Ringe & Körper

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

(R1) $(R, \oplus)$ abelsche Gruppe

(R2a) $\odot$ assoziativ

(R2b) $\odot$ besitzt neutrales Element

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

$$(x \oplus y) \odot z = x \odot z \oplus y \odot z$$
$$z \cdot (x \oplus y) = z \odot x \oplus z \odot y$$

Der Ring ist **kommutativ**, falls $\odot$ kommutativ ist.

Notation: 0 neutrales Element für $\oplus$

1 neutrales Element für $\odot$

(eindeutig (vgl. Notiz 2.4))

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

$$0 \cdot x = (0+0) \cdot x \underset{R3}{=} 0 \cdot x + 0 \cdot x \quad \Big| -(0 \cdot x)$$
$$0 = 0 \cdot x$$

Beispiele:

$0+0 = 0\cdot 0 = 0$

① Nullring: $(\{0\}, +, \cdot)$

② $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ sind Ringe

gewöhnliche Addition & Multiplikation

③ $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist ein Ring:

$[x]\cdot[y] := [x\cdot y]$ ist wohldefiniert:

$$\begin{aligned}
&[x+k\cdot m][y+\ell\cdot m] \qquad k,\ell\in\mathbb{Z}\\
&= [(x+km)\cdot(y+\ell m)]\\
&= [x\cdot y + m(ky + x\ell + k\ell m)]\\
&= [x\cdot y] \quad \checkmark
\end{aligned}$$

Axiome prüfen: Übung

3.3 Def: Ein Ringhomomorphismus $f: R \longrightarrow S$ ist eine Abbildung, für die gilt:

$$\forall x,y\in R \begin{cases} f(x+y) = f(x)+f(y)\\ f(x\cdot y) = f(x)\cdot f(y)\\ f(1) = 1 \end{cases}$$

(Es ist dann auch $f(-x) = -f(x)$ und $f(0) = 0$ – vgl. Notiz 2.11)

3.4 Def: Einheitengruppe

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

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

Beispiele:

$$\mathbb{Z}^\times = (\{\pm 1\}, \cdot)$$

$$\mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}, \cdot)$$

$$\mathbb{R}^+ = (\mathbb{R} \setminus \{0\}, \cdot)$$

$$(\mathbb{Z}/8\mathbb{Z})^\times \ni [3], \text{ denn } [3] \cdot [3] = [9] = [1]$$
$$\notin [2] \quad [\ldots]$$

geändert

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

Ein Körperhomomorphismus ist ein Ringhomomorphismus zwischen Körpern.

Nachtrag

3.6 Notiz: In Körpern und in $\mathbb{Z}$ gilt:

$$a \cdot b = 0 \iff (a = 0 \vee b = 0)$$

(($\Leftarrow$) siehe Notiz 3.2

($\Rightarrow$ für Körper): Falls $b \neq 0$ folgt durch Multiplikation mit b^{-1}: $a = 0$.

($\Rightarrow$ für $\mathbb{Z}$): bekannt / nutze, dass $\mathbb{Z} \hookrightarrow \mathbb{Q}$ (Körper) Unterring ist)

⚠ I.A. falsch, z.B. $[2] \cdot [2] = [0]$ in $\mathbb{Z}/4\mathbb{Z}$

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 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

Beweis:

$p \in \mathbb{Z}$ ist Primzahl, falls:

1. $p \neq 0, 1, -1$ und
2. $\forall n, m \in \mathbb{Z}$: ($p$ teilt n)

$$p \mid (n \cdot m) \Longrightarrow (p \mid n \vee p \mid m)$$

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

seien $n, m \in \mathbb{Z}$ sodass $p \mid n \cdot m$.

Dann $\exists k \in \mathbb{Z}$:

$$n \cdot m = k \cdot p \in \mathbb{Z}, \text{ also}$$

$$[n] \cdot [m] = [k] \cdot \underbrace{[p]}_{[0]} \in \mathbb{Z}/p\cdot\mathbb{Z},$$

also $[n] \cdot [m] = [0] \in \mathbb{Z}/p\cdot\mathbb{Z}$.

