2.9 Ideale

Sei R ein Ring.

2.9.1 Definition: Ein *Ideal von R* ist eine Teilmenge $\mathfrak{a} \subset R$ mit den Eigenschaften:

(a) $\mathfrak{a} \neq \varnothing$. $\Leftarrow\!\!\Rightarrow$ $0 \in \mathfrak{a}$.
(b) $\forall a, b \in \mathfrak{a}\colon\ a + b \in \mathfrak{a}$.
} additive Untergruppe.
(c) $\forall x \in R\ \forall a \in \mathfrak{a}\colon\ xa \in \mathfrak{a}$.

$(-1) \cdot a = -a$

Wegen (c) gilt dann auch $\forall a \in \mathfrak{a}\colon\ -a \in \mathfrak{a}$; wegen (a) und (b) ist das Ideal also eine additive Untergruppe von R. Die Bedingungen bedeuten auch, dass für alle $n \geqslant 0$, alle $x_i \in R$, und alle $a_i \in \mathfrak{a}$ auch $\sum_{i=1}^{n} x_i a_i \in \mathfrak{a}$ ist. Ein Ideal $\mathfrak{a} \subsetneqq R$ heisst ein *echtes Ideal*.

2.9.2 Proposition-Definition: Für jedes Element $a \in R$ ist

$$(a) := \{xa \mid x \in R\} = Ra$$

ein Ideal von R, genannt das *von a erzeugte Hauptideal.*

Bew.: $0 \in (a)$

$xa, ya \in (a) \Rightarrow (x+y)a \in (a)$ ($xa + ya$)

$t \in R \quad (tx)a = t \cdot (xa) \in (a)$

qed.

2.9.3 Beispiel: Das *Nullideal* $(0) = \{0\}$.

2.9.4 Beispiel: Das *Einsideal* $(1) = R$. $\{x \cdot 1 \mid x \in R\}$

2.9.5 Proposition: (a) Es ist $(a) = (1)$ genau dann, wenn a eine Einheit von R ist.

(b) Ein Ideal $\mathfrak{a}$ ist gleich (1) genau dann, wenn es das Einselement enthält.

Bew. (b) $1 \in \mathfrak{a} \Rightarrow R = R1 \subset \mathfrak{a} \Rightarrow \mathfrak{a} = (1)$.

(a) $(a) = (1) \Rightarrow \exists x \in R : xa = 1 \Rightarrow a \in R^\times$. ;

$a \in R^\times \Rightarrow 1 = \bar{a}^{-1} \cdot a \in (a) \Rightarrow (a) = (1)$.

qed.

2.9.6 Proposition: Für alle Elemente a, b eines Integritätsbereichs R gilt

$$a|b \iff (a) \ni b \iff (a) \supset (b).$$

$\exists x \in R : xa = b$ $\quad \{xa \mid x \in R\}$ ✓

$\Rightarrow$ weil $Rb \subset Rxa \subset Ra$.

qed.

2.9.7 Proposition: Der Durchschnitt jeder nichtleeren Kollektion von Idealen ist ein Ideal.

2.9.8 Proposition-Definition: Die Summe jeder Kollektion von Idealen $\{\mathfrak{a}_\nu \mid \nu \in N\}$ ist ein Ideal:

$$\sum_{\nu\in N} \mathfrak{a}_\nu \;:=\; \left\{ \sum_{\nu\in N}{}' a_\nu \;\middle|\; \begin{array}{l} \text{alle } a_\nu \in \mathfrak{a}_\nu, \\ \text{fast alle } a_\nu = 0 \end{array} \right\}.$$

2.9.9 Proposition-Definition: Für jede Teilmenge $A \subset R$ ist die folgende Menge ein Ideal:

$$(A) \;:=\; \left\{ \sum_{a\in A}{}' x_a a \;\middle|\; \begin{array}{l} \text{alle } x_a \in R, \\ \text{fast alle } x_a = 0 \end{array} \right\} \;=\; \sum_{a\in A} (a),$$

genannt *von A erzeugt.* Für endlich viele Elemente $a_1, \ldots, a_n \in R$ schreiben wir auch

$$(a_1, \ldots, a_n) \;:=\; (\{a_1, \ldots, a_n\}) \;=\; (a_1) + \ldots + (a_n)$$

und hoffen auf möglichst wenig Verwechslung mit dem Tupel $(a_1, \ldots, a_n)$.

