

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 (10.2)

- Ist R ein Ring und $b \in R$, dann ist die Menge der Vielfachen $\{ab \mid a \in R\}$ von b ein Ideal in R . Man nennt ein solches Ideal ein **Hauptideal** und bezeichnet es mit (b) .
- Ein **Hauptidealring** ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.
- In jedem Ring R ist das **Nullideal** $(0_R) = \{0_R\}$ das kleinste und das **Einheitsideal** $(1_R) = R$ das bezüglich Inklusion größte Ideal.

Bsp.: Ideale mit ein oder zwei Erzeugern

Hauptideale $(a) = \{ua \mid u \in R\}$

Ideale mit zwei Erzeugern: $(a, b) = \{ua + vb \mid u, v \in R\}$

Definition der Teilerrelation

Definition (10.3)

Seien R ein Ring und $a, b \in R$. Wir sagen, dass a ein **Teiler** von b ist und schreiben $a|b$, wenn ein $c \in R$ mit $b = ac$ existiert. Gilt sowohl $a|b$ als auch $b|a$, dann sagt man, die Elemente a und b sind **assoziiert** zueinander.

Lemma (10.4)

Ist R ein Integritätsbereich, so sind $a, b \in R$ genau dann zueinander assoziiert, wenn ein $\varepsilon \in R^\times$ mit $b = \varepsilon a$ existiert.

Beweis von Lemma 10.4:

geg. Integritätsbereich R , $a, b \in R$

Beh.: a, b sind zueinander
assoziiert (d.h. $a|b, b|a$) $\iff \exists \varepsilon \in R^\times$ mit $b = \varepsilon a$

" $\Leftarrow$ " $b = \varepsilon a \Rightarrow a|b$, $\varepsilon^{-1}b = a \Rightarrow b|a$

" $\Rightarrow$ " $a|b \Rightarrow \exists c \in R$ mit $b = ca$

$b|a \Rightarrow \exists d \in R$ mit $a = db$

einsetzen $\Rightarrow a = dca \Rightarrow 1_R \cdot a = dc \cdot a$

$\Rightarrow (dc - 1_R) a = 0_R \Rightarrow a = 0_R$ oder $dc - 1_R = 0_R$

1. Fall: $a = 0_R \Rightarrow b = c \cdot 0_R = 0_R$

Setzen wir $\varepsilon = 1_R$, dann gilt $\varepsilon \in R^\times$ und $b = \varepsilon a$

2. Fall: $a \neq 0_R \Rightarrow da - 1_R = 0_R \Rightarrow da = 1_R \Rightarrow c \in R^\times$

Wegen $b = ca$ folgt somit die Beh



Definition des größten gemeinsamen Teilers

Definition (10.5)

Sei R ein Ring mit $a_1, \dots, a_n \in R$. Wir sagen, ein Element $d \in R$ ist ein **größter gemeinsamer Teiler** (kurz ggT) von $a_1, \dots, a_n$, wenn gilt

- (i) $d|a_i$ für $1 \leq i \leq n$
- (ii) Ist $b \in R$ mit $b|a_i$ für $1 \leq i \leq n$, dann folgt $b|d$.

Wir nennen die Elemente $a_1, \dots, a_n$ **teilerfremd**, wenn 1_R ein ggT der Elemente ist.

Definition des kleinsten gemeinsamen Vielfachen

Definition (10.6)

Sei R ein Ring mit $a_1, \dots, a_n \in R$. Ein Element $e \in R$ heißt **kleinstes gemeinsames Vielfaches** (kurz kgV) von $a_1, \dots, a_n$, wenn gilt

- (i) $a_i | e$ für $1 \leq i \leq n$
- (ii) Ist $b \in R$ mit $a_i | b$ für $1 \leq i \leq n$, dann folgt $e | b$.

Lemma (10.7)

Sei R ein Ring und $d \in R$ ein größter gemeinsamer Teiler der Ringelemente $a_1, \dots, a_n$. Ein weiteres Element $d' \in R$ ist genau dann ein ggT von $a_1, \dots, a_n$, wenn d und d' zueinander assoziiert sind. Dieselbe Aussage gilt auch für das kleinste gemeinsame Vielfache.

Satz (10.8)

Sei R ein Ring, und seien $a, b \in R$.

- (i) Es gilt $(a) \subseteq (b)$ genau dann, wenn b ein Teiler von a ist.
- (ii) Ist $d \in R$ mit $(d) = (a, b)$, dann ist d ein ggT von a und b .
- (iii) Ist $e \in R$ mit $(e) = (a) \cap (b)$, dann ist e ein kgV von a und b .

Ist R ein **Hauptidealring**, dann gilt auch von (ii) und (iii) die Umkehrung.

