II. Kommutative Ringe

In diesem Kapitel sei R stehts ein nicht-trivialer komm. Ring.

Def. Ein Ideal $\mathfrak{p} \subseteq R$ heisst Primideal, falls $R/\mathfrak{p}$ ein Integritätsring (nicht-trivial) ist. [Fall $R = \mathbb{Z}$]

Proposition II.1 Ist $\mathfrak{p} \subseteq R$ ein Ideal, dann gilt:

$\mathfrak{p}$ ist Primideal $\iff$ $\mathfrak{p} \neq R$ und für alle $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$ gilt: $\boxed{a \in \mathfrak{p} \vee b \in \mathfrak{p}.}$

Beweis: ($\Rightarrow$) Ist $\mathfrak{p}$ Primideal, dann ist $R/\mathfrak{p}$ Integritätsring, also $R/\mathfrak{p} \neq \{0\}$ und somit $\mathfrak{p} \neq R$.

Seien $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$.

Betrachte $R \longrightarrow R/\mathfrak{p}$

$a \cdot b \longmapsto \bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{0}$ (weil $a \cdot b \in \mathfrak{p}$)

Weil $R/\mathfrak{p}$ als Integritätsring nullteilerfrei ist, ist also $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$, d.h. $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

($\Leftarrow$) zu zeigen: $R/\mathfrak{p}$ ist Integritätsring.

Seien $\bar{a}, \bar{b} \in R/\mathfrak{p}$ mit $\bar{a} \cdot \bar{b} = \bar{0}$, also $\overline{a \cdot b} = \bar{0}$.

Dann ist $a \cdot b \in \mathfrak{p}$ und mit der Voraussetzung ist dann $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, d.h. $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$, d.h. $R/\mathfrak{p}$ ist Integritätsring. ⊣

Def. Ein Ideal $\mathfrak{m} \subseteq R$ heisst maximal, falls gilt:

$\mathfrak{m} \neq R$ und es ex. kein Ideal $\mathfrak{a} \neq R$ mit $\mathfrak{m} \subsetneq \mathfrak{a}$.

[$\mathfrak{m} \neq R$ ist in keinem echten Ideal von R echt enthalten.]

Proposition II.2 Sei $\mathfrak{m} \subseteq R$ ein Ideal; dann gilt:

$\mathfrak{m}$ ist maximal $\iff$ $R/\mathfrak{m}$ ist Körper

<u>Beweis:</u> $\pi: R \to R/\mathfrak{m}$ sei die nat. Projektion.
$a \mapsto \bar{a}$

($\Rightarrow$) $\mathfrak{m} \subseteq R$ sei maximal und $\mathfrak{b} \subseteq R/\mathfrak{m}$ sei Ideal.
Dann ist $\pi^{-1}[\mathfrak{b}]$ ein Ideal in R [Übung]
mit $\mathfrak{m} \subseteq \pi^{-1}[\mathfrak{b}]$. Weil $\mathfrak{m}$ maximal ist, gilt
$\pi^{-1}[\mathfrak{b}] = \mathfrak{m}$ oder $\pi^{-1}[\mathfrak{b}] = R$, d.h.
$\mathfrak{b} = \pi[\pi^{-1}[\mathfrak{b}]] = \pi[\mathfrak{m}] = (\bar{0})$ oder $\mathfrak{b} = \pi[R] = R/\mathfrak{m}$.
Somit hat $R/\mathfrak{m}$ genau zwei Ideale, nämlich $(\bar{0})$
und $R/\mathfrak{m}$, also ist $R/\mathfrak{m}$ mit Prp. 10.3 ein Körper.

($\Leftarrow$) Sei $R/\mathfrak{m}$ ein Körper und sei $\mathfrak{a} \subseteq R$ ein Ideal
mit $\mathfrak{m} \subseteq \mathfrak{a}$. Dann ist $\pi[\mathfrak{a}] \subseteq R/\mathfrak{m}$ ein Ideal. [Übung]
Mit Proposition 10.3 gilt somit $\pi[\mathfrak{a}] = (\bar{0})$ oder
$\pi[\mathfrak{a}] = R/\mathfrak{m}$, d.h. $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$, also ist
$\mathfrak{m}$ ein maximales Ideal in R. ⊣

<u>Bem.</u> Jedes maximale Ideal ist Primideal. [Übung]

<u>Proposition 11.3</u> Seien R, S komm. Ringe, $\varphi: R \to S$ ein
Ringhomom., und $\mathfrak{p} \subseteq S$ ein Primideal in S.
Dann ist $\varphi^{-1}[\mathfrak{p}] \subseteq R$ ein Primideal in R.

<u>Beweis:</u> • $\varphi^{-1}[\mathfrak{p}] \neq R$: [Kontraposition]
$\varphi^{-1}[\mathfrak{p}] = R \Rightarrow 1_R \in \varphi^{-1}[\mathfrak{p}] \Rightarrow \varphi(1_R) = 1_S \in \mathfrak{p}$
$\Rightarrow \mathfrak{p} = S \Rightarrow \mathfrak{p}$ nicht Primideal in S.