2.9.10 Proposition: Das Ideal (A) ist das eindeutige kleinste Ideal $\mathfrak{a} \subset R$ mit [illegible].

2.9.11 Bemerkung: Jeder gemeinsame Teiler von Elementen $a_1, \ldots, a_n$ ist ein gemeinsamer Teiler aller Elemente des Ideals $(a_1, \ldots, a_n)$. Der Begriff des Ideals enthält also alle Informationen über Teilbarkeit, auch wenn der Ring nicht faktoriell ist. Genau zu diesem Zweck hat Dedekind den Begriff des Ideals erfunden, um seine Vorstellung von *idealen Zahlen* zu konkretisieren.

2.9.12 Proposition: Für jedes $x \in R$ und jedes Ideal $\mathfrak{a}$ ist die folgende Menge ein Ideal

$$x\mathfrak{a} \;:=\; x \cdot \mathfrak{a} \;:=\; \{xa \mid a \in \mathfrak{a}\}.$$

$x(a+a') = xa + xa'$

$y(xa) = x\cdot(ya)$

2.9.13 Definition: Das *Produkt* zweier Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R ist das von den Elementen ab für alle $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ erzeugte Ideal

$$\mathfrak{ab} \;:=\; \mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; \text{alle } n \geqslant 0,\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}. \quad \neq \{ab \mid a\in\mathfrak{a},\ b\in\mathfrak{b}\}$$

2.9.14 Definition: Die *n-te Potenz* eines Ideals $\mathfrak{a}$ ist definiert durch

$$\mathfrak{a}^n \;:=\; \begin{cases} \mathfrak{a}\cdots\mathfrak{a} \text{ mit } n \text{ Faktoren} & \text{falls } n > 0, \\ R = (1) & \text{falls } n = 0. \end{cases}$$

Bsp.: $R = \mathbb{Z}$

$(2)\cdot(3) = (6)$.

$(1)\cdot\mathfrak{a} = \{x \mid x\in R\}\cdot\mathfrak{a} = \left\{ \sum_{i=1}^{n} x_i a_i \;\middle|\; \begin{array}{l} \text{alle } x_i \in R \\ \text{alle } a_i \in \mathfrak{a} \end{array} \right\} = \mathfrak{a}$.

Es gilt stets $\mathfrak{ab} \subset \mathfrak{a}$ und $\mathfrak{ab} \subset \mathfrak{b}$.

2.9.15 Proposition: Für alle $x, y \in R$, alle Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, und alle $m, n \in \mathbb{Z}^{\geq 0}$ gilt

auch:
$\mathfrak{a}+\mathfrak{b} = \mathfrak{b}+\mathfrak{a}$
$\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b})+\mathfrak{c}$
$\mathfrak{a}+(0) = \mathfrak{a}$

insbesondere $(1)\mathfrak{a} = \mathfrak{a}$

$$
\begin{aligned}
(x)\mathfrak{a} &= x\mathfrak{a} \\
(x)(y) &= (xy) \\
\mathfrak{a}\mathfrak{b} &= \mathfrak{b}\mathfrak{a} \\
\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) &= \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c} \\
x(\mathfrak{a}+\mathfrak{b}) &= x\mathfrak{a}+x\mathfrak{b} \\
\mathfrak{a}(\mathfrak{b}\mathfrak{c}) &= (\mathfrak{a}\mathfrak{b})\mathfrak{c} \\
x(\mathfrak{a}\mathfrak{b}) &= (x\mathfrak{a})\mathfrak{b} \\
x(y\mathfrak{a}) &= (xy)\mathfrak{a} \\
(x)^n &= (x^n) \\
\mathfrak{a}^m\mathfrak{a}^n &= \mathfrak{a}^{m+n} \\
\mathfrak{a}^n\mathfrak{b}^n &= (\mathfrak{a}\mathfrak{b})^n
\end{aligned}
$$

