# Korrespondenzsatz für Ideale

**Satz (11.10)**

Sei $R$ ein Ring, $I$ ein Ideal und $\pi : R \to R/I$ der kanonische Epimorphismus. Sei $\bar{\mathcal{I}}$ die Menge der Ideale von $R/I$ und $\mathcal{I}_I$ die Menge der Ideale $J$ von $R$ mit $J \supseteq I$.

(i) Die Zuordnungen $\phi : \mathcal{I}_I \to \bar{\mathcal{I}}$, $J \mapsto \pi(J)$ und $\psi : \bar{\mathcal{I}} \to \mathcal{I}_I$, $\bar{J} \mapsto \pi^{-1}(J)$ sind bijektiv und zueinander invers.

(ii) Für alle Ideale $J, K \in \mathcal{I}_I$ gilt $J \subseteq K \Leftrightarrow \pi(J) \subseteq \pi(K)$.

# Körper als Faktorringe

## Lemma (11.11)

Ein Ring ist genau dann ein Körper, wenn (0) und (1) die einzigen Ideale des Rings sind und $(0) \neq (1)$ gilt.

## Satz (11.12)

Sei $R$ ein Ring, $\mathfrak{p} \subseteq R$ ein Ideal und $\bar{R} = R/\mathfrak{p}$.

(i) Genau dann ist $\mathfrak{p}$ ein Primideal, wenn $\bar{R}$ ein Integritätsbereich ist.

(ii) Genau dann ist $\mathfrak{p}$ ein maximales Ideal, wenn $\bar{R}$ ein Körper ist.

## Folgerung (11.13)

Jedes maximale Ideal ist ein Primideal.

Beweis von Lemma 11.11

Sei $R$ ein Ring. z.zg.:

$R$ ist Körper $\Longleftrightarrow$ $R$ hat genau zwei Ideale. und zwar $(0_R)$ und $(1_R)$

„$\Rightarrow$" Sei $I$ ein Ideal von $R$ mit $I \neq (0_R)$.

Sei $a \in I \setminus \{0_R\}$. $R$ ist Körper $\Rightarrow a \in R^\times$

$\Rightarrow 1_R = a^{-1} a \in I \Rightarrow (1_R) \subseteq I \Rightarrow I = (1_R)$

Ang. $(0_R) = (1_R)$. $\Rightarrow 1_R \in \{0_R\} \Rightarrow 1_R = 0_R$

$\Rightarrow R$ ist Nullring $\lightning$ (da Nullringe sind keine Körper)

„$\Leftarrow$" Unter der geg. Voraussetzung z.zg: $R^* = R \setminus \{0_R\}$

„$\subseteq$" Ang. $R^* \not\subseteq R \setminus \{0_R\}$. Dann gilt $0_R \in R^*$.

$\Rightarrow 1_R = 0_R^{-1} \cdot 0_R = 0_R \Rightarrow (1_R) = (0_R)$ $\lightning$

„$\supseteq$" Sei $a \in R \setminus \{0_R\}$ und $I = (a)$. Vor. $\Rightarrow I = (0_R)$ oder $I = (1_R)$. Dabei ist $I = (0_R)$ wegen $a \neq 0_R$, $a \in I$ ausgeschlossen. $\Rightarrow I = (1_R) \Rightarrow 1_R \in (a) \Rightarrow$
$\exists c \in R$ mit $1_R = ca \Rightarrow a \in R^*$. $\square$

Beweis von Satz 11.12

geg.: $R$ Ring, $\mathfrak{p}$ Ideal, $\bar{R} = R/\mathfrak{p}$

<u>zu (i)</u> z.zg.: $\mathfrak{p}$ ist Primideal $\Longleftrightarrow$ $\bar{R}$ ist ein Integritätsbereich

„$\Longrightarrow$" z.zg.: $0_{\bar{R}}$ ist einziger Nullteiler von $\bar{R}$

$0_{\bar{R}}$ ist Nullteiler, denn: $0_{\bar{R}} \cdot 1_{\bar{R}} = 0_{\bar{R}}$

