

# Zusammenfassung Kommutative Algebra

© Tim Baumann, <http://timbaumann.info/uni-spicker>

## Ringe und Ideale

**Def.** Ein Ring ist ein Tupel  $(A, +, \cdot, 0, 1)$  mit einer Menge  $A$ , Operationen  $+, \cdot : A \times A \rightarrow A$  und Elementen  $0, 1 \in A$ , sodass

- $(A, +, 0)$  eine abelsche Gruppe ist,
- $(A, \cdot, 1)$  ein Monoid ist und
- die Multiplikation distributiv über die Addition ist, d. h.

$$x(y + z) = xy + xz \text{ und } (y + z)x = yx + zx \quad \forall x, y, z \in A.$$

**Bspe.** •  $\mathbb{Z}$ , •  $K[x_1, \dots, x_n]$ , • **Nullring**: der Ring mit  $0 = 1$

**Def.** Sei  $(A, +, \cdot)$  ein Ring. Eine Teilmenge  $B \subseteq A$  heißt **Unterring**, falls  $0, 1 \in B$  und  $B$  unter  $+$  und  $\cdot$  abgeschlossen ist.

**Bspe.** •  $\mathbb{Z} \subset \mathbb{Q}$ , •  $K \subset K[X]$

**Def.** Ein **Ringhomomorphismus**  $\phi : A \rightarrow B$  ist eine Abbildung, welche sowohl ein Gruppenhomom.  $(A, +_A, 0_A) \rightarrow (B, +_B, 0_B)$  als auch ein Ringhomomorphismus  $(A, \cdot_A, 1_A) \rightarrow (B, \cdot_B, 1_B)$  ist.

*Bem.* Ringe und Ringhomomorphismen bilden eine Kategorie **Ring**.

**Lem.** Ein Ringhomomorphismus ist genau dann ein Isomorphismus (in dieser Kategorie), wenn er bijektiv ist.

**Konvention.** Seien  $A$  im Folgenden Ringe und  $\phi : A \rightarrow B$  ein Ringhomomorphismus.

**Def.** Eine Teilmenge  $\mathfrak{a} \subseteq A$  heißt (beidseitiges) **Ideal** von  $A$ , falls

- $\mathfrak{a} \subseteq A$  eine Untergruppe ist und
- für alle  $a \in A$  und  $x \in \mathfrak{a}$  gilt:  $ax, xa \in \mathfrak{a}$ .

**Lem.** Der Schnitt von (beliebig vielen) Idealen ist selbst ein Ideal.

**Def.** Sei  $M \subseteq A$  eine Teilmenge. Das von  $M$  **erzeugte Ideal** ist der Schnitt aller Ideale von  $A$ , die  $M$  umfassen.

*Bem.* Falls  $A$  kommutativ ist, so gilt

$$\text{von } M \text{ erzeugtes Ideal} = \left\{ \sum_{k=1}^n \lambda_k x_k \mid n \in \mathbb{N}, \lambda_k \in A, x_k \in M \right\}.$$

**Notation.**  $(x_1, \dots, x_n) \subseteq A$  ist das von  $\{x_1, \dots, x_n\}$  erzeugte Ideal.

*Bem.* • Das **Nullideal**  $(0)$  ist das kleinste Ideal, denn  $(0) = \{0\}$ .  
• Das **Einsideal**  $(1)$  ist das größte Ideal, denn  $(1) = A$ .

**Prop.** • Sei  $\mathfrak{b} \subseteq B$  ein Ideal. Dann ist auch  $\phi^{-1}(\mathfrak{b}) \subseteq A$  ein Ideal.  
• Sei  $A' \subseteq A$  ein Unterring. Dann ist auch  $\phi(A') \subseteq B$  ein Unterring.

**Def.** Das Ideal  $\ker \phi := \phi^{-1}((0))$  heißt **Kern** von  $\phi$ .

*Bem.*  $\phi$  ist injektiv  $\iff \ker \phi = 0$

**Prop.** Sei  $\phi : A \rightarrow B$  surjektiv,  $\mathfrak{a} \subseteq A$  ein Ideal. Dann ist auch das Bild  $\phi(\mathfrak{a}) \subseteq B$  ein Ideal.

**Prop.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Dann gibt es einen Ring  $A/\mathfrak{a}$  und einen Ringhomom.  $\pi : A \rightarrow A/\mathfrak{a}$  mit folgender universeller Eigenschaft:  
Für jeden Ring  $B$  und Ringhomom.  $\psi : A \rightarrow B$  mit  $\mathfrak{a} \subseteq \ker \psi$  gibt es genau einen Ringhomom.  $\tilde{\psi} : A/\mathfrak{a} \rightarrow B$  mit  $\psi = \tilde{\psi} \circ \pi$ .

*Konstr.* Sei durch  $x \sim y : \iff x - y \in \mathfrak{a}$  eine Äq'-relation  $\sim$  auf  $A$  definiert. Setze  $A/\mathfrak{a} := A/\sim$  und  $\pi(x) := [x]$ . Die Addition und Multiplikation auf  $A$  ind. die Addition bzw. Multiplikation auf  $A/\mathfrak{a}$ .

**Def.**  $A/\mathfrak{a}$  heißt **Quotientenring** von  $A$  nach  $\mathfrak{a}$ .

**Notation.** Man lässt häufig die Äquivalenzklammern weg, man schreibt also „ $x = y$  in  $A/\mathfrak{a}$ “ anstatt „ $[x] = [y]$ “.

**Prop.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Folgende Korresp. ist bij. und monoton:

$$\begin{array}{ccc} \{ \text{Ideale } \mathfrak{b} \subseteq A \text{ mit } \mathfrak{b} \supseteq \mathfrak{a} \} & \leftrightarrow & \{ \text{Ideale } \mathfrak{c} \subseteq A/\mathfrak{a} \} \\ \mathfrak{b} & \mapsto & \pi(\mathfrak{b}) \\ \pi^{-1}(\mathfrak{c}) & \leftarrow & \mathfrak{c} \end{array}$$

**Prop (Homomorphiesatz).** Sei  $\phi : A \rightarrow B$  ein Ringhomom. Dann ist  $\tilde{\phi} : A/\ker(\phi) \rightarrow \text{im}(\phi)$ ,  $[x] \mapsto \phi(x)$  ein Ringisomorphismus.

Im Folgenden seien alle Ringe **kommutativ**, d. h.  $xy = yx$  f. a.  $x, y$ .

**Def.** Sei  $A$  ein kommutativer Ring. Ein Element  $x \in A$  heißt

- **regulär**, falls  $\forall y \in A : xy = 0 \implies y = 0$ .
- **Nullteiler**, falls es nicht regulär ist, d. h. wenn ein  $y \in A \setminus \{0\}$  mit  $xy = 0$  existiert.

**Def.** Ein Ring  $A$  heißt **Integritätsbereich**, wenn  $0 \in A$  der einzige Nullteiler in  $A$  ist.

**Achtung.** Die Null im Nullring ist regulär!

*Bem.* Ein Ring  $A$  ist genau dann ein Integritätsbereich, wenn

$$0 \neq 1 \text{ in } A \quad \text{und} \quad \forall x, y \in A : xy = 0 \implies x = 0 \vee y = 0.$$

**Bsob.** Sei  $\phi : A \rightarrow B$  ein injektiver Ringhomomorphismus. Ist  $B$  ein Integritätsbereich, so auch  $A$ .

**Def.** Ein Ideal  $\mathfrak{a} \subseteq A$  heißt **Hauptideal**, falls  $\mathfrak{a} = (a)$  für ein  $a \in A$ . Ein Ring  $A$  heißt **Hauptidealbereich**, falls jedes Ideal in  $A$  ein Hauptideal ist.

**Bspe.** •  $\mathbb{Z}$ , •  $K[x]$

**Gegenbsp.** •  $K[x_1, \dots, x_n]$  für  $n \geq 2$

**Def.** Ein Element  $x \in A$  heißt **nilpotent**, falls  $\exists n \geq 0 : x^n = 0$ .

**Bsob.** Ist  $A$  ein Integritätsbereich, so ist  $0 \in A$  das einzige nilpotente Element in  $A$ .

**Def.** Sei  $A$  ein Ring, nicht notwendigerweise kommutativ. Ein Element  $x \in A$  heißt **Einheit**, falls ein  $y \in A$  mit  $xy = yx = 1$  existiert.  $A^\times := \{ \text{Einheiten in } A \}$  heißt **Einheitengruppe**. Der Ring  $A$  heißt **Schiefkörper**, falls  $0$  die einzige Nicht-Einheit ist. Falls zusätzlich  $A$  kommutativ ist, so heißt  $A$  ein **Körper**.

**Bsob.** •  $x \in A$  ist eine Einheit  $\iff (x) = (1) \iff A/(x) = 0$   
• Einheiten sind regulär.

**Prop.** Sei  $A$  ein kommutativer Ring. Dann sind äquivalent:

- $A$  ist ein Körper.
- $A$  besitzt genau zwei Ideale (nämlich  $(0)$  und  $(1)$ ).
- Ein Ringhomomorphismus  $A \rightarrow B$  ist genau dann injektiv, wenn  $B$  nicht der Nullring ist.

**Def.** • Ein Ideal  $\mathfrak{p} \subset A$  heißt **Primideal**, falls  $1 \notin \mathfrak{p}$  und  $\forall a, b \in A : ab \in \mathfrak{p} \implies a \in \mathfrak{p} \vee b \in \mathfrak{p}$ .

• Ein Ideal  $\mathfrak{m} \subset A$  heißt **maximal**, falls für jedes Ideal  $\mathfrak{p} \subseteq \mathfrak{a} \subseteq A$  entweder  $\mathfrak{p} = \mathfrak{a}$  oder  $\mathfrak{a} = A$  (nicht beides!) gilt.

**Bspe.** • Jedes Ideal in  $\mathbb{Z}$  hat die Form  $(m)$  mit  $m \in \mathbb{N}$ . Das Ideal  $(m)$  ist genau dann prim, wenn  $m = 0$  oder  $m$  eine Primzahl ist.  
• Sei  $f \in K[x_1, \dots, x_n]$  ein irred. Polynom. Dann ist  $(f)$  prim.

**Lem.**  $\mathfrak{p} \subseteq A$  ist prim  $\iff A/\mathfrak{p}$  ist ein Integritätsbereich  
 $\mathfrak{m} \subseteq A$  ist maximal  $\iff A/\mathfrak{m}$  ist ein Körper

**Kor.** Maximale Ideale sind prim.

**Prop.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Folgende Korresp. ist bij. und monoton:

$$\begin{array}{ccc} \{ \text{Primideale } \mathfrak{p} \subset A \text{ mit } \mathfrak{p} \supseteq \mathfrak{a} \} & \leftrightarrow & \{ \text{Primideale } \mathfrak{q} \subset A/\mathfrak{a} \} \\ \mathfrak{p} & \mapsto & \pi(\mathfrak{p}) \\ \pi^{-1}(\mathfrak{q}) & \leftarrow & \mathfrak{q} \end{array}$$

Genauso bekommt man eine bijektive, monotone Korrespondenz

$$\{ \text{max. Ideale } \mathfrak{m} \subset A \text{ mit } \mathfrak{m} \supseteq \mathfrak{a} \} \leftrightarrow \{ \text{max. Ideale } \mathfrak{n} \subset A/\mathfrak{a} \}$$

**Prop.** Ein Ring besitzt genau dann ein maximales Ideal, wenn er nicht der Nullring ist.

**Kor.** • Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Dann gibt es genau dann ein maximales Ideal  $\mathfrak{p} \subset A$  mit  $\mathfrak{p} \supseteq \mathfrak{a}$ , wenn  $\mathfrak{a} \neq (1)$ .

• Ein Element  $x \in A$  liegt genau dann in einem maximalen Ideal von  $A$ , wenn  $x$  keine Einheit ist.

**Def.** Ein **lokaler Ring** ist ein komm. Ring  $A$  mit genau einem max. Ideal  $\mathfrak{m}$ . Der Körper  $F := A/\mathfrak{m}$  heißt **Restklassenkörper** von  $A$ .

**Notation.** Man schreibt „Sei  $(A, \mathfrak{m}, F)$  ein lokaler Ring.“

**Def.** Ein **halblokaler Ring** ist ein kommutativer Ring mit nur endlich vielen maximalen Idealen.

**Lem.** Sei  $\mathfrak{m} \subset A$  ein Ideal mit  $A \setminus \mathfrak{m} = A^\times$ . Dann ist  $(A, \mathfrak{m})$  ein lokaler Ring.

**Prop.** Sei  $\mathfrak{m} \subset A$  ein maximales Ideal, sodass  $1 + x$  für alle  $x \in \mathfrak{m}$  eine Einheit ist. Dann ist  $A \setminus \mathfrak{m} = A^\times$ , also  $(A, \mathfrak{m})$  ein lokaler Ring.

**Prop.** Die Menge  $\mathfrak{n} := \{ \text{nilpotente Elemente} \} \subseteq A$  ist ein Ideal, das sogenannte **Nilradikal**.

*Bem.* Der Ring  $A/\mathfrak{n}$  hat außer  $0$  keine nilpotenten Elemente.

**Prop.** Das Nilradikal eines kommutativen Ringes ist der Schnitt aller seiner Primideale.

**Def.** Das **Jacobsonsche Ideal**  $\mathfrak{j} \subset A$  ist der Schnitt aller maximalen Ideale von  $A$ .

**Prop.** Ein Element  $x \in A$  liegt genau dann im Jacobsonischen Ideal  $\mathfrak{j}$ , wenn  $1 - xy$  für alle  $y \in A$  eine Einheit ist.

**Def.** Die **Summe von Idealen**  $(\mathfrak{a}_i)_{i \in I}$  von  $A$  ist das Ideal

$$\sum_{i \in I} \mathfrak{a}_i := \left\{ \sum_{k=1}^n x_k \mid k \in \mathbb{N}, x_k \in \mathfrak{a}_{i_k}, i_k \in I \right\}.$$

*Bem.*  $\sum_{i \in I} \mathfrak{a}_i$  ist das kleinste Ideal, das alle  $\mathfrak{a}_i$  umfasst.

**Beob.**  $(x_1) + \dots + (x_n) = (x_1, \dots, x_n)$

*Bem.* Ideale eines Ringes  $A$  bilden mit Schnitt und Summe einen vollständigen Verband bezüglich der Inklusionsordnung.

**Def.** Das **Produkt zweier Ideale**  $\mathfrak{a}, \mathfrak{b} \subseteq A$  ist

$$\mathfrak{a}\mathfrak{b} := \text{von } \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \text{ erzeugtes Ideal.}$$

**Beob.**  $\bullet \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}, \quad \bullet (x_1) \cdot \dots \cdot (x_n) = (x_1 \cdot \dots \cdot x_n)$

**Bsp.** In  $A = \mathbb{Z}$  gilt für  $m, n \in \mathbb{N}$   
 $\bullet (m) + (n) = (m, n) = (\text{ggT}(m, n)), \quad \bullet (m) \cap (n) = (\text{kgV}(m, n)).$

**Beob.**  $\bullet$  Summe, Schnitt und Produkt von Idealen sind assoziativ.  
 $\bullet$  Summe und Schnitt sind kommutativ. Das Produkt von Idealen ist kommutativ, wenn der Ring kommutativ ist.  
 $\bullet$  Distributivgesetz:  $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$   
 $\bullet$  Modularitätsgesetz: Ist  $\mathfrak{a} \supseteq \mathfrak{b}$  oder  $\mathfrak{a} \supseteq \mathfrak{c}$ , so folgt

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}).$$

**Def.** Zwei Ideale  $\mathfrak{a}, \mathfrak{b} \subseteq A$  heißen **koprim**, falls  $\mathfrak{a} + \mathfrak{b} = (1)$ .

