1.2.6 Zyklische Gruppen

Definition 1 Eine Gruppe $(C, \circ)$ heißt *zyklisch*, wenn es ein Element $c \in C$ gibt, sodass $C = \{c^k \mid k \in \mathbb{Z}\}$ gilt, d. h. wenn C genau aus den Potenzen (oder in additiver Schreibweise aus den Vielfachen $C = \{k \cdot c \mid k \in \mathbb{Z}\}$) eines einzigen Elementes c besteht. Man nennt dann c ein *erzeugendes Element* von C.

Beispiel 15 Die ganzen Zahlen $(\mathbb{Z}, +)$ bilden mit der Addition eine zyklische Gruppe. Die beiden erzeugenden Elemente sind 1 und -1, da $\mathbb{Z} = \{k \cdot 1 \mid k \in Z\} = \{k \cdot (-1) \mid k \in Z\}$ gilt.

Satz 11 *Jede Untergruppe $(U, +) \leq (\mathbb{Z}, +)$ hat die Form $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$, wobei $n \in \mathbb{N}_0$ und entweder $n = 0$ oder n die kleinste natürliche Zahl in U ist.*

BEWEIS Im Fall $U = \{0\}$ gilt $n = 0$. Daher gelte fortan $U \neq \{0\}$. Da mit jedem Element $u \in U$ auch das additiv Inverse $-u \in U$ ist, gibt es positive und negative Zahlen in U und daher auch eine kleinste natürliche Zahl $n \in U$. Es sei $m \in U$ eine beliebige Zahl aus U. Dann lässt sich m durch Division mit Rest in $m = nq + r$ mit $0 \leq r < n$ zerlegen. Da nq und m Elemente von U sind, ist wegen der Abgeschlossenheit von Gruppen auch ihre Differenz $m - nq = r$ ein Element von U. Da aber $r < n$ gilt und n die kleinste natürliche Zahl in U ist, gilt $r = 0$. Also ist $m = nq$ und daher $U = n\mathbb{Z}$.

Beispiel 16 Neben der Untergruppe $\{0\}$ enthält $(\mathbb{Z}, +)$ also ausschließlich Untergruppen, die aus ganzzahligen Vielfachen einer natürlichen Zahl n bestehen, also z. B. die Gruppe $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, die aus den Vielfachen von $n = 3$ besteht.

Satz 12 *Es sei $(n\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$. Dann ist $n\mathbb{Z}$ ein Normalteiler von $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ besteht aus den Nebenklassen*

$$a + n\mathbb{Z} = \{a + n \cdot z \mid z \in \mathbb{Z}\}$$

für $a \in \mathbb{Z}$. Man nennt $\mathbb{Z}/n\mathbb{Z}$ auch die Menge der Restklassen modulo n und schreibt abkürzend $\mathbb{Z}_n$ für $\mathbb{Z}/n\mathbb{Z}$ und $\overline{a}$ für $a + n\mathbb{Z}$. Mit der Addition $\overline{a} \oplus \overline{b} := \overline{a + b}$ ist $\mathbb{Z}_n$ ein zyklische Gruppe der Ordnung n.

BEWEIS Da $(\mathbb{Z}, +)$ kommutativ ist, ist nach Lemma 2 jede Untergruppe von $(\mathbb{Z}, +)$ ein Normalteiler. Die additive Struktur von $(n\mathbb{Z}, +)$ überträgt sich nach Satz 10 auf $(\mathbb{Z}_n, \oplus)$. Insbesondere ist dadurch $(\mathbb{Z}_n, \oplus)$ eine zyklische Gruppe mit $\overline{1}$ als einem erzeugenden Element. Nach dem Beweis zu Satz 11 besteht $\mathbb{Z}_n$ aus den Nebenklassen $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$. Daher hat $\mathbb{Z}_n$ die Ordnung n.

Beispiel 17 $\mathbb{Z}_4$ besteht aus den folgenden Nebenklassen:

$$\overline{0} \;=\; \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$

$$\begin{aligned}\overline{1} &= \{\ldots,-7,-3,1,5,9,\ldots\}\\ \overline{2} &= \{\ldots,-6,-2,2,6,10,\ldots\}\\ \overline{3} &= \{\ldots,-5,-1,3,7,11,\ldots\}\end{aligned}$$

Für $\mathbb{Z}_4$ sieht die Verknüpfungstafel bezüglich $\oplus$ folgendermaßen aus:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Tabelle 1.10: Verknüpfungstafel von $(\mathbb{Z}_4, \oplus)$

Satz 13 *Die Gruppe $(\mathbb{Z}_n, \oplus)$ besitzt für jeden Teiler $d \in \mathbb{N}$ von n genau eine Untergruppe U der Ordnung d. Dann ist $\frac{\overline{n}}{d}$ ein erzeugendes Element (aber nicht notwendigerweise das einzige erzeugende Element) von U (da d eine Teiler von n ist, ist $\frac{n}{d}$ stets eine natürliche Zahl).*

BEWEIS Man betrachte die Vielfachen $1 \cdot \frac{n}{d}, 2 \cdot \frac{n}{d}, \ldots, (d-1) \cdot \frac{n}{d}, d \cdot \frac{n}{d} = n$. Dann sind die Vielfachen $1 \cdot \frac{n}{d}, 2 \cdot \frac{n}{d}, \ldots, (d-1) \cdot \frac{n}{d}$ alle kleiner als n und daher sind alle Vielfachen $1 \cdot \frac{\overline{n}}{d}, 2 \cdot \frac{\overline{n}}{d}, \ldots, (d-1) \cdot \frac{\overline{n}}{d}$ ungleich $\overline{0}$. Andererseits ist $d \cdot \frac{\overline{n}}{d}$ das kleinste Vielfache, das mit $\overline{0}$ identisch ist. Also ist $\frac{\overline{n}}{d}$ tatsächlich ein erzeugendes Element von U und $|U| = d$.

