5. Vorlesung, 25.10.2010

§1.3. Zyklische Gruppen

1.3.1 Def Eine Gruppe G heißt zyklisch, wenn es $x \in G$ gibt, so dass $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$.

1.3.2 Bsp. (i) $(\mathbb{Z}, +)$ wird von 1 oder -1 erzeugt

(ii) $m\mathbb{Z} < \mathbb{Z}$ ist von m oder $-m$ erzeugt

(iii) $\mathbb{Z}/m\mathbb{Z}$ wird von $\hat{1} = 1 + m\mathbb{Z}$ erzeugt

1.3.3 Satz Sei G zyklisch. Falls G unendlich, so $G \cong \mathbb{Z}$. Falls $\operatorname{ord} G = m$, so $G \cong \mathbb{Z}/m\mathbb{Z}$

Beweis Sei $G = \langle x \rangle \rightsquigarrow \varphi : \mathbb{Z} \to G$, $\varphi(n) = x^n$ ist ein surjektiver Homom. Kor. 1.2.9 $\rightsquigarrow G \cong \mathbb{Z}/\operatorname{Ker}\varphi$

$\operatorname{Ker}\varphi < G \overset{1.1.7(iii)}{\rightsquigarrow} \operatorname{Ker}\varphi = n\mathbb{Z}$, $n \in \mathbb{N}_0$.

G unendlich $\rightsquigarrow \operatorname{Ker}\varphi = \{0\} \rightsquigarrow G \cong \mathbb{Z}$

G endlich $\rightsquigarrow G \cong \mathbb{Z}/n\mathbb{Z}$ mit $n = m = \operatorname{ord} G$. ☐

1.3.4 Def. Sei G eine Gruppe, $a \in G$. Die Ordnung von a ist $\operatorname{Ord} a := \operatorname{Ord}\langle a \rangle \in \mathbb{N} \cup \{\infty\}$.

Es gilt $\operatorname{Ord} a = \min\{n \in \mathbb{N} : a^n = e\}$ falls $\operatorname{ord} a < \infty$.

Bsp. $e \in G$ hat Ord 1; jede Transp. $(ij) \in S_n$ hat Ord 2, $1 \in \mathbb{Z}$ hat Ord ∞, $\hat{1} \in \mathbb{Z}/m\mathbb{Z}$ hat Ord m.

1.3.5 Satz (kleiner Fermatscher Satz)
Sei G endliche Gruppe. Dann gilt $\operatorname{ord} a \mid \operatorname{ord} G$, insbes. $a^{\operatorname{ord} G} = e$. Es gilt $a^n = e \Leftrightarrow \operatorname{ord} a \mid n$

Beweis Satz von Lagrange $\rightsquigarrow \operatorname{ord}\langle a \rangle \mid \operatorname{ord} G$ also $\operatorname{ord} G = k \operatorname{ord} a \rightsquigarrow a^{\operatorname{ord} G} = (a^{\operatorname{ord} a})^k = e^k = e$.

Zweite Aussage: „$\Leftarrow$" klar „$\Rightarrow$": Sei $\varphi : \mathbb{Z} \to G$, $\varphi(n) = a^n$

$\Rightarrow \{n \in \mathbb{Z} : a^n = e\} = \ker\varphi < \mathbb{Z} \rightsquigarrow \exists n_0$ mit $\ker\varphi = n_0\mathbb{Z}$

und $\mathbb{Z}/n_0\mathbb{Z} = \mathbb{Z}/\ker\varphi \cong \langle a\rangle$ also $n_0 = \operatorname{ord} a$.

Insb. $\operatorname{ord} a = n_0 \mid n$ für alle $n \in \mathbb{Z}$ mit $a^n = e$. ▤

1.3.6 Korollar Sei $p = \operatorname{ord}(G)$ prim. Dann ist G zyklisch und $G \cong \mathbb{Z}/p\mathbb{Z}$ und jedes Elem $a \in G\setminus\{e\}$ erzeugt G.