Bsp.:

$$\mathfrak{a}\cdot(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\cdot\{b+c \mid \substack{b\in\mathfrak{b}\\ c\in\mathfrak{c}}\} = \left\{\sum_{i=1}^{n} a_i(b_i+c_i) \;\middle|\; \substack{n\geq 0\\ a_i\in\mathfrak{a}\\ b_i\in\mathfrak{b}\\ c_i\in\mathfrak{c}}\right\}$$

$$= \left\{\sum_{i=1}^{n} a_ib_i + \sum_{i=1}^{n} a_ic_i \;\middle|\; \ldots\right\}$$

$$\subset \left\{\sum_{i=1}^{n} a_ib_i \;\middle|\; \substack{a_i\in\mathfrak{a}\\ b_i\in\mathfrak{b}}\right\} + \left\{\sum_{i=1}^{n} a_ic_i \;\middle|\; \substack{a_i\in\mathfrak{a}\\ c_i\in\mathfrak{c}}\right\} \subset \mathfrak{a}(\mathfrak{b}+\mathfrak{c})$$

$$= \mathfrak{a}\cdot\mathfrak{b} + \mathfrak{a}\cdot\mathfrak{c}$$

$$\mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c} = \left\{\sum_{i=1}^{n} a_ib_i + \sum_{j=1}^{m} a'_jc_j \;\middle|\; \substack{a_i,a'_j\in\mathfrak{a}\\ b_i\in\mathfrak{b},\ c_i\in\mathfrak{c}}\right\} = \left\{\sum_{i=1}^{n} a_i(b_i+0) + \sum_{j=1}^{m} a'_j(0+c_j) \;\middle|\; \ldots\right\}$$

2.9.16 Proposition: Für jeden Ringhomomorphismus $\varphi\colon R \to S$ ist

$$\begin{array}{lll} \mathrm{Kern}(\varphi) & := & \{a \in R \mid \varphi(a) = 0\} \quad \text{ein Ideal von } R, \text{ und} \\ \mathrm{Bild}(\varphi) & := & \{\varphi(a) \mid a \in R\} \qquad \text{ein Unterring von } S. \end{array}$$

Dabei ist $\mathrm{Kern}(\varphi) = (0)$ genau dann, wenn φ injektiv ist, und $\mathrm{Bild}(\varphi) = S$ genau dann, wenn φ surjektiv ist.

Bem.: $1_S = \varphi(1_R) \in \mathrm{Bild}(\varphi)$
$\mathrm{Bild}(\varphi)$ unter $+$ und $\cdot$ abgeschlossen
$\Rightarrow$ Unterring.

$\varphi(0) = 0 \Rightarrow 0 \in \mathrm{Kern}(\varphi)$.

$\forall a,b \in \mathrm{Kern}(\varphi) \Rightarrow \varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0 \Rightarrow a+b \in \mathrm{Kern}(\varphi)$.

$\forall a \in \mathrm{Kern}(\varphi)\ \forall x \in R: \quad \varphi(xa) = \varphi(x) \cdot \varphi(a) = \varphi(x) \cdot 0 = 0 \Rightarrow xa \in \mathrm{Kern}(\varphi)$

$\Rightarrow$ Ideal. qed.

2.10 Faktorringe

2.10.1 Definition: Sei $\mathfrak{a}$ ein Ideal von R. Für jedes $x \in R$ heisst die Teilmenge

$$x + \mathfrak{a} \;:=\; \{x + a \mid a \in \mathfrak{a}\} \;\subset\; R$$

eine *Nebenklasse von* $\mathfrak{a}$. Betrachte die Menge aller Nebenklassen

$$R/\mathfrak{a} \;:=\; \{x + \mathfrak{a} \mid x \in R\}.$$

2.10.2 Proposition: Je zwei Nebenklassen $x + \mathfrak{a}$ sind entweder gleich oder disjunkt, und die Vereinigung aller ist R. Genauer gilt für alle $x, x' \in R$:

$$x + \mathfrak{a} = x' + \mathfrak{a} \iff x \in x' + \mathfrak{a} \iff x' \in x + \mathfrak{a} \iff (x + \mathfrak{a}) \cap (x' + \mathfrak{a}) \neq \varnothing.$$

2.10.3 Proposition: Die Menge $R/\mathfrak{a}$ besitzt eine eindeutige Ringstruktur, so dass gilt:

(a) $\forall x, y \in R : (x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$.

