationsabbildung $\mathfrak{m} \otimes_R \mathfrak{m} \to \mathfrak{m}$ und hat $\mathfrak{m}^2$ als Bild. In der obigen Aufgabe haben wir im Wesentlichen $\operatorname{Tor}^1_R(R/\mathfrak{m}, \mathfrak{m}) \cong R/\mathfrak{m}$ mit Hilfe der üblichen Koszul-Auflösung von $R/\mathfrak{m}$ ausgerechnet.

Aufgabe 5.4.12. Sei R ein Hauptidealring. Zeigen Sie (unter Verwendung von Zusatzbemerkung 5.4.8), dass ein R-Modul flach ist genau dann, wenn er torsionsfrei[11] ist.

---

[11] Ein Modul M über einem Integritätsbereich R heißt **torsionsfrei**, falls für alle $r \in R$ und $m \in M$ gilt: Aus $rm = 0$ folgt $r = 0$ oder $m = 0$.

Für eine abelsche Gruppe bedeutet dies schlicht, dass jedes Element ungleich Null unendliche Ordnung hat.

5.5. **Restriktion und Erweiterung der Skalare.**

5.5.1. Sei $\varphi\colon A \to B$ ein Morphismus von Ringen. Ist N ein B-Modul, so definiert

$$a.n := \varphi(a).n \quad \text{für } a \in A \text{ und } n \in N$$

eine A-Modulstruktur auf der abelschen Gruppe N. Wir nennen diesen A-Modul die **Restriktion** von N entlang φ und notieren ihn als $\operatorname{res}_A^B(N)$. Jeder Morphismus $f\colon N \to N'$ in $\operatorname{Mod}(B)$ ist trivialerweise auch ein Morphismus $\operatorname{res}_A^B N \to \operatorname{res}_A^B N'$ in $\operatorname{Mod}(A)$, den man in der Regel mit demselben Symbol bezeichnet. Wir erhalten den Funktor **Restriktion der Skalare (entlang φ)**

$$\operatorname{res} = \operatorname{res}_A^B\colon \operatorname{Mod}(B) \to \operatorname{Mod}(A).$$

Der Restriktionsfunktor res ist offensichtlich exakt (da man Exaktheit auf dem Niveau der unterliegenden abelschen Gruppen überprüfen kann).

5.5.2. Oft ist φ eine Inklusion von Ringen $A \subset B$. In diesem Fall ist der Name „Restriktion der Skalare“ besonders gerechtfertigt, und er ist auch im Allgemeinen dadurch motiviert.

5.5.3. Beispielsweise liefert die Inklusion $\mathbb{R} \subset \mathbb{C}$ den Restriktionsfunktor $\operatorname{Mod}(\mathbb{C}) \to \operatorname{Mod}(\mathbb{R})$ von der Kategorie der komplexen Vektorräume in die Kategorie der reellen Vektorräume.

Proposition 5.5.4 (Erweiterung der Skalare)**.** *Sei $\varphi\colon A \to B$ ein Ringmorphismus. Sei M ein A-Modul. Auf der dem A-Modul $\operatorname{res}_A^B(B) \otimes_A M$ zugrundeliegenden abelschen Gruppe gibt es genau eine B-Modulstruktur, deren Skalarmultiplikation*

$$b.(b' \otimes m) := (bb') \otimes m$$

für alle $b, b' \in B$ und $m \in M$ erfüllt. Man notiert den so erhaltenen B-Modul als $B \otimes_A M$.

Beweis. Die Eindeutigkeit der B-Modulstruktur ist klar, da die reinen Tensoren $\operatorname{res}_B^A(B) \otimes_A M$ erzeugen.

Für $b \in B$ ist $(b\cdot)\colon B \to B$ ein Endomorphismus von B-Moduln und liefert per Restriktion der Skalare einen Endomorphismus $(b\cdot)\colon \operatorname{res}_A^B(B) \to \operatorname{res}_A^B(B)$ von A-Moduln. Wenden wir den Funktor $(- \otimes_R M)$ darauf an, erhalten wir einen Endomorphismus $(b\cdot) \otimes \mathrm{id}_M\colon \operatorname{res}(B) \otimes_A M \to \operatorname{res}(B) \otimes_A M$. Man prüft nun sofort, dass

$$b.x := ((b\cdot) \otimes \mathrm{id}_M)(x) \quad \text{für } b \in B \text{ und } x \in \operatorname{res}_A^B(B) \otimes_A M$$

eine B-Modulstruktur auf $\operatorname{res}_A^B(B) \otimes_A M$ definiert[12] und

$$b.(b' \otimes m) = ((b\cdot) \otimes \mathrm{id}_M)(b' \otimes m) = bb' \otimes m$$

erfüllt. □

5.5.5. Ist $f\colon M \to M'$ ein Morphismus in $\operatorname{Mod}(A)$, so ist die Abbildung $\mathrm{id}_{\operatorname{res}_A^B(B)} \otimes f\colon \operatorname{res}_A^B(B) \otimes_A M \to \operatorname{res}_A^B(B) \otimes_A M'$ ein Morphismus

$$\mathrm{id} \otimes f = \mathrm{id}_B \otimes f\colon B \otimes_A M \to B \otimes_A M'$$

von B-Moduln und wird wie angegeben notiert. Diese Konstruktionen definieren den rechtsexakten Funktor **Erweiterung der Skalare (entlang φ)**

$$(B \otimes_A -)\colon \operatorname{Mod}(A) \to \operatorname{Mod}(B).$$

Rechtsexaktheit folgt aus Proposition 5.3.16, da man Exaktheit auf den unterliegenden abelschen Gruppen testen kann.

5.5.6. Die Identität auf den zugrundeliegenden abelschen Gruppen liefert die Identifikation $\operatorname{res}_A^B(B \otimes_A M) \xrightarrow{\sim} \operatorname{res}_A^B(B) \otimes_A M$ als A-Moduln. Diese Morphismen definieren einen Isomorphismus $\operatorname{res}_A^B(B \otimes_A -) \xrightarrow{\sim} \operatorname{res}_A^B(B) \otimes_A -$ von Funktoren $\operatorname{Mod}(A) \to \operatorname{Mod}(A)$.

5.5.7. Erweiterung der Skalare $\operatorname{Mod}(\mathbb{R}) \to \operatorname{Mod}(\mathbb{C})$ entlang der Inklusion $\mathbb{R} \subset \mathbb{C}$ wird oft als **Komplexifizierung** eines reellen Vektorraums bezeichnet.

[12] Etwas abstrakter ist die B-Modulstruktur also durch die folgende Verknüpfung definiert:

$$B \xrightarrow{b \mapsto (b\cdot)} \operatorname{End}_B(B) \xrightarrow{\operatorname{res}} \operatorname{End}_B(\operatorname{res}(B)) \xrightarrow{- \otimes_A M} \operatorname{End}_A(\operatorname{res}(B) \otimes_A M) \xrightarrow{\operatorname{res}} \operatorname{End}_{\mathbb{Z}}(\operatorname{res}(B) \otimes_A M).$$

Proposition 5.5.8 (Adjungiertheit von Erweiterung und Restriktion der Skalare)**.** *Sei $\varphi\colon A \to B$ ein Morphismus von Ringen. Für $M \in \mathrm{Mod}(A)$ und $N \in \mathrm{Mod}(B)$ gibt es einen kanonischen Isomorphismus*

$$\begin{aligned} \mathrm{Hom}_B(B \otimes_A M, N) &\xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{res}_A^B N), \\ f &\mapsto \hat{f} := \big(m \mapsto f(1 \otimes m)\big), \\ \tilde{g} := \big((b \otimes m \mapsto bg(m)\big) &\mapsfrom g, \end{aligned}$$

von Mengen (sogar von A-Moduln, wenn man die linke Seite per Restriktion als A-Modul auffasst).

Beweis. Wir zeigen, dass für gegebenes f die Abbildung $\hat{f}$ A-linear ist. Additivität ist offensichtlich, und es gilt

$$\hat{f}(am) = f(1 \otimes am) = f(\varphi(a)1 \otimes m) = f(\varphi(a).(1 \otimes m)) = \varphi(a)f(1 \otimes m) = \varphi(a)\hat{f}(m) = a.\hat{f}(m).$$

Sei nun g gegeben. Die Abbildung

$$\begin{aligned} \mathrm{res}(B) \times M &\to \mathrm{res}(N), \\ (b, m) &\mapsto bg(m), \end{aligned}$$

von Mengen ist A-bilinear (Biadditivität ist klar) wegen

$$(a.b)g(m) = (\varphi(a)b)g(m) = \varphi(a)(bg(m)) = a.(bg(m))$$

und

$$bg(am) = b(a.g(m)) = b(\varphi(a)g(m)) = b\varphi(a)g(m) = \varphi(a)bg(m) = a.(bg(m)),$$

so dass wir die induzierte A-lineare Abbildung $\mathrm{res}(B) \otimes_A M \to \mathrm{res}(N)$ erhalten. Diese ist offenbar auch B-linear, und somit ist $\tilde{g}$ wohldefiniert.

Es ist leicht zu sehen, dass die beiden Abbildungen invers zueinander sind. □

5.5.9. Es folgt, dass der Morphismus $M \to \mathrm{res}(B \otimes_A M) = B \otimes_A M$, $m \mapsto 1 \otimes m$ von A-Moduln die aus dem folgenden Diagramm ersichtliche universelle Eigenschaft hat.

$$\begin{tikzcd} M \arrow[r] \arrow[dr, "\forall f\ (A\text{-linear})"'] & B \otimes_A M \arrow[d, dotted, "\exists! f'\ (B\text{-linear})"] \\ & N \end{tikzcd}$$

Proposition 5.5.10 (Erweiterung der Skalare kommutiert mit Tensorprodukt)**.** *Sei $\varphi\colon A \to B$ ein Ringmorphismus und seien M und N A-Moduln. Dann ist die Abbildung*

$$\begin{aligned} (B \otimes_A M) \otimes_B (B \otimes_A N) &\xrightarrow{\sim} B \otimes_A (M \otimes_A N), \\ (b \otimes m) \otimes (b' \otimes n) &\mapsto bb' \otimes (m \otimes n), \end{aligned}$$

ein Isomorphismus von B-Moduln (mit Umkehrabbildung gegeben durch $b \otimes (m \otimes n) \mapsto (b \otimes m) \otimes (1 \otimes n) = (1 \otimes m) \otimes (b \otimes n)$).

Beweis. Der einfachste Beweis besteht wohl darin, die Wohldefiniertheit der angegebenen Abbildung durch explizite Konstruktion zu zeigen, und dann ebenso die Umkehrabbildung zu konstruieren.

Wir geben einen abstrakteren Beweis.

Ist X ein B-Modul, so erhalten wir die schwarzen Bijektionen

$$\begin{aligned} \mathrm{Hom}_B(B \otimes_A (M \otimes_A N), X) &\xrightarrow{\sim} \mathrm{Hom}_A(M \otimes_A N, \mathrm{res}(X)) && \xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, \mathrm{res}(X))) \\ &\xrightarrow{\sim} \mathrm{Bil}_A(M \times N, \mathrm{res}(X)) && \xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{res}(\mathrm{Hom}_B(B \otimes_A N, X))) \\ &\xrightarrow{\sim} \mathrm{Bil}_B((B \otimes_A M) \times (B \otimes_A N), X) && \xrightarrow{\sim} \mathrm{Hom}_B(B \otimes_A M, \mathrm{Hom}_B(B \otimes_A N, X)) \\ &\xrightarrow{\sim} \mathrm{Hom}_B((B \otimes_A M) \otimes_B (B \otimes_A N), X) \end{aligned}$$

wobei der erste Isomorphismus Adjungiertheit von Erweiterung und Restriktion der Skalare ist, der dritte Isomorphismus die analoge Aussage für bilineare Abbildungen ausdrückt (die man durch die blauen Isomorphismen beweisen kann), und der zweite und vierte Isomorphismus aus der Definition des Tensorprodukts herrühren. Wer mag, kann auch die beiden Mengen der bilinearen Abbildungen vermeiden und die blauen Isomorphismen verwenden (diese verwenden die Tensor-Hom-Adjunktion).

Setzt man $X = B \otimes_A (M \otimes_A N)$, so entspricht id_X unter den obigen Isomorphismen einem Morphismus $(B \otimes_A M) \otimes_B (B \otimes_A N) \to B \otimes_A (M \otimes_A N)$, der, wie man leicht prüft, die angegebene Beschreibung hat.

Setzt man $X = (B \otimes_A M) \otimes_B (B \otimes_A N)$ so definiert das Urbild von id_X unter diesen Isomorphismen einen Morphismus $B \otimes_A (M \otimes_A N) \to (B \otimes_A M) \otimes_B (B \otimes_A N)$ von B-Moduln, der explizit durch $b \otimes (m \otimes n) \mapsto (b \otimes m) \otimes (1 \otimes n)$ gegeben ist.

Es ist offensichtlich, dass die beiden konstruierten Morphismen invers zueinander sind. □

5.5.11. Restriktion der Skalare kommutiert nicht mit dem Tensorprodukt. Zum Beispiel sind im Allgemeinen $\mathrm{res}(B \otimes_B B) \cong \mathrm{res}(B)$ und $\mathrm{res}(B) \otimes_A \mathrm{res}(B)$ nicht isomorph, etwa für $A = \mathbb{C} \subset B = \mathbb{C}[X]$.

Aufgabe 5.5.12 (Transitivität der Skalarerweiterung)**.** Seien Ringmorphismen $A \to B \to C$ gegeben. Zeigen Sie einen Isomorphismus von Funktoren $(C \otimes_B (B \otimes_A -)) \xrightarrow{\sim} (C \otimes_A -)\colon \mathrm{Mod}(A) \to \mathrm{Mod}(C)$.

Proposition 5.5.13. *Sei $\varphi\colon A \to B$ ein Morphismus von Ringen. Ist M ein flacher A-Modul, so ist $B \otimes_A M$ ein flacher B-Modul. Mit anderen Worten erhält Erweiterung der Skalare*

$$B \otimes_A -\colon \mathrm{Mod}(A) \to \mathrm{Mod}(B)$$

also Flachheit.

5.5.14 (Vorbemerkung zum Beweis von Proposition 5.5.13)**.** Ist X ein beliebiger B-Modul und M ein A-Modul, so kann man die abelsche Gruppe $\mathrm{res}(X) \otimes_A M$ mit genau einer B-Modulstruktur versehen, so dass $b.(x \otimes m) = (bx) \otimes m$ gilt. Wir notieren diesen B-Modul als $X \otimes_A M$.

Dies zeigt man genau analog zum Beweis von Proposition 5.5.4.

Beweis. Ist X ein beliebiger B-Modul, so behaupten wir, dass

$$\begin{aligned} X \otimes_A M &\to X \otimes_B (B \otimes_A M), \\ x \otimes m &\mapsto x \otimes (1 \otimes m), \end{aligned} \tag{5.5.1}$$

ein (wohldefinierter) Isomorphismus von B-Moduln ist.

Die Abbildung $\mathrm{res}(X) \times M \to \mathrm{res}(X \otimes_B (B \otimes_A M))$, $(x, m) \mapsto x \otimes (1 \otimes m)$ ist A-bilinear wegen

$$a.x \otimes (1 \otimes m) = \varphi(a)x \otimes (1 \otimes m) = x \otimes \varphi(a).(1 \otimes m) = x \otimes (\varphi(a) \otimes m) = x \otimes (a.1 \otimes m) = x \otimes (1 \otimes am)$$

und liefert eine Abbildung $\mathrm{res}(X) \otimes_A M \to \mathrm{res}(X \otimes_B (B \otimes_A M))$ von A-Moduln, die offenbar B-linear ist und so die gesuchte Abbildung (5.5.1) liefert.

Umgekehrt zeigt man, dass

$$\begin{aligned} X \otimes_B (B \otimes_A M) &\xrightarrow{\sim} X \otimes_A M, \\ x \otimes (b \otimes m) &\mapsto bx \otimes m, \end{aligned}$$

eine wohldefinierte Abbildung von B-Moduln ist (zur Konstruktion dieser Abbildung gehe man wie im Beweis des Isomorphismus (5.3.3) in Proposition 5.3.2 vor). Es ist offensichtlich, dass diese Abbildung invers zu (5.5.1) ist.

Für variables $X \in \mathrm{Mod}(B)$ definieren die Isomorphismen (5.5.1) einen Isomorphismus

$$(- \otimes_A M) \xrightarrow{\sim} (- \otimes_B (B \otimes_A M)) \tag{5.5.2}$$

von Funktoren $\mathrm{Mod}(B) \to \mathrm{Mod}(B)$. Ist M ein flacher A-Modul, so ist der linke Funktor offensichtlich[13] exakt (da man Exaktheit auf den unterliegenden abelschen Gruppen prüfen kann). $\square$

Aufgabe 5.5.15. Sei $\varphi\colon A \to B$ ein Ringmorphismus. Seien $N, X \in \mathrm{Mod}(B)$ und $M \in \mathrm{Mod}(A)$.

(a) Zeigen Sie, dass

$$\begin{gathered} N \otimes_B (X \otimes_A M) \xrightarrow{\sim} (N \otimes_B X) \otimes_A M, \\ n \otimes (x \otimes m) \mapsto (n \otimes x) \otimes m, \end{gathered} \tag{5.5.3}$$

ein wohldefinierter Isomorphismus von B-Moduln ist.

(b) Der Isomorphismus (5.5.3) ist funktoriell in $N \in \mathrm{Mod}(B)$ und definiert einen Isomorphismus

$$- \otimes_B (X \otimes_A M) \xrightarrow{\sim} (- \otimes_B X) \otimes_A M$$

von Funktoren $\mathrm{Mod}(B) \to \mathrm{Mod}(B)$.

(c) Folgern Sie den Isomorphismus (5.5.2).

Aufgabe 5.5.16. Erweiterung der Skalare kommutiert mit direkten Summen: $B \otimes_A \bigoplus M_i \xrightarrow{\sim} \bigoplus (B \otimes_A M_i)$.

Hinweis: Proposition 5.3.2.

Aufgabe 5.5.17. Erweiterung der Skalare erhält die folgenden Eigenschaften von Moduln: frei, projektiv, endlich erzeugt, von endlicher Darstellung.

Restriktion der Skalare erhält im Allgemeinen keine dieser Eigenschaften.

Lösung auskommentiert (endlich erzeugt, von endlicher Darstellung), frei und projektiv aufzuschreiben.

Aufgabe 5.5.18. Sei R ein Ring und $\mathfrak{a}$ ein Ideal. Ist M ein R-Modul, so $R/\mathfrak{a} \otimes_R M \xrightarrow{\sim} M/\mathfrak{a}M$ per $\overline{r} \otimes m \mapsto \overline{rm}$. Genauer sind die beiden Funktoren $R/\mathfrak{a} \otimes -$ und $M \mapsto M/\mathfrak{a}M$ von $\mathrm{Mod}(A)$ nach $\mathrm{Mod}(R/\mathfrak{a})$ isomorph.

5.6. **Tensorprodukt von Ringen.**

Proposition 5.6.1 (Tensorprodukt von Ringen und universelle Eigenschaft)**.** *Seien R, A, B Ringe und $\alpha\colon R \to A$ und $\beta\colon R \to B$ Ringmorphismen.*

(a) Auf der dem R-Modul $\mathrm{res}(A) \otimes_R \mathrm{res}(B)$ zugrundeliegenden abelschen Gruppe gibt es genau einen Ringstruktur, deren Multiplikation

$$(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$$

*für alle $a, a' \in A$ und $b, b' \in B$ erfüllt. Wir bezeichnen diesen Ring mit $A \otimes_R B$ und nennen ihn das **Tensorprodukt** der Ringe A und B über R. Die Abbildungen*

$$\begin{aligned} \iota_A\colon A &\to A \otimes_R B, & \qquad \iota_B\colon B &\to A \otimes_R B, \\ a &\mapsto a \otimes 1, & b &\mapsto 1 \otimes b, \end{aligned}$$

sind Ringmorphismen und machen das Diagramm

$$\begin{tikzcd} R \arrow[r, "\beta"] \arrow[d, "\alpha"'] & B \arrow[d, "\iota_B"'] \\ A \arrow[r, "\iota_A"] & A \otimes_R B \end{tikzcd}$$

[13] Genauer kommutiert nach Definition der B-Modulstruktur auf $X \otimes_A M$, für $X \in \mathrm{Mod}(B)$, das Diagramm

$$\begin{tikzcd} \mathrm{Mod}(B) \arrow[r, "- \otimes_A M"] \arrow[d, "\mathrm{res}"] & \mathrm{Mod}(B) \arrow[d, "\mathrm{res}"] \\ \mathrm{Mod}(A) \arrow[r, "- \otimes_A M"] & \mathrm{Mod}(A) \end{tikzcd}$$

von Funktoren. Da M ein flacher A-Modul ist, ist der untere horizontale Funktor exakt. Da der Restriktionsfunktor exakt ist, sind die beiden übereinstimmenden Verknüpfungen von links oben nach rechts unten exakt. Da eine Folge von B-Moduln exakt ist genau dann, wenn ihr Bild unter dem Restriktionsfunktor exakt ist („Restriktion reflektiert Exaktheit“), ist somit der obere horizontale Funktor exakt.

kommutativ.

(b) *(Pushout in der Kategorie der kommutativen Ringe) Gegeben beliebige Ringmorphismen $\lambda\colon A \to T$ und $\mu\colon B \to T$ mit $\lambda\alpha = \mu\beta$ existiert genau ein Ringmorphismus $\rho\colon A \otimes_R B \to T$, so dass das Diagramm*

$$\begin{tikzcd}
R \arrow[r, "\beta"] \arrow[d, "\alpha"'] & B \arrow[d, "\iota_B"'] \arrow[ddr, bend left, "\mu"] & \\
A \arrow[r, "\iota_A"] \arrow[drr, bend right, "\lambda"'] & A \otimes_R B \arrow[dr, "\rho"] & \\
& & T
\end{tikzcd}$$

kommutiert. Explizit gilt $\rho(a \otimes b) = \lambda(a)\mu(b)$.

5.6.2. Ist man ganz genau, so schreibt man $A \otimes_{\alpha,R,\beta} B$ statt $A \otimes_R B$.

5.6.3. Seien A und B Ringe. Dann gibt es eindeutige Ringmorphismen $\mathbb{Z} \to A$ und $\mathbb{Z} \to B$ (siehe 2.2.2.(a)). Insbesonder erhalten wir den Ring $A \otimes_{\mathbb{Z}} B$.

5.6.4. In der algebraischen Geometrie entspricht diese Konstruktion dem sogenannten Faserprodukt. Man stelle sich etwa vor, dass $R = \mathbb{C}$ und $B = \mathbb{C}[X]$ und $A = \mathbb{C}[Y, Z]$ gelten. Dann sind B die polynomialen komplexwertigen Funktionen auf $\mathbb{C}$, A sind die polynomialen komplexwertigen Funktionen auf $\mathbb{C}^2$, und $A \otimes_R B$ sind die polynomialen komplexwertigen Funktionen auf dem Produkt $\mathbb{C} \times \mathbb{C}^2 = \mathbb{C}^3$. In Aufgabe 5.6.5 werden wir in der Tat sehen, dass in diesem Fall $A \otimes_R B = \mathbb{C}[X, Y, Z]$ gilt. Geometrisch entspricht dem obigen Diagramm das Diagramm

$$\begin{tikzcd}
\mathrm{pt} & \mathbb{C} \arrow[l] \\
\mathbb{C}^2 \arrow[u] & \mathbb{C}^3 \arrow[l, "\text{Projektion auf } y{,}z\text{-Ebene}"] \arrow[u, "\text{Projektion auf } x\text{-Achse}"']
\end{tikzcd}$$

wobei pt ein einpunktiger Raum ist. Die Abbildungen auf dem Level von Ringen entsprechen dem Zurückholen von Funktionen.

Beweis. (a) Wir kürzen $A \otimes_R B := \operatorname{res}(A) \otimes_R \operatorname{res}(B)$ ab. Für $(a, b) \in A \times B$ ist die Abbildung

$$\begin{aligned}\mu_{(a,b)}\colon A \times B &\to A \otimes_R B,\\ (a', b') &\mapsto aa' \otimes bb',\end{aligned}$$

R-bilinear und liefert somit eine R-lineare Abbildung

$$\mu'_{(a,b)}\colon A \otimes_R B \to A \otimes_R B$$

Die Abbildung

$$\begin{aligned}A \times B &\to \operatorname{Hom}_R(A \otimes_R B, A \otimes_R B),\\ (a, b) &\mapsto \mu'_{(a,b)},\end{aligned}$$

ist ebenfalls R-bilinear und induziert somit eine R-lineare Abbildung

$$A \otimes_R B \to \operatorname{Hom}_R(A \otimes_R B, A \otimes_R B).$$

Nach Proposition 5.2.10 entspricht diese einer R-linearen Abbildung

$$(A \otimes_R B) \otimes_R (A \otimes_R B) \to A \otimes_R B.$$

Die Verknüpfung

$$(A \otimes_R B) \times (A \otimes_R B) \to (A \otimes_R B) \otimes_R (A \otimes_R B) \to A \otimes_R B.$$

ist somit R-bilinear und insbesondere $\mathbb{Z}$-bilinear. Sie ist nach Konstruktion durch

$$(a \otimes b, a' \otimes b) \mapsto aa' \otimes bb'$$

gegeben. Es ist leicht zu sehen, dass dies eine Ringstruktur auf $A \otimes_R B$ definiert. Die Eindeutigkeitsaussage ist offensichtlich.

Es ist offensichtlich, dass ι_A und ι_B Ringmorphismen sind. Für $r \in R$ gilt $\alpha(r) \otimes 1 = r.1 \otimes 1 = 1 \otimes r.1 = 1 \otimes \beta(r)$ in $A \otimes_R B$. Daraus folgt die Kommutativität $\iota_A \alpha = \iota_B \beta$ im angegebenen Diagramm.

(b) Die Abbildung

$$\begin{aligned} A \times B &\to T, \\ (a, b) &\mapsto \lambda(a)\mu(b), \end{aligned}$$

ist R-linear und liefert deswegen einen Morphismus $\rho\colon A \otimes_R B \to T$ von R-Moduln. Man rechnet sofort nach, dass dieser ein Ringmorphismus ist und die gewünschten Eigenschaften hat. Eindeutigkeit von ρ ist klar, weil jedes Element von $A \otimes_R B$ eine endliche Linearkombination von reinen Tensoren

(5.6.1) $$a \otimes b = (a \otimes 1)(1 \otimes b) = \iota_A(a)\iota_B(b)$$

ist und $\iota_A(a)$ bzw. $\iota_B(b)$ unter dem Ringmorphismus ρ auf $\lambda(a)$ bzw. $\mu(b)$ abgebildet werden müssen. ☐

Aufgabe 5.6.5. (a) Finden Sie einen Isomorphismus von Ringen $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathbb{C} \times \mathbb{C}$.
(b) Sei $k = \mathbb{F}_2(t)$ der Körper der rationalen Funktionen und $K = k(\sqrt{t})$. (Somit ist $k \subset K$ eine rein inseparable Körpererweiterung.) Finden Sie einen Isomorphismus von Ringen $K \otimes_k K \xrightarrow{\sim} K[X]/(X^2)$.
(c) Sei $\varphi\colon A \to B$ ein Morphismus von Ringen. Zeigen Sie $B \otimes_A A[X_1, \dots, X_n] \xrightarrow{\sim} B[X_1, \dots, X_n]$.
(d) Für $\varphi\colon A \to B$ und $\mathfrak{a} \subset A$ ein Ideal gilt $B \otimes_A A/\mathfrak{a} \xrightarrow{\sim} B/\langle \varphi(\mathfrak{a}) \rangle$.
(e) $R[X] \otimes_R R[Y] \xrightarrow{\sim} R[X, Y]$ und analog in mehreren Variablen.

6. Lokalisierung

6.1. Lokalisierung von Ringen.
Sei A ein Ring.

Definition 6.1.1. Eine Teilmenge $S \subset A$ heißt **multiplikativ abgeschlossen**, falls $1 \in S$ gilt und für alle $s, t \in S$ auch $st \in S$ gilt.

Beispiele 6.1.2. (a) Sei $f \in A$. Dann ist die Menge $\{f^n \mid n \in \mathbb{N}\} = \{1, f, f^2, \dots\}$ multiplikativ abgeschlossen.
(b) Ist $\mathfrak{p} \subset A$ ein Primideal, so ist $A - \mathfrak{p}$ multiplikativ abgeschlossen.
(c) Ist $\mathfrak{a} \subset A$ ein Ideal, so ist $1 + \mathfrak{a}$ multiplikativ abgeschlossen.

Definition 6.1.3. Eine **Lokalisierung** eines Ringes A an einer multiplikativ abgeschlossenen Teilmenge $S \subset A$ ist ein Paar (L, λ) bestehend aus einem Ring L und einem Ringmorphismus $\lambda\colon A \to L$, so dass gelten:
(a) Alle Elemente von S werden invertierbar in L, d. h. $\lambda(S) \subset L^\times$.
(b) Ist $\rho\colon A \to R$ ein beliebiger Ringmorphismus mit $\rho(S) \subset R^\times$, so gibt es genau einen Ringmorphismus $\rho'\colon L \to R$ mit $\rho' \circ \lambda = \rho$:

$$\begin{tikzcd} A \arrow[r, "\lambda"] \arrow[dr, "\forall\rho"', "\rho(S)\subset R^\times"'] & L \arrow[d, "\exists!\rho'"] \\ & R \end{tikzcd}$$

Wenn klar ist, welches λ gemeint ist, sagt man oft kurz, dass L eine Lokalsierung von A an S ist.

6.1.4. Wir könnten alternativ auch Lokalisierungen an beliebigen Teilmengen $S' \subset A$ betrachten. Sei S die kleinste multiplikativ abeschlossene Teilmenge von A, die S' enthält, also die Menge aller endlichen Produkte von Elementen von S' (es gilt $1 \in S$, da das Produkt über die leere Menge 1 ist). Ist nun $\rho\colon A \to R$ ein Ringmorphismus, so gilt $\rho(S') \subset R^\times$ genau dann, wenn $\rho(S) \subset R^\times$. Deswegen ist die Lokalisierung von A an S' eindeutig isomorph zur Lokalisierung von A an S.

6.1.5. Eine Lokalisierung von A an S ist eindeutig bis auf eindeutigen Isomorphismus.

6.1.6. Gilt $S \subset A^\times$, so ist $\mathrm{id}_A\colon A \to A$ eine/die Lokalsierung von A an S.

Proposition 6.1.7 (Existenz der Lokalisierung eines Ringes)**.** *Lokalisierungen von Ringen an multiplikativ abgeschlossenen Teilmengen existieren.*

Beweis. Sei S eine multiplikativ abgeschlossene Teilmenge eines Ringes A.

Wir definieren eine Relation $\sim$ auf $A \times S$ durch

$$(a,s) \sim (b,t) :\Longleftrightarrow \exists u \in S : u(ta - sb) = 0. \tag{6.1.1}$$

Wir behaupten, dass diese Relation eine Äquivalenzrelation ist.

Symmetrie und Reflexivität (wegen $1 \in S$) sind offensichtlich. Wir zeigen Transitivität. Gelte $(a,s) \sim (b,t)$ und $(b,t) \sim (c,u)$. Also gibt es $x, y \in S$ mit

$$\begin{aligned} xta &= xsb, \\ yub &= ytc. \end{aligned}$$

Es folgt

$$(xyt)ua = (yu)(xta) = (yu)(xsb) = (xs)(yub) = (xs)(ytc) = (xyt)sc.$$

Wegen $xyt \in S$ gilt also $(a,s) \sim (c,u)$.

Wir notieren die Äquivalenzklasse eines Elementes $(a,s) \in A \times S$ als $\frac{a}{s}$ (oder a/s oder as^{-1}). Sei $S^{-1}A$ die Menge der Äquivalenzklassen und

$$\begin{aligned} \mathrm{can}\colon A &\to S^{-1}A, \\ a &\mapsto \frac{a}{1}, \end{aligned}$$

die kanonische Abbildung.

Wir überlassen dem Leser den Beweis, dass die folgende Addition und Multiplikation auf der Menge $S^{-1}A$ wohldefiniert ist und $S^{-1}A$ zu einem Ring macht.

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &:= \frac{ta + sb}{st}, \\ \frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st}. \end{aligned}$$

Damit ist die kanonische Abbildung $\mathrm{can}\colon A \to S^{-1}A$ ein Ringmorphismus und bildet alle Elemente von S auf Einheiten in $S^{-1}A$ ab wegen $\frac{s}{1}\frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1_{S^{-1}A}$ für $s \in S$.

Sei nun $\rho\colon A \to R$ ein Ringmorphismus mit $\rho(S) \subset R^\times$. Dann überprüft man sofort, dass

$$\begin{aligned} \rho'\colon S^{-1}A &\to R, \\ \frac{a}{s} &\mapsto \rho(s)^{-1}\rho(a), \end{aligned}$$

ein wohldefinierter Ringmorphismus ist. Er erfüllt offensichtlich $\rho' \circ \mathrm{can} = \rho$.

Sei nun $\sigma\colon S^{-1}A \to R$ ein Ringmorphismus mit $\sigma \circ \mathrm{can} = \rho$. Aus

$$\rho(s)\sigma(\frac{a}{s}) = \sigma(\frac{s}{1})\sigma(\frac{a}{s}) = \sigma(\frac{sa}{s}) = \sigma(\frac{a}{1}) = \rho(a)$$

folgt $\sigma(\frac{s}{a}) = \rho(s)^{-1}\rho(a)$ und somit $\sigma = \rho'$.

Dies zeigt, dass $\mathrm{can}\colon A \to S^{-1}A$ eine Lokalisierung von A an S ist. $\square$

Notation 6.1.8. Meist schreibt man $S^{-1}A$ für die Lokalisierung eines Ringes A an einer multiplikativ abgeschlossenen Teilmenge S.

6.1.9. Für explizite Rechnungen verwenden wir in der Regel die im obigen Beweis konstruierte Lokalisierung.[14] Notieren wir ein Element von $S^{-1}A$ als $\frac{a}{s}$, so meint dies implizit, dass $a \in A$ und $s \in S$ gelten.

6.1.10. Man darf mit Elementen von S kürzen und erweitern: Für $a \in A$, $s \in S$ und $t \in S$ gilt $\frac{a}{s} = \frac{ta}{ts}$.

6.1.11. Genau dann ist $S^{-1}A$ der Nullring, wenn $0 \in S$.

6.1.12. Ist A ein Integritätsbereich und $S \subset A$ eine multiplikativ abgeschlossene Teilmenge, die die Null nicht enthält, so gilt $\frac{a}{s} = \frac{b}{t}$ genau dann, wenn $at = bs$ gilt. Die Definition (6.1.1) der Äquivalenzrelation ist in diesem Fall also einfacher und stimmt mit der aus der Schule bekannten Gleichheit von Brüchen überein.

[14] Da eine beliebige Lokalisierung $\lambda\colon A \to L$ von A an S eindeutig isomorph zu dieser Konstruktion ist, läßt sich jedes Elemet von L als $\lambda(a)\lambda(s)^{-1}$ schreiben, und man mag dieses Element schlicht als $\frac{a}{s}$ notieren. Die Gleichheit zweier Brüche ist dann genau wie oben gegeben.

Beispiel 6.1.13. Die Lokalisierung von $\mathbb{Z}$ an der multiplikativ abgeschlossenen Teilmenge $\mathbb{Z} - \{0\}$ ist $\mathbb{Q}$.

6.1.14. Der Kern der Lokalisierungsabbildung $\mathrm{can}\colon A \to S^{-1}A$ ist

$$\ker(\mathrm{can}) = \{a \in A \mid \exists s \in S \text{ mit } sa = 0\}.$$

Ist A ein Integritätsbereich und gilt $0 \notin S$, so ist also $A \to S^{-1}A$ injektiv.

Aufgabe 6.1.15. Die Abbildung $A \to S^{-1}A$ ist genau dann injektiv, wenn kein Element von S Nullteiler in A ist. Ist dies der Fall, so ist $A \to S^{-1}A$ ist genau dann bijektiv, wenn $S \subset A^\times$ gilt.

Notation 6.1.16. Ist A ein Ring und $\mathfrak{p}$ ein Primideal, so schreibt man meist $A_\mathfrak{p}$ für die Lokalisierung von A an $A - \mathfrak{p}$, also $A_\mathfrak{p} := (A - \mathfrak{p})^{-1}A$, und nennt $A_\mathfrak{p}$ die **Lokalisierung** von A **bei** (oder **an der Stelle**) $\mathfrak{p}$.

6.1.17. Explizit ist $A_\mathfrak{p}$ die Menge aller Brüche $\frac{a}{s}$ mit $s \notin \mathfrak{p}$.

Beispiel 6.1.18. (a) $\mathbb{Z}_{(0)} = \mathbb{Q}$.
bis hier, Mittwoch 7. Dezember
(b) Ist A ein Integritätsbereich und $S = A - \{0\}$, so ist $S^{-1}A = A_{(0)} = \mathrm{Quot}(A)$ der Quotientenkörper von A.
(c) Ist $p \in \mathbb{Z}$ eine Primzahl, so ist $\mathbb{Z}_{(p)}$ die Menge aller Brüche $\frac{a}{s}$, so dass s nicht durch p teilbar ist.

6.1.19. Sind $S \subset T$ multiplikativ abgeschlossene Teilmengen von A, so bildet $A \to T^{-1}A$ alle Elemente von S auf Einheiten ab und faktorisiert somit als $A \to S^{-1}A \to T^{-1}A$.

Ist A ein Integritätsbereich mit $0 \notin T$, so sind beide Abbildungen $S^{-1}A \to T^{-1}A \to \mathrm{Quot}(A)$ injektiv (weil nach 6.1.12 in jedem dieser Ringe ein Bruch genau dann Null ist, wenn sein Zähler Null ist). In der Regel faßt man sie als Inklusionen $S^{-1}A \subset T^{-1}A \subset \mathrm{Quot}(A)$ auf. Es ist dann jedoch nicht richtig, dass ein Element $\frac{a}{b} \in \mathrm{Quot}(A)$ genau dann in $S^{-1}A$ liegt, wenn $b \in S$ gilt. Zum Beispiel liegt das Element $1 = \frac{b}{b}$ für alle $b \in A - \{0\}$ in $S^{-1}A$.

Beispiel 6.1.20. Die Abbildung $\mathbb{Z}_{(p)} \to \mathbb{Z}_{(0)} = \mathbb{Q}$ ist injektiv. Ein Element $\frac{a}{s} \in \mathbb{Q}$ liegt in ihrem Bild genau dann, wenn die maximale Potenz von p, die s teilt, auch a teilt.

Notation 6.1.21. Ist A ein Ring und $f \in A$ ein Element, so schreibt man meist A_f oder $A[f^{-1}]$ für die Lokalisierung von A an $S := \{1, f, f^2, \dots\}$ und nennt sie kurz die **Lokalisierung** von A an f.

Sind endlich viele Elemente $f_1, \dots, f_m \in A$ gegeben, so schreibt man oft $A[f_1^{-1}, \dots, f_m^{-1}]$ für die Lokalisierung von A an der multiplikativ abgeschlossenenen Menge $\{f_1^{a_1} \cdot f_m^{a_m} \mid a_1, \dots, a_m \in \mathbb{N}\}$.

6.1.22. Explizit ist A_f die Menge aller Brüche $\frac{a}{f^n}$.

Aufgabe 6.1.23. (a) $A_f \cong A[X]/(fX - 1)$.
(b) $A[f_1^{-1}, \dots, f_m^{-1}] = A[(f_1 f_2 \cdots f_m)^{-1}]$.

Aufgabe 6.1.24. Ein Ringmorphismus $\lambda\colon A \to L$ ist genau dann eine Lokalisierung an S, falls die folgenden Bedingungen gelten:

(a) $\lambda(S) \subset L^\times$;
(b) für alle $a \in A$ mit $\lambda(a) = 0$ gibt es ein $s \in S$ mit $sa = 0$;
(c) jedes Element von L ist von der Form $\lambda(a)\lambda(s)^{-1}$ für geeignete $a \in A$ und $s \in S$.

Aufgabe 6.1.25. Sei $S \subset A$ eine multiplikativ abgeschlossene Teilmenge.

(a) Ist A ein Integritätsbereich und $0 \notin S$, so ist auch $S^{-1}A$ ein Integritätsbereich.
(b) Ist A ein noetherscher Ring, so ist auch $S^{-1}A$ noethersch.
(c) Ist A ein faktorieller Ring und $0 \notin S$, so ist auch $S^{-1}A$ ein faktorieller Ring. nicht überlegt

Aufgabe 6.1.26 (Transitivität der Lokalisierung)**.** Seien $S \subset T$ multiplikativ abgeschlossene Teilmengen eines Ringes A. Seien $\sigma\colon A \to S^{-1}A$ und $\tau\colon A \to T^{-1}A$ die Lokalisierungen an S bzw. T. Dann gibt es genau einen Ringmorphismus $\lambda\colon S^{-1}A \to T^{-1}A$ mit $\tau = \lambda\sigma$. Zeigen Sie, dass λ eine Lokalisierung an $\sigma(T)$ ist.

Aufgabe 6.1.27. Sei $\varphi\colon A \to B$ ein Ringmorphismus und $\mathfrak{q} \in \operatorname{Spec} B$. Sei $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) \in \operatorname{Spec} A$, d. h. $\mathfrak{p}$ ist das Bild von $\mathfrak{q}$ unter $\operatorname{Spec}\varphi = \varphi^{-1}\colon \operatorname{Spec} B \to \operatorname{Spec} A$. Dann gibt es ein kommutatives Diagramm

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d] & B \arrow[d] \\ A_{\mathfrak{p}} \arrow[r] & B_{\mathfrak{q}} \end{tikzcd}$$

mit offensichtlichen Abbildungen.

6.2. Beziehung zwischen den Idealen von A und $S^{-1}A$.

Notation 6.2.1. Ist $\mathfrak{a} \subset A$ ein Ideal, so schreiben wir $S^{-1}\mathfrak{a}$ für das von $\operatorname{can}(\mathfrak{a}) \subset S^{-1}A$ erzeugte Ideal.

Aufgabe 6.2.2. Genau dann gilt $S^{-1}\mathfrak{a} \subsetneq S^{-1}A$, wenn $S \cap \mathfrak{a} = \emptyset$.

Proposition 6.2.3. *(a) Ist $\mathfrak{a} \subset A$ ein Ideal, so liegt ein Element $\frac{x}{s} \in S^{-1}A$ genau dann in $S^{-1}\mathfrak{a}$, wenn es ein $t \in S$ gibt mit $tx \in \mathfrak{a}$. Es gilt*

(6.2.1) $$\mathfrak{a} \subset \operatorname{can}^{-1}(S^{-1}\mathfrak{a}) = \{x \in A \mid \textit{es gibt ein } t \in S \textit{ mit } tx \in \mathfrak{a}\}.$$

Die Inklusion ist eine Gleichheit genau dann, wenn kein Element $t \in S$ Nullteiler in $A/\mathfrak{a}$ ist. In diesem Fall liegt ein Element $\frac{x}{s} \in S^{-1}A$ genau dann in $S^{-1}\mathfrak{a}$, wenn $x \in \mathfrak{a}$ gilt.

(b) Ist $\mathfrak{b} \subset S^{-1}A$ ein Ideal, so gilt

$$S^{-1}\operatorname{can}^{-1}(\mathfrak{b}) = \mathfrak{b}.$$

Insbesondere hat jedes Ideal von $S^{-1}A$ die Gestalt $S^{-1}\mathfrak{a}$ für ein Ideal $\mathfrak{a} \subset A$.

(c) Die folgenden Abbildungen definieren eine Bijektion

$$\operatorname{Spec} S^{-1}A \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \emptyset\},$$
$$\mathfrak{q} \mapsto \operatorname{can}^{-1}(\mathfrak{q}),$$
$$S^{-1}\mathfrak{p} \leftarrow\!\shortmid \mathfrak{p}.$$

Für $\mathfrak{p} \in \operatorname{Spec} A$ mit $\mathfrak{p} \cap S = \emptyset$ liegt ein Element $\frac{x}{s} \in S^{-1}A$ genau dann in $S^{-1}\mathfrak{p}$, wenn $x \in \mathfrak{p}$ gilt.

(d) Für Ideale $\mathfrak{a}, \mathfrak{b} \subset A$ gilt $S^{-1}(\mathfrak{a}\mathfrak{b}) = S^{-1}(\mathfrak{a})S^{-1}\mathfrak{b}$ und $S^{-1}(\sqrt{\mathfrak{a}}) = \sqrt{S^{-1}\mathfrak{a}}$.
Insbesondere gilt $S^{-1}\operatorname{Nil}(A) = \operatorname{Nil}(S^{-1}A)$.
(Ebenso gelten $S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}$ (auch beliebige direkte Summen) und $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$; dies zeigen wir allgemeiner in Korollar 6.3.11.)

Beweis. (a): Jedes Element von $S^{-1}\mathfrak{a}$ kann als $\frac{a}{s}$ mit $a \in \mathfrak{a}$ und $s \in S$ geschrieben werden, denn die Elemente dieser Form bilden offenbar das kleinste Ideal in $S^{-1}A$, das $\operatorname{can}(\mathfrak{a})$ enthält.

Sei $\frac{x}{s} \in S^{-1}A$. Gilt $\frac{x}{s} \in S^{-1}\mathfrak{a}$, so gibt es $a \in \mathfrak{a}$ und $v \in S$ mit $\frac{x}{s} = \frac{a}{v}$, also existiert ein $u \in S$ mit $uvx = usa \in \mathfrak{a}$, und es gilt $uv \in S$. Gibt es umgekehrt ein $t \in S$ mit $tx \in \mathfrak{a}$, so gilt $\frac{x}{s} = \frac{tx}{ts} \in S^{-1}\mathfrak{a}$.

Die Inklusion und Gleichheit in (6.2.1) sind nun offensichtlich.

Gleichheit $\mathfrak{a} = \operatorname{can}^{-1}(S^{-1}\mathfrak{a})$ ist äquivalent zu der Aussage, dass für alle $x \in A$ und $t \in S$ mit $tx \in \mathfrak{a}$ bereits $x \in \mathfrak{a}$ gilt. Dies ist äquivalent zu der Aussage, dass für alle $t \in S$ und alle $\overline{x} \in A/\mathfrak{a}$ mit $t\overline{x} = 0$ bereits $\overline{x} = 0$ gilt. Dies bedeutet, dass kein Element von T Nullteiler in $A/\mathfrak{a}$ ist.

Die letzte Behauptung ist nun klar.

(b): $\subset$: Jedes Element von $S^{-1}\operatorname{can}^{-1}(\mathfrak{b})$ kann als $\frac{a}{s}$ geschrieben werden mit $a \in \operatorname{can}^{-1}(\mathfrak{b})$ und $s \in S$. Es folgt $\frac{a}{s} = \frac{1}{s}\frac{a}{1} \in \mathfrak{b}$.

$\supset$: Sei $\frac{x}{s} \in \mathfrak{b}$. Dann gilt $\frac{x}{1} = \frac{s}{1}\frac{x}{s} \in \mathfrak{b}$ und somit $x \in \operatorname{can}^{-1}(\mathfrak{b})$. Es folgt $\frac{x}{s} \in S^{-1}\operatorname{can}^{-1}(\mathfrak{b})$.

(c): Aus (b) folgt insbesondere $S^{-1}\operatorname{can}^{-1}(\mathfrak{q}) = \mathfrak{q}$ für $\mathfrak{q} \in \operatorname{Spec} S^{-1}A$.

Für $\mathfrak{p} \in \operatorname{Spec} A$ ist $A/\mathfrak{p}$ ein Integritätsbereich. Gelte $\mathfrak{p} \cap S = \emptyset$. Dann ist für jedes Element $s \in S$ das Element $\overline{s} \in A/\mathfrak{p}$ ungleich Null und damit kein Nullteiler. Nun zeigt (a) einerseits, dass $\mathfrak{p} = \operatorname{can}^{-1}(S^{-1}\mathfrak{p})$ gilt, und andererseits, dass $S^{-1}\mathfrak{p}$ ein Primideal ist: Aus $\frac{x}{s}\frac{y}{t} = \frac{xy}{st} \in S^{-1}\mathfrak{p}$ folgt sofort $xy \in \mathfrak{p}$, also $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$ und somit $\frac{x}{s} \in S^{-1}\mathfrak{p}$ oder $\frac{y}{t} \in S^{-1}\mathfrak{p}$.