**Bsp.** In  $A = \mathbb{Z}$  gilt:  $(m), (n)$  sind koprim  $\iff \text{ggT}(m, n) = 1$

**Prop.** Seien  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$  paarweise kopprime Ideale. Dann gilt

$$\bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i.$$

**Def.** Das **direkte Produkt** einer Familie  $(A_i)_{i \in I}$  von Ringen ist der Ring  $\prod_{i \in I} A_i := \{(a_i \in A_i)_{i \in I}\}$  mit kmpnntnwsr Verknüpfung.

*Bem.* Das direkte Produkt ist das kategorienth. Produkt in **Ring**.

**Prop.** Seien  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$  Ideale. Dann ist

$$\phi : A \rightarrow \prod_{i=1}^n (A/\mathfrak{a}_i), \quad x \mapsto ([x], \dots, [x])$$

genau dann surjektiv, wenn die Ideale  $\mathfrak{a}_i$  paarweise koprim sind.

*Bem.* Der Ringhomomor.  $\phi$  ist genau dann injektiv, wenn  $\bigcap_{i=1}^n \mathfrak{a}_i = 0$ .

**Prop.** Seien  $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$  Primideale und  $\mathfrak{a} \subseteq A$  ein Ideal.

Gilt  $\mathfrak{a} \subseteq \bigcap_{i=1}^n \mathfrak{p}_i$ , so gibt es ein  $j \in \{1, \dots, n\}$  mit  $\mathfrak{a} \subseteq \mathfrak{p}_j$ .

**Prop.** Seien  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$  Ideale und  $\mathfrak{p} \subset A$  ein Primideal.

Gilt  $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i$ , so gibt es ein  $j \in \{1, \dots, n\}$  mit  $\mathfrak{p} \supseteq \mathfrak{a}_j$ .

**Def.** Seien  $\mathfrak{a}, \mathfrak{b} \subseteq A$  zwei Ideale. Der **Idealquotient** von  $\mathfrak{a}$  nach  $\mathfrak{b}$  ist das Ideal  $(\mathfrak{a} : \mathfrak{b}) := \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$ .

**Notation.**  $\bullet (x : \mathfrak{b}) := ((x) : \mathfrak{b}), \quad \bullet (\mathfrak{a} : y) := (\mathfrak{a} : (y))$

**Def.** Der **Annulator** eines Ideals  $\mathfrak{b} \subseteq A$  ist  $\text{ann}(\mathfrak{b}) := (0 : \mathfrak{b})$ .

**Lem.**  $\bullet \mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b}) \quad \bullet (\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a} \quad \bullet ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$   
 $\bullet (\bigcap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i \in I} (\mathfrak{a}_i : \mathfrak{b}) \quad \bullet (\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i) = \bigcap_{i \in I} (\mathfrak{a} : \mathfrak{b}_i)$

**Def.** Das **Wurzelideal** eines Ideals  $\mathfrak{a} \subseteq A$  ist das Ideal

$$\sqrt{\mathfrak{a}} := \{x \in A \mid \exists n \in \mathbb{N} : x^n \in \mathfrak{a}\}.$$

*Bem.* Das Nilradikal ist  $\sqrt{(0)}$ , das Wurzelideal des Nullideals.  
 Es gilt  $\sqrt{\mathfrak{a}} = \pi^{-1}(\sqrt{(0)})$  mit  $\pi : A \rightarrow A/\mathfrak{a}, x \mapsto [x]$ .

**Lem.**  $\bullet \sqrt{\mathfrak{a}} \supseteq \mathfrak{a} \quad \bullet \sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$  für  $n \geq 1 \quad \bullet \sqrt{\mathfrak{a}} = (1) \iff \mathfrak{a} = (1)$   
 $\bullet \sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}} \quad \bullet \sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} \quad \bullet \sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$

**Def.** Ein Ideal  $\mathfrak{a} \subseteq A$  heißt **Wurzelideal**, falls  $\mathfrak{a} = \sqrt{\mathfrak{a}}$ .

**Prop.** Das Wurzelideal von  $\sqrt{\mathfrak{a}}$  ist der Schnitt aller Primideale von  $A$ , die  $\mathfrak{a}$  enthalten.

**Prop.**  $\{ \text{Nullteiler von } A \} = \bigcup_{x \in A \setminus \{0\}} \sqrt{\text{ann}(x)}$

**Lem.**  $\sqrt{\mathfrak{a}}$  und  $\sqrt{\mathfrak{b}}$  koprim  $\implies \mathfrak{a}$  und  $\mathfrak{b}$  koprim

**Def.** Sei  $\phi : A \rightarrow B$  ein Homomorphismus komm. Ringe.  
 Die **Kontraktion** von  $\mathfrak{b} \subseteq B$  (bzgl.  $\phi$ ) ist das Ideal  $A \cap \mathfrak{b} := \phi^{-1}(\mathfrak{b})$ .

*Bem.* Es wird also  $\phi$  in der Notation unterdrückt. Falls  $\phi$  die Inklusion eines Unterrings ist, so ist  $A \cap \mathfrak{b}$  wörtlich zu verstehen.

**Beob.**  $A \cap \mathfrak{b} = \ker(A \rightarrow B \rightarrow B/\mathfrak{b})$

**Lem.** Ist  $\mathfrak{q} \subset B$  ein Primideal, so auch  $A \cap \mathfrak{q} \subset A$ .

**Achtung.** Die Kontraktion max. Ideale ist i. A. nicht maximal!

**Def.** Sei  $\phi : A \rightarrow B$  ein Homomorphismus komm. Ringe.  
 Die **Erweiterung** von  $\mathfrak{a} \subseteq A$  (bzgl.  $\phi$ ) ist das Ideal  $B\mathfrak{a} := (\phi(\mathfrak{a}))$ , das von  $\phi(\mathfrak{a})$  erzeugte Ideal.

*Bem.* Ist  $\phi$  die Inklusion eines Unterrings, so ist  $B\mathfrak{a}$  tatsächlich die Menge der  $B$ -Linearkombinationen von Elementen in  $\mathfrak{a}$ .

*Bem.* Die Erweiterung eines Primideals ist i. A. nicht mehr prim.

**Prop.** Sei  $\phi : A \rightarrow B$  ein Homomorphismus komm. Ringe.  
 Die Erweiterung und Kontraktion von Idealen (bzgl.  $\phi$ ) bilden eine Galois-Verbindung, d. h. für Ideale  $\mathfrak{a} \subseteq A$  und  $\mathfrak{b} \subseteq B$  gilt

$$B\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a} \subseteq A \cap \mathfrak{b}.$$

Äquivalent dazu sind Erw. und Kontraktion monoton und es gelten

$$\mathfrak{a} \subseteq A \cap (B\mathfrak{a}) \quad \text{und} \quad \mathfrak{b} \supseteq B(A \cap \mathfrak{b}).$$

Außerdem folgt aus den Eigenschaften einer Galois-Verbindung, dass

$$B\mathfrak{a} = B(A \cap (B\mathfrak{a})) \quad \text{und} \quad A \cap \mathfrak{b} = A \cap (B(A \cap \mathfrak{b})).$$

Damit induzieren Erweiterung und Kontraktion eine bijektive ordnungserhaltende Korrespondenz zwischen den kontrahierten Idealen von  $A$  und den erweiterten Idealen von  $B$ .

**Lem.** Für Ideale  $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2 \subseteq A$  und  $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2 \subseteq B$  gilt

- $\bullet B\sqrt{\mathfrak{a}} \subseteq \sqrt{B\mathfrak{a}}$
- $\bullet B(\mathfrak{a}_1 + \mathfrak{a}_2) = B\mathfrak{a}_1 + B\mathfrak{a}_2$
- $\bullet B(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subseteq B\mathfrak{a}_1 \cap B\mathfrak{a}_2$
- $\bullet B(\mathfrak{a}_1 \mathfrak{a}_2) = (B\mathfrak{a}_1)(B\mathfrak{a}_2)$
- $\bullet B(\mathfrak{a}_1 : \mathfrak{a}_2) \subseteq (B\mathfrak{a}_1 : B\mathfrak{a}_2)$
- $\bullet A \cap \sqrt{\mathfrak{b}} = \sqrt{A \cap \mathfrak{b}}$
- $\bullet A \cap (\mathfrak{b}_1 + \mathfrak{b}_2) \supseteq A \cap \mathfrak{b}_1 + A \cap \mathfrak{b}_2$
- $\bullet A \cap (\mathfrak{b}_1 \cap \mathfrak{b}_2) = (A \cap \mathfrak{b}_1) \cap (A \cap \mathfrak{b}_2)$
- $\bullet A \cap (\mathfrak{b}_1 \mathfrak{b}_2) \supseteq (A \cap \mathfrak{b}_1)(A \cap \mathfrak{b}_2)$
- $\bullet A \cap (\mathfrak{b}_1 : \mathfrak{b}_2) \subseteq (A \cap \mathfrak{b}_1 : A \cap \mathfrak{b}_2)$

# Moduln

**Def.** Sei  $A$  ein Ring. Ein **A-(Links-)Modul** ist eine abelsche Gruppe  $(M, +, 0)$  zusammen mit einer Abb.  $\cdot : A \times M \rightarrow M$ , sodass

- die Multiplikation eine Operation von  $(A, \cdot, 1)$  auf  $M$  ist, d. h.  $(ab)x = a(bx)$  und  $1 \cdot x = x$  für alle  $a, b \in A$  und  $x \in M$ .
- die Multiplikation distributiv über die Addition ist, d. h.  $a(x + y) = ax + ay$  und  $(a + b)x = ax + bx$  f. a.  $a, b \in A, x, y \in M$ .

**Achtung.** Es heißt *der* Modul, nicht *das* Modul!

**Bspe.** • Der Ring  $A$  ist selbst ein  $A$ -Modul.

- Jedes Ideal  $\mathfrak{a} \subseteq A$  ist (durch Einschränkung der Multiplikation) ein  $A$ -Modul.
- Ein  $K$ -Modul ( $K$  ein Körper) ist dasselbe wie ein  $K$ -VR.
- Ein  $\mathbb{Z}$ -Modul ist dasselbe wie eine abelsche Gruppe.
- Ein  $K[x]$ -Modul ist dasselbe wie ein  $K$ -Vektorraum  $V$  zusammen mit einem Endomorphismus  $V \rightarrow V$ .
- Sei  $G$  eine endliche Gruppe und

$$A := K[G] := \left\{ \sum_{g \in G} a_g \cdot g \mid g \in G, a_g \in K \right\}$$

die **Gruppenalgebra** von  $G$  über  $K$ . Ein  $A$ -Modul ist dasselbe wie ein  $K$ -VR  $V$  mit einer linearen Darstellung  $G \rightarrow \text{End}_K(V)$ .

**Def.** Ein  $A$ -Modulhomomorphismus ist eine Abbildung  $\phi : M \rightarrow N$  zwischen  $A$ -Moduln  $M$  und  $N$ , welche ein Gruppenhomomorphismus  $(M, +_M, 0_M) \rightarrow (N, +_N, 0_N)$  und verträglich mit der Wirkung des multiplikativen Monoids von  $M$  und  $N$  ist, d. h.  $\phi(ax) = a\phi(x)$  für alle  $a \in A$  und  $x \in M$ .

**Bem.**  $A$ -Moduln und  $A$ -Modulhomom. bilden eine Kat.  **$A$ -Mod.**

**Lem.** Ein  $A$ -Modulhomomorphismus ist genau dann ein Isomorphismus (in dieser Kategorie), wenn er bijektiv ist.

**Def.** Sei  $M$  ein  $A$ -Modul. Eine Teilmenge  $M' \subseteq M$  heißt **Untermodul** von  $M$ , falls

- $M'$  eine Untergruppe von  $(M, +, 0)$  ist und
- $M'$  abgeschlossen unter Multiplikation mit Elementen aus  $A$  ist, d. h.  $ax \in M'$  für alle  $a \in A$  und  $x \in M'$ .

**Bsp.** Sei  $A$  kommutativ. Eine Teilmenge  $\mathfrak{a} \subseteq A$  ist genau dann ein Ideal von  $A$ , wenn  $\mathfrak{a}$  ein Untermodul von  $A$  ist.

**Def.** Sei  $\phi : M \rightarrow N$  eine  $A$ -Modulhomomorphismus. Der **Kern** v.  $\phi$  ist der Untermodul  $\ker \phi := \{x \in M \mid \phi(x) = 0\} \subseteq M$ . Das **Bild** von  $\phi$  ist der Untermodul  $\text{im } \phi := \phi(M) \subseteq N$ .

**Prop.** Sei  $M$  ein  $A$ -Modul und  $M' \subseteq M$  ein Untermodul. Dann gibt es ein  $A$ -Modul  $M/M'$  und einen Ringhomom.  $\pi : M \rightarrow M/M'$  mit folgender universeller Eigenschaft:

Für jeden  $A$ -Modul  $N$  und  $A$ -Modulhomom.  $\psi : M \rightarrow N$  mit  $M' \subseteq \ker \psi$  gibt es genau einen  $A$ -Modulhomom.  $\tilde{\psi} : M/M' \rightarrow N$  mit  $\psi = \tilde{\psi} \circ \pi$ .

**Konstr.**  $M/M' := M/\sim$  mit  $x \sim y : \iff x - y \in M'$

**Def.** Der Modul  $M/M'$  heißt **Quotientenmodul** von  $M$  nach  $M'$ .

**Prop.** Sei  $M$  ein  $A$ -Modul und  $M' \subseteq M$  ein Untermodul. Folgende Korrespondenz ist bijektiv und monoton:

$$\begin{aligned} \{ \text{Untermoduln } M' \subseteq N \subseteq M \} &\leftrightarrow \{ \text{Untermoduln } \overline{N} \subseteq M/M' \} \\ N &\mapsto \pi(N) \\ \pi^{-1}(\overline{N}) &\leftarrow \overline{N} \end{aligned}$$

**Def.** Der **Kokern** eines  $A$ -Modulhomomorphismus  $\phi : M \rightarrow N$  ist

$$\text{coker } \phi := N / \text{im}(\phi).$$

**Bem.** •  $\phi$  injektiv  $\iff \ker \phi = 0$  •  $\phi$  surjektiv  $\iff \text{coker } \phi = 0$

**Prop (Homomorphiesatz).** Sei  $\phi : M \rightarrow N$  ein  $A$ -Modulhomom. Dann ist  $\underline{\phi} : M / \ker(\phi) \rightarrow \text{im}(\phi), [x] \mapsto \phi(x)$  ein  $A$ -Modulisomor.

**Def.** Sei  $M$  ein  $A$ -Modul. Die **Summe** einer Familie  $(M_i)_{i \in I}$  von Untermoduln von  $M$  ist

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in I} x_i \mid x_i \in M_i \right\}$$

(Dabei ist  $\sum_{i \in I} x_i$  endlich, d. h.  $x_i = 0$  für alle bis auf endl. viele  $i \in I$ .)

**Prop.** Sei  $(M_i)_{i \in I}$  eine Familie von Untermoduln von  $M$ . Dann ist auch der Schnitt  $\bigcap_{i \in I} M_i$  ein Untermodul von  $M$ .

**Bem.** Untermoduln eines Moduls  $M$  bilden mit Schnitt und Summe einen vollständigen Verband bezüglich der Inklusionsordnung.

**Prop (Isomorphiesätze).** Sei  $A$  ein Ring.

1. Sei  $M$  ein  $A$ -Modul und  $M_1, M_2 \subseteq M$  zwei Untermoduln. Dann existiert ein kanonischer  $A$ -Modulisomorphismus

$$(M_1 + M_2) / M_1 \cong M_2 / (M_1 \cap M_2).$$

2. Sei  $L$  ein  $A$ -Modul und  $N \subseteq M \subseteq L$  Untermoduln. Dann existiert ein kanonischer  $A$ -Modulisomorphismus

$$(L/N) / (M/N) \cong L/M.$$

**Def.** Sei  $A$  kommutativ,  $M$  ein  $A$ -Modul und  $\mathfrak{a} \subseteq A$  ein Ideal. Das **Produkt** von  $\mathfrak{a}$  und  $M$  ist  $\mathfrak{a}M := \{ax \mid a \in \mathfrak{a}, x \in M\}$ .