(b) $\forall x, y \in R : (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = xy + \mathfrak{a}$.

Für diese gilt weiter:

(c) Das Nullelement von $R/\mathfrak{a}$ ist $0 + \mathfrak{a} = \mathfrak{a}$.

(d) Das Einselement von $R/\mathfrak{a}$ ist $1 + \mathfrak{a}$.

(e) Das additive Inverse von $x + \mathfrak{a}$ ist $(-x) + \mathfrak{a}$.

(f) $\pi : R \to R/\mathfrak{a}$, $x \mapsto x + \mathfrak{a}$ ist ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$.

zu zeigen: wohldefiniert.
$x + U = x' + U \Rightarrow x' - x \in U$
$y + U = y' + U \Rightarrow y' - y \in U$
$\Rightarrow x'y' - xy = x'(y' - y) + (x' - x)y \in U$
($\in U$, $\in U$)
$\Leftarrow$ (c) $\Rightarrow x'y' + U = xy + U$.

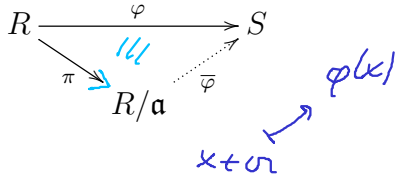
qed

2.10.4 Definition: Der Ring $R/\mathfrak{a}$ heisst der *Faktorring von R nach $\mathfrak{a}$*.

2.10.5 Beispiel: (a) Es ist $\mathfrak{a} = R$ genau dann, wenn $R/\mathfrak{a}$ der Nullring ist.

(b) Es ist $\mathfrak{a} = 0$ genau dann, wenn π ein Isomorphismus ist.

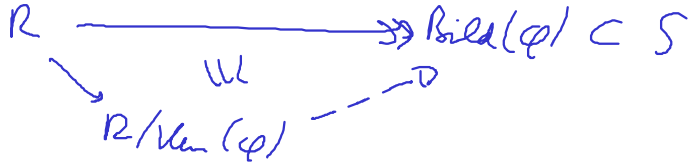
2.10.6 Proposition: *(Universelle Eigenschaft)* Für jeden Ring S und jeden Ringhomomorphismus $\varphi\colon R \to S$ mit $\mathfrak{a} \subset \mathrm{Kern}(\varphi)$ existiert genau ein Ringhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \to S$ mit $\overline{\varphi} \circ \pi = \varphi$, das heisst, so dass das folgende Diagramm kommutiert:



2.10.7 Proposition: *(Homomorphiesatz)* Jeder Ringhomomorphismus $\varphi\colon R \to S$ induziert einen Isomorphismus

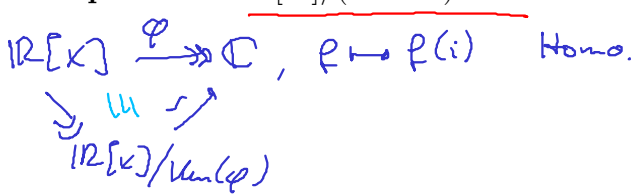
$$R/\operatorname{Kern}(\varphi) \xrightarrow{\sim} \operatorname{Bild}(\varphi).$$

Bew.:

