

Man schreibt $a \equiv b \pmod{\mathcal{O}} : \Leftrightarrow a - b \in \mathcal{O}$

2.3.10 Homomorphiesatz

$\mathcal{O} \subset R$ Ideal, $\varphi: R \rightarrow R'$ Ringhomom mit $\mathcal{O} \subset \text{Ker } \varphi \leadsto$
 $\exists!$ Ringhomom $\bar{\varphi}: R/\mathcal{O} \rightarrow R'$ mit $\bar{\varphi} \circ \pi = \varphi$

Es gilt $\text{Im } \bar{\varphi} = \text{Im } \varphi$, $\text{Ker } \bar{\varphi} = \pi(\text{Ker } \varphi)$, $\text{Ker } \varphi = \pi^{-1}(\text{Ker } \bar{\varphi})$

Insbes. $\bar{\varphi}$ injektiv $\Leftrightarrow \text{Ker } \varphi = \mathcal{O}$; $R/\text{Ker } \varphi \cong \text{Im } \varphi$ (Ringisom.)

Beweis Schon bewiesen bzgl. Addition (1.2.8), wobei

$$\begin{aligned} \bar{\varphi}(a + \mathcal{O}) &= \varphi(a). \text{ z.z. } \bar{\varphi} \text{ Ringhomom: } \bar{\varphi}(1 + \mathcal{O}) = \varphi(1) = 1 \\ \text{und } \bar{\varphi}(a + \mathcal{O})(b + \mathcal{O}) &= \bar{\varphi}(ab + \mathcal{O}) = \varphi(ab) = \varphi(a)\varphi(b) \\ &= \varphi(a + \mathcal{O})\varphi(b + \mathcal{O}) \quad \square \end{aligned}$$

2.3.11 Bem. Die Isomorphiesätze 1.2.10-11 gelten analog für Ringe, wenn man überall "Normalteiler" mit "Ideal" ersetzt.

2.3.12 Bsp. Sei $m \in \mathbb{N} \leadsto m\mathbb{Z} \subset \mathbb{Z}$ Ideal $\leadsto \mathbb{Z}/m\mathbb{Z}$ Restklassenring modulo m .

2.3.13 Satz Sei $m \in \mathbb{N}$. (i) m nicht prim $\Leftrightarrow \mathbb{Z}/m\mathbb{Z}$ kein Int.ring
 (ii) m prim $\Leftrightarrow \mathbb{Z}/m\mathbb{Z}$ Körper.

Beweis Laut Blatt 8: $\forall R$ endlicher Ring: R Int.ring $\Leftrightarrow R$ Körper.

Also (i) ist äquiv. zu (ii). Wir beweisen (ii): " $\Rightarrow$ " Sei $\hat{a} \in \mathbb{Z}/m\mathbb{Z}$ ein Nullteiler $\leadsto \exists \hat{b} \neq \hat{0}: \hat{a}\hat{b} = \hat{0} \leadsto m|ab \leadsto m|a$ oder $m|b$
 $\leadsto m|a \leadsto \hat{a} = \hat{0}$. " $\Leftarrow$ " Angenommen $m = a \cdot b$, $0 < a, b < m$
 $\leadsto \hat{a}, \hat{b} \neq \hat{0}$ aber $\hat{a}\hat{b} = \hat{m} = \hat{0} \quad \square$

2.3.14 Def. (i) Ein Ideal $\mathfrak{p} \subset R$ heißt Primideal, wenn $\mathfrak{p} \neq R$ und für alle $a, b \in R$ gilt: $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

(ii) Ein Ideal $\mathfrak{m} \subset R$ heißt maximal, wenn $\mathfrak{m} \neq R$ und
 $\forall \mathcal{O}$ Ideal: $\mathfrak{m} \subset \mathcal{O} \Rightarrow \mathfrak{m} = \mathcal{O}$ oder $R = \mathcal{O}$.

2.3.15 Satz Seien $M, P \subset R$ Ideale.

(i) M maximal $\Leftrightarrow R/M$ Körper

(ii) P prim $\Leftrightarrow R/P$ Integritätsring

Insbesondere: Jedes maximales Ideal ist prim.

