

Definition (10.1)

Sei R ein Ring. Ein **Ideal** in R ist eine Teilmenge $I \subseteq R$ mit den Eigenschaften

- (i) $0_R \in I$
- (ii) Für alle $a, b \in I$ und $r \in R$ gilt $a + b \in I$ und $ra \in I$.

Proposition (10.9)

Sei R ein Ring und $(I_j)_{j \in A}$ eine Familie von Idealen in R .
Dann ist $I = \bigcap_{j \in A} I_j$ ein Ideal in R .

Proposition (10.10)

Sei ein Ring, und seien I, J Ideale in R . Dann ist auch die
Teilmenge $I + J = \{ a + b \mid a \in I, b \in J \}$ von R ein Ideal in R .

Die Elemente endlich erzeugter Ideale

Proposition (10.12)

Sei R ein Ring, und seien $a_1, \dots, a_n \in R$. Dann gilt

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^n r_i a_i \mid r_1, \dots, r_n \in R \right\}.$$

Die folgende Regel wird beim Rechnen mit Idealen häufig verwendet.

Lemma (10.13)

Sei R ein Ring, und seien $S, T \subseteq R$ beliebige Teilmengen. Gilt für die erzeugten Ideale $S \subseteq (T)$ und $T \subseteq (S)$, dann folgt $(S) = (T)$.

Definition (10.14)

Sei R ein Ring, und seien I, J Ideale in R . Dann ist das **Produktideal** IJ das von der Menge $\{ab \mid a \in I, b \in J\}$ **erzeugte** Ideal in R .

Das elementweise Produkt $\{ab \mid a \in I, b \in J\}$ selbst ist im Allgemeinen **kein** Ideal. Beispielsweise erhält man im Fall $R = \mathbb{Z}[x]$, $I = (2, x)$, $J = (3, x)$ auf diese Weise kein Ideal.

Proposition (10.15)

Sei R ein Ring, und seien I, J von endlichen vielen Ringelementen erzeugte Ideale, $I = (a_1, \dots, a_m)$ und $J = (b_1, \dots, b_n)$ mit $m, n \in \mathbb{N}$, $a_i, b_j \in R$ für $1 \leq i \leq m$, $1 \leq j \leq n$. Dann wird IJ von der Menge

$$S = \{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

erzeugt, es gilt also $IJ = (S)$.

Beispiel für die Berechnung eines Produktideals

$p_1 = (3, 1+2\sqrt{-5})$, $p_2 = (3, 1-2\sqrt{-5})$ sind Primideale
im Ring $R = \mathbb{Z}[\sqrt{-5}]$ Beh.: $p_1 p_2 = (3)$

$$\begin{aligned} p_1 p_2 &= (3, 1+2\sqrt{-5}) \cdot (3, 1-2\sqrt{-5}) = (3 \cdot 3, 3 \cdot (1-2\sqrt{-5}), (1+2\sqrt{-5}) \cdot 3, \\ & (1+2\sqrt{-5})(1-2\sqrt{-5})) = (9, 3-6\sqrt{-5}, 3+6\sqrt{-5}, 21) \stackrel{(\Delta)}{=} \\ & (3, 3-6\sqrt{-5}, 3+6\sqrt{-5}) \stackrel{(\Delta\Delta)}{=} (3) \end{aligned}$$

Erinnerung: $S \subseteq (T), T \subseteq (S) \Rightarrow (S) = (T)$

(Δ) folgt aus $9 = 3 \cdot 3 \in (3, 3-6\sqrt{-5}, 3+6\sqrt{-5})$ und
 $21 = 7 \cdot 3 \in (3, 3-6\sqrt{-5}, 3+6\sqrt{-5})$

sowie $3 = (-2) \cdot 9 + 1 \cdot 21 \in (9, 3-6\sqrt{-5}, 3+6\sqrt{-5}, 21)$

($\Delta\Delta$) „ $\geq$ “ ist offensichtlich „ $\leq$ “ folgt aus $(1-2\sqrt{-5}) \cdot 3 \in (3)$
und $(1+2\sqrt{-5}) \cdot 3 \in (3)$

Das Distributivgesetz für Ideale

Lemma (10.16)

Für Ideale I, J, K in einem Ring R gilt das **Distributivgesetz** $I(J + K) = IJ + IK$, außerdem gilt $IJ \subseteq I$ und $IJ \subseteq J$.

