§ 15 . Gruppen, Ringe und Körper

A) Mengen mit Verknüpfungen

(15.1) DEF: Eine **Verknüpfung** (oder **Rechenoperation)** $\star$ auf einer nichtleeren Menge M ordnet je zwei Elementen x und y aus M in eindeutiger Weise wieder ein Element aus M zu, das mit $\boldsymbol{x \star y}$ bezeichnet wird.

Ist $\star$ eine Verknüpfung auf M, so heißt $\boldsymbol{(M, \star)}$ eine **Menge mit Verknüpfung** .

(15.2) Beispiele:

(15.3) DEF: Sei $\star$ eine Verknüpfung auf einer Menge M .

a) $\star$ heißt **assoziativ**, wenn gilt

$\forall\, x, y, z \in M \; : \; (x \star y) \star z = x \star (y \star z)$

b) $\star$ heißt **kommutativ**, wenn gilt

$\forall\, x, y \in M \; : \; x \star y = y \star x$

c) Ein Element $e \in M$ heißt **neutral bzgl.** $\star$, wenn gilt:

$\forall\, x \in M \; : \; x \star e = x = e \star x \, .$

(15.4) Beispiele:

(15.5) BEM: Ist $\star$ eine Verknüpfung auf M, so gibt es höchstens ein bzgl. $\star$ neutrales Element in M .

(15.6) DEF: Sei $(M, \star)$ eine Menge mit einer Verknüpfung $\star$ und einem bzgl. $\star$ neutralen Element $e \in M$. Ein Element $x \in M$ heißt **invertierbar bzgl.** $\star$, wenn es ein Element $y \in M$ gibt mit der Eigenschaft

$$x \star y \; = \; e \; = \; y \star x$$

(15.7) Beispiele:

(15.8) SATZ: $(M, \star)$ sei eine Menge mit einer assoziativen Verknüpfung $\star$ und einem neutralen Element $e \in M$. Dann gilt:

a) Ist $x \in M$ invertierbar bzgl. $\star$, so gibt es genau ein $y \in M$ mit der Eigenschaft $x \star y = e = y \star x$. y heißt dann das **Inverse von** x **bzgl.** $\star$ und wird mit $\overline{x}$ bezeichnet. Es gilt

$$x \star \overline{x} \;=\; e \;=\; \overline{x} \star x$$

b) Sind $x_1, x_2 \in M$ invertierbar bzgl. $\star$, so ist auch $x_1 \star x_2$ invertierbar bzgl. $\star$, und es gilt

$$\overline{x_1 \star x_2} \;=\; \overline{x_2} \star \overline{x_1}$$

c) e ist invertierbar bzgl. $\star$ mit $\overline{e} = e$

d) Ist $x \in M$ invertierbar bzgl. $\star$, so ist auch $\overline{x}$ invertierbar bzgl. $\star$, und es gilt $\overline{\overline{x}} \;=\; x$.

B) Gruppen

(15.9) DEF: G sei eine Menge und $\star$ eine Verknüpfung auf G. Dann heißt $(G, \star)$ eine **Gruppe**, wenn folgende Bedingungen erfüllt sind:

i) $\star$ ist assoziativ

ii) Es gibt ein bzgl. $\star$ neutrales Element e in G

iii) Jedes Element aus G ist invertierbar bzgl. $\star$.

Ist darüberhinaus $\star$ kommutativ, so heißt $(G, \star)$ eine **kommutative Gruppe** oder eine **abelsche Gruppe**.

(15.10) BEM: $(G, \star)$ ist genau dann eine Gruppe, wenn die folgenden Bedingungen erfüllt sind:

$\mathbf{G_0}$) $\forall\, a, b \in G \;:\; a \star b \in G$

$\mathbf{G_1}$) $\forall\, a, b, c \in G \;:\; (a \star b) \star c = a \star (b \star c)$

$\mathbf{G_2}$) $\exists\, e \in G\, \forall\, a \in G \;:\; a \star e = a = e \star a$

$\mathbf{G_3}$) $\forall\, a \in G\, \exists\, b \in G :\; a \star b = e = b \star a$

Gilt zusätzlich

$\mathbf{G_4}$) $\forall\, a, b \in G \;:\; a \star b = b \star a$

so ist $(G, \star)$ eine abelsche Gruppe.

