§ 2. Der Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen

Auf der Menge $\mathbb{Z}$ der ganzen Zahlen gibt es zwei Rechenoperationen: die Addition und die Multiplikation. Dafür gelten die folgenden grundlegenden Rechenregeln, aus denen sich die weiteren Regeln herleiten lassen.

(2.1) Rechenregeln in $(\mathbb{Z}, +, \cdot)$

a) Für die Addition gilt:

0) Für alle $a, b \in \mathbb{Z}$ gilt: $a + b \in \mathbb{Z}$

1) Für alle $a, b \in \mathbb{Z}$ gilt: $a + b = b + a$ (**Kommutativgesetz der Addition**)

2) Für alle $a, b, c \in \mathbb{Z}$ gilt: $(a + b) + c = a + (b + c)$
(**Assoziativgesetz der Addition**)

3) Für alle $a \in \mathbb{Z}$ gilt: $a + 0 = a$ (**Existenz eines Nullelementes**)

4) Zu jedem $a \in \mathbb{Z}$ gibt es ein $b \in \mathbb{Z}$ mit $a + b = 0$ Bezeichnung: $b =: -a$
(**Zu jeder Zahl existiert eine negative Zahl**)

b) Für die Multiplikation gilt:

0) Für alle $a, b \in \mathbb{Z}$ gilt: $a \cdot b \in \mathbb{Z}$

1) Für alle $a, b \in \mathbb{Z}$ gilt: $a \cdot b = b \cdot a$ (**Kommutativgesetz der Multiplikation**)

2) Für alle $a, b, c \in \mathbb{Z}$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(**Assoziativgesetz der Multiplikation**)

3) Für alle $a \in \mathbb{Z}$ gilt: $1 \cdot a = a$ (**Existenz eines Einselementes**)

c) **Distributivgesetz** Für alle $a, b, c \in \mathbb{Z}$ gilt: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Fazit: $(\mathbb{Z}, +)$ ist eine **abelsche Gruppe**
$(\mathbb{Z}, +, \cdot)$ ist ein **kommutativer Ring** mit 0 als Nullement und 1 als Einselement .

(2.2) BEM: a) Wie in jedem Ring gilt $a \cdot 0 = 0 = 0 \cdot a$ $(\forall\, a \in \mathbb{Z})$.

b) Der Ring $\mathbb{Z}$ ist **nullteilerfrei**, d.h. $\forall\, a, b \in \mathbb{Z} \, : \, a \cdot b = 0 \implies (a = 0 \vee b = 0)$.

c) In $\mathbb{Z}$ gelten die folgenden Kürzungsregeln $(a, b, c \in \mathbb{Z})$:

i) $a + c = b + c \implies a = b$

ii) $a \cdot c = b \cdot c$ und $\underline{c \neq 0} \implies a = b$

(2.3) BEM: Addition und Multiplikation auf $\mathbb{Z}$ sind mit der $\leq$–Beziehung **verträglich**, d.h. es gilt für alle $a, b \in \mathbb{Z}$

a) $a \leq b \implies a + c \leq b + c$ für alle $c \in \mathbb{Z}$

b) $a \leq b \implies a \cdot c \leq b \cdot c$ für alle $c \in \mathbb{Z}$ mit $\mathbf{c \geq 0}$.

Damit ist $(\mathbb{Z}, +, \cdot, \leq)$ ein **angeordneter Ring**.

(2.4) SATZ: Division mit Rest

Zu jeder ganzen Zahl $a \in \mathbb{Z}$ und jeder natürlichen Zahl $n \geq 1$ gibt es eindeutig bestimmte ganze Zahlen q und r mit folgenden Eigenschaften:

$$a \;=\; qn + r \quad \text{und} \quad 0 \leq r < n\,.$$

Dabei heißt q der **Quotient bei Division von** a **durch** n und r der **Rest bei Division von** a **durch** n.

Bezeichnungen: $\quad q = a \text{ div } n \;\;,\;\; r = a \text{ mod } n\,.$

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

I$_1$) $0 \in I$

I$_2$) $\forall\, a, b \in I \,:\, a - b \in I$

I$_3$) $\forall\, a \in I\, \forall\, r \in R \,:\, ra \in I\,.$

(2.6) BEM: **a)** Ist $I \subseteq R$ ein Ideal, so ist I eine Untergruppe von $(R, +)$.

b) Für jedes $a \in R$ ist $Ra := \{\, ra \,|\, r \in R\,\} =: (a)$ ein Ideal in R, das sog. von a erzeugte **Hauptideal** von R.

c) Sind I und J Ideale in R, so ist auch $I + J := \{a + b \,|\, a \in I, b \in J\}$ ein Ideal in R, das sog. **Summenideal** von I und J.

d) Sind I und J Ideale in R, so ist auch $I \cap J$ ein Ideal.

(2.7) DEF:

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

b) Ein IB R, in dem jedes Ideal ein Hauptideal ist, heißt ein **Hauptidealbereich (HIB)**.

(2.8) SATZ: Für eine Teilmenge $I \subseteq \mathbb{Z}$ sind folgende Aussagen äquivalent:

a) I ist ein Ideal von $\mathbb{Z}$

b) I ist eine Untergruppe von $(\mathbb{Z}, +)$

c) Es gibt genau ein $n \in \mathbb{N}_0$ mit $I = (n)$.

(2.9) KOROLLAR: $\mathbb{Z}$ ist ein HIB.

(2.10) BEISPIELE: **a)** Jeder Körper ist ein HIB.

b) Ist K ein Körper, so ist der Polynomring $K[T]$ in einer Unbestimmten T über K ein HIB.