Beweis $a \in G\setminus\{e\} \Rightarrow \operatorname{ord} a > 1 \overset{\operatorname{ord} a \mid p}{\Longrightarrow} \operatorname{ord} a = p \Rightarrow G = \langle a\rangle$.

1.3.7 Satz Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis Sei $H < G = \langle x\rangle$. Sei $\varphi: \mathbb{Z} \to G$, $\varphi(n) = x^n$

$\rightsquigarrow \varphi^{-1}(H) < \mathbb{Z} \rightsquigarrow \varphi^{-1}(H) = m\mathbb{Z} \overset{\varphi \text{ surj}}{\rightsquigarrow} H = \varphi(m\mathbb{Z})$

$= \langle \varphi(m)\rangle = \langle x^m\rangle$. ▤

1.3.8 Lemma Seien $a, b \in \mathbb{Z}$. Dann:

(i) $a\mathbb{Z} + b\mathbb{Z} := \{ax + by : x, y \in \mathbb{Z}\} = ggT(a,b)\,\mathbb{Z}$

(ii) $a\mathbb{Z} \cap b\mathbb{Z} = kgV(a,b)\,\mathbb{Z}$

Beweis $a\mathbb{Z} + b\mathbb{Z} < \mathbb{Z} \Rightarrow \exists d \in \mathbb{N}_0$ mit $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Es muss $d \neq 0$ ($a \in d\mathbb{Z}$ und $a \neq 0$). Es gilt $a, b \in d\mathbb{Z}$

$\Rightarrow d \mid a, d \mid b \Rightarrow d \mid ggT(a,b)$. Außerdem $\exists x, y$ mit

$d = ax + by \Rightarrow ggT(a,b) \mid d \Rightarrow d = ggT(a,b)$.

(ii) $\exists m \in \mathbb{N}_0$ mit $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Es muss $m \neq 0$, da sonst

$ab \in a\mathbb{Z} \cap b\mathbb{Z} = \{0\}$. Nun $m \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow a \mid m, b \mid m$

$\Rightarrow kgV(a,b) \mid m$. Aber $kgV(a,b) \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

$\Rightarrow m \mid kgV(a,b)$. Daher $m = kgV(a,b)$. ▤

1.3.9 Bemerkung Seien $a,b \in \mathbb{Z}$, nicht beide Null.

$ggT(a,b) := (a,b) := \max\{d \in \mathbb{N} : d|a,\ d|b\}$

(größter gemeinsamer Teiler)

Seien $a,b \in \mathbb{Z}$, keine Null. Setze

$kgV(a,b) := [a,b] := \min\{v \in \mathbb{N} : a|v,\ b|v\}$

(kleinstes gemeinsames Vielfaches)

Für $a,b \in \mathbb{Z}^*$ gilt

$$ab = ggT(a,b) \cdot kgV(a,b)$$

Beweis: $ab/ggT(a,b)$ ist ein Vielfaches von $a,b \rightsquigarrow kgV(a,b) \le \frac{ab}{ggT(a,b)}$

1.3.8 (i) $\rightsquigarrow \exists x,y \in \mathbb{Z}: ggT(a,b) = xa + yb \quad | \cdot kgV(a,b)$

$\Rightarrow ggT(a,b)\cdot kgV(a,b) = xa\,kgV(a,b) + yb\,kgV(a,b) \xrightarrow{a \text{ und } b \text{ teilen}}$

$\Rightarrow ab \mid ggT(a,b)\,kgV(a,b) \Rightarrow ab \le ggT(a,b)\,kgV(a,b)$.