(d): Die erste Gleichheit ist offensichtlich. Wir zeigen die zweite Gleichheit.

$\subset$: Jedes Element von $S^{-1}\sqrt{\mathfrak{a}}$ kann als $\frac{a}{s}$ mit $a \in \sqrt{\mathfrak{a}}$ und $s \in S$ geschrieben werden. Sei $n \in \mathbb{N}$ mit $a^n \in \mathfrak{a}$. Dann gilt $(\frac{a}{s})^n = \frac{a^n}{s^n} \in S^{-1}\mathfrak{a}$ und somit $\frac{a}{s} \in \sqrt{S^{-1}\mathfrak{a}}$.

$\supset$: Sei $\frac{x}{s} \in \sqrt{S^{-1}\mathfrak{a}}$. Dann gibt es ein $n \in \mathbb{N}_{>0}$ mit $\frac{x^n}{s^n} \in S^{-1}\mathfrak{a}$. Also gibt es $a \in \mathfrak{a}$ und $t \in S$ mit $\frac{x^n}{s^n} = \frac{a}{t}$. Also existiert ein $u \in S$ mit $utx^n = us^n a \in \mathfrak{a}$. Es folgt $(utx)^n \in \mathfrak{a}$, also $utx \in \sqrt{\mathfrak{a}}$, und es gilt $\frac{x}{s} = \frac{utx}{uts} \in S^{-1}\sqrt{\mathfrak{a}}$. □

Notation 6.2.4. Sei $\mathfrak{p} \in \operatorname{Spec} A$. Ist $\mathfrak{a} \subset A$ ein Ideal, so schreiben wir $\mathfrak{a}_\mathfrak{p} := S^{-1}\mathfrak{a}$, wobei $S := A - \mathfrak{p}$. Oft wird dieses Ideal auch als $\mathfrak{a}A_\mathfrak{p}$ notiert.

Korollar 6.2.5 (Lokalisierungen an Primidealen sind lokale Ringe)**.** *Sei $\mathfrak{p} \in \operatorname{Spec} A$. Dann ist die Abbildung*

$$\operatorname{can}^{-1}\colon \operatorname{Spec} A_\mathfrak{p} \xrightarrow{\sim} \{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{q} \subset \mathfrak{p}\}$$

bijektiv und verträglich mit Inklusionen.

Insbesondere ist $A_\mathfrak{p}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{p}_\mathfrak{p}$. Sein Restklassenkörper $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ wird auch als ***Restklassenkörper von*** *$\mathfrak{p}$ bezeichnet. (Er ist kanonisch isomorph zu $\operatorname{Quot}(A/\mathfrak{p})$, siehe Proposition 6.2.8.(b).)*

Ist $\mathfrak{q} \in \operatorname{Spec} A$ mit $\mathfrak{q} \subset \mathfrak{p}$ gegeben, so liegt ein Element $\frac{x}{s} \in S^{-1}A$ genau dann in $\mathfrak{q}_\mathfrak{p}$, wenn $x \in \mathfrak{q}$ gilt.

Beweis. Alle Aussagen folgen sofort aus Proposition 6.2.3.(c). Da die Menge auf der rechten Seite der Bijektion das größte Element $\mathfrak{p}$ hat, ist $\mathfrak{p}_\mathfrak{p}$ das größte Primideal in $A_\mathfrak{p}$ und damit das eindeutige maximale Ideal von $A_\mathfrak{p}$. □

Korollar 6.2.6. *Sei $f \in A$. Dann ist die Abbildung*

$$\operatorname{can}^{-1}\colon \operatorname{Spec}(A_f) \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\} = (\operatorname{Spec} A)_f := (\operatorname{Spec} A) - \mathcal{V}(f)$$

bijektiv und verträglich mit Inklusionen (siehe Aufgabe 2.12.5 für die Notation $(\operatorname{Spec} A)_f$).

Beweis. Man verwende Proposition 6.2.3.(c). Es gilt $\mathfrak{p} \cap \{1, f, f^2, \dots\} \neq \emptyset$ genau dann, wenn $f \in \mathfrak{p}$ gilt, wenn also $\mathfrak{p} \in \mathcal{V}(f)$ gilt. □

Notation 6.2.7. Sei $f \in A$. Ist $\mathfrak{a} \subset A$ ein Ideal, so schreiben wir $\mathfrak{a}_f := S^{-1}\mathfrak{a}$, wobei $S := \{1, f, f^2, \dots\}$.

Proposition 6.2.8 (Lokalisierung kommutiert mit Quotientenringen)**.** *Sei $\mathfrak{a}$ ein Ideal eines Ringes A. Sei S eine multiplikativ abgeschlossene Teilmenge von A und $\overline{S}$ ihr Bild in $A/\mathfrak{a}$. Dann ist*

$$\begin{aligned} S^{-1}A/S^{-1}\mathfrak{a} &\xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{a}), \\ \overline{\left(\frac{a}{s}\right)} &\mapsto \frac{\overline{a}}{\overline{s}}, \end{aligned}$$

ein Isomorphismus von Ringen.

Insbesondere erhalten wir die folgenden Isomorphismen von Ringen:

(a) $A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} \xrightarrow{\sim} (A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}}$ *für $\mathfrak{p} \in \mathcal{V}(\mathfrak{a}) \subset \operatorname{Spec} A$. (Isomorphismus von Integritätsbereichen.)*

(b) $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \xrightarrow{\sim} (A/\mathfrak{p})_{(0)} = \operatorname{Quot}(A/\mathfrak{p})$ *für $\mathfrak{p} \in \operatorname{Spec} A$. (Isomorphismus von Körpern.)*

(c) $A_\mathfrak{m}/\mathfrak{m}_\mathfrak{m} \xrightarrow{\sim} A/\mathfrak{m}$ *für $\mathfrak{m} \in \operatorname{MaxSpec} A$. (Isomorphismus von Körpern.)*

Beweis. Man konstruiert die angegebene Abbildung wie im folgenden kommutativen Diagramm angedeutet.

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & A/\mathfrak{a} \arrow[r] & \overline{S}^{-1}(A/\mathfrak{a}) \\
S^{-1}A \arrow[d] \arrow[urr, dotted, "\exists!"] & & \\
S^{-1}A/S^{-1}\mathfrak{a} \arrow[uurr, dotted, "\exists!"] & &
\end{tikzcd}$$

Ihre Umkehrabbildung konstruiert man wie im folgenden kommutativen Diagramm angedeutet.

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & A/\mathfrak{a} \arrow[r] \arrow[ddl, dotted, "\exists!"'] & \overline{S}^{-1}(A/\mathfrak{a}) \arrow[ddll, dotted, "\exists!"] \\
S^{-1}A \arrow[d] & & \\
S^{-1}A/S^{-1}\mathfrak{a} & &
\end{tikzcd}$$

Der erste Spezialfall gilt, denn in diesem Fall ist $S = A - \mathfrak{p}$ und somit $\overline{S} = A/\mathfrak{a} - \mathfrak{p}/\mathfrak{a}$. Die beiden anderen Spezialfälle sind nun offensichtlich (da $A/\mathfrak{m}$ ein Körper ist, gilt $A/\mathfrak{m} = \mathrm{Quot}(A/\mathfrak{m})$). $\square$

6.2.9. Für $\mathfrak{p} \in \mathcal{V}(\mathfrak{a})$ liefern die Ringmorphismen

$$A \to A_\mathfrak{p} \twoheadrightarrow A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$$

Abbildungen

$$\operatorname{Spec} A \leftarrow \operatorname{Spec} A_\mathfrak{p} \leftarrow \operatorname{Spec} A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}.$$

Diese sind nach den Propositionen 2.11.17 und 6.2.3.(c) injektiv und wir erhalten genauer

$$\{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}\} \xleftarrow{\sim} \operatorname{Spec} A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}.$$

Alternativ können wir die Ringmorphismen $A \twoheadrightarrow A/\mathfrak{a} \to (A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}}$ betrachten und erhalten

$$\{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}\} \xleftarrow{\sim} \operatorname{Spec}(A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}}.$$

Aufgabe 6.2.10 (Iterierte Lokalisierungen)**.**
(a) Für $\mathfrak{q} \subset \mathfrak{p}$ mit $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} A$ gilt kanonisch $(A_\mathfrak{p})_{\mathfrak{q}_\mathfrak{p}} \xrightarrow{\sim} A_\mathfrak{q}$ als Ringe.
(b) Sei $f \in A$ und $\mathfrak{p} \in \operatorname{Spec} A$ mit $f \notin \mathfrak{p}$. Dann gilt kanonisch $(A_f)_{\mathfrak{p}_f} \xrightarrow{\sim} A_\mathfrak{p}$ als Ringe.
(c) Für $f, g \in A$ und $l \in \mathbb{N}$ gilt kanonisch $(A_f)_{\frac{g}{f^l}} \xrightarrow{\sim} A_{fg}$ als Ringe.

6.3. **Lokalisierung von Moduln.** Sei S eine multiplikativ abgeschlossene Teilmenge eines Ringes A.

6.3.1. Sei M ein A-Modul. Wie im Beweis von Proposition 6.1.7 (wo wir stets die Elemente von A rechts geschrieben haben) sieht man, dass

$$(m, s) \sim (m', t) :\Longleftrightarrow \exists u \in S : u(tm - sm') = 0.$$

eine Äquivalenzrelation auf $M \times S$ definiert. Wir notieren die Äquivalenzklasse eines Elementes $(m, s) \in m \times S$ als $\frac{m}{s}$ (oder m/s). Sei $S^{-1}M$ die Menge der Äquivalenzklassen. Wir überlassen dem Leser den Beweis, dass die folgende Addition und Skalarmultiplikation auf der Menge $S^{-1}M$ wohldefiniert ist und $S^{-1}M$ zu einem $S^{-1}A$-Modul macht.

$$\frac{m}{s} + \frac{m'}{t} := \frac{tm + sm'}{st},$$
$$\frac{a}{s}.\frac{m}{t} := \frac{am}{st}.$$

Definition 6.3.2. Der gerade definierte $S^{-1}A$-Modul $S^{-1}M$ heißt die **Lokalisierung** von M an S.

6.3.3. Fassen wir A als A-Modul auf und lokalisieren, so erhalten wir den $S^{-1}A$-Modul $S^{-1}A$. Andererseits ist $S^{-1}A$ ein Ring, den wir als Modul über sich selbst auffassen können. Diese beiden Konstruktionen liefern offensichtlich denselben $S^{-1}A$-Modul.

Notation 6.3.4. Ist $\mathfrak{p} \subset A$ ein Primideal, so schreiben wir $M_\mathfrak{p}$ für die Lokalisierung von M an $(A - \mathfrak{p})$. Somit ist $M_\mathfrak{p}$ ein $A_\mathfrak{p}$-Modul. Er heißt **Lokalisierung** von M **bei** (oder **an der Stelle**) $\mathfrak{p}$.

Notation 6.3.5. Ist $f \in A$ ein Element, so schreiben wir M_f oder $M[f^{-1}]$ für die Lokalisierung von M an $\{1, f, f^2, \dots\}$ und nennen sie die **Lokalisierung** von M an f. Sie ist ein Modul über $A_f = A[f^{-1}]$.

6.3.6. Ist $\varphi\colon M \to N$ ein Morphismus von A-Moduln, so definiert

$$\begin{aligned} S^{-1}\varphi\colon S^{-1}M &\to S^{-1}N, \\ \frac{m}{s} &\mapsto \frac{f(m)}{s}, \end{aligned}$$

einen Morphismus von $S^{-1}A$-Moduln. Wir überlassen dem Leser den Nachweis, dass dies wohldefiniert ist.

6.3.7. Wir erhalten offenbar einen Funktor

$$S^{-1}(-)\colon \operatorname{Mod}(A) \to \operatorname{Mod}(S^{-1}A).$$

Er wird als **Lokalisierung(sfunktor)** oder **Lokalisierung an** S bezeichnet.

Notation 6.3.8. Ist $\varphi\colon M \to N$ ein Morphismus, so notiert $\varphi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ und $\varphi_f\colon M_f \to N_f$ die induzierten Morphismen.

Proposition 6.3.9. *Sei S eine multiplikativ abgeschlossene Teilmenge eines Ringes A. Dann ist der Lokalisierungsfunktor*

$$S^{-1}(-)\colon \operatorname{Mod}(A) \to \operatorname{Mod}(S^{-1}A)$$

exakt.

Beweis. Sei $M' \xrightarrow{f} M \xrightarrow{g} M''$ eine exakte Folge (d. h. $\operatorname{im}(f) = \ker(g)$). Es genügt zu zeigen, dass die Folge

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

exakt ist. Wegen $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = S^{-1}0 = 0$ gilt $\operatorname{im}(S^{-1}f) \subset \ker(S^{-1}g)$.

Zu zeigen bleibt $\ker(S^{-1}g) \subset \operatorname{im}(S^{-1}f)$. Sei nun $\frac{m}{s} \in \ker(S^{-1}g)$, also $\frac{g(m)}{s} = 0$ in $S^{-1}M''$. Nach Definition bedeutet dies, dass es ein $t \in S$ gibt mit $tg(m) = 0$ in M''. Wegen $g(tm) = tg(m) = 0$ liegt tm im Kern von g, also im Bild von f. Sei $m' \in M'$ mit $f(m') = tm$. Dann folgt

$$(S^{-1}f)(\frac{m'}{st}) = \frac{f(m')}{st} = \frac{tm}{st} = \frac{m}{s}.$$

Dies zeigt die Behauptung. □

Aufgabe 6.3.10. Sei M ein endlich erzeugter A-Modul. Dann gilt $S^{-1}M = 0$ genau dann, wenn es ein $s \in S$ mit $sM = 0$ gibt.

Korollar 6.3.11. *Sei $U \subset M$ ein Untermodul eines A-Moduls M. Dann kann man $S^{-1}U$ kanonisch als Untermodul von $S^{-1}M$ auffassen und erhält einen Isomorphismus*

$$\begin{aligned} S^{-1}M/S^{-1}U &\xrightarrow{\sim} S^{-1}(M/U), \\ \overline{(\frac{m}{s})} &\mapsto \frac{(\overline{m})}{s}, \end{aligned}$$

von $S^{-1}A$-Moduln. Speziell gilt $M_{\mathfrak{p}}/U_{\mathfrak{p}} \xrightarrow{\sim} (M/U)_{\mathfrak{p}}$ für $\mathfrak{p} \in \operatorname{Spec} A$.

Ist V ein weiterer Untermodul von M, so gelten[15]

$$\begin{aligned} S^{-1}(U + V) &= S^{-1}U + S^{-1}V, \\ S^{-1}(U \cap V) &= S^{-1}U \cap S^{-1}V. \end{aligned}$$

6.3.12. Ist $\mathfrak{a} \subset A$ ein Ideal, so liefert Korollar 6.3.11 den $S^{-1}A$-Untermodul $S^{-1}\mathfrak{a}$ von $S^{-1}A$. Er stimmt mit dem in 6.2.1 ad hoc definierten Ideal überein, so dass sich kein Notationskonflikt ergibt.

---

[15] Allgemeiner gilt $S^{-1}(\sum U_i) = \sum S^{-1}U_i$ für eine beliebige Familie $(U_i)_{i\in I}$ von Untermoduln. Es gilt aber im Allgemeinen nicht $S^{-1}(\cap U_i) = \cap(S^{-1}U_i)$ (man betrachte zum Beispiel die Familie $U_n = n\mathbb{Z}$ von Untermoduln von $\mathbb{Z}$ für $n \in \mathbb{N}_{>0}$ und $S = \mathbb{Z} - \{0\}$).

Beweis. Die kurze exakte Sequenz $0 \to U \to M \to M/U \to 0$ in $\mathrm{Mod}(A)$ liefert wegen der Exaktheit der Lokalisierung (Proposition 6.3.9) eine kurze exakte Sequenz

$$0 \to S^{-1}U \to S^{-1}M \to S^{-1}(M/U) \to 0$$

in $\mathrm{Mod}(S^{-1}A)$. Wir können also einerseits $S^{-1}U$ mit seinem Bild in $S^{-1}M$ identifizieren[16], andererseits erhalten wir den ersten im Korollar angegebenen Isomorphismus.

$S^{-1}(U+V) = S^{-1}U+S^{-1}V$: Jedes Element von $S^{-1}(U+V)$ kann als $\frac{u+v}{s} = \frac{u}{s}+\frac{v}{s}$ geschrieben werden für geeignete Elemente $u \in U$, $v \in V$, $s \in S$ und liegt damit in $S^{-1}U + S^{-1}V$. Jedes Elemet von $S^{-1}U + S^{-1}V$ kann als $\frac{u}{s} + \frac{v}{t} = \frac{ts+sv}{st}$ geschrieben werden für geeignete Elemente $u \in U$, $v \in V$, $s,t \in S$ und liegt damit in $S^{-1}(U+V)$.

$S^{-1}(U \cap V) = S^{-1}U \cap S^{-1}V$: Die Inklusion $\subset$ ist klar. Sei $x \in S^{-1}U \cap S^{-1}V$. Dann gilt $x = \frac{u}{s} = \frac{v}{t}$ für geeignete Elemente $u \in U$, $v \in V$, $s,t \in S$. Also gibt es ein $r \in S$ mit $rtu = rsv \in U \cap V$, und es folgt $x = \frac{u}{s} = \frac{rtu}{rts} \in S^{-1}(U \cap V)$. □

Aufgabe 6.3.13. Sind M ein A-Modul und $\mathfrak{a}$ ein Ideal von A, so gilt $S^{-1}\mathfrak{a} \cdot S^{-1}M = S^{-1}(\mathfrak{a}M)$.

Proposition 6.3.14 (Lokalisierung als Skalarerweiterung)**.** *Sei M ein A-Modul. Dann ist*

$$\begin{aligned} S^{-1}M &\xrightarrow{\sim} S^{-1}A \otimes_A M, \\ \frac{m}{s} &\mapsto \frac{1}{s} \otimes m, \end{aligned}$$

ein Isomorphismus von $S^{-1}A$-Moduln.

Genauer definieren diese Isomorphismen einen Isomorphismus $S^{-1}(-) \xrightarrow{\sim} (S^{-1}A \otimes_A -)$ von Funktoren $\mathrm{Mod}(A) \to \mathrm{Mod}(S^{-1}A)$.

Beweis. Gelte $\frac{m}{s} = \frac{m'}{t}$ in $S^{-1}M$. Dann gibt es ein $u \in S$ mit $utm = usm'$. Daraus folgt

$$\frac{1}{s} \otimes m = \frac{ut}{uts} \otimes m = \frac{1}{uts} \otimes utm = \frac{1}{uts} \otimes usm' = \frac{us}{uts} \otimes m' = \frac{1}{t} \otimes m'.$$

Also ist die angegebene Abbildung als Abbildung von Mengen wohldefiniert. Sie ist offensichtlich $S^{-1}A$-linear.

Andererseits ist die Abbildung $M \to \mathrm{res}(S^{-1}M)$, $m \mapsto \frac{m}{1}$, offensichtlich A-linear und liefert deshalb nach Proposition 5.5.8 einen eindeutigen Morphismus $S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$ von $S^{-1}A$-Moduln, der explizit durch $\frac{a}{s} \otimes m \mapsto \frac{a}{s}\frac{m}{1} = \frac{am}{s}$ gegeben ist.

Es ist klar, dass die beiden so definierten Abbildungen invers zueinander sind.

Man prüft leicht, dass die Konstruktion funktoriell in M ist. □

Bis hier am Dienstag, 13. Dezember.

6.3.15. nicht in Vorlesung erwähnen Kombiniere wir die Propositionen 6.3.14 und 5.5.8, so erhalten wir für jeden $S^{-1}A$-Modul N ein Isomorphismus

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N) \xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{res}(N)).$$

Wie in 5.5.9 angedeutet, kann man somit auch die Lokalisierung eines Moduls per universeller Eigenschaft definieren, vgl. auch Aufgabe 6.5.18.

Korollar 6.3.16. *Der A-Modul $S^{-1}A$ ist flach. (Hier wird $S^{-1}A$ per Restriktion als A-Modul aufgefasst.)*

Beweis. Dies folgt aus den Propositionen 6.3.14 und 6.3.9 und der Trivialität 5.5.6. Genauer verwenden wir die Isomorphismen $(\mathrm{res}(S^{-1}A) \otimes_A -) \cong \mathrm{res} \circ (S^{-1}A \otimes_A -) \cong \mathrm{res} \circ S^{-1}(-)$ und Exaktheit von res und $S^{-1}(-)$. □

Beispiel 6.3.17.
(a) Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist flach (wie in 5.4.6 behauptet).
(b) Ist R ein Integritätsbereich, so ist sein Quotientenkörper $\mathrm{Quot}(R)$ ein flacher R-Modul.
(c) $A_\mathfrak{p}$ ist ein flacher A-Modul, für $\mathfrak{p} \in \mathrm{Spec}\, A$.
(d) $A_f = A[f^{-1}]$ ist flacher A-Modul, für $f \in A$.

---

[16] Es ist im Allgemeinen nicht richtig, dass ein Element $\frac{m}{s} \in S^{-1}M$ genau dann in diesem Bild liegt, wenn $m \in U$ gilt. Definiert man jedoch $U' := \{x \in M \mid \exists t \in S : tx \in U\}$ (was ein Untermodul von M ist), so liegt $\frac{m}{s}$ genau dann in diesem Bild, wenn $m \in U'$ gilt.

Korollar 6.3.18 (Lokalisieren und Tensorprodukt). *Für $M, N \in \operatorname{Mod}(A)$ ist*

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_A N),$$
$$\frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{st}$$

ein Isomorphismus von $S^{-1}A$-Moduln.

Insbesondere erhalten wir einen Isomorphismus $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{\sim} (M \otimes_A N)_{\mathfrak{p}}$ von $A_{\mathfrak{p}}$-Moduln, für $\mathfrak{p} \in \operatorname{Spec} A$.

6.3.19. Dies folgt aus den Propositionen 6.3.14 und Proposition 5.5.10.

Korollar 6.3.20 (Lokalisierung vertauscht mit direkten Summen). *nicht in Vorlesung erwähnen Sei $(M_i)_{i \in I}$ eine Familie von A-Moduln. Dann ist*

$$S^{-1}\Big(\bigoplus M_i\Big) \xrightarrow{\sim} \bigoplus S^{-1}M_i,$$
$$\frac{(m_i)_{i \in I}}{s} \mapsto \Big(\frac{m_i}{s}\Big)_{i \in I},$$

ein Isomorphismus von $S^{-1}A$-Moduln.

Beweis. Klar nach Aufgabe 5.5.16 und Proposition 6.3.14. □

6.4. **Punktweise lokale Aussagen.**

Notation 6.4.1. Ist M ein A-Modul und $m \in M$ ein Element, so schreibt man das Element $\frac{m}{1} \in S^{-1}M$ manchmal schlicht als m; man sollte dann aber explizit sagen, dass man m als Element von $S^{-1}M$ auffasst.

Satz 6.4.2. *Sei M ein A-Modul und $m \in M$. Dann sind die folgenden Aussagen äquivalent:*

(a) $m = 0$ in M;
(b) $m = 0$ in $M_{\mathfrak{p}}$ für alle $\mathfrak{p} \in \operatorname{Spec} A$ (gemeint ist das Element $\frac{m}{1} \in M_{\mathfrak{p}}$);
(c) $m = 0$ in $M_{\mathfrak{m}}$ für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$.

Beweis. Die Implikationen (a) ⇒ (b) ⇒ (c) sind offensichtlich.

(c) ⇒ (a): Betrachte den **Annihilator** von m in A

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

Dies ist offensichtlich ein Ideal in A.

Ist $\operatorname{Ann}_A(m)$ ein echtes Ideal, so ist es in einem maximalen Ideal $\mathfrak{m}$ von A enthalten (Korollar 2.6.16). Aus $\frac{m}{1} = 0$ in $M_{\mathfrak{m}}$ folgt, dass es ein $s \in A - \mathfrak{m}$ gibt mit $sm = 0$ in M. Wir erhalten den Widerspruch $s \in \operatorname{Ann}_A(m) \subset \mathfrak{m}$.

Also gilt $\operatorname{Ann}_A(m) = A$ und somit $m = 1m = 0$. □

Korollar 6.4.3 (Punktweise Lokalität von Nullsein). *Sei M ein A-Modul. Dann sind äquivalent:*

(a) $M = 0$;
(b) $M_{\mathfrak{p}} = 0$ für alle $\mathfrak{p} \in \operatorname{Spec} A$;
(c) $M_{\mathfrak{m}} = 0$ für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$.

Beweis. Die Implikationen (a) ⇒ (b) ⇒ (c) sind offensichtlich, und (c) ⇒ (a) folgt direkt aus Satz 6.4.2. □

Korollar 6.4.4 (Punktweise Lokalität von Exaktheit). *Sei $M' \to M \to M''$ eine Sequenz von A-Moduln. Dann sind äquivalent:*

(a) $M' \to M \to M''$ ist exakt (bei M);
(b) für alle $\mathfrak{p} \in \operatorname{Spec} A$ ist $M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}}$ exakt;
(c) für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$ ist $M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to M''_{\mathfrak{m}}$ exakt.

Insbesondere ist ein Morphismus $f \colon M \to N$ von A-Moduln genau dann injektiv/surjektiv/bijektiv, wenn alle Morphismen $f_{\mathfrak{p}} \colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$, für $\mathfrak{p} \in \operatorname{Spec} A$ (bzw. für alle $\mathfrak{p} \in \operatorname{MaxSpec} A$), diese Eigenschaft haben.

Beweis. (a) $\Rightarrow$ (b): Folgt aus der Exaktheit der Lokalisierung (Proposition 6.3.9).

(b) $\Rightarrow$ (c): Trivial.

(c) $\Rightarrow$ (a): Sei $M' \xrightarrow{f} M \xrightarrow{g} M''$ unsere gegebene Folge.

Wir zeigen zuerst $\operatorname{im}(f) \subset \ker(g)$. Sei $x \in M'$. Dann ist zu zeigen, dass $g(f(x)) = 0$ gilt. Nach Satz 6.4.2 ist dies äquivalent zu der Aussage $0 = \frac{g(f(x))}{1} = g_{\mathfrak{m}}(f_{\mathfrak{m}}(\frac{x}{1}))$ in $M_{\mathfrak{m}}$ für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$. Dies ist aber nach Annahme wahr und zeigt die gewünschte Inklusion $\operatorname{im}(f) \subset \ker(g)$.

Nun zeigen wir Gleicheit $\operatorname{im}(f) = \ker(g)$. Kurz gesagt gilt

$$(\ker(g)/\operatorname{im}(f))_{\mathfrak{m}} \cong \ker(g)_{\mathfrak{m}}/\operatorname{im}(f)_{\mathfrak{m}} \cong \ker(g_{\mathfrak{m}})/\operatorname{im}(f_{\mathfrak{m}}) = 0.$$

Es folgt $\ker(g)/\operatorname{im}(f) = 0$ nach Korollar 6.4.3 und damit Gleichheit $\operatorname{im}(f) = \ker(g)$.

Ausführlicher betrachten wir das Diagramm

$$\begin{tikzcd}
 & 0 \arrow[d] & & \\
M' \arrow[r, "b"] & \operatorname{im}(f) \arrow[r] \arrow[d, "i"] & 0 & \\
0 \arrow[r] & \ker(g) \arrow[r, "j"] \arrow[d] & M \arrow[r, "g"] & M'' \\
 & \ker(g)/\operatorname{im}(f) \arrow[d] & & \\
 & 0 & &
\end{tikzcd}$$

in $\operatorname{Mod}(A)$ mit exakten Zeilen und exakter Spalte. Es gilt $f = jib$. Wir lokalisieren dieses Diagramm bei $\mathfrak{m} \in \operatorname{MaxSpec} A$ und erhalten das Diagramm

$$\begin{tikzcd}
 & 0 \arrow[d] & & \\
M'_{\mathfrak{m}} \arrow[r, "b_{\mathfrak{m}}"] & \operatorname{im}(f)_{\mathfrak{m}} \arrow[r] \arrow[d, "i_{\mathfrak{m}}"] & 0 & \\
0 \arrow[r] & \ker(g)_{\mathfrak{m}} \arrow[r, "j_{\mathfrak{m}}"] \arrow[d] & M_{\mathfrak{m}} \arrow[r, "g_{\mathfrak{m}}"] & M''_{\mathfrak{m}} \\
 & (\ker(g)/\operatorname{im}(f))_{\mathfrak{m}} \arrow[d] & & \\
 & 0 & &
\end{tikzcd}$$

in $\operatorname{Mod}(A_{\mathfrak{m}})$, dessen Zeilen und Spalte exakt sind wegen Exaktheit der Lokalisierung (Proposition 6.3.9). Dies bedeutet insbesondere, dass $b_{\mathfrak{m}}$ surjektiv ist, dass $i_{\mathfrak{m}}$ injektiv ist, und dass $j_{\mathfrak{m}}$ der Kern von $g_{\mathfrak{m}}$ (und insbesondere injektiv) ist. Es gilt $f_{\mathfrak{m}} = j_{\mathfrak{m}} i_{\mathfrak{m}} b_{\mathfrak{m}}$, weil Lokalisieren ein Funktor ist. Fassen wir $\operatorname{im}(f)_{\mathfrak{m}}$ und $\ker(g)_{\mathfrak{m}}$ als Untermoduln von $M_{\mathfrak{m}}$ auf, so bedeutet dies $\operatorname{im}(f)_{\mathfrak{m}} = \operatorname{im}(f_{\mathfrak{m}})$ und $\ker(g)_{\mathfrak{m}} = \ker(g_{\mathfrak{m}})$. Laut Annahme gilt $\operatorname{im}(f_{\mathfrak{m}}) = \ker(g_{\mathfrak{m}})$. Also ist $i_{\mathfrak{m}}$ ein Isomorphismus, und Exaktheit der Spalte zeigt $(\ker(g)/\operatorname{im}(f))_{\mathfrak{m}} = 0$. Nach Korollar 6.4.3 gilt also $\ker(g)/\operatorname{im}(f) = 0$ und somit Gleichheit $\operatorname{im}(f) = \ker(g)$. $\square$

Proposition 6.4.5 (Punktweise Lokalität von Flachheit)**.** *Sei M ein A-Modul. Dann sind äquivalent:*

(a) M ist flacher A-Modul;

(b) $M_{\mathfrak{p}}$ ist flacher $A_{\mathfrak{p}}$-Modul, für alle $\mathfrak{p} \in \operatorname{Spec} A$;

(c) $M_{\mathfrak{m}}$ ist flacher $A_{\mathfrak{m}}$-Modul, für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$.

Beweis. (a) $\Rightarrow$ (b): Lokalisierung ist eine Skalarerweiterung (Proposition 6.3.14) und erhält somit Flachheit (Proposition 5.5.13).

(b) $\Rightarrow$ (c): Trivial.

(c) $\Rightarrow$ (a): Sei $U \hookrightarrow N$ ein Monomorphismus in $\mathrm{Mod}(A)$. Wir müssen zeigen, dass $U \otimes_A M \to N \otimes_A M$ injektiv ist. Nach Korollar 6.4.4 reicht es zu zeigen, dass $(U \otimes_A M)_\mathfrak{m} \to (N \otimes_A M)_\mathfrak{m}$ für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$ injektiv ist. Nach Korollar 6.3.18 können wir diese Abbildung mit $U_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \to N_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m}$ identifizieren.

Diese ist aber injektiv: Die Abbildung $U_\mathfrak{m} \to N_\mathfrak{m}$ ist injektiv, da Lokalisieren exakt ist, und bleibt injektiv, wenn wir sie mit dem flachen $A_\mathfrak{m}$-Modul $M_\mathfrak{m}$ tensorieren. □

6.5. **Aussagen für endlich erzeugte Moduln.**

6.5.1. Ist M ein endlich erzeugter A-Modul, so ist $S^{-1}M$ ein endlich erzeugter $S^{-1}A$-Modul: Nach Annahme gibt es einen Epimorphismus $A^m \twoheadrightarrow M$. Lokalisieren ist exakt und liefert somit einen Epimorphismus $S^{-1}(A^m) \twoheadrightarrow S^{-1}M$, der nach Korollar 6.3.20 einem Epimorphismus $(S^{-1}A)^m \twoheadrightarrow S^{-1}M$ entspricht.

Korollar 6.5.2. *nicht in Vorlesung Sei M ein endlich erzeugter A-Modul.*

(a) *Sei $\mathfrak{p} \in \operatorname{Spec} A$. Gilt $M/\mathfrak{p}M = 0$ (oder äquivalent $(A/\mathfrak{p}) \otimes_A M = 0$), so folgt bereits $M_\mathfrak{p} = 0$*

(b) *Gilt $M/\mathfrak{m}M = 0$ (oder äquivalent $(A/\mathfrak{m}) \otimes_A M = 0$) für alle $\mathfrak{m} \in \operatorname{MaxSpec} A$, so folgt $M = 0$.*

Beweis. (a): Lokalisieren wir $M/\mathfrak{p}M = 0$ bei $\mathfrak{p}$, so erhalten wir

$$0 = (M/\mathfrak{p}M)_\mathfrak{p} \xrightarrow{\sim} M_\mathfrak{p}/(\mathfrak{p}M)_\mathfrak{p} = M_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}M_\mathfrak{p}$$

als $A_\mathfrak{p}$-Moduln (siehe Korollar 6.3.11 und Aufgabe 6.3.13 für die zweite Gleichheit). Da $M_\mathfrak{p}$ ein endlich erzeugter Modul (siehe 6.5.1) über dem lokalen Ring $A_\mathfrak{p}$ ist (Proposition 6.2.5), zeigt Nakayamas Lemma für lokale Ringe (Korollar 3.9.9), dass $M_\mathfrak{p} = 0$ gilt.

(b): Aus (a) folgt $M_\mathfrak{m} = 0$ für alle $\mathfrak{m} \in \operatorname{Spec} A$, und damit $M = 0$ nach Korollar 6.4.3. □

Definition 6.5.3. Der **Träger** (englisch: **Support**) eines A-Moduls M ist

$$\operatorname{Supp}(M) := \{\mathfrak{p} \in \operatorname{Spec} A \mid M_\mathfrak{p} \neq 0\}.$$

Definition 6.5.4. Der **Annihilator** eines A-Moduls M ist

$$\operatorname{Ann}_A(M) := \{a \in A \mid am = 0 \text{ für alle } m \in M\}.$$

Der **Annihilator** eines Elements $m \in M$ ist

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

Proposition 6.5.5. (a) *Ist $\mathfrak{a}$ ein Ideal in A, so gilt $\operatorname{Supp}(A/\mathfrak{a}) = \mathcal{V}(\mathfrak{a})$.*

(b) *Ist $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz in $\mathrm{Mod}(A)$, so gilt*

$$\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'').$$

(c) *Sind U, V Untermoduln eines A-Moduls M, so gilt $\operatorname{Supp}(U+V) = \operatorname{Supp}(U) \cup \operatorname{Supp}(V)$.*

(d) *Ist M ein endlich erzeugter A-Modul, so gilt*

$$\operatorname{Supp}(M) = \mathcal{V}(\operatorname{Ann}_A(M)).$$

Insbesondere ist der Träger eines endlich erzeugten Moduls eine abgeschlossene Teilmenge von $\operatorname{Spec} A$.

Beispiel 6.5.6. Ist p eine Primzahl, so ist der Träger von $\mathbb{Z}/p\mathbb{Z}$ nach (a) gerade $\mathcal{V}(p\mathbb{Z}) = \{(p)\}$. Allgemeiner gilt $\operatorname{Supp}(\mathbb{Z}/p^n\mathbb{Z}) = \{(p)\}$ für alle $n > 0$.

6.5.7. Die Bedingung, dass M endlich erzeugt ist, ist unabdingbar in (d): Der Träger von $\bigoplus_{p \text{ prim}} \mathbb{Z}/p\mathbb{Z}$ ist $\operatorname{Spec}\mathbb{Z} - \{(0)\}$ (nach (a), da Lokalisieren mit direkten Summen vertauscht), was nicht abgeschlossen in $\operatorname{Spec}\mathbb{Z}$ ist, während der Annihilator dieses Moduls das Nullideal ist und $\mathcal{V}(0) = \operatorname{Spec}\mathbb{Z}$.

Beweis. (a) Sei $\mathfrak{p} \in \operatorname{Spec} A$. Dann sind äquivalent:

- $(A/\mathfrak{a})_\mathfrak{p} = 0$;
- $\frac{\overline{1}}{1} = 0$ in $(A/\mathfrak{a})_\mathfrak{p}$; (weil $\frac{\overline{1}}{1}$ den $A_\mathfrak{p}$-Modul $(A/\mathfrak{a})_\mathfrak{p}$ erzeugt: Lokalisiere den Morphismus $A \twoheadrightarrow A/\mathfrak{a}$ von A-Moduln).
- es gibt ein $u \in A - \mathfrak{p}$ mit $0 = u.\overline{1} = \overline{u}$ in $A/\mathfrak{a}$;

- $(A - \mathfrak{p}) \cap \mathfrak{a} \neq \emptyset$;

Also gilt $\mathfrak{p} \in \operatorname{Supp}(A/\mathfrak{a})$ genau dann, wenn $\mathfrak{a} \subset \mathfrak{p}$ oder äquivalent $\mathfrak{p} \in \mathcal{V}(\mathfrak{a})$.

(b) Sei $\mathfrak{p} \in \operatorname{Spec} A$. Dann ist $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$ eine kurze exakte Sequenz, und somit gilt $M_{\mathfrak{p}} \neq 0$ genau dann, wenn $M'_{\mathfrak{p}} \neq 0$ oder $M''_{\mathfrak{p}} \neq 0$.

(c) Dies folgt sofort aus $(U + V)_{\mathfrak{p}} = U_{\mathfrak{p}} + V_{\mathfrak{p}}$ für $\mathfrak{p} \in \operatorname{Spec} A$.

(d) Sei $M = Am_1 + \cdots + Am_n$ für Erzeuger $m_1, \dots, m_n$. Der Epimorphismus $A \twoheadrightarrow Am_i$, $a \mapsto am_i$, hat Kern $\operatorname{Ann}_A(m_i)$. Also gilt $A/\operatorname{Ann}_A(m_i) \xrightarrow{\sim} Am_i$ und somit nach (a) $\operatorname{Supp}(Am_i) = \mathcal{V}(\operatorname{Ann}_A(m_i))$. Wegen $\operatorname{Ann}_A(M) = \operatorname{Ann}_A(m_1) \cap \cdots \cap \operatorname{Ann}_A(m_n)$ und Proposition 2.11.6 erhalten wir somit

$$\begin{aligned}\operatorname{Supp}(M) &\overset{(c)}{=} \operatorname{Supp}(Am_1) \cup \cdots \cup \operatorname{Supp}(Am_n) = \mathcal{V}(\operatorname{Ann}_A(m_1)) \cup \cdots \cup \mathcal{V}(\operatorname{Ann}_A(m_n)) \\ &= \mathcal{V}(\operatorname{Ann}_A(m_1) \cap \cdots \cap \operatorname{Ann}_A(m_n)) = \mathcal{V}(\operatorname{Ann}_A(M)).\end{aligned}$$

□

Erinnerung 6.5.8. Wir verwenden in einigen der folgenden Aussagen, dass $X = \operatorname{Spec} A$ mit der Zariski-Topologie ein topologischer Raum ist, dessen offene Mengen genau die Mengen der Form $X - \mathcal{V}(I)$ sind, wobei I ein Ideal (oder eine Teilmenge) von A ist.

Insbesondere sind die Mengen der Form $X_f := X - \mathcal{V}(f)$, für $f \in A$, offene Teilmengen.

Sie bilden eine Basis der Zariski-Topologie (Aufgabe 2.12.5): Ist U eine beliebige offene Teilmenge von X und $\mathfrak{p} \in U$, so gibt es ein $f \in A - \mathfrak{p}$ mit $\mathfrak{p} \in X_f \subset U$ (die Bedingung $f \notin \mathfrak{p}$ ist natürlich äquivalent zu $\mathfrak{p} \in X_f$):

Dies war Übungsaufgabe 3.3 und ist einfach zu beweisen: Sei $U = X - \mathcal{V}(I)$ für ein Ideal I von A. Da $\mathfrak{p} \notin \mathcal{V}(I)$ schlicht bedeutet, dass $I \not\subset \mathfrak{p}$ gilt, gibt es ein $f \in I$ mit $f \notin \mathfrak{p}$. Daraus folgt zum einen $\mathcal{V}(f) \supset \mathcal{V}(I)$, also $X_f \subset X - \mathcal{V}(I) = U$, und zum anderen $\mathfrak{p} \notin \mathcal{V}(f)$, also $\mathfrak{p} \in X_f$.

Proposition 6.5.9 (Null-Locus (oder Verschwindungslocus) ist offen). *Sei M ein endlich erzeugter A-Modul. Gilt $M_{\mathfrak{p}} = 0$ für ein $\mathfrak{p} \in X = \operatorname{Spec} A$, so gibt es ein $f \in A - \mathfrak{p}$ (d. h. $\mathfrak{p} \in X_f$), so dass $M_f = 0$ gilt. Insbesondere gilt $M_{\mathfrak{q}} = 0$ für alle $\mathfrak{q}$ in der offenen Umgebung X_f von $\mathfrak{p}$ (denn $(M_f)_{\mathfrak{q}_f} \cong M_{\mathfrak{q}}$).*

Beweis. Nach Proposition 6.5.5.(d) ist $X - \operatorname{Supp}(M) = X - \mathcal{V}(\operatorname{Ann}_A(M))$ eine offene Umgebung von $\mathfrak{p}$ in X. Es gibt also nach 6.5.8 ein $f \in A - \mathfrak{p}$ mit $\mathfrak{p} \subset X_f \subseteq X - \operatorname{Supp}(M)$. Insbesondere gilt $M_{\mathfrak{q}} = 0$ für alle $\mathfrak{q} \in X_f$.

Um zu zeigen, dass der A_f-Modul M_f Null ist, reicht es nach Korollar 6.4.3 zu zeigen, dass $(M_f)_{\mathfrak{r}} = 0$ für alle $\mathfrak{r} \in \operatorname{Spec}(A_f)$ gilt. Nach Korollar 6.2.6 hat jedes solche $\mathfrak{r}$ die Form $\mathfrak{q}_f$, für ein (eindeutiges) $\mathfrak{q} \in X_f = (\operatorname{Spec} A)_f$. Nun gilt

$$(M_f)_{\mathfrak{r}} = (M_f)_{\mathfrak{q}_f} \cong M_{\mathfrak{q}}$$

als $(A_f)_{\mathfrak{q}_f} = A_{\mathfrak{q}}$-Moduln nach Aufgabe 6.5.16.(b). Wir haben aber X_f oben so gewählt, dass $M_{\mathfrak{q}} = 0$ gilt. □

Korollar 6.5.10 (Endlich erzeugter Locus ist offen). *Sei M ein endlich erzeugter A-Modul. Für $r \geq 0$ sei*

$$U_r := \{\mathfrak{p} \in \operatorname{Spec} A \mid M_{\mathfrak{p}} \textit{ kann über } A_{\mathfrak{p}} \textit{ durch } r \textit{ Elemente erzeugt werden}\}.$$

Dann ist jedes U_r offen in $\operatorname{Spec} A$ und es gilt $U_0 \subset U_1 \subset \dots$. (Ist M von l Elementen erzeugt, so gilt $U_l = \operatorname{Spec} A$.)

Genauer gilt für $\mathfrak{p} \in X = \operatorname{Spec} A$: Ist $M_{\mathfrak{p}}$ von r Elementen erzeugt, so gibt es eine offene Umgebung $X_f \subset U_r$ von $\mathfrak{p}$ in X, für ein geeignetes $f \in A - \mathfrak{p}$, so dass der A_f-Modul M_f von r Elementen erzeugt wird.

Beweis. Sei $r \in \mathbb{N}$. Sei $\mathfrak{p} \in U_r$. Sind $\frac{m_1}{s_1}, \dots, \frac{m_r}{s_r}$ Erzeuger von $M_{\mathfrak{p}}$ als $A_{\mathfrak{p}}$-Modul, so sind auch die Elemente $\frac{m_1}{1}, \dots, \frac{m_r}{1}$ Erzeuger von $M_{\mathfrak{p}}$. Die Elemente $m_1, \dots, m_r$ definieren einen Morphismus $\pi \colon A^r \to M$, der lokalisiert bei $\mathfrak{p}$ ein Epimorphismus wird. Es folgt also $\operatorname{cok}(\pi)_{\mathfrak{p}} = 0$.

Da $\operatorname{cok}(\pi)$ als Quotient von M endlich erzeugt ist, gibt es nach Proposition 6.5.9 ein $f \in A - \mathfrak{p}$, so dass $\operatorname{cok}(\pi)_f = 0$ und $\operatorname{cok}(\pi)_{\mathfrak{q}} = 0$ für alle $\mathfrak{q} \in X_f$. Also ist $\pi_f \colon A_f^r \to M_f$ surjektiv, und somit ist M_f von r Elementen erzeugt. Analog ist $M_{\mathfrak{q}}$ für alle $\mathfrak{q} \in X_f$ von r Elementen erzeugt. Es folgt $\mathfrak{p} \in X_f \subset U_r$. Somit ist U_r offen in X. □

Beispiel 6.5.11. nicht in Vorlesung Sei M eine endlich erzeugte abelsche Gruppe. Dann gilt (nach dem Hauptsatz über endlich erzeugte Moduln über Hauptidealringen)

$$M \cong \mathbb{Z}^{n(0)} \oplus \bigoplus_{p \text{ prim}} \bigoplus_{r>0} (\mathbb{Z}/p^r)^{n(p,r)}$$

für (eindeutig bestimmte) natürliche Zahlen $n(0)$ und $n(p,r)$, die fast alle Null sind.

Wir nehmen nun an, dass M ein endlich erzeugter Torsions-$\mathbb{Z}$-Modul ist. Dann gilt

$$M \cong \bigoplus_{p \text{ prim}} \bigoplus_{i \in I_p} (\mathbb{Z}/p^{n_i}).$$

Dann gilt $(p) \in U_r$ genau dann, wenn $|I_p| \leq r$. Weiter gilt $(0) \in U_0$, da $M_{(0)} = 0$.

6.5.12. Ist M ein A-Modul von endlicher Darstellung, so ist $S^{-1}M$ ein $S^{-1}A$-Modul von endlicher Darstellung: Eine endliche Darstelung $A^p \to A^q \to M \to 0$ liefert per Lokalisieren eine endliche Darstellung $(S^{-1}A)^p \to (S^{-1}A)^q \to S^{-1}M \to 0$.

Proposition 6.5.13 (Freier Locus ist offen)**.** *Sei M ein A-Modul von endlicher Darstellung. Dann ist*

$$U = \{\mathfrak{p} \in \operatorname{Spec} A \mid M_\mathfrak{p} \text{ ist freier } A_\mathfrak{p}\text{-Modul}\}$$

eine offene Teilmenge von $\operatorname{Spec} A$.

Genauer gilt für $\mathfrak{p} \in X = \operatorname{Spec} A$: Ist $M_\mathfrak{p}$ ein freier (notwendig endlich erzeugter) $A_\mathfrak{p}$-Modul vom Rang n, so gibt es eine offene Umgebung $X_f \subset U$ von $\mathfrak{p}$ in X, für ein geeignetes $f \in A - \mathfrak{p}$, so dass der A_f-Modul frei vom Rang n ist.

bis hier, Mittwoch 14. Dezember

Beweis. Sei $\mathfrak{p} \in U$. Also ist $M_\mathfrak{p}$ ein freier $A_\mathfrak{p}$-Modul. Es ist klar, dass er endlich erzeugt ist (siehe 6.5.1).

Sei $x_1, \dots, x_n$ eine (geordnete) $A_\mathfrak{p}$-Basis von $M_\mathfrak{p}$. Wir können annehmen, dass alle Erzeuger x_i die Form $x_i = \frac{m_i}{1}$ für geeignete $m_i \in M$ haben.

Die Elemente $m_1, \dots, m_n$ definieren eine Abbildung $\pi \colon A^n \to M$. Wir notieren ihren Kern mit K und ihren Kokern mit C und erhalten so eine exakte Sequenz

$$0 \to K \to A^n \xrightarrow{\pi} M \to C \to 0. \tag{6.5.1}$$

Da M endlich erzeugt ist, ist auch C endlich erzeugt. (Es ist nicht klar, ob K endlich erzeugt ist.)