Beweis von Satz 10.8

geg: Ring R , $a, b \in R$

zu (i) z.zg: $a \mid b \Leftrightarrow (a) \supseteq (b)$

" $\Rightarrow$ " $a \mid b \Rightarrow \exists c \in R$ mit $b = ca$

Sei $r \in (b) \Rightarrow \exists d \in R$ mit $r = db$
 $\Rightarrow r = dca \Rightarrow r \in (a)$

" $\Leftarrow$ " $(b) \subseteq (a) \Rightarrow b = 1_R b \in (a) \Rightarrow$

$\exists c \in R$ mit $b = ca \Rightarrow a \mid b$

zu (ii) Vor: $c \in R$, $(c) = (a, b)$

Beh: c ist ggT von a, b , dafür

zu überprüfen (1) $c|a$ und $c|b$

(2) $\forall d \in R : d|a \text{ und } d|b \Rightarrow d|c$

Nach Def. $(a, b) = \{ua + vb \mid u, v \in R\}$

zu (1)

$$a = 1_R \cdot a + 0_R \cdot b \in (a, b) \xRightarrow{\text{Lsg.}} a \in (c) \Rightarrow c|a$$

$$b = 0_R \cdot a + 1_R \cdot b \in (a, b) \Rightarrow b \in (c) \Rightarrow c|b$$

zu (2) Sei $d \in R$ mit $d|a$ und $d|b \Rightarrow \exists u, v \in R$

mit $a = ud$ und $b = vd$ z.zg: $d|c$.

gleichbed. $c \in (d)$ Vor $\Rightarrow (c) = (a, b)$,

insb. $c \in (a, b)$, d.h. $\exists r, s \in R$ mit

$$c = ra + sb = r(ud) + s(vd) = (ru + sv) \cdot d$$

$$\Rightarrow c \in (d)$$

zu (ii) $\text{Vor.} : e \in R \text{ mit } (e) = (a) \cap (b)$

z.zg. e ist kgV von a und b , d.h.

(1) $a|e$ und $b|e$

(2) $\forall e' \in R : a|e' \text{ und } b|e' \Rightarrow e|e'$

zu (1) $\text{Vor.} \Rightarrow e \in (a) \text{ und } e \in (b)$

$\Rightarrow a|e \text{ und } b|e$

zu (2) Sei $e' \in R$ mit $a|e'$ und $b|e' \Rightarrow$

$e' \in (a) \text{ und } e' \in (b) \Rightarrow e' \in (a) \cap (b)$

$\text{Vor.} \Rightarrow e' \in (e) \Rightarrow e|e'$

Setze nun voraus, dass R ein Hauptidealring ist. Wir zeigen nur die Umkehrung von (i).

daher

Voraussetzung also: c ist ggT von a und b
z.zg: $(c) = (a, b)$

" $\supseteq$ " Sei $r \in (a, b) \Rightarrow \exists u, v \in R$ mit $r = ua + vb$
Voa $\Rightarrow c \mid a$ und $c \mid b \Rightarrow \exists s, t \in R$ mit
 $a = sc$, $b = tc$ einsetzen $\Rightarrow r = usc + vtc$
 $= (us + vt)c \Rightarrow r \in (c)$

" $\subseteq$ " Da R ein Hauptidealring ist, existiert
ein $d \in R$ mit $(a, b) = (d)$. Nach (ii) ist
 d ein ggT von a, b . Da c ebenfalls ein ggT
ist, sind c und d assoziiert, vsl. gilt $d \mid c$
 $\Rightarrow c \in (d) \Rightarrow c \in (a, b)$ $\square$

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 .

Beweis von Prop. 10.10

geg R Ring, I, J Ideale in R

z.zg: $I+J = \{a+b \mid a \in I, b \in J\}$ ist Ideal in R

zu überprüfen: (i) $0_R \in I+J$

(ii) $\forall c, c' \in I+J \forall r \in R: c+c' \in I+J, rc \in I+J$

zu (i) I, J Ideale $\Rightarrow 0_R \in I$ und $0_R \in J \Rightarrow 0_R = 0_R + 0_R \in I+J$

zu (ii) Seien $c, c' \in I+J$ und $r \in R$. Nach Def. von $I+J$ gibt es $a, a' \in I, b, b' \in J$ mit $c = a+b, c' = a'+b'$

I Ideal, $a, a' \in I, r \in R \Rightarrow a+a' \in I$ und $ra \in I$

J Ideal, $b, b' \in J, r \in R \Rightarrow b+b' \in J$ und $rb \in J$

$\Rightarrow c+c' = (a+b) + (a'+b') = (a+a') + (b+b') \in I+J$

$rc = r(a+b) = ra+rb \in I+J$ □

Definition (10.11)

Sei R ein Ring und $S \subseteq R$ eine Teilmenge. Man sagt, ein Ideal I in R wird von S **erzeugt** und schreibt $I = (S)$, wenn folgende Bedingungen erfüllt sind.