Beweis von Lemma 10.16:

geg: Ring R , I, J, K Ideale in R

überprüfe: (i) $I(J+K) = IJ + IK$

(ii) $IJ \subseteq I$

zu (i) " $\subseteq$ " Das Produktideal $I(J+K)$ wird erzeugt von $S = \{a \cdot b \mid a \in I, b \in J+K\}$.

Weil $IJ + IK$ ist, genügt es zu überprüfen,

dass $S \subseteq IJ + IK$ gilt. Sei $s \in S \Rightarrow$

$\exists a \in I, b \in J+K$ mit $s = a \cdot b$ $b \in J+K$

$\Rightarrow \exists c \in J, d \in K$ mit $b = c + d \Rightarrow$

$s = a \cdot (c + d) = ac + ad$ $ac \in IJ$.

$$ad \in IK \Rightarrow s \in IJ + IK$$

„ $\supseteq$ “ Beh.: $IJ \subseteq I(J+K), IK \subseteq I(J+K)$

Nach Def. werden IJ bzw. IK erzeugt von

$$T = \{ab \mid a \in I, b \in J\} \text{ bzw. } U = \{ac \mid a \in I, c \in K\}$$

Da $I(J+K)$ ein Ideal ist, genügt es, $T \subseteq I(J+K)$

und $U \subseteq I(J+K)$ zu überprüfen.

$$\text{Sei } t \in T \Rightarrow \exists a \in I, b \in J \text{ mit } t = ab$$

$$0_R \in K \Rightarrow b = b + 0_K \in J+K$$

$$a \in I, b \in J+K \Rightarrow t = ab \in I(J+K)$$

$$\text{Sei } u \in U \Rightarrow \exists a' \in I, c \in K \text{ mit } u = a'c$$

$$0_R \in J \Rightarrow c = 0_R + c \in J+K$$

$$\Rightarrow u = a'c \in I(J+K) \quad (\Rightarrow \text{Beh.})$$

Sei nun $r \in IJ + IK \Rightarrow \exists t' \in IJ, u' \in IK$

mit $r = t' + u'$ Beh. $\Rightarrow t', u' \in I(J+K)$

$$\underline{IJ+K} \quad r = t' + u' \in I(J+K)$$

ist Ideal

zu ii) Da $S = \{ab \mid a \in I, b \in J\}$ ein Erzeugendensystem von IJ ist, reicht es, $S \subseteq I$ zu überprüfen.

Sei also $s \in S \Rightarrow \exists a \in I, b \in J$

mit $s = ab \quad a \in I, b \in R, I \text{ Ideal}$

$$\Rightarrow s = ba \in I$$

□

Definition (10.17)

- Ein Ideal $\mathfrak{p}$ in einem Ring R wird **Primideal** genannt, wenn $\mathfrak{p} \neq (1)$ gilt und für alle $a, b \in R$ die Implikation

$$ab \in \mathfrak{p} \quad \Rightarrow \quad a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

erfüllt ist.

- Man nennt $\mathfrak{p}$ ein **maximales** Ideal, wenn $\mathfrak{p} \neq (1)$ ist und kein Ideal I mit der Eigenschaft $\mathfrak{p} \subsetneq I \subsetneq (1)$ existiert, das Ideal also abgesehen vom Einheitsideal bezüglich Inklusion maximal ist.

Proposition (10.18)

Ein Ideal $\mathfrak{p}$ in einem Ring R ist genau dann ein Primideal in R , wenn $\mathfrak{p} \neq (1)$ ist und für beliebige Ideale I, J mit $IJ \subseteq \mathfrak{p}$ eine der Bedingungen $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$ erfüllt ist.