Da die Lokalisierung von π bei $\mathfrak{p}$ bijektiv ist, folgen $C_\mathfrak{p} = 0$ und $K_\mathfrak{p} = 0$. Proposition 6.5.9 liefert eine offene Umgebung X_f von $\mathfrak{p}$ in X, für ein $f \in A - \mathfrak{p}$, so dass $C_f = 0$ gilt. Wir erhalten eine exakte Sequenz

$$0 \to K_f \to (A_f)^n \xrightarrow{\pi_f} M_f \to 0$$

von A_f-Moduln. Da mit M auch M_f von endlicher Darstellung ist (siehe 6.5.12), ist K_f endlich erzeugt als A_f-Modul nach Satz 3.13.5. Deswegen und wegen $(K_f)_{\mathfrak{p}_f} \cong K_\mathfrak{p} = 0$ gibt es nach Proposition 6.5.9 ein $h = \frac{g}{f^l} \in A_f - \mathfrak{p}_f$ mit $(K_f)_h = 0$. Nach Aufgabe 6.5.16.(b) gilt $K_{fg} = (K_f)_h = 0$. Natürlich gilt auch $C_{fg} = (C_f)_{\frac{g}{1}} = 0$.

Die kurze exakte Sequenz (6.5.1) liefert also per Lokalisierung an fg den Isomorphismus $\pi_{fg} \colon A^n_{fg} \xrightarrow{\sim} M_{fg}$ von A_{fg}-Moduln. Für jedes $\mathfrak{q} \in X_{fg}$ erhalten wir durch weiteres Lokalisieren an $\mathfrak{q}_{fq}$ den Isomorphismus $\pi_\mathfrak{q} \colon A^n_\mathfrak{q} \to M_\mathfrak{q}$ von $A_\mathfrak{q}$-Moduln. Es folgt $X_{fg} \subset U$, und wir sind fertig, sobald wir uns davon überzeugt haben, dass $\mathfrak{p} \in X_{fg}$ gilt. Aus $\frac{g}{f^l} \in A_f - \mathfrak{p}_f$ folgt aber $g \notin \mathfrak{p}$ (Proposition 6.2.3.(c)), und wegen $f \notin \mathfrak{p}$ gilt $fg \notin \mathfrak{p}$, also $\mathfrak{p} \in X_{fg}$. $\square$

6.5.14. Genauer haben wir für beliebiges $n \in \mathbb{N}$ gezeigt, dass der Locus aller $\mathfrak{p} \in X$, wo $M_\mathfrak{p}$ frei vom Rang n ist, offen in X ist.

Aufgabe 6.5.15. Sei A ein Ring und $X = \operatorname{Spec} A$. Ein A-Modul M heißt **lokal endlich erzeugt frei**, falls für jeden Punkt $\mathfrak{p} \in \operatorname{Spec} A$ ein $f \in A$ existiert mit $\mathfrak{p} \in X_f$ (d. h. $f \notin \mathfrak{p}$), so dass M_f ein endlich erzeugter freier A_f-Modul ist.

Zeigen Sie: Ein A-Modul ist genau dann endlich erzeugt projektiv, wenn er lokal endlich erzeugt frei ist.[17]

[17] eine andere äquivalente Bedingung ist: endlich präsentiert und flach [Sta16, 00NX].

Hinweise: Die Implikation $\Rightarrow$ wurde im Wesentlichen in der Vorlesung gezeigt (Propositionen 3.12.12 und 6.5.13). Für die Implikation $\Leftarrow$ gehe man etwa wie folgt vor.

(a) Seien $M, N \in \operatorname{Mod}(A)$ mit M von endlicher Darstellung. Ist S eine multiplikativ abgeschlossene Teilmenge von A, so gilt kanonisch

$$S^{-1}\operatorname{Hom}_A(M,N) \xrightarrow{\sim} \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

Insbesondere gilt $\operatorname{Hom}_A(M,N)_f \xrightarrow{\sim} \operatorname{Hom}_{A_f}(M_f, N_f)$.

Hinweis: Lokalisieren Sie eine endliche Darstellung von M und wenden dann einen geeigneten Hom-Funktor an, bzw. gehen Sie umgekehrt vor.

(b) Sei $H' \to H \to H''$ eine Sequenz von A-Moduln. Dann sind äquivalent:
  (i) $H' \to H \to H''$ ist exakt;
  (ii) $H'_f \to H_f \to H''_f$ ist exakt für alle $f \in A$.
  (iii) $H'_{f_i} \to H_{f+i} \to H''_{f_i}$ ist exakt für eine Familie $(f_i)_{i \in I}$ von Elementen von A, so dass $X = \bigcup_{i \in I} X_{f_i}$.

(c) Seien $f_1, \dots, f_n$ Elemente von A, so dass $X = X_{f_1} \cup \dots \cup X_{f_n}$ gilt. Ist M ein A-Modul, so dass M_{f_i} für jedes $i = 1, \dots, n$ ein endlich erzeugter A_{f_i}-Modul ist, so ist M ein endlich erzeugter A-Modul.

(d) Mit $f_1, \dots, f_n$ wie eben, sei M ein A-Modul, so dass M_{f_i} für jedes $i = 1, \dots, n$ ein A_{f_i}-Modul von endlicher Darstellung ist. Dann ist M von endlicher Darstellung als A-Modul.

(e) Folgern Sie, dass ein lokal endlich erzeugter freier A-Modul von endlicher Darstellung ist. Verwenden Sie, dass X quasi-kompakt ist (siehe Aufgabe 2.12.5 bzw. Übungsaufgabe 3.3.(e)): Aus $X = \bigcup_{i \in I} X_{f_i}$ folgt bereits $X = \bigcup_{i \in E} X_{f_i}$ für eine endliche Teilmenge $E \subset I$.

(f) Folgern Sie, dass ein lokal endlich erzeugter freier A-Modul projektiv ist.

Aufgabe 6.5.16. Dies ist die Ausdehnung von Aufgabe 6.2.10 auf Moduln. Wir schreiben die dortigen kanonischen Isomorphismen von Ringen als Gleichheiten. Sei M ein A-Modul.

(a) Für $\mathfrak{q} \subset \mathfrak{p}$ mit $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} A$ gilt kanonisch $(M_\mathfrak{p})_{\mathfrak{q}_\mathfrak{p}} \xrightarrow{\sim} M_\mathfrak{q}$ als Moduln über $(A_\mathfrak{p})_{\mathfrak{q}_\mathfrak{p}} = A_\mathfrak{q}$.

(b) Sei $f \in A$ und $\mathfrak{p} \in \operatorname{Spec} A$ mit $f \notin \mathfrak{p}$. Dann gilt kanonisch $(M_f)_{\mathfrak{p}_f} \xrightarrow{\sim} M_\mathfrak{p}$ als Moduln über $(A_f)_{\mathfrak{p}_f} = A_\mathfrak{p}$.

(c) Für $f, g \in A$ und $l \in \mathbb{N}$ gilt kanonisch $(M_f)_{\frac{g}{f^l}} \xrightarrow{\sim} M_{fg}$ als Moduln über $(A_f)_{\frac{g}{f^l}} = A_{fg}$.

Aufgabe 6.5.17 (Transitivität der Lokalisierung von Moduln)**.** Seien $S \subset T$ multiplikativ abgeschlossene Teilmengen eines Ringes A, und sei M ein A-Modul. Dann gilt $\sigma(T)^{-1}(S^{-1}M) = T^{-1}M$ als Modul über $\sigma(T)^{-1}(S^{-1}A) = T^{-1}A$ (vgl. Aufgabe 6.1.26 oder Aufgabe 5.5.12).

Aufgabe 6.5.18. Ist M ein A-Modul, so sagen wir, dass alle Elemente von S invertierbar auf M operieren, falls für alle $s \in S$ die Abbildung $(s.)\colon M \to M$ invertierbar ist.

Zeigen Sie, dass der Restriktionsfunktor $\operatorname{Mod}(S^{-1}A) \to \operatorname{Mod}(A)$ die Kategorie $\operatorname{Mod}(S^{-1}A)$ mit der Kategorie aller A-Moduln, auf denen alle Elemente von S invertierbar operieren, identifiziert.[18]

Man mag damit 6.3.15 umschreiben.

Aufgabe 6.5.19. Ist M ein A-Modul, so können wir $S^{-1}M$ per Restriktion als A-Modul auffassen. Die Abbildung $M \to S^{-1}M$, $m \mapsto \frac{m}{1}$ ist dann A-linear. Diese Abbildung ist ein Isomorphismus genau dann, wenn alle Elemente von S invertierbar auf M operieren (siehe Aufgabe 6.5.18).

[18] Genauer sind die folgenden Aussagen zu zeigen:

(a) Für $N \in \operatorname{Mod}(S^{-1}A)$ operieren alle Elemente von S invertierbar auf $\operatorname{res}(N)$.

(b) Operieren alle Elemente von S invertierbar auf $M \in \operatorname{Mod}(A)$, so gibt es genau ein $N \in \operatorname{Mod}(S^{-1}A)$ mit $\operatorname{res}(N) = M$ (d. h. die A-Modulstruktur auf der abelschen Gruppe kommt von einer eindeutigen $S^{-1}A$-Modulstruktur).

(c) Für $N, P \in \operatorname{Mod}(S^{-1}A)$ induziert der Restriktionsfunktor einen Bijektion

$$\operatorname{Hom}_{S^{-1}A}(N,P) \xrightarrow{\sim} \operatorname{Hom}_A(\operatorname{res}(N), \operatorname{res}(P)).$$

7. Ganze Ringerweiterungen

7.1. Ganzheit.

Definition 7.1.1. Ist A ein Teilring eines Ringes B, so nennen wir $A \subset B$ eine **Ringerweiterung**.

Sei $A \subset B$ eine Ringerweiterung.

Notation 7.1.2. Gegeben Elemente $x_1, \ldots, x_n \in B$, sei $A[x_1, \ldots, x_n]$ der kleinste Unterring von B, der alle Elemente $x_1, \ldots, x_n$ enthält. Er besteht offensichtlich aus allen A-Linearkombinationen von Produkten $x_1^{f_1} x_2^{f_2} \ldots x_n^{f_n}$ für $f_i \in \mathbb{N}$. Mit anderen Worten ist er das Bild des Auswertungsmorphismus $A[X_1, \ldots, X_n] \to B$, $p = p(X_1, \ldots, X_n) \mapsto p(x_1, \ldots, x_n)$.

Analog definiert man $A[E]$ für eine beliebige Teilmenge $E \subset B$.

Beispiel 7.1.3. Für $\mathbb{Z} \subset \mathbb{C}$ gilt $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$. Dieser Ring heißt der Ring der **Gaußschen Zahlen**. Anschaulich ist er durch das „quadratische Gitter“ $\mathbb{Z} \oplus \mathbb{Z}i$ in der komplexen Zanlenebene $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ gegeben.

Zeichnung? Abbildung 1 adaptieren.

Definition 7.1.4.
(a) Ein Element $x \in B$ heißt **ganz** über A, falls ein normiertes Polynom $p \in A[X]$ existiert mit $p(x) = 0$, d. h. falls es ein $n \in \mathbb{N}_{>0}$ und Elemente $a_1, \ldots, a_n \in A$ mit

$$x^n + a_1 x^{n-1} + \ldots a_{n-1} x + a_n = 0 \tag{7.1.1}$$

gibt. Eine solche Gleichung heißt **Ganzheitsgleichung** von x über A.

(b) Die Ringerweiterung $A \subset B$ heißt **ganz**, falls jedes Element von B ganz über A ist. Man sagt dann auch, dass B **ganz** über A ist.

Beispiel 7.1.5. Jedes Element $a \in A$ ist ganz über A, denn es ist Nullstelle des normierten Polynoms $X - a \in A[X]$.

Beispiel 7.1.6. Sei $k \subset K$ eine Körpererweiterung. Dann ist ein Element von K genau dann ganz über k, wenn es algebraisch über k ist. Die Körpererweiterung ist genau dann ganz, wenn sie algebraisch ist.

Beispiel 7.1.7. Die Erweiterung $\mathbb{Z} \subset \mathbb{Z}[i]$ ist eine ganze Ringerweiterung: Jedes Element $x = a + bi \in \mathbb{Z}[i]$ ist Nullstelle des normierten Polynoms $(X - x)(X - \overline{x}) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{Z}[X]$, wobei $\overline{x} = a - bi$.

Proposition 7.1.8. *Für $x \in B$ sind äquivalent:*

(a) x ist ganz über A;
(b) $A[x] = A + Ax + Ax^2 + \ldots$ ist als A-Modul endlich erzeugt;
(c) $A[x]$ ist in einem Unterring C von B enthalten, der als A-Modul endlich erzeugt ist; mit anderen Worten: Es gibt einen Zwischenring $A \subset C \subset B$ mit $x \in C$, so dass C als A-Modul endlich erzeugt ist;
(d) der Ring $A[x]$ besitzt einen treuen Modul M, der als A-Modul endlich erzeugt ist. (Treuheit bedeutet $\operatorname{Ann}_{A[x]}(M) = 0$.)

Beweis. (a) $\Rightarrow$ (b): Ist (7.1.1) eine Ganzheitsgleichung von x über A, so gilt $A[x] = A1 + Ax + \cdots + Ax^{n-1}$: Wegen $x^{n+l} = -a_1 x^{n-1+l} - \cdots - a_0 x^l$ für alle $l \in \mathbb{N}$ können wir sukzessive alle Potenzen x^N mit $N \geq n$ durch A-Linearkombinationen von kleineren Potenzen von x ersetzen.

(b) $\Rightarrow$ (c): Nimm $C = A[x]$.

(c) $\Rightarrow$ (d): Nimm $M = C$. Dieser $A[x]$-Modul ist treu, denn aus $q \in \operatorname{Ann}_{A[x]}(C)$ folgt $q = q.1 = 0$.

(d) $\Rightarrow$ (a): Wir wenden den Determinantentrick (Satz 3.7.1) auf den Endomorphismus $(x.)\colon M \to M$ des endlich erzeugten A-Moduls M an (und das Ideal A). Er liefert Elemente $a_1, \ldots, a_n \in A$ und eine Gleichheit

$$(x^n.) + a_1(x^{n-1}.) + \ldots a_{n-1}(x.) + a_n = 0$$

in $\operatorname{End}_A(M)$. Dies bedeutet $x^n + a_1 x^{n-1} + \ldots a_{n-1} x + a_n \in \operatorname{Ann}_{A[x]}(M)$. Nach Voraussetzung ist dieser Annihilator null, und wir erhalten die gesuchte Ganzheitsgleichung. □

Korollar 7.1.9. *Sind $x_1, \ldots, x_n \in B$ ganz über A, so ist $A[x_1, \ldots, x_n]$ ein endlich erzeugter A-Modul.*

Beweis. Erfülle x_i eine Ganzheitsgleichung vom Grad d_i. Dann ist $A[x_1, \ldots, x_n]$ von den endlich vielen Elementen $x_1^{f_1} x_2^{f_2} \ldots x_n^{f_n}$, für $0 \leq f_i < d_i$, als A-Modul erzeugt. □

Korollar 7.1.10. *Die Menge der über A ganzen Elemente von B bildet einen Zwischenring von $A \subset B$.*

Beweis. Es ist klar, dass diese Menge ganz A enthält. Sind $x, y \in B$ ganz über A, so ist der Unterring $C := A[x, y]$ von B endlich erzeugt als A-Modul (Korollar 7.1.9). Er enthält die Elemente $\pm x, x \pm y$ und xy, die somit ganz über A sind (Proposition 7.1.8). □

Korollar 7.1.11. *Ist $E \subset B$ eine Menge von Elementen von B, die ganz über A sind, so ist $A \subset A[E]$ eine ganze Ringerweiterung.*

Beweis. Klar nach Korollar 7.1.10. □

Definition 7.1.12. (a) Der Ring der über A ganzen Elemente von B heißt der **ganze Abschluss** von A in B.
(b) Stimmt A mit seinem ganzen Abschluss in B überein, so heißt A **ganz abgeschlossen** in B.
(c) Ein Integritätsbereich R heißt **normal** (oder **ganz abgeschlossen**), falls er ganz abgeschlossen in $\mathrm{Quot}(R)$ ist.

Proposition 7.1.13. *Jeder faktorielle Ring ist normal.*

Beispiel 7.1.14. Der Ring der ganzen Zahlen ist normal, also ganz abgeschlossen in $\mathbb{Q}$. Dies bedeutet zum Beispiel, dass jede rationale Zahl, die Nullstelle eines normierten Polynoms mit ganzen Koeffizienten ist, bereits ganz ist im Sinne, dass sie in $\mathbb{Z}$ liegt. Zum Beispiel sind alle rationalen Wurzeln (oder allgemeiner n-ten Wurzeln für $n \geq 1$) einer ganzen Zahl bereits ganze Zahlen.

Beispiel 7.1.15. Ist k ein Körper, so ist $k[X_1, \dots, X_n]$ normal.

Beweis. Sei R ein faktorieller Ring. Sei $x \in \mathrm{Quot}(R)$ ganz über R und sei $x^n + a_1 x^{n-1} + \dots a_{n-1}x + a_n = 0$ eine Ganzheitsgleichund von x mit $a_i \in R$. Schreibe $x = \frac{r}{s} \in \mathrm{Quot}(R)$ mit $r, s \in R$, $s \neq 0$. Durch Kürzen können wir annehmen, dass r und s teilerfremd sind (es gibt also kein Primelement, dass sowohl r als auch s teilt). Es gilt also

$$\frac{r^n}{s^n} + a_1 \frac{r^{n-1}}{s^{n-1}} + \dots a_{n-1} \frac{r}{s} + a_n = 0$$

Multiplizieren wir dies mit s^n, so erhalten wir (weil $R \hookrightarrow \mathrm{Quot}(R)$ injektiv ist) die Gleichung

$$r^n + a_1 r^{n-1} s + \dots a_{n-1} r s^{n-1} + a_n s^n = 0$$

in R. Also wird r^n von s geteilt. Wegen der Teilerfremdheit von r und s folgt $s \in R^\times$ und damit $x = \frac{r}{s} = \frac{s^{-1}r}{1} = s^{-1}r \in R$. □

Definition 7.1.16. Sei A ein Ring. Eine **A-Algebra** ist ein Ring B zusammen mit einem Ringmorphismus $\sigma \colon A \to B$ (ist B nicht notwendig kommutativ, so verlangt man, dass $\sigma(A)$ im Zentrum von B liegt). Man nennt σ den **Strukturmorphismus**.

7.1.17. Elemente a von A faßt man oft als Elemente von B auf und schreibt a statt $\sigma(a)$.
Insbesondere ist B per Restriktion ein A-Modul. Für $a \in A$ gilt $a = \sigma(a) = \sigma(a)1 = a.1$.

Aufgabe 7.1.18. Sei A ein Ring. Eine äquivalente Definition einer A-Algebra ist: Eine A-Algebra ist ein Ring B zusammen mit einer A-Modulstruktur auf B, so dass die Multiplikation $B \times B \to B$ A-bilinear ist.

Beispiel 7.1.19. Jeder Ring ist in eindeutiger Weise eine $\mathbb{Z}$-Algebra (Beispiel 2.2.2.(a)).

Beispiel 7.1.20. Ist $A \subset B$ eine Ringerweiterung, so ist B eine A-Algebra.

Definition 7.1.21. Eine A-Algebra B ist **endlich erzeugt** (oder **von endlichem Typ**[19]), falls es endlich viele Elemente $x_1, \dots, x_n \in B$ gibt, so dass die Auswertungsabbildung $A[X_1, \dots, X_n] \to B$, $X_i \mapsto x_i$, (die den Strukturmorphismus fortsetzt) surjektiv ist. Dies bedeutet äquivalent, dass $\sigma(A)[x_1, \dots, x_n] = B$.

Korollar 7.1.22. *Sei $A \subset B$ eine Ringerweiterung. Dann sind äquivalent:*
(a) B ist endlich erzeugt als A-Modul.
(b) B ist endlich erzeugt als A-Algebra und ganz über A.

[19] das ist der Begriff, den man im geometrischen Kontext verwendet

(c) *B ist als A-Algebra von endlich vielen Elementen erzeugt, die ganz über A sind.*

7.1.23. Ist B endlich erzeugt als A-Modul, so sagt man, dass B endlich über A ist (siehe die spätere Definition 7.5.1). Als Slogan kann man damit die Äquivalenz der ersten beiden Aussagen in Korollar 7.1.22 wie folgt zusammenfassen:

$$\text{endlich} = \text{endlicher Typ} + \text{ganz} \qquad \text{für Ringerweiterungen.} \tag{7.1.2}$$

Beweis. (a) $\Rightarrow$ (b): Endlich viele Erzeuger von B als A-Modul erzeugen offensichtlich B als A-Algebra. Jedes Element $x \in B$ ist in dem (Zwischen-)Ring B enthalten, der als A-Modul endlich erzeugt ist, und somit ganz über A nach Proposition 7.1.8.

(b) $\Rightarrow$ (c): Das ist offensichtlich.

(c) $\Rightarrow$ (a): Gelte $B = A[x_1, \dots, x_n]$ für geeignete $x_1, \dots, x_n$, die ganz über A sind. Dann ist B endlich erzeugt als A-Modul nach Korollar 7.1.9. □

Korollar 7.1.24 (Transitivität von Ganzheit)**.** *Seien $A \subset B \subset C$ Ringerweiterungen. Genau dann sind $A \subset B$ und $B \subset C$ ganz, wenn $A \subset C$ ganz ist.*

Beweis. Ist $A \subset C$ ganz, so sind offensichtlich $A \subset B$ und $B \subset C$ ganz (denn eine Ganzheitsgleichung eines Elements von C über A ist auch eine Ganzheitsgleichung über B).

Seien $A \subset B$ und $B \subset C$ ganz. Sei $x \in C$. Da x ganz über B ist, erfüllt x eine Ganzheitsgleichung

$$x^n + b_1 x^{n-1} + \dots b_{n-1} x + b_n = 0$$

mit $b_i \in B$. Alle b_i sind ganz über A. Also ist $A[b_1, \dots, b_n]$ ein endlich erzeugter A-Modul (Korollar 7.1.9). Aus der obigen Ganzheitsgleichung folgt sofort, dass $A[b_1, \dots, b_n][x]$ ein endlich erzeugter A-Modul ist. Dieser Zwischenring von $A \subset B$ enthält x. Somit ist x ganz über A nach Proposition 7.1.8. □

Korollar 7.1.25. *Sei $A \subset B$ eine Ringerweiterung und sei A' der ganze Abschluss von A in B. Dann ist A' ganz abgeschlossen in B.*

Beweis. Sei A'' der ganze Abschluss von A' in B. Dann ist A'' ganz über A wegen der Transitivität von Ganzheit (Korollar 7.1.24). Es folgt $A'' = A'$. □

Proposition 7.1.26. *Sei $A \subset B$ eine ganze Ringerweiterung.*

(a) *Ist $\mathfrak{b} \subset B$ ein Ideal und $\mathfrak{a} := A \cap \mathfrak{b}$, so ist $A/\mathfrak{a} \subset B/\mathfrak{b}$ ganz.*

(b) *Ist $S \subset A$ eine multiplikativ abgeschlossene Teilmenge, so ist $S^{-1}A \subset S^{-1}B$ ganz.*

Beweis. Sei $x \in B$ mit Ganzheitsgleichung $x^n + a_1 x^{n-1} + \dots a_{n-1} x + a_n = 0$ über A.

(a). Der Kern der Verknüpfung $A \to B \to B/\mathfrak{b}$ ist $\mathfrak{a}$. Deswegen ist $A/\mathfrak{a}$ ein Unterring von $B/\mathfrak{b}$. Die obige Ganzheitsgleichung liefert $\overline{x}^n + \overline{a}_1 \overline{x}^{n-1} + \dots \overline{a}_{n-1}\overline{x} + \overline{a}_n = 0$ in $B/\mathfrak{b}$. Dies ist eine Ganzheitsgleichung von $\overline{x} \in B/\mathfrak{b}$ über $A/\mathfrak{a}$ und zeigt die Behauptung, da $x \in B$ beliebig war.

(b) Der offensichtliche Ringmorphismus $S^{-1}A \to S^{-1}B$ ist injektiv. Sei $s \in S$. Bilden wir die obige Ganzheitsgleichung nach $S^{-1}B$ ab und multiplizieren mit $\frac{1}{s^n}$, so erhalten wir

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s} \cdot \left(\frac{x}{s}\right)^{n-1} + \dots \frac{a_{n-1}}{s^{n-1}} \cdot \frac{x}{s} + \frac{a_n}{s^n} = 0$$

in $S^{-1}B$. Diese Gleichung zeigt, dass $\frac{x}{s}$ ganz über $S^{-1}A$ ist. Da $x \in B$ und $s \in S$ beliebig waren, zeigt dies die Behauptung. □

7.2. Das Going-Up-Theorem (und anderes zur Ganzheit).

Proposition 7.2.1. *Sei $A \subset B$ eine ganze Ringerweiterung und sei B (und damit A) ein Integritätsbereich. Dann ist A genau dann ein Körper, wenn B ein Körper ist.*

7.2.2. Dies verallgemeinert die folgende Aussage: Ist $k \subset K$ eine Körpererweiterung und $x \in K$ algebraisch über k, so ist $k[x]$ bereits ein Körper.

Beispiel 7.2.3. Die Ringerweiterung $\mathbb{C} \subset \mathbb{C}[\varepsilon]/(\varepsilon^2)$ ist ganz und $\mathbb{C}$ ist ein Körper, aber $\mathbb{C}[\varepsilon]/(\varepsilon^2)$ ist kein Integritätsbereich.

Beweis. Sei A ein Körper. Sei $x \in B - \{0\}$ und $x^n + a_1 x^{n-1} + \dots a_{n-1}x + a_n = 0$ eine Ganzheitsgleichung über A von kleinstem möglichen Grad $n \geq 1$. Dann gilt $a_n \neq 0$, denn sonst könnten wir mit x kürzen (da B ein Integritätsbereich ist). Multiplizieren wir

$$x(x^{n-1} + a_1 x^{n-2} + \dots a_{n-1}) = -a_n$$

mit $-a_n^{-1} \in A$ (welches existiert, da A ein Körper ist), so sehen wir, dass x invertierbar ist. Also ist B ein Körper.

Sei umgekehrt B ein Körper. Sei $x \in A - \{0\}$. Dann ist $x^{-1} \in B$ ganz über A und erfüllt somit eine Ganzheitsgleichung

$$x^{-n} + a_1 x^{1-n} + \dots a_{n-1}x^{-1} + a_n = 0$$

über A. Multiplizieren wir diese mit x^{n-1}, so erhalten wir

$$x^{-1} + \underbrace{a_1 + a_2 x + \dots a_{n-1}x^{n-2} + a_n x^{n-1}}_{\in A} = 0.$$

Also liegt x^{-1} bereits in A. □

bis hier, 21. Dezember 2016

Korollar 7.2.4. *Sei $A \subset B$ eine ganze Ringerweiterung. Sei $\mathfrak{q} \in \operatorname{Spec} B$ und $\mathfrak{p} = A \cap \mathfrak{q} \in \operatorname{Spec} A$. Dann ist $\mathfrak{p}$ genau dann maximal, wenn $\mathfrak{q}$ maximal ist. In Formeln: $\mathfrak{p} \in \operatorname{MaxSpec} A \Leftrightarrow \mathfrak{q} \in \operatorname{MaxSpec} B$.*

Bezeichnet $\iota\colon A \hookrightarrow B$ die Inklusion, so wird die Aussage durch die Existenz des gestrichelten Pfeils und durch die Gleichheit im folgenden kommutativen Diagramm illustriert.

$$\begin{tikzcd}
\operatorname{Spec} B \arrow[d, "f := \iota^{-1}"] & \supset & \operatorname{MaxSpec} B \arrow[d, dotted] & = & f^{-1}(\operatorname{MaxSpec} A) \\
\operatorname{Spec} A & \supset & \operatorname{MaxSpec} A,
\end{tikzcd}$$

Beweis. Betrachte die ganze Erweiterung $A/\mathfrak{p} \subset B/\mathfrak{q}$ von Integritätsbereichen (dies verwendet Proposition 7.1.26.(a) und Proposition 2.6.5). Nach Proposition 7.2.1 ist $A/\mathfrak{p}$ genau dann ein Körper, wenn $B/\mathfrak{q}$ ein Körper ist. Also ist $\mathfrak{p}$ genau dann maximal, wenn $\mathfrak{q}$ maximal ist (Proposition 2.6.5). □

Korollar 7.2.5. *Sei $A \subset B$ eine ganze Ringerweiterung. Seien $\mathfrak{q}_1, \mathfrak{q}_2 \in \operatorname{Spec} B$ mit $\mathfrak{q}_1 \subset \mathfrak{q}_2$ und $A \cap \mathfrak{q}_1 = A \cap \mathfrak{q}_2$. Dann gilt $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Beweis. Sei $\mathfrak{p} := A \cap \mathfrak{q}_1 = A \cap \mathfrak{q}_2$ und $S = A - \mathfrak{p}$. Betrachte das kommutative Diagramm

$$\begin{tikzcd}
B \arrow[r] & S^{-1}B \\
A \arrow[u, phantom, "\cup"] \arrow[r] & S^{-1}A \arrow[u, "j"] & = & A_{\mathfrak{p}}
\end{tikzcd} \tag{7.2.1}$$

von Ringen. Der vertikale Pfeil ist injektiv und eine ganze Ringerweiterung (Proposition 7.1.26.(b)).

Wir verwenden Proposition 6.2.3.(c) und Proposition 6.2.5 mehrfach. Es sind $S^{-1}\mathfrak{q}_1 \subset S^{-1}\mathfrak{q}_2$ Primideale in $S^{-1}B$ (da $\mathfrak{q}_1 \cap S \subset \mathfrak{q}_2 \cap S = \emptyset$ wegen $\mathfrak{q}_2 \cap A = \mathfrak{p}$), und $\mathfrak{p}_{\mathfrak{p}} = S^{-1}\mathfrak{p}$ ist das maximale Ideal im lokalen Ring $A_{\mathfrak{p}}$. Die Primideale $\mathfrak{p}_{\mathfrak{p}}$ und $j^{-1}(S^{-1}\mathfrak{q}_1) = S^{-1}A \cap S^{-1}\mathfrak{q}_1$ von $A_{\mathfrak{p}}$ stimmen überein, denn ihre Urbilder $\mathfrak{p}$ und $A \cap \mathfrak{q}_1$ in A sind nach Annahme gleich. Da $\mathfrak{p}_{\mathfrak{p}}$ das maximale Ideal von $A_{\mathfrak{p}}$ ist, ist $S^{-1}\mathfrak{q}_1$ maximales Ideal von $S^{-1}B$ nach Korollar 7.2.4. Die Inklusion $S^{-1}\mathfrak{q}_1 \subset S^{-1}\mathfrak{q}_2$ ist also eine Gleichheit, und es folgt $\mathfrak{q}_1 = \mathfrak{q}_2$. □

Satz 7.2.6. *Ist $A \subset B$ eine ganze Ringerweiterung, so ist die induzierte Abbildung*

$$\operatorname{Spec} B \twoheadrightarrow \operatorname{Spec} A,$$
$$\mathfrak{q} \mapsto A \cap \mathfrak{q},$$

auf den Spektren surjektiv.

7.2.7. Korollar 7.2.5 besagt, dass es keine echten Inklusionen in den Fasern von $f\colon \operatorname{Spec} B \twoheadrightarrow \operatorname{Spec} A$ gibt: Gegeben $x = \mathfrak{p} \in \operatorname{Spec} A$ und $y_1 = \mathfrak{q}_1, y_2 = \mathfrak{q}_2 \in f^{-1}(x)$, gibt es keine echte Inklusion zwischen den Idealen $\mathfrak{q}_1$ und $\mathfrak{q}_2$.

Beweis. Sei $\mathfrak{p} \in \operatorname{Spec} A$. Setze $S = A - \mathfrak{p}$ und betrachte das kommutative Diagramm (7.2.1). Sei $\mathfrak{m} \in \operatorname{MaxSpec}(S^{-1}B)$ beliebig (so ein $\mathfrak{m}$ existiert nach Satz 2.6.13, denn $S^{-1}B \neq 0$ wegen $0 \notin S$). Weil j eine ganze Ringerweiterung ist, ist $j^{-1}(\mathfrak{m}) = A_\mathfrak{p} \cap \mathfrak{m} \in \operatorname{Spec} A_\mathfrak{p}$ nach Korollar 7.2.4 maximal. Da $A_\mathfrak{p}$ ein lokaler Ring ist mit (eindeutigem) maximalen Ideal $\mathfrak{p}_\mathfrak{p}$, folgt $j^{-1}(\mathfrak{m}) = \mathfrak{p}_\mathfrak{p}$. Sei $\mathfrak{q} :=$„$B \cap \mathfrak{m}$“$\in \operatorname{Spec} B$ das Urbild von $\mathfrak{m}$ in B. Dann gilt $A \cap \mathfrak{q} = \mathfrak{p}$. □

Aufgabe 7.2.8. Sei $A \subset B$ eine ganze Ringerweiterung. Zeigen Sie, dass die Abbildung $\operatorname{Spec} B \to \operatorname{Spec} A$ abgeschlossen ist, d. h. abgeschlossene Teilmengen auf abgeschlossene Teilmengen abbildet.

Satz 7.2.9 (Going-up)**.** *Sei $A \subset B$ eine ganze Ringerweiterung. Seien $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ eine Primidealkette in A und $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_m$ eine Primidealkette in B mit $0 \leq m \leq n$, so dass $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $1 \leq i \leq m$. Dann läßt sich die zweite Kette zu einer Primidealkette $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m \subset \mathfrak{q}_{m+1} \subset \cdots \subset \mathfrak{q}_n$ in B erweitern mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $1 \leq i \leq n$.*

7.2.10. Hier ist die Illustration für $m = 2 < n = 4$. Going-up liefert den blauen Teil des Diagramms und erkärt den Namen des Satzes.

$$\begin{tikzcd}
\operatorname{Spec} B \arrow[d] & \mathfrak{q}_1 \arrow[d, mapsto] & \subset & \mathfrak{q}_2 \arrow[d, mapsto] & \subset & \mathfrak{q}_3 \arrow[d, mapsto] & \subset & \mathfrak{q}_4 \arrow[d, mapsto] \\
\operatorname{Spec} A & \mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & \mathfrak{p}_3 & \subset & \mathfrak{p}_4
\end{tikzcd}$$

Beweis. Es reicht, den Fall $m = 1 < n = 2$ zu betrachten. (Im Fall $m = 0 < n$ gibt es nach Satz 7.2.6 ein Primideal $\mathfrak{q}_1 \subset B$ mit $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.)

Betrachte das kommutative Diagramm

$$\begin{tikzcd}
 & \mathfrak{q}_1 & & \subset & B \arrow[r, two heads] & B/\mathfrak{q}_1 & \\
 & \cup & & & \cup & \cup & \\
\mathfrak{q}_1 \cap A & = & \mathfrak{p}_1 & \subset \; \mathfrak{p}_2 \; \subset & A \arrow[r, two heads] & A/\mathfrak{p}_1 & \supset \; \mathfrak{p}_2/\mathfrak{p}_1
\end{tikzcd}$$

Da $A/\mathfrak{p}_1 \subset B/\mathfrak{q}_1$ eine ganze Ringerweiterung ist (Proposition 7.1.26.(a)), ist $\operatorname{Spec}(B/\mathfrak{q}_1) \twoheadrightarrow \operatorname{Spec}(A/\mathfrak{p}_1)$ nach Satz 7.2.6 surjektiv. Also gibt es ein Primideal $\mathfrak{q}_2/\mathfrak{q}_1$ in $B/\mathfrak{q}_1$, gegeben durch ein Primideal $\mathfrak{q}_2$ in B mit $\mathfrak{q}_1 \subset \mathfrak{q}_2$, so dass $A/\mathfrak{p}_1 \cap \mathfrak{q}_2/\mathfrak{q}_1 = \mathfrak{p}_2/\mathfrak{p}_1$ gilt. Es folgt $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ wie gewünscht. □

7.3. **Normale Integritätsbereiche und das Going-Down-Theorem.**

Proposition 7.3.1. *Sei $A \subset B$ eine Ringerweiterung und C der ganze Abschluss von A in B. Sei S eine multiplikativ abgeschlossene Teilmenge von A. Dann ist $S^{-1}C$ der ganze Abschluss von $S^{-1}A$ in $S^{-1}B$.*

Beweis. Nach Proposition 7.1.26.(b) ist $S^{-1}A \subset S^{-1}C$ ganz.

Sei $\frac{b}{s} \in S^{-1}B$ ganz über $S^{-1}A$. Sei

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{t_1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{t_n} = 0$$

eine zugehörige Ganzheitsgleichung mit $a_i \in A$ und $t_i \in S$. Sei $t = t_1 t_2 \ldots t_n$. Multiplikation der Ganzheitsgleichung mit $s^n t^n$ ergibt

$$\frac{(tb)^n + a_1'(tb)^{n-1} + \cdots + a_n'}{1} = 0$$

in $S^{-1}B$ für geeignete $a_i' \in A$. Also gibt es ein $u \in S$ mit

$$u\Big((tb)^n + a_1'(tb)^{n-1} + \cdots + a_n'\Big) = 0$$

in A. Multiplikation mit u^{n-1} ergibt

$$(utb)^n + a_1''(utb)^{n-1} + \cdots + a_n'' = 0$$

in A für geeignete $a_i'' \in A$. Also ist utb ganz über A und somit gilt $utb \in C$. Daraus folgt

$$\frac{b}{s} = \frac{utb}{uts} \in S^{-1}C.$$

$\square$

Proposition 7.3.2. *Ist A ein Integritätsbereich, so sind äquivalent:*

(a) A ist normal (= ganz abgeschlossen);
(b) $A_{\mathfrak{p}}$ ist normal, für jedes $\mathfrak{p} \in \operatorname{Spec} A$;
(c) $A_{\mathfrak{m}}$ ist normal, für jedes $\mathfrak{p} \in \operatorname{MaxSpec} A$.

Beweis. Sei $K = \operatorname{Quot}(A) = A_{(0)}$ der Quotientenkörper von A. Sei C der ganze Abschluss von A in K. Sei $\mathfrak{p} \in \operatorname{Spec} A$ beliebig mit Komplement $S = A - \mathfrak{p}$. Nach Proposition 7.3.1 ist $S^{-1}C$ der ganze Abschluss von $S^{-1}A = A_{\mathfrak{p}}$ in $S^{-1}K = K = \operatorname{Quot}(A_{\mathfrak{p}})$. Man beachte, dass $S^{-1}C = C_{\mathfrak{p}}$ als $A_{\mathfrak{p}}$-Moduln gilt.

Sei $i\colon A \to C$ die Inklusion. Dann übersetzen sich unsere drei Bedingungen in die folgenden Bedingungen.

(a)' $i\colon A \to C$ ist surjektiv;
(b)' $i_{\mathfrak{p}}\colon A_{\mathfrak{p}} \to S^{-1}C = C_{\mathfrak{p}}$ ist surjektiv, für jedes $\mathfrak{p} \in \operatorname{Spec} A$;
(c)' $i_{\mathfrak{m}}\colon A_{\mathfrak{m}} \to S^{-1}C = C_{\mathfrak{m}}$ ist surjektiv, für jedes $\mathfrak{m} \in \operatorname{MaxSpec} A$.

Diese drei Bedingungen sind aber äquivalent wegen der Lokalität der Exaktheit (Korollar 6.4.4). $\square$

Definition 7.3.3. Sei $A \subset B$ eine Ringerweiterung und $\mathfrak{a} \subset A$ ein Ideal. Ein Element $x \in B$ heißt **ganz** über $\mathfrak{a}$, falls es eine **$\mathfrak{a}$-Ganzheitsgleichung** erfüllt, also eine Ganzheitsgleichung, deren sämtliche Koeffizienten mit Ausnahme des Leitkoeffizienten in $\mathfrak{a}$ liegen. Der **ganze Abschluss** von $\mathfrak{a}$ in B ist die Menge aller Elemente von B, die ganz über $\mathfrak{a}$ sind.

Lemma 7.3.4. *Sei $A \subset B$ eine Ringerweiterung, $\mathfrak{a} \subset A$ ein Ideal, und C der ganze Abschluss von A in B. Sei $\mathfrak{c}$ der ganze Abschluss von $\mathfrak{a}$ in B (es gilt natürlich $\mathfrak{c} \subset C$). Dann gilt $\mathfrak{c} = \sqrt{C\mathfrak{a}}$ (wobei $C\mathfrak{a}$ das von $\mathfrak{a}$ in C erzeugte Ideal ist). Insbesondere ist $\mathfrak{c}$ ein Ideal in C, also insbesondere abgeschlossen unter Addition und unter Multiplikation mit Elementen von C.*

Insbesondere gelten:

(a) Ist A ganz abgeschlossen in B, so sind die über $\mathfrak{a}$ ganzen Elemente von B genau die Elemente von $\sqrt{\mathfrak{a}}$.
(b) Ist $A \subset B$ ganz, so sind die über $\mathfrak{a}$ ganzen Elemente von B genau die Elemente von $\sqrt{B\mathfrak{a}}$.

Beweis. Sei $x \in \mathfrak{c}$. Sei
$$x^n + \underbrace{a_1 x^{n-1} + \dots a_{n-1}x + a_n}_{\in C\mathfrak{a}} = 0$$
eine $\mathfrak{a}$-Ganzheitsgleichung, also mit Koeffizienten $a_i \in \mathfrak{a}$. Wie bereits durch die Unterklammer angedeutet, liegt $x^n \in C\mathfrak{a}$ (da $x \in C$). Also folgt $x \in \sqrt{C\mathfrak{a}}$.

Sei umgekehrt $x \in \sqrt{C\mathfrak{a}}$. Dann gilt $x^n = c_1 a_1 + \dots c_m a_m$ für ein $n \in \mathbb{N}$ und geeignete $c_i \in C$ und $a_i \in \mathfrak{a}$. Da alle c_i ganz über A sind, ist der Zwischenring $M := A[c_1, \dots, c_m]$ von $A \subset C$ als A-Modul endlich erzeugt nach Korollar 7.1.9. Wegen $x^n = \sum a_i c_i \in \mathfrak{a}M$ gilt $x^n M \subset \mathfrak{a}M$. Wenden wir den Determinantentrick (Satz 3.7.1) auf den A-linearen Endomorphismus $(x^n\cdot)\colon M \to M$ und das Ideal $\mathfrak{a}$ an, so erhalten wir ein $N \in \mathbb{N}$ und Elemente $b_i \in \mathfrak{a}^i \subset \mathfrak{a}$, für $i = 1, \dots, N$, mit
$$x^{Nn} + b_1 x^{(N-1)n} + \dots + b_{N-1}x^n + b_N = 0$$
in $\operatorname{End}_A(M)$. Auswerten bei $1 \in M$ liefert dieselbe Gleichung in M. Sie ist eine $\mathfrak{a}$-Ganzheitsgleichung (von x^n und auch) von x über $\mathfrak{a}$. Es folgt $x \in \mathfrak{c}$. $\square$

Dienstag, 10. Januar

Proposition 7.3.5. *Seien $A \subset B$ Integritätsbereiche. Sei A normal und $x \in B$ ganz über einem Ideal $\mathfrak{a}$ von A. Dann ist $x \in B \subset \operatorname{Quot}(B)$ offensichtlich algebraisch (= ganz) über $K = \operatorname{Quot}(A)$. Ist $T^n + a_1 T^{n-1} + \dots + a_n \in K[T]$ das Minimalpolynom von x über K, so liegen alle seine Koeffizienten a_i in $\sqrt{\mathfrak{a}}$.*

Beweis. Es gilt $K \subset \operatorname{Quot}(B)$ und $x \in \operatorname{Quot}(B)$. Betrachte den Zwischenkörper $K \subset K[x] \subset \operatorname{Quot}(B)$ (dass $K[x]$ ein Körper ist, folgt aus Proposition 7.2.1 oder ist wohlbekannt aus der Theorie der algebraischen Körpererweiterungen). Sei L ein Oberkörper von $K[x]$, in dem das Minimalpolyom $p(T) := T^n + a_1 T^{n-1} + \dots + a_n$ von x über K in Linearfaktoren zerfällt (etwa ein algebraischer Abschluss von $K[x]$), sagen wir
$$p(T) = (T - x_1)(T - x_2) \dots (T - x_n)$$

für geeignete $x_1 := x, x_2, \dots, x_n \in L$. Die Situation wird im folgenden kommutativen Diagramm illustriert.

$$\begin{array}{ccccccc}
B & \subset & \mathrm{Quot}(B) & & \\
 & & \cup & & \\
\cup & & K[x] & \subset & L \\
 & & \cup & & \\
A & \subset & K & = & \mathrm{Quot}(A)
\end{array}$$

Sei $f(T) \in A[T]$ ein normiertes Polynom mit Koeffizienten in $\mathfrak{a}$, so dass die $\mathfrak{a}$-Ganzheitsgleichung $f(x) = 0$ gilt. Dann gilt $p(T)|f(T)$ in $K[T]$. Als Nullstelle von p ist jedes x_i auch Nullstelle von $f(T)$ und damit ganz über $\mathfrak{a}$.

Wegen $p(T) = (T - x_1)(T - x_2) \dots (T - x_n)$ sind die Koeffizienten $a_1, \dots, a_n$ von $p = p(T)$ bis auf Vorzeichen Summen von endlichen Produkten der x_i und somit ganz über $\mathfrak{a}$ nach Lemma 7.3.4, angewandt auf $A \subset L$ (genauer sind die a_i bis auf Vorzeichen die elementarsymmetrischen Polynome ausgewertet bei $x_1, \dots, x_n$). Da A normal ist (also ganz abgeschlossen in K) und alle a_i in K liegen, liegen alle a_i in A. Genauer zeigt Lemma 7.3.4.(a), angewandt auf $A \subset K$, dass alle a_i in $\sqrt{\mathfrak{a}}$ liegen. □

7.3.6. Das folgende Korollar 7.3.7 ist nützlich, um etwa den ganzen Abschluss von $\mathbb{Z}$ in einer Körpererweiterung von $\mathbb{Q}$ zu berechnen (siehe Abschnitt 7.4).

Korollar 7.3.7. *Sei A ein normaler Integritätsbereich mit Quotientenkörper $K = \mathrm{Quot}(A)$. Sei $K \subset L$ eine Körpererweiterung. Dann ist ein Element $x \in L$ genau dann ganz über A, wenn es algebraisch über K ist und sein Minimalpolynom $\mathrm{Min}(x/K)$ über K in $A[T]$ enthalten ist:*

$$(\textit{ganzer Abschluss von } A \textit{ in } L) = \{x \in L \mid x \textit{ algebraisch über } K \textit{ mit } \mathrm{Min}(x/K) \in A[T]\}.$$

Beweis. Die Inklusion $\subset$ folgt aus Proposition 7.3.5 für $B = L$ und $\mathfrak{a} = A$. Die Inklusion $\supset$ ist trivial, denn das Minimalpolynom liefert eine Ganzheitsgleichung. □

7.3.8. Die folgende Proposition 7.3.9 hat nichts mit Ganzheit zu tun, wird aber im Beweis von Going-down (Satz 7.3.10) verwendet.

Proposition 7.3.9. *Sei $\varphi \colon A \to B$ ein Ringmorphismus und $f = \varphi^{-1} = \mathrm{Spec}\,\varphi \colon \mathrm{Spec}\,B \to \mathrm{Spec}\,A$ die induzierte Abbildung auf den Spektren. Ein Primideal $\mathfrak{p} \in \mathrm{Spec}\,A$ liegt genau dann im Bild von f, wenn $\mathfrak{p} = \varphi^{-1}(B\varphi(\mathfrak{p}))$ gilt (die Inklusion $\mathfrak{p} \subset \varphi^{-1}(B\varphi(\mathfrak{p}))$ gilt stets).*

Beweis. $\Rightarrow$: Sei $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ für ein $\mathfrak{q} \in \mathrm{Spec}\,B$. Es folgt $\varphi(\mathfrak{p}) \subset \mathfrak{q}$, also $B\varphi(\mathfrak{p}) \subset \mathfrak{q}$ und somit $\varphi^{-1}(B\varphi(\mathfrak{p})) \subset \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. Wegen der offensichtlichen Inklusion $\mathfrak{p} \subset \varphi^{-1}(B\varphi(\mathfrak{p}))$ erhalten wir die gewünschte Gleichheit.

