10. Ideale und Homomorphismen

Def. Sei R ein Ring und $\mathfrak{a} \subseteq R$.
Dann heisst $\mathfrak{a}$ Ideal (in R) falls gilt:
(i) $\mathfrak{a}$ ist additive Untergruppe von R,
(ii) für $r \in R$ und $a \in \mathfrak{a}$ ist $r \cdot a \in \mathfrak{a}$ und $a \cdot r \in \mathfrak{a}$.

Faktum 10.1 $\mathfrak{a} \subseteq R$ ist genau dann ein Ideal in R, wenn gilt:
(1) $\mathfrak{a} \neq \emptyset$
(2) $a, b \in \mathfrak{a} \Rightarrow a + b \in \mathfrak{a}$
(3) $r \in R,\ a \in \mathfrak{a} \Rightarrow r \cdot a, a \cdot r \in \mathfrak{a}$

Beweis: ($\Rightarrow$) klar

($\Leftarrow$) (3) entspricht (ii), somit ist nur zu zeigen, dass $\mathfrak{a}$ eine additive Untergruppe ist:
Mit (3) ist mit $b \in \mathfrak{a}$ auch $(-1) \cdot b = -b \in \mathfrak{a}$,
also ist mit (2) mit $a, b \in \mathfrak{a}$ auch $a + (-b) \in \mathfrak{a}$. ⊣

[Unterschied Unterring – Ideal]

Beispiele: • Ist $\varphi : R \to S$ ein Ringhomom., so ist $\ker(\varphi)$ ein Ideal in R.

• $\{0\} \subseteq R$ ist ein Ideal

[Ist $S = \{0\}$, so ist $\ker(\varphi) = R$]

Für $a, b \in \ker(\varphi)$, $r \in R$ gilt: $\underbrace{\varphi(0) = 0}_{(1)}$; $\underbrace{\varphi(a+b) = \varphi(a) + \varphi(b) = 0}_{(2)}$;

$$\underbrace{\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = 0}_{(3)}$$

• $m\mathbb{Z}$ (für $m \in \mathbb{Z}$) ist ein Ideal in $\mathbb{Z}$.

• $C(\mathbb{R})$ sei der Ring aller Fkt. $f : \mathbb{R} \to \mathbb{R}$ mit punktweiser Add. & Mult. und sei $M \subseteq \mathbb{R}$. Dann ist $\mathfrak{a}_M := \{ f : f|_M = \{0\} \}$ ein Ideal in $C(\mathbb{R})$.

Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal.

Da $\mathfrak{a} \leq (R,+)$ (d.h. $\mathfrak{a}$ ist add. UG der abelschen Gruppe $(R,+)$) ist $\mathfrak{a} \trianglelefteq (R,+)$, d.h. $R/\mathfrak{a}$ ist abelsche Gruppe bzgl. $+$.

Definieren wir nun die Mult. auf $R/\mathfrak{a}$ durch

$$\underbrace{(a+\mathfrak{a})}_{\text{Nebenklasse}} \cdot (b+\mathfrak{a}) := (a\cdot b) + \mathfrak{a},$$

so wird $R/\mathfrak{a}$ zu einem Ring.

- wohldefiniert: $a+\mathfrak{a} = a'+\mathfrak{a} \Rightarrow a+(-a') \in \mathfrak{a}$

  also $a-a' \in \mathfrak{a}$

  analog $b-b' \in \mathfrak{a}$ für $b+\mathfrak{a} = b'+\mathfrak{a}$.

  $$\Rightarrow (a-a')\cdot b = ab - a'b \in \mathfrak{a}$$
  $$a'\cdot(b-b') = a'b - a'b' \in \mathfrak{a} \quad \oplus$$

  $$\Rightarrow ab - a'b' \in \mathfrak{a}, \text{ also } (a\cdot b)+\mathfrak{a} = (a'\cdot b')+\mathfrak{a}$$

- weiter gilt: $((a+b)\cdot c)+\mathfrak{a} = ((a\cdot c)+(b\cdot c))+\mathfrak{a}$ etc.

