

Weiter zu A11:

Hatten: R Ring, $I \subseteq R$ heißt (zweiseitiges) Ideal: \Leftrightarrow

$$(1) 0 \in I, \quad (2) \forall a, b \in I : a + b \in I$$

$$(3) \forall a \in I \quad \forall b \in R : ab \in I \text{ und } ba \in I$$

Falls anstelle (3) die Bed. $(3)_{\text{links}}$ $\forall a \in I \forall b \in R : ba \in I$

gilt, dann heißt I Linksideal.

Falls anstelle (3) die Bed. $(3)_{\text{rechts}}$ $\forall a \in I \forall b \in R : ab \in I$

gilt, dann heißt I Rechtsideal.

11.9. Bem.: Sei $(I_m)_{m \in M}$ eine Familie von Idealen in R .

Dann: $\bigcap_{m \in M} I_m =: D$ ist Ideal.

Bew.: $\forall a \in D \quad \forall b \in R : ab, ba \in D \quad D$

11.10. Bem.: $I, J \subseteq R$ Ideale $\Rightarrow I + J$ Ideal

$$:= \overbrace{\{a+b; a \in I, b \in J\}}^{} \quad \square$$

Bew.: $a = a_1 + a_2 \in I + J$ mit $a_1 \in I, a_2 \in J, b \in R$

$$\Rightarrow ba = b(a_1 + a_2) = ba_1 + ba_2 \in I + J.$$

$$\Rightarrow ab = (a_1 + a_2)b = a_1b + a_2b \in I + J. \quad \square$$

11.11. Lemma: Sei R Ring, $I \subseteq R$ Ideal. Dann $R/I = \{a+I; a \in R\}$

Ring bzgl. "Plus" $+ : (a+I) + (b+I) := (a+b)+I$

"Mal" $\cdot : (a+I) \cdot (b+I) := (ab)+I$

mit $\bar{0} = 0+I = I, \bar{1} = 1+I$.

Bew.: * R/I ist ab. Gruppe bzgl. $+$

* ist wohldef.: Seien $a+I = a'+I, b+I = b'+I$.

$$\Rightarrow a-a' \in I \ni b-b'$$

$$\Rightarrow ab - a'b' = ab - ab' + ab' - a'b'$$

$$= \underbrace{a(b-b')}_{\substack{b \in I \\ \text{Linkideal}}} + \underbrace{(a-a')b'}_{\substack{a \in I \\ \text{Rechtsideal}}} \in I + I = I$$

$$\Rightarrow ab+I = a'b'+I.$$

* Axiome nachzurechnen.

□

Bsp.: Mit Konzept "Unterring" ist R/R' i.a. kein Ring!

$$Q/Z = \{ a + \underline{Z}; a \in [0,1] \cap Q \}$$

$$\hookrightarrow (\frac{1}{2} + \underline{Z}) \cdot (\frac{1}{3} + \underline{Z}) = \frac{1}{6} + \underline{Z} \neq (-\frac{1}{2} + \underline{Z}) \cdot (\frac{1}{3} + \underline{Z}) = -\frac{1}{6} + \underline{Z}$$

$$= -\frac{1}{2} + \underline{Z}$$

$$= \frac{5}{6} + \underline{Z}$$

11.12. Def.: R/I heißt Faktoring (Quotientring) R modulo I .

11.13. Bem.: Die Faktorringe von \mathbb{Z} : \mathbb{Z}/\mathbb{Z}_r , $r \in \mathbb{N}$.

\mathbb{Z}/\mathbb{Z}_r heißt Restklassenring modulo r

$$\mathbb{Z}/\mathbb{Z}_r = \{ a + \mathbb{Z}_r; a \in \mathbb{Z} \} = \{ \underbrace{0 + \mathbb{Z}_r}_0, \underbrace{1 + \mathbb{Z}_r}_1, \dots, \underbrace{r-1 + \mathbb{Z}_r}_{r-1} \}$$

Restklassenabb. $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/\mathbb{Z}_r$

$$m \mapsto \underline{m} := m + \mathbb{Z}_r.$$

Fall 1: $r = p$ prim. Dann $\mathbb{F}_p := \mathbb{Z}/\mathbb{Z}_p$ Körper.

