

3. Ringe & Körper

3.1 Def.: Ein Ring $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, sodass gilt:

(R1) $(R, +)$ abelsche Gruppe
mit neutralem Element 0
und Inversen $-x$ für $x \in R$

(R2a) $\cdot$ assoziativ

(R2b) $\cdot$ besitzt ein neutrales Element 1

(R3) Distributivität: $\forall x, y, z \in R$:

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

und $z \cdot (x + y) = z \cdot x + z \cdot y$

Wir nennen den Ring kommutativ, falls $\cdot$ kommutativ ist.

Beispiele:

(a) Nullring: $(\{0\}, +, \cdot)$ ↓ $0+0=0, 0 \cdot 0=0$
In diesem atypischen Ring ist $1=0$.

(b) $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$

gewöhnliche Add. & Multiplikation

(c) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein Ring für die in Satz 2.22 eingeführte Add. und die Multiplikation
 $[x] \cdot [y] := [x \cdot y]$

(Multiplikation ist wohldef.:

Sei $[x'] = [x]$, $[y'] = [y]$.

Dann ist $x' = x + k \cdot u$ für ein $k \in \mathbb{Z}$,

$y' = y + l \cdot u$ für ein $l \in \mathbb{Z}$,

und somit $x' \cdot y' = x \cdot y + (y \cdot k + x \cdot l + k \cdot l \cdot u) \cdot u$,

also $[x' \cdot y'] = [x \cdot y]$. —

Axiome prüfen: Selbststudium.)

3.2 Notiz: $\forall x \in R: 0 \cdot x = 0 = x \cdot 0$

$$\left(\begin{array}{l} 0 \cdot x = (0 + 0) \cdot x \\ \text{R1} \end{array} \right.$$

$$\xRightarrow{\text{R3}} 0 \cdot x = 0 \cdot x + 0 \cdot x \quad \left| + (-0 \cdot x) \right.$$

$$\begin{aligned} \Rightarrow 0 &= 0 \cdot x + 0 \\ &= 0 \cdot x \end{aligned}$$

analog: $0 = x \cdot 0$)

3.3 Def.: Ein Ringhomomorphismus $f: R \rightarrow S$

ist eine Abb., für die $\forall x, y \in R$ gilt:

$$f(x + y) = f(x) + f(y)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

$$f(1) = 1$$

(Es ist dann auch

$$f(-x) = -f(x)$$

$$f(0) = 0$$

denn f definiert insbesondere Gruppenhomom.

$(R, +) \rightarrow (S, +)$; vgl. Notiz 2.11.)

3.4 Def.: Einheitsgruppe eines Rings $(R, +, \cdot)$ ist

$$R^* = \left(\left\{ x \in R \mid x \text{ besitzt Inverses bzgl. } \cdot \right\}, \cdot \right)$$

Notiz: Das ist eine Gruppe [...].

3.5 Def.: Ein Körper (engl. field) ist ein kommutativer Ring $(K, +, \cdot)$ mit $K^* = K \setminus \{0\}$.

Ein Körperhomomorphismus ist ein Ringhomomorphismus zwischen Körpern.

Beispiele:

$$\mathbb{Z}^* = (\{\pm 1\}, \cdot) \quad - \mathbb{Z} \text{ ist kein Körper}$$

$$\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot) \quad - \mathbb{Q} \text{ ist ein Körper} \checkmark$$

$$\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot) \quad - \mathbb{R} \text{ ist ein Körper} \checkmark$$

$$(\mathbb{Z}/8\mathbb{Z})^* \ni [3], \text{ denn } [3] \cdot [3] = [9] = [1].$$

$$\nexists [2], \text{ denn } [0] \cdot [2] = \dots \neq [1]$$

$$[1] \cdot [2] = \dots \neq [1]$$

$$[2] \cdot [2] = \dots \neq [1]$$

$$[3] \cdot [2] = \dots \neq [1]$$

$$[4] \cdot [2] = \dots \neq [1]$$

$$[5] \cdot [2] = \dots \neq [1]$$

$$[6] \cdot [2] = \dots \neq [1]$$

$$[7] \cdot [2] = \dots \neq [1]$$

$-\mathbb{Z}/8\mathbb{Z}$ ist kein Körper

Der Nullring $R = (\{0\}, +, \cdot)$ ist kein Körper, denn $0 = 1$ in R , also $R^* = R \neq R \setminus \{0\}$.