Die Abbildung $\pi: R \to R/\mathfrak{a}$, $a \mapsto a+\mathfrak{a}$ ist ein surj. Ringhomom. (natürlicher Ringhom.)

<u>Bem.</u> Ist $\mathfrak{a} = R$, so ist $R/\mathfrak{a} = \{0+\mathfrak{a}\}$.

<u>Def.</u> Der Ring $R/\mathfrak{a}$ heisst <u>Quotientenring</u> von R bzgl. $\mathfrak{a}$. Zwei Elemente $a,b \in R$ heissen <u>kongruent modulo $\mathfrak{a}$</u> falls $a-b \in \mathfrak{a}$, bzw. $a+\mathfrak{a} = b+\mathfrak{a}$, bezeichnet mit $a \equiv b \pmod{\mathfrak{a}}$. Die <u>Restklasse</u> von a bzgl. $\mathfrak{a}$ ist $\bar{a} := \{b \in R : a \equiv b \pmod{\mathfrak{a}}\}$ bzw. $\bar{a} = a+\mathfrak{a}$ (mit Lem. 2.4.(e)).

<u>Bsp.</u> $m \in \mathbb{N}$, $R = \mathbb{Z}/m\mathbb{Z}$; $\bar{a}\cdot\bar{b} = \overline{a\cdot b}$.

<u>Def.</u> Sei R ein Ring und $S \subseteq R$ eine Teilmenge.
Dann ist

$$(S) := \bigcap_{\substack{\mathfrak{a} \subseteq R \text{ Ideal} \\ S \subseteq \mathfrak{a}}} \mathfrak{a}$$

das von S erzeugte Ideal in R.

Faktum 10.2 (a) (S) ist Ideal in R.

(b) (S) ist das kl. Ideal in R das S enthält.

Beweis: (a) $0 \in (S)$ weil $0 \in \mathfrak{a}$ für alle Ideale $\mathfrak{a}$ von R.

$a, b \in (S)$, dann $a + b \in (S)$ (nach Def. von (S)).

$a \in (S)$ und $r \in R$, dann $r \cdot a \in (S)$ (nach Def. von (S)).
$a \cdot r$,

(b) klar.

$\dashv$

Notation: Ist S endlich, d.h. $S = \{a_0, \dots, a_n\}$, so schreiben wir $(a_0, \dots, a_n)$ für (S).

Def. Ein Ideal heisst *Hauptideal* wenn es von einem Element erzeugt wird. Ein *Hauptidealring* ist ein *Integritätsring* (d.h. nicht-trivial, komm., nullteilerfrei) in dem jedes Ideal ein Hauptideal ist.

Bsp. $\mathbb{Z}$ ist ein Hauptidealring; insbesondere ist jedes Ideal $\mathfrak{a} \subseteq \mathbb{Z}$ von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$:

- Sei $\mathfrak{a} \subseteq \mathbb{Z}$ ein Ideal und sei $m := \min\{a \in \mathfrak{a} : a > 0\}$; wenn m nicht ex. dann ist $\mathfrak{a} = (0) = 0 \cdot \mathbb{Z}$.
- Für jedes $x \in \mathfrak{a}$ ex. $b, r \in \mathbb{Z}$ mit $x = b \cdot m + r$ und $0 \leq r < m$. Also $r = x - b \cdot m$, und weil $x, bm \in \mathfrak{a}$, ist auch $r \in \mathfrak{a}$.
- Wegen der Minimalität von m ist $r = 0$, d.h. $x \in (m)$, und weil $x \in \mathfrak{a}$ beliebig war ist $\mathfrak{a} = (m) = m\mathbb{Z}$.