Beweis von Prop. 10.18

geg. R Ring, $\mathfrak{p}$ Ideal von R .

z.zg. $\mathfrak{p}$ ist Primideal $\iff \mathfrak{p} \neq (1)$ und für alle Ideale I, J von R folgt aus $IJ \subseteq \mathfrak{p}$ jeweils $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$

" $\implies$ " $\mathfrak{p}$ Primideal $\implies \mathfrak{p} \neq (1)$ Seien nun I, J Ideale von R mit $IJ \subseteq \mathfrak{p}$. z.zg. $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$

Ang. $I \not\subseteq \mathfrak{p}$ und $J \not\subseteq \mathfrak{p} \implies \exists a \in I \setminus \mathfrak{p}, b \in J \setminus \mathfrak{p}$
 $a, b \in IJ \xrightarrow{IJ \subseteq \mathfrak{p}} ab \in \mathfrak{p} \xrightarrow{\mathfrak{p} \text{ Primideal}} a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p} \nmid$

" $\impliedby$ " $\mathfrak{p} \neq (1)$ nach Voraussetzung erfüllt

Ang. $I \not\subseteq \mathfrak{p}$ und $J \not\subseteq \mathfrak{p} \Rightarrow \exists a \in I \setminus \mathfrak{p}, b \in J \setminus \mathfrak{p}$
 $a, b \in R \quad IJ \subseteq \mathfrak{p} \quad a, b \in R \quad \xRightarrow{\text{Prinideal}} a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$

Seien $a, b \in R$ mit $ab \in \mathfrak{p}$. z.zeg: $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$

Sei $I = (a), J = (b) \Rightarrow IJ = (a) \cdot (b) = (ab)$

$ab \in \mathfrak{p} \Rightarrow IJ = (ab) \subseteq \mathfrak{p} \xRightarrow{\text{Vor.}} I \subseteq \mathfrak{p} \text{ oder } J \subseteq \mathfrak{p}$

$a \in I, b \in J$ $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ □

Kerne und Bilder von Ringhomomorphismen

Definition (10.19)

Sei $\phi : R \rightarrow S$ Ringhomomorphismus. Dann nennt man $\ker(\phi) = \phi^{-1}(\{0_S\})$ den **Kern** und $\operatorname{im}(\phi) = \phi(R)$ das **Bild** von ϕ .

Proposition (10.20)

Seien R, S Ringe und $\phi : R \rightarrow S$ ein Ringhomomorphismus.

- (i) Ist J ein Ideal in S , dann ist $\phi^{-1}(J)$ ein Ideal in R .
- (ii) Ist I ein Ideal in R und ϕ surjektiv, dann ist die Bildmenge $\phi(I)$ ein Ideal in S .

Insbesondere ist also der Kern eines Ringhomomorphismus $\phi : R \rightarrow S$ ein Ideal in R . Das Bild ist zwar stets ein **Teilring** von S , aber im Allgemeinen kein Ideal.

Nachweis, dass das Bild eines Ideals unter einem Ringhom. im Allgemeinen kein Ideal ist:

Betrachte den Ringhom. $\phi: \mathbb{Z} \rightarrow \mathbb{Q}$, $a \mapsto a$
und in $\mathbb{Z}$ das Ideal $I = (2) = 2\mathbb{Z}$. Dann ist
 $\phi(I) = I = 2\mathbb{Z}$, aber I ist kein Ideal in $\mathbb{Q}$,
denn: $2 \in I$, $\frac{1}{2} \in \mathbb{Q}$, aber $\frac{1}{2} \cdot 2 = 1 \notin I$

§ 6. Faktorringe und Konstruktion von Ringerweiterungen

Definition (11.1)

Sei R ein Ring, I ein Ideal und $a \in R$. Dann nennen wir die Menge

$$a + I = \{a + i \mid i \in I\}$$

die **Nebenklasse** von a modulo I . Die Menge $\{a + I \mid a \in R\}$ aller Nebenklassen von Elementen aus R bezeichnen wir mit R/I .

