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 $ra \in I$.

wichtiger Spezialfall: Hauptideale

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.

Ideale gegeben durch Erzeugendensysteme

Proposition (10.3)

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.

Definition (10.4)

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 (10.5)

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

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

Die folgende Regel wird beim Rechnen mit Idealen häufig verwendet.

Lemma (10.6)

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 Proposition 10.5

geg: Ring R, $a_1, \dots, a_n \in R$ ($n \in \mathbb{N}_0$)

Sei $M = \{ \sum_{i=1}^{n} r_i a_i \mid r_1, \dots, r_n \in R \}$.

<u>Beh.</u> $(a_1, \dots, a_n) = M$

Überprüfe, dass M die definierenden Eigenschaften von $(a_1, \dots, a_n)$ besitzt, d.h.

(1) M ist ein Ideal in R

(2) $M \supseteq \{a_1, \dots, a_n\}$

(3) Ist J ein Ideal von R mit $J \supseteq \{a_1, \dots, a_n\}$, dann folgt $J \supseteq M$.

zu (1) überprüfe: (i) $0_R \in M$ (ii) $\forall r \in R,\ a, b \in M: a+b,\ ra \in M$

zu (i) Es gilt $0_R = \sum_{i=1}^{n} 0_R \cdot a_i \in M$.

zu (ii) Sei $r \in R$, seien $a, b \in M$. $\Rightarrow \exists\, r_1, \dots, r_n, s_1, \dots, s_n \in R$

mit $a = \sum_{i=1}^{n} r_i a_i$, $b = \sum_{i=1}^{n} s_i a_i \Rightarrow a+b = \sum_{i=1}^{n} \underbrace{(r_i + s_i)}_{\in R} a_i$

$\Rightarrow a+b \in M$. ebenso $ra = \sum_{i=1}^{n} \underbrace{r r_i}_{\in R} a_i \Rightarrow ra \in M$

zu (2) Für $1 \le r \le n$ gilt $a_i = \sum_{j=1}^{n} \delta_{ij} a_j \in M$, wobei $\delta_{ij} = \begin{cases} 1_R & \text{falls } i = j \\ 0_R & \text{falls } i \ne j \end{cases}$

zu (3) Sei J ein Ideal in R mit $J \supseteq \{a_1, \dots, a_n\}$ z.zg.: $J \supseteq M$

Sei $a \in M$. $\Rightarrow \exists\, r_1, \dots, r_n \in R$ mit $a = \sum_{i=1}^{n} r_i a_i$

$r_1, \dots, r_n \in R$, $a_1, \dots, a_n \in J$, J Ideal $\Rightarrow r_i a_i \in J$ für $1 \le i \le n$

$\xRightarrow{J \text{ Ideal}} r_1 a_1 + \dots + r_n a_n \in J \Rightarrow a \in J$ $\square$

Definition der Teilerrelation

Definition (10.7)

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 (10.8)

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.

Definition des größten gemeinsamen Teilers

Definition (10.9)

Sei R ein Ring mit $a_1, ..., a_n \in R$. Wir sagen, ein Element $d \in R$ ist ein größter gemeinsamer Teiler (kurz ggT) von $a_1, ..., a_n$, 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 $a_1, ..., a_n$ teilerfremd, wenn 1_R ein ggT der Elemente ist.

Definition des kleinsten gemeinsamen Vielfachens

Definition (10.10)

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

Eindeutigkeit von ggT und kgV

Lemma (10.11)

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

Idealtheoretische Charakterisierung von ggT und kgV

Satz (10.12)

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 10.12

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

zu (i) bereits erledigt

zu (ii) Sei $d \in R$ mit $(d) = (a, b)$

Beh. d ist ein ggT von a und b.

zu überprüfen: (1) $d \mid a$, $d \mid b$

(2) Ist $c \in R$ mit $c \mid a$, $c \mid b$, dann folgt daraus $c \mid d$.

zu (1) $(d) = (a, b) \Rightarrow a, b \in (d)$

$a \in (d) \Rightarrow \exists\, r \in R$ mit $a = rd \Rightarrow d \mid a$

Ebenso überprüft man $d \mid b$.

<u>zu (2)</u> ggf: $c \in R$ mit $c \mid a$ und $c \mid b$.

$\Rightarrow \exists r, s \in R : a = rc, b = sc$

$d \in (a, b) \Rightarrow \exists t, t' \in R$ mit

$d = ta + t'b = trc + t'sc =$

$(tr + t's)c \Rightarrow c \mid d$

Setze nun voraus, dass R ein Hauptidealring ist. Sei $d' \in R$ ein ggT von a und b. Beh: $(d') = (a, b)$

Da R ein Hauptidealring ist, existiert ein $d'' \in R$ mit $(a, b) = (d'')$. Dann ist die Beh äquivalent zu $(d') = (d'')$

äquivalent dazu: $d' \mid d''$ und $d'' \mid d$, nach ii)

Aus $(a,b) = (d'')$ folgt, dass d'' ein ggT von a und b ist.