Bew.: $m \in \mathbb{F}_p \setminus \{0\} \Rightarrow p \nmid m \Rightarrow p, m$ teilerfremd

$$\stackrel{\text{A 4.3}}{\Rightarrow} \exists m, n \in \mathbb{Z}: 1 = mp + nm$$

$$\stackrel{\text{Berechnung}}{\Rightarrow} 1 - nm = mp \in \mathbb{Z}_p$$

$$\Rightarrow \underline{1} = \underline{nm} = \underline{n} \cdot \underline{m} \Rightarrow (\underline{m})^{-1} = \underline{n}. \quad \square$$

← endl. Körper mit p Elementen
Es gibt noch mehr endl. Körper!

Fall 2: $r = s \cdot t$, $s, t \neq \pm 1$. Dann in $\mathbb{Z}/\mathbb{Z}(st)$:

$$\underline{s} \cdot \underline{t} = \underline{st} = \underline{0}, \text{ aber } \underline{s} \neq \underline{0} \neq \underline{t}, \text{ d.h. } \underline{s}, \underline{t} \text{ sind Nullteiler!}$$

$$\text{Später: } s, t \text{ teilerfremd} \Rightarrow \mathbb{Z}/\mathbb{Z}(st) \cong \mathbb{Z}/\mathbb{Z}_s \times \mathbb{Z}/\mathbb{Z}_t \quad (\text{CRS, A 12.5})$$

11.14. Def.: R, R' Ringe, $\varphi: R \rightarrow R'$ Ringhomomorphismus

$$\Leftrightarrow \forall a, b \in R: (1) \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$(2) \varphi(ab) = \varphi(a)\varphi(b)$$

$$(3) \varphi(1_R) = 1_{R'} \quad \begin{matrix} \text{muss gefordert werden, da} \\ \text{"." nur Halbgruppe} \end{matrix}$$

-3-

11.15. Bew.: Die Projektionen $\pi_i : R_1 \times \dots \times R_m \rightarrow R_i$
 $(a_1, \dots, a_m) \mapsto a_i$

sind Ringhomomorphismen.

11.16. Bew.: Sei $\varphi : R \rightarrow R'$ Ringhom. Dann:

- (1) $I' \subseteq R'$ Ideal $\Rightarrow \varphi^{-1}(I') := \{a \in R; \varphi(a) \in I'\}$ Ideal in R
- (2) $\ker \varphi$ ist Ideal
- (3) φ injektiv $\Leftrightarrow \ker \varphi = 0$
- (4) $\varphi(R^\times) \subseteq (R')^\times$

$\widetilde{\text{Einheiten}}: R^\times = \{a \in R; \exists b \in R: ab = 1 = ba\}$

Bew.: (1): Sei $a \in \varphi^{-1}(I')$, $b \in R$. Dann $\varphi(ab) = \varphi(a)\varphi(b) \in I'$
 $\Rightarrow ab \in \varphi^{-1}(I')$. Analog ba .

(2): $a \in \ker \varphi$, $b \in R \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = 0$ ($\varphi(b) = 0 \Rightarrow ab \in \ker \varphi$ analog ba)

(3): φ injektiv $\Leftrightarrow (\varphi(a) = \varphi(b) \Rightarrow a = b) \Leftrightarrow (\varphi(a-b) = 0 \Rightarrow a-b = 0) \Leftrightarrow \ker \varphi = 0$.

(4): Sei $u \in R^\times$, etwa $uv = vu = 1$. Dann: $1 = \varphi(uv) = \varphi(u)\varphi(v) \Rightarrow \varphi(u) \in (R')^\times$.

D

11.17. Bew.: Bilder von Idealen sind i.a. keine Ideale.

Bew.: $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$, $I = \mathbb{Z} \cdot 2 \rightarrow \mathbb{Z} \cdot 2$ kein Ideal in \mathbb{Q} .

11.18. Def.: Ringisomorphismen, Ringendomorphismen, Ringautomorphismen analog
wie bei Gruppen.

11.19. Def.: R Ring, $R' \subseteq R$ heißt Unterring (UR): \Leftrightarrow
(1) R' UG der add. Gr. von R ,
(2) R' ist abg. bzgl.
(3) $1 \in R'$.