$\Leftarrow$: Gelte $\mathfrak{p} = \varphi^{-1}(B\varphi(\mathfrak{p}))$. Wir erhalten somit eine Inklusion

$$\varphi' \colon A' := A/\mathfrak{p} \hookrightarrow B' := B/B\varphi(\mathfrak{p})$$

wobei A' ein Integritätsbereich ist. Es reicht zu zeigen, dass $(0) = \mathfrak{p}/\mathfrak{p}$ im Bild von $\mathrm{Spec}\,B' \to \mathrm{Spec}\,A'$ liegt.

Sei $K = \mathrm{Quot}(A')$ und betrachte das kommutative Diagramm

$$\begin{tikzcd}
A' \arrow[r, hook, "\varphi'"] \arrow[d, hook, "\kappa'"'] & B' \arrow[d, "\iota_{B'}"] \\
K' \arrow[r, "\iota_{K'}"] & K' \otimes_{A'} B'
\end{tikzcd}$$

Da K' ein flacher A'-Modul ist (Korollar 6.3.16) und φ' injektiv ist, ist $K' \xrightarrow{\sim} K' \otimes_{A'} A' \xrightarrow{\mathrm{id} \otimes \varphi'} K' \otimes_{A'} B'$ injektiv (und diese Verknüpfung ist die untere horizontale Abbildung). Insbesondere ist $K' \otimes_{A'} B'$ nicht der Nullring und enthält somit ein maximales Ideal $\mathfrak{m}$ (Satz 2.6.13). Dann ist $\iota_{B'}^{-1}(\mathfrak{m})$ das gesuchte Urbild von $0 \in \mathrm{Spec}\,A'$, denn es gilt (wir verwenden $\mathrm{Spec}\,K' = \{(0)\}$)

$$\varphi'^{-1}(\iota_{B'}^{-1}(\mathfrak{m})) = \kappa'^{-1}(\iota_{K'}^{-1}(\mathfrak{m})) = \kappa'^{-1}((0)) = (0).$$

□

Satz 7.3.10 (Going-down)**.** *Sei $A \subset B$ eine ganze Ringerweiterung. Sei B (und damit auch A) ein Integritätsbereich und sei A normal. Seien $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ eine Primidealkette in A und $\mathfrak{q}_{m+1} \subset \cdots \subset \mathfrak{q}_n$ eine Primidealkette in B mit $0 \leq m \leq n$, so dass $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $m+1 \leq i \leq n$ gilt. Dann läßt sich die zweite Kette zu einer Primidealkette $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m \subset \mathfrak{q}_{m+1} \subset \cdots \subset \mathfrak{q}_n$ in B erweitern mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $1 \leq i \leq n$.*

7.3.11. Die Voraussetzung, dass A normal ist, ist unabdingbar, siehe (privater) Anhang.

7.3.12. Hier ist die Illustration für $m = 2 < n = 4$. Going-down liefert den blauen Teil des Diagramms und erklärt den Namen des Satzes.

$$\begin{tikzcd}
\operatorname{Spec} B \arrow[d] & & \mathfrak{q}_1 \arrow[d, mapsto] & \subset & \mathfrak{q}_2 \arrow[d, mapsto] & \subset & \mathfrak{q}_3 \arrow[d, mapsto] & \subset & \mathfrak{q}_4 \arrow[d, mapsto] \\
\operatorname{Spec} A & & \mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & \mathfrak{p}_3 & \subset & \mathfrak{p}_4
\end{tikzcd}$$

Beweis. Es reicht offensichtlich, den Fall $m = 1 < n = 2$ zu beweisen. (Im Fall $1 \leq m = n$ gibt es nach Satz 7.2.6 ein Primideal $\mathfrak{q}_n \subset B$ mit $\mathfrak{q}_n \cap A = \mathfrak{p}_n$.)

Sei $\mathfrak{q} := \mathfrak{q}_2$. Betrachte das kommutative Diagramm

$$\begin{array}{ccccccccc}
 & & \mathfrak{q}_\mathfrak{q} & \subset & B_\mathfrak{q} & \subset & \operatorname{Quot}(B) & & \\
 & & \cup & & \cup & & & & \\
 & & \mathfrak{q} & \subset & B & & \cup & & \\
 & & \cup & & \cup & & & & \\
\mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & A & \subset & \operatorname{Quot}(A) & =: & K \\
 & & \| & & & & & & \\
 & & \mathfrak{q} \cap A & & & & & &
\end{array}$$

Es gilt $\mathfrak{q}_\mathfrak{q} \cap B = \mathfrak{q}$.

Es genügt nun zu zeigen, dass $\mathfrak{p}_1$ im Bild der Abbildung $\operatorname{Spec} B_\mathfrak{q} \to \operatorname{Spec} A$ liegt: Sei nämlich $\mathfrak{r} \in \operatorname{Spec} B_\mathfrak{q}$ mit $\mathfrak{r} \cap A = \mathfrak{p}_1$. Weil $B_\mathfrak{q}$ ein lokaler Ring mit (eindeutigem) maximalen Ideal $\mathfrak{q}_\mathfrak{q}$ ist, folgt $\mathfrak{r} \subset \mathfrak{q}_\mathfrak{q}$ und somit $\mathfrak{r} \cap B \subset \mathfrak{q}_\mathfrak{q} \cap B = \mathfrak{q}$. Das Primideal $\mathfrak{r} \cap B \in \operatorname{Spec} B$ ist also das gesuchte Urbild von $\mathfrak{p}_1$.

Nach Proposition 7.3.9, angewandt auf $A \hookrightarrow B_\mathfrak{q}$, bleibt also $B_\mathfrak{q}\mathfrak{p}_1 \cap A \subset \mathfrak{p}_1$ zu zeigen.

Sei $x \in B_\mathfrak{q}\mathfrak{p}_1$. Dann gibt es $y \in B\mathfrak{p}_1$ und $s \in B - \mathfrak{q}$ mit $x = \frac{y}{s}$. Lemma 7.3.4.(b) zeigt, dass $\sqrt{B\mathfrak{p}_1}$ der ganze Abschluss von $\mathfrak{p}_1$ in B ist. Insbesondere ist y ganz über $\mathfrak{p}_1$. Da A normal ist, zeigt Proposition 7.3.5, dass das Minimalpolynom von y über $K = \operatorname{Quot}(A)$ die Form

$$T^r + u_1 T^{r-1} + \cdots + u_r \in A[T]$$

hat mit $u_i \in \sqrt{\mathfrak{p}_1} = \mathfrak{p}_1$. Insbesondere erfüllt y die $\mathfrak{p}_1$-Ganzheitsgleichung

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0. \tag{7.3.1}$$

Nun nehmen wir zusätzlich an, dass $x = \frac{y}{s}$ in A liegt und $x \neq 0$ gilt. Somit gilt $x^{-1} \in K$, und wir folgern, das die Minimalpolynome über K der beiden Elemente y und $s = \frac{y}{x} = yx^{-1}$ in $\operatorname{Quot}(B)$ denselben Grad r haben. Teilen wir die Ganzheitsgleichung (7.3.1) durch x^r, so erhalten wir mit $v_i := \frac{u_i}{x^i} \in K$ die Gleichung

$$s^r + v_1 s^{r-1} + \cdots + v_r = 0 \tag{7.3.2}$$

in K. Das Minimalpolynom von s über K ist also $T^r + v_1 T^{r-1} + \cdots + v_r$. Da A normal ist und $s \in B - \mathfrak{q} \subset B$ ganz über A, zeigt Proposition 7.3.5 (mit $\mathfrak{a} = A$) $v_i \in \sqrt{A} = A$, so dass also (7.3.2) eine Ganzheitsgleichung von s über A ist.

Zu zeigen ist $x \in \mathfrak{p}_1$.

Nehmen wir $x \notin \mathfrak{p}_1$ an. Nach Definition der v_i gilt

$$x^i v_i = u_i \in \mathfrak{p}_1 \qquad \text{für alle } i = 1, \ldots, r.$$

Da $\mathfrak{p}_1$ prim ist (und $x \in A$ und $v_i \in A$ gelten), folgt $v_i \in \mathfrak{p}_1$ für alle $i = 1, \dots, r$. Die Ganzheitsgleichung (7.3.2) von $s \in B$ über A zeigt dann $s^r \in B\mathfrak{p}_1 \subset B\mathfrak{p}_2 \subset \mathfrak{q}$ und somit $s \in \mathfrak{q}$. Dies steht im Widerspruch zu $s \in B - \mathfrak{q}$.

Es muss also $x \in \mathfrak{p}_1$ gelten, was die gesuchte Inklusion $B_\mathfrak{q}\mathfrak{p}_1 \cap A \subset \mathfrak{p}_1$ zeigt. □

Aufgabe 7.3.13 (Geometrische Punkte liften entlang ganzer Morphismen)**.** eher schwierig [AM69, p. 67, Aufgabe 2] Sei $A \subset B$ eine ganze Ringerweiterung und sei $\varphi\colon A \to K$ ein Ringmorphismus, wobei K ein algebraisch abgeschlossener Körper ist. Zeigen Sie, dass man φ zu einem Ringmorphismus $B \to K$ ausdehnen kann.

Lösung auskommentiert

geometrischen(?) Punkt liften

Aufgabe 7.3.14. Seien $z_1, \dots, z_n \in \mathbb{C}$ gegeben und sei

$$A := \{a \in \mathbb{C}[T] \mid a(z_1) = \dots = a(z_n)\}$$

die Menge aller Polynome, die an den Punkte $z_1, \dots, z_n$ denselben Wert annehmen. Zeigen Sie, dass $A \subset \mathbb{C}[T]$ eine endliche Ringerweiterung ist.

Bonusaufgabe: Finden Sie im Fall $n = 2$ für $z_1 = 1$ und $z_2 = -1$ ein Polynom $f \in \mathbb{C}[X, Y]$, so dass $\mathbb{C}[X, Y]/(f) \xrightarrow{\sim} A$. Zeichnen Sie $\mathbf{V}(f) \subset \mathbb{C}^2$.

Aufgabe 7.3.15. Zeigen Sie, dass $\mathbb{C}[T^2, T^3] \subset \mathbb{C}[T]$ eine ganze Ringerweiterung ist. Zeigen Sie einen Isomorphismus $\mathbb{C}[X, Y]/(X^3 - Y^2) \xrightarrow{\sim} \mathbb{C}[T^2, T^3]$ von $\mathbb{C}$-Algebren.

Aufgabe 7.3.16. Seien A ein Ring und $f \in A[T]$ ein normiertes Polynom vom Grad m. Zeigen Sie, dass $A \to B := A[T]/(f)$ injektiv ist und eine ganze Ringerweiterung. Zeigen Sie, dass B ein freier A-Modul mit Basis $1, T, T^2, \dots, T^{m-1}$ ist

Aufgabe 7.3.17. Sei $A \subset B$ eine Ringerweiterung und $x \in B$ ganz über A. Sei $f \in A[T]$ eine Ganzheitsgleichung von minimalem Grad. Wir erhalten einen surjektiven Ringmorphismus $A[T] \twoheadrightarrow A[x]$, $p(T) \mapsto p(x)$. Ist dieser immer ein Isomorphismus?

Zeigen Sie: Ist A ein Körper, so ja. Im Allgemeinen nein, schon für A einen Hauptidealring kann dies schiefgehen.

Definition 7.3.18. nicht in Vorlesung gemacht Ein Morphismus von Ringen $\varphi\colon A \to B$ heißt ganz, falls $\varphi(A) \subset B$ eine ganze Ringerweiterung ist.

Aufgabe 7.3.19. Zeigen Sie, dass $\mathbb{C}[X] \to \mathbb{C}[X] \times \mathbb{C}$, $f = f(X) \mapsto (f(X), f(0))$, ganz ist (die Abbildung ist offensichtlich injektiv).

(Man kann dies auch aus den drei folgenden Aufgaben folgern.) Geben Sie eine Ganzheitsgleichung für das Element $(0, 1)$ an.

Aufgabe 7.3.20. Einfach kopiert von endlich. Stimmt alles?

Seine $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ Ringmorphismen. Zeigen Sie:

(a) Sind φ und ψ ganz, so ist auch $\psi\varphi$ ganz.
(b) Ist $\psi\varphi$ ganz, so ist auch ψ ganz.
(c) Surjektive Ringmorphismen sind ganz.
(d) Folgern Sie: Ist $\varphi\colon A \to B$ ganz und ist $\mathfrak{b} \subset B$ ein Ideal, so ist der induzierte (injektive) Ringmorphismus $A/\varphi^{-1}\mathfrak{b} \to B/\mathfrak{b}$ ganz.

Aufgabe 7.3.21. Sei A ein Ring und D das Bild des „diagonalen“ Ringmorphismus $\Delta\colon A \to A \times A$, $a \mapsto (a, a)$. Dann ist $D \subset A$ eine ganze Ringerweiterung (mit anderen Worten ist Δ ganz).

Finden Sie explizit für ein beliebiges Element $(a, b) \in A \times A$ eine Ganzheitsgleichung über D.

Aufgabe 7.3.22. Sind $\varphi_1\colon A_1 \to B_1$ und $\varphi_2\colon A_2 \to B_2$ ganz, so ist auch $\varphi_1 \times \varphi_2\colon A_1 \times A_2 \to B_1 \times B_2$ ganz.

Aufgabe 7.3.23. Sei $\varphi\colon A \to B$ ganz und sei $\psi\colon A \to C$ ein Ringmorphismus. Zeigen Sie, dass $C \to B \otimes_A C$ ganz ist.

7.4. **Ganzer Abschluss für quadratische Zahlkörper.** Wir erklären nun einige der Behauptungen in Abschnitt 1.3.

Definition 7.4.1. Eine ganze Zahl d heißt **quadratfrei**, falls sie durch keine Quadratzahl > 1 teilbar ist: Aus $n^2|d$ für $n \in \mathbb{N}$ folgt $n = 1$.

7.4.2. Die Null ist nicht quadratfrei. Jedes $0 \neq d' \in \mathbb{Z}$ kann eindeutig als $d' = m^2 d$ mit quadratfreiem d und $m \in \mathbb{N}_{>0}$ geschrieben werden. Dann gilt $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$.

Proposition 7.4.3. *Sei $d \in \mathbb{Z}$ quadratfrei. Betrachte die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$. Dann ist der ganze Abschluss R von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ wie folgt gegeben:*

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d = 2, 3 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d = 1 \mod 4. \end{cases} \tag{7.4.1}$$

(Dies deckt alle Fälle ab, denn d ist nicht durch 4 teilbar.)

7.4.4. Hier bezeichnet $\mathbb{Q}(\sqrt{d})$ einen Zerfällungskörper des Polynoms $T^2 - d$ über $\mathbb{Q}$, und das Element $\sqrt{d}$ ist eine beliebig gewählte Quadratwurzel in einem solchen Zerfällungskörper. In der Regel stellt man sich $\mathbb{Q}(\sqrt{d})$ als Teilkörper von $\mathbb{C}$ vor. Ist $d > 0$, so mag man annehmen, dass $\sqrt{d}$ die positive Wurzel aus d bezeichnet. Ist $d < 0$, so mag man annehmen, dass $\sqrt{d}$ die Wurzel aus d mit positivem Imaginärteil ist.

Beispiele 7.4.5. (a) Für $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ erhält man $R = \mathbb{Z}[i]$ den Ring der Gaußschen Zahlen.

(b) Für $K = \mathbb{Q}(\sqrt{-3})$ gilt $R = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Es ist $\omega := -\frac{1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel (und $-\omega = \frac{1+\sqrt{-3}}{2}$ ist eine primitive sechste Einheitswurzel). Also ist $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ der dritte und der sechste Kreisteilungskörper.

Der Ring $R = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\omega]$ heißt der **Ring der Eisensteinzahlen**. Anschaulich ist er durch das „Dreiecksgitter“ $\mathbb{Z} \oplus \mathbb{Z}\omega$ in der komplexen Zahlenebene $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ gegeben.

Zeichnung? 1 adaptieren.

(c) Für $K = \mathbb{Q}(\sqrt{3})$ gilt $R = \mathbb{Z}[\sqrt{3}]$.

(d) Für $K = \mathbb{Q}(\sqrt{5})$ gilt $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Mitwoch, 11. Januar

Beweis. Gilt $d = 1$, so ist die Aussage offensichtlich richtig, denn $\sqrt{d} \in \pm 1$ und $\frac{1+\sqrt{d}}{2} \in \{0, 1\}$.

Wir nehmen im Folgenden an, dass $d \neq 1$ gilt. Dann hat die Körpererweiterung $\mathbb{Q} \subset L := \mathbb{Q}(\sqrt{d})$ Grad zwei: Weil $\sqrt{d}$ Nullstelle von $T^2 - d \in \mathbb{Z}[T]$ ist, ist ihr Grad ≤ 2, und $\sqrt{d}$ ist ganz über $\mathbb{Z}$. Nehmen wir an, dass der Grad eins ist, so gilt $\sqrt{d} \in \mathbb{Q}$. Da $\mathbb{Z}$ normal ist (Proposition 7.1.13), folgt daraus $\sqrt{d} \in \mathbb{Z}$. Also ist $\sqrt{d}^2 = d \neq 1$ eine Quadratzahl > 1 im Widerspruch zur Annahme, dass d quadratfrei ist.

Sei $x = a + b\sqrt{d} \in L - \mathbb{Q}$, mit $a \in \mathbb{Q}$ und $b \in \mathbb{Q} - \{0\}$. Dann ist

$$T^2 - 2aT + (a^2 - b^2 d) = (T - x)(T - (a - b\sqrt{d})) \in \mathbb{Q}[T] \tag{7.4.2}$$

das Minimalpolynom von x über $\mathbb{Q}$. Nach Korollar 7.3.7 gilt also $x \in R$ genau dann, wenn die beiden Bedingungen

$$\begin{gathered} 2a \in \mathbb{Z}, \\ a^2 - b^2 d \in \mathbb{Z} \end{gathered} \tag{7.4.3}$$

gelten. Daraus folgt sofort

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \subset R. \tag{7.4.4}$$

Setzen wir $a' := 2a \in \mathbb{Q}$ und $b' := 2b \in \mathbb{Q} - \{0\}$, so sind die beiden Bedingungen (7.4.3) äquivalent zu

$$\begin{gathered} a' \in \mathbb{Z}, \\ a'^2 - b'^2 d \in 4\mathbb{Z}. \end{gathered} \tag{7.4.5}$$

Wir nehmen nun $x \in R$ an, so dass also all diese Bedingungen gelten. Wir behaupten, dass $b' \in \mathbb{Z}$ gilt.

Die beiden Bedingungen (7.4.5) zeigen $b'^2 d \in \mathbb{Z}$. Schreiben wir $b' = \pm \prod_{p \text{ prim}} p^{v_p}$ mit $v_p \in \mathbb{Z}$, fast alle Null, und $d = \pm \prod_{p \text{ prim}} p^{w_p}$ mit $w_p \in \{0,1\}$ (da $d \in \mathbb{Z}$ quadratfrei), fast alle Null, so folgt für alle Primzahlen p, dass $2v_p + w_p \geq 0$ gilt. Also sind alle $v_p \geq 0$, d. h. $b' \in \mathbb{Z}$.

Somit wissen wir, dass a' und b' ganze Zahlen sind, die

$$\overline{a}'^2 = \overline{d}\, \overline{b}'^2 \quad \text{in } \mathbb{Z}/4\mathbb{Z} \tag{7.4.6}$$

erfüllen.

Weil die Quadrate in $\mathbb{Z}/4$ genau $0 = 0^2 = 2^2$ und $1 = 1^2 = 3^2$ sind, erhalten wir:

- Im Fall $\overline{d} = 2, 3 \mod 4$ muss $\overline{a}'^2 = \overline{b}'^2 = 0$ gelten (denn $0 \neq d1$, $1 \neq d0$, $1 \neq d1$), also $a', b' \in 2\mathbb{Z}$. Damit folgt $a = \frac{1}{2}a' \in \mathbb{Z}$ und $b = \frac{1}{2}b' \in \mathbb{Z}$, also $x = a + b\sqrt{d} \in \mathbb{Z} \cdot 1 + \mathbb{Z}\sqrt{d} = \mathbb{Z}[\sqrt{d}]$, und wir erhalten $R \subset \mathbb{Z}[\sqrt{d}]$. Zusammen mit der trivialen Inklusion (7.4.4) zeigt dies $R = \mathbb{Z}[\sqrt{d}]$.
- Im Fall $\overline{d} = 1 \mod 4$ muss $\overline{a}'^2 = \overline{b}'^2$ gelten, also $a' - b' \in 2\mathbb{Z}$, oder, mit anderen Worten, $(a', b') \in (2\mathbb{Z} \times 2\mathbb{Z}) \cup ((1,1) + (2\mathbb{Z} \times 2\mathbb{Z}))$. Dies impliziert

$$(a, b) \in (\mathbb{Z} \times \mathbb{Z}) \cup ((\frac{1}{2}, \frac{1}{2}) + (\mathbb{Z} \times \mathbb{Z})) = \mathbb{Z}v + \mathbb{Z}w,$$

wobei $v := (1, 0)$ und $w := (\frac{1}{2}, \frac{1}{2})$ und die Gleichheit eine Gleichheit von Teilmengen (oder abelschen Untergruppen) von $\mathbb{Q}^2$ ist, vergleiche Abbildung 1 (man überprüfe diese Gleichheit).

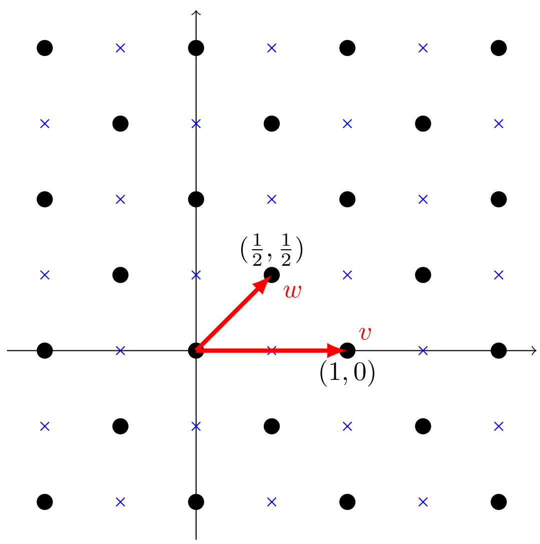


Abbildung 1. Die schwarzen Kreise sind die $\mathbb{Z}$-Linearkombinationen von v und w in $\mathbb{Q}^2$.

Aus dem $\mathbb{Q}$-Vektorraumisomorphismus $\mathbb{Q}^2 \xrightarrow{\sim} L$, $(\alpha, \beta) \mapsto \alpha + \beta\sqrt{d}$, der $v \mapsto 1$ und $w \mapsto \frac{1+\sqrt{d}}{2}$ erfüllt, folgt nun die erste Inklusion in

$$R \subset \mathbb{Z} \cdot 1 + \mathbb{Z}\frac{1+\sqrt{d}}{2} \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}],$$

die zweite Inklusion ist offensichtlich. Nach (7.4.2) (der per Rechnung) ist das Minimalpolynom von $\frac{1+\sqrt{d}}{2}$ durch

$$T^2 - T + \frac{1-d}{4}$$

gegeben und hat wegen der Annahme $\overline{d} = 1$ in $\mathbb{Z}/4$ Koeffizienten in $\mathbb{Z}$. Also ist $\frac{1+\sqrt{d}}{2}$ ganz über $\mathbb{Z}$, und somit gilt $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset R$ (nach Korollar 7.1.11). Es folgt die Behauptung $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

□

Proposition 7.4.6. *Sei $d \in \mathbb{Z}$ quadratfrei mit $d = 2, 3 \mod 4$. Betrachte die Ringerweiterung $A := \mathbb{Z} \subset B := \mathbb{Z}[\sqrt{d}]$ (vgl. Proposition 7.4.3) und den assoziierten Morphismus*

$$f\colon \operatorname{Spec} B \to \operatorname{Spec} A.$$

Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist die Faser von f über dem maximalen Ideal $Ap = p\mathbb{Z}$ wie folgt gegeben:

(a) *Ist d kein Quadrat modulo p (dies impliziert[20] $p \nmid d$ und $p \neq 2$), so ist Bp ein Primideal und es gilt*

$$f^{-1}(Ap) = \{Bp\}.$$

(Es it Ap „unverzweigt“ mit „Trägheitsgrad“ 2 bei Bp.)

(b) *Ist d ein Quadrat modulo p und gelten $p \nmid d$ und $p \neq 2$, so wähle man $\delta \in \mathbb{Z}$ mit $\overline{\delta}^2 = \overline{d}$ in $\mathbb{Z}/p$. Dann sind $\mathfrak{q}_- := B(\sqrt{d} - \delta) + Bp$ und $\mathfrak{q}_+ := B(\sqrt{d} + \delta) + Bp$ verschiedene Primideale[21] und es gilt*

$$f^{-1}(Ap) = \{\mathfrak{q}_-, \mathfrak{q}_+\}.$$

Es sind $\mathfrak{q}_-$ und $\mathfrak{q}_+$ relativ koprim und es gilt $Bp = \mathfrak{q}_- \cdot \mathfrak{q}_+$.
(Es ist Ap „unverzweigt“ mit „Trägheitsgrad“ 1 sowohl bei $\mathfrak{q}_-$ als auch bei $\mathfrak{q}_+$.)

(c) *Gelten $p \mid d$ oder $p = 2$ (dann ist d Null modulo p und somit ein Quadrat), so ist*

$$\mathfrak{q} := \begin{cases} B\sqrt{d} + Bp & \text{falls } p \mid d, \\ B(\sqrt{d} + 1) + B2 & \text{falls } p = 2 \nmid d. \end{cases}$$

ein Primideal und es gilt

$$f^{-1}(Ap) = \{\mathfrak{q}\}.$$

(Genauer gilt $Bp = \mathfrak{q}^2$. Es ist Ap „verzweigt“ mit „Verzweigungsindex“ 2 und „Trägheitsgrad“ 1 bei $\mathfrak{q}$.)

7.4.7. Der Vollständigkeit halber sei bemerkt, dass $f^{-1}((0)) = \{(0)\}$ gilt. Dies folgt aus Korollar 7.2.5 (und benötigt nur, dass $A \subset B$ eine ganze Erweiterung von Integritätsbereichen ist).

7.4.8. Für fixiertes d tritt der Fall (c) nur für endlich viele Primzahlen p ein, nämlich für die Primteiler von d und für 2.
(Der Morphismus $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ verzweigt also nur an endlich vielen Punkten von $\operatorname{Spec} A$.)

Beispiel 7.4.9. Wir betrachten die Ringerweiterung $A = \mathbb{Z} \subset B = \mathbb{Z}[i]$ und die zugehörige Abbildung $f\colon \operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$. Wir bestimmen mit Proposition 7.4.6, für $d = -1 \equiv 3 \mod 4$, die Faser von f über dem Primideal $p\mathbb{Z}$, für einige Primzahlen p. Veranschauliche Primideale der Fasern im Zahlengitter.

- $p = 2$: Wir sind im Fall (c) und im Unterfall $p = 2 \nmid d = -1$. Die Faser besteht genau aus dem Primideal $B(1 + i) + B2 = B(1 + i) = \mathbb{Z}[i](1 + i)$. Hier kann man $B2$ wegen $-i(1 + i)^2 = (-i)2i = 2$ weglassen.
- $p = 3$: Es ist $d = -1 \equiv 2$ modulo $p = 3$ kein Quadrat, wir sind also im Fall (a) und die Faser besteht genau aus dem Primideal $3\mathbb{Z}[i]$.
- $p = 5$: Es ist $d = -1 \equiv 4$ modulo $p = 5$ ein Quadrat und $2 \neq p = 5 \nmid -1$. Wir sind also im Fall (b). Die Faser besteht aus den beiden Primidealen (wir nehmen $\delta = 2$)

$$B(2 - i) + B5 = \mathbb{Z}[i](2 - i),$$
$$B(2 + i) + B5 = \mathbb{Z}[i](2 + i).$$

Hier verwenden wir $(2 + i)(2 - i) = 5$.

Beweis. Wir behaupten

$$f^{-1}(Ap) = \operatorname{Spec}(B/Bp), \tag{7.4.7}$$

wobei wir $\operatorname{Spec}(B/Bp)$ mit der Teilmenge $\mathcal{V}(Bp)$ aller Primideale $\mathfrak{q} \in \operatorname{Spec} B$ identifizieren, die Bp enthalten (Proposition 2.11.17).

$\subset$: Sei $\mathfrak{q} \in \operatorname{Spec} B$ mit $f(\mathfrak{q}) = A \cap \mathfrak{q} = Ap$. Es folgt $p \in \mathfrak{q}$ und somit $Bp \subset \mathfrak{q}$.

[20] Gilt $p \mid d$, so ist d Null modulo p und somit ein Quadrat. Gilt $p = 2$, so sind alle Elemente von $\mathbb{Z}/p = \mathbb{Z}/2$ Quadrate.
[21] Für eine andere Wahl von δ bekommt man bis auf Vertauschung dieselben Ideale.

$\supset$: Sei $\mathfrak{q} \in \operatorname{Spec} B$ mit $Bp \subset \mathfrak{q}$. Dann folgt $Ap \subset A \cap Bp \subset A \cap \mathfrak{q}$. Da $Ap = p\mathbb{Z}$ ein maximales Ideal in $A = \mathbb{Z}$ ist und $A \cap \mathfrak{q}$ ein echtes (da primes) Ideal, folgt Gleichheit $Ap = A \cap Bp = A \cap \mathfrak{q} = f(\mathfrak{q})$.

Einige formal unnötige Bemerkungen: Da Ap maximal ist, sind alle Elemente von $f^{-1}(Ap)$ maximale Ideale in B (oder B/Bp) (Korollar 7.2.4). Wir können also (7.4.7) zu

$$f^{-1}(Ap) = \operatorname{MaxSpec}(B/Bp) \tag{7.4.8}$$

präzisieren (zwischen verschiedenen Elementen der Faser $f^{-1}(Ap)$ gibt es insbesondere keine Inklusionen; dies folgt auch aus Korollar 7.2.5). Außerdem ist die Faser $f^{-1}(Ap)$ nicht leer (Satz 7.2.6), es gilt also $Bp \subsetneq B$.

Wir identifizieren $\mathbb{Z}[X]/(X^2 - d) = B$ via $X \mapsto \sqrt{d}$. Es gilt dann (mit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$)

$$B/Bp = \mathbb{Z}[X]/(X^2 - d, p) = \mathbb{F}_p[X]/(X^2 - \overline{d}). \tag{7.4.9}$$

(a): Die Annahme, dass $\overline{d}$ kein Quadrat in $\mathbb{F}_p$ ist, ist äquivalent zur Aussage, dass $X^2 - \overline{d}$ irreduzibel in $\mathbb{F}_p[X]$ ist. Äquivalent ist $(X^2 - \overline{d})$ ein maximales Ideal in $\mathbb{F}_p[X]$ (Beispiel 2.6.4). Äquivalent ist B/Bp ein Körper nach (7.4.9) (er hat p^2 Elemente, ist also isomorph zu $\mathbb{F}_{p^2}$). Also besteht $\operatorname{Spec}(B/Bp)$ nur aus dem (maximalen) Nullideal, und es folgt $f^{-1}(Ap) = \{Bp\}$ nach (7.4.7).

Wir nehmen nun an, dass d ein Quadrat modulo p ist. Wir sind also im Fall (b) oder im Fall (c). Sei $\delta \in \mathbb{Z}$ mit $\overline{\delta}^2 = \overline{d}$ in $\mathbb{F}_p$. In $\mathbb{F}_p[X]$ gilt $X^2 - \overline{d} = (X - \overline{\delta})(X + \overline{\delta})$. Die beiden Faktoren sind verschieden oder gleich, was uns auf die beiden Fälle (b) und (c) führt. Die folgenden Bedingungen sind nämlich äquivalent:

- die beiden Faktoren $X - \overline{\delta}$ und $X + \overline{\delta}$ sind gleich,
- $\overline{\delta} = -\overline{\delta}$ in $\mathbb{F}_p$,
- $\overline{2}\,\overline{\delta} = 0$ in $\mathbb{F}_p$,
- $p = 2$ oder $\overline{\delta} = 0$,
- $p = 2$ oder $\overline{d} = \overline{\delta}^2 = 0$,
- $p = 2$ oder $p \mid d$ (das ist die Bedingung in (c)).

Fall (b): Die beiden Ideale $(X - \overline{\delta})$ und $(X + \overline{\delta})$ in $\mathbb{F}_p[X]$ sind relativ prim wegen $(X - \overline{\delta}) - (X + \overline{\delta}) = -\overline{2}\,\overline{\delta} \neq 0$, und ihr Produkt ist $(X^2 - \overline{d})$. Der Chinesische Restsatz 2.10.5 liefert den Isomorphismus

$$\frac{\mathbb{F}_p[X]}{(X^2 - \overline{d})} \xrightarrow{\sim} \frac{\mathbb{F}_p[X]}{(X - \overline{\delta})} \times \frac{\mathbb{F}_p[X]}{(X + \overline{\delta})} \xrightarrow[\sim]{(X,X) \mapsto (\overline{\delta}, -\overline{\delta})} \mathbb{F}_p \times \mathbb{F}_p.$$

Die Primideale der rechten Seite sind genau die Ideale $(0) \times \mathbb{F}_p$ und $\mathbb{F}_p \times (0)$ (siehe Aufgabe 7.4.11 für die allgemeine Ausage). Sie sind relativ koprim und ihr Schnitt ist das Nullideal. Also besteht $\operatorname{Spec}(\mathbb{F}_p[X]/(X^2 - \overline{d}))$ genau aus den beiden relativ koprimen Primidealen $(X - \overline{\delta})$ und $(X + \overline{\delta})$ mit trivialem Schnitt. Ihre Urbilder unter

$$B \twoheadrightarrow B/Bp \xrightarrow[\sim]{(7.4.9)} \mathbb{F}_p[X]/(X^2 - \overline{d})$$

sind offensichtlich genau die beiden Ideale $\mathfrak{q}_- = B(X - \delta) + Bp$ und $\mathfrak{q}_+ = B(X + \delta) + Bp$, die somit prim und relativ koprim sind und deren Schnitt gerade Bp ist; es folgt $Bp = \mathfrak{q}_- \cap \mathfrak{q}_+ = \mathfrak{q}_- \cdot \mathfrak{q}_+$ (Proposition 2.10.4). Aus (7.4.7) erhalten wir $f^{-1}(Ap) = \{\mathfrak{q}_-, \mathfrak{q}_+\}$. Als echte Ideale, die relativ koprim sind, sind $\mathfrak{q}_-$ und $\mathfrak{q}_+$ verschieden.

Fall (c): Wir nehmen im Folgenden ohne Einschränkung an, dass

$$\delta = \begin{cases} 0 & \text{falls } p \mid d, \\ 1 & \text{falls } p = 2 \nmid d, \end{cases}$$

gilt, denn damit gilt $\overline{\delta}^2 = \overline{d}$ in $\mathbb{F}_p$. Dann gilt $\mathfrak{q} = B(X + \delta) + Bp$.

Lemma 7.4.10. *wohin?*

Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal, das nur aus nilpotenten Elementen besteht (zum Beispiel das Nilradikal). Dann liefert $R \twoheadrightarrow R/\mathfrak{a}$ eine bijektive Abbildung

$$\operatorname{Spec}(R/\mathfrak{a}) \xrightarrow{\sim} \operatorname{Spec} R.$$

Insbesondere gilt $\operatorname{Spec}(R/\operatorname{Nil}(R)) \xrightarrow{\sim} \operatorname{Spec} R$.

Beweis. Die Abbildung $\operatorname{Spec}(R/\mathfrak{a}) \to \operatorname{Spec} R$ ist injektiv, und ein Primideal $\mathfrak{p} \in \operatorname{Spec} R$ liegt genau dann in ihrem Bild, wenn $\mathfrak{a} \subset \mathfrak{p}$ gilt (Proposition 2.11.17). Diese Inklusion gilt aber stets: Für $a \in \mathfrak{a}$ gilt $a^n = 0$ für geeginetes $n \in \mathbb{N}$, also $a^n \in \mathfrak{p}$ und damit $a \in \mathfrak{p}$. □

Wegen $(X-\overline{\delta})^2 = (X-\overline{\delta})(X+\overline{\delta}) = X^2 - \overline{d}$ in $\mathbb{F}_p[X]$ ist $X - \overline{\delta}$ als Element von $\mathbb{F}_p[X]/(X^2-\overline{d})$ nilpotent, und somit liefert

$$\mathbb{F}_p[X]/(X^2-\overline{d}) \twoheadrightarrow \mathbb{F}_p[X]/(X-\overline{\delta}) \xrightarrow[\sim]{X \mapsto \overline{\delta}} \mathbb{F}_p$$

nach Lemma 7.4.10 eine Bijektion auf den Spektren. Rechts steht ein Körper. Das Spektrum der linken Seite besteht somit genau aus dem Primideal $(X-\overline{\delta}) = (X+\overline{\delta})$. Sein Urbild unter

$$B \twoheadrightarrow B/Bp \xrightarrow[\sim]{(7.4.9)} \mathbb{F}_p[X]/(X^2-\overline{d}) \tag{7.4.10}$$

ist $\mathfrak{q}$. Aus (7.4.7) folgt $f^{-1}(Ap) = \{\mathfrak{q}\}$.

Ab hier nicht in Vorlesung machen, nur Zusatzinfo, interessant für algebraische Zahlentheorie bzw. Theorie von Dedekindringen.

Es bleibt $Bp = \mathfrak{q}^2$ zu zeigen.

$\supset$: Das Ideal $\mathfrak{q}^2$ geht unter (7.4.10) auf das Ideal $(X-\overline{\delta})\cdot(X-\overline{\delta}) = (X^2-\overline{d}) = (0)$. Es folgt $\mathfrak{q}^2 + Bp = Bp$, also $\mathfrak{q}^2 \subset Bp$.

$\subset$: Zu zeigen ist $p \in \mathfrak{q}^2$.

- Fall $p \mid d$: Dann gilt $\mathfrak{q} = BX + Bp = B\sqrt{d} + Bp$ und $\mathfrak{q}^2 = Bd + Bp\sqrt{d} + Bp^2$. Weil d quadratfrei ist, folgt $\operatorname{ggT}(d, p^2) = p$ und somit $p \in \mathbb{Z}p = \mathbb{Z}d + \mathbb{Z}p^2 \subset Bd + Bp^2 \subset \mathfrak{q}^2$.
- Fall $p = 2 \nmid d$: Es gilt $\mathfrak{q} = B(X+1) + Bp = B(\sqrt{d}+1) + B2$. Also ist $\mathfrak{q}^2$ von den drei Elementen $d + 1 + 2\sqrt{d}$ und $2(\sqrt{d}+1)$ und 4 erzeugt. Wir erhalten
$$d - 1 = d + 1 + 2\sqrt{d} - 2(\sqrt{d}+1) \in \mathfrak{q}^2.$$
Wir behaupten $\operatorname{ggT}(4, d-1) = 2$. Wegen $2 \nmid d$ ist $d-1$ gerade. Wäre $d-1$ durch 4 teilbar, so wäre $d = 1 \mod 4$ im Widerspruch zur Annahme $d = 2, 3 \mod 4$. Es folgt $\operatorname{ggT}(4, d-1) = 2$ und somit $p = 2 \in 2\mathbb{Z} = (d-1)\mathbb{Z} + 4\mathbb{Z} \subset \mathfrak{q}^2$.

□

Aufgabe 7.4.11. Sind A und B Ringe, so ist

$$\begin{gathered}(\operatorname{Spec} A) \sqcup (\operatorname{Spec} B) \xrightarrow{\sim} \operatorname{Spec}(A \times B), \\ \operatorname{Spec} A \ni \mathfrak{p} \mapsto \mathfrak{p} \times B, \\ \operatorname{Spec} B \ni \mathfrak{q} \mapsto A \times \mathfrak{q},\end{gathered}$$

eine Bijektion [22] von Mengen.

Proposition 7.4.12. *Nicht in Vorlesung machen: Bis auf die Beobachtung (7.4.12) für $p \neq 2$ enthält der Beweis keine neue Idee, sondern nur nervige Fallunterscheidungen.*

Sei $1 \neq d \in \mathbb{Z}$ quadratfrei mit $d = 1 \mod 4$. Betrachte die Ringerweiterung $A := \mathbb{Z} \subset B := \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ (vgl. Proposition 7.4.3) und den assoziierten Morphismus

$$f\colon \operatorname{Spec} B \to \operatorname{Spec} A.$$

Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist die Faser von f über dem maximalen Ideal $Ap = p\mathbb{Z}$ wie folgt gegeben:

(a) Ist d kein Quadrat modulo p (dies impliziert[23] $p \nmid d$ und $p \neq 2$), so ist Bp ein Primideal und es gilt
$$f^{-1}(Ap) = \{Bp\}.$$
(Es it Ap „unverzweigt“ mit „Trägheitsgrad“ 2 bei Bp.)

[22] Sie ist induziert durch die Projektionen $A \times B \to A$ und $A \times B \to B$ und sogar ein Isomorphismus von topologischen Räumen (= ein Homöomorphismus).

[23] Gilt $p \mid d$, so ist d Null modulo p und somit ein Quadrat. Gilt $p = 2$, so sind alle Elemente von $\mathbb{Z}/2\mathbb{Z}$ Quadrate.

(b) Ist d ein Quadrat modulo p und gelten $p \nmid d$ und $p \neq 2$, so wähle man $\delta \in \mathbb{Z}$ mit $\overline{\delta}^2 = \overline{d}$ in $\mathbb{Z}/p$. Dann sind $\mathfrak{q}_- := B(\sqrt{d} - \delta) + Bp$ und $\mathfrak{q}_+ := B(\sqrt{d} + \delta) + Bp$ verschiedene Primideale[24] *und es gilt*

$$f^{-1}(Ap) = \{\mathfrak{q}_-, \mathfrak{q}_+\}.$$

Es sind $\mathfrak{q}_-$ und $\mathfrak{q}_+$ relativ koprim und es gilt $Bp = \mathfrak{q}_- \cdot \mathfrak{q}_+$.
(Es ist Ap „unverzweigt“ mit „Trägheitsgrad“ 1 sowohl bei $\mathfrak{q}_-$ als auch bei $\mathfrak{q}_+$.)

(c) Gelten $2 \neq p \mid d$ (dann ist d Null modulo p und somit ein Quadrat), so ist $\mathfrak{q} := B\sqrt{d} + Bp$ ein Primideal und es gilt

$$f^{-1}(Ap) = \{\mathfrak{q}\}.$$

(Genauer gilt $Bp = \mathfrak{q}^2$. Es ist Ap „verzweigt“ mit „Verzweigungsindex“ 2 und „Trägheitsgrad“ 1 bei $\mathfrak{q}$.)

(d) Gelten $p = 2$ und $\frac{d-1}{4}$ ungerade (d. h. $d = 5 \mod 8$), so ist Bp ein Primideal und es gilt

$$f^{-1}(Ap) = \{Bp\}.$$

(Es it Ap „unverzweigt“ mit „Trägheitsgrad“ 2 bei Bp.)

(e) Gelten $p = 2$ und $\frac{d-1}{4}$ gerade (d. h. $d = 1 \mod 8$), so sind $\mathfrak{r}_1 := B\frac{1+\sqrt{d}}{2} + B2$ und $\mathfrak{r}_2 := B\frac{3+\sqrt{d}}{2} + B2$ verschiedene Primideale und es gilt

$$f^{-1}(Ap) = \{\mathfrak{r}_1, \mathfrak{r}_2\}.$$

Es sind $\mathfrak{r}_1$ und $\mathfrak{r}_2$ relativ koprim und es gilt $Bp = \mathfrak{r}_1 \cdot \mathfrak{r}_2$
(Es ist Ap „unverzweigt“ mit „Trägheitsgrad“ 1 sowohl bei $\mathfrak{r}_1$ als auch bei $\mathfrak{r}_2$.)

Beweis. Wegen $d \neq 1$ und

$$\Big(\frac{1+\sqrt{d}}{2}\Big)^2 = \frac{1+d+2\sqrt{d}}{4} = \frac{1+\sqrt{d}}{2} - \underbrace{\frac{1-d}{4}}_{\in \mathbb{Z}}$$

können wir $\mathbb{Z}[Y]/(Y^2 - Y + \frac{1-d}{4})$ via $\overline{Y} \mapsto \frac{1+\sqrt{d}}{2}$ identifizieren. Es gilt dann

$$B/Bp = \mathbb{Z}[Y]/(Y^2 - Y + \tfrac{1-d}{4}, p) = \mathbb{F}_p[Y]/(Y^2 - Y + \tfrac{1-d}{4}). \tag{7.4.11}$$

Wir nehmen zunächst an, dass $p \neq 2$. Dann ist 2 in $\mathbb{F}_p$ invertierbar und wir erhalten einen Isomorphismus

$$\begin{aligned} \frac{\mathbb{F}_p[Y]}{(Y^2 - Y + \frac{1-d}{4})} &\xrightarrow{\sim} \frac{\mathbb{F}_p[X]}{(X^2 - d)}, \\ Y &\mapsto 2^{-1}(X+1), \\ 2Y - 1 &\leftarrow\!\shortmid X, \end{aligned} \tag{7.4.12}$$

von Ringen (wie man leicht prüft). Die Fälle (a), (b), (c) kann man nun genauso wie die analogen Fälle im Beweis von Proposition 7.4.6 abhandeln. Man beachte, dass die beiden Ideale $(X \pm \delta)$ im Ring auf der rechten Seite von (7.4.12) den Idealen $(2Y - 1 \pm \delta)$ im Ring auf der linken Seite entsprechen, und dass deren Urbilder in B die Ideale

$$B \cdot (2\frac{1+\sqrt{d}}{2} - 1 \pm \delta) + Bp = B(\sqrt{d} \pm \delta) + Bp$$

sind.

Nun behandeln wir den Fall $p = 2$. Wegen (7.4.11) erhalten wir

$$B/Bp = \mathbb{F}_2[Y]/(Y^2 + Y + \tfrac{1-d}{4}).$$

Wir erinnern daran, dass $1 - d \in 4\mathbb{Z}$. Es folgt also $d \equiv 1, 5 \mod 8$.

- Fall $d \in 5 + 8\mathbb{Z}$. Dann gilt $\frac{1-d}{4} = 1$ in $\mathbb{F}_2$, und somit ist $Y^2 + Y + \frac{1-d}{4} = Y^2 + Y + 1$ irreduzibel in $\mathbb{F}_2[Y]$ (da es keine Nullstelle in $\mathbb{F}_2$ hat). Also ist B/Bp ein Körper mit 4 Elementen, Bp ist ein maximales Ideal, und es folgt $f^{-1}(Ap) = Bp$.

[24] Für eine andere Wahl von δ bekommt man bis auf Vertauschung dieselben Ideale.

- Fall $d \in 1+8\mathbb{Z}$. Dann gilt $\frac{1-d}{4} = 0$ in $\mathbb{F}_2$. Der Chinesische Restsatz 2.10.5, angewandt auf die relativ koprimen Ideale Y und $Y+1$, liefert
$$B/Bp = \mathbb{F}_2[Y]/(Y^2+Y) \xrightarrow{\sim} \frac{\mathbb{F}_2[Y]}{(Y)} \times . \frac{\mathbb{F}_2[Y]}{(Y+1)} \xrightarrow{\sim} \mathbb{F}_2 \times \mathbb{F}_2.$$
Somit besteht $\operatorname{Spec} B/Bp$ genau aus den beiden relativ koprimen Primidealen (Y) und $(Y+1)$. Nun schließe man man wie im Beweis von (b).

□

7.5. **Endliche Morphismen.**

Definition 7.5.1. Ein Morphismus $A \to B$ von Ringen heißt **endlich**, falls B ein endlich erzeugter A-Modul ist. Man sagt auch, dass B **endlich über** A ist.

7.5.2. Vor allem interessieren wir uns für injektive endliche Ringmorphismen, die man auch als endliche Ringerweiterungen bezeichnet. Dies verallgemeinert den Begriff einer endlichen Körpererweiterung.