Da für d' dasselbe gilt, sind d' und d'' assoziiert,

d.h. $d' \mid d''$ und $d'' \mid d'$.

zu iii) siehe Skript. $\square$

Summen und Produkte von Idealen

Proposition (10.13)

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.

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.

Produkte endlich erzeugter Ideale

Proposition (10.15)

Sei R ein Ring, und seien I, J von endlichen vielen Ringelementen erzeugte Ideale, $I = (a_1, ..., a_m)$ und $J = (b_1, ..., b_n)$ 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

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

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

Beweis von Prop. 10.15:

geg: Ring R, endlich erzeugte Ideale I, J definiert durch $I = (a_1, \dots, a_m)$, $J = (b_1, \dots, b_n)$

<u>Beh</u>. $IJ = (S)$, wobei $S = \{ a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n \}$

Sei $T = \{ ab \mid a \in I, b \in J \}$ Nach Def. gilt $IJ = (T)$.

zu zeigen also: $(S) = (T)$ Dafür genügt es zu überprüfen, dass (1) $S \subseteq (T)$ (2) $T \subseteq (S)$ gilt

<u>zu (1)</u> $S \subseteq T$ (da $a_i \in I \; \forall i$, $b_j \in J \; \forall j$), $T \subseteq (T)$
$\implies S \subseteq (T)$

<u>zu (2)</u> Seien $a \in I$, $b \in J$. z.zg. $ab \in (S)$

zu (2) Seien $a \in I$, $b \in J$. z.zg. $ab \in (S)$

$a \in I \Rightarrow \exists r_1, \dots, r_m \in R$ mit $a = \sum_{i=1}^{m} r_i a_i$

$b \in J \Rightarrow \exists s_1, \dots, s_n \in R$ mit $b = \sum_{j=1}^{n} s_j b_j$

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

$\Rightarrow a \cdot b \in (S)$

$\square$

Anwendungsbeispiel:

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

In R gibt es keine „eindeutige Primfaktorzerlegung". Zum Beispiel gilt

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

und die Elemente $3, 7, 1 \pm 2\sqrt{-5} \in R$ lassen sich bis auf Einheiten nicht weiter zerlegen. $(\mathbb{Z}[\sqrt{5}])^\times = \{\pm 1\}$

Betrachte in R die Ideale

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

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

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

Prop. 10.15

$$= \left(3\cdot 3,\ 3\cdot(1-2\sqrt{-5}),\ (1+2\sqrt{-5})\cdot 3,\ (1+2\sqrt{-5})(1-2\sqrt{-5})\right)$$

$9 = 3\cdot 3$, $21 = 7\cdot 3$ $\Rightarrow$ 9, 21 liegen im Ideal rechts

$$= (9, 3-6\sqrt{-5}, 3+6\sqrt{-5}, 21) = (3, 3-6\sqrt{-5}, 3+6\sqrt{-5})$$

$3 = 21 + (-2)\cdot 9$ $\Rightarrow$ 3 liegt im linken Ideal

Alle drei Elemente sind Vielfache von 3, liegen also in (3)

$= (3)$

$[S \subseteq (T),\ T \subseteq (S) \Rightarrow (S) = (T)]$

Genauso überprüft man $\mathfrak{p}_1 \mathfrak{p}_3 = (1+2\sqrt{-5})$, $\mathfrak{p}_2 \mathfrak{p}_4 = (1-2\sqrt{-5})$,

$\mathfrak{p}_3 \mathfrak{p}_4 = (7)$

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

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

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

$$\stackrel{\text{Prop. 10.15}}{=} \left(3\cdot 3,\ 3\cdot(1-2\sqrt{-5}),\ (1+2\sqrt{-5})\cdot 3,\ (1+2\sqrt{-5})(1-2\sqrt{-5})\right)$$

$9 = 3\cdot 3$, $21 = 7\cdot 3$ $\Rightarrow$ $9, 21$ liegen im Ideal rechts

$$= (9, 3-6\sqrt{-5}, 3+6\sqrt{-5}, 21) = (3, 3-6\sqrt{-5}, 3+6\sqrt{-5})$$

Alle drei Elemente sind Vielfache von 3, liegen also in (3)

$\hookrightarrow 3 = 21 + (-2)\cdot 9$ $\Rightarrow$ 3 liegt im linken Ideal

$= (3)$

$[S \subseteq (T), T \subseteq (S) \Rightarrow (S) = (T)]$

Genauso überprüft man $\mathfrak{p}_1 \mathfrak{p}_3 = (1+2\sqrt{-5})$, $\mathfrak{p}_2 \mathfrak{p}_4 = (1-2\sqrt{-5})$,

$\mathfrak{p}_3 \mathfrak{p}_4 = (7)$

Das Distributivgesetz für Ideale

Lemma (10.16)

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

Primideale und maximale Ideale

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.