- (i) $I \supseteq S$
- (ii) Ist J ein Ideal in R mit $J \supseteq S$, dann folgt $J \supseteq I$.

Insgesamt ist I also das **kleinste** Ideal mit der Eigenschaft $I \supseteq S$.

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 $(S) = (T)$.

Beweis von Prop. 10.12

geg. Ring R , $n \in \mathbb{N}$, $a_1, \dots, a_n \in R$

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

Beh.: $\langle S \rangle = T$

Überprüfe dafür, dass T die definierenden Eigenschaften von $\langle S \rangle$ besitzt, im Einzelnen (1) T ist Ideal

(2) $T \supseteq S$ (3) J Ideal, $J \supseteq S \Rightarrow J \supseteq T$

zu (1) ähnlich wie in Prop. 10.10, siehe Skript

zu (2) Definiere $\delta_{ij} = \begin{cases} 1_R & \text{falls } i=j \text{ für } 1 \leq i, j \leq n \\ 0_R & \text{sonst} \end{cases}$

Dann gilt für $1 \leq j \leq n$ jeweils $a_j = \sum_{i=1}^n \delta_{ij} a_i \Rightarrow a_j \in T$

Insgesamt gilt also $S = \{a_1, \dots, a_n\} \subseteq T$

zu (3) Sei J ein Ideal mit $J \supseteq S$. z.zg:

$T \subseteq J$ Sei also $a \in T \Rightarrow \exists r_1, \dots, r_n$

$\in R$ mit $a = \sum_{i=1}^n r_i a_i$ Vor $\Rightarrow a_i \in J$ für

$1 \leq i \leq n \xRightarrow{J \text{ Ideal}} r_i a_i \in J$ für $1 \leq i \leq n$

J Ideal $\Rightarrow a = r_1 a_1 + \dots + r_n a_n \in J. \quad \square$

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 $IJ = (S)$.

Beweis von Prop 10.15:

geg: R Ring, $m, n \in \mathbb{N}$, $a_1, \dots, a_m \in R$,
 $b_1, \dots, b_n \in R$, $I = (a_1, \dots, a_m)$, $J =$
 $(b_1, \dots, b_n)$ Sei $S = \{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$

Beh: $IJ = (S)$

Sei $T = \{a b \mid a \in I, b \in J\}$. Nach Def.
gilt $IJ = (T)$. z.zg also: $(T) = (S)$
genügt: (1) $S \subseteq (T)$ und (2) $T \subseteq (S)$

zu (1) Offenbar gilt $S \subseteq T$. Wegen $T \subseteq (T)$
folgt daraus $S \subseteq (T)$

zu (2) Sei $c \in T \Rightarrow \exists a \in I, b \in J$ mit

$$c = a \cdot b \quad a \in I \Rightarrow \exists r_1, \dots, r_m \in R \text{ mit}$$

$$a = \sum_{i=1}^m r_i a_i, \text{ ebenso: } b \in J \Rightarrow \exists s_1, \dots, s_n \in R \text{ mit}$$

$$b = \sum_{j=1}^n s_j b_j \Rightarrow a \cdot b = \left(\sum_{i=1}^m r_i a_i \right) \left(\sum_{j=1}^n s_j b_j \right)$$

$$= \sum_{i=1}^m \sum_{j=1}^n r_i s_j \underbrace{a_i b_j}_{\in S} \in (S)$$

□

Bem. In allgemeinen Ringen gilt das Gesetz von der eindeutigen Primfaktorzerlegung nicht mehr.

Beispiel: $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

Dies sind zwei wesentlich verschiedene Zerlegungen, d.h. 3 ist zu keinem der beiden Faktoren $1 \pm 2\sqrt{-5}$ assoziiert, und dasselbe gilt für 7.

Betrachtet man dagegen die Ideale

$$\mathfrak{p}_1 = (3, 1 + 2\sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 - 2\sqrt{-5}),$$

$$\mathfrak{p}_3 = (7, 1 + 2\sqrt{-5}), \quad \mathfrak{p}_4 = (7, 1 - 2\sqrt{-5})$$

(das sind sog. Primideale, s. nächste Stunde), so kann man zeigen, dass $p_1 p_2 = (3)$ und $p_3 p_4 = (7)$ gilt, und somit $(21) = (3)(7) = p_1 p_2 p_3 p_4$. Man kann zeigen, dass dies (bis auf Reihenfolge) die einzige Darstellung des Hauptideals (21) als Produkt von Primidealen ist. (Es gilt $p_1 p_3 = (1 + 2\sqrt{-5})$, $p_2 p_4 = (1 - 2\sqrt{-5})$.)