11.20. Bew.: * \mathbb{Z} ist UR von \mathbb{Q}

* $2\mathbb{Z}$ ist kein UR von \mathbb{Q} , da $1 \notin 2\mathbb{Z}$

* $\mathbb{Q}^{n \times n}$ ist UR von $\mathbb{R}^{n \times n}$

* Körper $K \subseteq L \Rightarrow K^{n \times n}$ ist UR von $L^{n \times n}$

* $\varphi : R \rightarrow R'$ Ringhom. $\Rightarrow \varphi(R)$ UR von R'

11.21. Bem.: $I \subseteq R$ Ideal, $\varphi: R \rightarrow R'$ surjektiver Ringhom. $\Rightarrow \varphi(I) \subseteq R'$ Ideal.

Bew.: Sei $a \in I$, $b' \in R'$ $\Rightarrow \exists b \in R : \varphi(b) = b'$, da φ surj.

Dann: $\underbrace{\varphi(a) \cdot b'}_{\in \varphi(I)} = \varphi(a) \cdot \varphi(b) = \underbrace{\varphi(a \cdot b)}_{\in I} \in \varphi(I), \quad b' \cdot \varphi(a) \text{ analog.}$ □

11.22. Homomorphismen (für Ringe):

Vor.: R Ring, $I \subseteq R$ Ideal.

Bem.: (i) $\pi: R \rightarrow R/I$ "Projektion" zu I

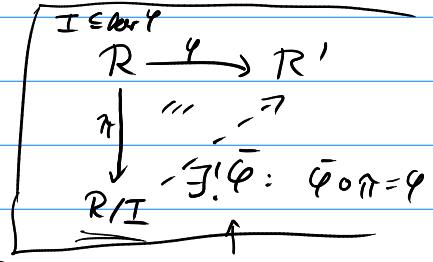
$a \mapsto a + I$ ist subjektiver Ringhom., für $\eta = I$.

(ii) "Universelle Eigenschaft":

$\forall \varphi \in R\text{-Hom}(R, R')$, R' Ring, $I \subseteq \ker \varphi$

$$\exists! \bar{\varphi} \in R\text{-}\mathrm{Hom}(R/I, R') : \quad \bar{\varphi} \circ \overline{\pi} = \varphi.$$

zu untersuchen: {
 (a) $\text{im } \bar{\varphi} = \text{im } \varphi$
 (b) $\bar{\varphi}$ inj. \Leftrightarrow ~~ker~~ $\varphi = I$



Bew.: (i): π R-Hom, surj ν , $\ker \pi = I : a + I = \pi(a) = 0 = 0 + I = I$ \hookrightarrow Bild "

(ii): Hom. satz für Gruppen $\Rightarrow \exists ! \bar{\varphi} \in \text{Gr.-Hom.}(R, R')$, das genügt. Ist Ringhom.:

$$\overline{\varphi}(\underbrace{1+I}_{\text{units in } R/I}) = \overline{\varphi}(\pi(\frac{1}{R})) = \varphi(\frac{1}{R}) = 1_{R'}$$

Zeige noch: $\bar{\varphi}(\bar{a}\bar{b}) = \bar{\varphi}(\bar{a}) \bar{\varphi}(\bar{b})$

$$\begin{aligned} \text{Bew.: } & \bar{\varphi}(a+I)(b+I) = \bar{\varphi}(ab+I) = \bar{\varphi}(\pi(ab)) = \varphi(ab) \\ &= \varphi(a)\varphi(b) = \bar{\varphi}(\pi(a))\bar{\varphi}(\pi(b)) = \bar{\varphi}(a+I)\bar{\varphi}(b+I). \end{aligned}$$

(a), (b): nach Hauptsatz für Gruppen ✓

$$(\sigma): R \xrightarrow{\varphi} \text{im } \varphi \subseteq R'$$

$$R/\overline{a_0}q \xrightarrow{\cong} T$$

\bar{q} sur. da & sur. lant (a)

\bar{q} ist, da $R_q \varphi = T(\text{ant})$

$$\left. \begin{array}{l} \bar{q} \text{ surj., da } \varphi \text{ surj. laut (a)} \\ \bar{q} \text{ inj., da } \ker \varphi = I(\text{laut (b)}) \end{array} \right\} \text{im } \varphi \cong R/\ker \bar{\varphi}$$

mit Ringisom. $\bar{\varphi}$.