**Notation.**  $\mathfrak{a}M := (a)M = \{ax \mid x \in M\}$  für  $a \in A$

**Def.** Sei  $A$  komm. und  $N, P$  Untermoduln eines  $A$ -Moduls  $M$ . Das Ideal  $(N : P) := \{a \in A \mid aP \subseteq N\} \subseteq A$  heißt **Quotient** von  $N$  nach  $P$ .

**Def.** Das Ideal  $\text{ann } M := (0 : M)$  heißt **Annulator** von  $M$ .

**Bem.** Ist  $\mathfrak{a} \subseteq A$  ein Ideal mit  $\mathfrak{a} \subseteq \text{ann } M$ , so können wir  $M$  auch als  $A/\mathfrak{a}$ -Modul auffassen.

**Def.** Der  $A$ -Modul  $M$  heißt **treu**, falls  $\text{ann } M = 0$ .

**Lem.** Sei  $A$  kommutativ,  $N, P \subseteq M$  Untermoduln. Dann gilt

- $\text{ann}(N + P) = \text{ann}(N) + \text{ann}(P)$  •  $(N : P) = \text{ann}((N + P)/N)$

**Def.** Sei  $M$  ein  $A$ -Modul,  $X \subseteq M$  eine Teilmenge.

Der von  $X$  **erzeugte Untermodul** ist

$$L(X) := \sum_{x \in X} Ax = \sum_{x \in X} \{ax \mid a \in A\} = \left\{ \sum_{x \in X} \lambda_x x \mid \lambda_x \in A \right\}.$$

**Def.** Eine Teilmenge  $X \subseteq M$  heißt **Erzeugendensystem**, falls  $L(X) = M$ . Ein  $A$ -Modul  $M$  heißt **endlich erzeugt**, falls ein endliches Erzeugendensystem von  $M$  existiert.

**Bem.** Ein  $A$ -Modul  $M$  ist genau dann endlich erzeugt, wenn ein  $n \in \mathbb{N}$  und ein surj.  $A$ -Modulhomomorphismus  $\phi : A^n \rightarrow M$  existiert.

**Def.** Das **direkte Produkt** einer Familie  $(M_i)_{i \in I}$  von  $A$ -Moduln ist das  $A$ -Modul  $\prod_{i \in I} M_i := \{(x_i \in M_i)_{i \in I}\}$  mit kmpntnswr Verkn.

**Bem.** Das direkte Produkt ist das kategorienth. Produkt in  **$A$ -Mod.**

**Def.** Die **direkte Summe** einer Familie  $(M_i)_{i \in I}$  von  $A$ -Moduln ist

$$\begin{aligned} \bigoplus_{i \in I} M_i &:= \{(x_i \in M_i)_{i \in I} \mid x_i = 0 \text{ für alle bis auf endl. viele } i \in I\} \\ &\subseteq \prod_{i \in I} M_i. \end{aligned}$$

**Bem.** Die dir. Summe ist das kategorienth. Koprodukt in  **$A$ -Mod.** Ist  $I$  endlich, so gilt  $\bigoplus_{i \in I} M_i \cong \prod_{i \in I} M_i$ .

**Bsp** (Direkte Summenzerlegung). Sei  $A = \sum_{i=1}^n A_i$  ein endl. direktes Produkt komm. Ringe. Dann gilt  $A \cong \mathfrak{a}_1 \oplus \dots \oplus \mathfrak{a}_n$  als  $A$ -Modul mit  $\mathfrak{a}_i := \{(x_i)_{i=1}^n \mid x_j = 0 \text{ für } j \neq i\}$ .

**Def.** Ein  **$A$ -Modul**  $M$  heißt frei, falls eine Menge  $I$  existiert, sodass  $M \cong \bigoplus_{i \in I} A$  als  $A$ -Modul.

**Bem.** Ein endlicher freier Modul ist ein Modul, der zu  $A^n := A \oplus \dots \oplus A$  für ein  $n \in \mathbb{N}$  isomorph ist.

**Prop.** Sei  $A$  ein Ring. Ein  $A$ -Modul  $M$  ist genau dann endl. erzeugt, wenn  $M$  der Quotient eines  $A$ -Moduls der Form  $A^n$  für ein  $n \in \mathbb{N}$  ist.

**Prop.** Sei  $A$  ein komm. Ring,  $M$  ein endlich erzeugter  $A$ -Modul und  $\mathfrak{a} \subseteq A$  ein Ideal. Sei  $\phi \in \text{End}_A(M)$  mit  $\text{im } \phi \subseteq \mathfrak{a}M$ . Dann erfüllt  $\phi$  eine Gleichung der Form  $\phi^n + a_1 \phi^{n-1} + \dots + a_n = 0$  mit  $a_i \in \mathfrak{a}$ .

**Kor.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal und  $M$  ein  $A$ -Modul mit  $\mathfrak{a}M = M$ . Dann existiert ein  $x \in A$  mit  $x = 1$  modulo  $\mathfrak{a}$  und  $xM = 0$ .

**Lem (Nakayama).** Sei  $\mathfrak{a}$  ein Ideal von  $A$ , welches im Jacobsonschen Radikal  $\mathfrak{j}$  von  $A$  enthalten ist. Dann folgt aus  $\mathfrak{a}M = M$  schon  $M = 0$ .

**Kor.** Sei  $N \subseteq M$  ein Untermodul und  $\mathfrak{a} \subseteq A$  ein Ideal, welches im Jacobsonschen Ideal  $\mathfrak{j}$  enthalten ist. Dann folgt aus  $M = \mathfrak{a}M + N$  schon  $M = N$ .

**Def.** Sei  $(A, \mathfrak{m}, F)$  ein lokaler Ring. Sei  $M$  ein endlich erz.  $A$ -Modul. Setze  $M(\mathfrak{m}) := M/\mathfrak{m}M$ . Wegen  $\mathfrak{m} \subseteq \text{ann}(M(\mathfrak{m}))$  ist  $M(\mathfrak{m})$  in natürl. Art ein (endlich-dim.)  $F$ -Vektorraum, die **spezielle Faser** von  $M$ . Das Bild eines Elements  $x \in M$  in  $M(\mathfrak{m})$  wird **Wert des Schnittes**  $x$  in der speziellen Faser genannt.

**Prop.** Sei  $(A, \mathfrak{m}, F)$  ein lokaler Ring,  $M$  ein endlich erz.  $A$ -Modul. Seien  $x_1, \dots, x_n$  Schnitte von  $M$ , deren Werte in  $M(\mathfrak{m})$  eine Basis bilden. Dann erzeugen  $x_1, \dots, x_n$  den  $A$ -Modul  $M$ .

## Exakte Sequenzen

**Def.** Sei  $A$  ein Ring. Eine Sequenz

$$\dots \rightarrow M^{i-1} \xrightarrow{\phi^{i-1}} M^i \xrightarrow{\phi^i} M^{i+1} \rightarrow \dots$$

von  $A$ -Moduln und  $A$ -Modulhomomorphismen heißt **exakt** bei  $M^i$ , falls im  $\phi^{i-1} = \ker \phi^i$ . Die Sequenz heißt **exakt**, falls sie exakt bei jedem  $M^i$  ist.

**Bsp.** Sei  $\phi : M \rightarrow N$  ein  $A$ -Modulhomomorphismus. Dann gilt

$$\begin{aligned} \phi \text{ ist injektiv} &\iff 0 \rightarrow M \xrightarrow{\phi} N \text{ ist exakt} \\ \phi \text{ ist surjektiv} &\iff M \xrightarrow{\phi} N \rightarrow 0 \text{ ist exakt} \end{aligned}$$

**Def.** Eine **kurze exakte Sequenz** k. e. S. von  $A$ -Moduln ist eine exakte Sequenz der Form  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ .

*Bem.* Jede lange exakte Sequenz  $\dots \rightarrow M^{i-1} \rightarrow M^i \rightarrow M^{i+1} \rightarrow \dots$  zerfällt in kurze exakte Sequenzen: Mit  $N^i = \operatorname{im} \phi^{i-1} = \ker \phi^i$  haben wir kurze exakte Sequenzen  $0 \rightarrow N^i \rightarrow M^i \rightarrow N^{i+1} \rightarrow 0$ . Andersherum kann man solche kurzen exakten Sequenzen zu einer langen exakten Sequenz zusammenkleben.

**Lem.** Sei  $A$  ein komm. Ring. Eine Seq.  $E : M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \rightarrow 0$  ist genau dann exakt, wenn für alle  $A$ -Moduln  $N$  die Sequenz

$$\operatorname{Hom}(E, N) : 0 \rightarrow \operatorname{Hom}(M'', N) \xrightarrow{\psi^*} \operatorname{Hom}(M, N) \xrightarrow{\phi^*} \operatorname{Hom}(M', N).$$

exakt ist.

**Lem.** Sei  $A$  ein kommutativer Ring.

- Eine Sequenz  $E : M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \rightarrow 0$  ist genau dann exakt, wenn für alle  $A$ -Moduln  $N$  folgende induzierte Sequenz exakt ist:

$$\operatorname{Hom}(E, N) : 0 \rightarrow \operatorname{Hom}(M'', N) \xrightarrow{\psi^*} \operatorname{Hom}(M, N) \xrightarrow{\phi^*} \operatorname{Hom}(M', N).$$

- Eine Sequenz  $F : 0 \rightarrow N' \xrightarrow{\phi} N \xrightarrow{\psi} N''$  ist genau dann exakt, wenn für alle  $A$ -Moduln  $M$  folgende induzierte Sequenz exakt ist:

$$\operatorname{Hom}(M, F) : \operatorname{Hom}(M, N') \xrightarrow{\phi_*} \operatorname{Hom}(M, N) \xrightarrow{\psi_*} \operatorname{Hom}(M, N'') \rightarrow 0.$$

**Lem (Schlangenlemma).** Sei  $A$  ein Ring. Sei folgendes komm. Diagramm von  $A$ -Moduln mit exakten Zeilen gegeben:

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

Dann gibt es einen Verbindungshomomorphismus  $\delta : \ker \phi'' \rightarrow \operatorname{coker} \phi'$ , mit dem folgende Sequenz exakt ist:

$$\ker \phi' \rightarrow \ker \phi \rightarrow \ker \phi'' \xrightarrow{\delta} \operatorname{coker} \phi' \rightarrow \operatorname{coker} \phi \rightarrow \operatorname{coker} \phi''.$$

**Def.** Sei  $A$  ein Ring und  $\mathfrak{C}$  eine Klasse von  $A$ -Moduln. Eine Abb.  $\lambda : \mathfrak{C} \rightarrow G$  in eine ab. Gruppe heißt **additive Funktion**, falls für alle kurzen exakten Seq.  $0 \rightarrow C' \rightarrow C \rightarrow C'' \rightarrow 0$  von Moduln aus  $\mathfrak{C}$  gilt, dass  $\lambda(C) = \lambda(C') + \lambda(C'')$ .

**Bsp.** Sei  $K$  ein Körper und  $\mathfrak{C}$  die Klasse der endlich-dim. VR über  $K$ . Dann ist  $\dim : \mathfrak{C} \rightarrow \mathbb{Z}$  eine additive Funktion.

**Prop.** Sei  $A$  ein Ring,  $\mathfrak{C}$  eine Klasse von  $A$ -Moduln und  $\lambda : \mathfrak{C} \rightarrow G$  eine additive Funktion. Sei

$$0 \rightarrow M^0 \xrightarrow{\phi^0} M^1 \rightarrow \dots \rightarrow M^{n-1} \xrightarrow{\phi^{n-1}} M^n \rightarrow 0$$

eine exakte Sequenz von Moduln in  $\mathfrak{C}$ , sodass auch die Kerne der  $\phi^i$  in  $\mathfrak{C}$  liegen. Dann gilt  $\sum_{i=0}^n (-1)^i \lambda(M^i) = 0$ .

## Tensorprodukt

**Def.** Seien  $M, N$  und  $P$  drei  $A$ -Moduln. Eine Abbildung  $\beta : M \times N \rightarrow P$  heißt **A-bilinear**, falls für alle  $x \in M$  die Abbildung  $\beta(x, -)$  und für alle  $y \in N$  die Abbildung  $\beta(-, y)$  ein  $A$ -Modulhomomorphismus ist.

**Bsp.** Die Multiplikation  $\cdot : A \times A \rightarrow A$  ist  $A$ -bilinear.

**Prop.** Seien  $M$  und  $N$  zwei  $A$ -Moduln. Dann existiert ein  $A$ -Modul  $M \otimes_A N$  und eine bilineare Abbildung  $\gamma : M \times N \rightarrow M \otimes_A N$  mit folgender universellen Eigenschaft:

Für jeden  $A$ -Modul  $P$  und für jede bilineare Abbildung  $\beta : M \times N \rightarrow P$  gibt es genau einen  $A$ -Modulhomomorphismus  $\underline{\beta} : M \otimes_A N \rightarrow P$  mit  $\beta = \underline{\beta} \circ \gamma$ .

**Def.**  $M \otimes_A N$  heißt **Tensorprodukt** von  $M$  und  $N$  über  $A$ .

*Konstr.* • Sei  $C$  der freie  $A$ -Modul  $A^I$  mit  $I := M \times N$ . Elemente von  $C$  haben die Form  $\sum_{i=1}^n \lambda_i(x_i, y_i)$  mit  $\lambda_i \in A, x_i \in M, y_i \in N$ .

- Sei  $D \subset C$  der von allen Elementen der Form

$$\begin{aligned} (x + x', y) - (x, y) - (x', y), & \quad (ax, y) - a(x, y), \\ (x, y + y') - (x, y) - (x, y'), & \quad (x, ay) - a(x, y) \end{aligned}$$

mit  $x, x' \in M, y, y' \in N$  und  $a \in A$  erzeugte Untermodul.

- Setze  $M \otimes_A N := C/D$ .

**Notation.**  $x \otimes y := \gamma(x, y)$

*Bem.* Jedes Element in  $M \otimes_A N$  lässt sich als  $\sum_{i=1}^n x_i \otimes y_i$  mit  $x_i \in M, y_i \in N$  schreiben. In  $M \otimes_A N$  gelten folgende Rechenregeln:

$$\begin{aligned} x \otimes (ay) &= a(x \otimes y) = (ax) \otimes y \\ (x + x') \otimes (y + y') &= x \otimes y + x' \otimes y + x \otimes y' + x' \otimes y' \end{aligned}$$

**Lem.** Das Tensorprodukt induziert einen Bifunktor

$$\otimes_A : A\text{-Mod} \times A\text{-Mod} \rightarrow A\text{-Mod}.$$

**Lem.** Sei  $A$  ein komm. Ring,  $M$  und  $N$  zwei  $A$ -Moduln,  $x_i \in M$  und  $y_i \in N$  mit  $\sum_{i=1}^n x_i \otimes y_i = 0$  in  $M \otimes_A N$ . Dann gibt es endlich erzeugte Untermoduln  $M_0 \subseteq M$  und  $N_0 \subseteq N$  mit  $x_1, \dots, x_n \in M_0, y_1, \dots, y_n \in N_0$  und  $\sum_{i=1}^n x_i \otimes y_i = 0$  in  $M_0 \otimes_A N_0$

**Def.** Sei  $A$  ein komm. Ring,  $M_1, \dots, M_r$  und  $P$   $A$ -Moduln. Eine Abbildung  $\mu : M_1 \times \dots \times M_r \rightarrow P$  heißt **A-multilinear**, falls sie linear in jedem Argument ist.

**Prop.** Sei  $A$  ein komm. Ring,  $M_1, \dots, M_r$   $A$ -Moduln. Es existiert ein  $A$ -Modul  $M_1 \otimes_A \dots \otimes_A M_r$  und eine multilineare Abbildung  $\gamma : M_1 \times \dots \times M_r \rightarrow M_1 \otimes_A \dots \otimes_A M_r$  mit der univ. Eigenschaft Für jeden  $A$ -Modul  $P$  und für jede multilineare Abbildung  $\mu : M_1 \times \dots \times M_r \rightarrow P$  gibt es genau einen  $A$ -Modulhomomorphismus  $\underline{\mu} : M_1 \otimes_A \dots \otimes_A M_r \rightarrow P$  mit  $\mu = \underline{\mu} \circ \gamma$ .