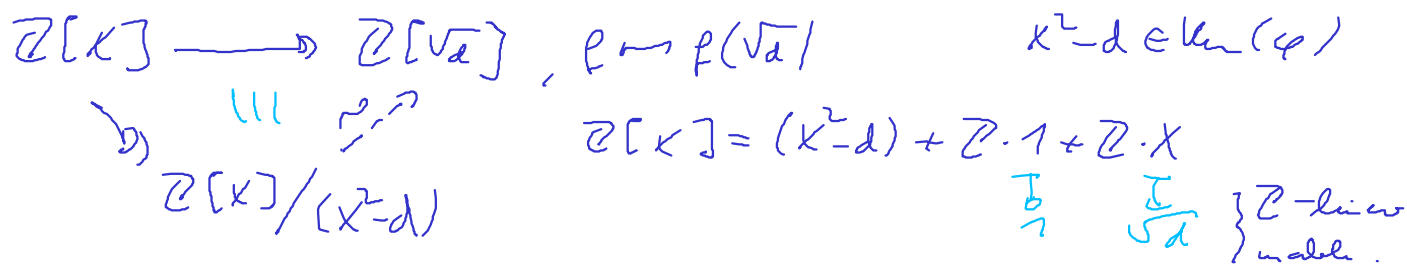


qed.

2.10.8 Beispiel: Es ist $\mathbb{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{C}$.



2.10.9 Beispiel: Für jede ganze Zahl d, die kein Quadrat ist, gilt $\mathbb{Z}[X]/(X^2-d) \cong \mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$.



2.11 Primideale

$\mathfrak{p} = (p)$ ist Primideal g.d.w. $p \notin R^\times$ und $\forall x,y \in R$: $p \mid xy \Rightarrow (p \mid x \vee p \mid y)$

2.11.1 Definition: Ein *Primideal von R* ist ein echtes Ideal $\mathfrak{p} \subsetneq R$ mit der Eigenschaft:

$$\forall x, y \in R\colon xy \in \mathfrak{p} \longrightarrow (x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}).$$

2.11.2 Proposition: Ein Ideal $\mathfrak{p}$ von R ist ein Primideal genau dann, wenn der Faktorring $R/\mathfrak{p}$ ein Integritätsbereich ist.

Bew.: $1 \neq 0$ in $R/\mathfrak{p} \iff R/\mathfrak{p} \neq \{0\} \iff \mathfrak{p} \subsetneq R$.

$R/\mathfrak{p}$ nullteilerfrei $\iff \forall \bar{x}, \bar{y} \in R/\mathfrak{p}: (\bar{x}\bar{y} \neq 0 \Rightarrow \bar{x} \neq 0)$

$\iff \forall x, y \in R: (xy \notin \mathfrak{p} \Rightarrow xy \notin \mathfrak{p})$ $\iff (xy \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \vee y \in \mathfrak{p}))$ qed.

2.11.3 Definition: Ein *maximales Ideal von R* ist ein echtes Ideal $\mathfrak{m} \subsetneq R$, welches unter allen echten Idealen maximal ist, das heisst, so dass jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subset \mathfrak{a}$ entweder gleich $\mathfrak{m}$ oder gleich R ist.

2.11.4 Proposition: Ein Ideal $\mathfrak{m}$ von R ist maximal genau dann, wenn der Faktorring $R/\mathfrak{m}$ ein Körper ist.

Beweis: $1 \neq 0$ in $R/\mathfrak{m} \iff \mathfrak{m} \subsetneq R$ wie oben.

$R/\mathfrak{m}$ Körper $\iff \forall \bar{x} \in R/\mathfrak{m}, (\bar{x} \neq 0 \Rightarrow \exists \bar{y} \in R/\mathfrak{m}: \bar{x}\bar{y} = 1)$

$\iff \forall x \in R \setminus \mathfrak{m}: \exists y \in R: xy + \mathfrak{m} = 1 + \mathfrak{m}$

Dann: Sei $\mathfrak{m} \subsetneq \mathfrak{a} \subset R \Rightarrow$ wähle $x \in \mathfrak{a} \setminus \mathfrak{m} \Rightarrow 1 \in xy + \mathfrak{m} \in \mathfrak{a} \Rightarrow \mathfrak{a} = (1) = R$.

Umgekehrt: Ist $\mathfrak{m}$ maximal, gilt für alle $x \in R \setminus \mathfrak{m}$: $(x) + \mathfrak{m} \neq \mathfrak{m} \Rightarrow (x) + \mathfrak{m} = (1)$ qed

$\Rightarrow \exists y \in R: xy + \mathfrak{m} = 1 + \mathfrak{m}$.