• $a, b \in R$ mit $a \cdot b \in \varphi^{-1}[\mathfrak{p}]$, dann $a \in \varphi^{-1}[\mathfrak{p}] \vee b \in \varphi^{-1}[\mathfrak{p}]$:
$a \cdot b \in \varphi^{-1}[\mathfrak{p}] \Rightarrow \varphi(a \cdot b) \in \mathfrak{p} \Leftrightarrow \varphi(a) \cdot \varphi(b) \in \mathfrak{p}$,
und weil $\mathfrak{p} \subseteq S$ Primideal ist, gilt $\varphi(a) \in \mathfrak{p} \vee \varphi(b) \in \mathfrak{p}$,
d.h. $a \in \varphi^{-1}[\mathfrak{p}] \vee b \in \varphi^{-1}[\mathfrak{p}]$.
⊣

Beispiele: • $(0) \subsetneq R$ ist max. Ideal $\Leftrightarrow$ R ist ein Körper
(denn $R/(0) \cong R$)

• $R = \mathbb{Z}$: (m) Primideal $\Leftrightarrow$ m ist prim $\Leftrightarrow$ (m) ist maximal
$m \in \mathbb{Z}$ $\Leftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ ist Körper

Quotientenkörper eines Integritätsrings

Sei R ein Integritätsring und sei $\dot{R} := R \setminus \{0\}$.
Auf $R \times \dot{R}$ definieren wir die binäre Relation "$\sim$" wie folgt:

$$(a, b) \sim (a', b') \iff a \cdot b' = b \cdot a'$$

Dann ist "$\sim$" eine Äquivalenzrelation, also reflexiv, symm., transitiv. Für $(a,b) \in R \times \dot{R}$ sei $\frac{a}{b}$ die Äquivalenzklasse von (a,b) und

klar klar nachprüfen

$$\mathrm{Quot}(R) := \left\{ \frac{a}{b} : (a,b) \in R \times \dot{R} \right\}$$

sei die Menge der Äquivalenzklassen.

Auf $\mathrm{Quot}(R)$ definieren wir zwei binäre Operationen $+$ & $\cdot$ wie folgt:
$$\frac{a}{b} + \frac{a'}{b'} := \frac{ab' + ba'}{b \cdot b'} \quad ; \quad \frac{a}{b} \cdot \frac{a'}{b'} := \frac{a \cdot a'}{b \cdot b'}$$

Dann ist die Addition $+$ und Mult. $\cdot$ wohldefiniert. [nachrechnen]

Weiter sei $\imath : R \longrightarrow \mathrm{Quot}(R)$; $0_Q := \imath(0_R) = \frac{0_R}{1_R}$

$a \longmapsto \frac{a}{1_R}$ $\qquad 1_Q := \imath(1_R) = \frac{1_R}{1_R}$

Proposition II.4 $(\mathrm{Quot}(R), 0_Q, 1_Q, +, \cdot)$ ist ein Körper.

Beweis: • $(\mathrm{Quot}(R), 0_Q, +)$ ist abelsche Gruppe
 ∘ $+$ ist assoz. und komm. (nachrechnen)
 ∘ $0_Q + \frac{a}{b} = \frac{0}{1} + \frac{a}{b} = \frac{0 + a}{b} = \frac{a}{b}$ ∘ $-\left(\frac{a}{b}\right) = \frac{-a}{b}$

• Mult. ist komm. (nachrechnen) und assoz. (nachprüfen).

• $1_Q \cdot \frac{a}{b} = \frac{1}{1} \cdot \frac{a}{b} = \frac{1 \cdot a}{1 \cdot b} = \frac{a}{b}$

• Es gelten die Distributivgesetze (nachprüfen).

• $\mathrm{Quot}(R)^* = \mathrm{Quot}(R) \setminus \{0_Q\}$:

Ist $\frac{a}{b} \in \mathrm{Quot}(R)$ und $\frac{a}{b} \neq 0_Q$, dann ist $a \neq 0_R$, also $a \in \dot{R}$.

[Beachte: $(0,b) \sim (0,b')$]

Somit ist $\frac{b}{a} \in \mathrm{Quot}(R)$ und es gilt:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{1}{1} = 1_Q$$

weil $(ab, ba) \sim (1,1)$

$\dashv$

<u>Def.</u> Der Körper $(\mathrm{Quot}(R), 0, 1, +, \cdot)$ heisst <u>Quotientenkörper von R</u>.

<u>Proposition 11.5</u> (a) Die Abbildung

$$\iota : R \hookrightarrow \mathrm{Quot}(R), \quad a \longmapsto \frac{a}{1_R}$$

ist ein injektiver Ringhomomorphismus.