Proposition (11.2)

Sei R ein Ring und I ein Ideal. Dann ist die Relation auf R gegeben durch

$$a \equiv b \pmod{I} \iff b - a \in I$$

eine Äquivalenzrelation, und die Elemente von R/I sind genau die Äquivalenzklassen dieser Relation. Man spricht in diesem Zusammenhang von einer **Kongruenzrelation** und bezeichnet zwei Elemente a, b derselben Äquivalenzklasse als **kongruent modulo I** .

Beweis von Prop. 11.2 geg. R Ring, I Ideal in R

Beh. (i) Die Relation $\equiv$ auf R geg. durch

$a \equiv b \iff b - a \in I$ ist eine Äquivalenzrelation.

(ii) Für jedes $a \in R$ ist $a + I$ genau die Äquivalenzklasse $[a]$ von a bzgl. $\equiv$.

zuli) Seien $a, b, c \in R$.

Reflexivität: $a - a = 0_R \in I$ (da I Ideal)

$$\Rightarrow a \equiv a$$

Symmetrie: Setze $a \equiv b$ voraus. $\Rightarrow b - a \in I \stackrel{I \text{ Ideal}}{=} \Rightarrow$

$$a - b = (-1_R)(b - a) \in I \Rightarrow a - b \in I$$

Transitivität. Vor: $a \equiv b, b \equiv c$ z.zg: $a \equiv c$

$$a \equiv b \Rightarrow b - a \in I, b \equiv c \Rightarrow c - b \in I \Rightarrow$$

$$c - a = (c - b) + (b - a) \in I \text{ (da } I \text{ Ideal)}$$

zu ii) Sei $a \in R$, z.zg: $[a] = a + I$

$$\text{"} \subseteq \text{" Sei } b \in [a] \Rightarrow a \equiv b \Rightarrow b - a \in I \Rightarrow b = a + (b - a) \\ \in a + I$$

$$\text{"} \supseteq \text{" Sei } b \in a + I \Rightarrow \exists i \in I \text{ mit } b = a + i \Rightarrow b - a = i \in I \\ \Rightarrow a \equiv b \Rightarrow b \in [a] \quad \square$$

Erinnerung: G Gruppe, $U \subseteq G$, $g, h \in G$
 $gU = hU \Leftrightarrow h \in gU \Leftrightarrow g \in hU$

Wichtige Rechenregel für Kongruenzklassen

Nach Definition sind zwei Elemente $a, b \in R$ also genau dann kongruent modulo I , wenn ihre Kongruenzklassen übereinstimmen. Da je zwei Äquivalenzklassen entweder disjunkt oder gleich sind, erhalten wir die Äquivalenz

$$a \equiv b \pmod{I} \Leftrightarrow b - a \in I \Leftrightarrow a + I = b + I \Leftrightarrow b \in a + I.$$

Die Elemente des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Proposition (11.3)

Die Menge $\mathbb{Z}/n\mathbb{Z}$ der Kongruenzklassen ist n -elementig, es gilt

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}, 0 \leq a < n\}.$$

Gleichbedeutend damit ist die Feststellung, dass die Elemente der Menge $\{0, 1, \dots, n-1\}$ ein **Repräsentantensystem** von $\mathbb{Z}/n\mathbb{Z}$ bildet.

Proposition (11.4)

Sei K ein Körper, $R = K[x]$ und $f \in K[x]$ ein Polynom vom Grad $n \geq 1$. Dann ist die Teilmenge

$$S = \{g \in K[x] \mid g \neq 0, \text{grad}(g) < n\} \cup \{0\}$$

von $K[x]$ ein Repräsentantensystem von $R/(f)$.

