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 $+, \cdot : A \times A \to A$ 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.

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

Bspe. • \mathbb{Z} , • $K[x_1,\ldots,x_n]$, • **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. \bullet $\mathbb{Z} \subset \mathbb{Q}$, \bullet $K \subset K[X]$

Def. Ein Ringhomomorphismus $\phi: A \to B$ ist eine Abbildung, welche sowohl ein Gruppenhomomor. $(A, +_A, 0_A) \to (B, +_B, 0_B)$ als auch ein Ringhomomorphismus $(A, \cdot_A, 1_A) \to (B, \cdot_B, 1_B)$ 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 Aim Folgenden Ringe und $\phi:A\to B$ 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

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

Notation. $(x_1, \ldots, x_n) \subseteq A$ ist das von $\{x_1, \ldots, x_n\}$ 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 ϕ .

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

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

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

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:

Prop (Homomorphiesatz). Sei $\phi: A \to B$ ein Ringhomomor. Dann ist $\phi: A/\ker(\phi) \to \operatorname{im}(\phi), \ [x] \mapsto \phi(x)$ 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!

 $Bem.\ {\rm Ein}\ {\rm Ring}\ A$ ist genau dann ein Integritätsbereich, wenn

$$0 \neq 1$$
 in A und $\forall x, y \in : xy = 0 \implies x = 0 \lor y = 0$.

Beob. Sei $\phi:A\to B$ 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. \bullet \mathbb{Z} , \bullet K[x]

Gegenbsp. • $K[x_1, \ldots, x_n]$ für $n \ge 2$

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

Beob. 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. $A^{\times} := \{$ 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**.

Beob. • $x \in A$ ist eine Einheit \iff $(x) = (1) \iff A/(x) = 0$

• Einheiten sind regulär.

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

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

Def. • Ein Ideal $\mathfrak{p} \subset A$ heißt **Primideal**, falls $1 \not\in \mathfrak{p}$ und $\forall a, b \in A : ab \in \mathfrak{p} \implies a \in \mathfrak{p} \lor b \in \mathfrak{p}$.

Ein Ideal m ⊂ A heißt maximal, falls für jedes Ideal p ⊆ a ⊆ A entweder p = a oder 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 $f \in K[x_1, \ldots, x_n]$ ein irred. Polynom. Dann ist (f) prim.

 $\begin{array}{lll} \textbf{Lem.} & \mathfrak{p} \subseteq A \text{ ist prim} & \iff & A/\mathfrak{p} \text{ ist ein Integritätsbereich} \\ & \mathfrak{m} \subseteq A \text{ ist maximal} & \iff & A/\mathfrak{m} \text{ ist ein K\"{o}rper} \\ \end{array}$

Kor. Maximale Ideale sind prim.

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

```
 \{ \text{ Primideale } \mathfrak{p} \subseteq A \text{ mit } \mathfrak{p} \supseteq \mathfrak{a} \ \} \quad \leftrightarrow \quad \{ \text{ Primideale } \mathfrak{q} \subseteq A/\mathfrak{a} \ \}   \qquad \qquad \mathfrak{p} \quad \mapsto \quad \pi(\mathfrak{p})   \qquad \qquad \pi^{-1}(\mathfrak{q}) \quad \leftrightarrow \quad \mathfrak{q}
```

Genauso bekommt man eine bijektive, monotone Korrespondenz $\{ \text{ max. Ideale } \mathfrak{m} \subseteq A \text{ mit } \mathfrak{m} \supset \mathfrak{a} \} \leftrightarrow \{ \text{ max. Ideale } \mathfrak{n} \subseteq A/\mathfrak{a} \}$

The District of the state of th

 ${\bf Prop.}\,$ 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 ∈ 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 $F \coloneqq A/\mathfrak{m}$ 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 $\mathfrak{n} := \{ \text{ nilpotente Elemente } \} \subseteq A \text{ ist ein Ideal, das sogenannte Nilradikal.}$

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 i $\subset A$ ist der Schnitt aller maximalen Ideale von A.

Prop. Ein Element $x \in A$ liegt genau dann im Jacobsonschen Ideal i, 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

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

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

Beob.
$$(x_1) + \ldots + (x_n) = (x_1, \ldots, x_n)$$

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

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

Beob. •
$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$$
, • $(x_1) \cdot \ldots \cdot (x_n) = (x_1 \cdot \ldots \cdot x_n)$

Bsp. In $A = \mathbb{Z}$ gilt für $m, n \in \mathbb{N}$

•
$$(m) + (n) = (m, n) = (ggT(m, n)),$$
 • $(m) \cap (n) = (kgV(m, n)).$

Beob. • Summe, Schnitt und Produkt von Idealen sind assoziativ.

- Summe und Schnitt sind kommutativ. Das Produkt von Idealen ist kommutativ, wenn der Ring kommutativ ist.
- Distributivgesetz: $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$
- Modularitätsgesetz: Ist $\mathfrak{a} \supset \mathfrak{b}$ oder $\mathfrak{a} \supset \mathfrak{c}$, 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 ggT $(m, n) = 1$

Prop. Seien $\mathfrak{a}_1, \ldots \mathfrak{a}_n \subseteq A$ paarweise koprime 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 $\prod_{i \in I} A_i \coloneqq \{(a_i \in A_i)_{i \in I}\}$ mit kmpnntnwsr Verknüpfung.

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

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

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

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

Bem. Der Ringhomomor. ϕ ist genau dann injektiv, wenn $\bigcap_{i=1}^{n} a_i = 0$.

Prop. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq A$ Primideale und $\mathfrak{a} \subseteq A$ ein Ideal. Gilt $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, so gibt es ein $j \in \{1, \dots, n\}$ mit $\mathfrak{a} \subseteq \mathfrak{p}_j$.

Prop. Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ Ideale und $\mathfrak{p} \subseteq A$ ein Primideal Gilt $\mathfrak{p} \supseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$, so gibt es ein $j \in \{1, \ldots, n\}$ 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. •
$$(x : \mathfrak{b}) := ((x) : \mathfrak{b}),$$
 • $(\mathfrak{a} : y) := (\mathfrak{a} : (y))$

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

$$\begin{array}{llll} \mathbf{Lem.} & \bullet & \mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b}) & \bullet & (\mathfrak{a} : \mathfrak{b}) \mathfrak{b} \subseteq \mathfrak{a} & \bullet & ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b} \mathfrak{c}) \\ \bullet & (\bigcap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i \in I} (\mathfrak{a}_i : \mathfrak{b}) & \bullet & (\mathfrak{a} : \sum_{i \in I} \mathfrak{b}) = \bigcap_{i \in I} (\mathfrak{a} : \mathfrak{b}_i) \\ \end{array}$$

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 $\pi: A \to A/\mathfrak{a}, x \mapsto [x]$

Lem. •
$$\sqrt{\mathfrak{a}} \supseteq \mathfrak{a}$$
 • $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$ für $n \ge 1$ • $\sqrt{\mathfrak{a}} = (1) \iff \mathfrak{a} = (1)$
• $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$ • $\sqrt{\mathfrak{ab}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$ • $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$

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

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

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

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

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

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

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

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

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

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

Prop. Sei $\phi: A \to B$ ein Homomorphismus komm. Ringe. Die Erweiterung und Kontraktion von Idealen (bzgl. ϕ) 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

$$\mathfrak{a} \subseteq A \cap (B\mathfrak{a})$$
 und $\mathfrak{b} \supset B(A \cap \mathfrak{b})$.

Außerdem folgt aus den Eigenschaften einer Galois-Verbindung, dass

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

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

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