7.5.3. Ist $\varphi \colon A \to B$ ein endlicher Ringmorphismus, so ist $\varphi(A) \subset B$ eine ganze Ringerweiterung (Korollar 7.1.22). Insbesondere ist eine endliche Ringerweiterung ganz. (Allgemeiner ist jeder endliche Ringmorphismus ganz im Sinne der Definition 7.3.18.)

Lemma 7.5.4 (Transitivität von Endlichkeit)**.** *Die Verknüpfung endlicher Ringmorphismen ist endlich.*

Beweis. Sind $\varphi \colon A \to B$ und $\psi \colon B \to C$ endliche Ringmorphismen, so gilt $B = \sum_{i=1}^n A.b_i = \sum_{i=1}^n \varphi(A)b_i$ und $C = \sum_{j=1}^m Bc_j = \sum_{j=1}^m \psi(B)c_j$ für geeignete $b_i \in B$ und $c_j \in C$. Es folgt
$$C = \sum_{j=1}^m \psi(B)c_j = \sum_{j=1}^m \sum_{i=1}^i \psi(\varphi(A))\psi(b_i)c_j.$$
Also ist $\psi\varphi \colon A \to C$ endlich. □

Aufgabe 7.5.5. Seine $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ Ringmorphismen. Zeigen Sie:

(a) Sind φ und ψ endlich, so ist auch $\psi\varphi$ endlich. (Dies ist Lemma 7.5.4.)
(b) Ist $\psi\varphi$ endlich, so ist auch ψ endlich.
(c) Surjektive Ringmorphismen sind endlich.
(d) Folgern Sie (oder zeigen Sie direkt): Ist $\varphi \colon A \to B$ endlich und ist $\mathfrak{b} \subset B$ ein Ideal, so ist der induzierte (injektive) Ringmorphismus $A/\varphi^{-1}\mathfrak{b} \to B/\mathfrak{b}$ endlich.
(e) Ist $\varphi \colon A \to B$ endlich und $A \to C$ ein Ringmorphismus, so ist $C \to B \otimes_A C$ endlich.
(f) Folgern Sie (oder zeigen Sie direkt): Ist $A \to B$ endlich, so ist $A[X] \to B[X]$ endlich.

Aufgabe 7.5.6. Ist $\varphi \colon A \to B$ ein endlicher Morphismus, so sind die Fasern von $\operatorname{Spec} \varphi \colon \operatorname{Spec} B \to \operatorname{Spec} A$ endlich. (Hinweise: siehe Übungsblatt).

Für ganze (injektive) Ringmorphismen ist dies falsch, man betrachte etwa $\mathbb{F}_2 \hookrightarrow \prod_{\mathbb{N}} \mathbb{F}_2$.

8. Endlich erzeugte Algebren über einem Körper

8.1. **Noether-Normalisierung.**

Konvention 8.1.1. In diesem Kapitel sei k stets ein Ring.

8.1.2. Der Leser mag annehmen, dass k ein Körper ist, denn wir interessieren uns hauptsächlich für diesen Fall.

Erinnerung 8.1.3. Eine k-Algebra A ist ein Ring A zusammen mit einem Ringmorphismus $\sigma = \sigma_A \colon k \to A$; dieser heißt Strukturmorphismus (Definition 7.1.16).

Beispiele 8.1.4. (a) Jeder Ring k ist eine k-Algebra (mit der Identität $k \to k$ als Strukturmorphismus).
(b) Der Polynomring $k[X]$ ist in kanonischer Weise eine k-Algebra: Der Strukturmorphismus $k \to k[X]$ ist die offensichtliche Inklusion. Insofern solle man besser Polynomalgebra statt Polynomring sagen.
(c) In analoger Weise sind die Polynomringe $k[X_1, \dots, X_n]$ und $k[X_i \mid i \in I]$ k-Algebren.

(d) Ist A eine k-Algebra und ist $\varphi\colon A \to B$ ein Ringmorphismus, so ist B in kanonischer Weise eine eine k-Algebra: Man nehme die Verknüpfung $k \to A \xrightarrow{\varphi} B$ als Strukturmorphismus (und dann ist $\varphi\colon A \to B$ ein Morphismus von k-Algebren im Sinne der folgenden Definition 8.1.6).

(e) Speziell sind Quotienten $k[X_1, \dots, X_n]/\mathfrak{a}$ von Polynomringen nach Idealen k-Algebren.

8.1.5. Ist k ein Körper und $A \neq 0$ eine k-Algebra, so ist der Strukturmorphismus $k \to A$ automatisch injektiv, so dass wir k als Unterring von A auffassen können.

Definition 8.1.6. Seien k-Algebren A und B gegeben. Ein **Morphismus von k-Algebren** $\varphi\colon A \to B$ ist ein Ringmorphismus $\varphi\colon A \to B$, so dass das Diagramm

$$\begin{tikzcd} A \arrow[rr, "\varphi"] & & B \\ & k \arrow[ul, "\sigma_A"] \arrow[ur, "\sigma_B"'] & \end{tikzcd}$$

kommutiert. Hier sind σ_A und σ_B die Strukturmorphismen. Äquivalent ist ein Morphismus von k-Algebren ein Ringmorphismus, der auch ein Morphismus von k-Moduln ist.

8.1.7. Es ist klar, dass k-Algebren eine Kategorie bilden.

Notation 8.1.8. Wir notieren die Kategorie der k-Algebren als Alg_k.

8.1.9. Ein Isomorphismus von k-Algebren ist per Definition ein Isomorphismus in Alg_k. Dies ist schlicht ein Morphismus von k-Algebren, der bijektiv ist als Abbildung von Mengen.

Beispiele 8.1.10.

- Sind $a_1, \dots, a_n$ Elemente einer k-Algebra A, so gibt es genau einen Morphismus $k[X_1, \dots, X_n] \to A$ von k-Algebren mit $X_i \mapsto a_i$, für alle $i = 1, \dots, n$. Dies ist schlicht eine Umformulierung der universellen Eigenschaft des Polynomrings. Mit anderen Worten ist für jede k-Algebra A die Abbildung
$$\begin{aligned} \mathrm{Alg}_k(k[X_1, \dots, X_n], A) &\to A^n, \\ \varphi &\mapsto (\varphi(X_1), \dots, \varphi(X_n)), \end{aligned}$$
eine Bijektion.
- Die analoge Aussage gilt für Polynomringe $k[X_i \mid i \in I]$ in beliebig vielen Variablen. Insbesondere erhält man für jede A-Algebra eine surjektiven Morphismus $k[X_a \mid a \in A] \twoheadrightarrow A$, $X_a \mapsto a$, von k-Algebren.

Erinnerung 8.1.11. Wir erinnern an den Begriff einer endlich erzeugten k-Algebra (siehe Definition 7.1.21).

8.1.12. Eine k-Algebra ist genau dann endlich erzeugt, wenn sie isomorph (als k-Algebra) zu einer k-Algebra der Form $k[X_1, \dots, X_n]/\mathfrak{a}$ ist, für ein $n \in \mathbb{N}$ und ein Ideal $\mathfrak{a} \subset k[X_1, \dots, X_n]$.

Erinnerung 8.1.13. Sei A eine k-Algebra. Wir sagen, dass Elemente $y_1, \dots, y_n \in A$ **algebraisch unabhängig** (über k) sind, falls der Morphismus

$$\begin{aligned} k[Y_1, \dots, Y_n] &\to A, \\ Y_i &\mapsto y_i, \end{aligned} \tag{8.1.1}$$

von k-Algebren injektiv ist.

8.1.14. Ist (8.1.1) injektiv, so ist notwendig der Strukturmorphismus $k \to A$ injektiv, so dass wir k als Unterring von A auffassen können. Algebraische Unabhängigkeit ist also nur für k-Algebren mit injektivem Strukturmorphismus interessant, also insbesondere für Algebren $\neq 0$ über Körpern (vgl. 8.1.5).

8.1.15. Dann ist also $k[Y_1, \dots, Y_n] \xrightarrow{\sim} k[y_1, \dots, y_n]$ bijektiv. Somit können wir $k[y_1, \dots, y_n]$ als Polynomring in den $y_1, \dots, y_n$ auffassen und insbesondere jedes Element von $k[y_1, \dots, y_n]$ eindeutig als k-Linearkombination von Monomen $y_1^{i_1} y_2^{i_2} \cdots y_n^{i_n}$ schreiben.

Definition 8.1.16. Sei A eine k-Algebra. Sagen wir, dass $k[y_1, \dots, y_n] \subset A$ ein Polynomring/eine Polynomalgebra ist, so meinen wir damit, dass $y_1, \dots, y_n$ über k algebraisch unabhängige Elemente von A sind.

Beispiel 8.1.17 (Substitution)**.** Betrachte die k-Algebra $A = k[X_1, \dots, X_n]$. Für $i = 1, \dots, n$ seien $g_i(X_n) \in k[X_n]$ Polynome in der Variablen X_n, für $i = 1, \dots, n-1$. Wir behaupten, dass die Elemente

$$\begin{aligned} y_1 &:= X_1 - g_1(X_n), \\ y_2 &:= X_2 - g_2(X_n), \\ &\dots \\ y_{n-1} &:= X_{n-1} - g_{n-1}(X_n), \\ y_n &:= X_n \end{aligned}$$

algebraisch unabhängig sind. In der Tat, der Morphismus

$$\begin{aligned} k[Y_1, \dots, Y_n] &\to k[X_1, \dots, X_n], \\ Y_i &\mapsto y_i, \end{aligned}$$

ist bijektiv mit Umkehrabbildung

$$\begin{aligned} k[Y_1, \dots, Y_n] &\leftarrow k[X_1, \dots, X_n], \\ Y_i + g_i(Y_n), &\hookleftarrow X_i \qquad \text{für } i = 1, \dots, n-1, \\ Y_n &\hookleftarrow X_n. \end{aligned}$$

Es folgt

$$k[X_1, \dots, X_n] = k[y_1, \dots, y_{n-1}, X_n] = k[y_1, \dots, y_{n-1}][X_n].$$

Man wechselt von links nach rechts mit Hilfe der Substitution

$$X_i = y_i + g_i(X_n) \quad \text{für } i = 1, \dots, n-1.$$

8.1.18. Wir benötigen das folgende Lemma 8.1.19 im Beweis des Noetherschen Normalisierungssatzes 8.1.26.

Lemma 8.1.19. *Sei k ein Körper und $0 \neq f \in k[X_1, \dots, X_n]$.*

(a) Dann gibt es Elemente $r_1, \dots, r_{n-1} \in \mathbb{N}$, so dass mit

$$y_i := X_i - X_n^{r_i}, \quad \textit{für } i = 1, \dots, n-1,$$

nach der Substitution

$$X_i = y_i + X_n^{r_i}, \quad \textit{für } i = 1, \dots, n-1,$$

das Polynom f die Gestalt

$$f = f(y_1, \dots, y_{n-1}, X_n) = cX_n^m + h_1 X_n^{m-1} + \dots + h_m$$

hat für ein $m \in \mathbb{N}$ und ein $c \in k^\times$ und geeignete Elemente $h_1, \dots, h_m$ des Polynomrings $k[y_1, \dots, y_{n-1}]$ (vgl. Beispiel 8.1.17).

(b) Sei k unendlich. Dann gibt es Elemente $a_1, \dots, a_{n-1} \in k$, so dass mit

$$y_i := X_i - a_i X_n, \quad \textit{für } i = 1, \dots, n-1,$$

nach der Substitution

$$X_i = y_i + a_i X_n, \quad \textit{für } i = 1, \dots, n-1,$$

das Polynom f die Gestalt

$$f = f(y_1, \dots, y_{n-1}, X_n) = cX_n^m + h_1 X_n^{m-1} + \dots + h_m$$

hat für ein $m \in \mathbb{N}$ und ein $c \in k^\times$ und geeignete Elemente $h_1, \dots, h_m$ des Polynomrings $k[y_1, \dots, y_{n-1}]$.

8.1.20. Der springenden Punkt ist, dass der Leitkoeffizient c von f nicht von $y_1, \dots, y_{n-1}$ abhängt.

Beweis. Zunächst (b) (weil wichtiger): Schreibe $f = f_m + f_{m-1} + \dots + f_0$ wobei f_s der homogene Anteil von f vom (Total-)Grad s ist und $f_m \neq 0$, also

$$f_s = \sum_{\substack{\sigma \in \mathbb{N}^n, \\ \sigma_1 + \dots + \sigma_n = s}} b_\sigma X_1^{\sigma_1} \cdots X_n^{\sigma_n},$$

für geeignete $b_\sigma \in k$. Substituieren wir $X_i = y_i + a_i X_n$ für näher zu bestimmende $a_1, \dots, a_{n-1} \in k$, so ergibt dies

$$\begin{aligned} f_s &= \sum_{\substack{\sigma \in \mathbb{N}^n, \\ \sigma_1 + \cdots + \sigma_n = s}} b_\sigma (y_1 + a_1 X_n)^{\sigma_1} \cdots (y_{n-1} + a_{n-1} X_n)^{\sigma_{n-1}} X_n^{\sigma_n} \\ &= \Big(\sum_{\substack{\sigma \in \mathbb{N}^n, \\ \sigma_1 + \cdots + \sigma_n = s}} b_\sigma a_1^{\sigma_1} \cdots a_{n-1}^{\sigma_{n-1}} \Big) X_n^s + (\text{Summanden mit } X_n\text{-Grad} < s) \\ &= f_s(a_1, \dots, a_{n-1}, 1) X_n^s + (\text{Summanden mit } X_n\text{-Grad} < s). \end{aligned}$$

Es folgt

$$f = f_m(a_1, \dots, a_{n-1}, 1) X_n^m + (\text{Summanden mit } X_n\text{-Grad} < m).$$

Es reicht also zu zeigen, dass $f_m(a_1, \dots, a_{n-1}, 1) \neq 0$ für geeignete Elemente $a_1, \dots, a_{n-1} \in k$.

Schreibe

$$f_m = g_0 X_n^m + g_1 X_n^{m-1} + \cdots + g_m$$

mit eindeutigen $g_j \in k[X_1, \dots, X_{n-1}]$ vom Totalgrad j. Wegen $f_m \neq 0$ ist ein g_j ungleich Null. Weil alle g_j verschiedenen Totalgrad haben, gilt

$$f_m(X_1, \dots, X_{n-1}, 1) = g_0 + g_1 + \cdots + g_m \neq 0$$

in $k[X_1, \dots, X_{n-1}]$. Da k unendlich ist, gibt es nach Aufgabe 8.1.21 ein Element $(a_1, \dots, a_{n-1})$ mit

$$f_m(a_1, \dots, a_{n-1}, 1) \neq 0.$$

Die Behauptung folgt.

(a): Schreibe

$$f = \sum_{\sigma \in \mathbb{N}^n} b_\sigma X_1^{\sigma_1} \cdots X_n^{\sigma_n}$$

für geeignete $b_\sigma \in k$. Substituieren wir $X_i = y_i + X_n^{r_i}$ für näher zu bestimmende $r_1, \dots, r_{n-1} \in \mathbb{N}$, so haben die Summanden die Form

$$\begin{aligned} b_\sigma X_1^{\sigma_1} \cdots X_n^{\sigma_n} &= b_\sigma (y_1 + X_n^{r_1})^{\sigma_1} \cdots (y_{n-1} + X_n^{r_{n-1}})^{\sigma_{n-1}} X_n^{\sigma_n} \\ &= b_\sigma X_n^{\sigma_1 r_1 + \cdots + \sigma_{n-1} r_{n-1} + \sigma_n} + (\text{Summanden mit kleinerem } X_n\text{-Grad}). \end{aligned}$$

Wir behaupten, dass wir $r_1, \dots, r_{n-1}$ so wählen können, dass für verschiedene $\sigma \in \mathbb{N}^n$ mit $b_\sigma \neq 0$ die Exponenten $\sigma_1 r_1 + \cdots + \sigma_{n-1} r_{n-1} + \sigma_n$ verschieden sind. Daraus folgt dann offensichtlich die Behauptung, denn es gibt dann genau ein σ mit $b_\sigma \neq 0$ und maximalem Exponenten bei X_n.

Da nur endlich viele b_σ ungleich Null sind, gibt es ein $M \in \mathbb{N}$ mit $b_\sigma = 0$ für alle $\sigma \in \mathbb{N}^n - \{0, 1, \dots, M-1\}^n$. Setzen wir $r_1 := M$, $r_2 = M^2$, …, $r_{n-1} := M^{n-1}$, so sind die Zahlen

$$\sigma_1 r_1 + \cdots + \sigma_{n-1} r_{n-1} + \sigma_n = \sigma_n + \sigma_1 M + \sigma_2 M^2 + \cdots + \sigma_{n-1} M^{n-1}$$

für $\sigma \in \{0, 1, \dots, M\}$ paarweise verschieden, denn die M-adische Darstellung einer natürlichen Zahl ist eindeutig im M-adischen Stellenwertsystem. □

Aufgabe 8.1.21 (Polynome als Abbildungen/Funktionen)**.** Expliziter: Sei k ein unendlicher Körper und $f \in k[T_1, \dots, T_n]$ mit $f(x_1, \dots, x_n) = 0$ für alle $x \in k^n$. Dann gilt bereits $f = 0$ in $k[T_1, \dots, T_n]$.

Sei k ein Ring und betrachte den Ringmorphismus

$$\varphi\colon k[T_1, \dots, T_n] \to \mathrm{Abb}(k^n, k),$$

der einem Polynom p die k-wertige Funktion $k^n \to k$, $x \mapsto p(x)$, zuordnet.

(a) Ist k ein unendlicher Körper (zum Beispiel ein algebraisch abgeschlossener Körper), so ist φ injektiv.
Hinweis: Löse zunächst den Fall $n = 1$ und verwende dann Induktion.

Dies bedeutet, dass man $k[X_1, \dots, X_n]$ mit seinem Bild, dem **Ring der polynomialen Funktionen auf** k^n, identifizieren kann.

(b) Ist k ein endlicher Körper, so ist φ nicht injektiv.
Bonusaufgabe: Bestimme in diesem Fall den Kern von φ. Siehe Aufgabeim (privaten) Anhang.

Lemma 8.1.22. *Seien U ein Ring und $0 \neq f \in U[X]$ ein Polynom vom Grad m mit in U invertierbarem Leitkoeffizienten. Dann gelten:*

(a) *Als U-Modul ist $U[X]/(f)$ frei mit Basis $1, X, \ldots, X^{m-1}$. Insbesondere ist $U \to U[X]/(f)$ injektiv und endlich.*

(b) *Ist $\deg(f) = m > 0$, so ist $U[f]$ ein Polynomring und $U[X]$ ist als $U[f]$-Modul frei mit Basis $1, X, \ldots, X^{m-1}$. Insbesondere ist $U[f] \subset U[X]$ endlich.*

Erster Beweis mit Polynomdivision. Wir verwenden Existenz und Eindeutigkeit der Division mit Rest durch f: Für jedes $a \in U[X]$ gilt $a = bf + r$ für eindeutige $b, r \in U[X]$ mit $\deg(r) < \deg(f) = m$. Das Element r heißt der Rest von a durch f.[25]

(a) Sei $U[X]_{<m} := U \oplus UX \oplus \cdots \oplus X^{m-1} \subset U[X]$ der Unter-U-Modul der Polynome vom Grad $< m$. Er ist frei mit Basis $1, \ldots, X^{m-1}$.

Betrachte die Abbildung $U[X] \to U[X]_{<m}$, die ein Polynom $a \in U[X]$ auf seinen Rest bei Division durch f abbildet. Diese Abbildung ist offensichtlich U-linear, surjektiv, und ihr Kern ist (f). Somit erhalten wir einen Isomorphismus $U[X]/(f) \xrightarrow{\sim} U[X]_{<m}$ von U-Moduln.

(b) Da der Leitkoeffizient von f invertierbar ist und $\deg(f) = m > 0$ gilt, ist $U[F] \to U[X]$, $F \mapsto f$, injektiv mit Bild $U[f]$. Also ist $U[f]$ ein Polynomring.

Sei $a \in U[X]$. Division von a durch f liefert $a = a_0 f + r_0$ mit $a_0 \in U[X]$ und $r_0 \in U[X]_{<m}$. Wegen $\deg(f) = m > 0$ gilt $\deg(a_0) < \deg(a)$ (mit der Konvention $\deg(0) = -\infty$ und $-\infty < -\infty$). Division von a_0 durch f liefert $a_0 = a_1 f + r_1$. Es gelten $a = a_1 f^2 + r_1 f + r_0$ und $\deg(a_1) < \deg(a_0)$. Wir iterieren diesen Prozess. Wegen $\deg(a) < \infty$ bricht er nach endlich vielen Schritten in dem Sinne ab, dass $0 = a_N = a_{N+1} = \ldots$ gilt für ein $N \in \mathbb{N}$, und somit $0 = r_{N+1} = r_{N+2} \ldots$. In diesem Sinne ist $(r_0, r_1, \ldots)$ eine Nullfolge in $U[X]_{<m}$. Sie ist durch

$$a = r_0 + r_1 f + r_2 f^2 + \ldots \quad \text{(die Summe ist endlich)}$$

eindeutig gegeben (vergleiche: Entwicklung einer Zahl im Dezimalsystem; wir haben also a im f-adischen System entwickelt). Schreiben wir $r_i = r_i^{(0)} 1 + r_i^{(1)} X + \ldots r_i^{(m-1)} X^{m-1}$, mit eindeutigen $r_i^{(j)} \in U$, so ergibt sich

$$\begin{aligned} a = \;& r_0 + r_1 f + r_2 f^2 + \ldots, \\ = \;& (r_0^{(0)} 1 + r_0^{(1)} X + \ldots r_0^{(m-1)} X^{m-1}) 1 \\ & + (r_1^{(0)} 1 + r_1^{(1)} X + \ldots r_1^{(m-1)} X^{m-1}) f \\ & + (r_2^{(0)} 1 + r_2^{(1)} X + \ldots r_2^{(m-1)} X^{m-1}) f^2 \\ & + \ldots, \end{aligned}$$

Liest man dies spaltenweise und definiert $R^{(l)} := r_0^{(l)} + r_1^{(l)} f + r_2^{(l)} f^2 + \cdots \in U[f]$ für $l = 0, \ldots, m-1$, so erhalten wir

$$a = R^{(0)} + R^{(1)} X + \cdots + R^{(m-1)} X^{m-1}.$$

Nach Konstruktion ist klar, dass die $R^{(l)} \in U[f]$ eindeutig bestimmt sind. Dies zeigt $U[X] = U[f]1 \oplus U[f]X \oplus \cdots \oplus U[f]X^{m-1}$. ☐

Zweiter Beweis. (a) Wir können ohne Einschränkung annehmen, dass f normiert ist, also $f = X^m + f_1 X^{m-1} + \cdots + f_0$. Daraus folgt sofort, dass die angegebenen Elemente $U[X]/(f)$ als U-Modul erzeugen, denn in $U[X]/(f)$ gilt $X^m = -f_1 X^{m-1} - \cdots - f_0$ und man kann somit Potenzen $\geq m$ von X sukzessive durch U-Linearkombinationen kleinerer Potenzen ersetzen.

Die U-lineare Unabhängigkeit sieht man wie folgt: Seien $u_0, \ldots, u_{m-1} \in U$ Elemente, nicht alle Null, so dass das Element $u := u_0 + u_1 X + \cdots + u_{m-1} X^{m-1} \in U[X]$ in $U[X]/(f)$ Null ist. Dann ist u ein Vielfaches von f, sagen wir $u = gf$ für ein $g \in U[X]$. Da $u \neq 0$ gilt, erhalten wir den Widerspruch $m > \deg(u) = \deg(g) + \deg(f) \geq \deg(f) = m$.

[25] Möglicherweise ist dies nur für normierte Polynome f bekannt; dies ist aber offensichtlich äquivalent zur obigen Aussage. Falls die Aussage nur für normierte Polynome über einem Körper bekannt ist, sieht man leicht, dass der Standardbeweis auch für beliebige Ringe funktioniert.

(b) Ist V ein beliebiger Ring und $f \in V$ ein Element, so ist die Verknüpfung $V \hookrightarrow V[F] \twoheadrightarrow V[F]/(f - F)$ ein Ringisomorphismus (hier ist $V[F]$ der Polynomring): Ihre Umkehrabbildung kommt von dem V-Algebrenmorphismus $V[F] \to V$, $F \mapsto f$. (Alternativ folgt dies aus (a).)

Wenden wir dies auf $f \in V = U[X]$ an, so erhalten wir den Ringisomorphismus

$$U[X] \xrightarrow{\sim} U[X][F]/(f - F) = U[F][X]/(f - F). \tag{8.1.2}$$

Leitkoeffizient und Grad von $f - F \in U[F][X]$ als Polynom in X stimmen wegen $\deg(f) > 0$ mit Leitkoeffizient und Grad von $f \in U[X]$ überein. Somit zeigt (a), dass $U[F][X]/(f - F)$ ein freier $U[F]$-Modul mit Basis $1, X, \ldots, X^{m-1}$ ist.

Da der Leitkoeffizient von f invertierbar ist und $\deg(f) = m > 0$ gilt, ist $U[F] \to U[X]$, $F \mapsto f$, injektiv mit Bild $U[f]$. Also ist $U[f]$ ein Polynomring. Der Isomorphismus (8.1.2) ist offensichtlich ein Isomorphismus von $U[F]$-Algebren. Also ist $U[X]$ ein freier $U[f]$-Modul mit Basis $1, X, \ldots, X^{m-1}$. □

Proposition 8.1.23. *Seien k ein Körper und $0 \neq f \in P := k[X_1, \ldots, X_n]$. Dann gibt es einen Polynomring $U = k[y_1, \ldots, y_{n-1}] \subset P$ und ein Element $m \in \mathbb{N}$, so dass gelten:*

- *(a) Als U-Modul ist $P/(f)$ frei mit Basis $1, X, \ldots, X^{m-1}$. Insbesondere ist $U \to P/(f)$ injektiv und endlich.*
- *(b) Ist $f \notin k$, so ist $U[f] = k[y_1, \ldots, y_{n-1}, f]$ ein Polynomring (über U bzw. k) und P ist als $U[f]$-Modul frei mit Basis $1, X, \ldots, X^{m-1}$. Insbesondere ist $U[f] \subset U[X]$ endlich.*

Beweis. Lemma 8.1.19 liefert einen Polynomring $U = k[y_1, \ldots, y_{n-1}] \subset P$ und ein Element $m \in \mathbb{N}$, so dass $U[X_n] = P$ gilt und $f \in U[X_n] = P$ als Polynom in X_n mit Koeffizienten in U Grad m hat und als Leitkoeffizienten ein Element von $k^\times$ hat. Damit können wir Lemma 8.1.22 anwenden. Im Fall $f \notin k$ muss $m > 0$ gelten. □

Satz 8.1.24 (Noetherscher Normalisierungssatz, schwache Version)**.** *Sei k ein Körper und $A \neq 0$ eine endlich erzeugte k-Algebra. Dann existiert ein Polynomring $P := k[y_1, \ldots, y_d] \subset A$, so dass A endlich über P ist.*[26]

8.1.25. Die Terminologie kommt vermutlich daher, dass Polynomringe über Körpern normal sind (siehe Proposition 7.1.13).

Satz 8.1.26 (Noetherscher Normalisierungssatz, starke Version)**.** *Sei k ein Körper, A eine endlich erzeugte k-Algebra, und $I \subsetneq A$ ein echtes Ideal (also insbesondere $A \neq 0$). Dann existieren*

- *ein Polynomring $P := k[y_1, \ldots, y_d] \subset A$, für ein $d \in \mathbb{N}$,*[27] *und*
- *ein $\delta \leq d$,*

so dass

- *A endlich über P ist und*
- *$I \cap P = (y_{\delta+1}, \ldots, y_d)$ gilt, wobei rechts das im Polynomring $P = k[y_1, \ldots, y_d]$ erzeugte Ideal $Py_{\delta+1} + \cdots + Py_d$ gemeint ist.*

8.1.27. Die schwache Version ist der Spezialfall $I = (0)$ der starken Version.

8.1.28. Ist A als k-Algebra von n Elementen erzeugt, so liefern unsere Beweise sowohl der schwachen Version 8.1.24 als auch der starken Version 8.1.26 des Noetherschen Normalisierungsatzes $d \leq n$. Dies ist automatisch der Fall, denn nach Korollar 9.1.26 gilt $d = \dim A \leq n$. Wissen wir sogar, dass A isomorph zu einer Polynomalgebra $k[X_1, \ldots, X_n]$ in n Variablen ist, so liefern unsere Beweise $d = n$ (dies ist nur in der starken Version interessant). Auch dies ist automatisch der Fall, denn dann gilt $\dim A = n$ nach Satz 9.1.23.

[26] Genauer, aber weniger prägnant: Dann existieren algebraisch unabhängige Elemente $y_1, \ldots, y_d \in A$, für ein $d \in \mathbb{N}$, so dass $k[y_1, \ldots, y_d] \subset A$ endlich ist.

[27] d. h. es gibt algebraisch unabhängige Elemente $y_1, \ldots, y_d \in A$

8.1.29. Die Schlussfolgerung des Noetherschen Normalisierungssatzes wird durch den linken Teil des folgenden kommutativen Diagramms illustriert.
(8.1.3)

$$\begin{tikzcd}[column sep=small]
 & I \arrow[r, phantom, "\subsetneq"] & A \arrow[r, two heads] & A/I & \\
 & {} \arrow[u, phantom, "\cup"] & {} \arrow[u, phantom, "\cup\text{endlich}"] & & \\
(y_{\delta+1}, \dots, y_d) \arrow[r, phantom, "="] & I \cap k[y_1, \dots, y_d] \arrow[r, phantom, "\subsetneq"] & k[y_1, \dots, y_d] \arrow[r, two heads] & k[y_1, \dots, y_d]/(y_{\delta+1}, \dots, y_d) \arrow[uu, hook, "\text{endlich}"'] \arrow[r, phantom, "="] & k[y_1, \dots, y_\delta]
\end{tikzcd}$$

Es ist offensichtlich, dass der induzierte rechte vertikale Pfeil injektiv und endlich ist. Wir haben den kanonischen Isomorphismus zwischen den beiden Ringen rechts unten als Gleichheit geschrieben.[28]

Geometriebemerkung 8.1.30. Mit der üblichen Definition $\mathbb{A}^n_k = \operatorname{Spec} k[Z_1, \dots, Z_n]$ (was man sich als k^n vorstellen sollte, denn dies sind seine k-Punkte) übersetzt sich das Diagramm (8.1.3) in das kommutative Diagramm

$$\begin{tikzcd}
\operatorname{Spec} A \arrow[d, "\text{endlich}"] \arrow[r, phantom, "\supset"] & \mathcal{V}(I) \arrow[d, "\text{endlich}"] \arrow[r, phantom, "="] & \operatorname{Spec} A/I \\
\mathbb{A}^d_k \arrow[r, phantom, "\supset"] & \mathbb{A}^\delta_k &
\end{tikzcd}$$

von Mengen oder besser affinen Schemata. Die beiden vertikalen Morphismen sind endlich, die untere Inklusion „ist“ die Inklusion $k^\delta \hookrightarrow k^\delta \times k^{d-\delta} = k^d$, $a \mapsto (a, 0)$.

Bis auf endliche Morphismen entspricht die Inklusion $\mathcal{V}(I) \subset \operatorname{Spec} A$ also der offensichtlichen Inklusion $k^\delta \hookrightarrow k^d$ von Vektorräumen.

Beweis der schwachen Version 8.1.24. Wir können ohne Einschränkung annehmen (nach 8.1.12), dass $A = k[X_1, \dots, X_n]/\mathfrak{a}$ gilt für ein $n \in \mathbb{N}$ und ein Ideal $\mathfrak{a} \subset k[X_1, \dots, X_n]$.

Wir führen den Beweis per Induktion über n.

Im Fall $n = 0$ gilt $A = k$ (da $A \neq 0$), und die Aussage ist trivial.

Gelte $n > 0$. Im Fall $\mathfrak{a} = (0)$ ist A ein Polynomring und die Aussage ist trivial.

Gelte also $\mathfrak{a} \neq (0)$. Sei $0 \neq f \in \mathfrak{a}$. Nach Proposition 8.1.23.(a) gibt es einen Polynomring

$$U = k[y_1, \dots, y_{n-1}] \subset P := k[X_1, \dots, X_n],$$

so dass $U[X_n] = P$ gilt und $U \to P/(f)$ injektiv und endlich ist.

Der schwarze Teil des folgenden kommutativen Diagramms illustriert die bisherigen Überlegungen. (Der vertikale Pfeil $P/(f) \twoheadrightarrow P/\mathfrak{a} = A$ existiert wegen $f \in \mathfrak{a}$.)

$$\begin{tikzcd}
 & U[X_n] \arrow[r, phantom, "="] & P \arrow[r, phantom, "="] \arrow[dd, two heads] & k[X_1, \dots, X_n] \arrow[dddd, two heads] \\
 & {} \arrow[u, phantom, "\cup"] & & \\
 & U \arrow[r, hook, "\text{endlich}"] \arrow[dd, two heads] & P/(f) \arrow[dd, two heads] & \\
 & & & \\
k[z_1, \dots, z_d] \arrow[r, phantom, "\overset{\text{endlich}}{\subset}"] & U/\mathfrak{b} \arrow[r, hook, "\text{endlich}"] & P/\mathfrak{a} \arrow[r, phantom, "="] & A
\end{tikzcd}$$

Sei $\mathfrak{b} := \mathfrak{a} \cap U$. Dies ist der Kern der Verknüpfung $U \hookrightarrow P \twoheadrightarrow A$, so dass wir die Inklusion $U/\mathfrak{b} \hookrightarrow P/\mathfrak{a}$ erhalten. Sie ist endlich, da $U \hookrightarrow P/(f)$ endlich ist (das ist offensichtlich, vgl. Aufgabe 7.5.5).

Da $U/\mathfrak{b}$ als Quotient von $U = k[y_1, \dots, y_{n-1}]$ als k-Algebra von $n-1$ Elementen erzeugt ist, finden wir per Induktion einen Polynomring $k[z_1, \dots, z_d] \subset U/\mathfrak{b}$, für ein $d \leq n-1$, so dass $U/\mathfrak{b}$ endlich über $k[z_1, \dots, z_d]$ ist. Transitivität von Endlichkeit (Lemma 7.5.4) zeigt, dass A endlich über $k[z_1, \dots, z_d]$ ist. □

Beweis der starken Version 8.1.26. Der Beweis geht in mehreren Schritten. Wir beweisen die Behauptung zunächst in drei Spezialfällen und folgern dann den allgemeinen Fall.

(a) A ist ein Polynomring und $I = Af \neq 0$ ist ein nichttriviales echtes Hauptideal.
(b) A ist ein Polynomring und I ist beliebig.

[28] Das rechte Quadrat ist im Allgemeinen kein Push-out (siehe Proposition 5.6.1.(b).

(c) $A \neq 0$ ist beliebig und $I = (0)$ (dies ist die schwache Version, siehe 8.1.27).

(d) Allgemeiner Fall (starke Version).

(a) Sei $A = k[X_1, \dots, X_n]$ ein Polynomring und $(0) \neq I = Af \subsetneq A$ ein echtes Hauptideal mit Erzeuger f. Wir zeigen zusätzlich zur Behauptung, dass man $d = n$ und $y_n = f$ wählen kann.

Es gilt $f \notin k$. Proposition 8.1.23.(b) liefert Elemente $y_1, \dots, y_{n-1} \in A$ und ein Element $m \in \mathbb{N}$, so dass $V := k[y_1, \dots, y_{n-1}, f] \subset A$ ein Polynomring ist und A ein freier V-Modul mit Basis $1, X_n, \dots, X_n^{m-1}$. Ein beliebiges Element $a \in A$ hat also die Form $a = v_0 1 + v_1 X_n + \dots + v_{m-1} X_n^{m-1}$ für eindeutige $v_i \in V$. Es gelten

$$\begin{aligned} a \in Af = I &\iff v_0, v_1, \dots, v_{m-1} \in Vf, \\ a \in V &\iff v_1 = \dots = v_{m-1} = 0. \end{aligned}$$

Es folgt $I \cap V = Vf$. Dies zeigt die Behauptung (setze $d = n$, $y_n = f$ und $\delta = n - 1$).

(b) Sei $A = k[X_1, \dots, X_n]$ ein Polynomring und $I \subsetneq A$ ein echtes Ideal. Wir zeigen per Induktion über n, dass die Behauptung samt der Aussage $d = n$ gilt.

Ist $I = (0)$, so ist die Aussage trivial (setze $d = \delta = n$ und $y_i = X_i$).

Gelte also $I \neq (0)$. Ist $n = 1$, so ist A ein Hauptidealring und die Aussage folgt aus (a). Gelte $n > 1$. Das folgende kommutative Diagramm illustriert das folgende Argument.

$$\begin{array}{ccccccc} & & & & A & \supsetneq & I \\ & & & & \cup\text{endlich} & & \\ & & P = W[y_n] & \underset{\text{endlich}}{\subset} & V = U[f] = U[y_n] & \supsetneq & \cup \\ & & \cup & & \cup & & \\ I \cap W & \subsetneq & W & \underset{\text{endlich}}{\subset} & U & \supsetneq & I \cap U \end{array}$$

Sei $0 \neq f \in I$. Nach (a) finden wir einen Polynomring $V := k[y_1, \dots, y_{n-1}, y_n = f] \subset A$, so dass A endlich über V ist. (Wir könnten zusätzlich annehmen, dass $Af \cap V = Vf$ gilt, werden dies aber nicht benötigen Benötigt wird aber $f \in I$.)

Im Polynomring $U := k[y_1, \dots, y_{n-1}]$ betrachten wir das Ideal $I \cap U \subsetneq U$. Per Induktion finden wir einen Polynomring $W := k[z_1, \dots, z_{n-1}] \subset U$ (ebenfalls in $n-1$ Variablen), so dass U ein endlicher W-Modul ist, und ein $\delta \leq n - 1$, so dass

$$I \cap W = I \cap U \cap W = Wz_{\delta+1} + \dots + Wz_{n-1}. \tag{8.1.4}$$

Das Element $y_n = f$ ist algebraisch unabhängig über W, denn es ist algebraisch unabhängig über U. Also ist $P := W[y_n] = k[z_1, \dots, z_{n-1}, y_n]$ ein Polynomring in n Variablen. Weil $W \subset U$ endlich ist, ist $P = W[y_n] \subset U[y_n] = V$ endlich (Aufgabe 7.5.5). Da auch $V \subset A$ endlich ist, ist $P \subset A$ endlich (Lemma 7.5.4).

Zu zeigen bleibt

$$I \cap P = Pz_{\delta+1} + \dots + Pz_{n-1} + Py_n.$$

$\supset$: Wegen (8.1.4) liegen die Elemente $z_{\delta+1}, \dots, z_{n-1}$ in $I \cap W \subset I \cap P$, und natürlich gilt $y_n = f \in Af \subset I$, also $y_n \in I \cap P$.

$\subset$: Sei $g \in I \cap P$. Schreibe $g = g' + g'' y_n \in P = W[y_n] = W \oplus Py_n$ mit (eindeutigen) $g' \in W$ und $g'' \in P$. Wegen $g'' y_n \in Py_n \subset I \cap P$ nach der bereits gezeigten Inklusion folgt

$$g' = g - g'' y_n \in I \cap P \cap W = I \cap W \overset{(8.1.4)}{=} Wz_{\delta+1} + \dots + Wz_{n-1} \subset Pz_{\delta+1} + \dots + Pz_{n-1}$$

Wegen $g'' y_n \in Py_n$ folgt $g = g' + g'' y_n \in Pz_{\delta+1} + \dots + Pz_{n-1} + Py_n$.

(c) Wir zeigen die schwache Version der Noether-Normalisierung 8.1.24. Zur Orientierung dient das folgende kommutative Diagramm.

$$\begin{tikzcd} & & \mathfrak{a} & \subsetneq & k[X_1, \dots, X_n] \arrow[rr, two heads] & & A \\ & & \cup & & \cup\text{endlich} & & \\ (y_{\delta+1}, \dots, y_n) & = & \mathfrak{a} \cap k[y_1, \dots, y_n] & \subsetneq & k[y_1, \dots, y_n] \arrow[r, two heads] & k[y_1, \dots, y_n]/(y_{\delta+1}, \dots, y_n) \arrow[ur, hook, "\text{endlich}"'] & = & k[y_1, \dots, y_\delta] \end{tikzcd}$$

Sei $k[X_1, \dots, X_n] \twoheadrightarrow A$ ein surjektiver Morphismus von k-Algebren mit Kern $\mathfrak{a}$. Dieser Kern ist ein echtes Ideal in $k[X_1, \dots, X_n]$, da $A \neq 0$. Nach (b) gibt es ein $\delta \leq n$ und einen Polynomring $R := k[y_1, \dots, y_n] \subset k[X_1, \dots, X_n]$ (ebenfalls in n Variablen) mit $\mathfrak{a} \cap R = Ry_{\delta+1} + \cdots + Ry_n$. Wir erhalten einen injektiven Ringmorphismus (der rechte vertikale Morphismus im obigen Diagramm)

$$k[y_1, \dots, y_n]/(y_{\delta+1}, \dots, y_n) = R/(\mathfrak{a} \cap R) \hookrightarrow A.$$

Er ist endlich, da $R \subset k[X_1, \dots, X_n]$ endlich ist (Aufgabe 7.5.5). Die linke Seite ist in offensichtlicher Weise zum Polynomring $k[y_1, \dots, y_\delta]$ isomorph.

Dies zeigt die schwache Version der Noether-Normalisierung 8.1.24.

(d): Nun zeigen wir Satz 8.1.26. Hier ist die Illustration dazu (die vertikalen Inklusionen sind echte Inklusionen).

$$\begin{array}{ccccccc} k[y_1, \dots, y_d] & = & P & \underset{\text{endlich}}{\subset} & Q & \underset{\text{endlich}}{\subset} & A \\ & & \cup & & \cup & & \cup \\ (y_{\delta+1}, \dots, y_d) & = & I \cap P & \subset & I \cap Q & \subset & I \end{array}$$

Sei A von n Elementen erzeugt. Nach der schwachen Version (c) gibt es einen Polynomring $Q \subset A$ in $d \leq n$ Variablen, so dass A über Q endlich ist.

Wir wenden (b) auf das Ideal $I \cap Q \subset Q$ in diesem Polynomring an und erhalten ein $\delta \leq d$ und einen Polynomring $P = k[y_1, \dots, y_d] \subset Q$, so dass Q endlich über P ist und $I \cap P = I \cap Q \cap P = Py_{\delta+1} + \dots Py_d$ gilt. Mit $P \subset Q$ und $Q \subset A$ ist auch $P \subset A$ endlich (Lemma 7.5.4). Dies zeigt die Behauptung. □

Aufgabe 8.1.31. Berechnen Sie eine (schwache) Noether-Normalisierung für $\mathbb{C}[X, Y]/(XY - 1)$.

8.2. Der Hilbertsche Nullstellensatz.

Satz 8.2.1 (Hilbertscher Nullstellensatz (schwache Version) - Zariskis Lemma)**.** *Sei A eine endlich erzeugte Algebra über einem Körper k. Ist A ein Körper, so ist $k \hookrightarrow A$ eine endliche (und damit algebraische) Körpererweiterung.*

Ist insbesondere $\mathfrak{m}$ ein maximales Ideal in einem Polynomring $k[X_1, \dots, X_n]$ über einem Körper k, so ist $k \subset k[X_1, \dots, X_n]/\mathfrak{m}$ eine endliche Körpererweiterung.

8.2.2. Ist A eine endlich erzeugte k-Algebra, die ein Körper ist, so ist A notwendig von der Gestalt $k[X_1, \dots, X_n]/\mathfrak{m}$, für ein geeignetes maximales Ideal $\mathfrak{m}$ in einem Polynomring $k[X_1, \dots, X_n]$.

8.2.3 (Umformulierung der schwachen Version 8.2.1 des Hilbertschen Nullstellensatzes)**.** Ist $k \subset L$ eine Körpererweiterung, so dass L als k-Algebra endlich erzeugt ist, so ist L/k bereits endlich.

Als Slogan:

$$\text{endlich} = \text{endlicher Typ} \qquad \text{für Körpererweiterungen.} \tag{8.2.1}$$

Man vergleiche dies mit dem Slogan (7.1.2) für Ringerweiterungen.

Beweis. Die schwache Version der Noether-Normalisierung 8.1.24 (beachte $A \neq 0$) liefert einen Polynomring $P = k[y_1, \dots, y_d] \subset A$, so dass A endlich über P ist. Die endliche Ringerweiterung $P \subset A$ ist ganz (siehe 7.5.3), und somit ist mit A auch P ein Körper (Proposition 7.2.1). Es folgt $d = 0$, denn für $d > 0$ ist der Polynomring $P = k[y_1, \dots, y_d]$ kein Körper, beispielweise ist y_1 nicht invertierbar. Also ist $k = P \subset A$ eine endliche Körpererweiterung.

Für die letzte Aussage betrachte man $A = k[X_1, \dots, X_n]/\mathfrak{m}$. □

Satz 8.2.4 (Hilbertscher Nullstellensatz)**.** *Sei A eine endlich erzeugte Algebra über einem Körper k. Sei $\overline{k}$ ein algebraischer Abschluss von k. Dann gelten die folgenden Aussagen:*

- *(a) Ein Ideal $\mathfrak{a} \subset A$ ist genau dann maximal, wenn es einen Morphismus von k-Algebren $\varphi \colon A \to \overline{k}$ mit $\mathfrak{a} = \ker(\varphi)$ gibt.*
- *(b) Zwei solche Morphismen $\varphi_1, \varphi_2 \colon A \to \overline{k}$ von k-Algebren haben genau dann denselben Kern, wenn ein Automorphismus $\sigma \colon \overline{k} \to \overline{k}$ von k-Algebren mit $\varphi_2 = \sigma\varphi_1$ existiert.*
- *(c) Ein Element $a \in A$ ist genau dann nilpotent, wenn $\varphi(a) = 0$ für alle Morphismen $\varphi \colon A \to \overline{k}$ von k-Algebren gilt.*

8.2.5 (Umformulierung des Hilbertschen Nullstellensatzes)**.** Die Aussage (a) besagt, dass die Abbildung

$$\begin{aligned} \mathrm{Alg}_k(A, \overline{k}) &\twoheadrightarrow \mathrm{MaxSpec}(A), \\ \varphi &\mapsto \ker(\varphi), \end{aligned} \tag{8.2.2}$$

wohldefiniert und surjektiv ist. (Hier bezeichnet $\mathrm{Alg}_k(A, \overline{k})$ die Menge der Morphismen $A \to \overline{k}$ von k-Algebren.) Sei $\mathrm{Aut}_k(\overline{k})$ die Menge der Automorphismen der k-Algebra $\overline{k}$ (also die Menge der invertierbaren Elemente in $\mathrm{Alg}_k(\overline{k}, \overline{k})$). Nach (b) liefert die obige Surjektion eine Bijektion

$$\mathrm{Alg}_k(A, \overline{k})/\mathrm{Aut}_k(\overline{k}) \xrightarrow{\sim} \mathrm{MaxSpec}(A), \tag{8.2.3}$$

wobei die Menge auf der linken Seite die Menge der Äquivalenzklassen bezüglich der Äquivalenzrelation $\varphi_1 \sim \varphi_2 \iff \exists \sigma \in \mathrm{Aut}_k(\overline{k}) : \varphi_2 = \sigma\varphi_1$ ist.[29] Unter Verwendung von (a) ist (c) äquivalent zu

$$\mathrm{Nil}(A) = \bigcap_{\mathfrak{m} \in \mathrm{MaxSpec}\, A} \mathfrak{m}. \tag{8.2.4}$$

Die rechte Seite ist per Definition 2.8.1 das Jacobsonradikal $\mathrm{Jac}(A)$ von A, d. h.

$$\mathrm{Nil}(A) = \mathrm{Jac}(A).$$

Für endlich erzeugte Algebren über einem Körper stimmen also Nilradikal und Jacobsonradikal überein.

8.2.6. Man kann (8.2.4) auch als Verschärfung der Charakterisierung $\mathrm{Nil}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\, R} \mathfrak{p}$ des Nilradikals für einen beliebigen Ring R verstehen ((2.7.2) in Proposition 2.7.11).

