5. Zyklische Gruppen

Definition: Eine Gruppe G heißt zyklisch, wenn Sie von einem ihrer Elemente erzeugt wird, d.h. wenn $\exists a \in G : G = \langle a \rangle$.

Bemerkung: Wegen Satz 15 gilt offenbar folgendes: Eine endliche Gruppe G der Ordnung $|G| = m$ ist genau dann zyklisch, wenn sie ein Element der Ordnung m enthält.

Beispiele: 1) $(\mathbb{Z}, +)$ ist zyklisch, da $\mathbb{Z} = \langle +1 \rangle = \langle -1 \rangle$.
2) $(m\mathbb{Z}, +)$ ist zyklisch, da $m\mathbb{Z} = \langle m \rangle = \langle -m \rangle$.
3) Für jedes $m \in \mathbb{N} \setminus \{0, 1\}$ ist $(\mathbb{Z}_m, +)$ zyklisch, da $\mathbb{Z}_m = \langle \overline{1} \rangle$.
4) Die einelementige Gruppe $\{e\}$ ist zyklisch, da $\{e\} = \langle e \rangle$.
5) Für jedes $m \in \mathbb{N} \setminus \{0, 1\}$ ist die Gruppe der m-ten Einheitswurzeln zyklisch, da sie von $\zeta = e^{2\pi i/m}$ erzeugt wird.
6) Die Gruppe $(\mathbb{Z}_9^*, \cdot)$ ist zyklisch, da $\mathbb{Z}_9^* = \langle \overline{2} \rangle = \langle \overline{5} \rangle$.
7) Die Symmetriegruppe $\{I, R, S_1, S_2\}$ des Rechtecks ist nicht zyklisch, da sie Ordnung 4 hat, aber nur Elemente der Ordnung 1 und 2 enthält.
8) Die Gruppe $(\mathbb{Z}_8^*, \cdot)$ ist nicht zyklisch, da sie Ordnung 4 hat, aber nur Elemente der Ordnung 1 und 2 enthält.
9) Die Gruppe $(\mathbb{R}, +)$ ist nicht zyklisch, da eine zyklische Gruppe nur abzählbar viele Elemente enthält.

Bemerkung: Ein von Gauß bewiesener Satz aus der Zahlentheorie besagt folgendes: Die prime Restklassengruppe $(\mathbb{Z}_m^*, \cdot)$ ist (für $m \geq 2$) genau dann zyklisch, wenn

$$m \in \{2, 4\} \cup \{p^\alpha \mid p \geq 3 \text{ ist Primzahl}, \alpha \geq 1\} \cup \{2p^\alpha \mid p \geq 3 \text{ ist Primzahl}, \alpha \geq 1\}.$$

In der elementaren Zahlentheorie wird dieser Satz meistens so formuliert, dass für genau diese $m \geq 2$ eine Primitivwurzel existiert. Diese ist aber nichts anderes als ein erzeugendes Element von $\mathbb{Z}_m^*$.

Satz 34: Jede zyklische Gruppe ist abelsch.

Beweis: Ist die Gruppe G zyklisch, so gibt es ein $a \in G$ sodass $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Sind $x, y \in G$, so $\exists k, \ell \in \mathbb{Z} : x = a^k, y = a^\ell$ und daher

$$xy = a^k a^\ell = a^{k+\ell} = a^{\ell+k} = a^\ell a^k = yx.$$

Satz 35: Es sei G eine zyklische Gruppe.
(i) Ist H eine Gruppe und $\varphi : G \to H$ ein Homomorphismus, so ist $\operatorname{Im} \varphi$ eine zyklische Gruppe.
(ii) Ist $H \leq G$, so ist H eine zyklische Gruppe.

Beweis: Es sei $G = \langle a \rangle$ für $a \in G$.
(i) Folgt aus

$$\operatorname{Im}\varphi = \varphi(G) = \varphi\big(\{a^n \mid n \in \mathbb{Z}\}\big) = \{\varphi(a^n) \mid n \in \mathbb{Z}\} = \{\varphi(a)^n \mid n \in \mathbb{Z}\} = \langle \varphi(a) \rangle.$$

(ii) Ist $H = \{e\}$, so ist $H = \langle e \rangle$ zyklisch. Wenn $H \neq \{e\}$, so $\exists n \in \mathbb{Z} \setminus \{0\} : a^n \in H \setminus \{e\}$. Da dann auch $a^{|n|} \in H \setminus \{e\}$, kann man o.B.d.A. $n > 0$ voraussetzen. Wir wählen nun $m > 0$ minimal mit dieser Eigenschaft (d.h. $m = \min\{n \in \mathbb{Z} \mid n > 0, a^n \in H \setminus \{e\}\}$).
Wir behaupten nun $H = \langle a^m \rangle$. Aus $a^m \in H$ folgt sofort $\langle a^m \rangle \subseteq H$. Ist $a^k \in H$, so sei $k = qm + r$, $0 \leq r < m$. Dann ist $(a^m)^q a^r = a^k \in H$ und daher $a^r = a^k (a^m)^{-q} \in H$. Da $r < m$ muss $r = 0$ gelten. Daher ist $a^k = (a^m)^q \in \langle a^m \rangle$, womit auch $H \subseteq \langle a^m \rangle$ gezeigt ist.