Proposition 10.3 Sei R ein komm., nicht-trivialer Ring. Dann gilt:

R ist ein Körper $\Longleftrightarrow$ die einzigen Ideale von R sind (0) und R.

Beweis: ($\Rightarrow$) Sei R ein Körper und $\mathfrak{a} \subseteq R$, $\mathfrak{a} \neq (0)$ ein Ideal.

zu zeigen: $\mathfrak{a} = R$

- Weil $\mathfrak{a} \neq (0)$ ex. ein $x \in \mathfrak{a}$ mit $x \neq 0$.
- Weil R ein Körper ist ex. $x^{-1} \in R$, und weil $x \in \mathfrak{a}$ ist auch $\underbrace{x^{-1}}_{\in R} \cdot \underbrace{x}_{\in \mathfrak{a}} = 1 \in \mathfrak{a}$.
- Ist $r \in R$ beliebig, dann ist auch $\underbrace{r}_{\in R} \cdot \underbrace{1}_{\in \mathfrak{a}} = r \in \mathfrak{a}$, also ist $\mathfrak{a} = R$.

($\Leftarrow$) Die einzigen Ideale in R seien (0) und R.

zu zeigen: $R^* = R \setminus \{0\}$.

- Sei $a \in R$, $a \neq 0$ beliebig. Dann ist $(0) \subsetneq (a)$, also ist mit Vorraussetzung $(a) = R$.
- Da $1 \in R$ ist somit $1 \in (a)$, und da

  $(a) = \{r \cdot a : r \in R\}$ [beachte: $a+a = (1+1) \cdot a$; $-a = (-1) \cdot a$]

  ex. $r \in R$ mit $r \cdot a = 1$, also $a \in R^*$.

$\dashv$

Def. Sei R ein Ring und $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in R.

$\mathfrak{a} + \mathfrak{b} := \{x + y : x \in \mathfrak{a} \wedge y \in \mathfrak{b}\}$

$\mathfrak{a} \cdot \mathfrak{b} := (\{x \cdot y : x \in \mathfrak{a} \wedge y \in \mathfrak{b}\})$ [das von "$x \cdot y$" erzeugte Ideal die Prod. selbst bilden i.A. kein Ideal]

Lemma 10.4 Sei R ein Ring und $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in R.

(1) $\mathfrak{a} + \mathfrak{b}$ ist ein Ideal in R.

(2) $(\mathfrak{a} \cup \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ (2') $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{a} \cdot \mathfrak{b}$

(3) $\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=0}^{n} x_i \cdot y_i : n \in \mathbb{N} \wedge x_i \in \mathfrak{a} \wedge y_i \in \mathfrak{b}\}$

(4) "$\cdot$" ist assoziativ

(5) Es gelten die Links- & Rechtsdistributivgesetze.

Beweis. (1) Mit $x_1 + y_1$ und $x_2 + y_2$ in $\mathfrak{a} + \mathfrak{b}$, ist auch

$(x_1 + y_1) - (x_2 + y_2) = (x_1 + y_1) + (-x_2 - y_2) = \underbrace{\underbrace{(x_1 - x_2)}_{\in \mathfrak{a}} + \underbrace{(y_1 - y_2)}_{\in \mathfrak{b}}}_{\in \mathfrak{a} + \mathfrak{b}}$

in $\mathfrak{a} + \mathfrak{b}$, sowie $r(x_1 + y_1) = \underbrace{r x_1}_{\in \mathfrak{a}} + \underbrace{r y_1}_{\in \mathfrak{b}}$.

(2) • Es gilt $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$, also gilt $\mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ und mit (1) ist $(\mathfrak{a} \cup \mathfrak{b}) \subseteq \mathfrak{a} + \mathfrak{b}$.