Außerdem gilt $1_{\bar{R}} \neq 0_{\bar{R}}$, denn: Ang. $1_{\bar{R}} = 0_{\bar{R}}$

$\Rightarrow 1_R + \mathfrak{p} = \mathfrak{p} \Rightarrow 1_R \in \mathfrak{p} \Rightarrow \mathfrak{p} = (1_R)$

↯ da Primideale in $R$ ungleich $(1_R)$ sind

Ang. $\bar{a} \in \bar{R}$ ist Nullteiler, $\bar{a} \neq 0_{\bar{R}}$ $\Rightarrow$

$\exists\, \bar{b} \in \bar{R},\ \bar{b} \neq 0_{\bar{R}}$ mit $\bar{a} \cdot \bar{b} = 0_{\bar{R}}$

Seien $a, b \in R$ mit $\bar{a} = a + \mathfrak{p},\ \bar{b} = b + \mathfrak{p}$.

$\bar{a} \cdot \bar{b} = 0_{\bar{R}} \Rightarrow (a + \mathfrak{p}) \cdot (b + \mathfrak{p}) = \mathfrak{p}$

$\Rightarrow ab + \mathfrak{p} = \mathfrak{p} \Rightarrow ab \in \mathfrak{p}$

andererseits: $\bar{a} \neq 0_{\bar{R}} \Rightarrow a + \mathfrak{p} \neq \mathfrak{p} \Rightarrow a \notin \mathfrak{p}$

ebenso: $\bar{b} \neq 0_{\bar{R}} \Rightarrow b \notin \mathfrak{p}$

also: $ab \in \mathfrak{p}$, aber $a, b \notin \mathfrak{p}$ ↯ zu $\mathfrak{p}$ Primideal

„$\Leftarrow$" z.zg.: (1) $\mathfrak{p} \neq (1_R)$ (2) $\forall a, b \in R: ab \in \mathfrak{p}$
$\Rightarrow a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$

<u>zu (1)</u> Ang. $\mathfrak{p} = (1_R) \Rightarrow 1_R \in \mathfrak{p} \Rightarrow 1_R + \mathfrak{p} = \mathfrak{p}$
$\Rightarrow 1_{\bar{R}} = 0_{\bar{R}}$ ↯ da $\bar{R}$ Integritätsbereich

<u>zu (2)</u> Seien $a, b \in R$ mit $ab \in \mathfrak{p}$.

$ab \in \mathfrak{p} \Rightarrow ab + \mathfrak{p} = \mathfrak{p} \Rightarrow (a+\mathfrak{p})\cdot(b+\mathfrak{p}) = \mathfrak{p} = 0_{\bar{R}}$

$\bar{R}$ Int.-bereich $\Longrightarrow$ $a+\mathfrak{p} = 0_{\bar{R}} = \mathfrak{p}$ oder $b+\mathfrak{p} = \mathfrak{p}$ $\Longrightarrow$

$a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

zu (ii) z.zg. $\mathfrak{p}$ ist maximales Ideal $\Longleftrightarrow$ $\bar{R}$ ist Körper

„$\Longrightarrow$" $\mathfrak{p}$ maximal $\Rightarrow$ $\mathfrak{p} \subsetneq (1_R)$, aber es gibt kein Ideal $I$ von $R$ mit $\mathfrak{p} \subsetneq I \subsetneq (1_R)$ Korrespondenzsatz $\Longrightarrow$ Es gibt kein Ideal $\bar{I}$ von $\bar{R}$ mit $(0_{\bar{R}}) \subsetneq \bar{I} \subsetneq (1_{\bar{R}})$, und $(0_{\bar{R}}) \subsetneq (1_{\bar{R}})$, d.h. $\bar{R}$ hat genau zwei Ideale, $(0_{\bar{R}})$ und $(1_{\bar{R}})$ $\xRightarrow{\text{Lemma 11.11}}$ $\bar{R}$ ist Körper.