8.2.7. Ist $\mathfrak{a} \subset A$ ein beliebiges Ideal, so gilt

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m} \in \mathcal{V}(\mathfrak{a}) \cap (\mathrm{MaxSpec}\, A)} \mathfrak{m}, \tag{8.2.5}$$

denn (8.2.4), angewandt auf $A/\mathfrak{a}$, liefert $\mathrm{Nil}(A/\mathfrak{a}) = \bigcap_{\mathfrak{n} \in \mathrm{MaxSpec}\, A/\mathfrak{a}} \mathfrak{n}$, und das inverse Bild dieser Gleichheit unter $A \twoheadrightarrow A/\mathfrak{a}$ ist die gesuchte Gleichheit.

Diese Gleichheit zeigt, dass endlich erzeugte Algebren über Körpern Jacobson-Ringe sind, siehe 00FZ.

8.2.8. Ist k algebraisch abgeschlossen, so spezialisiert (8.2.3) zu der Bijektion

$$\mathrm{Alg}_k(A, k) \xrightarrow{\sim} \mathrm{MaxSpec}(A),$$

denn dann gilt $\mathrm{Aut}_k(\overline{k}) = \mathrm{Aut}_k(k) = \{\mathrm{id}_k\}$.

Beweis. (a) Sei $\mathfrak{a} \subset A$ ein maximales Ideal. Nach der schwachen Version des Hilbertschen Nullstellensatzes 8.2.1 ist $k \subset A/\mathfrak{m}$ eine endliche und damit algebraische Körpererweiterung. Also gibt es einen (injektiven) Morphismus $A/\mathfrak{m} \to \overline{k}$ von k-Algebren, oder, mit anderen Worten, von Körpererweiterungen von k (nach einem wohlbekannten Fortsetzungssatz für algebraische Körpererweiterungen[30]). Die Verknüpfung $A \twoheadrightarrow A/\mathfrak{a} \hookrightarrow \overline{k}$ ist dann ein Morphismus von k-Algebren mit Kern $\mathfrak{a}$.

Sei $\varphi\colon A \to \overline{k}$ ein Morphismus von k-Algebren. Wir erhalten den injektiven Morphismus $\overline{\varphi}\colon A/\ker(\varphi) \hookrightarrow \overline{k}$ von k-Algebren, d. h. ein kommutatives Diagramm

$$\begin{tikzcd}
A/\ker(\varphi) \arrow[r, hook, "\overline{\varphi}"] & \overline{k} \\
k \arrow[u, hook] \arrow[ur, hook]
\end{tikzcd}$$

von Ringen. Man beachte, dass alle Morphismen injektiv sind. Da $k \subset \overline{k}$ algebraisch ist, ist $k \hookrightarrow A/\ker(\varphi)$ eine ganze Ringerweiterung. Da k ein Körper ist und $A/\ker(\varphi)$ ein Integritätsbereich (da es nach $\overline{k}$ einbettet), ist auch $A/\ker(\varphi)$ ein Körper (Proposition 7.2.1). Also ist $\ker(\varphi)$ ein maximales Ideal.

(b) Existiert ein Automorphismus σ mit $\varphi_2 = \sigma\varphi_1$, so gilt offensichtlich $\ker(\varphi_1) = \ker(\varphi_2)$.

---

[29] Die Notation kommt daher, dass dies der Raum der Bahnen der offensichtlichen Operation der Gruppe $\mathrm{Aut}_{\mathrm{Alg}_k}(\overline{k})$ auf der Menge $\mathrm{Hom}_{\mathrm{Alg}_k}(A, \overline{k})$ ist.

[30] Brutal kann man wie folgt argumentieren. Sei L ein algebraischer Abschluss von $A/\mathfrak{m}$. Dann ist L auch ein algebraischer Abschluss von k, und somit (nichtkanonisch) isomorph zu $k \subset \overline{k}$

Gelte nun $\ker(\varphi_1) = \ker(\varphi_2)$. Nach (a) ist dies ein maximales Ideal $\mathfrak{m} := \ker(\varphi_1) = \ker(\varphi_2)$. Wir erhalten das kommutative Diagramm

$$\begin{tikzcd}
\overline{k} \arrow[rr, "\sigma", "\sim"'] & & \overline{k} \\
\cup & & \cup \\
\varphi_1(A) & A/\mathfrak{m} \arrow[l, "\sim", "\overline{\varphi}_1"'] \arrow[r, "\sim", "\overline{\varphi}_2"'] & \varphi_2(A) \\
& A \arrow[ul, "\varphi_1"] \arrow[u, two heads] \arrow[ur, "\varphi_2"'] &
\end{tikzcd}$$

Der Isomorphismus $\overline{\varphi}_2\overline{\varphi}_1^{-1}$ von Körpern läßt sich wie angedeutet zu einem Isomorphismus $\sigma\colon \overline{k} \xrightarrow{\sim} \overline{k}$ der algebraischen Abschlüsse ausdehnen. Es folgt $\sigma\varphi_1 = \varphi_2$.

(c) Sei $a \in A$. Ist a nilpotent, so ist für alle $\varphi\colon A \to \overline{k}$ in Alg_k das Element $\varphi(a) \in \overline{k}$ nilpotent und somit Null, da $\overline{k}$ ein Körper ist.

Sei nun a nicht nilpotent. Es folgt $A[a^{-1}] = A_a \neq 0$ für die Lokalisierung (siehe 6.1.11). Somit gibt es ein maximales Ideal $\mathfrak{m}$ in $A[a^{-1}]$ (Satz 2.6.13). Mit A ist auch $A[a^{-1}]$ eine endlich erzeugte k-Algebra (zu Erzeugern von A füge man a^{-1} hinzu). Somit liefert Teil (a) einen Morphismus $A[a^{-1}] \to \overline{k}$ von k-Algebren mit Kern $\mathfrak{m}$. Er bildet das invertierbare Element $\frac{a}{1}$ auf eine Einheit in $\overline{k}$ ab. Die Verknüpfung $\varphi\colon A \to A[a^{-1}] \to \overline{k}$ ist also der gesuchte Morphismus von k-Algebren mit $\varphi(a) \neq 0$. □

Aufgabe 8.2.9. Folgern Sie die schwache Version des Hilbertschen Nullstellensatzes 8.2.1 aus der starken Version 8.2.4.

Korollar 8.2.10. *Sei $\varphi\colon A \to B$ ein Morphismus von Algebren über einem Körper k und sei B endlich erzeugt als k-Algebra. Ist $\mathfrak{m} \subset B$ ein maximales Ideal, so ist $\varphi^{-1}(\mathfrak{m}) \subset A$ ebenfalls maximal.*

Mit anderen Worten erhalten wir ein kommutatives Diagramm

$$\begin{tikzcd}
\operatorname{Spec} A & \operatorname{Spec} B \arrow[l, "\operatorname{Spec}\varphi"'] \\
\cup & \cup \\
\operatorname{MaxSpec} A & \operatorname{MaxSpec} B. \arrow[l, dotted]
\end{tikzcd}$$

Beweis. Nach Teil (a) des Hilbertschen Nullstellensatzes 8.2.4 gilt $\mathfrak{m} = \ker(\psi)$ für einen Morphismus $B \to \overline{k}$ von k-Algebren, wobei $\overline{k}$ ein algebraischer Abschluss von k ist. Wir erhalten Inklusionen

$$k \hookrightarrow A/\varphi^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$$

von Ringen. Da der Körper $B/\mathfrak{m}$ als k-Algebra endlich erzeugt ist, ist $k \subset B/\mathfrak{m}$ eine endliche und damit algebraische Körpererweiterung, nach der schwachen Version des Hilbertschen Nullstellensatzes 8.2.1. Insbesondere ist $A/\varphi^{-1}(\mathfrak{m}) \subset B/\mathfrak{m}$ eine ganze Ringerweiterung. Mit $B/\mathfrak{m}$ ist damit auch $A/\varphi^{-1}(\mathfrak{m})$ ein Körper (Proposition 7.2.1). Also ist $\varphi^{-1}(\mathfrak{m})$ ein maximales Ideal in A. □

8.2.11. Ist $\varphi\colon A \to B$ ein Morphismus endlich erzeugter k-Algebren, so erhalten wir das folgende kommutative Diagramm, dessen vertikalen Pfeile nach (8.2.2) surjektiv sind.

$$\begin{tikzcd}
\operatorname{Spec} A & \operatorname{Spec} B \arrow[l, "\operatorname{Spec}\varphi"'] \\
\cup & \cup \\
\operatorname{MaxSpec} A & \operatorname{MaxSpec} B \arrow[l, dotted] \\
\mathrm{Alg}_k(A, \overline{k}) \arrow[u, two heads] & \mathrm{Alg}_k(B, \overline{k}) \arrow[l, "\varphi^*"'] \arrow[u, two heads]
\end{tikzcd}$$

Es folgt, dass der gestrichelte Pfeil existiert, so dass das Diagramm kommutativ bleibt. Insbesondere bildet $\varphi^{-1}\colon \operatorname{Spec} B \to \operatorname{Spec} A$ maximale Ideale auf maximale Ideale ab. Dies liefert einen Beweis von Korollar 8.2.10 unter der Zusatzvoraussetzung, dass auch A von endlichem Typ ist.

Es folgt, dass MaxSpec einen Funktor von der Kategorie der endlich erzeugte Algebren über einem fixierten Körper in die Kategorie der Mengen (oder topologischen Räume) definiert.

Korollar 8.2.12. *Sei A eine endlich erzeugte Algebra über einem Körper k und sei $\mathfrak{a} \subset A$ ein Ideal. Dann ist $\mathcal{V}(\mathfrak{a}) \cap \operatorname{MaxSpec} A$ dicht in $\mathcal{V}(\mathfrak{a})$.*

Beweis. Sei $\mathfrak{b} \subset A$ ein Ideal mit $\mathcal{V}(\mathfrak{a}) \cap \operatorname{MaxSpec} A \subset \mathcal{V}(\mathfrak{b})$. Es folgt $\mathcal{V}(\mathfrak{a}) \cap \operatorname{MaxSpec} A \subset \mathcal{V}(\mathfrak{b}) \cap \operatorname{MaxSpec} A$. Aus (8.2.5) erhalten wir $\sqrt{\mathfrak{a}} \supset \sqrt{\mathfrak{b}}$. Daraus folgt $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\sqrt{\mathfrak{a}}) \subset \mathcal{V}(\sqrt{\mathfrak{b}}) = \mathcal{V}(\mathfrak{b})$. Die Behauptung folgt, denn $\mathcal{V}(\mathfrak{a})$ ist eine abgeschlossene Teilmenge, die $\mathcal{V}(\mathfrak{a}) \cap \operatorname{MaxSpec} A$ enthält. □

8.2.13. Ist k ein beliebiger Ring und R eine k-Algebra, so ist die Abbildung

$$
\begin{aligned}
R^n &\xrightarrow{\sim} \operatorname{Alg}_k(k[T_1, \dots, T_n], R), \\
x &\mapsto \operatorname{ev}_x, \\
(f(T_1), \dots, f(T_n)) &\mapsfrom f,
\end{aligned}
\tag{8.2.6}
$$

bijektiv. Ist $\mathfrak{a} \subset k[T_1, \dots, T_n]$ ein Ideal oder allgemeiner eine Teilmenge, so definieren wir

$$
\mathbf{V}(\mathfrak{a})_R := \{x \in R^n \mid f(x) = 0 \text{ für alle für alle } f \in \mathfrak{a}\}. \tag{8.2.7}
$$

Sei nun $\mathfrak{a} \subset k[T_1, \dots, T_n]$ ein Ideal. Die kanonische Surjektion $\operatorname{can}\colon k[T_1, \dots, T_n] \to k[T_1, \dots, T_n]/\mathfrak{a}$ von k-Algebren liefert eine injektive Abbildung

$$
\begin{aligned}
\operatorname{can}^*\colon \operatorname{Alg}_k(k[T_1, \dots, T_n]/\mathfrak{a}, R) &\to \operatorname{Alg}_k(k[T_1, \dots, T_n], R), \\
\varphi &\mapsto \varphi \circ \operatorname{can}.
\end{aligned}
$$

Nach der universellen Eigenschaft des Quotienten liegt ein Element $\psi \in \operatorname{Alg}_k(k[T_1, \dots, T_n], R)$ genau dann im Bild dieser Injektion, wenn $\psi(\mathfrak{a}) = 0$ gilt.

Für $x \in R^n$ gilt genau dann $x \in \mathbf{V}(\mathfrak{a})_R$, wenn $\operatorname{ev}_x(\mathfrak{a}) = 0$ gilt. Die Bijektion (8.2.6) liefert somit ein kommutatives Diagramm

$$
\begin{tikzcd}
R^n \arrow[r, "\sim"] & \operatorname{Alg}_k(k[T_1, \dots, T_n], R) \\
\mathbf{V}(\mathfrak{a})_R \arrow[u, phantom, "\cup"] \arrow[r, "\sim"] & \operatorname{Alg}_k(k[T_1, \dots, T_n]/\mathfrak{a}, R) \arrow[u, hook, "\operatorname{can}^*"]
\end{tikzcd}
$$

Explizit ist die untere Horizontale wie folgt gegeben.

$$
\begin{aligned}
\mathbf{V}(\mathfrak{a})_R &\xrightarrow{\sim} \operatorname{Alg}_k(k[T_1, \dots, T_n]/\mathfrak{a}, R), \\
x &\mapsto \Big(\overline{\operatorname{ev}}_x\colon \overline{f} \mapsto f(x_1, \dots, x_n)\Big).
\end{aligned}
\tag{8.2.8}
$$

Korollar 8.2.14. *Sei k ein Körper, $\mathfrak{a} \subset k[T_1, \dots, T_n]$ ein Ideal, und $\overline{k}$ ein algebraischer Abschluss von k. Die Abbildung*

$$
\begin{aligned}
\mathbf{V}(\mathfrak{a})_{\overline{k}} &\twoheadrightarrow \operatorname{MaxSpec}(k[T_1, \dots, T_n]/\mathfrak{a}), \\
x &\mapsto \ker(\overline{\operatorname{ev}}_x) = \ker(\operatorname{ev}_x)/\mathfrak{a},
\end{aligned}
$$

ist surjektiv und induziert eine Bijektion

$$
\mathbf{V}(\mathfrak{a})_{\overline{k}}/\operatorname{Aut}_k(\overline{k}) \xrightarrow{\sim} \operatorname{MaxSpec}(k[T_1, \dots, T_n]/\mathfrak{a}), \tag{8.2.9}
$$

wobei die Menge auf der linken Seite die Menge der Äquivalenzklassen bezüglich der Äquivalenzrelation $x \sim y \iff \exists \sigma \in \operatorname{Aut}_k(\overline{k}) : y = \sigma(x) := (\sigma(x_1), \dots, \sigma(x_n))$ ist.

Beweis. Dies folgt aus dem Hilbertschen Nullstellensatz 8.2.4, Teilaussagen (a) und (b), und den elementaren Überlegungen in 8.2.13. Genauer kombinieren wir die Bijektion (8.2.8) für $R = \overline{k}$ mit der Surjektion (8.2.2) und erhalten

$$
\mathbf{V}(\mathfrak{a})_{\overline{k}} \xrightarrow{\sim} \operatorname{Alg}_k(k[T_1, \dots, T_n]/\mathfrak{a}, \overline{k}) \twoheadrightarrow \operatorname{MaxSpec}(k[T_1, \dots, T_n]/\mathfrak{a}).
$$

Wir haben die Fasern der Surjektion in 8.2.5 durch eine Äquivalenzrelation beschrieben, siehe (8.2.3). Diese Äquivalenzrelation ist kompatibel mit der im Korollar definierten Äquivalenzrelation auf $\mathbf{V}(\mathfrak{a})_{\overline{k}}$: Für $x \in \mathbf{V}(\mathfrak{a})_{\overline{k}}$ und $\sigma \in \operatorname{Aut}_k(\overline{k})$ gilt nämlich $\sigma \overline{\operatorname{ev}}_x = \overline{\operatorname{ev}}_{\sigma x}$: Für $f \in k[T_1, \dots, T_n]$ gilt $\sigma(f(x)) = f(\sigma(x))$, denn $\sigma|_k = \operatorname{id}_k$ ist die Identität auf den Koeffizienten von f. Die Behauptung folgt. □

Beispiel 8.2.15. Sei $A = \mathbb{R}[X,Y]/(X^2+Y^2-1)$. Dann spezialisiert (8.2.9) zu der Bijektion

$$\mathbf{V}(X^2+Y^2-1)_{\mathbb{C}}/\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \xrightarrow{\sim} \operatorname{MaxSpec} A.$$

Für jedes maximale Ideal $\mathfrak{m}$ von A gibt es also ein Element $(x,y) \in \mathbb{C}^2$ mit $x^2+y^2 = 1$, so dass $\mathfrak{m} = \ker(\overline{\mathrm{ev}_{(x,y)}}\colon A \to \mathbb{C})$. Die Faser der obigen Abbildung über diesem maximalen Ideal $\mathfrak{m}$ ist $\{(x,y),(\overline{x},\overline{y})\}$. Sie besteht genau dann aus nur einem Element, wenn sowohl x als auch y reell sind.

Korollar 8.2.16. *Sei k ein algebraisch abgeschlossener Körper und $n \in \mathbb{N}$. Dann ist die Abbildung*

$$k^n \xrightarrow{\sim} \operatorname{MaxSpec} k[T_1,\dots,T_n], \qquad (8.2.10)$$
$$x = (x_1,\dots,x_n) \mapsto \ker\Big(\mathrm{ev}_x\colon f \mapsto f(x_1,\dots,x_n)\Big),$$

bijektiv. Ist $\mathfrak{a} \subset k[T_1,\dots,T_n]$ ein Ideal, so erhalten wir genauer das kommutative Diagramm

$$\begin{tikzcd} k^n \arrow[rr, "\sim"] & & \operatorname{MaxSpec} k[T_1,\dots,T_n] \\ \mathbf{V}(\mathfrak{a})_k \arrow[u, phantom, "\cup"] \arrow[r, "\sim"] & \operatorname{MaxSpec}(k[T_1,\dots,T_n]/\mathfrak{a}) \arrow[r, "\sim"] & \mathcal{V}(\mathfrak{a}) \cap \operatorname{MaxSpec} k[T_1,\dots,T_n] \arrow[u, phantom, "\cup"] \end{tikzcd} \qquad (8.2.11)$$

mit horizontalen Bijektionen.

Insbesondere ist die Bijektion (8.2.10) ein Isomorphismus von topologischen Räumen, wenn man die Teilmenge $\operatorname{MaxSpec} k[T_1,\dots,T_n] \subset \operatorname{Spec} k[T_1,\dots,T_n]$. mit der Unterraumtopologie versieht.

8.2.17. Die erste Behauptung von Korollar 8.2.16 wird auch oft als Hilbertscher Nullstellensatz bezeichnet.

8.2.18. Korollar 8.2.16 wird auch oft als Hilbertscher Nullstellensatz bezeichnet.

8.2.19. Die Bijektion (8.2.10) besagt, dass es für jedes maximale Ideal $\mathfrak{m} \subset k[T_1,\dots,T_n]$ genau einen Punkt $x \in k^n$ gibt, an dem alle Elemente von $\mathfrak{m}$ verschwinden.

Da jedes echte Ideal in einem maximalen Ideal enthalten ist, hat jedes Ideal $\mathfrak{a} \subsetneq k[S_1,\dots,S_n]$ eine gemeinsame Nullstelle x in k^n in dem Sinne, dass alle Elemente von $\mathfrak{a}$ bei x verschwinden. Daher kommt wohl der Name Nullstellensatz.

Beweis. Die Bijektionen sind Spezialfälle von Korollar 8.2.14, und Kommutativität ist offensichtlich. □

Aufgabe 8.2.20. Seien $a, b \in \mathbb{C}[T]$ Polynome. Betrachten Sie den durch $X \mapsto a$, $Y \mapsto b$ definierten Morphismus

$$\varphi\colon \mathbb{C}[X,Y] \to \mathbb{C}[T]$$

von $\mathbb{C}$-Algebren.

(a) Geben Sie den gestrichelten Morphismus p explizit an, der das folgende Diagramm kommutativ macht. Seine vertikalen Pfeile sind die Bijektionen aus Korollar 8.2.16, der untere horizontale Morphismus ist der von φ induzierte Morphismus $\mathfrak{m} \mapsto \varphi^{-1}(\mathfrak{m})$ auf den Maximalspektren (siehe Korollar 8.2.10).

$$\begin{tikzcd} \mathbb{C}^2 \arrow[r, dotted, "p"] \arrow[d, "\sim"] & \mathbb{C} \arrow[d, "\sim"] \\ \operatorname{MaxSpec} \mathbb{C}[X,Y] \arrow[r, "\varphi^{-1}"] & \operatorname{MaxSpec} \mathbb{C}[T] \end{tikzcd}$$

(b) Seien $a = T^2 - 1$ und $b = T(T^2-1)$. Zeigen Sie, dass in diesem Fall das Bild von p genau $\mathbf{V}(X^2(X+1)-Y^2)_{\mathbb{C}}$ ist. Skizzieren Sie den reellen Teil $\mathbf{V}(X^2(X+1)-Y^2)_{\mathbb{R}}$.

(c) Ist φ endlich? Was ist der Kern von φ. (Gelöst in Abschnitt **??** im Anhang.)

8.2.21. Korollar 8.2.14 liefert im Spezialfall $\mathfrak{a} = (0)$ die Bijektion

$$\overline{k}^n/\mathrm{Aut}_k(\overline{k}) \xrightarrow{\sim} \operatorname{MaxSpec}(k[T_1,\dots,T_n]).$$

Beispiel 8.2.22. Jedes Element $x \in \mathbb{C}^n$ definiert per $\ker(\mathrm{ev}_x)$ ein maximales Ideal von $\mathbb{R}[X_1, \dots, X_n]$, und jedes maximale Ideal ist von dieser Form. Zwei Elemente $x, y \in \mathbb{C}^n$ liefern genau dann dasselbe maximale Ideal, wenn $y = x$ gilt oder $y = \overline{x} := (\overline{x}_1, \dots, \overline{x}_n)$ (der Überstrich meint hier komplexe Konjugation, $\overline{a + bi} = a - bi$ für $a, b \in \mathbb{R}$). Man erhält also beispielsweise

$$\mathbb{C}_{\mathrm{Im}(z) \geq 0} \xrightarrow{\sim} \mathbb{C}/\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \xrightarrow{\sim} \mathrm{MaxSpec}\, \mathbb{R}[X]. \tag{8.2.12}$$

Man vergleiche dies mit (2.11.1).

bis hier, Mittwoch, 25. Januar

8.3. **Algebraische Teilmengen.** In Vorlesung annehmen, dass k ein Körper ist. Dazusagen, wann algebraisch abgeschlossen.

In diesem Abschnitt sei k ein Ring. Der Einfachheit halber mag der Leser annehmen, dass k ein algebraisch abgeschlossener Körper ist.

8.3.1. Ist $\mathfrak{a} \subset k[S_1, \dots, S_n]$ eine Teilmenge, so erinnern wir an die Definition

$$\mathbf{V}(\mathfrak{a}) := \mathbf{V}(\mathfrak{a})_k = \{x \in k^n \mid f(x) = 0 \text{ für alle } f \in \mathfrak{a}\},$$

siehe (8.2.7).

Notation 8.3.2. Wir schreiben $\mathbf{V}(f_1, \dots, f_m) := \mathbf{V}(\{f_1, \dots, f_m\})$.

8.3.3. Ist $E \subset k[S_1, \dots, S_n]$ eine Teilmenge und $\mathfrak{a}$ das von E erzeugte Ideal, so gilt $\mathbf{V}(E) = \mathbf{V}(\mathfrak{a})$.

8.3.4. Aus $E \subset F$ folgt $\mathbf{V}(E) \supset \mathbf{V}(F)$.

Proposition 8.3.5. *Sei k ein Integritätsbereich und betrachte $X = k^n$. Dann gelten*

$$\mathbf{V}(0) = X, \qquad \mathbf{V}(1) = \emptyset,$$

$$\bigcap_{i \in I} \mathbf{V}(E_i) = \mathbf{V}(\bigcup_{i \in I} E_i), \qquad \mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a}\mathfrak{b})$$

für beliebige Familien $(E_i)_{i \in I}$ von Teilmengen von $k[S_1, \dots, S_n]$ und Ideale $\mathfrak{a}, \mathfrak{b} \subset k[S_1, \dots, S_n]$.

Beweis. Die ersten drei Gleichheiten sind offensichtlich. Wegen $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$ und $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$ folgt

$$\mathbf{V}(\mathfrak{a} \cdot \mathfrak{b}) \supset \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) \supset \mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}).$$

Zu zeigen bleibt $\mathbf{V}(\mathfrak{a} \cdot \mathfrak{b}) \subset \mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b})$. Sei $x \in \mathbf{V}(\mathfrak{a} \cdot \mathfrak{b})$. Gilt $x \in \mathbf{V}(\mathfrak{a})$, so sind wir fertig. Sonst gibt es ein $a \in \mathfrak{a}$ mit $a(x) \neq 0$. Für alle $b \in \mathfrak{b}$ gilt dann $0 = (ab)(x) = a(x)b(x)$ in k. Da k ein Integritätsbereich ist, folgt $b(x) = 0$, und somit $x \in \mathbf{V}(\mathfrak{b})$. □

8.3.6. Ist man an der Aussage von Proposition 8.3.5 nur für algebraisch abgeschlossene Körper k interessiert, so kann man sie auch wie folgt beweisen: Nach Korollar 8.2.16 gilt für ein Ideal (oder auch eine Teilmenge) $\mathfrak{a} \subset k[S_1, \dots, S_n]$

$$\mathbf{V}(\mathfrak{a}) \xrightarrow{\sim} \mathcal{V}(\mathfrak{a}) \cap \mathrm{MaxSpec}\, k[S_1, \dots, S_n].$$

Damit folgen alle Gleichheiten aus den entsprechenden Gleichheiten in Proposition 2.11.6.

Definition 8.3.7. Eine Teilmenge $X \subset k^n$ heißt **algebraisch**, falls es eine Teilmenge $\mathfrak{a} \subset k[S_1, \dots, S_n]$ gibt mit $X = \mathbf{V}(\mathfrak{a})$.

8.3.8. Ist k ein Körper, so nennen manche Autoren (etwa [Kem11]) eine algebraische Teilmenge eine affine Varietät. Manche Autoren verlangen Zusatzbedingungen: In [Har77, Kapitel I] etwa wird zusätzlich verlangt, dass k algebraisch abgeschlossen ist und dass die algebraische Teilmenge irreduzibel ist (im Sinne der Definition 8.3.24).

Beispiel 8.3.9. Für jedes $x \in k^n$ ist die einelementige Menge $\{x\} = \mathbf{V}(S_1 - x_1, \dots, S_n - x_n) \subset k^n$ algebraisch.

Aufgabe 8.3.10. Sei k ein endlicher Körper. Dann ist jede Teilmenge $X \subset k^n$ algebraisch.

Aufgabe 8.3.11. Welche der folgenden Teilmengen von $\mathbb{C}$ bzw. $\mathbb{C}^2$ sind algebraisch?

$$\begin{aligned} A &:= \mathbb{N} \\ B &:= \mathbb{Z} \times \mathbb{Z}, \\ C &:= \{(x, y) \mid \exp(x^7 + 3xy) = \pi\}, \\ D &:= \{(x, \sin(x)) \in \mathbb{C}^2 \mid x \in \mathbb{C}\}, \\ E &:= \{(x, \exp(x)) \in \mathbb{C}^2 \mid x \in \mathbb{C}\}, \\ F &:= \{(y^5 + 3y^4 + y + \pi, y) \in \mathbb{C}^2 \mid y \in \mathbb{C}\}, \\ G &:= E \cap F. \end{aligned}$$

Achtung bei der Menge C! Die Antwort für $C \cap \mathbb{R}^2$ als Teilmenge von $\mathbb{R}^2$ fällt anders aus.

8.3.12. Proposition 8.3.5 besagt, dass wir k^n als topologischen Raum auffassen können, dessen abgeschlossene Mengen genau die algebraischen Teilmengen sind.

Definition 8.3.13. Die **Zariski-Topologie** auf k^n ist die Topologie, deren abgeschlossene Mengen genau die algebraischen Teilmengen sind. Man nennt diese Teilmengen auch **Zariski-abgeschlossene** Teilmengen.

Aufgabe 8.3.14. Die Zariski-Topologie auf k^n ist die gröbste Topologie, so dass für alle Polynome $f \in k[S_1, \dots, S_n]$ die polynomiale Abbildung $k^n \to k$, $x \mapsto f(x)$, stetig ist.

Aufgabe 8.3.15. Jede Abbildung $\mathbb{C} \to \mathbb{C}$ mit endlichen Fasern ist stetig bezüglich der Zariski-Topologie. Zum Beispiel ist jede Bijektion von $\mathbb{C}$ stetig.

Lemma 8.3.16. *Sind k ein reduzierter Ring (siehe Definition 2.7.8) und $\mathfrak{a} \subset k[S_1, \dots, S_n]$ ein Ideal, so gilt $\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\sqrt{\mathfrak{a}})$.*

Beweis. Wegen $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ gilt $\mathbf{V}(\mathfrak{a}) \supset \mathbf{V}(\sqrt{\mathfrak{a}})$. Sei $x \in \mathbf{V}(\mathfrak{a})$ und $f \in \sqrt{\mathfrak{a}}$. Dann gilt $f^n \in \mathfrak{a}$ für ein $n \in \mathbb{N}$, und somit $0 = f^n(x) = f(x)^n$. Da k reduziert ist, folgt $f(x) = 0$, also $x \in \mathbf{V}(\sqrt{\mathfrak{a}})$. □

Definition 8.3.17. Ist $X \subset k^n$ eine beliebige Teilmenge, so definieren wir das **Verschwindungsideal** von X durch

$$\begin{aligned} \mathbf{I}(X) &:= \{f \in k[S_1, \dots, S_n] \mid f(x) = 0 \text{ für alle } x \in X\} \\ &= \bigcap_{x \in X} \ker(\mathrm{ev}_x). \end{aligned}$$

8.3.18. Aus $X \subset Y$ folgt $\mathbf{I}(X) \supset \mathbf{I}(Y)$.

Lemma 8.3.19. *Sind k ein reduzierter Ring (siehe Definition 2.7.8) und $X \subset k^n$ eine Teilmenge, so ist $\mathbf{I}(X)$ ein Radikalideal: $\mathbf{I}(X) = \sqrt{\mathbf{I}(X)}$.*

Beweis. Sei $f \in \sqrt{\mathbf{I}(X)}$, also $f^n \in \mathbf{I}(X)$ für ein $n \in \mathbb{N}$. Für $x \in X$ gilt dann $0 = f^n(x) = f(x)^n$. Da k reduziert ist, folgt $f(x) = 0$, also $f \in \mathbf{I}(X)$. □

8.3.20. Die Zuordnungen $X \mapsto \mathbf{I}(X)$ und $E \mapsto \mathbf{V}(E)$ definieren Abbildungen

$$\mathbf{I} \colon \{\text{Teilmengen von } k^n\} \rightleftarrows \{\text{Teilmengen von } k[S_1, \dots, S_n]\} \colon \mathbf{V}$$

Satz 8.3.21. *Sei k ein algebraisch abgeschlossener Körper. Dann gelten:*

(a) Ist $E \subset k[S_1, \dots, S_n]$ eine Teilmenge, so gilt

$$\mathbf{I}(\mathbf{V}(E)) = \sqrt{\langle E \rangle}. \tag{8.3.1}$$

Hier bezeichnet $\langle E \rangle$ das von E erzeugte Ideal.[31]

(b) Ist $X \subset k^n$ eine Teilmenge, so gilt

$$\mathbf{V}(\mathbf{I}(X)) = \overline{X}. \tag{8.3.2}$$

Hier bezeichnet $\overline{X}$ den Abschluss von X in k^n, also die kleinste algebraische Teilmenge von k^n, die X enthält.

[31] Dies ist die Formulierung des Hilbertschen Nullstellensatzes in [AM69, Aufgabe 14, Seite 85].

Insbesondere erhalten wir zueinander inverse inklusionsumkehrende Bijektionen

$$\mathbf{I}\colon \{\textit{algebraische Teilmengen von } k^n\} \overset{\sim}{\rightleftarrows} \{\textit{Radikalideale von } k[S_1,\dots,S_n]\}\colon \mathbf{V}. \tag{8.3.3}$$

8.3.22. Behauptung (a) wird auch oft als Hilbertscher Nullstellensatz bezeichnet. In [Har77, Theorem 1.3A] etwa wird er so formuliert: Sei $\mathfrak{a} \subset k[S_1,\dots,S_n]$ ein Ideal. Ist $f \in k[S_1,\dots,S_n]$ ein Polynom, das auf dem Nullstellengebilde $\mathbf{V}(\mathfrak{a})$ verschwindet, so liegt eine Potenz von f bereits in $\mathfrak{a}$. Dies ist schlicht die verbale Formulierung von $\mathbf{I}(\mathbf{V}(\mathfrak{a})) \subset \sqrt{\mathfrak{a}}$.

Beweis. (a) Sei $\mathfrak{a} := \langle E\rangle$ das von E erzeugte Ideal. Wegen $\mathbf{V}(E) = \mathbf{V}(\mathfrak{a})$ genügt es, $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ zu zeigen.

$\supset$: Offensichtlich gilt $\mathfrak{a} \subset \mathbf{I}(\mathbf{V}(\mathfrak{a}))$. Daraus folgt $\sqrt{\mathfrak{a}} \subset \sqrt{\mathbf{I}(\mathbf{V}(\mathfrak{a}))} = \mathbf{I}(\mathbf{V}(\mathfrak{a}))$ (Lemma 8.3.19).

$\subset$: Sei $f \in \mathbf{I}(\mathbf{V}(\mathfrak{a}))$. Wir betrachen $\overline{f} \in A := k[S_1,\dots,S_n]/\mathfrak{a}$. Sei $\varphi\colon A \to k$ ein beliebiger Morphismus von k-Algebren. Nach der Bijektion (8.2.8) (für $R = k$) gilt $\varphi = \overline{\mathrm{ev}}_x$ für ein eindeutiges $x \in \mathbf{V}(\mathfrak{a})$. Somit gilt $\varphi(\overline{f}) = \overline{\mathrm{ev}}_x(\overline{f}) = \mathrm{ev}_x(f) = f(x) = 0$. Nach Teilaussage (c) des Hilbertschen Nullstellensatzes 8.2.4 ist also $\overline{f} \in A$ nilpotent. Dies bedeutet, dass es ein $n \in \mathbb{N}$ gibt mit $f^n \in \mathfrak{a}$. Es gilt also $f \in \sqrt{\mathfrak{a}}$.

Formellastiger und im wesentlichen äquivalent kann man die Aussage auch so zeigen:

$$\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \bigcap_{x\in\mathbf{V}(\mathfrak{a})} \ker(\mathrm{ev}_x) \overset{(8.2.11)}{=} \bigcap_{\mathfrak{m}\in\mathcal{V}(\mathfrak{a})\cap\operatorname{MaxSpec} k[S_1,\dots,S_n]} \mathfrak{m} \overset{(8.2.5)}{=} \sqrt{\mathfrak{a}}.$$

(b) Offenbar gilt $X \subset \mathbf{V}(\mathbf{I}(X))$. Sei $\mathfrak{a} \subset k[S_1,\dots,S_n]$ ein Ideal mit $X \subset \mathbf{V}(\mathfrak{a})$. Es folgt

$$\mathbf{I}(X) \supset \mathbf{I}(\mathbf{V}(\mathfrak{a})) \overset{(a)}{=} \sqrt{\mathfrak{a}} \supset \mathfrak{a}$$

und somit $\mathbf{V}(\mathbf{I}(X)) \subset \mathbf{V}(\mathfrak{a})$. Somit ist $\mathbf{V}(\mathbf{I}(X))$ die kleinste algebraische Teilmenge von k^n, die X enthält, d. h. $\overline{X} = \mathbf{V}(\mathbf{I}(X))$. □

Beispiel 8.3.23. Für Körper, die nicht algebraisch abgeschlossen sind, ist die Aussage falsch. Zum Beispiel gilt $\mathbf{V}(S^2+1)_{\mathbb{R}} = \emptyset$, also $\mathbf{I}(\mathbf{V}(S^2+1)) = \mathbb{R}[S] \neq \sqrt{(S^2+1)} = (S^2+1)$. Dasselbe Argument funktioniert über einem beliebigen nicht algebraisch abgeschlossenen Körper k: Statt S^2+1 wähle man ein irreduzibles Polynom in $k[S]$ ohne Nullstelle in k.

Definition 8.3.24. Ein topologischer Raum X heißt **irreduzibel**, falls $X \neq \emptyset$ gilt und für alle abgeschlossenen Teilmengen A, B von X mit $X = A \cup B$ schon $X = A$ oder $X = B$ folgt.

8.3.25. Jede Teilmenge $X \subset k^n$ ist mit der Teilmengentopologie ein topologischer Raum. Genau dann ist X irreduzibel, wenn $X \neq 0$ gilt und aus $X \subset \mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b})$ bereits $X \subset \mathbf{V}(\mathfrak{a})$ oder $X \subset \mathbf{V}(\mathfrak{b})$ folgt.

Beispiel 8.3.26. Das Koordinatenkreuz $\mathbf{V}(XY) \subset \mathbb{C}^2$ ist nicht irreduzibel, denn es ist die Vereinigung $\mathbf{V}(XY) = \mathbf{V}(X) \cup \mathbf{V}(Y)$ von y- und x-Achse, die beide echte Teilmengen des Koordinatenkreuzes sind.

Aufgabe 8.3.27. Für einen topologischer Raum X sind äquivalent:

(a) X ist irreduzibel;
(b) für je zwei nichtleere offene Teilmengen U und V von X ist der Schnitt $U \cap V$ nichtleer;
(c) jede nichtleere offene Teilmenge von X ist dicht.

Aufgabe 8.3.28. Vervollständigen Sie: Ein Hausdorffraum ist genau dann irreduzibel, wenn ...
Bestimmen Sie alle irreduziblen Teilmengen von $\mathbb{R}^n$ mit der Standardtopologie.

Aufgabe 8.3.29. (a) Eine Teilmenge Z eines topologischen Raumes ist genau dann irreduzibel, wenn ihr Abschluss $\overline{Z}$ irreduzibel ist.
(b) Eine stetige Abbildung $f\colon X \to Y$ topologischer Räume bildet irreduzible Teilmengen auf irreduzible Teilmengen ab.

Aufgabe 8.3.30. Sei k ein algebraisch abgeschlossener Körper und $X \subset k^n$ eine beliebige Teilmenge. Dann ist X genau dann irreduzibel, wenn $\mathbf{I}(X)$ ein Primideal ist.

Satz 8.3.31. *Sei k ein algebraisch abgeschlossener Körper. Unter der Bijektion (8.3.3) aus Satz 8.3.21 entsprechen sich:*

(a) irreduzible algebraische Teilmengen und Primideale;
(b) einelementige Teilmengen[32] und maximale Ideale.

[32] Diese sind automatisch algebraisch, siehe Beispiel 8.3.9.

Mit anderen Worten erhalten wir die horizontalen Bijektionen in dem kommutativen Diagramm

$$
\begin{tikzcd}
 & \{\textit{algebraische Teilmengen von } k^n\} \arrow[r, leftrightarrow, "\sim"] & \{\textit{Radikalideale von } k[S_1, \dots, S_n]\} \\
 & \{\textit{irreduzible algebraische Teilmengen von } k^n\} \arrow[r, leftrightarrow, "\sim"] \arrow[u, phantom, "\cup"] & \operatorname{Spec} k[S_1, \dots, S_n] \arrow[u, phantom, "\cup"] \\
k^n \arrow[r, "\sim"] & \{\textit{einelementige Teilmengen von } k^n\} \arrow[r, leftrightarrow, "\sim"] \arrow[u, phantom, "\cup"] & \operatorname{MaxSpec} k[S_1, \dots, S_n]. \arrow[u, phantom, "\cup"]
\end{tikzcd} \tag{8.3.4}
$$

8.3.32. Die Verknüpfung der unteren Horizontale ist offensichtlich die Bijektion (8.2.10).

Beweis. Sei X eine algebraische Teilmenge von k^n und $\mathfrak{a} = \mathbf{I}(X)$ das entsprechende Radikalideal, also $\mathbf{V}(\mathfrak{a}) = X$. Es gilt genau dann $X = \emptyset$, wenn $\mathfrak{a} = k[S_1, \dots, S_n]$.

(a) Sei X irreduzibel. Zu zeigen ist, dass $\mathfrak{a}$ prim ist. Wegen $X \neq \emptyset$ ist $\mathfrak{a}$ ein echtes Ideal. Gelte $fg \in \mathfrak{a}$ für $f, g \in k[S_1, \dots, S_n]$. Es gilt dann

$$\mathbf{V}(f) \cup \mathbf{V}(g) = \mathbf{V}(fg) \supset \mathbf{V}(\mathfrak{a}) = X.$$

Da X irreduzibel ist, folgt $X \subset \mathbf{V}(f)$ oder $X \subset \mathbf{V}(g)$. Gelte ohne Einschränkung $X \subset \mathbf{V}(f)$. Es folgt $\mathfrak{a} = \mathbf{I}(X) \supset \mathbf{I}(\mathbf{V}(f)) \ni f$. Also ist $\mathfrak{a}$ prim.

Sei $\mathfrak{a}$ ein Primideal. Es folgt zunächst $X \neq \emptyset$. Gelte $X \subset \mathbf{V}(\mathfrak{e}) \cup \mathbf{V}(\mathfrak{f})$ für Ideale $\mathfrak{e}, \mathfrak{f} \subset k[S_1, \dots, S_n]$. Wegen $\mathbf{V}(\mathfrak{e}) \cup \mathbf{V}(\mathfrak{f}) = \mathbf{V}(\mathfrak{e} \cdot \mathfrak{f})$ folgt

$$\mathfrak{a} = \mathbf{I}(X) \supset \mathbf{I}(\mathbf{V}(\mathfrak{e} \cdot \mathfrak{f})) \supset \mathfrak{e} \cdot \mathfrak{f}.$$

Falls $\mathfrak{e} \subset \mathfrak{a}$ gilt, folgt $\mathbf{V}(\mathfrak{e}) \supset \mathbf{V}(\mathfrak{a}) = X$, und wir sind fertig. Sonst gibt es ein Element $e \in \mathfrak{e} - \mathfrak{a}$. Sei $f \in \mathfrak{f}$ beliebig. Da $\mathfrak{a}$ prim ist, folgt aus $ef \in \mathfrak{e} \cdot \mathfrak{f} \subset \mathfrak{a}$ bereits $f \in \mathfrak{a}$. Dies zeigt $\mathfrak{f} \subset \mathfrak{a}$ und damit $\mathbf{V}(\mathfrak{f}) \supset \mathbf{V}(\mathfrak{a}) = X$. Also ist X irreduzibel.

(b) Gilt $X = \{x\}$ für ein $x \in k^n$, so ist $\mathfrak{a} = \mathbf{I}(X) = \ker(\mathrm{ev}_x)$ offensichtlich ein maximales Ideal.

Sei $\mathfrak{a}$ maximal. Nach Korollar 8.2.16 gibt es genau ein $x \in k^n$ mit $\mathfrak{a} = \ker(\mathrm{ev}_y) = \mathbf{I}(\{x\})$. Da $\{x\}$ eine algebraische Teilmenge von k^n ist, folgt $X = \mathbf{V}(\mathfrak{a}) = \{x\}$. □

Korollar 8.3.33. *Seien k ein algebraisch abgeschlossener Körper und $\mathfrak{a} \subset k[S_1, \dots, S_n]$ ein Ideal. Setze $A := k[S_1, \dots, S_n]/\mathfrak{a}$ und $Z = \mathbf{V}(\mathfrak{a})$ (ist $\mathfrak{a}$ ein Radikalideal, so gilt $\mathbf{I}(Z) = \mathfrak{a}$). Dann induziert das Diagramm* (8.3.4) *aus Satz 8.3.31 das folgende Diagramm mit offensichtlichen horizontalen Bijektionen (die explizit in Bemerkung 8.3.36 beschrieben werden).*

$$
\begin{tikzcd}
 & \{\textit{algebraische Teilmengen von } Z\} \arrow[r, leftrightarrow, "\sim"] & \{\textit{Radikalideale von } A\} \\
 & \{\textit{irreduzible algebraische Teilmengen von } Z\} \arrow[r, leftrightarrow, "\sim"] \arrow[u, phantom, "\cup"] & \operatorname{Spec} A \arrow[u, phantom, "\cup"] \\
Z \arrow[r, "\sim"] & \{\textit{einelementige Teilmengen von } Z\} \arrow[r, leftrightarrow, "\sim"] \arrow[u, phantom, "\cup"] & \operatorname{MaxSpec} A. \arrow[u, phantom, "\cup"]
\end{tikzcd} \tag{8.3.5}
$$

8.3.34. Diese Aussage gibt eine gute Anschauung für das Primspektrum von A, oder allgemeiner für das Primspektrum von endlich erzeugten Algebren über einem algebraisch abgeschlossenen Körper.

Beweis. Für eine algebraische Teilmenge $X \subset k^n$ gilt genau dann $X \subset Z$, wenn $\mathbf{I}(X) \supset \mathfrak{a}$ gilt (verwende $\mathbf{I}(Z) = \mathbf{I}(\mathbf{V}(\mathfrak{a})) \supset \mathfrak{a}$). Außerdem beachte man, dass die kanonischen Bijektion (siehe Proposition 2.3.12)

$$\{\text{Ideale von } A\} \to \{\text{Ideale von } k[S_1, \dots, S_n], \text{ die } \mathfrak{a} \text{ enthalten}\}$$

Bijektionen auf den Teilmengen der Radikal-, Prim- und maximalen Ideale induziert. □

8.3.35. Sei k ein Ring, $\mathfrak{a} \subset k[S_1, \dots, S_n]$ ein Ideal mit Quotientenring $A := k[S_1, \dots, S_n]/\mathfrak{a}$, und $Z = \mathbf{V}(\mathfrak{a})$. Dann kann man jedem Element a von A eine k-wertige Funktion $a = \tilde{a} \colon Z \to k$ zuordnen: Der gestrichelte Pfeil in dem folgenden kommutativen Diagramm von k-Algebren existiert, denn $\mathfrak{a}$ liegt im Kern der Komposition von links oben (über rechts oben) nach rechts unten.

$$\begin{tikzcd} k[S_1,\dots,S_n] \arrow[r] \arrow[d, two heads] & \mathrm{Abb}(k^n,k) \arrow[d, two heads, "\text{Restriktion auf } Z"] \\ A \arrow[r, dotted] & \mathrm{Abb}(Z,k) \end{tikzcd}$$

Bemerkung 8.3.36. In der Situation von Korollar 8.3.33 sind die Abbbildungen in der obersten Horizontalen von (8.3.5) wie folgt gegeben.

(a) Ist $X \subset Z$ eine algebraische Teilmenge, so ist das zugehörige Radikalideal

$$\mathbf{I}_A(X) := \{a \in A \mid a(x) = 0 \text{ für alle } x \in X\}.$$

Diese Ideal ist nämlich gerade $\mathbf{I}(X)/\mathfrak{a}$.

(b) Ist $\mathfrak{b} \subset A$ ein Radikalideal, so ist die zugehörige algebraische Teilmenge

$$\mathbf{V}_Z(\mathfrak{b}) := \{z \in Z \mid b(z) = 0 \text{ für alle } b \in \mathfrak{b}\}.$$

Bezeichnet $\tilde{\mathfrak{b}} \supset \mathfrak{a}$ das Urbild von $\mathfrak{b}$ in $k[S_1,\dots,S_n]$, so ist diese Teilmenge nämlich gerade $\mathbf{V}(\tilde{\mathfrak{b}}) \subset \mathbf{V}(\mathfrak{a}) = Z$.

Aufgabe 8.3.37. (Analogon von Korollar 8.3.33 für einen beliebigen Ring. Die Beweise übertragen sich Eins-zu-Eins.)

Seien R ein Ring und $X = \operatorname{Spec} R$. Betrachten Sie die Abbildungen

$$\mathcal{I}\colon \{\text{Teilmengen von } X\} \rightleftarrows \{\text{Teilmengen von } R\} \colon \mathcal{V}$$

wobei $\mathcal{I}(Z) := \bigcap_{\mathfrak{p}\in Z} \mathfrak{p}$ und $\mathcal{V}(E) := \{\mathfrak{p} \in X \mid E \subset \mathfrak{p}\}$. Nach (2.11.2) wissen wir bereits $\mathcal{I}(\mathcal{V}(E)) = \sqrt{\langle E\rangle}$.

