

§1.6. Endliche abelsche Gruppen

6.1.1. Lemma Sei G endlich und abelsch, $\langle a \rangle \subset G$ zyklisch von maximaler Ordnung n . Sei $H' \subset G' := G/\langle a \rangle$ zyklisch. Dann gibt es $b \in \pi^{-1}(H') \subset G$ mit $\langle \pi(b) \rangle = H'$, $\text{ord}(b) = \text{ord} H'$.

Beweis Sei $\text{ord} H' = m$. Sei $c' \in H'$ ein Erzeuger, also $\text{ord}(c') = m$. Sei $c \in \pi^{-1}(c')$, also $\hat{c} = c'$. Dann gilt $\hat{c}^m = c'^m = \hat{e}$, daher $c^m \in \langle a \rangle$, somit $\exists s \in \mathbb{N}_0$ so dass $c^m = a^s$. Wir suchen ein Element b in der Klasse $\hat{c} = c\langle a \rangle$ mit $\text{ord}(b) = m$, insbesondere $b^m = e$.

(Kommentar: wäre s durch m teilbar, so könnte man $b = ca^{-s/m}$ setzen, und dann $b^m = c^m a^{-s} = e$. Weil wir apriori nicht wissen, dass $m|s$ verwenden wir den Satz über Division mit Rest.) Schreibe $s = qm + r$, $q \in \mathbb{N}_0$, $0 \leq r < m$. Setze $b := ca^{-q}$. Dann gilt (G abelsch):

$$b^m = c^m a^{-mq} = \underbrace{c^m a^{-s}}_{=e} a^r = a^r$$

Wir wissen, dass $m | \text{ord}(b)$, denn $b^l = e \Rightarrow c^l = \pi(b)^l = \pi(b^l) = e'$ also $m = \text{ord}(c') | l$. Es gilt

$$\text{ord}(a^r) = \text{ord}(b^m) = \frac{\text{ord}(b)}{\text{ggT}(m, \text{ord}(b))} = \frac{\text{ord}(b)}{m} \leq \frac{n}{m}$$

(nach der Wahl von n). Angenommen $r \geq 1$, so gilt

$$\text{ord}(a^r) = \frac{\text{ord}(a)}{\text{ggT}(r, \text{ord}(a))} = \frac{n}{\text{ggT}(r, n)} \geq \frac{n}{r}$$

da $\text{ggT}(r, n) \leq r$.

$\leadsto \frac{n}{r} \geq \frac{n}{r} \Rightarrow r \geq m$, Widerspruch zur $r < m$.

Es muss also $r=0 \leadsto b^m = e \leadsto \text{ord}(b) \mid m$

Da $m \mid \text{ord}(b)$ folgt $\text{ord}(b) = m$. Außerdem $\pi(b) = \pi(c) = c'$

$\leadsto \langle \pi(b) \rangle = H'$. $\square$

1.6.2 Satz Sei G endlich, abelsch. Dann ist G isomorph zu einem direkten Produkt $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$.

Beweis Induktion nach $\text{ord}(G)$. Fall $\text{ord}(G) = 1$ trivial.

Sei $\text{ord}(G) = k > 1$, und sei $A = \langle a \rangle$ eine zyklische UG von maximaler Ordnung, und $\pi: G \rightarrow G/A$.

Da $\text{ord}(G/A) < \text{ord}(G)$ gilt nach Induktionsvoraussetzung

$G/A \cong H'_1 \times \dots \times H'_r$ wobei H'_i zyklisch sind.

Lemma 1.6.1 $\leadsto \exists b_i \in \pi^{-1}(H'_i)$ mit $\text{ord}(b_i) = \text{ord}(H'_i)$

und $\langle \pi(b_i) \rangle = H'_i$. Setze $H := \langle \{b_1, \dots, b_r\} \rangle$.

Jedes Element $g \in G$ ist von der Form $g = h_1 \dots h_r a^u$

mit $h_i \in H_i = \pi^{-1}(H'_i) = \langle \pi(b_i) \rangle$. Weil G abelsch ist, folgt, dass $\exists v \in \mathbb{Z}: g = b_1^{n_1} \dots b_r^{n_r} a^v$.

Außerdem $H \cap A = \{e\}$. Ist $b = b_1^{n_1} \dots b_r^{n_r} \in A$, so gilt

$$\underbrace{\pi(b_1^{n_1})}_{\in H'_1} \dots \underbrace{\pi(b_r^{n_r})}_{\in H'_r} = e \in G/A = H'_1 \times \dots \times H'_r$$

$\Rightarrow \forall i: \pi(b_i^{n_i}) = e \Rightarrow n_i$ Vielfaches von $\text{ord}(H'_i) = \text{ord}(b_i)$

$\Rightarrow \forall i: b_i^{n_i} = e \Rightarrow G = H \times A$

Gleiches Argument zeigt $H = \langle b_1 \rangle \times \dots \times \langle b_r \rangle$. Also

$$G = \langle b_1 \rangle \times \dots \times \langle b_r \rangle \times \langle a \rangle \quad \square$$

1.6.3 Satz Sei $G \neq \{e\}$ endlich und abelsch.

Im Satz 1.6.2 kann man die zyklischen Faktoren wie folgt wählen:

$$G \cong \mathbb{Z}/p_1^{l_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{l_r}\mathbb{Z}$$

wobei p_i Primzahlen sind und $l_i \in \mathbb{N}$.

Beweis Ist $m = 2_1^{k_1} \dots 2_s^{k_s}$ mit $2_1, \dots, 2_s$ paarweise verschiedene Primzahlen, so gilt

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/2_1^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/2_s^{k_s}\mathbb{Z}. \quad \square$$