„$\Longleftarrow$" $\bar{R}$ ist Körper $\Rightarrow$ $(0_{\bar{R}}) \subsetneq (1_{\bar{R}})$, und es gibt kein Ideal $\bar{I}$ von $\bar{R}$ mit $(0_{\bar{R}}) \subsetneq \bar{I} \subsetneq (1_{\bar{R}})$. Korrespondenzsatz $\Longrightarrow$ $\exists$ kein Ideal $I$ in $R$ mit $\mathfrak{p} \subsetneq I \subsetneq (1_R)$ und $\mathfrak{p} \subsetneq (1_R)$ $\Rightarrow$ $\mathfrak{p}$ ist maximal. $\square$

# Übertragung von Verknüpfungen

## Lemma (11.14)

Seien $X$ und $Y$ Mengen, $\phi : Y \to X$ eine Bijektion und $\cdot$ eine Verknüpfung auf $X$. Wir definieren auf $Y$ eine Vernüpfung $\odot$, indem wir $a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b))$ für alle $a, b \in Y$ definieren. Die neue Verknüpfung $\odot$ hängt dann mit $\cdot$ auf folgende Weise zusammen.

(i) Ist die Verknüpfung $\cdot$ auf $X$ assoziativ bzw. kommutativ, dann gilt dasselbe jeweils für die Verknüpfung $\odot$ auf $Y$.

(ii) Ist $e_X \in X$ ein Neutralelement in $X$ bezüglich $\cdot$, dann ist $e_Y = \phi^{-1}(e_X)$ ein Neutralelement in $Y$ bezüglich $\odot$.

(iii) Seien $e_X$ und $e_Y$ wie in (ii) und $a, b \in X$. Ist $b$ ein Inverses von $a$ bezüglich $\cdot$, dann ist $\phi^{-1}(b)$ ein Inverses von $\phi^{-1}(a)$ bezüglich $\odot$.

# Übertragung einer Ringstruktur

**Satz (11.15)**

Sei $(R, +, \cdot)$ ein Ring, $S$ eine Menge und $\phi : S \to R$ eine bijektive Abbildung. Seien die Verknüpfungen $\oplus$ und $\odot$ auf $S$ definiert durch

$$a \oplus b = \phi^{-1}(\phi(a) + \phi(b)) \qquad \text{und} \qquad a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b)).$$

Dann ist $(S, \oplus, \odot)$ ein Ring, und $\phi$ ist ein Isomorphismus von Ringen.

# Konstruktion von Ringerweiterungen

## Satz (11.16)

Sei $\phi : R \to S$ ein Monomorphismus von Ringen. Dann gibt es einen Erweiterungsring $\hat{R} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$.

Anwendung:
Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen

Beweis von Satz 11.16 (Skizze)

$$\begin{tikzcd} \hat{R} \arrow[r, "\hat{\phi}", "\sim"'] & S \\ R \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\phi"] & \phi(R) \arrow[u, phantom, sloped, "\subseteq"] \end{tikzcd}$$

geg.: injektiver Ringhomomorphismus $\phi : R \to S$

zzg. Es gibt einen Erweiterungsring $\hat{R}$ von $R$ und ein Isomorphismus $(\sim)$ $\hat{\phi} : \hat{R} \to S$ von Ringen mit der Eigenschaft $\hat{\phi}|_R = \phi$

Setze $\hat{R} = \big(S \setminus \phi(R)\big) \cup R$. Dann gilt $R \subseteq \hat{R}$.

Definiere $\hat{\phi} : \hat{R} \to S$ durch $r \mapsto \begin{cases} \phi(r) & \text{falls } r \in R \\ r & \text{falls } r \in S \setminus \phi(R) \end{cases}$

Dann gilt $\hat{\phi}|_R = \phi$. überprüfe: $\hat{\phi}$ ist bijektiv

Verwende Satz 11.15, um die Addition und die Multiplikation von $S$ auf $\hat{R}$ zu übertragen. Kontrolliere dann, dass $\hat{R} | \mathbb{R}$ eine Ringerweiterung und $\hat{\phi}$ ein Isomorphismus ist.