• Sei $\mathfrak{d} \subseteq R$ ein Ideal mit $\mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{d}$ und somit $(\mathfrak{a} \cup \mathfrak{b}) \subseteq \mathfrak{d}$. Für $x \in \mathfrak{a}$ und $y \in \mathfrak{b}$ gilt dann $x, y \in \mathfrak{d}$, d.h. $x + y \in \mathfrak{d}$ und somit gilt, weil x, y beliebig waren, $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{d}$.

(2') • Aus dem Beweis von Faktum 10.2. (a) folgt, dass $\mathfrak{a} \cap \mathfrak{b}$ ein Ideal ist und per Def. ist $\mathfrak{a} \cdot \mathfrak{b}$ ein Ideal. [$z_1, z_2 \in \mathfrak{a} \cap \mathfrak{b} \Rightarrow z_1 + z_2 \in \mathfrak{a} \cap \mathfrak{b}$ ist klar]

• Ist nun $x \in \mathfrak{a}$ und $y \in \mathfrak{b}$, dann ist

$$\underbrace{x}_{\in R} \cdot \underbrace{y}_{\in \mathfrak{b}} \in \mathfrak{b} \quad \text{und} \quad \underbrace{x}_{\in \mathfrak{a}} \cdot \underbrace{y}_{\in R} \in \mathfrak{a}, \text{ also } x \cdot y \in \mathfrak{a} \cap \mathfrak{b}.$$

Also ist $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

(3)-(5) Definitionen benutzen und nachrechnen. ⊣

Bsp. $R = \mathbb{Z}$, $\mathfrak{a} = 3\mathbb{Z}$, $\mathfrak{b} = 5\mathbb{Z}$: $(\mathfrak{a} \cup \mathfrak{b}) = \mathbb{Z}$; $\mathfrak{a} \cdot \mathfrak{b} = 15\mathbb{Z} = \mathfrak{a} \cap \mathfrak{b}$.

Das folgende Lemma ist ähnlich wie der 1. Isom-Satz für Gruppen:

<u>Lemma 10.5</u> Sei $\varphi : R \to S$ ein Ringhomom. und $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a} \subseteq \ker(\varphi)$. Dann ex. ein eindeutig bestimmter Ringhomom. $\bar{\varphi} : R/\mathfrak{a} \to S$, sodass das Diag.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\ R/\mathfrak{a} \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

kommutiert. Insbesondere gilt:

$$\bar{\varphi}[R/\mathfrak{a}] = \varphi[R] \quad \text{und}$$
$$\ker(\bar{\varphi}) = \ker(\varphi)/\mathfrak{a}$$

<u>Beweis:</u> Wir definieren $\bar{\varphi}(\overbrace{x + \mathfrak{a}}^{\bar{x}}) := \varphi(x)$.

• $\bar{\varphi}$ ist wohldefiniert:

$$\bar{x} = \bar{y} \Leftrightarrow x - y \in \mathfrak{a} \overset{\mathfrak{a} \subseteq \ker(\varphi)}{\Longrightarrow} x - y \in \ker(\varphi) \Leftrightarrow \varphi(x-y) = 0$$
$$\Leftrightarrow \varphi(x) - \varphi(y) = 0 \Leftrightarrow \varphi(x) = \varphi(y).$$

• $\bar{\varphi}$ ist Ringhomom.: folgt direkt aus "φ ist Ringhomom." und der Def. von $\bar{\varphi}$ (nachrechnen).

- $\bar{\varphi}$ ist eindeutig und $\bar{\varphi}[R/\mathfrak{a}] = \varphi[R]$: das ist analog zum Beweis vom 1. Isom. Satz für Gruppen.

- $\ker(\bar{\varphi}) = \ker(\varphi)/\mathfrak{a}$:

$$\ker(\bar{\varphi}) = \{x+\mathfrak{a} \in R/\mathfrak{a} : \varphi(x) = 0\}$$
$$= \{x+\mathfrak{a} \in R/\mathfrak{a} : x \in \ker(\varphi)\} = \ker(\varphi)/\mathfrak{a}$$

[Beispiel]

<u>Folgerung</u>: Für $\mathfrak{a} = \ker(\varphi)$ erhalten wir mit

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \varphi[R] \subseteq S \\ R/\ker(\varphi) \arrow[ur, "\bar{\varphi}", "\cong"'] & \end{tikzcd}$$

dass gilt: $\varphi[R] \cong R/\ker(\varphi)$.