3.6 Notiz: In Körpern und in $\mathbb{Z}$ gilt:
 $a \cdot b = 0 \iff (a = 0 \vee b = 0)$

Beweis: zu $\mathbb{Z}$: Schulwissen; zu Körpern:

($\Leftarrow$) Notiz 3.2

($\Rightarrow$) Sei $a \cdot b = 0$. Falls $b = 0$: ✓

Falls $b \neq 0$: multipliziere
beide Seiten mit b^{-1}

$$\underbrace{a \cdot b \cdot b^{-1}}_a = \underbrace{0 \cdot b^{-1}}_0$$

□



In allgemeinen Ringen ist das falsch,
z.B. gilt in $\mathbb{Z}/4\mathbb{Z}$:

$$[2] \cdot [2] = [4] = [0],$$

aber $[2] \neq 0$.

Beispiel: Primkörper

3.7 Satz: $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Körper,
wenn $p \in \mathbb{Z}$ eine Primzahl ist.
Wir schreiben dann auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

Beweis:

Vorüberlegung 1: $p \in \mathbb{Z}$ ist genau dann eine Primzahl,
wenn gilt: $p \neq 0, 1, -1$ und
 $\forall u, m \in \mathbb{Z}: p \mid u \cdot m \Rightarrow p \mid u \vee p \mid m$
"teilt"

Vorüberlegung 2: $\forall p, u \in \mathbb{Z}$:
 $p \mid u \Leftrightarrow [u] = [0] \text{ in } \mathbb{Z}/p\mathbb{Z}$

($\Rightarrow$) Sei $\mathbb{Z}/p\mathbb{Z}$ ein Körper.

- $p \neq 0$ (denn $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ ist kein Körper)
- $p \neq \pm 1$ (denn $\mathbb{Z}/\mathbb{Z}$ ist der Nullring)
- Seien $u, m \in \mathbb{Z}$ gegeben, sodass $p \mid u \cdot m$.

Dann ist

$$[u] \cdot [m] = [u \cdot m] \stackrel{(\text{Z})}{=} [0] \text{ in } \mathbb{Z}/p\mathbb{Z}.$$

Nach Notiz 3.6 folgt:

$$\begin{array}{ccc} [u] = 0 & \vee & [m] = 0, \text{ also} \\ p \mid u & & p \mid m. \end{array}$$

($\Leftarrow$) Sei p eine Primzahl.

Sei $[u] \in \mathbb{Z}/p\mathbb{Z}$, $[u] \neq 0$.

z.z.: $[u]$ besitzt mult. Inverses.

Betrachte dazu Multiplikation mit $[n]$ als Abb.

$$f: (\mathbb{Z}/p\mathbb{Z}, +) \xrightarrow{\cdot [n]} (\mathbb{Z}/p\mathbb{Z}, +)$$
$$[m] \mapsto [m] \cdot [n]$$

Wegen Distributivität ist diese Abb. ein Gruppenhomom., und es gilt:

$$\ker(f) = \{[0]\}:$$

Für beliebiges $[m] \in \ker(f)$ gilt

$$f([m]) = [0], \text{ also } [m] \cdot [n] = [0]$$

$$\text{also } [m \cdot n] = [0]$$

$$\text{also } p \mid m \cdot n$$

$$\text{also (da } p \text{ prim): } p \mid m \vee p \mid n,$$

$$\text{also } [m] = [0] \vee [n] = [0].$$

Nach Injektivitätskriterium (2.76) folgt also:
 f ist injektiv.

Da Def.- und Wertemenge von f endlich sind mit gleich vielen Elementen, folgt aus Satz 1.26: f ist surjektiv.

Insbesondere $\exists [m] \in \mathbb{Z}/p\mathbb{Z}$ mit $f([m]) = [1]$,
d.h. $[m] \cdot [n] = [1]$.

□

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt:

$$[1]^{-1} = [1]$$

$$[2]^{-1} = [3]$$

$$[3]^{-1} = [2]$$

$$[4]^{-1} = [4]$$

Beispiel: Komplexe Zahlen

3.8 Def.: Die komplexen Zahlen $\mathbb{C}$ sind die Menge $\mathbb{R}^2$ zusammen mit den Verknüpfungen

$$(x, y) +_{\mathbb{C}} (x', y') := (x + x', y + y')$$

$$(x, y) \cdot_{\mathbb{C}} (x', y') := (xx' - yy', xy' + yx')$$

Notation: $i := (0, 1)$

Per Definition ist $i^2 = (0, 1) \cdot_{\mathbb{C}} (0, 1) = (-1, 0)$.

3.9 Satz: $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ ist ein Körper, und

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & (x, 0) \end{array}$$

ist ein Körperhomomorphismus.