(15.11) Beispiele: für abelsche Gruppen:

a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ (nicht aber $(\mathbb{N}, +)$)

b) $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$ (nicht aber $(\mathbb{Z} \setminus \{0\}, \cdot)$)

c) $(V, +)$, falls V ein Vektorraum ist.

d) $(\mathbb{R}^n, +)$, $(\mathrm{M}_{m,n}(\mathbb{R}), +)$

e) $(\mathbb{Z}_n, \oplus)$

f) $(\mathbb{Z}_3 \setminus \{0\}, \odot)$ (nicht aber $(\mathbb{Z}_4 \setminus \{0\}, \odot)$)

(15.12) SATZ: In einer Gruppe $(G,\star)$ gelten die folgenden **Kürzungsregeln**:

a) $\forall\, a,x,y \in G \,:\, a\star x = a\star y \quad\Longrightarrow\quad x=y$

b) $\forall\, a,x,y \in G \,:\, x\star a = y\star a \quad\Longrightarrow\quad x=y$

(15.13) FOLG: Sei $(G,\star)$ eine endliche Gruppe. Dann kommt in jeder Zeile und in jeder Spalte der Verknüpfungstafel (Gruppentafel) von $(G,\star)$ jedes Element von G genau einmal vor.

(15.14) DEF: $(G,\star)$ sei eine Gruppe mit dem neutralen Element e. Eine Teilmenge $U\subseteq G$ heißt eine **Untergruppe von** $(G,\star)$, wenn gilt:

UG$_1$) U ist abgeschlossen bzgl. $\star$ (d.h. $\forall\, a,b\in U \,:\, a\star b\in U$)

UG$_2$) $e\in U$

UG$_3$) $\forall\, a\in U \,:\, \overline{a}\in U$.

(15.15) Beispiele: **a)** $\{e\}$ und G sind Untergruppen von $(G,\star)$

b) Sei $k\in\mathbb{Z}$ fest: $\mathbb{Z}\,k := \{zk \mid z\in\mathbb{Z}\}$ ist eine Untergruppe von $(\mathbb{Z},+)$

c) Ist U ein Untervektorraum des Vektorraumes V, so ist U eine Untergruppe von $(V,+)$

d) $\mathbb{R}_{>0} := \{r|r\in\mathbb{R}, r>0\}$ ist eine Untergruppe von $(\mathbb{R}\setminus\{0\},\cdot)$.

C) Ringe

(15.16) DEF: R sei eine Menge mit zwei Verknüpfungen $+$ und $\cdot$. (Diese werden Addition bzw. Multiplikation auf R genannt).

$(R,+,\cdot)$ heißt ein **Ring**, wenn gilt:

R$_1$) $(R,+)$ ist eine abelsche Gruppe

R$_2$) Die Verknüpfung $\cdot$ ist assoziativ und besitzt ein neutrales Element

R$_3$) Es gelten die **Distributivgesetze**: $\forall\, a,b,c\in R$:

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

Ist zusätzlich die Verknüpfung $\cdot$ kommutativ, so heißt $(R,+,\cdot)$ ein **kommutativer Ring.**

Bezeichnungen: **a)** $0_R\in R$ neutrales Element bzgl. $+$ (Nullelement)

b) $1_R\in R$ neutrales Element bzgl. $\cdot$ (Einselement)

c) $-r$ inverses Element von $r\in R$ bzgl $+$ (negatives Element von r)

d) $r-s := r+(-s)$ (Differenz von r und s)

e) In R$_3$) vereinfacht man die Bezeichnungsweise zu
$a\cdot(b+c) = a\cdot b + a\cdot c$ ("Punktrechnung geht vor Strichrechnung")
und häufig (wie gewohnt) zu $a(b+c) = ab+ac$.

(15.17) Beispiele: für kommutative Ringe:

a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

b) $(\mathbb{R}^n, +, \cdot)$ mit den Verknüpfungen: $(x_i) + (y_i) := (x_i + y_i)$, $(x_i) \cdot (y_i) := (x_i \cdot y_i)$

c) $\emptyset \neq M \subseteq \mathbb{R}$: $\operatorname{Abb}(M, \mathbb{R})$ mit den Verknüpfungen:
$\forall\, x \in M$: $(f + g)(x) := f(x) + g(x)$, $(f \cdot g)(x) := f(x) \cdot g(x)$
(Man sagt: Die Verknüpfungen sind "argumentweise" definiert), Beweis s. Aufgabe 11a)

d) $(\mathbb{Z}_n, \oplus, \odot)$ für alle $n \in \mathbb{N}, n \geq 1$.