<u>Anwendung</u>: Konstruktion von $\mathbb{C}$

Erinnerung: $\mathbb{C} = \mathbb{R}[x]/(f)$, $f = x^2+1$, $\iota : \mathbb{R} \to \mathbb{C}$ geg. durch $a \mapsto a + (f)$, $i = x + (f)$ mit $i^2 = -1$

<u>Beh</u>: Der Ringhom. $\iota$ ist injektiv.

denn: Sei $a \in \mathbb{R}$ mit $\iota(a) = 0_{\mathbb{C}} \Rightarrow a + (f) = (f) \Rightarrow$
$a \in (f) \Rightarrow \exists\, h \in \mathbb{R}[x]$ mit $a = hf \xRightarrow{\mathrm{grad}(f)=2} a = 0$

Nach Satz 11.16 gibt es einen Erweiterungsring $C \supseteq \mathbb{R}$ und einen Isom. $\hat{\phi} : C \to \underline{\mathbb{C}}$ mit $\hat{\phi}|_{\mathbb{R}} = \iota$.

überprüfe: (i) $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$

wobei $i = \hat{\phi}^{-1}(\mathbf{i})$

(ii) $i^2 = -1$

<u>zu (i)</u> „$\supseteq$" klar, denn wegen $a, b, i \in \mathbb{C}$ $\forall a, b \in \mathbb{R}$ liegt auch $a + ib$ in $\mathbb{C}$.

„$\subseteq$" Sei $z \in \mathbb{C} \Rightarrow \hat{\phi}(z) \in C$ bereits gezeigt: $\exists a, b \in \mathbb{R}$ mit $\iota(a) + \iota(b)\mathbf{i} = \hat{\phi}(z) \longrightarrow \hat{\phi}(a) + \hat{\phi}(b)\hat{\phi}(i) = \hat{\phi}(z)$

$\longrightarrow \hat{\phi}(a + bi) = \hat{\phi}(z) \xrightarrow{\hat{\phi} \text{ bij}} a + bi = z$

<u>zu (ii)</u> $\hat{\phi}(i^2) = \hat{\phi}(i)^2 = \mathbf{i}^2 = -1 + (f) = \iota(-1)$

$= \hat{\phi}(-1) \xrightarrow{\hat{\phi} \text{ bij}} i^2 = -1$ $\square$

# Definition der Quotientenkörper

**Definition (11.17)**

Sei $R$ ein Integritätsbereich. Ein Erweiterungsring $K \supseteq R$ wird Quotientenkörper von $R$ genannt, wenn $K$ ein Körper ist und

$$K = \{ab^{-1} \mid a, b \in R\ ,\ b \neq 0_R\} \qquad \text{gilt.}$$

Beispielsweise ist $\mathbb{Q}$ ein Quotientenkörper von $\mathbb{Z}$.

Definition von Addition und Multiplikation auf $\mathbb{Q}$: Fix $a, b \in \mathbb{Z}$, $c, d \in \mathbb{N}$

Sei $$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Addition von Polynomen:

$$\left(\sum_{k=0}^{n} a_k x^k\right) + \left(\sum_{k=0}^{n} b_k x^k\right) = \sum_{k=0}^{n} (a_k + b_k) x^n$$

Multiplikation von Polynomen:

$$\left(\sum_{k=0}^{n} a_k x^k\right) \cdot \left(\sum_{k=0}^{n} b_k x^k\right) = \sum_{k=0}^{2n} c_k x^k; \quad c_k = \sum_{j=0}^{k} a_{k-j} b_j$$

# Konstruktion des Quotientenkörpers

Wir definieren auf der Menge $X_R = R \times (R \setminus \{0_R\})$ eine Relation $\sim$ durch die Festlegung

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc$$

für alle $(a, b), (c, d) \in X_R$.

**Lemma (11.18)**

Die Relation $\sim$ ist eine Äquivalenzrelation auf $R \times (R \setminus \{0_R\})$.

# Konstruktion des Quotientenkörpers (Forts.)

**Proposition (11.19)**

Auf der Menge $\hat{R} = X_R/\sim$ gibt es eindeutig bestimmte Verknüpfungen $\oplus$ und $\odot$ mit

$$[a,b] \oplus [c,d] = [ad+bc, bd] \qquad \text{und} \qquad [a,b] \odot [c,d] = [ac, bd]$$

für alle $(a,b),(c,d) \in X_R$, und $\hat{R}$ bildet mit diesen Verknüpfungen einen Körper.

