§12 Ringhomomorphismen und Einheitengruppe

(12.1) Def (Ringhomomorphismus)

Ein Homomorphismus zwischen Ringen R und S ist eine Abbildung $\varphi : R \to S$ mit

$$(a+b)\varphi = a\varphi + b\varphi \quad \text{und} \quad (ab)\varphi = (a\varphi)(b\varphi)$$

für alle $a, b \in R$.

Sind R, S Ringe mit $1 \neq 0$, so verlangt man oft zusätzlich $1\varphi = 1$.

Bspl: a) Für jedes $m \in \mathbb{N}$ ist die Restklassenabb.

$$\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad a \mapsto a + m\mathbb{Z}$$

ein Ringhomomorphismus.

b) Ebenso ist die Inklusionsabbildung

$$\mathbb{Z} \to \mathbb{Q}, \quad a \mapsto a$$

ein Ringhomomorphismus.

(12.2) Def (Ringisomorphismus)

Ein Isomorphismus zwischen Ringen R und S ist ein bijektiver Ringhomomorphismus $\varphi : R \to S$, für den die Umkehrabbildung $\varphi^{-1} : S \to R$ ebenfalls ein Homomorphismus ist.

Besteht ein Isomorphismus $R \to S$,

so heißen R und S <u>isomorph</u>, in Zeichen $R \cong S$.

<u>Bem</u>: Ist $\varphi: R \to S$ ein bijektiver Ringhomomorphismus, so ist $\varphi^{-1}: S \to R$ in Wahrheit automatisch ein Homomorphismus: Für $a, b \in S$ gilt

$$(a+b)\varphi^{-1} = ((a\varphi^{-1}\varphi) + (b\varphi^{-1}\varphi))\varphi^{-1}$$

$$= ((a\varphi^{-1})\varphi + (b\varphi^{-1})\varphi)\varphi^{-1}$$

$$= ((a\varphi^{-1} + b\varphi^{-1})\varphi)\varphi^{-1}$$

$$= (a\varphi^{-1} + b\varphi^{-1})(\varphi\varphi^{-1}) = a\varphi^{-1} + b\varphi^{-1}$$

und ähnlich

$$(ab)\varphi^{-1} = (a\varphi^{-1})(b\varphi^{-1}).$$

(12.3) <u>Bspl</u> (komplexe Zahlen)

Auf $\mathbb{R} \times \mathbb{R}$ wird durch

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2)$$

eine Ringstruktur erklärt,

so daß $\mathbb{R} \times \mathbb{R} \to \mathbb{C}$, $(x, y) \mapsto x + yi$

einen Ringisomorphismus liefert.

In diesem Sinne ist $\mathbb{R} \times \mathbb{R}$ ein „Modell" für die komplexen Zahlen.

(12.4) Def (Gruppe)

Eine Gruppe $G=(G,\cdot)$ ist eine Menge G mit einer Verknüpfung $\cdot : G\times G \to G$, $(g,h)\mapsto gh$, so daß gilt

(G1) $\forall\ g_1,g_2,g_3 \in G: (g_1g_2)g_3 = g_1(g_2g_3)$ [assoziativ]

(G2) Es ex genau ein Elmt in G, welches mit 1 bezeichnet wird, für das gilt:

$\forall\ g\in G: 1\cdot g = g\cdot 1 = g$ [neutrales Elmt]

(G3) Zu jedem $g\in G$ ex genau ein Elmt in G, welches mit g^{-1} bezeichnet wird, für das gilt:

$g\,g^{-1} = g^{-1}g = 1$ [Inverses]

Gilt zusätzlich

$\forall\ g,h\in G: gh = hg$, [kommutativ]

so heißt die Gruppe G abelsch, und in dieser Situation schreibt man oft $+, 0, -g$ statt $\cdot, 1, g^{-1}$.

Bem: In (G2), (G3) darf auf die Eindeutigkeit verzichtet werden:

$1 = 1\cdot\tilde{1} = \tilde{1}$ und $g^{-1} = g^{-1}\cdot 1 = g^{-1}g\,\tilde{g}^{-1} = 1\cdot\tilde{g}^{-1} = \tilde{g}^{-1}$.