Bemerkung: Aus dem Beweis von Satz 35 (ii) folgt sofort die folgende Aussage: Ist $H \neq \{0\}$ eine Untergruppe von $(\mathbb{Z}, +)$ und $m = \min\{k \in \mathbb{Z} \mid k > 0, k \in H\}$, so ist $H = \langle m \rangle = m\mathbb{Z}$ (wobei wir $a = 1$ gewählt haben).

Satz 36: (i) Jede unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}, +)$.
(ii) Jede endliche zyklische Gruppe der Ordnung $m \geq 2$ ist isomorph zu $(\mathbb{Z}_m, +)$

Beweis: Es sei $a \in G$ derart dass $G = \langle a \rangle$. Die Abbildung $\varphi : \mathbb{Z} \to G$, $\varphi(k) = a^k$ ist ein Epimorphismus, da $\varphi(k + \ell) = a^{k+\ell} = a^k a^\ell = \varphi(k)\varphi(\ell)$ $\forall k, \ell \in \mathbb{Z}$ und φ trivialerweise surjektiv ist. Nach Lemma 26 (i) ist $\ker\varphi \leq \mathbb{Z}$. Da $(\mathbb{Z}, +)$ zyklisch ist, ist $\ker\varphi$ ebenfalls zyklisch (nach Satz 35 (ii)).
Falls $\ker\varphi = \{0\}$ ist φ nach Lemma 26 (ii) auch injektiv und daher ein Isomorphismus, also gilt $G \cong \mathbb{Z}$. Falls $\ker\varphi = \mathbb{Z}$, so ist $G \cong \mathbb{Z}/\ker\varphi = \mathbb{Z}/\mathbb{Z} \cong \{e\}$.
Falls $\{0\} \subsetneqq \ker\varphi \subsetneqq \mathbb{Z}$, so ist $\ker\varphi = n\mathbb{Z}$ (wobei $n = \min\{k \in \mathbb{Z} \mid k > 0, k \in \ker\varphi\} \geq 2$) und daher $G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Aus $m = |G| = |\mathbb{Z}_n| = n$ folgt $G \cong \mathbb{Z}_m$.

Satz 37: Es sei G eine zyklische Gruppe, die von $a \in G$ erzeugt wird, d.h. $G = \langle a \rangle$.
(i) Wenn G unendlich ist, sind a und a^{-1} die einzigen Erzeuger von G.
(ii) Wenn G endlich ist und Ordung $|G| = m$ besitzt, ist gilt

$$a^k \in G \text{ ist Erzeuger von } G \quad \Longleftrightarrow \quad \operatorname{ggT}(k, m) = 1.$$

Beweis: (i) Da

$$\langle a^{-1} \rangle = \{(a^{-1})^k \mid k \in \mathbb{Z}\} = \{a^{-k} \mid k \in \mathbb{Z}\} = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle,$$

ist a^{-1} ebenfalls Erzeuger. Da G unendlich ist, hat a unendliche Ordnung und $a^k \neq a^\ell$ für $k, \ell \in \mathbb{Z}$, $k \neq \ell$ nach Satz 14 (iii). Ist $k \in \mathbb{Z} \setminus \{+1, -1\}$, so ist $a \notin \langle a^k \rangle$ und a^k daher kein Erzeuger. (Wäre $a \in \langle a^k \rangle$, so würde es ein $\ell \in \mathbb{Z}$ mit der Eigenschaft $a = (a^k)^\ell = a^{k\ell}$ geben. Wegen Satz 14 (iii) würde daraus $k\ell = 1$ folgen. D.h. es würde $k \mid 1$ gelten, ein Widerspruch.)

(ii) Aus Satz 15 folgt $\operatorname{ord}(a) = m$.
($\Rightarrow$) Nach Voraussetzung ist $G = \langle a^k \rangle$. Daher gibt es ein $\ell \in \mathbb{Z}$ mit der Eigenschaft $a^{k\ell} = (a^k)^\ell = a$. Aus Satz 15 (iv) folgt $k\ell \equiv 1 \pmod{m}$, woraus, nach einem Satz aus der Zahlentheorie, $\operatorname{ggT}(k, m) = 1$ folgt.
($\Leftarrow$) Aus $\operatorname{ggT}(k, m) = 1$ folgt, nach einem Satz aus der Zahlentheorie, die Existenz von $x, y \in \mathbb{Z}$, sodass $kx + my = 1$. Wegen

$$(a^k)^x = (a^k)^x (a^m)^y = a^{kx+my} = a$$

ist $a \in \langle a^k \rangle$. Daraus folgt $G = \langle a \rangle \subseteq \langle a^k \rangle \subseteq G$ und somit $G = \langle a^k \rangle$.