

§3 Körper und Ringe

$(\mathbb{R}, +, \cdot)$

Allg. Mengen A mit 2 Verknüpfungen „+“ und „·“.
 Neutralelemente „0“ und „1“. Inverse werden mit
 „-x“ bezüglich der Addition bzw x^{-1} bezüglich der
 Multiplikation bezeichnet.

Definition:

Sei A eine Menge mit Verknüpfungen „+“ und „·“.

$(A, +, \cdot)$ heißt Körper, wenn gilt:

- (a) $(A, +)$ ist abelsche Gruppe
- (b) $(A \setminus \{0\}, \cdot)$ ist abelsche Gruppe
- (c) es gelten die Distributivgesetze:

$$\forall x, y, z \in A: x(y+z) = xy + xz,$$

$$(x+y)z = xz + yz$$

Schreibweise:

Der Punkt „·“ der Multiplikation lässt man meist
 weg und außerdem schreibt man $xy + z$ statt
 $(x \cdot y) + z$.

Bemerkungen:

(1) Jeder Körper hat mindestens zwei Elemente
 0, 1 (verschieden). Der kleinste Körper ist

$\mathbb{F}_2 = \{0, 1\}$:

+	0	1
0	0	1
1	1	0

wg. $A \setminus \{0\} = \mathbb{F}_2^\times$

·	0	1
0	0	0
1	0	1

(2) In jedem Körper gilt $0x = x0 = 0 \quad \forall x \in A$.

Denn: $x(x+0) = x \cdot x + x \cdot 0$

$\underbrace{x \cdot x}_{x \cdot x} = x \cdot x + x \cdot 0$

$\xrightarrow{\text{Subtr.}} \text{wegen } x \cdot x - x \cdot x + 0 \Rightarrow x \cdot 0 = 0$

Andere Gleichung analog.

(3) In jedem Körper gilt: $x(-y) = (-x)y = -xy \quad \forall x, y \in A$.

Denn: $x(y-y) = x \cdot 0 = 0$ (nach (2))

$\stackrel{\text{Subtr.}}{=} xy + x(-y) \Rightarrow x(-y) = -xy$

Analog $(-x)y = -xy$.

(4) Ein Körper $(A, +, \cdot)$ ist nullteilerfrei.

Aus $x \neq 0, y \neq 0$ folgt $xy \neq 0$.

Denn: $x \neq 0, y \neq 0 \Rightarrow x, y \in A \setminus \{0\} \stackrel{(2)}{\Rightarrow} xy \in A \setminus \{0\}$

Beispiele:

(1) $(\mathbb{Z}, +)$ kein Körper, weil jedes $z \notin \{0, \pm 1\}$ kein Inverses besitzt (bezügl. der Multiplikation).

$(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

(2) $A = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ mit üblichen Verknüpfungen
 $+, \cdot$ ist ein Körper $\mathbb{Q}(\sqrt{2})$. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ (Übungen)

Weiteres Beispiel sind die Restklassenkörper:

Sei $m \in \mathbb{N}$ fest. Äquivalenzrelation \sim auf \mathbb{Z} :

$x \sim y \Leftrightarrow x - y \in m \cdot \mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$

$\Leftrightarrow x, y$ haben den gleichen Rest bei Division durch m

$\Leftrightarrow f(x) = f(y)$, wo $f: \mathbb{Z} \rightarrow \{0, 1, \dots, m-1\}$

$x \mapsto r$ mit $x = m \cdot z + r; z \in \mathbb{Z}$

$\mathbb{Z}_m := \mathbb{Z}/m = \mathbb{Z}/f = \underbrace{\{[0]_m, [1]_m, \dots, [m-1]_m\}}_{m \text{ Klassen}}$

Verknüpfungen: $[x]_m + [y]_m := [x+y]_m$

$[x]_m \cdot [y]_m := [x \cdot y]_m$

Funktioniert nur, wenn die rechte Seite von den Repräsentanten unabhängig sind: D.h. $x' \sim x, y' \sim y$

$$\Rightarrow x' + y' \sim x + y$$

$$x' \cdot y' \sim x \cdot y$$

Beweis:

$$x' \sim x, y' \sim y \Rightarrow x' - x = m \cdot z, y' - y = m \cdot \tilde{z}$$

$$\Rightarrow (x' + y') - (x + y) = x + mz + y + m\tilde{z} - x - y = m(z + \tilde{z}) \checkmark$$

$$\begin{aligned} x' \cdot y' - x \cdot y &= xy + x \cdot m \cdot \tilde{z} + y \cdot m \cdot z + m^2 z \cdot \tilde{z} - xy \\ &= m(x\tilde{z} + yz + mz\tilde{z}) \checkmark \end{aligned}$$

Frage:

Wann ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper?

$(\mathbb{Z}_m, +)$ ist abelsche Gruppe. Genauer: $m \in \mathbb{Z}$ Untergruppe von \mathbb{Z} . (\Rightarrow Normalteiler). $\Rightarrow \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ Faktorgruppe. (Restklassengruppe).

$(\mathbb{Z} \setminus \{0\}, \cdot)$ ist kommutative Halbgruppe mit Einselement $[1]_m$ und assoziativ.

Aber: atlg. nicht abgeschlossen gegen \cdot .

Sei $m \geq 2$ und m keine Primzahl. $\Rightarrow m = pq, p, q \in \{2, \dots, m-1\}$

$\Rightarrow \underbrace{[p]_m} \cdot \underbrace{[q]_m} = [m]_m = [0]_m \Rightarrow$ Wenn m keine Primzahl ist, ist $(\mathbb{Z}_m, +, \cdot)$ kein Körper.

Satz 9:

Ist $m \geq 2$ eine Primzahl, so ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper.

Beweis:

Zu zeigen ist nur noch, dass aus $[x]_m, [y]_m \neq [0]_m$ immer $[x]_m [y]_m \neq [0]_m$ folgt, und dass jedes $[x]_m \neq [0]_m$ ein Inverses bzgl. \cdot besitzt.

Es gilt:

Aus $[x]_m [y]_m = [y]_m [z]_m$ und $[x]_m \neq [0]_m$

folgt $[y]_m = [z]_m$.

$$\Rightarrow [x]_m [y]_m = [x]_m [z]_m \Rightarrow \frac{x \cdot y - xz}{x(y-z)} = \frac{m \cdot n}{p} \text{ Primzahl.}$$

$\Rightarrow m$ teilt $x(y-z)$ aber m teilt nicht x .

$\Rightarrow m$ teilt $y-z \Rightarrow [y]_m = [z]_m$