Beweis (i) Es gibt eine Bijektion:

$$\{\text{Ideale } \mathcal{O}' \subset R/M\} \leftrightarrow \{\text{Ideale } \mathcal{O} \subset R \text{ mit } M \subset \mathcal{O}\}$$

$$\mathcal{O}' \mapsto \pi^{-1}(\mathcal{O}')$$

$$\pi(\mathcal{O}) \longleftarrow \mathcal{O}$$

$$M \text{ maximal} \Leftrightarrow \{\text{Ideale } \mathcal{O} \subset R, M \subset \mathcal{O}\} = \{M, R\}$$

$$\Leftrightarrow \{\text{Ideale } \mathcal{O}' \subset R/M\} = \{(0), R\} \Leftrightarrow R/M \text{ Körper.}$$

(ii) P prim $\Leftrightarrow P \neq R$ und $ab \in P \Rightarrow a \in P$ oder $b \in P$

$$\Leftrightarrow R/P \neq 0 \text{ und } \hat{a} \cdot \hat{b} = 0 \Rightarrow \hat{a} = 0 \text{ oder } \hat{b} = 0$$

$$\Leftrightarrow R/P \text{ Integritätsring} \quad \blacksquare$$

2.3.16 Korollar Sei $m \in \mathbb{N}$. Dann gilt:

$$n \text{ Primzahl} \Leftrightarrow n\mathbb{Z} \subset \mathbb{Z} \text{ max. Ideal} \Leftrightarrow n\mathbb{Z} \subset \mathbb{Z} \text{ Primideal}$$

Beweis $(\mathbb{Z}/n\mathbb{Z})^* = \{\hat{m} \in \mathbb{Z}/n\mathbb{Z} : \text{ggT}(m, n) = 1\}$ (1.3.12)

$$\text{und } \{\hat{m} \in \mathbb{Z}/n\mathbb{Z} : \hat{m} \text{ Nullteiler}\} = \mathbb{Z}/n\mathbb{Z} \setminus (\mathbb{Z}/n\mathbb{Z})^*$$

$$\text{also } n \text{ Primzahl} \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ Körper} \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ Integritätsring.}$$

2.3.17 Korollar K Körper, $a \in K \rightsquigarrow (X-a) \subset K[X]$ maximal.

Beweis $\varphi: K[X] \rightarrow K, \varphi(P) = P(a)$ Homom., $\text{Ker } \varphi = \{P : P(a) = 0\} = (X-a) \rightsquigarrow K[X]/(X-a) \cong K. \quad \blacksquare$

Bem Sei $R \neq \{0\}$. Dann gilt: $\{0\}$ Primideal $\Leftrightarrow R$ Integr. ring.

§ 2.4. Primfaktorzerlegung

2.4.1 Def. Sei R Integritätsring.

$$\Leftrightarrow y \in (x)$$

(i) $x \in R$ teilt $y \in R$ (geschrieben $x|y$): $\Leftrightarrow \exists a \in R: y = ax$ (ii) $p \in R$ heißt Primelement (kurz prim), falls $p \neq 0, p \notin R^*$ und $p|xy \Rightarrow p|x$ oder $p|y$.(iii) $p \in R$ heißt irreduzibel, falls $p \neq 0, p \notin R^*$ und $\forall x, y: p = xy \Rightarrow x \in R^*$ oder $y \in R^*$; p heißt reduzibel falls $p \neq 0, p \notin R^*$ und p nicht irred. $(p)^{\max}$
 $\downarrow$ 2.4.2 Bem. (i) $x|y \Leftrightarrow (y) \subset (x)$ (ii) p Primelem. $\Leftrightarrow (p)^{\text{Primideal}}$ (da $p|xy \Leftrightarrow xy \in (p)$) (iii) p prim $\Rightarrow p$ irred. $(p = xy \Rightarrow p|xy \Rightarrow p|x \text{ oder } p|y. \text{ O.B.d.A. } p|x. \text{ Dann } x = pc \leadsto p = pc \leadsto cy = 1 \leadsto y \in R^*)$ 2.4.3 Satz Sei R Hauptidealring, $p \in R \setminus \{0\}, p \notin R^*$.Dann gilt: p irred. $\Leftrightarrow p$ prim $\Leftrightarrow (p)^{\text{Primideal}} \Leftrightarrow (p)^{\max}$.Beweis Sei p irred und $(p) \subset (a) \leadsto p = ac \leadsto a \in R^*$ oder $c \in R^* \leadsto (a) = R$ oder $(a) = (p) \leadsto (p)^{\text{maximal}} \quad \square$ 2.4.4 Bsp. (i) $R = \mathbb{Z}$: $\{\pm \text{Primzahlen}\} = \{\text{Primelem}\} = \{\text{Irred}\}$.(ii) $X - a \in K[X]$ prim, also irred.(iii) $X^2 + 1 \in R[X]$ prim, da $R[X]/(X^2 + 1) \cong \mathbb{C}$ ($R[X] \xrightarrow{\varphi} \mathbb{C}$, $P \mapsto P(i)$ Homom; $P \in \text{Ker}(\varphi) \Leftrightarrow P(i) = 0 \Leftrightarrow X - i | P \Leftrightarrow X + i | P \Leftrightarrow X^2 + 1 | P$)