Der Beweis von Prop. 11.4 beruht auf der Tatsache, dass man Polynome mit Rest dividieren kann (Polynomdivision):

Sind $f, g \in K[x]$ mit $g \neq 0$, dann gibt es $q, r \in K[x]$ mit $f = gq + r$ und $r = 0_K$ oder $\text{grad}(r) < \text{grad}(g)$.

Proposition (11.5)

Sei R ein Ring und I ein Ideal. Dann gibt es (eindeutig bestimmte) Verknüpfungen $+$ und $\cdot$ auf R/I mit der Eigenschaft

$$(a + I) + (b + I) = (a + b) + I \quad \text{und} \quad (a + I) \cdot (b + I) = ab + I$$

für alle $a, b \in R$.

zum Beweis von Prop. 11.5:

Sei R ein Ring, I ein Ideal von R .

z.zg.: Es gibt eine Verknüpfung $\cdot$ auf R/I

so dass $(a+I) \cdot (b+I) = ab+I \quad \forall a, b \in R$ gilt.

Ansatz: Wende Satz 4.25 an auf die Abb.

$$\phi: R \times R \rightarrow R/I, (a, b) \mapsto ab+I$$

zu überprüfen: Sind $a, a', b, b' \in R$ mit

$a \equiv a' \pmod{I}$, $b \equiv b' \pmod{I}$, dann ist $\phi(a, b) = \phi(a', b')$

Seien also a, a', b, b' Elemente, die diese Voraussetzungen erfüllen. z.zg.:

$$\phi(a, b) = \phi(a', b'), \text{ gleichbed. : } ab+I = a'b'+I$$

Dies wiederum ist äquivalent zu

$$ab \equiv a'b' \pmod{I} \text{ bzw. zu } a'b' - ab \in I.$$

$$\begin{aligned} \text{Es ist } a'b' - ab &= a'b' - ab' + ab' - ab \\ &= (a' - a)b' + a(b' - b) \end{aligned}$$

$$\begin{aligned} a &\equiv a' \pmod{I} \Rightarrow a' - a \in I \stackrel{I \text{ Ideal}}{\Rightarrow} (a' - a)b' \in I \\ b &\equiv b' \pmod{I} \Rightarrow b' - b \in I \rightarrow a(b' - b) \in I \end{aligned}$$

$$\text{Daraus folgt } a'b' - ab = (a' - a)b' + a(b' - b) \in I.$$

Nach Satz 4.25 existiert somit eine Abb.

$$\begin{aligned} \Phi: R/I \times R/I &\rightarrow R/I \text{ mit } \Phi(a+I, b+I) = \\ &= \phi(a, b) \text{ Definiere } (a+I) \cdot (b+I) = \Phi(a+I, b+I) \end{aligned}$$

$$\forall a+I, b+I \in R/I$$

Es gilt dann jeweils $(a+I) \cdot (b+I)$
 $= \phi(a,b) = ab+I$, für $a, b \in R$. $\square$

Rest

lt es

$= 0_K$

Satz (11.6)

Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist R/I mit den beiden soeben definierten Verknüpfungen ein Ring, den man als **Faktoring** bezeichnet. Die Abbildung $\pi_I : R \rightarrow R/I$ gegeben $a \mapsto a + I$ ist ein Epimorphismus von Ringen, der sog. **kanonische Epimorphismus**.

zum Beweis von Satz 11.6 : (exemplarisch)

Distributivgesetz : Seien $a, b, c \in R$

$$\begin{aligned}(a+I) \cdot ((b+I) + (c+I)) &= (a+I) \cdot ((b+c)+I) = \\ &= a(b+c) + I = (ab+ac) + I = (ab+I) + (ac+I) = \\ &= (a+I) \cdot (b+I) + (a+I) \cdot (c+I)\end{aligned}$$

Nachweis, dass $1_{R/I} = 1_R + I$ das Einselement von R/I ist :

$$\begin{aligned}\text{Sei } a \in R. \quad 1_{R/I} \cdot (a+I) &= (1_R + I) \cdot (a+I) = \\ &= 1_R \cdot a + I = a + I\end{aligned}$$