*Konstr.*  $M_1 \otimes_A \dots \otimes_A M_r := M_1 \otimes_A (M_2 \otimes_A (\dots \otimes_A M_r))$

**Prop.** Sei  $A$  ein komm. Ring und  $M, N$  und  $P$  drei  $A$ -Moduln. Es existieren kanonische Isomorphismen

$$\begin{aligned} M \otimes_A N &\cong N \otimes_A M, & (M \otimes_A N) \otimes_A P &\cong M \otimes_A (N \otimes_A P), \\ (M \oplus N) \otimes_A P &\cong (M \otimes_A P) \oplus (N \otimes_A P), & A \otimes_A M &\cong M. \end{aligned}$$

**Def.** Seien  $A$  und  $B$  zwei komm. Ringe. Ein  $(A, B)$ -Bimodul ist eine abelsche Gruppe, welche sowohl ein  $A$ - als auch ein  $B$ -Modul ist, sodass die Modulstrukturen miteinander verträglich sind, d. h. für alle  $a \in A, b \in B$  und  $x \in N$  gilt  $a(bx) = b(ax)$ .

**Lem.** Sei  $M$  ein  $A$ -Modul,  $P$  ein  $B$ -Modul und  $N$  ein  $(A, B)$ -Bimodul. Dann gibt es einen kanon. Isomorphismus abelscher Gruppen

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

**Def.** Sei  $\phi : A \rightarrow B$  ein Morphismus kommutativer Ringe.

- Die **Skalareinschränkung** eines  $B$ -Moduls  $N$  (vermöge  $\phi$ ) ist der  $A$ -Modul  $N^A$ , der als Menge und ab. Gruppe  $N$  ist und dessen Skalarmult. durch  $a \cdot x := \phi(a) \cdot x$  definiert ist.
- Die **Skalarerweiterung** eines  $A$ -Moduls  $M$  (vermöge  $\phi$ ) ist der  $B$ -Modul  $M_B := B^A \otimes_A M$  mit der Skalarmultiplikation definiert durch  $b(b' \otimes x) := (bb') \otimes x$ .

**Prop.** Sei  $\phi : A \rightarrow B$  ein Morphismus kommutativer Ringe.

- Sei  $N$  ein  $B$ -Modul. Ist  $B^A$  als  $A$ -Modul endlich erzeugt und  $N$  als  $B$ -Modul endlich erzeugt, so ist  $N^A$  als  $A$ -Modul endlich erzeugt.
- Sei  $M$  ein  $A$ -Modul. Ist  $m$  als  $A$ -Modul endlich erzeugt, so ist  $M_B$  als  $B$ -Modul endlich erzeugt.

**Lem.** Sei  $M$  ein  $A$ -Modul und  $N$  ein  $B$ -Modul. Dann existiert ein kanonischer Isomorphismus  $N \otimes_B M_B \cong N^A \otimes_A M$  von  $B$ -Moduln.

**Prop.** Sei  $A$  ein komm. Ring und  $M, N$  und  $P$  drei  $A$ -Moduln. Dann ist folgende Abbildung ein  $A$ -Modulisomorphismus:

$$\begin{aligned} \operatorname{Hom}_A(M \otimes_A N, P) &\rightarrow \operatorname{Hom}_A(M, \operatorname{Hom}_A(N, P)), \\ \beta &\mapsto (x \mapsto (y \mapsto \beta(x \otimes y))). \end{aligned}$$

*Bem.* Mit anderen Worten: Es ex. eine Adj.  $- \otimes_A N \dashv \operatorname{Hom}_A(N, -)$

**Prop.** Sei  $A$  ein komm. Ring. Das Tensorprodukt ist rechtsexakt, d. h. ist  $E : M' \rightarrow M \rightarrow M'' \rightarrow 0$  eine exakte Sequenz von  $A$ -Moduln und  $N$  ein weiterer  $A$ -Modul, so ist auch die induzierte Sequenz

$$E \otimes_A N : M' \otimes_A N \rightarrow M \otimes_A N \rightarrow M'' \otimes_A N \rightarrow 0 \quad \text{exakt.}$$



*Bem.* Dies folgt daraus, dass das Tensorprodukt als Linksadjungierter Kolimiten erhält.

**Achtung.** Das Tensorprodukt ist i. A. nicht exakt. Insbesondere erhält es keine injektiven Abbildungen.

**Def.** Sei  $A$  ein kommutativer Ring. Ein  $A$ -Modul  $M$  heißt *flach*, falls  $(-\otimes_A M)$  exakt ist, d. h. falls für jede (lange) exakte Sequenz  $E$  auch  $E \otimes_A M$  exakt ist.

**Prop.** Sei  $A$  komm. und  $M$  ein  $A$ -Modul. Es sind äquivalent:

- Der  $A$ -Modul  $M$  ist flach.
- Für jede kurze exakte Sequenz  $E : 0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$  ist die tensorierte Sequenz  $E \otimes_A M$  exakt.
- Für jede injektive  $A$ -lineare Abbildung  $\phi : N \rightarrow N'$  ist auch  $\phi \otimes \text{id}_M : N \otimes_A M \rightarrow N' \otimes_A M$  injektiv.
- Für jede inj.  $A$ -lineare Abb.  $\phi : N \rightarrow N'$  zw. endl. erzeugten  $A$ -Moduln ist auch  $\phi \otimes \text{id}_M : N \otimes_A M \rightarrow N' \otimes_A M$  injektiv.

**Prop.** Sei  $\phi : A \rightarrow B$  ein Homomorphismus kommutativer Ringe. Ist  $M$  ein flacher  $A$ -Modul, so ist  $M_B$  ein flacher  $B$ -Modul.

## Algebren

**Def.** Eine kommutative **A-Algebra**  $B$  ist ein kommutativer Ring  $B$  zusammen mit einem Ringhomomorphismus  $\phi : A \rightarrow B$ , dem *Strukturmorphismus* der Algebra.

*Bem.* Ist  $a \in A$  und  $b \in B$ , so definieren wir  $ab := \phi(a)b$  (wie bei der Skalareinschränkung).

**Bspe.** • Sei  $K$  ein Körper. Eine nichttriviale  $K$ -Algebra ist dasselbe wie ein Ring, der  $K$  als Unterring enthält.  
• Jeder Ring ist auf genau eine Weise eine  $\mathbb{Z}$ -Algebra.

**Def.** Ein *Homomorphismus* von  $A$ -Algebren  $B$  und  $C$  ist ein Ringhomomorphismus  $\chi : B \rightarrow C$ , welcher einen Homomorphismus  $\chi : B^A \rightarrow C^A$  von  $A$ -Moduln induziert.

*Bem.* Ein Ringhomomorphismus  $\chi : B \rightarrow C$  ist also genau dann ein  $A$ -Algebrenhomomor., wenn  $\chi(ab) = a\chi(b)$  für alle  $a \in A$  und  $b \in B$ .

*Bem.*  $A$ -Algebren und ihre Homomor. bilden eine Kategorie **A-Alg.**

**Def.** Sei  $A$  ein komm. Ring. Eine komm.  $A$ -Algebra  $B$  heißt eine ...

- ... **endliche A-Algebra**, falls  $B^A$  als  $A$ -Modul endlich erzeugt ist, d. h. falls endlich viele Elemente  $b_1, \dots, b_n \in B$  existieren, sodass jedes Element aus  $B$  als  $A$ -Linearkombination der  $b_i$  geschrieben werden kann.
- ... **endlich erzeugte A-Algebra** oder  $A$ -Algebra **endlichen Typs**, falls endlich viele Elemente  $b_1, \dots, b_n \in B$  existieren, sodass jedes andere Element von  $B$  als Polynom in den  $b_i$  mit Koeffizienten aus  $A$  geschrieben werden kann.

**Def.** Ein kommutativer Ring heißt **endlich erzeugt**, falls er eine  $\mathbb{Z}$ -Algebra endlichen Typs ist.

**Def.** Sei  $A$  ein kommutativer Ring. Seien  $\phi : A \rightarrow B$  und  $\psi : A \rightarrow C$  die Strukturabbildungen zweier  $A$ -Algebren  $B$  und  $C$ . Dann ist auf  $D := B^A \otimes_A C^A$  eine Multiplikation durch

$$\mu : D \times D \rightarrow D, \quad (b \otimes c, b' \otimes c') \mapsto (bb') \otimes (cc')$$

definiert. Der Ring  $D$  wird mit der Strukturabbildung

$$\rho : A \rightarrow D, \quad a \mapsto \phi(a) \otimes 1 = 1 \otimes \psi(a)$$

zu einer  $A$ -Algebra. Diese heißt **Tensorprodukt**  $B \otimes_A C$  der kommutativen Algebren  $B$  und  $C$ .

## Gerichtete Limiten

**Def.** Eine **gerichtete Menge** ist eine nichtleere teilweise geordnete Menge  $(I, \leq)$ , sodass  $\forall i, j \in I : \exists k \in I : i \leq k \wedge j \leq k$ .

*Bem.* Eine teilweise geordnete Menge  $(I, \leq)$  ist genau dann gerichtet, wenn in  $I$ , aufgefasst als Präordnungskategorie, jedes endliche Diagramm einen Koegel besitzt.

**Def.** Sei  $(I, \leq)$  eine gerichtete Menge und  $A$  ein Ring. Ein **gerichtetes System**  $M_\bullet$  von  $A$ -Moduln über  $I$  ist ein Funktor

$$M_\bullet : I \rightarrow A\text{-Mod}, \quad i \mapsto M_i, \quad (i \leq j) \mapsto \mu_j^i : M_i \rightarrow M_j,$$

wobei wir  $I$  als Präordnungskategorie auffassen.

**Prop.** Sei  $M_\bullet$  ein gerichtetes System von  $A$ -Moduln. Dann existiert der Kolimes  $\varinjlim M_i$  von  $M_\bullet$ .

**Def.** Dieser Kolimes wird **gerichteter Limes** von  $M_\bullet$  genannt.

*Konstr.* • Sei  $C := \bigoplus_{i \in I} M_i$ .

- Sei  $D \subseteq C$  der Untermodul, der von allen Elementen der Form  $x_i - \mu_j^i(x_i)$  mit  $i \leq j$  und  $x_i \in M_i$  erzeugt wird.
- Dann erfüllt  $M := C/D$  die geforderte universelle Eigenschaft.

*Bem.* • Jedes  $x \in \varinjlim M_i$  wird durch ein  $x_i \in M_i$  repräsentiert.

- Ein Element  $x_i \in M_i$  repräsentiert dabei genau dann das Nullelement, falls ein  $j \in I$  mit  $i \leq j$  existiert, sodass  $\mu_j^i(x_i) = 0$ .

**Lem.** Jeder  $A$ -Modul ist der gerichtete Limes seiner endlich erzeugten Untermoduln.

**Def.** Sei  $(I, \leq)$  eine gerichtete Menge. Ein *Homomorphismus* von gerichteten Systemen  $M_\bullet$  und  $N_\bullet$  von  $A$ -Moduln über  $I$  ist eine natürliche Transformation  $\phi_\bullet : M_\bullet \rightarrow N_\bullet$ .

*Bem.* Damit bilden gerichtete Systeme von  $A$ -Moduln über  $I$  zusammen mit ihren Homomorphismen eine Kategorie  $[I, A\text{-Mod}]$ .

**Prop.** Sei  $\phi_\bullet : M_\bullet \rightarrow N_\bullet$  ein Morphismus zwischen gerichteten Systemen von  $A$ -Moduln über  $I$ ,  $M := \varinjlim M_i$  und  $N := \varinjlim N_i$ .

Dann gibt es genau einen Morphismus  $\phi := \varinjlim \phi_i : M \rightarrow N$  mit

$$(M_i \rightarrow M \xrightarrow{\phi} N) = (M_i \xrightarrow{\phi_i} N_i \rightarrow N) \quad \text{für alle } i \in I.$$

*Bem.* Damit ist der gerichtete Limes ein Funktor

$$\varinjlim : [I, A\text{-Mod}] \rightarrow A\text{-Mod}.$$

**Def.** Eine Sequenz  $M_\bullet \xrightarrow{\phi_\bullet} N_\bullet \xrightarrow{\psi_\bullet} P_\bullet$  von gerichteten Systemen von  $A$ -Moduln über  $I$  heißt **exakt**, falls für alle  $i \in I$  die Sequenz  $M_i \xrightarrow{\phi_i} N_i \xrightarrow{\psi_i} P_i$  exakt ist.

**Prop.** Der Gerichteter-Limes-Funktor ist exakt:

Sei  $M_\bullet \xrightarrow{\phi_\bullet} N_\bullet \xrightarrow{\psi_\bullet} P_\bullet$  eine exakte Sequenz gerichteter Systeme von  $A$ -Moduln über  $I$ . Dann ist die induzierte Sequenz

$$\varinjlim M_i \xrightarrow{\varinjlim \phi_i} \varinjlim N_i \xrightarrow{\varinjlim \psi_i} \varinjlim P_i \quad \text{auch exakt.}$$

**Prop.** Sei  $M_\bullet$  ein gerichtetes System von  $A$ -Moduln über  $I$  und  $N$  ein  $A$ -Modul. Dann gibt es einen kanonischen Isomorphismus

$$\varinjlim (M_i \otimes_A N) \cong (\varinjlim M_i) \otimes_A N.$$

**Prop.** Sei  $A_\bullet$  ein gerichtetes System von Ringen und Ringhomomorphismen. Fasse  $A_\bullet$  als gerichtetes System von ab. Gruppen (d. h.  $\mathbb{Z}$ -Moduln) auf. Dann gibt es  $A := \varinjlim A_i$  eine Multiplikation, sodass

$A$  ein Ring ist und die Gruppenhomomorphismen  $A_i \rightarrow A$  sogar Ringhomomorphismen sind.

**Prop.** Ist  $\varinjlim A_i = 0$ , so gibt es ein  $i \in I$  mit  $A_i = 0$ .

**Def.** Sei  $(B_i)_{i \in I}$  eine Familie kommutativer  $A$ -Algebren. Für eine endliche Teilmenge  $J \subset I$  setzen wir  $B_J := \bigotimes_{i \in J} B_i$ .

Dann ist  $B_\bullet$  ein gerichtetes System über  $(\mathcal{P}(I)_{\text{fin}}, \subseteq)$ . Der Limes  $\bigotimes_{i \in I} B_i := \varinjlim_{J \subseteq I} B_J$  heißt **Tensorprodukt** über die Familie  $(B_i)_{i \in I}$ .

## Lokalisierung

**Def.** Sei  $A$  ein Ring. Eine **multiplikativ abgeschl. Teilmenge** von  $A$  ist eine Teilmenge  $S \subseteq A$  mit  $1 \in S$  und  $xy \in S$  für alle  $x, y \in S$ .

- Bspe.**
- Ein Ring  $A$  ist genau dann ein Integritätsbereich, wenn  $A \setminus \{0\}$  multiplikativ abgeschlossen ist.
  - Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Dann ist  $1 + \mathfrak{a}$  mult. abgeschlossen.

**Prop.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Dann gibt es einen komm. Ring  $S^{-1}A$  und einen Ringhomom.  $\iota: A \rightarrow S^{-1}A$  mit folgender universeller Eigenschaft:  
Für jeden Ring  $B$  und Ringhomom.  $\phi: A \rightarrow B$  mit  $\phi(S) \subseteq B^\times$  gibt es genau einen Ringhomom.  $\psi: S^{-1}A \rightarrow B$  mit  $\phi = \psi \circ \iota$ .

