Körper

Wir betrachten Mengen mit zwei Verknüpfungen, für denen gewisse Eigenschaften damit sich wieder gut rechnen lässt.

Definition: Eine Menge K zusammen mit zwei inneren Verknüpfungen $\oplus$ und $\odot$ nennt man Körper :$\Leftrightarrow$

a) $(K, \oplus)$ ist abelsche Gruppe

b) $(K \setminus \{0\}, \odot)$ ist abelsche Gruppe.

0 bezeichnet hier das Neutrale bzgl $\oplus$

(1 " " " " $\odot$)

c) Es gilt das Distributivgesetz :

$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ somit

$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

Satz: Es gilt in jedem Körper K, dass

$$a \odot 0 = 0 \odot a = 0 \qquad \forall\, a \in K$$

Beweis:

$$0 = a \oplus (-a) = (a \odot 1) \oplus (-a) =$$

$$= (a \odot (1 \oplus 0)) \oplus (-a) =$$

$$= ((a \odot 1) \oplus (a \odot 0)) \oplus (-a) =$$

$$= (a \oplus (a \odot 0)) \oplus (-a) =$$

$$\overset{\text{K.G.}\oplus}{\underset{\text{A.G.}\oplus}{=}} a \oplus (-a) \oplus (a \odot 0) = 0 \oplus (a \odot 0) = (a \odot 0)$$

Ebenso ("gespiegelte" Rechnung) $\Rightarrow \quad 0 = 0 \odot a$

Korollar: Es gilt das Kommutativgesetz und Assoziativgesetz auch bzgl. $\odot$ auf ganz K! (und nicht nur auf $K \setminus \{0\}$)

Beweis:

$$a \odot 0 = 0 = 0 \odot a$$

$a \odot (b \odot c) = 0$ falls mindestens ein Faktor 0 ist

$(a \odot b) \odot c = 0$ " " " " " "

Notation: Wir bezeichnen das Inverse von a bzgl $\oplus$ als $-a$

" " " " " " bzgl $\odot$ als a^{-1}

Wir benutzen die "Punkt vor Strich" Konvention:

$$a \odot b \oplus c := (a \odot b) \oplus c$$

Satz: $a \odot b = 0 \quad \Leftrightarrow \quad a = 0 \text{ oder } b = 0$

Beweis: "$\Leftarrow$" hatten wir gerade gezeigt.

"$\Rightarrow$" Annahme: $b \neq 0$, zeige $a = 0$.

$a \odot b = 0$

$$a = a \odot b \odot b^{-1} = 0 \odot b^{-1} = 0 \quad (\text{wegen } "\Leftarrow").$$

Satz: a) $a \odot (-b) = -(a \odot b)$

b) $(-a)^{-1} = -(a^{-1}) \quad \forall\, a \neq 0$

Beweis: a) $0 = a \odot 0 = a \odot (b \oplus (-b)) = a \odot b \oplus a \odot (-b)$

Das Inverse ist eindeutig $\Rightarrow a \odot (-b) = -(a \odot b)$ $\square$

b) o.B.d.A.: zeigen wir $(-1)^{-1} = -(1^{-1})$

Falls das gilt, so ist jedes $a \neq 0$:

$$a^{-1} \odot (-1)^{-1} = a^{-1} \odot \left(-(1)^{-1}\right)$$

$$\left(a \odot (-1)\right)^{-1} = -\left(a^{-1} \odot 1^{-1}\right) \quad (\Leftarrow a)$$

$$(-a)^{-1} = -(a^{-1})$$

Formel: $a^{-1} \odot b^{-1} = (a \odot b)^{-1}$

$(1^{-1} = 1)$

$$1 = (-1) \odot (-1)^{-1} = -\left(1 \odot (-1)^{-1}\right) = -\left((-1)^{-1}\right)$$

$\Rightarrow (-1)^{-1} = -1$ da $-(-1) = 1$

$\Rightarrow -1 = (-1)^{-1}$ da $1^{-1} = 1$ folgt

$-(1^{-1}) = (-1)^{-1}$

Bsp.: a) $(\mathbb{Q}, +, \cdot)$ sowie $(\mathbb{R}, +, \cdot)$ sind Körper.

b) Sei p eine Primzahl. Betrachte

$$K_p = \{0, 1, 2, \ldots p-1\}$$

Definiere $a \oplus b$ = Rest von $a+b$ nach Teilen durch p

$a \odot b$ = " " $a \cdot b$ " " " " ".

$(K_p, \oplus, \odot)$ ist ein Körper!

Gültigkeit der K.- und A. und D.-Gesetze folgen vergleichsweise direkt aus den entspr. Gesetzen für $+$ und $\cdot$.

$0, 1$ sind die neutralen Elemente bzgl $\oplus$ und $\odot$.

§ Für jedes $a \neq 0$, $a \in K_p$ ist $-a = p - a$

↖ Rechenzeichen - in $\mathbb{N}$.

$a \oplus (-a)$ = Rest von $a + (p-a)$ beim Teilen durch p $= 0$.

Wir zeigen nun, dass es für jedes $a \neq 0$ ein multiplikativ-inverses gibt.

Dazu: Sei $a \neq 0$. Wenn man a mit einer bel. Element $b \neq 0$ multipliziert: $a \odot b \neq 0$

(Warum! a und b haben p nicht als Teiler!

Da p Primzahl ist $a \cdot b$ kein Vielfaches von p)

$\Rightarrow a \odot b \neq 0$

Außerdem ist $a \odot b \neq a \odot c$ falls $b \neq c$.!

Man erhält also beim Multiplizieren von a mit den unterschiedlichen Elementen aus K_p genau p unterschiedliche Resultate. Genau eines der Produkte $\mu \cdot p$ also 1 sein.

z.z.:

Betrachte $a \odot b = a \odot c$ d.h $a \cdot b = a \cdot c + \mu \cdot p$; $\mu \in \mathbb{Z}$

$a \cdot (b-c) = \mu \cdot p \Rightarrow b-c$ ist vielfaches von p,

$\Rightarrow (b-c) = 0$ liegt aber zwischen $-(p-1)$ und $p-1$

c) K_2 ist der kleinste Körper.