

Sei R ein Ring und $\alpha \subseteq R$ ein Ideal.

Da $\alpha \subseteq (R, +)$ (d.h. α ist add. UG der abelschen Gruppe $(R, +)$)
ist $\alpha \trianglelefteq (R, +)$, d.h. R/α ist abelsche Gruppe bzgl. $+$.

Definieren wir nun die Mult. auf R/α durch

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

so wird R/α zu einem Ring.

• wohldefiniert: $a+\alpha = a'+\alpha \Rightarrow a+(-a') \in \alpha$

$$\text{also } a-a' \in \alpha$$

analog $b-b' \in \alpha$ für $b+\alpha = b'+\alpha$.

$$\Rightarrow b \cdot (a-a') = ab - a'b \in \alpha$$

$$a' \cdot (b-b') = a'b - a'b' \in \alpha$$

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

• weiter gilt: $((a+b) \cdot c) + \alpha = ((a \cdot c) + (b \cdot c)) + \alpha$ etc.

Die Abbildung $\pi: R \rightarrow R/\alpha$ ist ein surj. Ringhomom.

$$a \mapsto a+\alpha$$

(natürlicher Ringhom.)

Bem. Ist $\alpha = R$, so ist $R/\alpha = \{0+\alpha\}$.

Def. Der Ring R/α heißt Quotientenring von R bzgl. α .

Zwei Elemente $a, b \in R$ heißen kongruent modulo α

falls $a-b \in \alpha$, bzw. $a+\alpha = b+\alpha$, bezeichnet mit

$a \equiv b \pmod{\alpha}$. Die Restklasse von a bzgl. α ist

$$\bar{a} := \{b \in R : a \equiv b \pmod{\alpha}\} \text{ bzw. } \bar{a} = a+\alpha \text{ (mit Lem. 2.4.(e)).}$$

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

Def. Sei R ein Ring und $S \subseteq R$ eine Teilmenge.

Dann ist

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

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 $0 \in \alpha$ für alle Ideale α 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)).

(b) klar.

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, kommut., nullteilerfrei) in dem jedes Ideal ein Hauptideal ist.

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

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

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

Dann gilt:

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

Beweis: ($\Rightarrow$) Sei R ein Körper und $\alpha \subseteq R, \alpha \neq (0)$ ein Ideal.

zu zeigen: $\alpha = R$

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

($\Leftarrow$) 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 $(0) \neq (a)$, also ist mit Voraussetzung $(a) = R$.
- 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 $a \in R^*$.

Def. Sei R ein Ring und $\alpha, \beta \subseteq R$ Ideale in R .

$$\alpha + \beta := \{x+y : x \in \alpha \wedge y \in \beta\}$$

$$\alpha \cdot \beta := (\{x \cdot y : x \in \alpha \wedge y \in \beta\}) \quad [\text{das von "x.y" erzeugte Ideal}]$$

Lemma 10.4 Sei R ein Ring und $\alpha, \beta \subseteq R$ Ideale in R .

(1) $\alpha + \beta$ ist ein Ideal in R .

(2) $(\alpha \cup \beta) = \alpha + \beta$ (2') $\alpha \cap \beta \supseteq \alpha \cdot \beta$

(3) $\alpha \cdot \beta = \left\{ \sum_{i=0}^n x_i \cdot y_i : n \in \mathbb{N} \wedge x_i \in \alpha \wedge y_i \in \beta \right\}$

(4) " $\cdot$ " ist assoziativ

(5) Es gelten die Links- & Rechtsdistributivgesetze.

Beweis: (1) Mit $x_1 + y_1$ und $x_2 + y_2$ in $\alpha + \beta$, ist auch

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 + y_1) + (-x_2 - y_2) = \underbrace{(x_1 - x_2)}_{\in \alpha} + \underbrace{(y_1 - y_2)}_{\in \beta} \in \alpha + \beta$$

(2) • Es gilt $\alpha, \beta \subseteq \alpha + \beta$, also gilt $\alpha \cup \beta \subseteq \alpha + \beta$ und mit (1) ist $(\alpha \cup \beta) \subseteq \alpha + \beta$.

• Sei $d \subseteq R$ ein Ideal mit $\alpha \cup \beta \subseteq d$. Für $x \in \alpha$ und $y \in \beta$ gilt dann $x, y \in d$, d.h. $x+y \in d$ und somit gilt, weil x, y beliebig waren, $\alpha + \beta \subseteq d$.

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

• Ist nun $x \in \alpha$ und $y \in \beta$, dann ist

$$\begin{array}{ccc} x \cdot y \in \beta & \text{und} & x \cdot y \in \alpha \\ \uparrow \quad \downarrow & & \uparrow \quad \downarrow \\ \in R & \in \beta & \in \alpha & \in R \end{array} \quad , \text{ also } x \cdot y \in \alpha \cap \beta.$$

Also ist $\alpha \cdot \beta \subseteq \alpha \cap \beta$.

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

Das folgende Lemma ist ähnlich wie Lem. 4.4 für Gruppen:

Lemma 10.5 Sei $\varphi: R \rightarrow S$ ein Ringhomom. und $\alpha \subseteq R$ ein Ideal mit $\alpha \subseteq \ker(\varphi)$. Dann ex. ein eindeutig bestimmter Ringhomom. $\bar{\varphi}: R/\alpha \rightarrow S$, sodass

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ R/\alpha & & \end{array} \quad \text{kommuiert. Insbesondere gilt:}$$

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

Beweis: Wir definieren $\bar{\varphi}(\overline{x+\alpha}) := \varphi(x)$.

• $\bar{\varphi}$ ist wohldefiniert:

$$\begin{aligned} \bar{x} = \bar{y} &\Leftrightarrow x - y \in \alpha \Rightarrow x - y \in \ker(\varphi) \Leftrightarrow \varphi(x - y) = 0 \\ &\Leftrightarrow \varphi(x) - \varphi(y) = 0 \Leftrightarrow \varphi(x) = \varphi(y). \end{aligned}$$

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