<u>Bew.</u> Weil gilt $\ker(\bar{\varphi}) = \underbrace{\ker(\varphi)/\ker(\varphi)}_{=\{0\}}$, ist $\bar{\varphi}$ injektiv,

und aus $\bar{\varphi}[R/\ker(\varphi)] = \varphi[R]$ folgt $\bar{\varphi}$ ist surjektiv; also ist $\bar{\varphi}$ ein Isomorphismus. ⊣

<u>Theorem 10.6</u> (1. Isomorphiesatz)

Sei R ein Ring, $S \subseteq R$ ein Unterring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist $S+\mathfrak{a} = \{x+a : x \in S \wedge a \in \mathfrak{a}\}$ ein Unterring von R der $\mathfrak{a}$ als Ideal enthält und es gilt:

$$S/S\cap\mathfrak{a} \cong (S+\mathfrak{a})/\mathfrak{a}$$

[<u>Bem.</u> $S\cap\mathfrak{a}$ ist ein Ideal in S; lässt sich einfach zeigen, folgt aber später]

<u>Beweis:</u> • $S+\mathfrak{a}$ ist Unterring von R:

$$(x+a)\cdot(y+b) = \underbrace{x\cdot y}_{\in S} + \underbrace{x\cdot b}_{\in\mathfrak{a}} + \underbrace{a\cdot y}_{\in\mathfrak{a}} + \underbrace{a\cdot b}_{\in\mathfrak{a}} \in S+\mathfrak{a}$$

• $\mathfrak{a} \subseteq S+\mathfrak{a}$ ist ein Ideal: klar

• Betrachte

$$\begin{tikzcd} S \arrow[r, hook] \arrow[rr, bend left, "\varphi"] & S+\mathfrak{a} \arrow[r, "\pi"] & S+\mathfrak{a}/\mathfrak{a} \\ x \arrow[r, mapsto] & x+0 \arrow[r, mapsto] & (x+0)+\mathfrak{a} \end{tikzcd}$$

<u>Bem:</u> S ist Unterring von $S+\mathfrak{a}$

- φ ist Ringhomom.:

$$\varphi(x+y) = (\underbrace{(x+y)+\mathfrak{a}}_{(x+\mathfrak{a})+(y+\mathfrak{a})}) + \mathfrak{a} = (\underbrace{(x+\mathfrak{a})+\mathfrak{a}}_{\varphi(x)}) + (\underbrace{(y+\mathfrak{a})+\mathfrak{a}}_{\varphi(y)})$$

$$\varphi(x\cdot y) = (\underbrace{(x\cdot y)+\mathfrak{a}}_{(x+\mathfrak{a})\cdot(y+\mathfrak{a})}) + \mathfrak{a} = (\underbrace{(x+\mathfrak{a})+\mathfrak{a}}_{\varphi(x)}) \cdot (\underbrace{(y+\mathfrak{a})+\mathfrak{a}}_{\varphi(y)})$$

$$\varphi(1) = (1+\mathfrak{a})+\mathfrak{a} = 1_{S+\mathfrak{a}/\mathfrak{a}}$$

- $\ker(\varphi) = \{x \in S : x+\mathfrak{a} \in \mathfrak{a}\} = \{x \in S : x \in \mathfrak{a}\} = S \cap \mathfrak{a}$;

  insbesondere ist $S \cap \mathfrak{a}$ ein Ideal in S.