Nach Notiz 3.6 folgt:

$[n] = 0$ oder $[m] = 0$

also $p \mid n$ oder $p \mid m$.

veveinfacht

($\Leftarrow$) Sei p eine Primzahl.
Sei $[n] \in \mathbb{Z}/p\mathbb{Z}$, $[n] \neq [0]$.
(zz: $[n]$ besitzt Inverses bzgl. $\cdot$)

- Multiplikation mit $[n]$ definiert Gruppenhomomorphismus

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z}, +) & \xrightarrow{f} & (\mathbb{Z}/p\mathbb{Z}, +) \\ [m] & \longmapsto & [m] \cdot [n] \end{array}$$

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

$$\begin{aligned} f([m]) = [0] &\Rightarrow [m] \cdot [n] = [0] \\ &\Rightarrow [m \cdot n] = [0] \\ &\Rightarrow p \mid m \cdot n \\ p \text{ prim} \quad &\Rightarrow p \mid m \vee p \mid n, \\ \text{also } [m] = 0 \; &[\vee [n] = 0.] \end{aligned}$$

- Nach Injektivitätskriterium (2.16) folgt: f injektiv
- Nach Satz 1.26 (Def.- und Bildbereich gleich endlich viele Elemente) folgt: f surjektiv.

Also insbesondere:
$\exists [m] \in \mathbb{Z}/p\mathbb{Z}$ mit $f([m]) = [1]$,
also $[m] \cdot [n] = [1]$

□

Komplexe Zahlen

3.8 Def: Eine komplexe Zahl ist ein Symbol $x \oplus iy$ mit $x, y \in \mathbb{R}$

$$(x \oplus iy = x' \oplus iy' :\Leftrightarrow (x = x' \wedge y = y'))$$

x Realteil

y Imaginärteil

Für komplexe Zahlen definieren wir:

$$(x \oplus iy) +_{\mathbb{C}} (x' \oplus iy') := (x + x') \oplus i(y + y')$$

$$(x \oplus iy) \cdot_{\mathbb{C}} (x' \oplus iy') := (xx' - yy') \oplus i(xy' + x'y)$$

(in $\mathbb{R}$)

$\mathbb{C} :=$ Menge aller komplexen Zahlen

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

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & x \oplus i \cdot 0 \end{array}$$

ist ein Körperhomomorphismus.

Beweis:

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

$$0_{\mathbb{C}} = 0 \oplus i \cdot 0$$

(R2) $\cdot_{\mathbb{C}}$ assoziativ [... → Tutorium]

$$1_{\mathbb{C}} = 1 \oplus i \cdot 0$$

(R3) Distributivität [... nachrechnen]

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

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

Multiplikatives Inverse zu $x \oplus iy \neq 0_{\mathbb{C}}$:

$$(x \oplus iy)^{-1} = \underbrace{\frac{x}{x^2+y^2}}_{\neq 0} \oplus i \frac{-y}{x^2+y^2} \quad [...]$$

□

Notation: Ab sofort

$x + iy$ für $x \oplus iy$

$+$ für $+_{\mathbb{C}}$

$\cdot$ für $\cdot_{\mathbb{C}}$

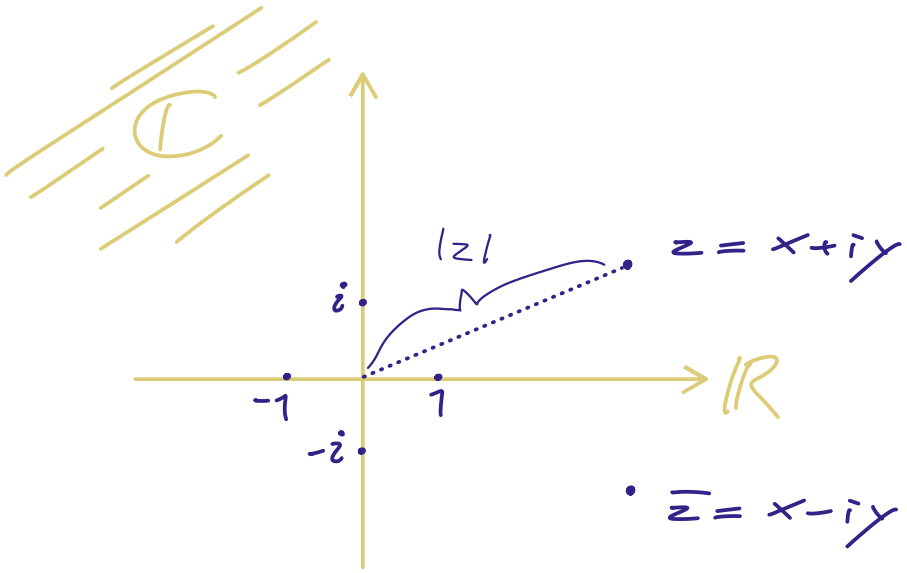
Es ist $i^2 = -1$. Daraus lassen sich Def. von $+_{\mathbb{C}}$ und $\cdot_{\mathbb{C}}$ leicht ableiten.

3.10 Def:

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

Betrag von $z = x+iy$ ist

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



3.11 Notiz:

(a) $- : \mathbb{C} \longrightarrow \mathbb{C}$, $z \mapsto \overline{z}$ Körperisomorphismus,

also insbesondere $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

$\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

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

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