**Konstr.** • Führe auf der Menge der Paare  $(a, s) \in A \times S$  eine Äquivalenzrelation ein durch

$$(a, s) \sim (b, t) \iff \exists u \in S : u(at - bs) = 0.$$

- Setze  $S^{-1}A := (A \times S)/\sim$ .
- Wir schreiben  $\frac{a}{s}$  für die Äquivalenzklasse von  $(a, s)$  in  $S^{-1}A$ .
- Auf  $S^{-1}A$  sind Addition und Mult. (wohl!) definiert durch

$$\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

- Der Ringhomomorphismus ist gegeben durch  $\iota(a) := \frac{a}{1}$ .

**Def.** Der kommutative Ring  $S^{-1}A$  heißt **Lokalisierung** von  $A$  nach  $S$  und  $\iota: A \rightarrow S^{-1}A$  ihr **Strukturhomomorphismus**.

**Prop.** Sei  $A$  komm. und  $S \subseteq A$  mult. abgeschlossen. Dann gilt:

- Für alle  $s \in S$  ist  $\iota(s)$  eine Einheit in  $S^{-1}A$ .
- Ist  $a \in A$  mit  $\iota(a) = 0$ , so gibt es ein  $s \in S$  mit  $as = 0$  in  $A$ .
- Jedes Element in  $S^{-1}A$  hat die Form  $\iota(a)\iota(s)^{-1}$  für ein  $a \in A$  und ein  $s \in S$ .

**Bem.** Diese drei Eigenschaften charakterisieren die Lokalisierung eindeutig: Ist  $\phi: A \rightarrow B$  ein Ringhomomorphismus, der die drei Eigenschaften von  $\iota$  aus der letzten Prop. erfüllt, so gilt  $B \cong S^{-1}A$ .

**Def.** Sei  $A$  ein komm. Ring und  $\mathfrak{p} \subset A$  ein Primideal. Dann ist  $A \setminus \mathfrak{p}$  multiplikativ abgeschlossen. Der komm. Ring  $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$  heißt **Lokalisierung** von  $A$  bei  $\mathfrak{p}$  oder **Halm** von  $A$  an  $\mathfrak{p}$ .

**Bem.**  $A_{\mathfrak{p}}$  ist ein lokaler Ring mit maximalem Ideal

$$\mathfrak{m} := A_{\mathfrak{p}}\mathfrak{p} = \left\{ \frac{a}{s} \mid a \in \mathfrak{p}, s \in A \setminus \mathfrak{p} \right\}.$$

**Def.** Sei  $A$  ein Integritätsbereich. Dann ist  $S := A \setminus \{0\}$  mult. abgeschlossen. Die Lokal.  $S^{-1}A$  heißt **Quotientenkörper** von  $A$ .

**Bem.** Der Strukturhomomorphismus  $A \rightarrow S^{-1}A$  ist in diesem Fall injektiv, wir können daher  $A$  als Unterring von  $S^{-1}A$  ansehen. Der Körper  $S^{-1}A$  ist der kleinste Körper, der  $A$  als Unterring enthält.

**Bsp.**  $\mathbb{Q}$  ist der Quotientenkörper von  $\mathbb{Z}$

**Bsp.**  $S^{-1}A = 0 \iff 0 \in S$

**Def.** Sei  $A$  ein komm. Ring,  $f \in A$ . Dann ist  $S := \{f^n \mid n \geq 0\}$  mult. abgeschlossen. Die Lokalisierung  $A[f^{-1}] := S^{-1}A$  heißt **Lokalisierung** von  $A$  **außerhalb** von  $f$ .

**Konstr.** Sei  $A$  ein kommutativer Ring,  $S \subseteq A$  multiplikativ abgeschlossen und  $M$  ein  $A$ -Modul.

- Wir definieren auf der Menge der Paare  $M \times S$  eine Äquivalenzrelation durch

$$(m, s) \sim (m', s') \iff \exists u \in S : u(ms' - m's) = 0.$$

- Wir schreiben  $\frac{m}{s}$  für die Äquivalenzklasse von  $(m, s)$ .
- Vermöge der Addition und der Skalarmultiplikation

$$\frac{m}{s} + \frac{n}{t} := \frac{mt+ns}{st} \quad \text{bzw.} \quad \frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$$

wird  $S^{-1}M := (M \times S)/\sim$  zu einem  $S^{-1}A$ -Modul.

**Def.** Der  $S^{-1}A$ -Modul  $S^{-1}M$  heißt **Lokalisierung** von  $M$  nach  $S$  und  $\iota: M \rightarrow (S^{-1}M)^A$ ,  $m \mapsto \frac{m}{1}$  sein **Strukturhomomorphismus**.

**Def.** Sei  $\mathfrak{p} \subset A$  ein Primideal. Der  $A_{\mathfrak{p}}$ -Modul  $M_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}M$  heißt **Lokalisierung** von  $M$  bei  $\mathfrak{p}$  oder **Halm** von  $M$  an  $\mathfrak{p}$ . Das Bild von  $m \in M$  in  $M_{\mathfrak{p}}$  heißt **Keim** von  $m$  an  $\mathfrak{p}$ .

**Def.** Sei  $f \in A$ . Dann heißt  $M[f^{-1}] := \{f^n \mid n \geq 0\}^{-1}M$  die **Lokalisierung** von  $M$  außerhalb von  $f$ . Das Bild von  $m \in M$  in  $M[f^{-1}]$  heißt **Einschränkung** von  $m$  außerhalb von  $f$ .

**Bem.** Sei  $A$  ein kommutativer Ring und  $S \subseteq A$  mult. abgeschlossen. Die Lokalisierung von  $A$ -Moduln nach  $S$  stiftet einen Funktor **A-Mod**  $\rightarrow (S^{-1}A)\text{-Mod}$ : Für einen Morphismus  $\phi: M \rightarrow N$  ist

$$S^{-1}\phi: S^{-1}M \rightarrow S^{-1}N, \quad \frac{m}{s} \mapsto \frac{\phi(m)}{s}.$$

**Prop.** Die Lokalisierung ist exakt: Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Ist  $M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$  exakt, so ist auch  $S^{-1}M' \xrightarrow{S^{-1}\phi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}M''$  exakt.

**Prop.** Sei  $A$  ein kommutativer Ring und  $S \subseteq A$  mult. abgeschlossen. Sei  $M$  ein  $A$ -Modul und  $P, N \subseteq M$  Untermoduln. Dann gilt:

- $S^{-1}(N + P) = S^{-1}N + S^{-1}P \subseteq S^{-1}M$
- $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$  als  $S^{-1}A$ -Moduln
- $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P \subseteq S^{-1}M$

**Prop.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Sei  $M$  ein  $A$ -Modul. Dann ist folgende Abb. ein Iso von  $S^{-1}A$ -Moduln:

$$\phi: S^{-1}A \otimes_A M \rightarrow S^{-1}M, \quad \frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

**Kor.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Dann ist  $S^{-1}A$  eine flache  $A$ -Algebra.

**Prop.** Sei  $A$  ein kommutativer Ring und  $S \subseteq A$  mult. abgeschlossen. Seien  $M$  und  $N$  zwei  $A$ -Moduln. Dann ist folgende Abbildung ein Isomorphismus von  $S^{-1}A$ -Moduln:

$$\phi: S^{-1}M \otimes_{S^{-1}A} S^{-1}N \rightarrow S^{-1}(M \otimes_A N), \quad \frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{st}$$

**Bsp.** Sei  $\mathfrak{p} \subset A$  ein Primideal. Dann gilt  $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \cong (M \otimes_A N)_{\mathfrak{p}}$ .

## Lokale Eigenschaften

**Sprechweise.** Eine Eigenschaft kommutativer Ringe (oder Moduln über einem solchen) heißt **lokal**, falls gilt:

Ein Ring  $A$  (bzw. Modul  $M$ ) besitzt die Eigenschaft genau dann, wenn all seine Halme  $A_{\mathfrak{p}}$  (bzw.  $M_{\mathfrak{p}}$ ) die Eigenschaft besitzen.

**Prop.** Sei  $A$  ein kommutativer Ring und  $M$  ein  $A$ -Modul. Dann sind äquivalent:

- $M = 0$
- $M_{\mathfrak{p}} = 0$  für alle Primideale  $\mathfrak{p} \subset A$
- $M_{\mathfrak{m}} = 0$  für alle max. Ideale  $\mathfrak{m} \subset A$

Mit der Exaktheit der Lokalisierung folgt:

**Kor.** Sei  $A$  ein kommutativer Ring und  $\phi: M \rightarrow N$  ein Homomorphismus von  $A$ -Moduln.

- Es sind äquivalent:

- $\phi: M \rightarrow N$  ist injektiv.
- $\phi_{\mathfrak{p}}: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$  ist injektiv für alle Primideale  $\mathfrak{p} \subset A$ .
- $\phi_{\mathfrak{m}}: M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$  ist injektiv für alle max. Ideale  $\mathfrak{m} \subset A$ .

- Es sind äquivalent:

- $\phi: M \rightarrow N$  ist surjektiv.
- $\phi_{\mathfrak{p}}: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$  ist surjektiv für alle Primideale  $\mathfrak{p} \subset A$ .
- $\phi_{\mathfrak{m}}: M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$  ist surjektiv für alle max. Ideale  $\mathfrak{m} \subset A$ .

**Prop.** Sei  $A$  ein kommutativer Ring und  $M$  ein  $A$ -Modul. Dann sind äquivalent:

- $M$  ist ein flacher  $A$ -Modul.
- $M_{\mathfrak{p}}$  ist ein flacher  $A_{\mathfrak{p}}$ -Modul für alle Primideale  $\mathfrak{p} \subset A$ .
- $M_{\mathfrak{p}}$  ist ein flacher  $A_{\mathfrak{m}}$ -Modul für alle max. Ideale  $\mathfrak{m} \subset A$ .

## Ideale in Lokalisierungen

**Notation.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Für ein Ideal  $\mathfrak{a} \subseteq A$  schreiben wir  $S^{-1}\mathfrak{a} := (S^{-1}A)\mathfrak{a}$ .

*Bem.* Dies ist gerechtfertigt, denn jedes Element in  $(S^{-1}A)\mathfrak{a}$  hat die Form  $\sum_i \frac{a_i}{s_i}$  und diese Terme können wir auf einen gemeinsamen Nenner bringen.

**Prop.** Alle Ideale in  $S^{-1}A$  sind erweiterte Ideale, d. h. von der Form  $S^{-1}\mathfrak{a}$  für ein Ideal  $\mathfrak{a} \subseteq A$ .

**Prop.**  $A \cap (S^{-1}\mathfrak{a}) = \bigcup_{s \in S} (\mathfrak{a} : s)$

**Bsp.**  $S^{-1}\mathfrak{a} = (1) \iff \mathfrak{a} \cap S \neq \emptyset$

**Prop.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Ein Ideal  $\mathfrak{a} \subseteq A$  ist genau dann ein kontrahiertes Ideal bezüglich  $A \rightarrow S^{-1}A$ , wenn kein Element von  $S$  ein Nullteiler in  $A/\mathfrak{a}$  ist.

**Prop.** Sei  $A$  ein komm. Ring. Die Lokalisierung nach einer mult. abg. Teilmenge  $S \subseteq A$  vertauscht mit folgenden Ideal-Operationen: endl. Summen, endl. Produkte, endl. Schnitte und Wurzeln. Das heißt, für zwei Ideale  $\mathfrak{a}, \mathfrak{b} \subseteq A$  gilt:

- $S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}$
- $S^{-1}(\mathfrak{a} \cdot \mathfrak{b}) = S^{-1}\mathfrak{a} \cdot S^{-1}\mathfrak{b}$
- $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$
- $S^{-1}\sqrt{\mathfrak{a}} = \sqrt{S^{-1}\mathfrak{a}}$

**Kor.**  $\sqrt{(0)} = S^{-1}\sqrt{(0)} \subseteq S^{-1}A$

**Prop.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Folgende Korrespondenz ist bijektiv und monoton:

$$\begin{array}{ccc} \{ \text{Primideale } \mathfrak{p} \subseteq A \text{ mit } \mathfrak{p} \cap S = \emptyset \} & \leftrightarrow & \{ \text{Primideale } \mathfrak{q} \subseteq S^{-1}A \} \\ \mathfrak{p} & \mapsto & S^{-1}\mathfrak{p} = (S^{-1}A)\mathfrak{p} \\ A \cap \mathfrak{q} & \leftarrow & \mathfrak{q} \end{array}$$

**Kor.** Für ein Primideal  $\mathfrak{r} \subseteq A$  liefert dies eine Korrespondenz

$$\{ \text{Primideale } \mathfrak{p} \subseteq A \text{ mit } \mathfrak{p} \subseteq \mathfrak{r} \} \leftrightarrow \{ \text{Primideale } \mathfrak{q} \subseteq A_{\mathfrak{r}} \}$$

*Bem.* Sei  $\mathfrak{p} \subseteq A$  ein Primideal und  $\mathfrak{q} \subseteq \mathfrak{p}$  ein weiteres Primideal. Lokalisieren bei  $\mathfrak{p}$  schneidet alle Primideale heraus, die nicht in  $\mathfrak{p}$  enthalten sind. Der Wechsel nach  $A/\mathfrak{q}$  schneidet alle Primideale heraus außer denen, die  $\mathfrak{q}$  enthalten. Somit enthält  $A_{\mathfrak{p}}/(A_{\mathfrak{p}}\mathfrak{q}) = (A/\mathfrak{q})_{\mathfrak{p}}$  nur Primideale zwischen  $\mathfrak{q}$  und  $\mathfrak{p}$ .

**Def.** Sei  $A$  ein komm. Ring und  $\mathfrak{p} \subseteq A$  ein Primideal. Der Körper  $A(\mathfrak{p}) := A_{\mathfrak{p}}/(A_{\mathfrak{p}}\mathfrak{p}) = (A/\mathfrak{p})_{\mathfrak{p}}$  heißt **Restklassenkörper** von  $A$  an  $\mathfrak{p}$ .

**Prop.** Sei  $\phi : A \rightarrow B$  ein Homomorphismus kommutativer Ringe. Dann ist ein Primideal  $\mathfrak{p} \subseteq A$  genau dann eine Kontraktion eines Primideals in  $B$ , falls  $A \cap (B\mathfrak{p}) = \mathfrak{p}$ .

**Prop.** Sei  $A$  ein komm. Ring,  $S \subseteq A$  mult. abgeschlossen und  $M$  ein endlich erzeugter  $A$ -Modul. Dann ist  $S^{-1}\text{ann}(M) = \text{ann}(S^{-1}M)$ .

**Kor.** Sei  $A$  ein komm. Ring,  $S \subseteq A$  mult. abgeschlossen,  $M$  ein  $A$ -Modul und  $N, P \subseteq M$  zwei Untermoduln. Ist  $P$  endlich erzeugt, so gilt  $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$ .

## Primärzerlegung

**Def.** Ein Ideal  $\mathfrak{q} \subseteq A$  heißt **primär**, falls  $1 \notin \mathfrak{q}$  und falls aus  $xy \in \mathfrak{q}$  schon  $x \in \mathfrak{q}$  oder  $\exists n \in \mathbb{N} : y^n \in \mathfrak{q}$  folgt.

**Lem.**  $\mathfrak{q} \subsetneq A$  ist primär  $\iff \{ \text{Nullteiler} \} = \sqrt{(0)}$  in  $A/\mathfrak{q}$

**Bspe.** • Primideale sind primär.

- Sei  $\phi : A \rightarrow B$  ein Homomorphismus kommutativer Ringe. Ist  $\mathfrak{b} \subseteq B$  primär, so auch  $A \cap \mathfrak{b} \subseteq A$ .

**Lem.** Sei  $\mathfrak{q}$  primär. Dann ist  $\sqrt{\mathfrak{q}}$  das kleinste Primideal mit  $\mathfrak{p} \supseteq \mathfrak{q}$ .

**Def.** Sei  $\mathfrak{q} \subseteq A$  ein primäres Ideal und  $\mathfrak{p} := \sqrt{\mathfrak{q}}$ . Dann heißt  $\mathfrak{q}$  ein **p-primäres** Ideal.