- $\varphi[S] = \{x+\mathfrak{a}+\mathfrak{a} : x \in S\} = \{x+a+\mathfrak{a} : x \in S \wedge a \in \mathfrak{a}\}$

  ergibt dieselben Nebenklassen

also ist $\varphi[S] = S+\mathfrak{a}/\mathfrak{a}$. Wir erhalten somit:

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d, "\pi"] & S+\mathfrak{a}/\mathfrak{a} = \varphi[S] \\
\underbrace{S/S\cap\mathfrak{a}}_{= S/\ker(\varphi)} \arrow[ur, "\cong"'] &
\end{tikzcd}$$

$\cong$ mit Folgerung aus Lem. 10.5

somit gilt: $S/S\cap\mathfrak{a} \cong S+\mathfrak{a}/\mathfrak{a}$ $\dashv$

Theorem 10.7 (2. Isomorphiesatz)

Seien R, S Ringe, $\varphi: R \to S$ ein surjektiver Ringhomom., und $\mathfrak{a} \subseteq R$ ein Ideal mit $\ker(\varphi) \subseteq \mathfrak{a}$. Dann ist

$$R/\mathfrak{a} \cong S/\varphi[\mathfrak{a}].$$

[Beweis in den Übungen.]

Beispiel: $R = \mathbb{Z}\times\mathbb{Z}$, $S = \mathbb{Z}\times\{0\}$, $\mathfrak{a} = 3\mathbb{Z}\times\mathbb{Z}$

$$\varphi: R \to S \;; \quad \ker(\varphi) = \{0\}\times\mathbb{Z}$$
$$(x,y) \mapsto (x,0) \qquad \varphi[\mathfrak{a}] = 3\mathbb{Z}\times\{0\}$$

Theorem 10.8 (Chinesischer Restsatz)

Sei R ein Ring, $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$, und seien $b_1, \dots, b_n \in R$. Dann ex. $b \in R$ mit $b \equiv b_i \pmod{\mathfrak{a}_i}$ für alle $1 \leq i \leq n$. Zudem ist b modulo $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$ eindeutig bestimmt.

[Thm. formulieren für $R = \mathbb{Z}$]

Beweis: Wir zeigen zuerst folgende

Beh. $R = \mathfrak{a}_k + \bigcap_{j \neq k} \mathfrak{a}_j$ für alle $1 \leq k \leq n$.

Bew. Mit Induktion nach n.

Vorraussetzung: $n = 2$ ✓

Annahme: $R = \mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1})$

$$\text{Es ist } R = R \cdot R = \underbrace{\left(\mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1})\right)}_{=R} \cdot \overbrace{(\mathfrak{a}_1 + \mathfrak{a}_n)}^{=R}$$

$$= \overbrace{\underbrace{R \cdot \mathfrak{a}_1}_{=\mathfrak{a}_1} + \underbrace{\mathfrak{a}_1 \cdot \mathfrak{a}_n}_{\subseteq \mathfrak{a}_1 \cap \mathfrak{a}_n}}^{=\mathfrak{a}_1} + \underbrace{(\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1}) \cdot \mathfrak{a}_n}_{\subseteq \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_n}$$

Lem. 10.4.(2') $\Rightarrow$ $\subseteq \mathfrak{a}_1$

$\Rightarrow R \subseteq \mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1}) \cdot \mathfrak{a}_n$

Also $R = \mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_n)$. ⊣ Beh.

- Seien nun $b_1, \dots, b_n \in R$. Dann ex. für jedes k mit $1 \leq k \leq n$ ein $a_k \in \mathfrak{a}_k$ und ein $r_k \in \bigcap_{j \neq k} \mathfrak{a}_j$ mit $b_k = a_k + r_k$.

  Definiere $b := r_1 + \dots + r_n$.