(b) Für jeden inj. Ringhom. $\varphi : R \hookrightarrow K$ in einen Körper K ex. genau ein Ringhom. $\bar{\varphi} : \mathrm{Quot}(R) \longrightarrow K$ mit $\bar{\varphi} \circ \iota = \varphi$,

d.h.

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & K \\ & \mathrm{Quot}(R) \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

kommutiert.

<u>Beweis:</u> (a) Die Abbildung ι ist ein Ringhom. (nachprüfen).

(b) • Wenn $\bar{\varphi}$ ex., so ist $\bar{\varphi}$ eindeutig: [$\bar{\varphi}$ habe die verlangten Eigensch.]

$$\bar{\varphi} \circ \iota(1_R) = \bar{\varphi}(1_Q) = 1_K = \varphi(1_R).$$

$\bar{\varphi}$ Ringhom.

Sei $a \in \dot{R}$, dann ist $1_K = \bar{\varphi}(1_Q) = \bar{\varphi}\left(\frac{a}{1} \cdot \frac{1}{a}\right) = \underbrace{\bar{\varphi}\left(\frac{a}{1}\right)}_{= \varphi(a)} \cdot \bar{\varphi}\left(\frac{1}{a}\right)$,
somit ist $1_K = \varphi(a) \cdot \bar{\varphi}\left(\frac{1}{a}\right)$ und weil das Inverse von $\varphi(a)$ eindeutig ist, gilt $\varphi(a)^{-1} = \bar{\varphi}\left(\frac{1}{a}\right)$, d.h. $\bar{\varphi}$ ist eindeutig. [$\bar{\varphi}$ bildet auch $\frac{1}{a}$ "richtig" ab]

• Wir definieren $\bar{\varphi}\left(\frac{a}{b}\right) := \varphi(a) \cdot \varphi(b)^{-1}$.

Dann gilt: $\bar{\varphi} \circ \iota(a) = \bar{\varphi}\left(\frac{a}{1}\right) = \varphi(a) \cdot \underbrace{\varphi(1_R)^{-1}}_{= 1_K} = \varphi(a)$,

insbesondere ist $\bar{\varphi} \circ \iota(1_R) = 1_K$.

- $\bar\varphi$ ist wohldefiniert:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow \varphi(ad) = \varphi(bc)$$
$$\Leftrightarrow \varphi(a)\cdot\varphi(d) = \varphi(b)\cdot\varphi(c)$$
$$\Leftrightarrow \underbrace{\varphi(a)\cdot\varphi(b)^{-1}}_{=\bar\varphi(\frac{a}{b})} = \underbrace{\varphi(c)\cdot\varphi(d)^{-1}}_{=\bar\varphi(\frac{c}{d})}$$

- $\bar\varphi$ Ringhomom.: ["$\cdot$" klar]

$$\bar\varphi\left(\frac{a}{b}+\frac{c}{d}\right) = \bar\varphi\left(\frac{ad+bc}{bd}\right) \overset{\text{Def.}}{=} \varphi(ad+bc)\cdot\underbrace{\varphi(bd)^{-1}}_{(\varphi(b)\cdot\varphi(d))^{-1}}$$
$$= \Big(\varphi(a)\cdot\varphi(d)+\varphi(b)\cdot\varphi(c)\Big)\cdot\left(\varphi(b)^{-1}\cdot\varphi(d)^{-1}\right)$$
$$= \underbrace{\varphi(a)\cdot\varphi(b)^{-1}}_{=\bar\varphi(\frac{a}{b})} + \underbrace{\varphi(c)\cdot\varphi(d)^{-1}}_{=\bar\varphi(\frac{c}{d})}$$

$\dashv$

<u>Folgerung</u>: Jeder injektive Ringhomom. $\varphi: R \hookrightarrow S$ von Integritätsringen R und S setzt sich fort zu einem eindeutigen Ringhomom. $\bar\varphi: \mathrm{Quot}(R) \hookrightarrow \mathrm{Quot}(S)$.

<u>Bemerkung</u>: - Sei R ein Integritätsring, K ein Körper mit $R \subseteq K$, so ist $\mathrm{Quot}(R) \hookrightarrow K$. D.h. $\mathrm{Quot}(R)$ ist der kleinste Körper der R enthält.

- Ist K ein Körper, so ist $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) = p$ für p prim.

$\mathrm{char}(K) = 0$: $\begin{array}{rcl}\mathbb{Z} & \hookrightarrow & K \\ n & \longmapsto & n\cdot 1_K\end{array}$ induziert Inj. $\mathbb{Q} \hookrightarrow K$.

$\mathrm{char}(K) = p$: $\begin{array}{rcl}\mathbb{Z} & \rightarrow & K \\ n & \longmapsto & n\cdot 1_K\end{array}$ induziert Inj. $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$.

<u>Def.</u> Der <u>kleinste Körper</u>, der in K enthalten ist, ist somit isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ mit p prim. Er ist somit eindeutig bestimmt und heisst <u>Primkörper</u>.