(a) Zeigen Sie $\mathcal{V}(\mathcal{I}(Z)) = \overline{Z}$ und folgern Sie die Bijektion

$$\mathcal{I}\colon \{\text{abgeschlossene Teilmengen von } X\} \overset{\sim}{\rightleftarrows} \{\text{Radikalideale von } R\} \colon \mathcal{V}.$$

(b) Unter dieser Bijektion entspricht die Teilmenge der einpunktigen abgeschlossenen Teilmengen von X der Menge $\operatorname{MaxSpec} R$.

(c) Unter dieser Bijektion entsprecht die Teilmenge der irreduziblen abgeschlossenen Teilmengen der Menge $\operatorname{Spec} R$.

Wir erhalten also Bijektionen

$$\begin{tikzcd} \{\text{abgeschlossene Teilmengen von } X\} \arrow[r, leftrightarrow, "\sim"] & \{\text{Radikalideale von } R\} \\ \{\text{irreduzible abgeschlossene Teilmengen von } X\} \arrow[r, leftrightarrow, "\sim"] \arrow[u, phantom, "\cup"] & \operatorname{Spec} R \arrow[u, phantom, "\cup"] \\ \{\text{einelementige abgeschlossene Teilmengen von } X\} \arrow[r, leftrightarrow, "\sim"] \arrow[u, phantom, "\cup"] & \operatorname{MaxSpec} R. \arrow[u, phantom, "\cup"] \\ \{\text{abgeschlossene Punkte von } X\} \arrow[u, "\sim"] & \end{tikzcd} \tag{8.3.6}$$

Dabei heißt ein Punkt p eines topologischen Raumes abgeschlossen, falls $\{p\}$ eine abgeschlossene Teilmenge ist.

Aufgabe 8.3.38. Motivation für diese Aufgabe: Ist k ein algebraisch abgeschlossener Körper und $A = k[S_1,\dots,S_n]/\mathfrak{a}$, so besteht die linke Spalte des Diagramms (8.3.5) modulo der Identifikation $\mathbf{V}(\mathfrak{a}) \xrightarrow{\sim} \operatorname{MaxSpec} A$ (siehe (8.2.11)) aus Teilmengen von MaxSpec, während die linke Spalte des Diagramms (8.3.6) (für $R = A$) aus Teilmengen von $\operatorname{Spec} A$ besteht.

(a) Seien X ein topologischer Raum und $D \subset X$ die Teilmenge seiner abgeschlossenen Punkte, also der Elemente $x \in X$ mit $\overline{\{x\}} = \{x\}$. Wir verlangen, dass jede abgeschlossene Teilmenge $A \subset X$ der Abschluss ihres Schnittes mit D ist, d. h. $\overline{A \cap D} = A$. Mit anderen Worten ist also $A \cap D$ dicht in A. Ein topologischer Raum mit dieser Eigenschaft heißt **Jacobson** (siehe 005T). Insbesondere ist D dicht in X.

Zeigen Sie: Die Abbildungen

$$\begin{aligned} \{\text{Teilmengen von } X\} &\rightleftarrows \{\text{Teilmengen von } D\} \\ T &\mapsto T \cap D, \\ \overline{S} &\leftarrow\!\shortmid S, \end{aligned}$$

liefern eine Bijektion

$$\{\text{abgeschlossene Teilmengen von } X\} \overset{\sim}{\rightleftarrows} \{\text{abgeschlossene Teilmengen von } D\}$$

Weiter gelten für $A \subset X$ abgeschlossen und $B = A \cap D$:

(i) A irreduzibel $\Leftrightarrow$ B irreduzibel;

(ii) A einpunktig $\Leftrightarrow$ B einpunktig.

(b) Sei nun A eine endlich erzeugte Algebra über einem Körper k. (Wir nehmen nicht an, dass k algebraisch abgeschlossen ist.)

Zeigen, sie, dass man die obigen Aussagen auf $\operatorname{MaxSpec} A \subset \operatorname{Spec} A$ anwenden kann.

Hinweis: Korollar 8.2.12.

Wir erhalten also eine Bijektion

$$\{\text{abgeschlossene Teilmengen von } \operatorname{Spec} A\} \overset{\sim}{\rightleftarrows} \{\text{abgeschlossene Teilmengen von } \operatorname{MaxSpec} A\},$$

die Bijektionen auf den Teilmengen der irreduziblen abgeschlossenen Mengen bzw. der einpunktigen abgeschlossenen Teilmengen induziert.

(c) Nehmen Sie nun an, dass k algebraisch abgeschlossen ist, und dass $A = k[S_1, \dots, S_n]/\mathfrak{a}$ gilt. Sei $Z = \mathbf{V}(\mathfrak{a})$.

Gegeben ein Ideal $\mathfrak{b} \subset A$, sinnieren Sie über den Zusammenhang zwischen $\mathbf{V}_Z(\mathfrak{b}) \subset Z \subset k^n$ und $\mathcal{V}(\mathfrak{b}) \subset \operatorname{Spec} A$ (siehe 8.3.36 für die Definition von $\mathbf{V}_Z$).

9. Dimensionstheorie

9.1. Dimension von Ringen und topologischen Räumen.

Konvention 9.1.1. Wir betrachten im folgenden Infima $\inf T$ und Suprema $\sup T$ von Teilmengen $T \subset \mathbb{N}$. Wir bilden diese in der größeren Menge $\{-\infty\} \cup \mathbb{N} \cup \{+\infty\}$ mit der offensichtlichen totalen Ordnung.[33]

Explizit gelten also

$$\sup T = \begin{cases} -\infty & \text{falls } T = \emptyset; \\ \max T & \text{falls } T \text{ nichtleer und endlich;} \\ +\infty & \text{falls } T \text{ unendlich.} \end{cases}$$

und

$$\inf T = \begin{cases} +\infty & \text{falls } T = \emptyset; \\ \min T & \text{falls } T \text{ nichtleer.} \end{cases}$$

Definition 9.1.2. Sei R ein Ring. Eine **Primidealkette** in R ist eine streng aufsteigende endliche Folge

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$$

von Primidealen von R. Die **Länge** einer solchen Folge ist n, also die Anzahl der echten Inklusionen.

Die **Dimension** $\dim R$ eines Ringes R ist das Supremum der Längen aller Primidealketten in R. Es gilt $\dim R \in \mathbb{N} \cup \{\pm\infty\}$ nach unserer Konvention 9.1.1.

[33] Statt mit $-\infty$ könnten wir genauso gut mit -1 arbeiten.

9.1.3. Wir haben den Begriff „Primidealkette“ bereits in den Going-Up- und Going-Down-Sätzen 7.2.9 und 7.3.10 verwendet. Dort haben wir nicht angenommen, dass die Inklusionen strikt sind; wir könnten dies aber tun, ohne die Essenz dieser Sätze zu ändern.

9.1.4. Ist $R \neq 0$, so gilt $\dim R \in \mathbb{N} \cup \{\infty\}$, denn es gibt dann ein maximales Ideal in R (Satz 2.6.13). Ist $R = 0$, so gilt $\dim R = -\infty$.

Beispiele 9.1.5. (a) Ist k ein Körper, so gilt $\dim k = 0$.

(b) Ist R ein Hauptidealring, der kein Körper ist, so gilt $\dim R = 1$. In der Tat, die einzigen Primideale sind das Nullideal und die Ideale der Form (f) mit $f \in R$ irreduzibel, und letztere sind sämtlich maximal (siehe 2.6.4).
  (i) $\dim \mathbb{Z} = 1$
  (ii) $\dim k[X] = 1$, falls k ein Körper ist.

(c) Ist k ein Körper, so werden wir in Bälde (siehe Satz 9.1.23 sehen, dass $\dim k[X_1, \dots, X_n] = n$ gilt. Die Primidealkette

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \cdots X_n)$$

zeigt schon einmal die Relation $\dim k[X_1, \dots, X_n] \geq n$.

(d) Ist k ein Körper, so hat der Polynomring $[X_1, X_2, \dots]$ in abzählbar vielen Variablen Dimension ∞, denn für jedes $n \in \mathbb{N}$ ist $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \cdots X_n)$ eine Primidealkette der Länge n.

9.1.6. Ist $\mathfrak{a} \subset R$ ein Ideal, so gilt $\dim R/\mathfrak{a} \leq \dim R$, denn die Bijektion $\operatorname{Spec} R/\mathfrak{a} \xrightarrow{\sim} \mathcal{V}(\mathfrak{a}) \subset \operatorname{Spec} R$ ist inklusionserhaltend (und erhält als Bijektion echte Inklusionen) (Proposition 2.11.17). Also liefert jede Primidealkette in $R/\mathfrak{a}$ eine Primidealkette in R derselben Länge.

9.1.7. Es gilt $\dim R = \dim R/\mathrm{Nil}(R)$, denn die Bijektion $\operatorname{Spec} R/\mathrm{Nil}(R) \xrightarrow{\sim} \mathcal{V}(\mathrm{Nil}(R)) = \operatorname{Spec} R$ ist inklusionserhaltend (siehe Lemma 7.4.10).

9.1.8. Ist $S \subset R$ eine multiplikativ abgeschlossene Teilmenge, so gilt $\dim S^{-1}R \leq \dim R$, denn die Bijektion $\operatorname{Spec} S^{-1}R \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\}$ ist inklusionserhaltend (Proposition 6.2.3.(c)).

Definition 9.1.9. Sei X ein topologischer Raum. Die (**Krull-**)**Dimension** $\dim X$ von X ist das Supremum der Längen n aller echt aufsteigenden Ketten

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$$

von irreduziblen abgeschlossenen Teilmengen.

9.1.10. Ist R ein Ring, so gilt $\dim \operatorname{Spec} R = \dim R$, denn nach der mittleren (inklusionsumkehrenden) Bijektion im Diagramm (8.3.6) in Aufgabe 8.3.37 entsprechen die Primidealketten in R den echt aufsteigenden Ketten irreduzibler abgeschlossener Teilmengen von $\operatorname{Spec} R$.

9.1.11. Ist $A \cong k[S_1, \dots, S_n]/\mathfrak{a}$ eine endlich erzeugte Algebra über einem algebraisch abgeschlossenen Körper k, so gilt $\dim A = \dim \mathbf{V}(\mathfrak{a})$ nach Korollar 8.3.33.

Beispiel 9.1.12. Der Begriff der Krull-Dimension ist auf topologische Räume der Form $\operatorname{Spec} R$ maßgeschneidert. Für viele wohlbekannte Räume ist er vollkommen langweilig. Alle Hausdorffräume haben beispielsweise Krulldimension 0 (vergleiche Aufgabe 8.3.28), es gilt also etwa $\dim \mathbb{R}^n = 0$ für $\mathbb{R}^n$ mit der Standardtopologie.

Definition 9.1.13. Sei X ein topologischer Raum und $Y \subset X$ eine irreduzible abgeschlossene Teilmenge. Die **Kodimension** $\operatorname{codim}_X Y$ von Y in X ist definiert als das Supremum der Längen n aller echt aufsteigenden Ketten

$$Y = X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$$

von irreduziblen abgeschlossenen Teilmengen, die bei Y starten.

9.1.14. Es gilt

$$\dim X \geq \dim Y + \operatorname{codim}_X Y,$$

denn die rechte Seite ist das Supremum der Längen aller echt aufsteigenden Ketten irreduzibler abgeschlossener Teilmengen von X, die durch Y gehen.

Definition 9.1.15. Sei R ein Ring und $\mathfrak{p} \subset R$ ein Primideal. Die **Höhe** $\mathrm{ht}(\mathfrak{p})$ von $\mathfrak{p}$ ist das Supremum der Längen aller Primidealketten

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

in R, die bei $\mathfrak{p}$ enden. (Das Symbol ht steht für englisch *height*). Es gilt $\mathrm{ht}(\mathfrak{p}) \in \mathbb{N} \cup \{+\infty\}$.

9.1.16. Die bei $\mathfrak{p}$ endenden Primidealketten in R entsprechen nach Proposition 6.2.5 genau den Primidealketten im lokalen Ring $R_{\mathfrak{p}}$. Es gilt also $\mathrm{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.

9.1.17. Es gilt $\mathrm{ht}(\mathfrak{p}) = \mathrm{codim}_{\mathrm{Spec}\, R} \mathcal{V}(\mathfrak{p})$.

9.1.18. Ist $A \cong k[S_1, \ldots, S_n]/\mathfrak{a}$ eine endlich erzeugte Algebra über einem algebraisch abgeschlossenen Körper k und ist $\mathfrak{p} \subset A$ ein Primideal, so gilt $\mathrm{ht}(\mathfrak{p}) = \mathrm{codim}_{\mathbf{V}(\mathfrak{a})} \mathbf{V}(\mathfrak{p})$.

9.1.19. Es gilt

$$\dim R \geq \mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p},$$

denn man kann jede in $\mathfrak{p}$ endende Primidealkette der Länge m mit dem Urbild jeder Primidealkette in $R/\mathfrak{p}$ der Länge n zu einer Primidealkette in R der Länge mindestens $m + n$ kombinieren (die Länge ist genau dann $m + n$, wenn die Kette in $R/\mathfrak{p}$ beim Nullideal startet).

Da umgekehrt jede Primidealkette in R, die durch $\mathfrak{p}$ geht, auf diese Weise entsteht, ist $\mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p}$ das Supremum der Längen aller Primidealketten in R, die durch $\mathfrak{p}$ gehen.

Satz 9.1.20. *Sei $A \subset B$ eine ganze Ringerweiterung. Dann gilt*

$$\dim A = \dim B.$$

Für $\mathfrak{q} \in \mathrm{Spec}\, B$ mit $\mathfrak{p} = \mathfrak{q} \cap A$ gilt

$$\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{q})$$

Sind A und B Integritätsbereiche und ist A normal, so gilt Gleichheit.

9.1.21. Es gilt $\dim A/\mathfrak{p} = \dim B/\mathfrak{q}$, denn $A/\mathfrak{p} \subset B/\mathfrak{q}$ ist ganz.

Beweis. Sei $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ eine Primidealkette in B. Dann ist

$$\mathfrak{q}_0 \cap A \subsetneq \mathfrak{q}_1 \cap A \subsetneq \cdots \subsetneq \mathfrak{q}_n \cap A$$

eine Primidealkette in A; beachte, dass die Inklusionen echt bleiben, da es keine echten Inklusionen in den Fasern von $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ gibt (Korollar 7.2.5): Aus $\mathfrak{q}_i \cap A = \mathfrak{q}_{i+1} \cap A$ würde $\mathfrak{q}_i = \mathfrak{q}_{i+1}$ folgen. Dies zeigt $\dim A \geq \dim B$. Betrachtet man nur Primidealketten in B mit $\mathfrak{q}_n = \mathfrak{q}$, so liefert dasselbe Argument $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{q})$.

Sei $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ eine Primidealkette in A. Der Going-Up-Satz 7.2.9 (ausgehend von der leeren Kette in B) liefert eine Primidealkette in B, deren Schnitt mit A die gegebene Primidealkette ist. Dies zeigt $\dim B \geq \dim A$.

Sei A normal. Dann können wir jede Primidealkette in A mit $\mathfrak{p}_n = \mathfrak{p}$ per Going-Down (Satz 7.3.10) zu einer Primidealkette in B liften, die bei $\mathfrak{q}$ endet. Dies zeigt $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p})$. ☐

Beispiel 9.1.22. Ist k ein Körper und $A \neq 0$ eine endlichdimensionale k-Algebra (hier ist die Dimension als k-Vektorraum gemeint, nicht die Dimension als Ring), so gilt $\dim A = 0$, denn $k \subset A$ ist eine ganze Ringerweiterung (siehe 7.5.3).

Satz 9.1.23. *Ist k ein Körper, so gilt*

$$\dim k[T_1, \ldots, T_n] = n.$$

Beweis. Wir haben in Beispiel 9.1.5.(c) bereits $\dim k[T_1, \ldots, T_n] \geq n$ beobachtet. Wir zeigen die Aussage $\dim k[T_1, \ldots, T_n] \leq n$ per Induktion über n. Für $n = 0$ ist die Aussage trivial, da k ein Körper ist.

Sei $n > 0$ und setze $A := k[T_1, \ldots, T_n]$. Sei

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

eine Primidealkette in A. Zu zeigen ist $m \leq n$. Im Fall $m = 0$ ist dies trivial, so dass wir also $m \geq 1$ annehmen können. Starke Noether-Normalisierung 8.1.26, angewandt auf $\mathfrak{p}_1 \subsetneq A$, liefert einen Polynomring

$P = k[y_1, \dots, y_n] \subset A$, ebenfalls in n Variablen[34] nach 8.1.28, so dass A endlich über P ist, und ein $\delta \leq n$ mit $\mathfrak{p}_1 \cap P = (y_{\delta+1}, \dots, y_n)$. Weil $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ eine echte Inklusion ist und $P \subset A$ als endliche Erweiterung ganz ist (siehe 7.5.3), ist auch $\mathfrak{p}_0 \cap P \subsetneq \mathfrak{p}_1 \cap P$ eine echte Inklusion (Korollar 7.2.5). Also ist $\mathfrak{p}_1 \cap P = (y_{\delta+1}, \dots, y_n)$ nicht das Nullideal, d. h. es gilt $\delta < n$. Die Inklusion

$$k[y_1, \dots, y_\delta] = P/(\mathfrak{p}_1 \cap P) \hookrightarrow A/\mathfrak{p}_1$$

ist endlich und somit ganz. Die Induktionsannahme und Satz 9.1.20 zeigen

$$\delta = \dim k[y_1, \dots, y_\delta] = \dim A/\mathfrak{p}_1.$$

Die Länge der Primidealkette

$$\mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1$$

in $A/\mathfrak{p}_1$ ist somit $\leq \delta$, d. h. es gilt $m - 1 \leq \delta < n$, also $m \leq n$. □

Beispiel 9.1.24. Wir bestimmen $\operatorname{Spec} \mathbb{C}[X, Y]$.

Die offensichtlichen Primideale sind das Nullideal und die maximalen Ideale. Nach Korollar 8.2.16 sind die maximalen Ideale genau die Ideale $(X - a, Y - b)$, für $(a, b) \in \mathbb{C}^2$, und diese sind paarweise verschieden.

Sei $(0) \subsetneq \mathfrak{p} \subset \mathbb{C}[X, Y]$ ein nicht maximales Primideal. Sei $0 \neq g \in \mathfrak{p}$. Ein irreduzibler Faktor von g muss auch in $\mathfrak{p}$ liegen. Sei also $f \in \mathfrak{p}$ irreduzibel. Dann ist (f) ein Primideal mit $(f) \subset \mathfrak{p}$. Wegen $\dim \mathbb{C}[X, Y] = 2$ (und $(0) \subsetneq (f) \subset \mathfrak{p} \subsetneq \mathfrak{m}$ für ein geeignetes maximales Ideal $\mathfrak{m}$) folgt $(f) = \mathfrak{p}$.[35]

Da andererseits jedes irreduzible Element ein Primideal erzeugt, erhalten wir

$$\operatorname{Spec} \mathbb{C}[X, Y] = \{(0)\} \cup \{(f) \mid f \in \mathbb{C}[X, Y] \text{ irreduzibel}\} \cup \{(X - a, Y - b) \mid (a, b) \in \mathbb{C}^2\}.$$

Sind f und g irreduzibel, so gilt genau dann $(f) = (g)$, wenn f und g assoziiert sind, also $f\mathbb{C}^\times = g\mathbb{C}^\times$ gilt (es ist $\mathbb{C}[X, Y]^\times = \mathbb{C}^\times$). Das Nullideal (0) hat Höhe Null, die Primideale der Form (f) haben Höhe Eins, und die maximalen Ideale haben Höhe Zwei.

Aufgabe 9.1.25. Bestimmen Sie in ähnlicher Weise $\operatorname{Spec} \mathbb{R}[X, Y]$.

Korollar 9.1.26. *Sei $A \neq 0$ eine endlich erzeugte Algebra über einem Körper k. Dann gilt $\dim A \in \mathbb{N}$, die Dimension von A ist also endlich. Ist A als k-Algebra von n Elementen erzeugt, so gilt $\dim A \leq n$. Ist A endlich (oder, äquivalent, ganz) über einem Polynomring $k[y_1, \dots, y_d] \subset A$, so gilt $d = \dim A$.*

Beweis. Da A ein Quotient von einem geeigneten Polynomring $k[T_1, \dots, T_n]$ ist, gilt $\dim A \leq \dim k[T_1, \dots, T_n] = n$ (nach 9.1.7 und Satz 9.1.23). Wegen $A \neq 0$ gilt $\dim A \geq 0$.

Die letzte Aussage folgt aus den Sätzen 9.1.20 und 9.1.23. (Da A bereits als k-Algebra endlich erzeugt ist, ist A genau dann endlich über einem Polynomring $P \subset A$, wenn A ganz über P ist (Korollar 7.1.22).) □

Korollar 9.1.27. *Sei A eine endlich erzeugte Algebra über einem Körper k, die ein Integritätsbereich ist. Dann gilt*

$$\dim A = \operatorname{trdeg}_k \operatorname{Quot}(A).$$

9.1.28. Diese Aussage impliziert sofort die schwache Version des Hilbertschen Nullstellensatzes 8.2.1: Ist $k \subset L$ eine Körpererweiterung, so gilt $\dim L = 0$. Ist L endlich erzeugt als k-Algebra, so liefert Korollar 9.1.27 $0 = \dim L = \operatorname{trdeg}_k L$. Also ist die Körpererweiterung L/k algebraisch. Endlich viele Erzeuger von L als k-Algebra erzeugen auch die Körpererweiterung L/k, die somit endlich ist.

Beweis. Schwache Noether-Normalisierung 8.1.24 liefert einen Polynomring $P = k[y_1, \dots, y_d] \subset A$, so dass A endlich (und somit ganz) über P ist. Es folgt

$$\dim A = \dim k[y_1, \dots, y_d] = d$$

nach Satz 9.1.20 und Satz 9.1.23.

Die Erweiterung der Quotientenkörper $\operatorname{Quot}(P) \subset \operatorname{Quot}(A)$ ist endlich (und somit algebraisch): Gilt $A = Pa_1 + \dots Pa_n$ für Elemente $a_1, \dots, a_n \in A$, so sind alle $a_i = \frac{a_i}{1} \in \operatorname{Quot}(A)$ ganz über P und damit algebraisch über $\operatorname{Quot}(P)$. Es ist leicht zu sehen, dass $\operatorname{Quot}(A)$ der kleinste Zwischenkörper von $\operatorname{Quot}(P) \subset \operatorname{Quot}(A)$ ist, der all diese Elemente enthält.

[34] Für den Rest des Beweises genügt es zu wissen, dass P ein Polynomring in $\leq n$ Variablen ist.

[35] Dieses Argument zeigt, dass in einem beliebigen faktoriellen Ring die minimalen Primideale über dem Nullideal gerade die von den irreduziblen Elementen erzeugten Ideale sind.

Der Körperturm $k \subset \operatorname{Quot}(P) \subset \operatorname{Quot}(A)$ liefert

$$\operatorname{trdeg}_k \operatorname{Quot}(A) = \operatorname{trdeg}_k \operatorname{Quot}(P) + \underbrace{\operatorname{trdeg}_{\operatorname{Quot}(P)} \operatorname{Quot}(A)}_{=0} = \operatorname{trdeg}_k \operatorname{Quot}(P) = d.$$

Hier verwenden wir wohlbekannte Aussagen für den Transzendenzgrad (siehe etwa 030D): Der Transzendenzgrad ist additiv für Körpertürme; algebraische Körpererweiterungen haben den Transzendenzgrad Null; der Transzendenzgrad von $\operatorname{Quot}(P) = \operatorname{Quot}(k[y_1, \dots, y_d]) = k(y_1, \dots, y_d)$ über k ist d. □

bis hier, Mittwoch, 1. Februar 2017

Korollar 9.1.29. *Sei k ein algebraisch abgeschlossener Körper. Ist $Z \subset k^n$ eine abgeschlossene Teilmenge, so gilt $\dim Z \leq n$ mit Gleichheit genau dann, wenn $Z = k^n$.*

Beweis. Es gilt $\dim k^n = \dim k[T_1, \dots, T_n] = n$ nach 9.1.11 und Satz 9.1.23.

Jede echt aufsteigende Kette $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$ von irreduziblen abgeschlossenen Teilmengen von Z ist auch eine solche Kette in k^n. Es folgt $\dim Z \leq \dim k^n = n$. Insbesondere ist $\dim Z$ endlich. Es gibt also eine maximale solche Kette in Z. Ist $Z \subsetneq k^n$ eine echte Teilmenge, so kann man diese Kette um k^n zu einer um Eins längeren Kette erweitern, erhält also $\dim Z < \dim k^n = n$. Gilt $Z = k^n$, so gilt natürlich $\dim Z = n$. □

9.1.30. Ist k ein algebraisch abgeschlossener Körper und ist $Z \subset k^n$ eine beliebige Teilmenge, so gilt $\dim Z \leq n$, denn jede echt aufsteigende Kette abgeschlossener irreduzibler Teilmengen von Z liefert per Abschluss-Nehmen eine ebensolche Kette in $\overline{Z}$, so dass also $\dim Z \leq \dim \overline{Z}$ gilt und damit $\dim Z \leq n$ nach Korollar 9.1.29.

Im Allgemeinen ist die Abschätzung $\dim Z \leq \dim \overline{Z}$ aber keine Gleichheit.

Betrachte $Z = \{(t, \exp(t^2)) \mid t \in \mathbb{R}\} \subset \mathbb{C}^2$.

Behauptung: Sei $f \in \mathbb{C}[X, Y]$ ein Polynom, das an unendlich vielen Punkten von Z verschwindet. Dann ist f das Nullpolynom. Es gilt also $\mathbf{I}(Z) = (0)$.

Glauben wir diese Behauptung für einen Moment. Sie impliziert sofort, dass die abgeschlossenen Teilmengen von Z ganz Z und die endlichen Teilmengen sind. Die irreduziblen abgeschlossenen Teilmengen sind somit ganz Z und die einpunktigen Teilmengen. Es folgt $\dim Z = 1$. Weiter gilt $\overline{Z} = \mathbf{V}(\mathbf{I}(Z)) = \mathbf{V}(0) = \mathbb{C}^2$, so dass also $\dim \overline{Z} = 2$ gilt.

Beweis der Behauptung: Sei $f = f(X, Y) \in \mathbb{C}[X, Y]$ wie in der Behauptung gegeben. Indem wir $f = f_1 + i f_2$ für eindeutige $f_1, f_2 \in \mathbb{R}[X, Y]$ schreiben, sehen wir, dass auch f_1 und f_2 an unendlich vielen Punkten von Z verschwinden. Wir können also ohne Einschränkung annehmen, dass $f \in \mathbb{R}[X, Y]$ gilt.

Es gibt also unendlich viele $t \in \mathbb{R}$ mit $f(t, \exp(t^2)) = 0$; hier verwenden wir, dass $\mathbb{R} \to Z$, $t \mapsto (t, \exp(t^2))$, bijektiv ist.

Gilt $f \in \mathbb{R}[X] \subset \mathbb{R}[X, Y]$, so ist f ein reelles Polynom in einer Variablen mit unendlich vielen Nullstellen, also das Nullpolynom. In diesem Fall verschwindet f auf ganz Z.

Gelte nun $f \in \mathbb{R}[X, Y] - \mathbb{R}[X]$. Schreibe $f = g(Y)X^m +$(Terme von kleinerem Grad in X) mit $0 \neq gv\mathbb{R}[Y]$ und $m > 0$. Für t groß genug bestimmt der Term $g(Y)X^m$ das Verhalten von $t \mapsto f(t, \exp(t^2))$. Es folgt (per elementarer Abschätzung), dass es ein $T > 0$ gibt, so dass $f(t, \exp(t^2)) \neq 0$ für alle $|t| \geq T$ gibt. Dies bedeutet, dass die Funktion $t \mapsto f(t, \exp(t^2))$ in $[-T, T]$ unendlich viele Nullstellen hat. Also hat auch die holomorphe Funktion $g \colon \mathbb{C} \to \mathbb{C}$, $z \mapsto f(z, \exp(z^2))$, unendlich viele Nullstellen in $[-T, T] \subset \mathbb{R} \subset \mathbb{C}$. Da $[-T, T]$ kompakt ist, hat diese Menge einen Häufungspunkt in $[-T, T]$. Nach dem Identitätssatz für holomorphe Funktionen ist g die Nullfunktion $\mathbb{C} \to \mathbb{C}$. Dies bedeutet insbesondere, dass f auf ganz Z verschwindet. Dies steht im Widerspruch zu $f(t, \exp(t^2)) \neq 0$ für alle $t \in \mathbb{R}$ mit $|t| \geq T$. Also tritt der Fall $f \in \mathbb{R}[X, Y] - \mathbb{R}[X]$ nicht auf. [36] [37]

9.1.31. Mit einer maximalen Primidealkette meinen wir eine Primidealkette, die sich nicht durch Hinzufügen eines Primideals an einem der Enden oder im Inneren verlängern läßt.

[36] Das Argument für $\{(t, \exp(t)) \mid t \in \mathbb{R}\}$ sollte analog gehen, nur muss man bei der Abschätzung die Fälle $t \to \infty$ und $t \to -\infty$ getrennt betrachten.

[37] Für die Menge $Z' := \{(t, \exp(t)) \mid t \in \mathbb{C}\}$ gilt die Behauptung aber nicht. Es gilt nämlich $\{(i\alpha, \sin(\alpha) + i\cos(\alpha)) \mid \alpha \in \mathbb{R}\} \subset Z'$. Indem man nur $\alpha \in 2\pi\mathbb{Z}$ betrachtet, erhält man $(2\pi i\mathbb{Z}) \times \{1\} \subset Z'$. Das Polynom $f(X, Y) = Y - 1 \neq 0$ verschwindet also an unendlich vielen Punkten von Z'. Der Schnitt der Nullstellenmenge von f mit Z' ist eine (unendliche) abgeschlossene irreduzible (echte) Teilmenge von Z' (da ihr Abschluss offensichtlich irreduzibel ist). Es folgt $\dim Z' = 2$.

Satz 9.1.32. *Sei A eine endlich erzeugte Algebra über einem Körper k, die ein Integritätsbereich ist. Dann haben alle maximalen Primidealketten in A dieselbe endliche Länge* $\dim A$.

Beweis. Wir zeigen zuerst die folgende **Hilfsaussage**. Sei $P = k[y_1, \dots, y_d]$ ein Polynomring in A, so dass A endlich (und damit ganz) über P ist, und sei

$$(0) = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$$

eine maximale Primidealkette in A (die notwendig beim Nullideal startet). Dann ist auch

$$(0) = \mathfrak{q}_0 \cap P \subsetneq \mathfrak{q}_1 \cap P \subsetneq \cdots \subsetneq \mathfrak{q}_n \cap P$$

eine maximale Primidealkette in P.

Beachte zunächst, dass die Inklusionen echt sind, da es keine echten Inklusionen in den Fasern von $\operatorname{Spec} A \to \operatorname{Spec} P$ gibt (Korollar 7.2.5). Angenommen, die Kette $(\mathfrak{q}_i \cap P)$ ist nicht maximal. Könnte man ein Primideal echt oberhalb von $\mathfrak{q}_n \cap P$ ergänzen, so käme dieses per Going-Up 7.2.9 von einem Primideal in A echt oberhalb von $\mathfrak{q}_n$, was aber auf Grund der Maximalität nicht möglich ist.

Nehmen wir nun an, dass man zwischen $\mathfrak{q}_i \cap P$ und $\mathfrak{q}_{i+1} \cap P$ ein weiteres Primideal einschieben kann, dass es also ein Primideal $\mathfrak{p} \subset P$ mit $\mathfrak{q}_i \cap P \subsetneq \mathfrak{p} \subsetneq \mathfrak{q}_{i+1} \cap P$ gibt. Starke Noether-Normalisierung 8.1.26, angewandt auf $\mathfrak{q}_i \cap P \subsetneq P$, liefert einen Polynomring $Q = k[t_1, \dots, t_d] \subset P$ (ebenfalls in d Variablen), so dass P endlich über Q ist, und ein $\delta \le d$ mit $\mathfrak{q}_i \cap Q = \mathfrak{q}_i \cap P \cap Q = (t_{\delta+1}, \dots, t_d)$. Wir erhalten endliche und damit ganze Ringerweiterungen

$$k[t_1, \dots, t_\delta] = Q/(y_{\delta+1}, \dots, y_d) = Q/(\mathfrak{q}_i \cap Q) \hookrightarrow P/(\mathfrak{q}_i \cap P) \hookrightarrow A/\mathfrak{q}_i. \tag{9.1.1}$$

Mit demselben Argument wie oben (keine echten Inklusionen in Fasern von $\operatorname{Spec} P \to \operatorname{Spec} Q$) sind die Inklusionen $\mathfrak{q}_i \cap Q \subsetneq \mathfrak{p} \cap Q \subsetneq \mathfrak{q}_{i+1} \cap Q$ echt. Also erhalten wir eine Primidealkette

$$(0) = \frac{\mathfrak{q}_i \cap Q}{\mathfrak{q}_i \cap Q} \subsetneq \frac{\mathfrak{p} \cap Q}{\mathfrak{q}_i \cap Q} \subsetneq \frac{\mathfrak{q}_{i+1} \cap Q}{\mathfrak{q}_i \cap Q}$$

im Polynomring $k[t_1, \dots, t_\delta] = Q/(\mathfrak{q}_i \cap Q)$. Dieser ist normal, so dass Going-down 7.2.9 entlang der ganzen Ringerweiterung (9.1.1) ein Primideal $\hat{\mathfrak{p}} \subsetneq \mathfrak{q}_{i+1}/\mathfrak{q}_i$ in $A/\mathfrak{q}_i$ liefert, das über $\frac{\mathfrak{p} \cap Q}{\mathfrak{q}_i \cap Q}$ liegt. Insbesondere gilt $(0) = \mathfrak{q}_i/\mathfrak{q}_i \subsetneq \hat{\mathfrak{p}} \subsetneq \mathfrak{q}_{i+1}/\mathfrak{q}_i$. Das Urbild von $\hat{\mathfrak{p}}$ in A ist ein Primideal, das echt zwischen $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$ liegt. Dieser Widerspruch zur Maximalität beweist die Hilfsaussage.

Reduktion auf den Fall eines Polynomrings. Schwache Noether-Normalisierung 8.1.24 liefert einen Polynomring $P = k[y_1, \dots, y_d] \subset A$, so dass A endlich (und damit ganz) über P ist. Dann gilt $\dim P = \dim A$ nach Satz 9.1.20. Um zu zeigen, dass jede maximale Primidealkette in A die Länge $\dim A$ hat, genügt es nach der Hilfsaussage zu zeigen, dass jede maximale Primidealkette in P die Länge $\dim P$ hat.

Der Fall eines Polynomrings. Wir zeigen nun die Aussage für Polynomringe. Sei also $A = k[T_1, \dots, T_d]$. Wir führen Induktion über d. Für $d = 0$ ist die Aussage trivial (ebenso ist sie für $d = 1$ recht offensichtlich). Gelte $d > 0$. Sei

$$(0) = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

eine maximale Primidealkette in $k[T_1, \dots, T_d]$. Wegen $\dim k[T_1, \dots, T_d] = d$ (siehe Satz 9.1.23) ist $n = d$ zu zeigen.

Starke Noether-Normalisierung 8.1.26, angewandt auf $\mathfrak{p}_1 \subsetneq A$, liefert einen Polynomring $P = k[y_1, \dots, y_d] \subset A$ (ebenfalls in d Variablen), so dass A endlich über P ist, und ein $\delta \le d$ mit $\mathfrak{p}_1 \cap P = (y_{\delta+1}, \dots, y_d)$. Da P als Polynomring über einem Körper normal ist (Proposition 7.1.13) und A ein Integritätsbereich ist, zeigt der letzte Teil von Satz 9.1.20 die erste Gleichheit in

$$\operatorname{ht}((y_{\delta+1}, \dots, y_d)) = \operatorname{ht}(\mathfrak{p}_1) = 1,$$

die zweite Gleichheit folgt aus der Maximalität der Primidealkette. Wir erhalten $\delta + 1 = d$, d. h. $\mathfrak{p}_1 \cap P = (y_d)$.

Nach der Hilfsaussage ist auch die Primidealkette

$$\mathfrak{p}_0 \cap P \subsetneq \mathfrak{p}_1 \cap P \subsetneq \cdots \subsetneq \mathfrak{p}_n \cap P$$

in dem Polynomring P maximal. Wir erhalten die maximale Primidealkette

$$(0) = \frac{\mathfrak{p}_1 \cap P}{\mathfrak{p}_1 \cap P} \subsetneq \cdots \subsetneq \frac{\mathfrak{p}_n \cap P}{\mathfrak{p}_1 \cap P}$$

der Länge $n-1$ in in $\frac{P}{\mathfrak{p}_1\cap P} = \frac{P}{(y_d)} = k[y_1,\dots,y_{d-1}]$. Die Induktionssannahme liefert $n-1=d-1$, also $n=d$. □

Korollar 9.1.33. *Sei A eine endlich erzeugte Algebra über einem Körper k, die ein Integritätsbereich ist. Ist*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$$

eine maximale Primidealkette in A, so gilt $\dim A = n$, und für jedes $i=0,\dots,n$ gilt $\operatorname{ht}(\mathfrak{p}_i)=i$ und $\dim A/\mathfrak{p}_i = n-i$.

Sei $\mathfrak{p}\in\operatorname{Spec} A$ ein Primideal. Dann sind $\dim A$, $\operatorname{ht}(\mathfrak{p})$ und $\dim A/\mathfrak{p}$ endlich und es gelten

(a) $\dim A = \dim A/\mathfrak{p} + \operatorname{ht}(\mathfrak{p})$;
(b) alle Primidealketten, die bei $\mathfrak{p}$ enden und maximal sind mit dieser Eigenschaft, haben dieselbe Länge $\operatorname{ht}(\mathfrak{p})$;
(c) alle Primidealketten, die bei $\mathfrak{p}$ starten und maximal sind mit dieser Eigenschaft, haben dieselbe Länge $\dim A/\mathfrak{p}$.

Beweis. Die Gleichheit $\dim A = n$ ist Satz 9.1.32. Es ist klar, dass $\operatorname{ht}(\mathfrak{p}_i)\geq i$ gilt. Es kann aber keine Primidealkette der Länge $> i$, geben, die bei $\mathfrak{p}$ endet, denn eine solche ließe sich mit $\mathfrak{p}_i \subsetneq \dots \subsetneq \mathfrak{p}_n$ zu einer Primidealkette der Länge $> n$ kombinieren, im Widerspruch zu Satz 9.1.32. Offensichtlich ist die Kette $(0)=\mathfrak{p}_i/\mathfrak{p}_i \subsetneq \dots \subsetneq \mathfrak{p}_n/\mathfrak{p}_i$ eine maximale Primidealkette in $A/\mathfrak{p}_i$. Satz 9.1.32, angewendet auf $A/\mathfrak{p}_i$, liefert $n-i=\dim A/\mathfrak{p}_i$.

Sei nun $\mathfrak{p}\in\operatorname{Spec} A$ ein Primideal. Dann sind A und $A/\mathfrak{p}$ nicht der Nullring und damit folgt $\dim A, \dim A/\mathfrak{p}\in\mathbb{N}$ nach Korollar 9.1.26. Wegen $0\leq\operatorname{ht}(\mathfrak{p})\leq\dim A$ ist auch $\operatorname{ht}(\mathfrak{p})$ endlich.

Die Gleichheit $\dim A = \dim A/\mathfrak{p} + \operatorname{ht}(\mathfrak{p})$ ist nun offensichtlich, denn $\mathfrak{p}$ liegt in einer maximalen Primidealkette.

Jede maximale bei $\mathfrak{p}$ endende Primidealkette kann man mit einer fest gewählten maximalen bei $\mathfrak{p}$ startenden Primidealkette zu einer maximalen Primidealkette kombinieren, die dann nach Satz 9.1.32 die Länge $\dim A$ hat. Also haben alle maximalen bei $\mathfrak{p}$ endenden Primidealketten dieselbe Länge. Diese Länge ist offensichtlich gerade $\operatorname{ht}(\mathfrak{p})$.

Bei $\mathfrak{p}$ beginnende Primidealketten in A entsprechen bijektiv den Primidealketten in $A/\mathfrak{p}$. Da $A/\mathfrak{p}$ ein Integritätsbereich ist und endlich erzeugt als k-Algebra, haben die maximalen unter diesen Ketten alle dieselbe Länge $\dim A/\mathfrak{p}$ nach Satz 9.1.32. □

Definition 9.1.34. Ein Ring R heißt **Kettenring** ("catenary ring"), falls für jedes Paar $\mathfrak{p}\subset\mathfrak{q}$ von Primidealen in R alle maximalen Primidealketten, die bei $\mathfrak{p}$ beginnen und bei $\mathfrak{q}$ enden, dieselbe Länge haben.

Korollar 9.1.35. *Endlich erzeugte Algebren über Körpern sind Kettenringe.*

Beweis. Sei A eine solche Algebra und seien $\mathfrak{p}\subset\mathfrak{q}$ Primideale in A. Die maximalen Primidealketten von $\mathfrak{p}$ nach $\mathfrak{q}$ in A entsprechen bijektiv den maximalen Primidealketten von $(0)=\mathfrak{p}/\mathfrak{p}$ nach $\mathfrak{q}/\mathfrak{p}$ in $A/\mathfrak{p}$. Da $\mathfrak{q}/\mathfrak{p}$ ein Primideal im Integritätsbereich $A/\mathfrak{p}$ ist und dieser als k-Algebra endlich erzeugt ist, haben die letzteren Ketten nach Korollar 9.1.33 alle dieselbe endliche Länge $\operatorname{ht}_{A/\mathfrak{p}}(\mathfrak{q}/\mathfrak{p})$. □

9.1.36. In der Situation des Beweises von Korollar 9.1.35 kann man die Zahl $\operatorname{ht}_{A/\mathfrak{p}}(\mathfrak{q}/\mathfrak{p})$ mit Korollar 9.1.33 genauer berechnen. Es gilt

$$\operatorname{ht}_{A/\mathfrak{p}}(\mathfrak{q}/\mathfrak{p}) = \dim A/\mathfrak{p} - \dim (A/\mathfrak{p})/(\mathfrak{q}/\mathfrak{p}) = \dim A/\mathfrak{p} - \dim A/\mathfrak{q}.$$

Alle maximalen Primidealketten von $\mathfrak{p}$ nach $\mathfrak{q}$ haben also dieselbe Länge $\dim A/\mathfrak{p} - \dim A/\mathfrak{q}$.

9.2. **Zerlegung in irreduzible Komponenten und minimale Primideale.**

Definition 9.2.1. Sei X ein topologischer Raum. Eine **irreduzible Komponente** von X ist eine maximale irreduzible Teilmenge von X, also ein maximales Element der bezüglich Inklusion partiell geordenten Menge aller irreduziblen Teilmengen von X.

Lemma 9.2.2. *Sei X ein topologischer Raum. Jede irreduzible Komponente von X ist abgeschlossen und somit eine maximale irreduzible abgeschlossene Teilmenge von X. Umgekehrt ist jede maximale irreduzible abgeschlossene Teilmenge von X bereits eine irreduzible Komponente.*

Beweis. Wir erinnern daran, dass eine Teilmenge $Z \subset X$ genau dann irreduzibel ist, wenn $\overline{Z}$ irreduzibel ist (das ist offensichtlich; Aufgabe 8.3.29).

Ist K eine irreduzible Komponente von X, so ist also $\overline{K}$ irreduzibel. Wegen $K \subset \overline{K}$ folgt $K = \overline{K}$ und K ist abgeschlossen. Da K maximal unter den irreduziblen Teilmengen von X ist, ist K erst recht maximal unter den abgeschlossenen irreduziblen Teilmengen.

Sei umgekehrt $L \subset X$ eine maximale abgeschlossene irreduzible Teilmgenge. Sei $Z \subset X$ irreduzibel mit $L \subset Z$. Dann ist auch $\overline{Z}$ irreduzibel. Aus $L \subset Z \subset \overline{Z}$ folgt damit $L = \overline{Z}$, also $L = Z$. □

Satz 9.2.3. *Sei X ein topologischer Raum. Dann gelten:*

(a) Jede irreduzible Teilmenge von X ist in einer irreduziblen Komponente enthalten.
(b) (Zerlegung[38] in irreduzible Komponenten) Es ist X die Vereinigung seiner irreduziblen Komponenten.

Beweis. (a): Sei $Z \subset X$ eine irreduzible Teilmenge. Wir zeigen die Aussage mit dem Zornschen Lemma 2.6.15.

Betrachte die partiell geordnete Menge $\mathcal{T}$ aller irreduziblen Teilmengen von X, die Z enthalten. Wegen $Z \in \mathcal{T}$ ist $\mathcal{T}$ nichtleer. Sei $\mathcal{K} \subset \mathcal{T}$ eine nichtleere Kette in $\mathcal{T}$. Wir behaupten, dass dann $S := \bigcup_{K \in \mathcal{K}} K \in \mathcal{T}$ gilt und somit $\mathcal{K}$ eine obere Schranke in $\mathcal{T}$ hat. Offensichtlich gilt $Z \subset S$. Zu zeigen ist, dass S irreduzibel ist. Gelte $S \subset A \cup B$ für abgeschlossene Teilmengen $A, B \subset X$. Gilt $S \subset A$, so sind wir fertig. Gelte $S \not\subset A$. Sei $K \in \mathcal{K}$ mit $K \not\subset A$. Sei $L \in \mathcal{K}$ beliebig mit $K \subset L$. Dann gilt sicherlich $L \not\subset A$. Wegen $L \subset S \subset A \cup B$ und Irreduzibilität von L folgt $L \subset B$. Da jedes Element von $\mathcal{K}$ in einem solchen L liegt, folgt $S \subset B$. Also ist S irreduzibel. Das Zornsche Lemma zeigt nun, dass $\mathcal{T}$ ein maximales Element enthält. Dieses Element ist offensichtlich eine maximale irreduzible Teilmenge von X, also eine irreduzible Komponente von X.

(b): Für jedes $x \in X$ ist $\{x\}$ irreduzibel, also nach (a) in einer irreduziblen Komponente von X enthalten. Also ist X die Vereinigung all seiner irreduziblen Komponenten. □

Satz 9.2.4. *Sei R ein Ring. Dann enthält jedes Primideal von R ein minimales Primideal. Insbesondere gilt* $\operatorname{Nil}(R) = \bigcap_{\mathfrak{p} \,\in\, \operatorname{Spec} R \text{ minimal}} \mathfrak{p}$.

Beweis. Die Primideale von R entsprechen genau den irreduziblen abgeschlossenen Teilmengen von $\operatorname{Spec} R$, per $\mathfrak{p} \mapsto \mathcal{V}(\mathfrak{p})$. Die minimalen Primideale entsprechen genau den maximalen irreduziblen abgeschlossenen Teilmengen. Dies sind nach Lemma 9.2.2 genau die irreduziblen Komponenten. Die Aussage folgt also aus Satz 9.2.3.(a).

Alternativ kann man dies auch direkt mit dem Zornschen Lemma 2.6.15 sehen: Der Schnitt über eine Kette von Primidealen ist wieder ein Primideal.

Die zweite Aussage folgt damit sofort aus $\operatorname{Nil}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$ (siehe Gleichung (2.7.2) in Proposition 2.7.11). □

Definition 9.2.5. Ein topologischer Raum X heißt **noethersch**, falls jede absteigende durch die natürlichen Zahlen indizierte Folge $Y_1 \supset Y_2 \supset Y_3 \supset \dots$ abgeschlossener Teilmengen von X stationär wird.

Lemma 9.2.6. *Jeder Unterraum Z eines noetherschen topologischen Raumes X ist noethersch.*

Beweis. Ist $Y \subset Z$ eine abgeschlossene Teilmenge, so gilt $Y = \overline{Y} \cap Z$, wobei $\overline{Y}$ der Abschluss von Y in X ist. (Ist nämlich $A \subset X$ abgeschlossen mit $Y = Z \cap A$, so folgt $\overline{Y} = \overline{Z \cap A} \subset \overline{A} = A$, also $Y = Z \cap Y \subset Z \cap \overline{Y} \subset Z \cap A = Y$ und damit $Y = Z \cap \overline{Y}$.)