Beweis:

R1: $(\mathbb{C}, +_{\mathbb{C}})$ abelsche Gruppe [...]

$$0_{\mathbb{C}} = (0, 0)$$

$$-(x, y) = (-x, -y)$$

R2: $\cdot_{\mathbb{C}}$ ist assoziativ: [...]

$$1_{\mathbb{C}} = (1, 0)$$

$$\begin{aligned} ((1, 0) \cdot_{\mathbb{C}} (x, y)) &= (1 \cdot x - 0 \cdot y, 1 \cdot y + 0 \cdot x) \\ &= (x, y) \quad \checkmark \end{aligned}$$

R3: Distributivität: [...]

$\leadsto (\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ Ring

$\cdot_{\mathbb{C}}$ kommutativ: $[...]$

Multiplikatives Inverse zu $(x, y) \neq 0_{\mathbb{C}}$:

$$(x, y)^{-1} = \left(\frac{x}{\underbrace{x^2 + y^2}_{\neq 0}}, \frac{-y}{x^2 + y^2} \right) \quad [...]$$

Abb. ist Ringhomomorphismus $[...]$. □

Notation: Ab sofort:

$$\begin{array}{lll} x & \text{für} & (x, 0) \\ x + iy & \text{für} & (x, y) \\ + & \text{für} & +_{\mathbb{C}} \\ \cdot & \text{für} & \cdot_{\mathbb{C}} \end{array}$$

In dieser Notation ergeben sich Def. von $+_{\mathbb{C}}$ und $\cdot_{\mathbb{C}}$, indem wir $i^2 = -1$ und Distributivität & Kommutativität fordern.

$$\begin{aligned} (x + iy) \cdot (x' + iy') &= xx' + iy \cdot iy' + x \cdot iy' + iy \cdot x' \\ &= xx' + i^2 yy' + xy'i + yx'i \\ &= (xx' - yy') + (xy' + yx')i \end{aligned}$$

3.10 Def.:

Realteil von $z = x + iy$ ist $x \in \mathbb{R}$.

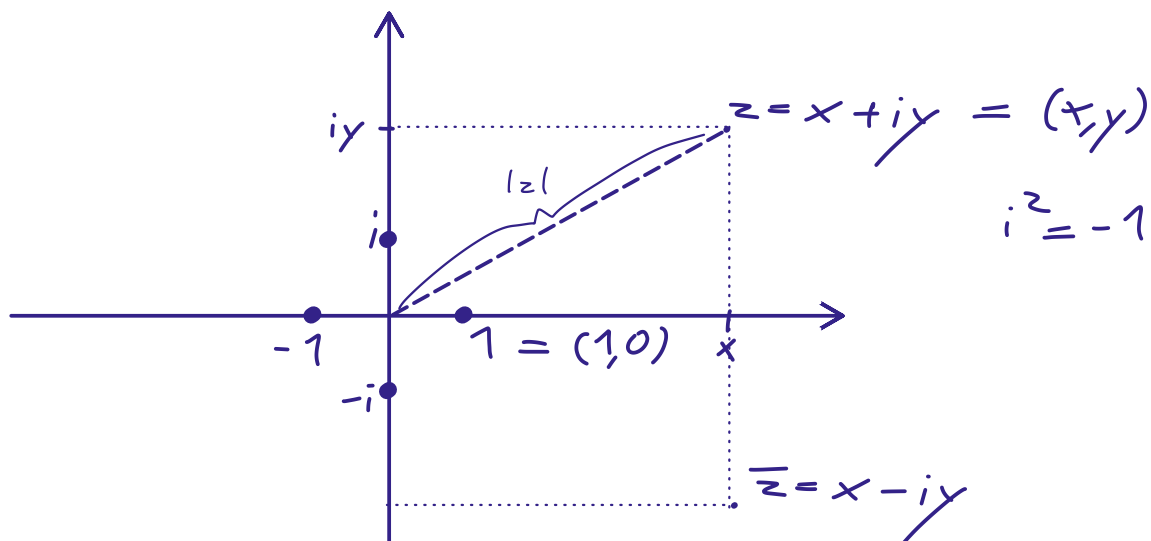
Imaginärteil von $z = x + iy$ ist $y \in \mathbb{R}$.

Komplex konjugierte Zahl zu $z = x + iy$
ist $\bar{z} := x - iy$

Betrag von $z = x + iy$ ist

$$|z| := \sqrt{x^2 + y^2} \in \mathbb{R}$$

(oder $\|z\|$)



3.11 Notiz:

(a) $z \mapsto \bar{z}$ ist ein Körperhomomorphismus
 (sogar -isomorphismus),

also $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$

und $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$

(b) $\overline{\bar{z}} = z$

(c) $|z|^2 = z \cdot \bar{z}$