# Existenz und Eindeutigkeit des Quotientenkörpers

### Satz (11.20)

Zu jedem Integritätsbereich existiert ein Quotientenkörper.

### Satz (11.21)

Sei $R$ ein Integritätsbereich, und seien $K$ und $L$ beides Quotientenkörper von $R$. Dann existiert ein Isomorphismus $\psi : K \to L$ von Körper mit $\psi|_R = \mathrm{id}_R$.

### Definition (11.22)

Sei $R$ ein Ring. Ein Erweiterungsring $S$ von $R$ wird Polynomring über $R$ genannt, wenn es ein ausgezeichnetes Element $x \in S$ gibt mit der Eigenschaft, dass für jedes Element $f \in R[x] \setminus \{0_R\}$ ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, ..., a_n \in R$ existieren, so dass $a_n \neq 0$ ist und $f$ in der Form

$$f \quad = \quad a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

dargestellt werden kann.

# Ergänzungen zur Definition

- Das ausgezeichnete Elemente $x$ nennt man die Variable (oder Unbestimmte) des Polynomrings.
- Für einen Polynomring $S$ über einem Ring $R$ mit der Variablen $x$ wird in der Regel die Bezeichnung $R[x]$ verwendet.
- Die Elemente von $R[x]$ heißen Polynome übe dem Ring $R$.
- Man bezeichnet die Zahl $n$ in der Definition als den Grad $\deg(f)$ des Polynoms $f$.
- Das Polynom $a_n x^n$ ist der Leitterm, das Element $a_n \in R$ der Leitkoeffizient von $f$.

wichtiger Hinweis: Das Element $x$ im Polynomring $R[x]$ ist kein Element des Rings $R$.

# Konstruktion der Polynomringe

- Sei $P_R$ die Menge aller Abbildungen $f : \mathbb{N}_0 \to R$ mit der Eigenschaft, dass $f(k) = 0_R$ für alle bis auf endlich viele $k \in \mathbb{N}_0$.
- Auf der Menge $P_R$ definieren wir eine Verknüpfung $\oplus$ durch

$$(f \oplus g)(n) \quad = \quad f(n) + g(n).$$

  Ebenso definieren wir eine Verknüpfung $\odot$ durch

$$(f \odot g)(n) = \sum_{k=0}^{n} f(n-k)g(k) = \sum_{k+\ell=n} f(\ell)g(k).$$

- Für jedes $a \in R$ sei $\tilde{a} \in P_R$ das Element gegeben durch $\tilde{a}(0) = a$ und $\tilde{a}(n) = 0_R$ für alle $n \geq 1$.
- Außerdem definieren wir ein Element $\tilde{x} \in P_R$ durch $\tilde{x}(1) = 1_R$ und $\tilde{x}(n) = 0_R$ für $n \neq 1$.

**Lemma (11.25)**

Das Tripel $(P_R, \oplus, \odot)$ ist ein Ring, mit $\tilde{0}$ als Null- und $\tilde{1}$ als Einselement.

# Konstruktion der Polynomringe (Forts.)

**Lemma (11.26)**

Sei $a \in R$ und $m \in \mathbb{N}_0$. Dann gilt $(\tilde{a} \odot \tilde{x}^m)(m) = a$, und $(\tilde{a} \odot \tilde{x}^m)(n) = 0_R$ für alle $n \in \mathbb{N}_0 \setminus \{m\}$.

**Lemma (11.27)**

Für jedes $f \in P_R \setminus \{\tilde{0}\}$ gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, a_1, ..., a_n \in R$, so dass $a_n \neq 0_R$ und

$$f \quad = \quad (\tilde{a}_n \odot \tilde{x}^n) \oplus \; ... \; \oplus \tilde{(}a_1 \odot \tilde{x}) \oplus \tilde{a}_0 \qquad \text{gilt.}$$

**Satz (11.28)**

Zu jedem Ring $R$ existiert ein Polynomring über $R$.