Gruppen und Körper

Definition. Eine **Gruppe** ist ein Paar $(G, \cdot)$ wobei G eine Menge ist und " $\cdot$ " eine Verknüpfung auf G ist, d.h. eine Abbildung $G \times G \to G$, $(a, b) \mapsto a \cdot b$ mit

G1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\, a, b, c \in G$

G2) $\exists\, e \in G$ sodass $e \cdot a = A \quad \forall\, a \in G$ (e ... neutrales Element)

G3) $\forall\, a \in G \;\; \exists\, a' \in G$ mit $a' \cdot a = e$ (a' ... inverses Element von a)

$(G, \cdot)$ heißt **abelsche Gruppe**, wenn $a \cdot b = b \cdot a \quad \forall\, a, b \in G$ ist (d.h. die Verknüpfung ist kommutativ).

Vereinfacht wird meist G statt $(G, \cdot)$ und ab statt $a \cdot b$ geschrieben.

Bemerkungen.

i) $\overset{1}{\exists}$ neutrales Element $e \in G$ und $a \cdot e = a \quad \forall\, a \in G$,

ii) mit $a'a = e$ gilt auch $aa' = e$,

$\overset{1}{\exists}$ inverses Element von a , dies wird in der Regel mit a^{-1} bezeichnet,

iii) $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$, $e^{-1} = e$.

Beispiele.

1) $(\mathbb{Z}, +)$ ist abelsche Gruppe bezüglich der üblichen Addition von ganzen Zahlen. Das neutrale Element ist 0 , das inverse Element von n ist $-n$.
In derselben Weise sind $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ ebenfalls abelsche Gruppen.

2) $(\mathbb{Q}^*, .)$, wobei $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, ist eine abelsche Gruppe bezüglich der üblichen Multiplikation. Das neutrale Element ist 1 , das inverse Element von $q \in \mathbb{Q}^*$ ist $\frac{1}{q}$.
Ebenso sind die Mengen $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{Q}_+^* = \{x \in \mathbb{Q} \;:\; x > 0\}$ und $\mathbb{R}_+^* = \{x \in \mathbb{R} \;:\; x > 0\}$ abelsche Gruppen bzgl. der Multiplikation.

3) Sei $M \neq \emptyset$ eine Menge, und sei $S(M) := \{f : M \to M \;:\; f \text{ ist bijektiv}\}$.
Dann ist $(S(M), \circ)$ eine Gruppe bzgl. der Verknüpfung von Abbildungen, und heißt die **symmetrische Gruppe** von M . Das neutrale Element ist die identische Abbildung id_M , das inverse Element zu $f \in S(M)$ ist die Umkehrabbildung f^{-1} .
Man beachte, daß $(S(M), \circ)$ im allgemeinen nicht abelsch ist.

Im speziellen sei $M = \{1, 2, ..., n\}$. Dann schreibt man S_n für $S(M)$. Jede Abbildung $\sigma \in S_n$ heißt eine **Permutation** der Zahlen $1, 2, ..., n$.

Definition. Ein **Körper** ist ein Tripel $(K, +, \cdot)$, wobei K eine Menge ist und "$+$" bzw. "$\cdot$" Verknüpfungen ("Addition" bzw. "Multiplikation") auf K sind, also Abbildungen $+ : K \times K \to K \quad (a, b) \mapsto a + b$ bzw. $\cdot : K \times K \to K \quad (a, b) \mapsto a \cdot b$ sodass

K1) $(K, +)$ ist abelsche Gruppe. Das neutrale Element wird mit 0 und das inverse Element von $a \in K$ mit $-a$ bezeichnet,

K2) $(K^*, \cdot)$ mit $K^* = K - \{0\}$ ist abelsche Gruppe mit neutralem Element 1 und a^{-1} als inversem Element zu $a \in K$.

K3) $a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad , \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Als vereinfachte Schreibweisen hat man K statt $(K, +, \cdot)$, ab statt $a \cdot b$, $a - b$ statt $a + (-b)$, $\frac{b}{a}$ statt $b \cdot a^{-1}$, und $ab + ac$ statt $(a \cdot b) + (a \cdot c)$.

Bemerkung. Für jeden Körper K gilt:

i) $0 \cdot a = a \cdot 0 = 0 \quad \forall\, a \in K$

ii) $a \cdot b = 0 \quad \Rightarrow \quad a = 0$ oder $b = 0$ (Nullteilerfreiheit)

iii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

Beispiele.

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

2) $\mathbb{R} \times \mathbb{R}$ wird ein Körper durch $(a, b) + (a', b') := (a + a', b + b')$ und $(a, b) \cdot (a', b') := (aa' - bb', ab' + a'b)$. Das neutrale Element bzgl. der Addition ist dann $(0, 0)$, das neutrale Element bzgl. der Multiplikation ist $(1, 0)$.
Dieser Körper heißt der **Körper der komplexen Zahlen** und wird mit $\mathbb{C}$ bezeichnet.

Man beachte, daß die Abbildung $\mathbb{R} \to \mathbb{R} \times \mathbb{R}$ mit $a \mapsto (a, 0)$ injektiv ist. Wegen $(a, 0) + (a', 0) = (a + a', 0)$ und $(a, 0) \cdot (a', 0) = (a \cdot a', 0)$ können $\mathbb{R}$ und $\mathbb{R} \times \{0\} \subseteq \mathbb{C}$ identifiziert werden, d.h. der Körper $\mathbb{R}$ kann als "Unterkörper" von $\mathbb{C}$ betrachtet werden.

Man definiert $i := (0,1) \in \mathbb{C}$ als die sogenannte **imaginäre Einheit** . Damit gilt dann $(a,b) = (a,0) + (b,0) \cdot (0,1) = a + bi$.

Zu $\lambda = a + bi \in \mathbb{C}$ heißt

$\mathrm{Re}\lambda := a$ der **Realteil** von λ ,

$\mathrm{Im}\lambda := b$ der **Imaginärteil** von λ ,

$\overline{\lambda} := a - bi$ die **konjugiert komplexe Zahl** zu λ .

Die folgenden Rechenregeln gelten für $\lambda, \mu \in \mathbb{C}$, $\lambda = a + bi$:

$\overline{\lambda + \mu} = \overline{\lambda} + \overline{\mu}$, $\overline{\lambda \cdot \mu} = \overline{\lambda} \cdot \overline{\mu}$, $\lambda \in \mathbb{R} \Leftrightarrow \lambda = \overline{\lambda}$

$|\lambda| := \sqrt{\lambda\overline{\lambda}} = \sqrt{a^2 + b^2} = \|(a,b)\|$ heißt der **Betrag** von λ

$|\lambda + \mu| \leq |\lambda| + |\mu|$, $|\lambda\mu| = |\lambda| \cdot |\mu|$.

3) Sei $K = \{0,1\}$ und definiere $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$ sowie $0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0$, $1 \cdot 1 = 1$.

Dann ist $(K, +, \cdot)$ ein (endlicher) Körper (der Körper der Restklassen mod 2) .