

§3 Körper

(3.1) Definition

Ein **Körper** ist eine Menge K auf der zwei Verknüpfungen

$$+ : K \times K \rightarrow K$$

$$\bullet : K \times K \rightarrow K$$

definiert sind derart dass gilt

- I. $(K, +)$ ist eine abelsche Gruppe
- II. $\bullet$ ist assoziativ, kommutativ, $\exists 1 \in K : a \cdot 1 = a \quad \forall a \in K$
 $\forall a \neq 0 \exists a^{-1} \in K : a \cdot a^{-1} = 1$
- III. Distributivgesetz $a(b + c) = ab + ac$
- IV. $1 \neq 0$

(3.2) Beispiele

- (1) $\mathbb{Q}, \mathbb{R}$ sind Körper
- (2) $\mathbb{Z}$ ist kein Körper

Sei p eine Primzahl

$$\Rightarrow \mathbb{Z}/\mathbb{Z} \cdot p \text{ ist ein Körper (mit } p \text{ Elementen)}$$

Beweis:

I klar

$$\text{II Sei } \bar{a} \in \mathbb{Z}/\mathbb{Z} \cdot p, \bar{a} \neq 0 \Leftrightarrow p \nmid a$$

$$\Leftrightarrow \text{ggT}(p, a) = 1$$

$$\Rightarrow \exists \bar{b} \in \mathbb{Z}/\mathbb{Z} \cdot p : \bar{b} \cdot \bar{a} = 1 \text{ (Satz 1.20)}$$

$$\Rightarrow \text{Behauptung}$$

q.e.d.

(3.3) Satz

Sei K ein Körper

- (1) $a \cdot 0 = 0 \quad \forall a \in K$
- (2) Sei $a \neq 0 \Rightarrow ax + b = c$ hat genau die Lösung $x = a^{-1}(c - b)$
- (3) $(-a)b = -(ab)$
- (4) $K^\times = K \setminus \{0\} \Rightarrow (K^\times, \bullet)$ ist eine abelsche Gruppe

Beweis zu (4):

Nur zu zeigen, dass $\bullet$ eine Verknüpfung auf $K^\times$ ist, d.h.

$$a, b \in K^\times \Rightarrow a \cdot b \in K^\times \text{ (und } K^\times \neq \emptyset \text{!)}$$

$$1 \in K^\times$$

Es gilt $a \cdot b \cdot b^{-1} \cdot a^{-1} = 1 \neq 0 \Rightarrow a \cdot b \neq 0 \Rightarrow K^\times$ ist abelsche Gruppe

(3.4) Folgerung

Sei $\bar{a} \in \mathbb{Z}/\mathbb{Z} \cdot p$, $a \neq 0$

Dann $\bar{a}^{p-1} = 1$, d.h.

$$\forall a \in \mathbb{Z} \quad \text{ggT}(a, p) = 1 \quad \text{gilt} \quad \bar{a}^{p-1} \equiv 1 \pmod{p}$$

Beweis:

$\left(\bar{a} \in \mathbb{Z}/\mathbb{Z} \cdot p \right)^\times$ ist Gruppe mit $p-1$ Elementen

Aus (2.20)(2) (kleiner Fermatscher Satz) folgt die Behauptung

Beispiel:

$\mathbb{Q}, \mathbb{R}, \mathbb{Z}/\mathbb{Z} \cdot p$, p prim

(3.5) Beispiel

Sei $d \in \mathbb{N}_+$, d sei kein Quadrat

$$\Rightarrow \sqrt{d} \notin \mathbb{Q}$$

Sei $K := \{a + b \cdot \sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$

$(K, +, \bullet)$ ist ein Körper

Beweis:

a) $+, \bullet$ sind Verknüpfungen auf K

Seien $a + b\sqrt{d}, a' + b'\sqrt{d} \in K$

$$(a + b\sqrt{d}) + (a' + b'\sqrt{d}) = (\underbrace{a + a'}_{\in \mathbb{Q}}) + (\underbrace{b + b'}_{\in \mathbb{Q}})\sqrt{d} \in K$$

$$\begin{aligned} (a + b\sqrt{d}) \cdot (a' + b'\sqrt{d}) &= aa' + ab'\sqrt{d} + a'b\sqrt{d} + bb'd \\ &= (aa' + bb'd) + (ab' + a'b)\sqrt{d} \in K \end{aligned}$$

b) $+$, $\bullet$ sind assoziativ, kommutativ, da das in R gilt

$$0 \in K : 0 = 0 + 0\sqrt{d}$$

$$1 \in K$$

$$-(a + b\sqrt{d}) = (-a) + (-b)\sqrt{d} \in K$$

Distributivgesetz: gilt in $R \Rightarrow$ in K

zu zeigen: Sei $x = a + b\sqrt{d} \in K$

$$\Rightarrow \exists y \in K : x \cdot y = 1$$

Betrachte $(a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - b^2d \in \mathbb{Q}$

Beh. Ist $a \neq 0$ oder $b \neq 0$, so ist $a^2 - b^2d \neq 0$

Falls $b = 0$, so ist dies wahr

$$\text{Sei } b \neq 0 \text{ Annahme: } a^2 - b^2d = 0 \Rightarrow d = \frac{a^2}{b^2} \Rightarrow \sqrt{d} \in \mathbb{Q} \quad \text{✗}$$

$$\Rightarrow (a + b\sqrt{d}) \cdot \underbrace{\left(\frac{a}{a^2 - b^2d} - \frac{b}{a^2b^2d} \sqrt{d} \right)}_{\in K} = 1$$

$\Rightarrow K$ ist Körper

$$K = \mathbb{Q}(\sqrt{d}) \quad (\mathbb{Q} \text{ adjungiert Wurzel } d)$$

q.e.d.