§ 10. Exkurs über endliche zyklische Gruppen

Im folgenden sei $(G, \cdot)$ eine multiplikativ geschriebene Gruppe mit dem neutralen Element 1.

(10.1) Für jedes $a \in G$ ist $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$ eine Untergruppe von G, die sog. **von a erzeugte zyklische Untergruppe von G**.

(10.2) Die Gruppe G heißt **zyklisch**, wenn es ein $a \in G$ gibt mit $G = \langle a \rangle$. a heißt dann ein **erzeugendes Element von G**.

(10.3) Zwei zyklische Gruppen dergleichen Ordnung sind isomorph.

(10.4) Die **Ordnung** eines Elementes $a \in G$ ist definiert durch $\operatorname{ord}(a) := |\langle a \rangle|$.

Im folgenden sei G eine endliche Gruppe der Ordnung n:

(10.5) Für alle $a \in G$ gilt $a^n = 1$.

(10.6) $\operatorname{ord}(a) = \min\{k \mid k \in \mathbb{N}, a^k = 1\}$.

(10.7) Im Falle $m = \operatorname{ord}(a)$ gilt:
a) $\langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\}$ **b)** $\forall\, k \in \mathbb{Z} : a^k = 1 \implies m \mid k$ **c)** $m \mid n$.

(10.8) Ist a ein erzeugendes Element der zyklischen Gruppe G, so ist a^k $(k \in \mathbb{Z})$ genau dann ein erzeugendes Element von G, wenn $\operatorname{ggT}(k, n) = 1$ gilt. Folglich besitzt eine zyklische Gruppe der Ordnung n genau $\varphi(n)$ erzeugende Elemente.

(10.9) In einer zyklischen Gruppe $G = \langle a \rangle$ der Ordnung n gibt es zu jedem positiven Teiler t der Gruppenordnung n genau eine Untergruppe von G, die die Ordnung t hat.

Beweisidee: Gilt $s \cdot t = n$, so ist a^s ein Element der Ordnung t, d.h. $|\langle a^s \rangle| = t$. $\langle a^s \rangle$ ist auch die einzige Untergruppe der Ordnung t.

(10.10) In einer endlichen zyklischen Gruppe gibt es höchstens ein Element der Ordnung 2.

(10.11) Sind G und H endliche Gruppen, so besitzt ein Element (a, b) aus der Produktgruppe $G \times H$ die Ordnung $\operatorname{kgV}(\operatorname{ord}(a), \operatorname{ord}(b))$.

(10.12) Ist $f : G \longrightarrow H$ ein surjektiver Gruppenhomomorphismus, so gilt:
G zyklisch $\implies$ H zyklisch.
Im Falle $G \cong H$ ist damit G genau dann zyklisch, wenn H zyklisch ist.

(10.13) Sind G und H endliche Gruppen, so ist die Produktgruppe $G \times H$ genau dann zyklisch, wenn beide Gruppen G und H zyklisch sind und ihre Ordnungen teilerfremd sind.

(10.14) Sind die natürlichen Zahlen m und n teilerfremd, so ist die Abbildung

$$f : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \quad , \quad [a]_{mn} \longmapsto ([a]_m, [a]_n)$$

ein Ringisomorphismus.

(10.15) Die Surjektivität der Abbildung f aus (10.14) hat die Gültigkeit des **Chinesischen Restsatzes** zur Folge: Sind m und n teilerfremde natürliche Zahlen, so gibt es zu beliebigen $a, b \in \mathbb{Z}$ ein $x \in \mathbb{Z}$ mit

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

(10.16) Isomorphe Ringe haben isomorphe Einheitengruppen. Insbesondere folgt

$$\mathbb{Z}_{mn}^\star \;\cong\; \mathbb{Z}_m^\star \times \mathbb{Z}_n^\star \,.$$

(10.17) Aus (10.16) folgt noch einmal die Multiplikativität der Eulerschen φ–Funktion:

$$\varphi(mn) \;=\; |\,\mathbb{Z}_{mn}^\star\,| \;=\; |\,\mathbb{Z}_m^\star \times \mathbb{Z}_n^\star\,| \;=\; |\,\mathbb{Z}_m^\star\,| \cdot |\,\mathbb{Z}_n^\star\,| \;=\; \varphi(m) \cdot \varphi(n)\,.$$

(10.18) G sei eine endliche abelsche Gruppe. Ferner seien $a, b \in G$ mit $\mathrm{ord}(a) = m$ und $\mathrm{ord}(b) = n$. Dann gilt: $\quad \mathrm{ggT}(m,n) = 1 \quad \Longrightarrow \quad \mathrm{ord}(ab) = mn\,.$

(10.19) G sei eine endliche abelsche Gruppe, und es sei

$$m := \max\{\mathrm{ord}(a) \,|\, a \in G\}\,.$$

Dann folgt $\quad \mathrm{ord}(a) \,|\, m \quad (\forall\, a \in G)\,.$

(10.20) Sei $p \in \mathbb{P}$. Ist dann K ein Körper mit p Elementen, so ist $(K^\star, \cdot)$ eine zyklische Gruppe.

(10.21) Der Beweis von (10.20) liefert das allgemeinere Ergebnis:
In einem beliebigen Körper K ist jede endliche Untergruppe von $(K^\star, \cdot)$ zyklisch.