1 Zyklische Gruppen

1.1 Beispiele

1. $(< (12 \dots n) >; \circ\ (1))$ ist eine zyklische Gruppe mit n Elementen.
2. $(\mathbb{Z}_2 \times \mathbb{Z}_2, \circ, (\bar{0}, \bar{0})$ ist keine zyklische Gruppe.
3. Jedes Element einer Gruppe baut eine zyklische Gruppe auf.
4. In S_6 betrachte man die von (123456) erzeugte Untergruppe

$$< (123456) >= \{(123456); (135)(246); (14)(25)(36); (153)(264); (165432); (1)\}$$

5. Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

1.2 Die Ordnung eines Elementes

Wird von einem Element s einer multiplikativen Gruppe $(G, \cdot, e)$ nur eine endliche Untergruppe $< s >$ in G erzeugt, so gibt es eine kleinste natürliche Zahl n, so dass $s^n = e$.
$< s >= \{s^1, s^2, \dots, s^{n-1}, s^n = e\}$. Diese Zahl n heißt Ordnung des Elementes $s \in G$.

$$\mathrm{ord} s = \min\{n \in \mathbb{N} : s^n = e\}$$

Wir notieren einen Spezialfall des 1. Sylowsatzes: (= Satz von Cauchy)
Sei $(G, \cdot, e)$ eine Gruppe mit $|G| = p^r \cdot m$, $p \in \mathbb{P};\ r, m \in \mathbb{N}$;
$(p, m) = 1$. Dann gibt es ein $g \in G$: $\mathrm{ord} g = p$.
Für die Ordnung von Potenzen von s gilt dann:

$$\forall k \in \mathbb{Z} : \mathrm{ord} s^k = \frac{\mathrm{ord} s}{\mathrm{ggT}(k, \mathrm{ord} s)}$$

und im Spezialfall:

$$< s >=< s^k > \iff \mathrm{ggT}(k, \mathrm{ord} s) = 1$$

Wir studieren eine n-elementige zyklische Gruppe und stellen fest, dass es genau $\varphi(n)$ verschiedene Elemente dieser Gruppe gibt, die die vollständige Gruppe zyklisch erzeugen können. Es lässt sich nun ein Satz formulieren, der uns über die Untergruppen und Untergruppenstruktur von endlichen zyklischen Gruppen exakt Auskunft gibt.

1.3 Satz über endliche zyklische Gruppen

Für die zyklische Gruppe $(G, \cdot, e)$ mit $|G| = n$ gilt:

1. Jede Untergruppe einer zyklischen endlichen Gruppe ist wieder eine zyklische endliche Gruppe. Die Ordnung der Untergruppe ist ein Teiler der Gruppenordnung.

   $$U \leq G \Rightarrow U =< s^k >,\ |U|/|G|$$

2. Zu jedem positiven Teiler d von n existiert genau eine Untergruppe U von G, deren Ordnung gerade d ist.

   $$\forall\ d \in \mathbb{N} \text{ mit } d/n\ \exists\ !\ U \leq G : |U| = d;\ U =< s^{\frac{n}{d}} >$$

Damit ist die Untergruppenstruktur für endliche zyklische Gruppen bereits vollständig durch die Primfaktorisierung der Gruppenordnung gegeben.