11.23. Satz: Vor.: R Ring, $I \subseteq R$ Ideal, $\pi: R \rightarrow R/I =: \bar{R}$ Projektion zu I .

$$\mathcal{J} := \{ J \subseteq R \text{ Ideal}; \underline{\underline{I}} \subseteq J \}, \quad \bar{\mathcal{J}} := \{ \bar{J} \subseteq \bar{R} \text{ Ideal} \}$$

$$\varphi: \mathcal{J} \rightarrow \bar{\mathcal{J}}, \quad \begin{aligned} \varphi: & \mathcal{J} \rightarrow \bar{\mathcal{J}} \\ J & \mapsto \pi(J) \end{aligned}, \quad \begin{aligned} \psi: & \bar{\mathcal{J}} \rightarrow \mathcal{J} \\ \bar{J} & \mapsto \pi^{-1}(\bar{J}). \end{aligned}$$

Beh.: (i) φ, ψ zueinander inverse Bijektionen zw. \mathcal{J} und $\bar{\mathcal{J}}$.

(ii) $L \in \bar{\mathcal{J}}$ Ideal in $\bar{R} \Leftrightarrow L := \pi^{-1}(L) \in \mathcal{J}$ Ideal in R .

$$\text{Dann: } \underline{\underline{R/L}} \cong \underline{\underline{\bar{R}/\bar{L}}} = (R/I)/(L/I) \quad \text{"? Isom. Satz"}$$

Ringisom.

Bew.: Wohldef.: $J \subseteq R$ Ideal $\Rightarrow \pi(J) \subseteq R'$ Ideal, da π surj. (Bem. 11.21).

Auso: φ wohldef., ebenso ψ nach Bem. 11.16.

Somit: 11.23. folgt aus A4.22., da bei dieser Bij.

gehen Ideale in Ideale über.

11.24. Bew.: Sei R Ring, $\varphi: \mathbb{Z} \rightarrow R$, $m \mapsto m_R := m \cdot 1_R = \underbrace{1_R + 1_R + \dots + 1_R}_{m-\text{mal}}$.
Dann φ Ringhom.

$$\begin{aligned} \text{Bew.: Haben } \varphi(1) &= 1_R, \text{ und } \varphi(m+m) = (m+m)_R = (m+m) \cdot 1_R \\ &= m \cdot 1_R + m \cdot 1_R = m_R + m_R = \varphi(m) + \varphi(m) \end{aligned}$$

$$\text{Ferner: } (mm)_R = m_R \cdot m_R, \text{ d.h. } \varphi(mm) = \varphi(m) \varphi(m).$$

$$\text{Bew.: } \underbrace{n \geq 0}_m: \text{ VI nach } n: \underbrace{m=0}: (0 \cdot m)_R = 0_R = \underbrace{0 \cdot m_R}_R$$

$$n \geq m+1: (m+1)m)_R = (mm+m)_R = \underbrace{(mm)_R + m_R}_R$$

$$= m_R m_R + m_R = (m_R + 1_R) m_R = (m+1)_R m_R.$$

$$\underbrace{n < 0}: (-1 \cdot m)_R = -m_R \Rightarrow (mm)_R = (-(-m)m)_R = -((-m)m)_R$$

$$= -(-m_R)m_R = m_R m_R. \quad \square$$

11.25. Def.: $\varphi: \mathbb{Z}$ mit φ aus 11.24 heißt Primring von R .

11.26. Bew.: $\varphi(\mathbb{Z})$ ist kleinste UR $\neq 0$ von R ($\neq 0$),

Bsp.: \mathbb{F}_2 hat Char. 2

$$\text{und: } \varphi \mathbb{Z} \cong \mathbb{Z}/\ker \varphi = \mathbb{Z}/\mathbb{Z}_r \text{ für ein } r \in \mathbb{N}_0.$$

Horn.Satz T

11.27. Def.: $r \in \mathbb{N}_0$ heißt Charakteristik von R .

Bsp.: \mathbb{Z} ist Primring von \mathbb{Q}