1. Der Ring $\mathbb{Z}$

$\mathbb{N} = \{1, 2, ...\}$

$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ ist bzgl. der Addition und Multiplikation ein Ring

Wiederholung für Ring:

R1: $\mathbb{Z}(+)$ ist eine abelsche Gruppe (0=neutrales Element)

Schreibweise: $a - b := a + (-b)$

R2: Die Multiplikation ist assotiativ

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

und es existiert ein neutrales Element (=1)

R3: Es gelten die Distributivgesetze

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

Zusätzlich: - $\mathbb{Z}$ ist kommutativ $(ab = ba)$

- $\mathbb{Z}$ ist **nullteilerfrei** $(a, b \neq 0 \Rightarrow a \cdot b \neq 0)$

Bezeichnung: Für $a \in \mathbb{Z}$ ist $\langle a \rangle := \{i \cdot a \mid i \in \mathbb{Z}\} = \{..., -2a, -a, 0, a, 2a, ...\}$
die Menge aller Vielfachen von a.

$U := \langle a \rangle$

1.1. a) U ist Untergruppe von $\mathbb{Z}(+)$

b) $u \in U, z \in \mathbb{Z} \Rightarrow z \cdot u \in U$ (d.h. U ist **Ideal** des Rings $\mathbb{Z}$)

Beweis: $u = ia,\ w = ja \in U$

$u + w = (i + j)a \in U$

$-u = (-i)a \in U$

$z \cdot u = z(ia) = (zi)a \in U$

Bezeichnung: Sei U eine Untergruppe von $\mathbb{Z}(+)$

Sei $U \neq \{0\}$ $(\neq 0)$

Dann ist $U \cap \mathbb{N} \neq \{0\}$

$\operatorname{Min} U := \min(U \cap \mathbb{N})$ (kleinste positive Zahl aus U)

Ist $U = 0$, so sei $\operatorname{Min} U := 0$

1.2. Satz

Sei U Untergruppe von $\mathbb{Z}(+)$ und sei $m := \operatorname{Min} U$

Dann ist $U = \langle m \rangle$

Beweis: $\text{Œ} U \neq 0$

$m \in U \Rightarrow ..., -2m, -m, 0, m, 2m, ...$

$\Rightarrow \langle m \rangle \subseteq U$

Sei $0 \neq u \in U$

Teile u durch m

$u = i \cdot m + r,\ r \in \{0,1,...,m-1\},\ i \in \mathbb{Z}$

$r = \underbrace{u}_{\in U} - \underbrace{i \cdot m}_{\in U} \Rightarrow r \in U$

$\underset{\text{von } m}{\overset{\text{Minimalität}}{\Rightarrow}} r = 0$ (weil m kleinste Zahl und $r<m$ sein soll)

Sei $n \in \mathbb{N},\ n > 1$

Bezeichnung: $\mathbb{Z}_n := \{0,1,...,n-1\} \subseteq \mathbb{Z}\ \ (= \mathbb{N}_0)$

Division mit Rest: Zu $a \in \mathbb{Z}$ existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$:

$a = q \cdot n + r,\ r \in \mathbb{Z}_n$

$a = q \cdot n + r = q'n + r' = qn + r'$

$qn - q'n = r' - r$

$\underbrace{(q - q')}_{=0} n = r - r'$

$\Rightarrow q = q'$

Bezeichnung: $\rho_n a := r$ Rest modulo n

$(\rho =)\ \rho_n : \mathbb{Z} \to \mathbb{Z}_n$ mit $a \to \rho_n a$ „Restabbildung modulo n“

1.3. a) $\rho a = 0 \Leftrightarrow a \in \langle n \rangle$

b) $\rho a = a \Leftrightarrow a \in \mathbb{Z}_n$

c) $\rho(a+b) = \rho(\rho a + \rho b)$

d) $\rho(a \cdot b) = \rho((\rho a) \cdot (\rho b))$

Beispiel für c): $a = 13,\ b = 9,\ n = 5$

$\rho(a+b) = \rho(13+9) = 2$

$\rho(a) = \rho(13) = 3,\ \rho(b) = \rho(9) = 4$

$\rho(\rho(a) + \rho(b)) = \rho(3+4) = 2$

Beweis für d): $a = qn + r,\ r = \rho a$

$b = pn + s,\ s = \rho b$

$a \cdot b = (qpn + qs + pr) \cdot n + \underbrace{rs}_{= ln + t}$

$= n(qpn + qs + pr + l) + t$

Zwischenbemerkung: Für $a,b,n \in \mathbb{Z}$

$$a \equiv b \pmod{n} \overset{\text{def.}}{\Leftrightarrow} \rho_n a = \rho_n b$$
$$\Leftrightarrow a - b \in \langle n \rangle$$
$$(\Leftrightarrow n \text{ teilt } a-b)$$
$$\equiv \text{def. Äquivalenzrelation auf } \mathbb{Z}$$
$$\text{Konkruenzklassen}$$

Äquvalenzklasse $[a] = \{b \in \mathbb{Z} \mid \rho a = \rho b\}$

$\mathbb{Z}_n$ ist Repräsentantensystem dieser Äquivalenzrelation

$\rho = \rho_n$ überträgt die Ringstruktur von $\mathbb{Z}$ auf $\mathbb{Z}_n$:

Für $r,s,t \in \mathbb{Z}_n$ $(r = \rho r,\ s = \rho s,\ t = \rho t)$

$$r +_n s \overset{\text{def.}}{=} \rho(r+s) \qquad (\text{Ausgesprochen}: + \bmod n)$$
$$r \cdot_n s \overset{\text{def.}}{=} \rho(r \cdot s)$$

1.4. Bezüglich dieser Verknüpfung ist $\mathbb{Z}_n$ ein kommutativer Ring mit Nullelement $0 \in \mathbb{Z}_n$ und Einselement $1 \in \mathbb{Z}_n$

Beweis: $0,1$ sind richtig (trivial)
Addition und Multiplikation ist kommutativ
$r +_n (n-r) = 0$ in $\mathbb{Z}_n$

Assoziativgesetz
Addition:

$$r +_n (s +_n t) = \rho(r + \rho(s+t)) =$$
$$= \rho(\rho r + \rho(s+t)) = \rho(r + (s+t)) =$$
$$= \rho((r+s)+t) = \rho(\rho(r+s)+t) =$$
$$= (r +_n s) +_n t$$

Multiplikation:

$$r \cdot_n \underbrace{(s \cdot_n t)}_{\rho(s \cdot t)} = \rho(r \cdot \rho(s \cdot t)) = \rho(\rho r \cdot \rho(s \cdot t)) = \rho(r \cdot (s \cdot t))$$
$$= \rho((r \cdot s) \cdot t) = \ldots = (r \cdot_n s) \cdot_n t$$

Beispiel: $n = 2,\ \mathbb{Z}_n = \{0,1\}$

$$\rho(1+1) = \rho(2) = 0$$