*Bem.* Primzahlen  $\hat{=}$  Primideale  
Primzahlpotenzen  $\hat{=}$  primäre Ideale

**Bsp.** Die primären Ideale in  $\mathbb{Z}$  sind die Ideale der Form  $(0)$  und  $(p^n)$  für eine Primzahl  $p$ .

**Achtung.** Im Allgemeinen ist ein primäres Ideal keine Potenz eines Primideals! Andersherum ist die Potenz eines Primideals auch nicht notwendigerweise primär. Analoges gilt aber für max. Ideale:

**Prop.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Ist  $\mathfrak{m} := \sqrt{\mathfrak{a}}$  ein maximales Ideal, so ist  $\mathfrak{a}$  ein m-primäres Ideal.

**Kor.** Ist  $\mathfrak{m}$  ein max. Ideal, so sind  $\mathfrak{m}^n$  mit  $n \geq 1$  alle m-primär.

**Def.** Sei  $A$  ein komm. Ring und  $\mathfrak{a} \subseteq A$  ein Ideal. Eine Darstellung von  $\mathfrak{a}$  als Schnitt  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$  endlich vieler primärer Ideale  $\mathfrak{q}_i$  heißt **Primärzerlegung** von  $\mathfrak{a}$ . Sind die  $\sqrt{\mathfrak{q}_i}$  paarweise verschieden und gilt  $\mathfrak{q}_i \not\supseteq \bigcap_{i \neq j} \mathfrak{q}_j$  für alle  $i$ , so heißt die Primärzerlegung **minimal**.

**Def.** Ein Ideal  $\mathfrak{a} \subseteq A$  heißt **zerlegbar**, wenn es eine Primärzerlegung besitzt.

**Lem.** Sei  $\mathfrak{p} \subseteq A$  ein Primideal und  $\mathfrak{q}_1, \dots, \mathfrak{q}_n$  alle p-primär. Dann ist auch  $(\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n)$  wieder p-primär.

**Kor.** Man kann eine Primärzerlegung eines Ideals zu einer minimalen Primärzerlegung reduzieren.

**Lem.** Sei  $\mathfrak{p} \subseteq A$  prim,  $\mathfrak{q}$  ein p-primäres Ideal und  $x \in A$ . Dann gilt:

- Ist  $x \in \mathfrak{q}$ , so gilt  $(\mathfrak{q} : x) = (1)$ .
- Ist  $x \notin \mathfrak{q}$ , so ist  $(\mathfrak{q} : x)$  ein p-primäres Ideal.
- Ist  $x \notin \mathfrak{p}$ , so ist  $(\mathfrak{q} : x) = \mathfrak{q}$ .

**Satz** (erster Eindeutigkeitssatz). Sei  $A$  ein komm. Ring und  $\mathfrak{a} \subseteq A$  ein Ideal mit minimaler Primärzerlegung  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ . Sei  $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ . Dann sind die Ideale  $\mathfrak{p}_i$  genau die Ideale, die von der Form  $\sqrt{(\mathfrak{a} : x)}$  mit  $x \in A$  sind.

*Bem.* Insb. sind die Ideale  $\mathfrak{p}_i$  unabh. von der Primärzerlegung.

**Def.** Die Ideale  $\mathfrak{p}_i$  heißen die zu  $\mathfrak{a}$  **assoziierten Primideale**.

**Lem.** Sei  $\mathfrak{p}$  ein zu  $\mathfrak{a}$  assoziiertes Primideal. Dann gibt es ein  $x \in A$ , sodass  $(\mathfrak{a} : x)$  ein p-primäres Ideal ist.

**Def.** Sei  $A$  ein komm. Ring und  $\mathfrak{a} \subseteq A$  ein Ideal mit minimaler Primärzerlegung  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ . Sei  $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ . Die minimalen Elemente der Menge der zu  $\mathfrak{a}$  assoz. Primideale heißen **isolierte Primideale**, alle anderen zu  $\mathfrak{a}$  assoz. Primideale **eingebettete Primideale**. Ein primäres Ideal  $\mathfrak{q}_i$  heißt isolierte / eingebettete **Primärkomponente** von  $\mathfrak{a}$ , wenn  $\mathfrak{p}_i$  isoliert / eingebettet ist.

**Prop.** Sei  $\mathfrak{a} \subseteq A$  ein zerlegbares Primideal. Jedes Primideal  $\mathfrak{p}$  mit  $\mathfrak{p} \supseteq \mathfrak{a}$  enthält ein assoziiertes (und damit auch ein isoliertes) Primideal zu  $\mathfrak{a}$ .

**Kor.** Die isolierten Primideale zu  $\mathfrak{a}$  sind genau die min. Elemente von  $\{ \text{Primideale } \mathfrak{p} \subseteq A \text{ mit } \mathfrak{p} \supseteq \mathfrak{a} \} \cong \{ \text{Primideale in } A/\mathfrak{a} \}$ .

**Prop.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal mit min. Primärzerl.  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ .

Sei  $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ . Dann gilt  $\bigcup_{i=1}^n \mathfrak{p}_i = \{ x \in A \mid (\mathfrak{a} : x) \neq \mathfrak{a} \}$ .

**Prop.** Sei  $A$  ein komm. Ring, in dem  $(0)$  zerlegbar ist. Dann gilt:

- Die Menge  $D$  der Nullteiler in  $A$  ist die Vereinigung der zu  $(0)$  assoziierten Primideale.
- Die Menge der nilpotenten Elemente ist der Schnitt aller (isolierten) Primideale, die zu  $(0)$  assoziiert sind.

**Prop.** Sei  $\mathfrak{p} \subseteq A$  ein Primideal,  $\mathfrak{q}$  ein p-primäres Ideal und  $S \subseteq A$  multiplikativ abgeschlossen. Dann gilt:

- Ist  $S \cap \mathfrak{p} \neq \emptyset$ , so folgt  $S^{-1}\mathfrak{q} = (1)$ .
- Ist  $S \cap \mathfrak{p} = \emptyset$ , so ist  $S^{-1}\mathfrak{q}$  ein  $S^{-1}\mathfrak{p}$ -primäres Ideal und es gilt  $A \cap S^{-1}\mathfrak{q} = \mathfrak{q}$ .

**Kor.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  multiplikativ abgeschlossen. Dann ist folgende Korrespondenz bijektiv und monoton:

$$\begin{array}{ccc} \{ \mathfrak{q} \subseteq A \text{ primär mit } \sqrt{\mathfrak{q}} \cap S = \emptyset \} & \leftrightarrow & \{ \mathfrak{r} \subseteq S^{-1}A \text{ primär} \} \\ \mathfrak{q} & \mapsto & S^{-1}\mathfrak{q} \\ A \cap \mathfrak{r} & \leftarrow & \mathfrak{r} \end{array}$$

**Def.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Die **Sättigung** eines Ideals  $\mathfrak{a} \subseteq A$  bzgl.  $S$  ist das Ideal  $S(\mathfrak{a}) := A \cap S^{-1}\mathfrak{a}$ .

**Prop.** Sei  $A$  ein komm. Ring und  $S \subseteq A$  mult. abgeschlossen. Sei  $\mathfrak{a} \subseteq A$  ein Ideal mit minimaler Primärzerlegung  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ . Sei  $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ . Seien die  $\mathfrak{q}_i$  so sortiert, dass ein  $m$  existiert mit  $S \cap \mathfrak{p}_i = \emptyset \iff i \leq m$ . Dann sind  $S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_1 \cap \dots \cap S^{-1}\mathfrak{q}_m$  und  $S(\mathfrak{a}) = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$  minimale Primärzerlegungen.

**Def.** Sei  $\mathfrak{a} \subseteq A$  ein zerlegbares Ideal in einem kommutativen Ring. Eine Menge  $\mathfrak{S}$  von zu  $\mathfrak{a}$  assoz. Primidealen heißt **isoliert**, falls gilt:

$$\mathfrak{p}' \subseteq \mathfrak{p} \in \mathfrak{S} \implies \mathfrak{p}' \in \mathfrak{S} \quad \text{für zu } \mathfrak{a} \text{ assoz. Ideale } \mathfrak{p}, \mathfrak{p}'.$$

**Prop.** Sei  $\mathfrak{S}$  eine isolierte Menge von zu  $\mathfrak{a}$  assoziierten Primidealen. Dann ist  $S := A \setminus \bigcup_{\mathfrak{p} \in \mathfrak{S}} \mathfrak{p}$  multiplikativ abgeschlossen und für jedes an  $\mathfrak{a}$  assoziierte Primideal  $\mathfrak{p}'$  gilt:  $\mathfrak{p}' \in \mathfrak{S} \iff \mathfrak{p}' \cap S = \emptyset$ .

**Satz** (zweiter Eindeutigkeitssatz). Sei  $\mathfrak{a} \subseteq A$  ein Ideal mit minimaler Primärzerlegung  $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ . Sei  $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ . Ist  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$  eine isolierte Menge von zu  $\mathfrak{a}$  assoziierten Primidealen, so ist  $\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$  unabhängig von der Zerlegung.

Für  $m = 1$  folgt:

**Kor.** Die isolierten Primärkomp. von  $\mathfrak{a}$  sind eindeutig bestimmt.

## Ganzheit

**Def.** Sei  $B$  ein komm. Ring und  $A \subseteq B$  ein Unterring. Ein Element  $x \in B$  heißt **ganz** über  $A$ , falls  $x$  eine Gleichung der Form  $x^n + a_1 x^{n-1} + \dots + a_n = 0$  mit  $a_i \in A$  erfüllt.

**Prop.** Sei  $A \subseteq B$  eine Erw. komm. Ringe. Es sind äquivalent:

- $x$  ist ganz über  $A$ .
- $A[x] \subseteq B$  ist als  $A$ -Modul endlich erzeugt.
- Es existiert ein Unterring  $C \subseteq B$  mit  $C \supseteq A[x]$ , der als  $A$ -Modul endlich erzeugt ist.
- Es ex. ein treuer  $A[x]$ -Modul  $M$ , der als  $A$ -Modul endl. erz. ist.

**Kor.** Sei  $A \subseteq B$  eine Erw. komm. Ringe.

- Seien  $x_1, \dots, x_n \in B$  jeweils ganz über  $A$ . Dann ist  $A[x_1, \dots, x_n]$  ein endlich erzeugter  $A$ -Modul.
- Die Menge  $C := \{ \text{über } A \text{ ganze Elemente } x \in B \} \subseteq B$  ist ein Unterring von  $B$  mit  $C \supseteq A$ .

**Def.** Die Menge  $C \subseteq B$  heißt **ganzer Abschluss** von  $A$  in  $B$ . Ist  $C = A$ , so heißt  $A$  **ganz abgeschlossen** in  $B$ . Ist  $C = B$ , so heißt  $B$  **ganz über**  $A$ .

**Bsp.**  $\mathbb{Z}$  ist in  $\mathbb{Q}$  ganz abgeschlossen.

**Def.** Sei  $\phi : A \rightarrow B$  ein Mor. komm. Ringe. (Dadurch wird  $B$  zu einer  $A$ -Algebra.) Dann heißt  $\phi$  ganz und  $B$  eine **ganze  $A$ -Algebra**, falls  $B$  ganz über  $\phi(A) \subseteq B$  ist.

**Lem.** Für eine  $A$ -Algebra  $B$  gilt:

$B$  endlich  $\iff B$  endlich erz.  $\wedge B$  ganz (jeweils als  $A$ -Algebra).

**Kor.** Seien  $A \subseteq B \subseteq C$  Erweiterungen kommutativer Ringe. Ist  $B$  ganz über  $A$  und  $C$  ganz über  $B$ , so ist auch  $C$  ganz über  $A$ .

**Kor.** Der ganze Abschluss von  $A$  in  $B$  ist in  $B$  ganz abgeschlossen.

**Prop.** Sei  $A \subseteq B$  eine ganze Erweiterung komm. Ringe. Dann gilt:

- Für jedes Ideal  $\mathfrak{b} \subseteq B$  ist  $B/\mathfrak{b}$  ganz über  $A/(A \cap \mathfrak{b})$ .
- Für jede mult. abg. Teilmenge  $S \subseteq A$  ist  $S^{-1}B$  ganz über  $S^{-1}A$ .

**Prop** (**Noethernormalisierung**). Sei  $K$  ein Körper und  $\mathfrak{a}$  ein Ideal in  $A := K[x_1, \dots, x_n]$ . Dann gibt es algebraisch unabhängige Elemente  $y_1, \dots, y_n \in A$ , sodass  $A$  ganz über  $B := K[y_1, \dots, y_n]$  ist, und ein  $0 \leq r \leq n$  mit  $B \cap \mathfrak{a} = (y_{r+1}, \dots, y_n)$ .

*Beweis.* Per Ind. über  $n$ . Der Fall  $n = 0$  ist trivial. Sei nun  $n > 0$ .

- Falls  $\mathfrak{a} = (0)$ , so setze  $y_1 = x_1, \dots, y_n = x_n$  und  $r := n$ .

- Ansonsten wähle ein Polynom  $f = \sum_{\alpha \in M} \lambda_\alpha x^\alpha \in \mathfrak{a} \setminus \{0\}$ , wobei  $M \subset \mathbb{N}^n$  endlich ist mit  $\lambda_\alpha \in K^\times$  für alle  $\alpha \in M$ .
- Wähle  $w_1, \dots, w_{n-1} \in \mathbb{N}$  und  $w_n := 1$ , sodass die Abbildung

$$w : M \rightarrow \mathbb{N}, \quad \alpha \mapsto \alpha \cdot w := \alpha_1 w_1 + \dots + \alpha_n w_n$$

injektiv ist. (Dies kann man etwa erreichen, indem man die Tupel in  $M$  als Zahlen in einem Stellenwertsystem mit genügend großer Basis  $b := 1 + \max_{\alpha \in M} \max_{i=1, \dots, n} \alpha_i$  ansieht und  $w_i := b^{n-i}$  setzt.)

- Setze  $z_i = x_i - x_n^{w_i}$  für  $i = 1, \dots, n-1$  und  $A' := K[z_1, \dots, z_{n-1}]$ .
- Dann kann man  $f$  im Polynomring  $K[z_1, \dots, z_{n-1}, x_n] = A'[x_n]$ ,

$$f = \sum_{\alpha \in M} \lambda_\alpha (z_1 + x_n^{w_1})^{\alpha_1} \dots (z_{n-1} + x_n^{w_{n-1}})^{\alpha_{n-1}} \cdot x_n^{\alpha_n},$$

auch schreiben als  $f = \lambda_\beta \cdot x_n^m + \mu_1 \cdot x_n^{m-1} + \dots + \mu_m$ , wobei  $\beta := \arg \max_{\alpha \in M} w(\alpha)$ ,  $m := w(\beta)$  und  $\mu_i \in K[z_1, \dots, z_{n-1}]$ .

Somit sind  $x_n$  und alle weiteren  $x_i$ , also  $A$ , ganz über  $A'[f]$ .

- Setze  $y_n := f$ . Die IH, angewendet auf  $A' := K[z_1, \dots, z_{n-1}]$ , liefert algebraisch unabhängige  $y_1, \dots, y_{n-1} \in A' \subset A$  mit  $A'$  ganz über  $B' := K[y_1, \dots, y_{n-1}]$  und  $0 \leq r \leq n-1$  mit  $B' \cap \mathfrak{a} = (y_{r+1}, \dots, y_{n-1})$ . Dann sind  $B = B'[y_n] \subseteq A'[y_n] \subseteq A$  ganze Körpererweiterungen und  $B \cap \mathfrak{a} = (y_{r+1}, \dots, y_n)$ .  $\square$

*Bem.* Insbesondere ist  $K[y_1, \dots, y_r] \rightarrow A/\mathfrak{a}$  ein endlicher injektiver Homomorphismus von  $K$ -Algebren.

## Die Cohen-Seidenbergsche Sätze

**Prop.** Sei  $A \subseteq B$  eine ganze Erweiterung von Integritätsbereichen. Dann ist  $B$  genau dann ein Körper, wenn  $A$  ein Körper ist.