Charakterisierung der Primideale

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.

Kerne und Bilder von Ringhomomorphismen

Definition (10.19)

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

Urbilder und Bilder von Idealen

Proposition (10.20)

Seien R, S Ringe und $\phi : R \to S$ 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 $\phi : R \to S$ ein Ideal in R. Das Bild ist zwar stets ein Teilring von S, aber im Allgemeinen kein Ideal.

Beweis von Proposition 10.20

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

I Ideal in R, J Ideal in S

<u>Beh</u>: (i) $\phi^{-1}(J)$ ist Ideal in R

(ii) Ist ϕ surjektiv, dann ist $\phi(I)$ ein Ideal in S

<u>zu (i)</u> überprüfe: (1) $0_R \in \phi^{-1}(J)$ (2) $\forall r \in R, a, b \in \phi^{-1}(J)$: $a+b, ra \in \phi^{-1}(J)$

<u>zu (1)</u> J Ideal in $S \Rightarrow 0_S \in J \Rightarrow \phi(0_R) = 0_S \in J \Rightarrow 0_R \in \phi^{-1}(J)$

<u>zu (2)</u>

Seien $r \in R$, $a, b \in \phi^{-1}(J)$. $\Rightarrow \phi(a), \phi(b) \in J$

$\Rightarrow \phi(a+b) = \phi(a) + \phi(b) \in J$ (da J Ideal)

$\Rightarrow a + b \in \phi^{-1}(J)$

ebenso: $\phi(ra) = \underbrace{\phi(r)}_{\in S} \phi(a) \in J$, da J Ideal in S

$\Rightarrow ra \in \phi^{-1}(J)$

zu (ii) überprüfe: (1) $0_S \in \phi(I)$ (2) $\forall c, d \in \phi(I), s \in S$:
$c+d, sc \in \phi(I)$

zu (1) I Ideal $\Rightarrow 0_R \in I \Rightarrow 0_S = \phi(0_R) \in \phi(I)$

zu (2) Seien $c, d \in \phi(I)$, $s \in S$. $\Rightarrow \exists a, b \in I$ mit $c = \phi(a)$,
$d = \phi(b)$. ϕ surjektiv $\Rightarrow \exists r \in R$ mit $\phi(r) = s$

I Ideal, $a, b \in I \Rightarrow a+b \in I \Rightarrow c+d = \phi(a) + \phi(b) = \phi(a+b) \in \phi(I)$.

I Ideal, $a \in I$, $r \in R \Rightarrow ra \in I \Rightarrow sc = \phi(r)\phi(a) = \phi(ra) \in \phi(I)$

Betrachte den Ringhom. $\phi: \mathbb{Z} \to \mathbb{Q}$, $r \mapsto r$.

$(2) = 2\mathbb{Z}$ ist Ideal in $\mathbb{Z}$, aber $\phi(2\mathbb{Z}) = 2\mathbb{Z}$ ist kein Ideal in $\mathbb{Q}$, denn: $\square$
$\frac{1}{2} \in \mathbb{Q}$, $2 \in 2\mathbb{Z}$, aber $\frac{1}{2} \cdot 2 = 1 \notin 2\mathbb{Z}$

Definition (11.1)

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

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

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.

Die Kongruenzrelation modulo eines Ideals

Proposition (11.2)

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

$$a \equiv b \mod I \quad \Leftrightarrow \quad b - a \in I$$

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.

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

$$a \equiv b \mod I \quad \Leftrightarrow \quad b - a \in I \quad \Leftrightarrow \quad a + I = b + I \quad \Leftrightarrow \quad b \in a + I.$$

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

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

Gleichbedeutend damit ist die Feststellung, dass die Elemente der Menge $\{0, 1, ..., n-1\}$ 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

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

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

Addition und Multiplikation auf Nebenklassen

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 $a, b \in R$.

Existenz des Faktorrings

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 Faktorring bezeichnet. Die Abbildung $\pi_I : R \to R/I$ gegeben $a \mapsto a + I$ ist ein Epimorphismus von Ringen, der sog. kanonische Epimorphismus.