Desweiteren genügt es, die geforderten Eigenschaften nur linksseitig (oder nur rechtsseitig) zu verlangen:

Erfüllt $(G,\cdot)$ die Bed (G1) und Klopsch

geeignen $1 \in G$ und $G \to G$, $g \mapsto g^{-1}$ den Bedingungen

$(G2)'_e$ $\forall\, g \in G : 1 \cdot g = g$

$(G3)'_e$ $\forall\, g \in G : g^{-1} g = 1$, so folgt für alle $g \in G$:

$$g g^{-1} = \underbrace{(g g^{-1})^{-1} (g g^{-1})}_{=1} (g g^{-1}) = (g g^{-1})^{-1} \underbrace{(g (g^{-1} g) g^{-1})}_{= g \cdot 1 \, g^{-1} = g g^{-1}}$$

$$= (g g^{-1})^{-1} (g g^{-1}) = 1 \quad \text{und}$$

$$g \cdot 1 = g (g^{-1} g) = (g g^{-1}) g = g .$$

(12.5) Def / Beobachtung (Einheiten)

Sei R ein Ring mit 1, möglicherweise nicht kommutativ. (Formal lassen wir hier auch $R = \{0\}$ mit $0 = 1$ zu.) Ein Elmt $a \in R$ heißt invertierbar oder eine Einheit in R, falls gelten

$$\exists\, b \in R : ba = 1 \quad \text{und} \quad \exists\, c \in R : ac = 1 .$$

(linkes-inv bar) (rechts-inv bar)

In diesem Falle ist dann ein eindeutiges (linkes- und rechts-) Inverses a^{-1} von a bestimmt.

[Aus $ba = 1 = ac$ folgt $b = b \cdot 1 = bac = 1c = c$.]

(12.6) Def / Beob (Einheitengruppe) Sei R ein Ring mit 1. Dann bildet die Menge R^* aller Einheiten in R eine Gruppe, die Einheitengruppe von R.

Bew: Für $a, b \in R^*$ gilt stets $a^{-1}, b^{-1} \in R^*$ und $(b^{-1} a^{-1})\, ab = 1 = ab\,(b^{-1} a^{-1})$, also $ab \in R^*$. Offenbar sind damit (G1), $(G2)'_e$, $(G3)'_e$ erfüllt.

(12.7) Bspe / Def

a) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Z}/m\mathbb{Z},+)$, ...

$(V,+)$ für einen bel VR V

„additive Gruppen" (abelsch)

b) $\mathbb{Z}^* = \{1,-1\}$

$\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$

$\{z \in \mathbb{C} \mid |z| = 1\}$

„multiplikative Gruppen" (abelsch)

$(\mathbb{Z}/m\mathbb{Z})^*$

Bspl: $(\mathbb{Z}/15\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$

Multiplikationstabelle:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	...			$\overline{13}$	$\overline{14}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{14}$	$\overline{1}$	$\overline{7}$	$\overline{11}$	$\overline{13}$
$\vdots$								
$\overline{13}$			...					
$\overline{14}$								

c) $\{1, i, j, k, -1, -i, -j, -k\} \subseteq \mathbb{H}$ bzgl $\cdot$.

„Quaternionengruppe der Ordnung 8"

nicht-abelsche Gruppe Multiplikationstabelle: Übung!

d) Symmetrische Gruppe

Sei X eine Menge. Eine Permutation von X ist eine bijektive Abb $\pi: X \to X$. Die Menge aller Permutationen von X bildet

Kapitel

bzgl der Hintereinanderausführung von Abbildungen eine Gruppe, die **symmetrische Gruppe** $Sym(X)$. Ist $X = \{1, 2, \dots, n\}$, so nennt man $Sym(n) = Sym(X)$ auch die **symmetrische Gruppe vom Grad n**.

Jedes Elmt $\pi \in Sym(n)$ läßt sich eindeutig durch eine **Abbildungstafel** $\begin{pmatrix} 1 & 2 & \dots & n \\ 1\pi & 2\pi & \dots & n\pi \end{pmatrix}$ beschreiben.

Die Identität $id = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ ist das neutrale Element, das Gruppeninverse die Umkehrabb.

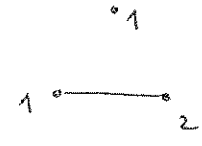
Eine Permutation $\tau \in Sym(n)$, die zwei Zahlen $i \neq j \in \{1, \dots, n\}$ vertauscht und alle anderen festläßt, heißt eine **Transposition**:

$$\tau = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

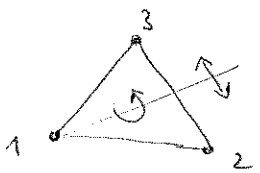
$n=0$ $\quad Sym(0) = \{\emptyset\} = \{()\}$

$n=1$ $\quad Sym(1) = \{id\} = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$

$n=2$ $\quad Sym(2) = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$



$n=3$ $\quad Sym(3)$ hat sechs Elmte:
id, drei Transpositionen,
zwei weitere Elemente



z.B. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

19
20

$n=4$ $\quad Sym(4)$ hat 24 Elmte

wirkt ↷ Raumdiagonalen eines Würfels