  Dann ist $b - b_i = b - a_i - r_i = \sum_{k \neq i} r_k - a_i$. $(*)$

  Weil $r_k \in \bigcap_{j \neq k} \mathfrak{a}_j$ gilt für $k \neq i$: $r_k \in \bigcap_{j \neq k} \mathfrak{a}_j \subseteq \mathfrak{a}_i$.

  D.h. $\sum_{k \neq i} r_k \in \mathfrak{a}_i$ und somit $b - b_i \in \mathfrak{a}_i$ (folgt aus $(*)$)

  also $b \equiv b_i \pmod{\mathfrak{a}_i}$.

- Seien $b, c \in R$ mit $b \equiv b_i \pmod{\mathfrak{a}_i}$ und $c \equiv b_i \pmod{\mathfrak{a}_i}$.

  Für $1 \leq i \leq n$ gilt: $b - b_i, c - b_i \in \mathfrak{a}_i$, d.h. $(b - b_i) - (c - b_i) \in \mathfrak{a}_i$

  und somit ist $b - c = (b - b_i) - (c - b_i) \in \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$. ⊣

Korollar 10.9 Seien R und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ wie in Thm. 10.8.

Dann ist $R/_{\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n} \cong R/_{\mathfrak{a}_1} \oplus \cdots \oplus R/_{\mathfrak{a}_n}$.

[Kor. formulieren für $R = \mathbb{Z}$]

Beweis: Betrachte $\varphi: R \to R/_{\mathfrak{a}_1} \oplus \cdots \oplus R/_{\mathfrak{a}_n}$

$r \longmapsto (r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n)$

- $\ker(\varphi) = \{r \in R : \forall i\, (r \equiv 0 \pmod{\mathfrak{a}_i})\} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$.
- Mit Lemma 10.5 bzw. der Folgerung gilt $R/_{\ker(\varphi)} \cong \varphi[R]$.
- Ist $\bar{b} = (b_1 + \mathfrak{a}_1, \ldots, b_n + \mathfrak{a}_n) \in R/_{\mathfrak{a}_1} \oplus \cdots \oplus R/_{\mathfrak{a}_n}$, so ex. mit Chin. Restsatz 10.8 ein $b \in R$ mit $\varphi(b) = \bar{b}$, d.h. φ ist surjektiv. ⊣

Def. Sei R ein Ring.

- Der Primring von R ist der kleinste nicht-triviale Unterring von R.
- Für $n \in \mathbb{N}$ und $a \in R$ sei $n \cdot a = \underbrace{(a + \ldots + a)}_{n\text{-mal}}$ und $(-n) \cdot a := -(n \cdot a)$.

Proposition 10.10 Der Primring eines nicht-trivialen Rings ist eindeutig bestimmt und isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n > 0$ ($n \in \mathbb{N}$).

Beweis: Sei R ein nicht-trivialer Ring. Definiere $\varphi: \mathbb{Z} \to R$

$n \longmapsto n \cdot 1_R$ mit $-n \cdot 1_R = n \cdot (-1_R)$

- Dann ist φ ein Ringhom. und $\varphi[\mathbb{Z}]$ ist Unterring von R.
- Sei $S := \varphi[\mathbb{Z}]$, dann ist $S \cong \mathbb{Z}/\ker(\varphi)$ und S ist der Primring von R. [$S \neq \{0\}$ und $S \subseteq S'$ für alle Unterringe $S' \subseteq R$]
- Weil $\mathbb{Z}$ ein Hauptidealring ist und $\ker(\varphi)$ ein Ideal in $\mathbb{Z}$ ist, ist $\ker(\varphi) = (n)$ für ein $n \in \mathbb{N}$.
- D.h. $\underbrace{S \cong \mathbb{Z} \text{ (für } n = 0)}_{}$ oder $\underbrace{S \cong \mathbb{Z}/n\mathbb{Z} \text{ (für } n > 0)}_{}$. ⊣

Def. Charakteristik von R: $\operatorname{char}(R) = 0$ $\qquad$ $\operatorname{char}(R) = n$