**Prop.** Sei  $A \subseteq B$  eine ganze Erweiterung komm. Ringe. Dann gilt:

- Ein Primideal  $\mathfrak{q} \subset B$  ist maximal  $\iff A \cap \mathfrak{q} \subset A$  ist maximal.
- Für Primideale  $\mathfrak{q} \subseteq \mathfrak{q}' \subseteq B$  gilt  $A \cap \mathfrak{q} = A \cap \mathfrak{q}' \iff \mathfrak{q} = \mathfrak{q}'$ .
- Für jedes Primideal  $\mathfrak{p} \subset A$  ex. ein Primideal  $\mathfrak{q} \subset B$  mit  $A \cap \mathfrak{q} = \mathfrak{p}$ .

**Satz** („**Going up**“). Sei  $A \subseteq B$  eine ganze Erw. komm. Ringe. Sei  $\mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$  eine Kette von Primidealen in  $A$  und  $\mathfrak{q}_1 \subset B$  ein Primideal mit  $A \cap \mathfrak{q}_1 = \mathfrak{p}_1$ . Dann gibt es eine Kette  $\mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_n$  von Primidealen in  $B$  mit  $A \cap \mathfrak{q}_i = \mathfrak{p}_i$  für  $i = 1, \dots, n$ .

**Prop.** Sei  $A \subseteq B$  eine Erweiterung komm. Ringe,  $C$  der ganze Abschluss von  $A$  in  $B$  und  $S \subseteq A$  multiplikativ abgeschlossen. Dann ist  $S^{-1}C$  der ganze Abschluss von  $S^{-1}A$  in  $S^{-1}C$ .

**Def.** Ein Integritätsbereich heißt **ganz abgeschlossen**, falls er in seinem Quotientenkörper ganz abgeschlossen ist.

**Bspe.**  $\mathbb{Z}$  und  $K[x_1, \dots, x_n]$  sind ganz abgeschlossen

**Prop.** Sei  $A$  ein Integritätsbereich. Dann sind äquivalent:

- $A$  ist ganz abgeschlossen.
- Für jedes Primideal  $\mathfrak{p} \subset A$  ist  $A_{\mathfrak{p}}$  ganz abgeschlossen.
- Für jedes maximale Ideal  $\mathfrak{m} \subset A$  ist  $A_{\mathfrak{m}}$  ganz abgeschlossen.

**Def.** Sei  $A \subseteq B$  eine Erweiterung komm. Ringe und  $\mathfrak{a} \subseteq A$  ein Ideal.

- Ein Element  $x \in B$  heißt **ganz** über  $\mathfrak{a}$ , falls  $x$  eine Gleichung der Form  $x^n + a_1 x^{n-1} + \dots + a_n = 0$  mit  $a_i \in \mathfrak{a}$  erfüllt.
- Der **ganze Abschluss** von  $\mathfrak{a}$  in  $B$  ist  $\{x \in B \mid x \text{ ist ganz über } \mathfrak{a}\}$ .

**Lem.** Sei  $A \subseteq B$  eine Erweiterung kommutativer Ringe,  $\mathfrak{a} \subseteq A$  ein Ideal und  $C$  der ganze Abschluss von  $A$  in  $B$ . Dann ist  $\sqrt{C}\mathfrak{a}$  der ganze Abschluss von  $\mathfrak{a}$  in  $B$ .

**Def.** Sei  $K \subseteq L$  eine Körpererweiterung. Ein Element  $x \in L$  heißt **algebraisch**, wenn es ganz über  $K$  ist.

**Prop.** Sei  $A \subseteq B$  eine Erweiterung von Integritätsbereichen. Sei  $A$  ganz abgeschlossen mit Quotientenkörper  $K$ . Sei  $x \in B$  ganz über einem Ideal  $\mathfrak{a} \subseteq A$ . Dann ist  $x$  algebraisch über  $K$  und für sein Minimalpolynom  $f \in K[t]$  gilt  $f \in \sqrt{\mathfrak{a}}[t]$ .

**Satz** („**Going down**“). Sei  $A \subseteq B$  eine ganze Erw. von Integritätsbereichen und  $A$  ganz abgeschlossen. Sei  $\mathfrak{p}_1 \supseteq \dots \supseteq \mathfrak{p}_n$  eine Kette von Primidealen in  $A$  und  $\mathfrak{q}_1 \subset B$  ein Primideal mit  $A \cap \mathfrak{q}_1 = \mathfrak{p}_1$ . Dann gibt es eine Kette  $\mathfrak{q}_1 \supseteq \dots \supseteq \mathfrak{q}_n$  von Primidealen in  $B$  mit  $A \cap \mathfrak{q}_i = \mathfrak{p}_i$  für  $i = 1, \dots, n$ .

**Prop.** Sei  $A$  ein ganz abgeschl. Integritätsbereich mit Quotientenkörper  $K$ . Sei  $L \supseteq K$  eine endliche, separable Körpererweiterung und  $B$  der ganze Abschluss von  $A$  in  $L$ . Dann ex. eine Basis  $v_1, \dots, v_n$  von  $L$  über  $K$ , sodass  $B \subseteq Av_1 + \dots + Av_n$ .

## Bewertungsringe

**Def.** Ein Integritätsbereich  $B$  mit Quotientenkörper  $K$  heißt **Bewertungsbereich** für  $K$ , falls gilt:  $\forall x \in K^\times : x \in B \vee x^{-1} \in B$ .

**Prop.** Sei  $B$  ein Bewertungsring. Dann gilt:

- $B$  ist ein lokaler Ring mit maximalem Ideal  $\mathfrak{m} := B \setminus B^\times$ .
- $B$  ist ganz abgeschlossen.

**Satz.** Sei  $K$  ein Körper,  $L \supset K$  ein algebraisch abgeschlossener Körper und  $B \subseteq K$  ein Unterring. Sei  $\phi : B \rightarrow L$  ein nicht in  $K$  fortsetzbarer Ringhomomorphismus, d. h. ist  $\hat{\phi} : B' \rightarrow L$  ein Ringhomomorphismus definiert auf einem Unterring  $B' \subseteq K$  mit  $B' \supseteq B$  mit  $\hat{\phi}|_B = \phi$ , so gilt  $B = B'$ . Dann gilt:

- $B$  ist ein lokaler Ring mit max. Ideal  $\mathfrak{m} = \ker \phi$ .
- Sei  $x \in K^\times$ . Dann gilt  $\mathfrak{m}[x] \neq B[x]$  oder  $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$ .
- $B$  ist ein Bewertungsring für  $K$ .

**Kor.** Sei  $\bar{A} \subseteq K$  ein Unterring eines Körpers. Dann ist der ganze Abschluss  $\bar{A}$  von  $A$  in  $K$  der Schnitt aller Bewertungsringe  $B$  von  $K$  mit  $B \supseteq A$ .

**Prop.** Sei  $A \subseteq B$  eine endlich erzeugte Erweiterung von Integritätsbereichen. Sei  $v \in B \setminus \{0\}$ . Dann existiert ein  $u \in A \setminus \{0\}$  mit folgender Eigenschaft: Jeder Homomorphismus  $\phi : A \rightarrow L$  in einen algebraisch abgeschlossenen Körper  $L$  mit  $\phi(u) \neq 0$  kann zu einem Homomorphismus  $\psi : B \rightarrow L$  mit  $\psi(v) \neq 0$  fortgesetzt werden.

**Kor.** Ist eine endlich erzeugte  $K$ -Algebra  $B$  ein Körper, so ist  $B$  eine endliche algebraische Erweiterung von  $K$ .

**Kor** (Schwacher Hilbertscher Nullstellensatz). Ist  $\mathfrak{m}$  ein max. Ideal einer endl. erz.  $K$ -Algebra  $A$ , so ist  $A/\mathfrak{m}$  eine endl. alg. Erweiterung von  $K$ . Insb. ist  $A/\mathfrak{m} \cong K$ , falls  $K$  algebraisch abgeschlossen ist.



Kettenbedingungen

- Prop.** Sei  $X$  eine teilweise geordnete Menge. Dann sind äquivalent:
- Jede aufsteigende Folge  $x_1 \leq x_2 \leq \dots$  in  $X$  ist **stationär**, d. h. es existiert ein  $N \in \mathbb{N}$  mit  $x_n = x_N$  für alle  $n \geq N$ .
  - Jede nicht leere Teilmenge  $A \subseteq X$  besitzt ein maximales Element, d. h.  $\exists a \in A : \forall b \in A : a \leq b \implies a = b$ .

- Def.** Sei  $A$  ein Ring und  $M$  ein  $A$ -Modul.
- Ist jede bzgl. der Inklusion aufsteigende Folge  $N_1 \subseteq N_2 \subseteq \dots$  von Untermoduln von  $N$  stationär, so heißt  $M$  **noethersch**.
  - Ist jede bzgl. der Inklusion absteigende Folge  $N_1 \supseteq N_2 \supseteq \dots$  von Untermoduln von  $N$  stationär, so heißt  $M$  **artinsch**.

Bspe.	$A$	$M$	noethersch?	artinsch?
	$\mathbb{Z}$	irgendeine endl. Gruppe	✓	✓
	$\mathbb{Z}$	$\{x \in \mathbb{Q}/\mathbb{Z} \mid \text{ord}(x) = p^n\}$ mit $p$ prim	✗	✓
	$\mathbb{Z}$	$\{\frac{a}{b} \in \mathbb{Q} \text{ gekürzt} \mid b = p^n\}$	✗	✗

- Prop.** Sei  $A$  ein Ring. Ein  $A$ -Modul  $M$  ist genau dann noethersch, wenn alle seine Untermodule endlich erzeugt sind.
- Prop.** Sei  $A$  ein Ring und  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  eine kurze exakte Sequenz von  $A$ -Moduln. Dann gilt:
- $M$  noethersch  $\iff M', M''$  noethersch
  - $M$  artinsch  $\iff M', M''$  artinsch

**Kor.** Die endliche direkte Summe von noetherschen/artinschen  $A$ -Moduln ist noethersch/artinsch.

**Def.** Ein Ring  $A$  heißt **noethersch/artinsch**, falls er als Modul über sich selbst noethersch/artinsch ist.

*Bem.* Ein Ring ist genau dann noethersch/artinsch, wenn die Menge seiner Ideale die aufsteigende/absteigende Kettenbedingung erfüllt. Ein Ring ist genau dann noethersch, wenn all seine Ideale endlich erzeugt sind.

Bspe.	$A$	noethersch?	artinsch?
	$\mathbb{Z}$	✓	✗
	ein bel. HIB	✓	?
	$K[x]$	✓	✗
	$K[x_1, x_2, \dots]$	✗	✗

**Achtung.** Unterringe von noetherschen Ringen sind nicht unbedingt noethersch.

**Prop.** Ist  $A$  ein noetherscher Ring und  $M$  ein endlich erzeugter  $A$ -Modul, so ist  $M$  noethersch.

- Def.** Sei  $A$  ein Ring und  $M$  ein  $A$ -Modul.
- Eine **Untermodulkette** von  $M$  der Länge  $n$  ist eine Kette von Untermoduln der Form  $M_\bullet : M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_n = 0$ .
  - $M$  heißt **einfach**, falls  $M$  nur  $0$  und  $M$  als Untermoduln besitzt.
  - Eine Untermodulkette heißt **Kompositionsreihe**, wenn die Quotienten  $M_i/M_{i+1}$  jeweils einfach sind.

- Die **Länge**  $\ell(M) \in \mathbb{N} \cup \{\infty\}$  von  $M$  ist das Infimum aller Längen von Kompositionsreihen von  $M$ .

**Prop.** Sei  $A$  ein Ring und  $M$  ein  $A$ -Modul der Länge  $n := \ell(M) < \infty$ . Dann gilt:

- Für jeden echten Untermodul  $N \subsetneq M$  gilt  $\ell(N) < \ell(M)$ .
- Die Länge jeder Untermodulkette in  $M$  ist  $\leq \ell(M)$ .
- Jede Kompositionsreihe von  $M$  hat die Länge  $n$ .
- Jede Untermodulkette von  $M$  lässt sich zu einer Kompositionsreihe erweitern.

**Prop.** Sei  $A$  ein kommutativer Ring. Ein  $A$ -Modul  $M$  besitzt genau dann eine Kompositionsreihe, wenn  $M$  noethersch und artinsch ist.

**Def.** Ein  $A$ -Modul  $M$  heißt **von endlicher Länge**, wenn  $M$  noethersch und artinsch ist.

**Prop.** Sei  $A$  ein Ring. Die Länge ist eine additive Funktion auf  $\mathfrak{C} := \{A\text{-Moduln endlicher Länge}\}$ .

**Satz** (Jordan-Hölder). Sind  $M_\bullet$  und  $M'_\bullet$  zwei Kompositionsreihen eines  $A$ -Moduls  $M$  endlicher Länge  $n$ , so existiert eine Permutation  $\sigma \in S_n$  mit  $M_{i-1}/M_i \cong M'_{\sigma(i-1)}/M'_{\sigma(i)}$ .

- Prop.** Für einen VR  $V$  über einem Körper  $K$  sind äquivalent:
- $V$  ist endlich-dimensional.
  - $V$  ist von endlicher Länge.
  - $V$  ist noethersch.
  - $V$  ist artinsch.

**Kor.** Seien  $\mathfrak{m}_1, \dots, \mathfrak{m}_n$  maximale Ideale in einem kommutativen Ring mit  $(0) = \mathfrak{m}_1 \dots \mathfrak{m}_n$ . Dann ist  $A$  genau dann noethersch, wenn  $A$  artinsch ist.

Noethersche Ringe

**Prop.** Der Quotient  $A/\mathfrak{a}$  eines noetherschen Rings  $A$  ist noethersch.

**Kor.** Sei  $\phi : A \rightarrow B$  ein Ringhomo. Ist  $A$  noethersch, so auch  $\phi(A)$ .

**Prop.** Sei  $A \subseteq B$  eine endliche Erweiterung kommutativer Ringe. Ist  $A$  noethersch, so auch  $B$ .

**Bsp.**  $\mathbb{Z}[i]$  ist noethersch als endl. Erw. von  $\mathbb{Z}$

**Prop.** Sei  $A$  ein kommutativer noetherscher Ring und  $S \subseteq A$  multiplikativ abgeschlossen. Dann ist  $S^{-1}A$  noethersch.

**Kor.** Die Halme  $A_{\mathfrak{p}}$  eines komm. noeth. Rings  $A$  sind noethersch.

**Satz** (**Hilbertscher Basissatz**). Ist  $A$  ein noetherscher kommutativer Ring, so ist auch der Polynomring  $A[x]$  noethersch.

**Kor.** Ist  $A$  ein noetherscher kommutativer Ring, so ist auch der Polynomring  $A[x_1, \dots, x_n]$  noethersch. Allgemeiner ist jede endlich erzeugte  $A$ -Algebra noethersch.

**Prop.** Seien  $A \subseteq B \subseteq C$  Erweiterungen von kommutativen Ringen. Sei  $A$  noethersch. Sei  $C$  endlich erzeugt als  $A$ -Algebra und endlich als  $B$ -Algebra. Dann ist  $B$  endlich erzeugt als  $A$ -Algebra.

**Def.** Sei  $A$  ein komm. Ring. Ein Ideal  $\mathfrak{a} \subseteq A$  heißt **irreduzibel**, falls für je zwei Ideale  $\mathfrak{b}, \mathfrak{c} \subseteq A$  gilt: Ist  $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ , so gilt  $\mathfrak{a} \in \{\mathfrak{b}, \mathfrak{c}\}$ .