(15.18) SATZ: $(R, +, \cdot)$ sei ein Ring. Dann gelten die folgenden Rechenregeln für beliebige $r, s \in R$:

a) $-(-r) = r$ **b)** $-(r + s) = -r - s$

c) $r \cdot 0_R = 0_R = 0_R \cdot r$

d) $r \cdot (-s) = -(r \cdot s) = (-r) \cdot s$

e) $(-r) \cdot (-s) = r \cdot s \quad s \in R)$.

(15.19) DEF: $(R, +, \cdot)$ sei ein Ring. Eine Teilmenge $U \subseteq R$ heißt ein **Unterring** von R, wenn gilt:

UR$_1$) $\forall\, a, b \in U : a - b \in U$

UR$_2$) $\forall\, a, b \in U : a \cdot b \in U$

UR$_3$) $1_R \in U$.

(15.20) BEM: **a)** Ein Unterring $U \subseteq R$ ist für sich betrachtet wieder ein Ring. Seine Verknüpfungen sind die Einschränkungen der Verknüpfungen des Ringes R auf U .

b) $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$ und auch von $\mathbb{R}$.

c) $U := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ ist ein Unterring von $\mathbb{R}$.

c) Für $k \in \mathbb{Z} \setminus \{-1, 1\}$ ist $\mathbb{Z}k$ kein Unterring von $\mathbb{Z}$.

(15.21) SATZ: Sind R und S Ringe, so ist auch das kartesische Produkt $R \times S$ ein Ring mit den "komponentenweise" erklärten Verknüpfungen
$(r, s) + (r', s') := (r + r', s + s')$, $(r, s) \cdot (r', s') := (r \cdot r', s \cdot s')$

(15.22) DEF: $(R, +, \cdot)$ sei ein Ring. Ein Element $r \in R$ heißt **Einheit in** R, wenn r invertierbar bzgl. $\cdot$ ist. Das Inverse einer Einheit $r \in R$ wird mit r^{-1} bezeichnet. Die Menge aller Einheiten in einem Ring R werde mit $R^\star$ bezeichnet.

(15.23) Beispiele: **a)** $\mathbb{Z}^\star = \{1, -1\}$

b) $\mathbb{Q}^\star = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\star = \mathbb{R} \setminus \{0\}$

c) R sei ein Ring. Dann ist $(R^\star, \cdot)$ eine Gruppe (s. Aufgabe 8), insbesondere gilt also $1_R \in R^\star$

d) Im Falle $1_R \neq 0_R$ kann 0_R keine Einheit in einem Ring R sein.

(15.24) DEF: **a)** Ein Ring R heißt **nullteilerfrei** wenn gilt:

$$\forall\, x, y \in R \,:\, x \cdot y = 0_R \quad \Longrightarrow \quad x = 0_R \;\vee\; y = 0_R \,.$$

b) Ein kommutativer nullteilerfreier Ring R mit $1_R \neq 0_R$ heißt ein **Integritätsbereich (IB)**.

(15.25) Beispiele: **a)** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind Integritätsbereiche.

b) Die Ringe $\mathbb{R} \times \mathbb{R}$ und $(\mathbb{Z}_4, \oplus, \odot)$ sind keine Integritätsbereiche.

(15.26) DEF: R sei ein Ring. Eine nichtleere Teilmenge $I \subseteq R$ heißt ein **Ideal** von R, wenn gilt:

1) $\forall\, a, b \in I \,:\, a - b \in I$

2) $\forall\, x \in R \,\forall\, a \in I \,:\, ax \in I \wedge xa \in I$.

(15.27) BEM: In einem kommutaiven Ring R ist $Ra := \{ra \,|\, r \in R\}$ für jedes $a \in R$ ein Ideal. $Ra =: (a)$ heißt das von a erzeugte **Hauptideal**.

(15.28) SATZ: In dem Ring $\mathbb{Z}$ ist jedes Ideal ein Hauptideal.

(15.29) DEF: Ein R heißt ein **Hauptidealbereich (HIB)**, wenn gilt:

1) R ist ein Integritätsbereich

2) Jedes Ideal von R ist ein Hauptideal .

Beispiel: $\mathbb{Z}$ ist ein HIB .