Nun ist noch zu zeigen, dass U die einzige Untergruppe von $\mathbb{Z}_n$ der Ordnung d ist. Es sei V eine weitere Untergruppe von $\mathbb{Z}_n$ mit $|V| = d$. Da V als Untergruppe einer zyklischen Gruppe ebenfalls zyklisch ist, hat V ein erzeugendes Element t. Nach Korollar 2 ist dann $d \cdot \overline{t} = \overline{0}$. Also ist n ein Teiler von $t \cdot d$. Umgekehrt ist nach Lemma 1 aber auch $\frac{n}{d} \mid t$, also ist $\overline{t}$ ein Element der von $\frac{\overline{n}}{d}$ erzeugten Untergruppe U. Daher ist $V \leq U$. Da aber $|V| = |U| = d$ ist, ist $V = U$.

Beispiel 18 In der folgenden Abbildung wird $\mathbb{Z}_{10}$ veranschaulicht.

Füllt man das Arbeitsblatt aus, so kann man aus ihm sämtliche Untergruppen von $(\mathbb{Z}_{10}, \oplus)$ einschließlich ihrer erzeugenden Elemente ablesen.

Satz 14 *Es sei $(C, \circ)$ eine zyklische Gruppe.*

1) Ist C unendlich, so ist $(C, \circ)$ isomorph zu $(\mathbb{Z}, +)$.

2) Hat C die Ordnung n, so ist $(C, \circ)$ isomorph zu $(\mathbb{Z}_n, \oplus)$.

BEWEIS Es sei c ein erzeugendes Element von $(C, \circ)$. Man betrachte die Abbildung $\varphi : \mathbb{Z} \to C : k \mapsto c^k$. Dann gilt $\varphi k + l = c^{k+l} = c^k \circ c^l = \varphi(k) \circ \varphi(l)$ nach Definition der Potenzen für Gruppenelemente für alle $k, l \in \mathbb{Z}$. Daher ist φ ein surjektiver Homomorphismus. Nach Satz 11 ist $Kern(\varphi) = \{0\}$ oder $Kern(\varphi) = n\mathbb{Z}$ für ein passendes

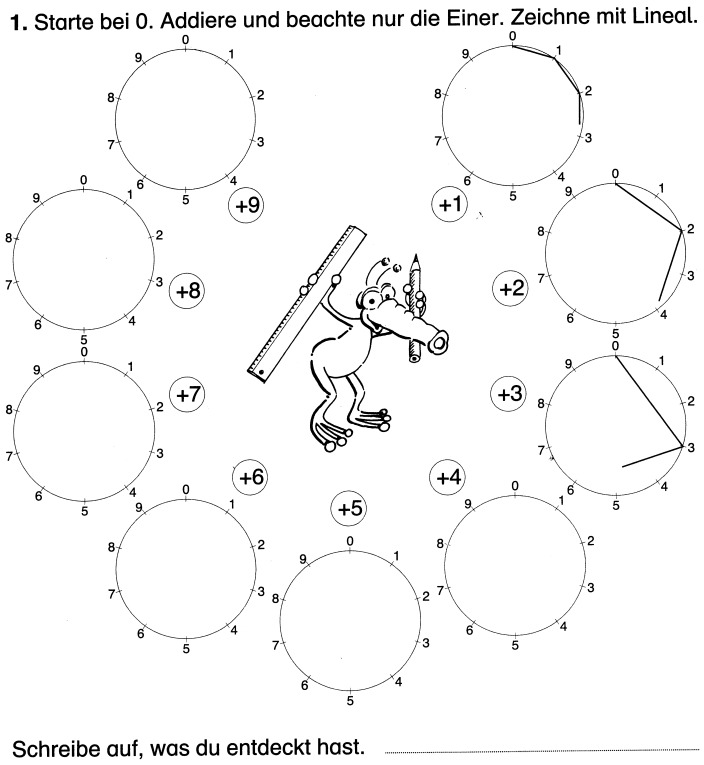

Abbildung 1.3: Untergruppen von $(\mathbb{Z}_{10}, \oplus)$ und ihre erzeugenden Elemente

$n \in \mathbb{N}$. Falls $Kern(\varphi) = \{0\}$ ist, so ist φ nach Satz 7 injektiv, also bijektiv und daher ein Isomorphismus, d. h. es gilt $(C, \circ) \cong (\mathbb{Z}, +)$. Falls $Kern(\varphi) = n\mathbb{Z}$ ist, so gilt nach Satz 10 $(C, \circ) \cong (\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, \oplus)$ mit $|C| = n$.