**Prop.** Sei  $A$  ein noetherscher kommutativer Ring. Dann gilt:

- Jedes Ideal von  $A$  ist Schnitt von endlich vielen irred. Idealen.
- Jedes irreduzible Ideal von  $A$  ist ein Primärideal.
- Folglich ist in  $A$  jedes Ideal zerlegbar.
- Jedes Ideal  $\mathfrak{a} \subseteq A$  enthält eine Potenz  $(\sqrt{\mathfrak{a}})^n$  seines Wurzelideals.
- Insbesondere ist  $\sqrt{(0)} \subseteq A$  nilpotent.
- Für ein max. Ideal  $\mathfrak{m} \subset A$  und ein Ideal  $\mathfrak{q} \subseteq A$  sind äquivalent:
  - $\mathfrak{q}$  ist ein  $\mathfrak{m}$ -primäres Ideal.
  - $\sqrt{\mathfrak{q}} = \mathfrak{m}$
  - $\exists n \in \mathbb{N} : \mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$
- Die zu einem Ideal  $\mathfrak{a} \subseteq A$  assoziierten Ideale sind genau die Primideale von  $A$  der Form  $(\mathfrak{a} : x)$  mit  $x \in A$ .

## Artinsche Ringe

**Prop.** Sei  $A$  ein artinscher kommutativer Ring. Dann gilt:

- Jedes Primideal  $\mathfrak{p} \subset A$  ist ein maximales Ideal.
- Das Nilradikal ist gleich dem Jacobsonschen Ideal.
- $A$  besitzt nur endlich viele maximale Ideale (d.h.  $A$  ist halblokal).
- Das Nilradikal von  $A$  ist nilpotent.

**Def.** Sei  $A$  ein komm. Ring. Eine **Primidealkette** der Länge  $n$  in  $A$  ist eine Kette  $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$  von Primidealen in  $A$ .

**Def.** Die **Dimension**  $\dim A \in \{-\infty\} \cup \mathbb{N}$  eines komm. Ringes  $A$  ist das Supremum über die Längen aller Primidealketten in  $A$ .

**Bspe.** •  $\dim A \geq 0 \iff A \neq 0$  •  $\dim K = 0$  •  $\dim \mathbb{Z} = 1$

**Satz.** Für einen kommutativen Ring  $A \neq 0$  gilt:

$$A \text{ ist artinsch} \iff A \text{ ist noethersch und } \dim A = 0$$

*Bem.* Ist  $(A, \mathfrak{m})$  ein artinscher lokaler Ring, so ist  $\mathfrak{m}$  das einzige Primideal von  $A$  und damit  $\sqrt{(0)} = \mathfrak{m}$ . Insbesondere ist  $\mathfrak{m}$  nilpotent und jedes Element von  $A$  entweder nilpotent oder eine Einheit.

**Prop.** Sei  $(A, \mathfrak{m})$  ein noetherscher lokaler Ring. Dann tritt genau einer der folgenden Fälle ein:

- Für alle  $n \in \mathbb{N}$  ist  $\mathfrak{m}^n \supsetneq \mathfrak{m}^{n+1}$ .
- Es ist  $\mathfrak{m}^n = (0)$  für ein  $n \in \mathbb{N}$  und  $A$  ist artinsch.

**Satz (Struktursatz** für artinsche kommutative Ringe). Jeder artinsche kommutative Ring ist eindeutig (bis auf Isomorphie der Faktoren) ein direktes Produkt artinscher lokaler Ringe.

**Def.** Sei  $(A, \mathfrak{m}, F)$  ein lokaler Ring. Dann heißt der  $F$ -Vektorraum  $\mathfrak{m}/\mathfrak{m}^2$  **Zariskischer Kotangentenraum** von  $A$ .

*Bem.*  $\mathfrak{m}/\mathfrak{m}^2$  ist die spezielle Faser von  $\mathfrak{m}$  als  $A$ -Modul. Ist  $\mathfrak{m}$  als  $A$ -Modul endlich erzeugt, so auch  $\mathfrak{m}/\mathfrak{m}^2$  als  $F$ -Vektorraum.

**Prop.** Für einen artinschen lokalen Ring  $(A, \mathfrak{m}, F)$  sind äquivalent:

- Jedes Ideal in  $A$  ist ein Hauptideal (also  $A$  ein HIB).
- Das maximale Ideal  $\mathfrak{m}$  ist ein Hauptideal.
- Es gilt  $\dim_F \mathfrak{m}/\mathfrak{m}^2 \leq 1$ .

**Bspe.** Artinsche lokale Ringe sind:

- $\mathbb{Z}/(p^n)$ , wobei  $p$  prim ist
- $K[x]/(f^n)$ , wobei  $f$  irreduzibel ist

## Diskrete Bewertungsringe

**Prop.** Sei  $A$  ein eindimensionaler noetherscher Integritätsbereich. Dann kann jedes Ideal  $0 \subsetneq \mathfrak{a} \subseteq A$  eindeutig als Produkt von primären Idealen mit paarweise verschiedenen Wurzelidealen geschrieben werden.

**Def.** Eine **diskrete Bewertung** auf einem Körper  $K$  ist eine surjektive Abbildung  $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ , für die gilt:

$$\nu^{-1}(\infty) = \{0\}, \quad \nu(xy) = \nu(x) + \nu(y), \quad \nu(x+y) \geq \min(\nu(x), \nu(y)).$$

**Lem.** •  $\nu(1) = 0$  •  $\nu(x^{-1}) = -\nu(x)$

**Def.** Der **Bewertungsring** von  $K$  (zu  $\nu$ ) ist der Unterring

$$\{x \in K \mid \nu(x) \geq 0\} \subset K.$$

**Lem.** Der Bewertungsring von  $K$  zu  $\nu$  ist in der Tat ein solcher.

**Def.** Ein Integritätsbereich  $A$  heißt **diskreter Bewertungsring**, falls  $A$  der Bewertungsring einer diskreten Bewertung auf dem Quotientenkörper  $K$  von  $A$  ist.

**Prop.** Sei  $A$  ein diskreter Bewertungsring mit Bewertung  $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ . Dann gilt:

- $x \in A^\times \iff \nu(x) = 0$  •  $\nu(x) = \nu(y) \iff (x) = (y)$
- $A$  ist ein lokaler Ring mit max. Ideal  $\mathfrak{m} := \{x \in A \mid \nu(x) > 0\}$ .
- Jedes Ideal in  $A$  hat die Form  $\mathfrak{m}_k = \nu^{-1}([k, \infty])$  mit  $k \in \mathbb{N} \cup \{\infty\}$ .
- $A$  ist noethersch. •  $A$  ist eindimensional.
- Jedes nichtverschwindende Ideal in  $A$  ist eine Potenz von  $\mathfrak{m}$ .

**Bspe.** • Sei  $p$  eine Primzahl. Jedes  $y \in \mathbb{Q}^\times$  kann man als  $y = p^n \frac{s}{t}$  mit  $p \nmid s, p \nmid t$  schreiben. Dabei ist  $n = n_y \in \mathbb{Z}$  eindeutig festgelegt. Setze  $\nu(x) := n_y$  und  $\nu(0) := \infty$ . Dann ist  $\nu$  eine Bewertung auf  $\mathbb{Q}$  mit Bewertungsring  $\mathbb{Z}_{(p)}$ .

- Sei  $F$  ein Körper und  $F(x) := \{\frac{h}{g} \mid h, g \in F[x], g \neq 0\}$  der Körper der rationalen Fktn über  $F$  in  $x$ . Sei  $f \in F[x]$  irreduzibel. Jedes  $y \in F(x)^\times$  kann man als  $y = f^n \frac{h}{g}$  mit  $p \nmid h, p \nmid g$  schreiben. Dabei ist  $n = n_y \in \mathbb{Z}$  eind. festgelegt. Setze  $\nu(x) := n_y$  und  $\nu(0) := \infty$ . Dann ist  $\nu$  eine Bewertung auf  $F(x)$  mit Bewertungsring  $F[x]_{(f)}$ .

**Prop.** Sei  $(A, \mathfrak{m}, F)$  ein eindimensionaler noetherscher lokaler Integritätsbereich. Dann sind äquivalent:

- $A$  ist ein diskreter Bewertungsring. •  $\mathfrak{m}$  ist ein Hauptideal.
- $A$  ist ganz abgeschlossen. •  $\dim_F \mathfrak{m}/\mathfrak{m}^2 = 1$
- Jedes (nicht verschwindende) Ideal von  $A$  ist eine Potenz von  $\mathfrak{m}$ .
- $\exists x \in A : \forall \text{ Ideal } \mathfrak{a} \subseteq A : \exists n \in \mathbb{N} : \mathfrak{a} = (x^n)$

## Dedekindsche Bereiche

**Lem/Def.** Ein eindim. noetherscher Integritätsbereich  $A$  heißt **Dedekindscher Bereich**, wenn er die folgenden äquivalenten Bedingungen erfüllt:

- $A$  ist ganz abgeschlossen.
- Jedes Primärideal in  $A$  ist Potenz eines Primideals.
- Für jedes Primideal  $\mathfrak{p} \neq (0)$  ist  $A_{\mathfrak{p}}$  ein disk. Bewertungsbereich.

**Kor.** In einem Dedekindschen Bereich lässt sich jedes Ideal  $\mathfrak{a} \neq (0)$  als eindeutiges Produkt von Primidealen schreiben.

**Bsp.** Jeder HIB ist ein Dedekindscher Bereich.

**Satz.** Sei  $K$  ein Zahlkörper, also eine endliche Erweiterung von  $\mathbb{Q}$ . Dann ist der Ring der ganzen Zahlen in  $K$ , d.h. der ganze Abschluss von  $\mathbb{Z}$ , ein Dedekindscher Bereich.

# Gebrochene und invertierbare Ideale

Sei  $A$  ein Integritätsbereich mit Quotientenkörper  $K$ .

**Def.** Ein  $A$ -Untermodul  $\mathfrak{r} \subseteq K$  heißt **gebrochenes Ideal** von  $A$ , falls ein  $x \in A$  mit  $x\mathfrak{r} \subseteq A$  existiert.

**Bspe.** • Jedes gewöhnliche Ideal ist auch ein gebrochenes Ideal.  
• Jedes  $u = \frac{s}{t} \in K$  erz. ein gebr. Ideal  $(u) := Au \subseteq K$ , da  $t(u) \subset A$ .

**Sprechweise.** Zur Unterscheidung von gebrochenen Idealen werden gewöhnliche Ideale auch **ganze Ideale** genannt.

**Prop.** • Ist  $\mathfrak{r}$  ein endlich erzeugtes Untermodul von  $K$ , so ist  $\mathfrak{r}$  ein gebrochenes Ideal.  
• Ist  $A$  noethersch, so ist jedes gebrochene Ideal  $\mathfrak{r}$  als  $A$ -Modul endlich erzeugt.

**Def.** Ein  $A$ -Untermodul  $\mathfrak{r} \subseteq K$  heißt **invertierbares Ideal**, falls ein  $A$ -Untermodul  $\mathfrak{s} \subseteq K$  mit  $\mathfrak{r}\mathfrak{s} = A$  existiert.

**Notation.** Für ein  $A$ -Untermodul  $\mathfrak{r} \subseteq K$  schreiben wir  $(1 : \mathfrak{r}) := \{x \in K \mid x\mathfrak{r} \subseteq A\}$ . Dies ist ein  $A$ -Untermodul von  $K$ .

**Prop.** Ist  $\mathfrak{r} \subseteq K$  ein invertierbares Ideal, so ist  $\mathfrak{s} = (1 : \mathfrak{r})$  das einzige  $A$ -Untermodul  $\mathfrak{s} \subseteq K$  mit  $\mathfrak{r}\mathfrak{s} = A$ .

**Notation.** In diesem Fall:  $\mathfrak{r}^{-1} := (1 : \mathfrak{r})$

**Prop.** Jedes invertierbare Ideal von  $A$  ist endlich erzeugt als  $A$ -Modul und damit insbesondere ein gebrochenes Ideal.

**Bsp.** Für  $u \in K^\times$  ist  $(u) \subseteq K$  invertierbar mit  $(u)^{-1} = (u^{-1})$ .

*Bem.* Bezüglich der Multiplikation von Idealen bilden die invertierbaren Ideale von  $A$  eine Gruppe mit  $e = (1)$ .

**Prop.** Für ein gebrochenes Ideal  $\mathfrak{r}$  von  $A$  sind äquivalent:

- $\mathfrak{r}$  ist invertierbar
- $\mathfrak{r}$  ist endlich erzeugt und für alle Primideale  $\mathfrak{p} \subset A$  ist  $\mathfrak{r}_{\mathfrak{p}}$  ein invertierbares Ideal von  $A_{\mathfrak{p}}$ .
- $\mathfrak{r}$  ist endlich erzeugt und für alle maximalen Ideale  $\mathfrak{m} \subset A$  ist  $\mathfrak{r}_{\mathfrak{m}}$  ein invertierbares Ideal von  $A_{\mathfrak{m}}$ .

**Prop.** Ein lokaler Integritätsbereich, der kein Körper ist, ist genau dann ein diskreter Bewertungsring, wenn jedes nicht verschwindende gebrochene Ideal invertierbar ist.

**Satz.** Ein Integritätsbereich, der kein Körper ist, ist genau dann ein Dedekindscher Bereich, wenn jedes nicht verschwindende gebrochene Ideal invertierbar ist.

**Kor.** In einem Dedekindschen Bereich  $A$  bilden die nicht verschwindenden gebrochenen Ideale eine abelsche Gruppe bzgl. der Multiplikation, die **Idealgruppe**  $I(A)$  von  $A$ .

*Bem.* Der Satz über die eindeutige Faktorisierbarkeit eines Ideals in Primideale in einem Dedekindschen Bereich  $A$  impliziert, dass  $I(A)$  von den Primidealen von  $A$  frei abelsch erzeugt wird.

**Def.** Sei  $A$  ein Dedekindscher Bereich mit Quotientenkörper  $K$ .

*Bem.* Es gibt einen Gruppenhomomorphismus

$$\phi : K^\times \rightarrow I(A), \quad x \mapsto (x),$$

dessen Bild die gebrochenen Hauptideale sind. Dessen Kern ist

$$\ker \phi = \{u \in K^\times \mid (u) = 1\} = A^\times.$$

**Def.**  $C(A) := I(A)/\text{im}(\phi)$  heißt **Idealklassengruppe** von  $A$ .

*Bem.* Es gibt eine exakte Sequenz

$$1 \rightarrow A^\times = \ker(\phi) \rightarrow K^\times \xrightarrow{\phi} I(A) \rightarrow C(A) \rightarrow 1$$

von (multiplikativ notierten) abelschen Gruppen.

*Bem.* Sei  $K$  ein Zahlkörper und  $A$  sein Ring ganzer Zahlen. Man kann dann zeigen:

- $C(A)$  ist endlich. Die Gruppenordnung  $\text{ord } C(A)$  heißt *Klassenzahl* von  $K$ .
- $\text{ord } C(A) = 1 \iff$  jedes invertierbare Ideal ist ein gebrochenes Hauptideal  $\iff A$  ist ein faktorieller Ring.
- $A^\times$  ist eine endlich erzeugte abelsche Gruppe. Die Elemente endlicher Ordnung sind genau die Einheitswurzeln  $\mu(K)$  von  $K$ . Der Rang der freien abelschen Gruppe  $A^\times/\mu(K)$  ist  $r_1 + r_2 - 1$ , wobei  $r_1$  die Anzahl der reellen und  $2r_2$  die Anzahl der echt komplexen Einbettungen von  $K$  in  $\mathbb{C}$  ist.

**Bspe.** •  $\mathbb{Q}(\sqrt{-1})$  besitzt genau zwei echt komplexe Einbettungen, keine reellen. Für dessen Ring der ganzen Zahlen,  $A = \mathbb{Z}[i]$ , gilt damit  $\text{ord}(A^\times/\mu(K)) = 0$ , also  $A^\times = \mu(K) = \{\pm 1, \pm i\}$ .  
•  $\mathbb{Q}(\sqrt{2})$  besitzt genau zwei reelle Einbettungen, keine echt komplexen. Für  $A = \mathbb{Z}[\sqrt{2}]$  gilt damit  $\text{ord}(A^\times/\mu(K)) = 1$ . Es ist  $\mu(K) = \{\pm 1\}$  und  $A^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$ .