1.3.10 Satz Sei $n \in \mathbb{N}$.

(i) Für $m \in \{0,1,\dots,n-1\}$ sei $d = ggT(m,n)$. Die von $\hat{m} = m + n\mathbb{Z}$ erzeugte UG in $\mathbb{Z}/n\mathbb{Z}$ ist $\langle \hat{m} \rangle = \{\hat{0}, \hat{m}, \dots, (\frac{n}{d}-1)\hat{m}\}$, insb. $ord(\hat{m}) = n/d$, $(\mathbb{Z}_n : \langle \hat{m} \rangle) = d$

(ii) Es gibt eine bijektive Korrespondenz zwischen $\{d : 1 \le d \le n-1,\ d|n\}$ und die UG von $\mathbb{Z}/n\mathbb{Z}$, $d \mapsto \langle \hat{d} \rangle$.

(iii) Eine Restklasse $\hat{m}$ erzeugt $\mathbb{Z}_n \Leftrightarrow ggT(m,n) = 1$.

Beweis (i) Sei $\varphi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\varphi(a) = a\cdot\hat{m}$. Dann $Im\varphi = \langle \hat{m} \rangle$ und $Ker\,\varphi = \frac{n}{d}\mathbb{Z}$; „$\supset$" gilt, denn $\frac{n}{d}\cdot\hat{m} = \widehat{\frac{nm}{d}} = \frac{m}{d}\cdot\hat{n} = \hat{0}$. Zu „$\subset$": sei $q \in Ker\,\varphi$, also $q\hat{m} = 0$ $\rightsquigarrow n \mid qm \rightsquigarrow \frac{n}{d} \mid q\frac{m}{d} \rightsquigarrow \frac{n}{d} \mid q$ weil $(\frac{n}{d}, \frac{m}{d}) = 1$.

Es folgt, dass $\langle \hat{m} \rangle = \operatorname{Im}\varphi \cong \mathbb{Z}/\frac{n}{d}\mathbb{Z}$ also $\operatorname{ord}(\hat{m}) = \frac{n}{d}$ und $\langle \hat{m} \rangle$ hat die gewünschte Form.
(ii) und (iii) folgen sofort aus (i). ▨

1.3.11 Def Sei $n \in \mathbb{N}$. Die Eulersche φ-Fkt. ist die Anzahl der zu n primen Restklassen, d.h.
$\varphi(n) = |\{\hat{m} \in \mathbb{Z}/n\mathbb{Z} : (m,n) = 1\}|$.

1.3.12 Lemma Die Gruppe $U(\mathbb{Z}/n\mathbb{Z}, \cdot)$ der bzgl. der Mult. invertierbaren Restklassen besteht aus $\{\hat{m} \in \mathbb{Z}/n\mathbb{Z} : (m,n) = 1\}$.

Beweis $\hat{m} \in \mathbb{Z}/n\mathbb{Z}$ invertierbar bzgl. Mult. $\Leftrightarrow \exists \hat{a} \in \mathbb{Z}/n\mathbb{Z}$ mit $\hat{a} \cdot \hat{m} = \hat{1}$. $\Leftrightarrow \exists a \in \mathbb{Z}$ $am \equiv 1 \pmod n$
$\Leftrightarrow \exists a, b \in \mathbb{Z}$ $am + bn = 1$ $\Leftrightarrow 1 = (m,n)$. ▨

1.3.13 Satz (Eulersche Satz)
Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $(a,n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod n$$

Beweis Ist $(a,n) = 1$, so ist $\hat{a} \in U(\mathbb{Z}/n\mathbb{Z}, \cdot)$.
Diese Gruppe hat Ordnung $\varphi(n)$ also Nach 1.2.4 (Lagrange) folgt $\hat{a}^{\varphi(n)} = \hat{1}$ in $\mathbb{Z}/n\mathbb{Z}$, äquiv. zur Behauptung. ▨

1.3.14 Satz (kleiner Fermatscher Satz)
Sei $p \in \mathbb{N}$ prim und $a \in \mathbb{N}$ mit $p \nmid a$. Dann gilt

$$a^{p-1} \equiv 1 \pmod p$$

Beweis Für p prim gilt $(a,p) = 1 \Leftrightarrow a \not\equiv 0 \pmod p$ ▨

Umformulierung von 1.3.14:

$$\forall a \in \mathbb{N} \quad a^p \equiv a \pmod p$$