Sei $Y_1 \supset Y_2 \supset Y_3 \supset \dots$ ein absteigende Folge abgeschlossener Teilmengen von Z. Da X noethersch ist, wird $\overline{Y}_1 \supset \overline{Y}_2 \supset \overline{Y}_3 \supset \dots$ stationär. Schneiden wir diese Folge mit Z, so erhalten wir unsere Ausgangsfolge, die somit auch stationär wird. □

Proposition 9.2.7. *(a) Sei R ein Noetherscher Ring. Dann ist* $\operatorname{Spec} R$ *noethersch. Jede Teilmenge von* $\operatorname{Spec} R$ *ist ebenfalls noethersch.*

[38] Zerlegung meint hier nicht „disjunkte Zerlegung“.

(b) Sei k ein algebraisch abgeschlossener[39] *Körper. Dann ist k^n mit der Zariski-Topologie noethersch. Jede Teilmenge von k^n ist ebenfalls noethersch.*

Beweis. Absteigende Folgen abgeschlossener Teilmengen von $\operatorname{Spec} R$ entsprechen nach Aufgabe 8.3.37 bijektiv aufsteigenden Folgen von Radikalidealen in R. Ist R noethersch, so wird jede aufsteigende Folge von Idealen stationär. Also ist $\operatorname{Spec} R$ noethersch.

Absteigende Folgen abgeschlossener Teilmengen von k^n entsprechen nach Satz 8.3.31 bijektiv aufsteigenden Folgen von Radikalidealen in $k[S_1, \dots, S_n]$. Da dieser Ring noethersch ist (Hilbertscher Basissatz 4.2.10 bzw. genauer sein Korollar 4.2.12), wird jede aufsteigende Folge von Idealen stationär. Also ist k^n noethersch.

Schließlich verwende man Lemma 9.2.6. □

Satz 9.2.8. *Sei X ein noetherscher topologischer Raum.*

(a) Dann besitzt X nur endlich viele irreduzible Komponenten, und keine irreduzible Komponente ist in der Vereinigung der übrigen irreduziblen Komponenten enthalten.

(b) (Kriterium für Zerlegung in irreduzible Komponenten) Sind $Y_1, \dots, Y_n$ irreduzible abgeschlossene Teilmengen von X, zwischen denen es keine nichttrivialen Inklusionen gibt (aus $Y_i \subset Y_j$ folgt also $i = j$), und gilt

$$X = Y_1 \cup Y_2 \cup \dots \cup Y_n, \tag{9.2.1}$$

so sind die (paarweise verschiedenen) Teilmengen $Y_1, \dots, Y_n$ genau die irreduziblen Komponenten von X.

Beweis. Wir beobachten zunächst, dass jede nichtleere Menge abgeschlossener Teilmengen von X ein minimales Element hat. Sonst konstruiert man leicht eine unendliche echt absteigende Folge abgeschlossener Teilmengen von X.

(Noethersche Induktion) Wir betrachten die Menge $\mathcal{M}$ aller nichtleeren abgeschlossenen Teilmengen von X, die nicht als endliche Vereinigung irreduzibler abgeschlossener Teilmengen geschrieben werden können. Angenommen, diese Menge $\mathcal{M}$ ist nichtleer, so hat sie ein minimales Element Y. Dann ist Y sicherlich nicht irreduzibel. Also existieren echte abgeschlossene Teilmengen $A, B \subsetneq Y$ mit $Y = A \cup B$. Da Y minimal gewählt war, sind A und B endliche Vereinigungen abgeschlossener irreduzibler Teilmengen. Dann ist aber auch Y eine solche Vereinigung, im Widerspruch zur Annahme.

Also ist $\mathcal{M}$ leer. Insbesondere kann also X als endliche Vereinigung

$$X = Y_1 \cup Y_2 \cup \dots \cup Y_n$$

irreduzibler abgeschlossener Teilmengen $Y_1, \dots, Y_n$ geschrieben werden. Solange es eine Inklusion $Y_i \subset Y_j$ für verschiedene Indizes $i \neq j$ gibt, können wir Y_i weglassen und somit annehmen, dass es keine nichttrivialen Inklusionen zwischen den $Y_1, \dots, Y_n$ gibt.

Sei $Z \subset X$ eine beliebige irreduzible Teilmenge. Dann gilt

$$Z = (Z \cap Y_1) \cup (Z \cap Y_2) \cup \dots \cup (Z \cap Y_n)$$

und somit $Z = Z \cap Y_i$ für ein $i \in \{1, \dots, n\}$, also $Z \subset Y_i$.

(i) Ist Z eine irreduzible Komponente, so folgt daraus $Z = Y_i$. Also ist jede irreduzible Komponente in der Menge $\{Y_1, \dots, Y_n\}$ enthalten.

(ii) Gilt $Y_j \subset Z$ für ein $j \in \{1, \dots, n\}$, so folgt $Y_j \subset Y_i$ und somit $i = j$ nach Annahme. Es folgt $Y_j = Z$. Also ist Y_j eine irreduzible Komponente von X.

Also ist $\{Y_1, \dots, Y_n\}$ genau die (n-elementige) Menge der irreduziblen Komponenten von X.

Die verbleibende Behauptung, dass keine irreduzible Komponente in der Vereinigung der übrigen irreduziblen Komponenten enthalten ist, ist trivial, da wir nun wissen, dass es nur endlich viele irreduzible

[39] Es reicht, dass k ein Körper ist, denn in diesem Fall stimmt die Zariski-Topologie auf k^n mit der Unterraumtopologie von $k^n \subset \overline{k}^n$ überein: Man wähle eine k-Basis $(b_i)_{i \in I}$ von $\overline{k}$. Dann ist $(b_i)_{i \in I}$ eine $k[S_1, \dots, S_n]$-Basis von $\overline{k}[S_1, \dots, S_n]$, man kann also jedes Polynom $f \in \overline{k}[S_1, \dots, S_n]$ eindeutig als endliche Linearkombination $f = \sum f_i b_i$ mit $f_i \in k[S_1, \dots, S_n]$ schreiben. Dann gilt $\mathbf{V}(f)_{\overline{k}} \cap k^n = \mathbf{V}(\{f_i \mid i \in I\})$. Jeder Unterraum-abgeschlossene Teilmenge ist also Zariski-abgeschlossen. Umgekehrt ist jede Zariski-abgeschlossene Teilmenge offensichtlich Unterraum-abgeschlossen.

Somit ist k^n als Teilmenge eines noetherschen Raumes noethersch (Lemma 9.2.6).

Komponenten gibt: Gelte $Y_l \subset \bigcup_{h \neq l} Y_h$ für ein $l \in \{1, \ldots, n\}$. Da Y_l irreduzibel ist, gibt es ein $h \neq l$ mit $Y_l \subset Y_h$ im Widerspruch zur Annahme. ☐

bis hier, Dienstag, 7. Februar

9.2.9 (Klassifikation der abgeschlossenen Teilmengen eines noetherschen topologischen Raums)**.** Sei X ein noetherscher topologischer Raum und $A \subset X$ eine abgeschlossene Teilmenge. Dann ist A selbst noethersch (Lemma 9.2.6) und somit die Vereinigung

$$A = Z_1 \cup \ldots, \cup Z_n$$

der endlich vielen irreduziblen Komponenten von A (Satz 9.2.8). Jede Komponenten Z_i ist eine irreduzible abgeschlossene Teilmenge von A, aber auch von X. In dieser Weise haben wir A die Menge $\{Z_1, \ldots, Z_n\}$ zugeordnet.

Satz 9.2.8 zeigt nun sofort, dass die Abbildung, die einer abgeschlossenen Teilmenge von X die Menge ihrer irreduziblen Komponenten zuordnet, eine Bijektion

$$\{\text{abgeschlossene Teilmengen von } X\} \xrightarrow{\sim} \left\{ T \in \mathcal{P}(X) \;\middle|\; \begin{array}{l} \text{für alle } Z \in T \text{ ist } Z \subset X \text{ eine irreduzible} \\ \text{abgeschlossene Teilmenge; für alle } Z, Z' \in \\ T \text{ folgt aus } Z \subset Z' \text{ bereits } Z = Z' \end{array} \right\}$$

definiert.

Beispiele 9.2.10. Man kann die Klassifikation 9.2.9 in den folgenden Fällen anwenden:

(a) $X = \operatorname{Spec} R$ für einen noetherschen Ring R;
(b) $X = k^n$ für einen algebraisch abgeschlossenen Körper k;
(c) $X = \mathbf{V}(\mathfrak{a})$ für ein Ideal $\mathfrak{a} \subset k[T_1, \ldots, T_n]$, wobei k ein algebraisch abgeschlossener Körper ist.

Definition 9.2.11. Sei R ein Ring. Ein Primideal $\mathfrak{p} \in \operatorname{Spec} R$ heißt **minimal**, falls $\mathfrak{p}$ ein minimales Element von $\operatorname{Spec} R$ ist, falls also für alle $\mathfrak{q} \in \operatorname{Spec} R$ aus $\mathfrak{q} \subset \mathfrak{p}$ bereits $\mathfrak{q} = \mathfrak{p}$ folgt.

Sei $E \subset R$ eine Teilmenge. Ein Primideal $\mathfrak{p} \in \operatorname{Spec} R$ heißt **minimal über** E, falls $\mathfrak{p}$ ein minimales Element der Menge $\mathcal{V}(E)$ ist.

9.2.12. Ein Primideal $\mathfrak{p} \in \mathcal{V}(E)$ ist genau dann minimal über E, wenn $\mathfrak{p}/\langle E \rangle$ ein minimales Primideal in $R/\langle E \rangle$ ist.

Beispiel 9.2.13. Ein Integritätsbereich hat genau ein minimales Primideal, nämlich das Nullideal.

Satz 9.2.14 (Minimale Primideale)**.** *Ist R ein noetherscher Ring, so ist die Menge der minimalen Primideale von R endlich. Ist $\mathfrak{a} \subset R$ ein Ideal, so ist die Menge der über $\mathfrak{a}$ minimalen Primideale endlich.*

Beweis. Sei R ein noetherscher Ring. Dann ist $\operatorname{Spec} R$ ein noetherscher topologischer Raum (Proposition 9.2.7). Nach Satz 9.2.8.(a) ist die Menge der irreduziblen Komponenten endlich. Die Primideale von R entsprechen bijektiv den irreduziblen abgeschlossenen Teilmengen von $\operatorname{Spec} R$. Die minimalen Primideale von R entsprechen bijektiv den maximalen irreduziblen abgeschlossenen Teilmengen von $\operatorname{Spec} R$, also den irreduziblen Komponenten von $\operatorname{Spec} R$ (Aufgabe 8.3.37 und Lemma 9.2.2). Also ist die Anzahl der minimalen Primideale in R endlich.

Ist $\mathfrak{a} \subset R$ ein Ideal, so wende man obiges auf den noetherschen Ring $R/\mathfrak{a}$ an. ☐

Beispiel 9.2.15. Sei R ein noetherscher Ring. Sei $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ die endliche Menge der minimalen Primideale von R (Satz 9.2.14). Wir nehmen an, dass die $\mathfrak{p}_i$ paarweise verschieden sind. Dann ist

$$\operatorname{Spec} R = \mathcal{V}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{V}(\mathfrak{p}_n)$$

die Zerlegung in irreduzible Komponenten. Es gilt $\operatorname{Nil}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.

9.2.16. Sei R ein noetherscher Ring und $\mathfrak{a} \subset R$ ein Ideal. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ die Urbilder der minimalen Primideale von $R/\mathfrak{a}$. Wir nehmen an, dass die $\mathfrak{p}_i$ paarweise verschieden sind. Dann sind die $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ genau die minimalen Primideale über $\mathfrak{a}$, und

$$\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{V}(\mathfrak{p}_n)$$

ist die Zerlegung in irreduzible Komponenten. Es gilt $\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.

Ist R von der Form $k[T_1, \dots, T_n]/\mathfrak{b}$, so ist

$$\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{p}_1) \cup \dots \cup \mathbf{V}(\mathfrak{p}_n)$$

die Zerlegung in irreduzible Komponenten.

9.2.17. Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \operatorname{Spec} R$ Primideale, und sei $\mathfrak{a} \subset R$ ein Ideal mit

$$\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{p}_1) \cup \dots \cup \mathcal{V}(\mathfrak{p}_n).$$

Gibt es keine nichttrivialen Inklusionen zwischen den $\mathcal{V}(\mathfrak{p}_i)$, so sind die $\mathfrak{p}_i$ die minimalen Primideale über $\mathfrak{a}$.

In der Tat, die Bijektion $\operatorname{Spec} R/\mathfrak{a} \xrightarrow{\sim} \mathcal{V}(\mathfrak{a})$ aus Proposition 2.11.17 ist ein Homöomorphhismus topologischer Räume. Das hätte längst gesagt sein müssen... Es gilt also

$$\operatorname{Spec} R/\mathfrak{a} = \mathcal{V}(\mathfrak{p}_1/\mathfrak{a}) \cup \dots \cup \mathcal{V}(\mathfrak{p}_n/\mathfrak{a}).$$

Nach Satz 9.2.8.(b) ist dies die Zerlegung von $\operatorname{Spec} R/\mathfrak{a}$ in irreduzible Komponenten $\mathcal{V}(\mathfrak{p}_i/\mathfrak{a})$. Also sind die $\mathfrak{p}_i/\mathfrak{a}$ die minimalen Primideale von $R/\mathfrak{a}$. Mit anderen Worten sind die $\mathfrak{p}_i$ die minimalen Primideale über $\mathfrak{a}$.

Aufgabe 9.2.18. Alle Teilmengen von $\mathbb{C}^n$ sind noethersch. Zerlegen Sie die folgenden Teilmengen in irreduzible Komponenten.

(a) $\mathbb{Z} \subset \mathbb{C}$;
(b) $Z = (\mathbb{Z} \times \{0\} \cup \{(0,1)\}) - \{(0,0)\} \subset \mathbb{C}^2$. Es ensteht also Z also aus allen ganzzahligen Punkten auf der x-Achse, indem man den Ursprung durch $(0,1)$ ersetzt.

9.3. Vorbereitungen für Krulls Hauptidealsatz.

9.3.1. *Nachtrag zu noetherschen Ringen.*

Lemma 9.3.1. *Sei $\mathfrak{a}$ ein Ideal in einem noetherschen Ring R. Dann gibt es ein $N \in \mathbb{N}$ mit $\sqrt{\mathfrak{a}}^N \subset \mathfrak{a} \subset \sqrt{\mathfrak{a}}$.*

Insbesondere gilt: Ist $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$ ein weiteres Ideal in R, so gibt es ein $N \in \mathbb{N}$ mit $\mathfrak{b}^N \subset \mathfrak{a}$.

Beweis. Die Inklusion $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ gilt immer. Da R noethersch ist, gilt $\sqrt{\mathfrak{a}} = (a_1, \dots, a_n)$ für geeignete Elemente $a_1, \dots, a_n \in \sqrt{\mathfrak{a}}$. Sei $N \in \mathbb{N}_{\geq 1}$ mit $a_i^N \in \mathfrak{a}$ für alle $i = 1, \dots, n$. Es folgt $\sqrt{\mathfrak{a}}^{(N-1)n+1} \subset \mathfrak{a}$. □

Beispiel 9.3.2. Wir zeigen, dass Lemma 9.3.1 falsch ist, wenn man auf die Annahme, dass der Ring noethersch ist, verzichtet.

Sei k ein Körper und $k[X_1, X_2, \dots, X_n, \dots]$ der Polynomring in abzählbar vielen Variablen. Sei A sein Quotient nach dem Ideal $(X_1, X_2^2, X_3^3, \dots, X_n^n, \dots)$. Da alle $\overline{X}_i \in A$ nilpotent sind, besteht das von diesen Elementen erzeugte Ideal $\mathfrak{m} := (\overline{X}_1, \overline{X}_2, \dots) \subset A$ aus nilpotenten Elementen. Wegen $A/\mathfrak{m} = k$ gilt $\mathfrak{m} = \operatorname{Nil}(A)$. (Es folgt auch $\operatorname{Spec} k \xrightarrow{\sim} \operatorname{Spec} A = \{\mathfrak{m}\}$ nach Lemma 7.4.10; insbesondere ist A ein lokaler Ring der Dimension Null.)

Da das Ideal $\mathfrak{m}$ offensichtlich nicht endlich erzeugt ist, ist A nicht noethersch.

Betrachte nun das Nullideal $\mathfrak{a} = (0)$. Es gilt $\sqrt{\mathfrak{a}} = \operatorname{Nil}(A)$. Es gibt aber kein $N \in \mathbb{N}$ mit $\sqrt{\mathfrak{a}}^N = \operatorname{Nil}(A)^N \subset \mathfrak{a} = (0)$, denn das Element $x_N \in \operatorname{Nil}(A)$ erfüllt $x_N^{N-1} \neq 0$.

9.3.2. *Artinsche Moduln.*

Definition 9.3.3. Sei R ein Ring. Ein R-Modul M heißt **artinsch**, falls jede durch die natürlichen Zahlen indizierte absteigende Kette $U_0 \supset U_1 \supset U_2 \supset \dots$ von Untermoduln von M stationär wird.

9.3.4. Man vergleiche diese Definition mit der Charakterisierung noetherscher Moduln durch aufsteigende Ketten in Proposition 4.1.8.

Beispiel 9.3.5. Ist k ein Körper, so sind für einen k-Vektorraum M die folgenden Bedingungen äquivalent:

(a) $\dim_k M < \infty$;
(b) M ist artinsch;
(c) M ist noethersch.

Ist M endlichdimensional, so ist M offensichtlich artinsch und noethersch.

Ist M unendlichdimensional, so sei $(b_n)_{n\in\mathbb{N}}$ eine Folge linear unabhängiger Vektoren in M.

Sei $U_n \subset M$ der von den Elementen $b_0, b_1, \dots, b_n$ erzeugte Untervektorraum. Dann ist $U_0 \subsetneq U_1 \subsetneq \dots$ eine echt aufsteigende Folge von Unterräumen, die nicht stationär wird. Also ist M nicht noethersch.

Sei $V_n \subset M$ der von den Elementen $b_n, b_{n+1}, \dots$ erzeugte Untervektorraum. Dann ist $V_0 \supsetneq V_1 \supsetneq \dots$ eine echt absteigende Folge von Unterräumen, die nicht stationär wird. Also ist M nicht artinsch.

Proposition 9.3.6. *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Folge von R-Moduln. Dann ist M genau dann artinsch, wenn M' und M'' artinsch sind.*

Beweis. Ist M artinsch, so folgt sofort, dass auch M' und M'' artinsch sind.

Seien nun M' und M'' artinsch. Wir können ohne Einschränkung annehmen, dass $M' \subset M$ ein Untermodul ist. Sei π die gegebene Abbildung $M \to M''$. Sei $U_0 \supset U_1 \supset U_2 \supset \dots$ eine absteigende von Untermoduln von M. Dann werden die beiden Ketten $(U_i \cap M')$ in M' und $\pi(U_i)$ in M'' laut Annahme stationär, es gibt also ein $n \in \mathbb{N}$ mit $U_n \cap M' = U_N \cap M'$ und $\pi(U_n) = \pi(U_N)$ für alle $N \geq n$.

Wir behaupten $U_n = U_N$ für alle $N \geq n$. Zu zeigen ist $U_n \subset U_N$. Sei also $x \in U_n$ gegeben. Wegen $\pi(x) \in \pi(U_n) = \pi(U_N)$ gibt es ein $y \in U_N$ mit $\pi(x) = \pi(y)$, also $x - y \in \ker(\pi) = M'$. Wir folgern $x - y \in M' \cap U_n = M' \cap U_N$ und somit $x = (x-y) + y \in U_N$. □

9.3.3. *Artinsche Ringe.*

Definition 9.3.7. Ein Ring heißt **artinsch**, falls er als Modul über sich selbst artinsch ist. Ein **Artin-Ring** ist ein artinscher Ring.

Lemma 9.3.8. *Sei R ein Ring und seien $\mathfrak{m}_1, \dots, \mathfrak{m}_n \in \operatorname{MaxSpec} R$ (nicht notwendig verschiedene) maximale Ideale mit*

$$\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_n = (0).$$

Dann gilt

$$\operatorname{MaxSpec} R = \operatorname{Spec} R = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$$

und es sind äquivalent:

(a) R ist artinsch;
(b) R ist noethersch.

9.3.9. Die Bedingung $\operatorname{MaxSpec} R = \operatorname{Spec} R$ ist äquivalent zu $\dim R \in \{0, -\infty\}$.

9.3.10. Gilt $\operatorname{MaxSpec} R = \operatorname{Spec} R$ und ist diese Menge endlich, so folgt daraus nicht, dass R noethersch oder artinsch ist, siehe Beispiel 9.3.14.

Beweis. Betrachte die absteigende Folge

$$I_0 := R \supset I_1 := \mathfrak{m}_1 \supset I_2 := \mathfrak{m}_1\mathfrak{m}_2 \supset \dots \supset I_n := \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n = (0)$$

von Idealen in R. Sukzessive Anwendung von Proposition 9.3.6 zeigt, dass R genau dann artinsch ist, wenn alle Quotienten I_{i-1}/I_i artinsch sind, für $i = 1, \dots, n$. Da I_{i-1}/I_i ein Modul über dem Körper $R/\mathfrak{m}_i$ ist, ist dieser genau dann artinsch, wenn er endlichdimensional ist, was genau dann der Fall ist, wenn er noethersch ist (Beispiel 9.3.5). (Hier verwenden wir, dass für einen Modul über einem Quotientenring $R/\mathfrak{a}$ von R die Eigenschaften „artinsch (bzw. noethersch) als R-Modul“ und „artinsch (bzw. noethersch) als $R/\mathfrak{a}$-Modul“ übereinstimmen.) Nach der analogen Proposition 4.1.4 für Noetherschheit zeigt dies die erste Behauptung.

Aus $(0) = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n$ folgt

$$\operatorname{Spec} R = \mathcal{V}(0) = \mathcal{V}(\mathfrak{m}_1 \cdots \mathfrak{m}_n) = \mathcal{V}(\mathfrak{m}_1) \cup \dots \cup \mathcal{V}(\mathfrak{m}_n) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\},$$

insbesondere sind also alle Primideale maximal. □

Satz 9.3.11 (Artinsche und noethersche Ringe)**.** *Ist R ein Ring, so sind die beiden folgenden Bedingungen äquivalent:*

(a) R ist artinsch;
(b) R ist noethersch mit $\dim R \in \{0, -\infty\}$ (letzteres bedeutet $\operatorname{Spec} R = \operatorname{MaxSpec} R$).

Sind sie erfüllt, so ist $\operatorname{MaxSpec} R = \operatorname{Spec} R$ endlich.

Beweis. (a) ⇒ (b): Sei R artinsch. Wir zeigen zuerst, dass $\operatorname{MaxSpec} R$ endlich ist. Ist dies nicht der Fall, so finden wir abzählbar viele paarweise verschiedene maximale Ideale $\mathfrak{m}_1, \mathfrak{m}_2, \dots$ in R. Dann ist

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supset \dots$$

eine absteigende Folge von Idealen. Da R artinsch ist, gibt es ein $l \in \mathbb{N}$ mit $\bigcap_{i=1}^{l} \mathfrak{m}_i = \bigcap_{i=1}^{l+1} \mathfrak{m}_i \subset \mathfrak{m}_{l+1}$. Es folgt

$$\{\mathfrak{m}_1, \dots, \mathfrak{m}_l\} = \bigcup_{i=1}^{l} \mathcal{V}(\mathfrak{m}_i) = \mathcal{V}(\bigcap_{i=1}^{l} \mathfrak{m}_i) \supset \mathcal{V}(\mathfrak{m}_{l+1}) = \{\mathfrak{m}_{l+1}\}$$

im Widerspruch dazu, dass die $\mathfrak{m}_i$ paarweise verschieden sind. Also ist $\operatorname{MaxSpec} R$ endlich.

Seien $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ die endlich vielen maximalen Ideale von R. Setze

$$I := \mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_n.$$

Die absteigende Folge $R \supset I \supset I^2 \supset \dots$ von Idealen wird stationär. Sei $M \in \mathbb{N}_{\geq 1}$ mit

$$J := I^M = I^N \quad \text{für alle } N \geq M.$$

Wir behaupten, dass $J = (0)$ gilt.

Wir führen die Annahme $J \neq (0)$ ad absurdum. Dann ist $JJ = I^{2M} = I^M = J \neq (0)$. Also ist die Menge

$$\mathcal{A} := \{\mathfrak{a} \subset R \mid \mathfrak{a} \text{ ist Ideal mit } \mathfrak{a}J \neq (0)\}$$

nichtleer. Sei $\mathfrak{b}$ ein minimales Element in $\mathcal{A}$; ein solches Element existiert, denn sonst konstruiert man sofort eine unendliche echt absteigende Kette von Idealen in R. Sei $b \in \mathfrak{b}$ mit $bJ \neq (0)$. Die obige Beobachtung $J^2 = J$ liefert

$$((b)J)J = (b)J \neq (0),$$

also sind $(b)J$ und (b) in $\mathcal{A}$. Wegen $(b)J \subset (b) \subset \mathfrak{b}$ und Minimalität von $\mathfrak{b}$ folgt $(b)J = (b) = \mathfrak{b}$. Insbesondere gibt es ein $c \in J$ mit $b = bc$. Nach Definition von J liegt c in allen maximalen Idealen von R. Also liegt $c-1$ in keinem maximalen Ideal von R, ist also invertierbar (Proposition 2.8.4). Aus $b(c-1) = bc - b = 0$ folgt somit $b = 0$ im Widerspruch zu $bJ \neq (0)$.

Es gilt also $J = 0$. Da J ein Produkt von endlich vielen maximalen Idealen ist, zeigt die Äquivalenz in Lemma 9.3.8, dass R noethersch ist.

(b) ⇒ (a): Sei R noethersch mit $\dim(R) \leq 0$. Der Fall $R = 0$ ist trivial. Wir können also $\dim R = 0$ annehmen. Da R Noethersch ist, gilt

$$\operatorname{Nil}(R) = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_l,$$

wobei $\mathfrak{p}_1, \dots, \mathfrak{p}_l$ die endlich vielen minimalen Primideale von R sind (Sätze 9.2.4 und 9.2.14).

Sei $I := \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_l \subset \operatorname{Nil}(R) = \sqrt{(0)}$. Da R Noethersch ist, liefert Lemma 9.3.1 ein $N \in \mathbb{N}$ mit $I^N \subset (0)$. Wegen $\dim(R) = 0$ sind alle Primideale in R maximal. Die Gleichung $I^N = 0$ zeigt somit, dass ein Produkt von maximalen Idealen von R Null ist. Die Äquivalenz in Lemma 9.3.8 zeigt somit, dass R artinsch ist. Der andere Teil dieses Lemmas zeigt, dass $\operatorname{MaxSpec} R = \operatorname{Spec} R$ endlich ist. □

Beispiel 9.3.12. Jeder artinsche Integritätsbereich ist ein Körper. Äquivalent (nach Satz 9.3.11): Jeder noethersche Integritätsbereich der Dimension Null ist ein Körper.

In der Tat ist in jedem Integritätsbereich das Nullideal prim. Ist unser Ring artinsch, so ist jedes Primideal maximal (Satz 9.3.11). Damit ist das Nullideal maximal und unser Ring ist ein Körper.

Alternativ kann man dies auch direkt aus der Definition eines artinschen Rings folgern: Sei R unser artinscher Integritätsbereich und sei $0 \neq x \in R$. Die absteigende Folge $R \supset (x) \supset (x^2) \supset \dots$ von Idealen wird stationär. Also gibt es ein $n \in \mathbb{N}$ mit $(x^n) = (x^{n+1})$, d. h. $x^n = yx^{n+1}$ für ein $y \in R_f$. Da R ein Integritätsbereich ist, gilt $x^n \neq 0$ und wir erhalten durch Kürzen $1 = yx$. Also ist R ein Körper.

Beispiel 9.3.13. Wir geben ein Beispiel eines lokalen Ringes der Dimension Null, der nicht noethersch (und damit auch nicht artinsch) ist.

Sei k ein Körper und $k[X_1, X_2, \dots, X_n, \dots]$ der Polynomring in abzählbar vielen Variablen. Sei A sein Quotient nach dem Ideal $(X_1^2, X_2^2, X_3^2, \dots)$. Da alle X_i in A nilpotent sind, ist das von diesen Elementen erzeugte Ideal $\mathfrak{m} := (\overline{X}_1, \overline{X}_2, \dots) \subset A$ nilpotent. Es gilt $A/\mathfrak{m} = k$ und somit $\{(0)\} = \operatorname{Spec} k \xrightarrow{\sim} \operatorname{Spec} A = \{\mathfrak{m}\}$ nach Lemma 7.4.10. (Es folgt natürlich auch $\mathfrak{m} = \operatorname{Nil}(A)$.)

Dies zeigt $\operatorname{Spec} A = \operatorname{MaxSpec} A = \{\mathfrak{m}\}$. Also ist A ein lokaler Ring der Dimension Null. Der Ring A ist aber nicht noethersch, denn das Ideal $\mathfrak{m}$ ist offensichtlich nicht endlich erzeugt.

Beispiel 9.3.14. Sei A mit maximalem Ideal $\mathfrak{m}$ wie in Beispiel 9.3.13. Dann gilt $\mathfrak{m}\mathfrak{m} = \mathfrak{m}^2 = 0$. Also ist die Voraussetzung von Lemma 9.3.8 erfüllt, A ist aber nicht noethersch (und damit auch nicht artinsch).

9.4. **Krulls Hauptidealsatz.**

Aufgabe 9.4.1 (Krulls Hauptidealsatz für faktorielle Ringe)**.** Seien R ein faktorieller Ring und $0 \neq a \in R$. Ist $\mathfrak{p}$ minimal in $\mathcal{V}(a)$, so gilt $\operatorname{ht}(\mathfrak{p}) = 1$.

Satz 9.4.2 (Krulls Hauptidealsatz)**.** *Seien A ein noetherscher Ring und $a \in A$ ein Element. Ist $\mathfrak{p}$ ein minimales Primideal*[40] *über a, so gilt* $\operatorname{ht}(\mathfrak{p}) \leq 1$. *Ist a kein Nullteiler, so gilt* $\operatorname{ht}(\mathfrak{p}) = 1$.

9.4.3. Der Spezialfall, dass A ein Integritätsbereich ist, ist wichtig: Gilt $a \neq 0$, so hat jedes minimale Primoberideal von a Höhe Eins.

Beweis. Proposition 6.2.5 zeigt erstens, dass das (eindeutige) maximale Ideal $\mathfrak{p}_\mathfrak{p} \in \operatorname{Spec} A_\mathfrak{p}$ minimal über $\frac{a}{1}$ ist, und zweitens, dass $\operatorname{ht}_A(\mathfrak{p}) = \operatorname{ht}_{A_\mathfrak{p}}(\mathfrak{p}_\mathfrak{p})$ gilt.

Ist a kein Nullteiler in A, so ist auch $\frac{a}{1}$ kein Nullteiler in $A_\mathfrak{p}$: Aus $\frac{a}{1} \cdot \frac{b}{s} = 0$ für $b \in A$ und $s \in A - \mathfrak{p}$ folgt, dass es ein $t \in A - \mathfrak{p}$ gibt mit $tab = 0$; da a kein Nullteiler ist, folgt $tb = 0$, also $\frac{b}{s} = \frac{tb}{ts} = 0$.

Schließlich ist mit A auch $A_\mathfrak{p}$ noethersch (Aufgabe 6.1.25).

Wir können also ohne Einschränkung annehmen, dass A ein lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{p}$ ist.

Der Quotient $A/(a)$ ist ebenfalls ein lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{p}/(a)$ (Proposition 4.2.5), und dieses maximale Ideal ist auch ein minimales Primideal (über 0). Es ist also das einzige Primideal von $A/(a)$. Also ist $A/(a)$ artinsch nach Satz 9.3.11.

Wir behaupten, dass dann auch A_a artinsch ist. Seien

$$A_a \xleftarrow{\lambda} A \xrightarrow{\pi} A/(a)$$

die offensichtlichen Abbildungen. Seien $I \subset J$ Ideale in A_a mit $\pi(\lambda^{-1}(I)) = \pi(\lambda^{-1}(J))$. Es reicht zu zeigen, dass $I = J$ gilt.

Sei $x \in \lambda^{-1}(J)$. Wegen $\pi(x) \in \pi(\lambda^{-1}(J)) = \pi(\lambda^{-1}(I))$ gibt es ein $y \in \lambda^{-1}(I)$ und ein $z \in A$ mit $x = y + az$. Es folgt $az = x - y \in \lambda^{-1}(J)$, d. h. $\frac{az}{1} \in J$. Es folgt $\frac{z}{1} = \frac{1}{a}\frac{az}{1} \in J$ und somit $z \in \lambda^{-1}(J)$. Also gilt $x = y + az \in \lambda^{-1}(I) + a\lambda^{-1}(J)$. Für den A-Modul $M := \frac{\lambda^{-1}(J)}{\lambda^{-1}(I)}$ bedeutet dies $M \subset aM$. Wir erhalten

$$M \subset aM \subset \mathfrak{p}M \subset M.$$

und somit Gleichheit $M = \mathfrak{p}M$. Nakayamas Lemma für lokale Ringe (Korollar 3.9.9) zeigt $M = 0$; Man beachte, dass $\lambda^{-1}(J)$ als Ideal im noetherschen Ring A endlich erzeugt ist, und somit M ein endlich erzeugter A-Modul ist. Somit gilt $\lambda^{-1}(I) = \lambda^{-1}(J)$. Daraus folgt sofort $I = J$: Sei $\frac{b}{a^n} \in J$ für $b \in A$ und $n \in \mathbb{N}$, so folgt $\frac{b}{1} \in J$, somit $b \in \lambda^{-1}(J) = \lambda^{-1}(I)$, also $\frac{b}{1} \in I$ und somit $\frac{b}{a^n} \in I$. Also ist A_a artinsch.

Nach Satz 9.3.11 ist A_a Noethersch mit $\dim A_a \in \{0, -\infty\}$.

Gibt es ein $\mathfrak{q} \in \operatorname{Spec} A$ mit $\mathfrak{q} \subsetneq \mathfrak{p}$, so ist $\operatorname{ht}(\mathfrak{q}) = 0$ zu zeigen, denn daraus folgt $\operatorname{ht}(\mathfrak{p}) \leq 1$. Da $\mathfrak{p}$ minimal über a ist, folgt $a \notin \mathfrak{q}$. Also ist $\mathfrak{q}_a$ ein Primideal in A_a und es gilt $\operatorname{ht}_A(\mathfrak{q}) = \operatorname{ht}_{A_a}(\mathfrak{q}_a)$ (siehe Korollar 6.2.6). Insbesondere ist A_a nicht der Nullring, so dass $\dim A_a = 0$ gelten muss. Daraus folgt $\operatorname{ht}_A(\mathfrak{q}) = \operatorname{ht}_{A_a}(\mathfrak{q}_a) = 0$ wie gewünscht.

Sei nun a kein Nullteiler. Dann ist a auch nicht nilpotent: Nehmen wir an, das a nilpotent ist. Sei $a^n = 0$ mit $n \in \mathbb{N}$ minimal. Wegen $1 \neq 0$ in $A_\mathfrak{p}$ (da dies ein lokaler Ring ist) folgt $n \geq 1$. Es folgt $aa^{n-1} = 0$. Wegen $a^{n-1} \neq 0$ ist also a ein Nullteiler im Widerspruch zur Annahme. Also ist a nicht nilpotent. Wir verwenden nur diese Eigenschaft von a im Rest des Beweises.[41]

---

[40] Gibt es ein solches, so ist a keine Einheit.

[41] Im Fall eines lokalen Ringes kann man also in der Aussage von Krulls Hauptideals die Bedingung „kein Nullteiler“ durch die Bedingung „nicht nilpotent“ ersetzen. Diese ist im Allgemeinen schächer: Betrachte etwa die Lokalisierung von $\mathbb{C}[X,Y]/(XY)$ am maximalen Ideal $(\overline{X}, \overline{Y})$; das Element $\frac{\overline{X}}{1}$ dieser Lokalisierung ist ein Nullteiler, aber nicht nilpotent.

Da a nicht nilpotent ist, gilt $A_a \neq 0$. Insbesondere gibt es in A_a ein maximales Ideal. Sein Urbild $\mathfrak{s}$ in A ist ein Primideal mit $a \notin \mathfrak{s}$. Da A lokal ist und sein maximales Ideal $\mathfrak{p}$ das Element a enthält, erhalten wir eine Primidealkette $\mathfrak{s} \subsetneq \mathfrak{p}$ der Länge Eins. Es folgt $\operatorname{ht}(\mathfrak{p}) \geq 1$. □

bis hier, Mittwoch, 8. Februar, Vorlesungsende.

Beispiel 9.4.4. Sei $A = \mathbb{C}[X,Y]/(XY)$. Dieser Ring hat die Elemente $1, X, X^2, \dots$ und $Y, Y^2, Y^3, \dots$ als $\mathbb{C}$-Basis. Das Element $a = X$ ist ein Nullteiler. Da $\mathfrak{p} := (a) = (X)$ ein Primideal ist, ist es das einzige minimale Primoberideal von (a). Man überzeugt sich sofort, dass $\operatorname{ht}(\mathfrak{p}) = 0$ gilt. Anschaulich ist ja eh klar, dass die y-Achse im Koordinatenkreuz Kodimension 0 hat.

Beispiel 9.4.5. Wir geben ein Beispiel eines nicht noetherschen Ringes samt einem primen Hauptideal, das Höhe zwei hat.

Sei $A := \mathbb{C}[X, Y, X^{-1}Y, X^{-2}Y, X^{-3}Y, \dots] \subset \mathbb{C}[X, X^{-1}, Y]$. Eine $\mathbb{C}$-Basis von A ist gegeben durch

$$\{X^n \mid n \in \mathbb{N}\} \cup \{X^n Y^m \mid n \in \mathbb{Z}, m \geq 1\}.$$

Sei $S \subset A$ die multiplikative Teilmenge aller Elemente mit konstantem Term $\neq 0$. (Dies ist das Komplement des Primideals AX von A; es gilt $A/AX = \mathbb{C}$.)

Jedes Element $a \in A$ kann man eindeutig als $a = X^n Y^m s$ schreiben für ein $s \in S$ und $m \in \mathbb{N}$ und $n \in \mathbb{Z}$ mit $n \geq 0$ falls $m = 0$.

Sei $R := S^{-1}A$. Jedes Element $r \in R$ kann man eindeutig als $r = X^n Y^m u$ schreiben für ein $u \in R^\times$ und $m \in \mathbb{N}$ und $n \in \mathbb{Z}$ mit $n \geq 0$ falls $m = 0$.

Es ist klar, dass R ein Integritätsbereich ist. Wir behaupten, dass $\operatorname{Spec} R$ genau aus den drei Elementen $(0), RX, \mathfrak{q} := RY + RX^{-1}Y + RX^{-2}Y + \dots$ besteht.

Sei $(0) \subsetneq \mathfrak{p} \subset R$ ein Primideal. Sei $0 \neq r \in \mathfrak{p}$. Schreibe $r = X^n Y^m u$ wie oben. Es folgt, dass es ein Element der Form $X^n Y^m \in \mathfrak{p}$ gibt, mit $(m,n) \neq (0,0)$. Falls es ein solches Element mit $m = 0$ gibt, so folgt $\mathfrak{p} = RX$. Sonst gibt es ein solches Element mit $m > 0$. Wir können zusätzlich annehmen, dass $n \geq 0$ gilt. Wegen $X^n \notin \mathfrak{p}$ folgt $Y^m \in \mathfrak{p}$ und damit $Y \in \mathfrak{p}$. Aus $Y = X^n(X^{-n}Y) \in \mathfrak{p}$ folgt $X^{-n}Y \in \mathfrak{p}$. Wir erhalten $\mathfrak{p} = RY + RX^{-1}Y + RX^{-2}Y + \dots = \mathfrak{q}$.

Aus $(0) \subsetneq \mathfrak{q} \subsetneq RX$ folgt, dass RX Höhe zwei hat.

Da $\operatorname{Spec} R$ genau aus diesen drei Primidealen besteht, gilt also $\dim R = 2$.

Satz 9.4.6. *Sei R ein noetherscher Ring.*

(a) Ist $\dim R \geq 2$, so ist $\operatorname{Spec} R$ unendlich.

(b) Seien $\mathfrak{p}_0 \subset \mathfrak{p}_2$ 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

$$\{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p}_0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_2\}$$

unendlich.

(c) Sei $(R, \mathfrak{m})$ ein lokaler noetherscher Integritätsbereich mit $\dim R \geq 2$. Dann ist

$$\{\mathfrak{p} \in \operatorname{Spec} R \mid \operatorname{ht}(\mathfrak{p}) = 1\}$$

unendlich.

Beispiel 9.4.7. Wir haben in Beispiel 9.4.5 einen nichtnoetherschen Ring der Dimension zwei kennengelernt, dessen Spektrum aus nur drei Elementen besteht.

Beweis. (a) $\Leftarrow$ (b): Offensichtlich.

(b) $\Leftarrow$ (c): Betrachte $(R/\mathfrak{p}_0)_{\mathfrak{p}_2/\mathfrak{p}_0} = R_{\mathfrak{p}_2}/(\mathfrak{p}_0)_{\mathfrak{p}_2}$ (und verwende Proposition 4.2.5, Aufgabe 6.1.25, und 6.2.9).

(c): Sonst sei $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ eine endliche Liste aller Primideale der Höhe Eins. Wegen $\dim R \geq 2$ gilt $n \geq 1$. Da $\mathfrak{m}$ maximal ist und $\dim R \geq 2$ gilt, folgt $\mathfrak{p}_i \subsetneq \mathfrak{m}$ für alle $i = 1, \dots, n$, d. h. es gibt für jedes solche i ein Element von $\mathfrak{m}$, das $\mathfrak{p}_i$ vermeidet. Nach Primvermeidung, Proposition 2.10.8, gibt es ein Element

$$f \in \mathfrak{m} - \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Wegen $(f) \subset \mathfrak{m}$ ist $R/(f)$ nicht der Nullring. Es gibt also ein maximales Ideal in $R/(f)$ (Satz 2.6.13), und dieses enthält ein minimales Primideal (Satz 9.2.4). Sein Urbild $\mathfrak{q} \subset R$ ist ein minimales Primideal über (f). Wegen $f \neq 0$ (da f nicht in $\mathfrak{p}_1$ liegt) und der Annahme, dass R ein Integrtiätsbereich ist, ist f kein Nullteiler. Also gilt $\operatorname{ht}(\mathfrak{q}) = 1$ nach dem Krullschen Hauptidealsatz 9.4.2. Wegen $f \in \mathfrak{q}$ kommt $\mathfrak{q}$ aber nicht in der Liste aller Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ der Höhe Eins vor. Dieser Widerspruch beweist die Behauptung. □

Satz 9.4.8 (Artin und Tate)**.** *Sei R ein noetherscher Integritätsbereich. Dann sind äquivalent:*

(a) $\operatorname{Spec} R$ *ist eine endliche Menge.*
(b) Es gibt ein $f \in R$ mit $R_f = \operatorname{Quot}(R)$.

Sind diese Bedingungen erfüllt, so gilt $\dim R \leq 1$. *Es besteht* $\operatorname{Spec} R$ *also aus dem Nullideal und endlich vielen Primidealen der Höhe Eins.*

Beweis. (a) → (b) Sei $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ eine Liste aller vom Nullideal verschiedenen Primideale von R. Im Fall $n = 0$ ist das Nullideal das einzige Primideal und somit maximal, so dass also R bereits ein Körper ist, und wir $f = 1$ wählen können. Gelte $n \geq 1$. Wähle $0 \neq f_i \in \mathfrak{p}_i$ für alle $i = 1, \dots, n$. Weil R ein Integritätsbereich ist, gilt $0 \neq f := f_1 f_2 \cdots f_n \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$. Es folgt $\operatorname{Spec} R_f = \{0\}$ (da f nicht nilpotent ist, ist $R_f \neq 0$). Der Ring R_f hat also Dimension 0; außerdem ist er noethersch (nach Aufgabe 6.1.25 oder (zu kompliziert) wegen $R_f = R[X]/(Xf - 1)$ samt Hilbertschem Basissatz 4.2.10 und Proposition 4.2.5). Nach Satz 9.3.11 ist R_f artinsch. Da R_f auch ein Integritätsbereich ist, ist R_f ein Körper (Beispiel 9.3.12). Also ist $R_f \hookrightarrow \operatorname{Quot}(R)$ surjektiv und wir erhalten $R_f = \operatorname{Quot}(R)$.

(b) → (a): Sei $f \in R$ mit $R_f = \operatorname{Quot}(R)$. Wegen $\operatorname{Spec} R_f = \operatorname{Spec} \operatorname{Quot}(R) = \{(0)\}$ ist f in jedem Primideal $(0) \neq \mathfrak{p} \in \operatorname{Spec} R$ enthalten. Alle Primideale der Höhe ≥ 1 enthalten also f. Insbesondere ist jedes Primideal $\mathfrak{p} \in \operatorname{Spec} R$ mit $\operatorname{ht}(\mathfrak{p}) = 1$ ein minimales Primoberideal von (f) Von diesen gibt es nach Satz 9.2.14 nur endlich viele. Das einzige Primideal der Höhe Null ist das Nullideal.

Angenommen, es gibt ein $\mathfrak{p} \in \operatorname{Spec} R$ mit $\operatorname{ht}(\mathfrak{p}) \geq 2$. Dann gilt $\dim R_{\mathfrak{p}} = \operatorname{ht}(\mathfrak{p}) \geq 2$. Da $R_{\mathfrak{p}}$ ein lokaler noetherscher Integritiätsbereich ist, gibt es in $\operatorname{Spec} R_{\mathfrak{p}}$ unendlich viele Primideale der Höhe Eins (Satz 9.4.6.(c)). Also gibt es in $\operatorname{Spec} R$ ebenfalls unendlich viele Primideale der Höhe Eins. Dies steht im Widerspruch zu den obigen Überlegungen. Also ist $\operatorname{Spec} R$ endlich.

Wir haben gerade gesehen, dass alle Primideale von R Höhe ≤ 1 haben. Also gilt $\dim R \leq 1$. □

Literatur

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Bos13] Siegfried Bosch, *Algebraic geometry and commutative algebra*, Universitext, Springer, London, 2013.

[Bou98] Nicolas Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation.

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hil90] David Hilbert, *Ueber die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), no. 4, 473–534.

[Kem11] Gregor Kemper, *A course in commutative algebra*, Graduate Texts in Mathematics, vol. 256, Springer, Heidelberg, 2011.

[Kun80] Ernst Kunz, *Einführung in die kommutative Algebra und algebraische Geometrie*, Vieweg Studium: Aufbaukurs Mathematik [Vieweg Studies: Mathematics Course], vol. 46, Friedr. Vieweg & Sohn, Braunschweig, 1980, With an English preface by David Mumford.

[Mat89] Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989.

[Pes96] Christian Peskine, *An algebraic introduction to complex projective geometry. 1*, Cambridge Studies in Advanced Mathematics, vol. 47, Cambridge University Press, Cambridge, 1996, Commutative algebra.

[Rei95] Miles Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, vol. 29, Cambridge University Press, Cambridge, 1995.

[Ser65] Jean-Pierre Serre, *Algèbre locale. Multiplicités*, Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel. Seconde édition, 1965. Lecture Notes in Mathematics, vol. 11, Springer-Verlag, Berlin-New York, 1965.

[Ser00] ———, *Local algebra*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, Translated from the French by CheeWhye Chin and revised by the author.

[Sta16] The Stacks Project Authors, *Stacks project*, http://stacks.math.columbia.edu, 2016.

[ZS75a] Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. 1*, Springer-Verlag, New York-Heidelberg-Berlin, 1975, With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

[ZS75b] ———, *Commutative algebra. Vol. II*, Springer-Verlag, New York-Heidelberg, 1975, Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

Mathematisches Institut, Universität Bonn, Endenicher Allee 60, 53115 Bonn, Germany
E-mail address: olaf.schnuerer@math.uni-bonn.de