§9. Endliche abelsche Gruppen

Eine endliche abelsche Gruppe G heißt **primär**, wenn die Ordnung von G eine Primzahlpotenz ist. Im Falle $|G| = p^k$ mit $p \in \mathbb{P}$ nennen wir G dann auch p–primär. Wir haben bewiesen:

(9.6) SATZ: Eine endliche **zyklische** Gruppe ist isomorph zu einem direkten Produkt von primären zyklischen Gruppen.

(9.9) SATZ: Primärzerlegung

Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt von primären Gruppen.

Bew: Sei G eine endliche abelsche Gruppe mit $n := |G| \geq 2$.

(1) Für einen Primteiler p von n sei

$$H := \{\, a \mid a \in G\,,\ \mathrm{ord}\,(a) \text{ ist eine Potenz von } p \,\}\,.$$

In der Vorlesung wurde bewiesen, daß H eine p–primäre Untergruppe von G ist.

(2) Sei $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ die kanonische PFZ von n. Dann sind insbesondere $p_1, p_2, \ldots, p_r$ alle Primteiler von n. Nach (1) ist

$$H_i := \{\, a \mid a \in G\,,\ \mathrm{ord}\,(a) \text{ ist eine Potenz von } p_i \,\} \quad (i = 1, 2, \ldots, r)$$

eine p_i–primäre Untergruppe von G. Wir wollen zeigen, daß sich jedes Element $a \in G$ eindeutig in der Form

$$(\star) \qquad a \;=\; a_1 \cdot a_2 \cdot \ldots \cdot a_r \quad \text{ mit } a_i \in H_i \ \ (\forall\, i = 1, 2, \ldots, r)$$

darstellen läßt.

Setze $q_i := p_i^{k_i}$ $(i = 1, 2, \ldots, r)$. Dann ist $n = q_1 \cdot q_2 \cdot \ldots \cdot q_r$.

Setze weiter $n_i := \dfrac{n}{q_i}$. Wegen $q_i \mid n$ gilt $n_i \in \mathbb{N}$.

Wir zeigen, daß die Zahlen $n_1, n_2, \ldots, n_r$ teilerfremd sind.

Anderenfalls würde es einen gemeinsamen Primteiler p dieser Zahlen geben.

$p \mid n_1 \implies p \mid p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \implies p \mid p_j^{k_j}$ für ein $j \in \{2, \ldots, r\} \implies p = p_j$ mit $j \neq 1$

Es muß aber auch $p \mid n_j$ gelten, woraus sich wie oben $p = p_l$ für ein $l \neq j$ ergibt. Daraus folgt $p_l = p_j$ mit $l \neq j$. **Widerspruch!** Folglich ist $\mathrm{ggT}(n_1, n_2, \ldots, n_r) = 1$, so daß es Zahlen $m_1, m_2, \ldots, m_r \in \mathbb{Z}$ gibt mit

$$\sum_{i=1}^{r} m_i n_i \;=\; 1$$

Sei nun $a \in G$ beliebig. Dann gilt

$$a \;=\; a^1 \;=\; a^{\sum_{i=1}^{r} m_i\, n_i} \;=\; (a^{m_1 n_1}) \cdot \ldots \cdot (a^{m_r n_r})$$

Wir behaupten nun $a_i := a^{m_i n_i} \in H_i$ für alle $i = 1, \ldots, r$. Es gilt nämlich

$$a_i^{q_i} \;=\; (a^{m_i n_i})^{q_i} \;=\; a^{m_i \frac{n}{q_i} q_i} \;=\; a^{m_i n} \;=\; (a^n)^{m_i} \;=\; 1$$

wegen $a^n = 1$, da $n = |G|$. Folglich ist $\mathrm{ord}\,(a_i)$ als Teiler von $q_i = p_i^{k_i}$ eine Potenz von p_i, so daß a_i ein Element aus H_i ist. Dies sichert die Existenz der Darstellung $(\star)$ von $a \in G$. Wir beweisen nun deren Eindeutigkeit. Gelte

$$a_1 \cdot a_2 \cdot \ldots \cdot a_r \;=\; b_1 \cdot b_2 \cdot \ldots \cdot b_r \;\text{ mit }\; a_i, b_i \in H_i \;\; (1 = 1, 2, \ldots, r)$$

Dann folgt $1 = (a_1 \cdot a_2 \cdot \ldots \cdot a_r) \cdot (b_1 \cdot b_2 \cdot \ldots \cdot b_r)^{-1} \;=\; (a_1 b_1^{-1}) \cdot \ldots \cdot (a_r b_r^{-1})$, woraus sich

$$a_k^{-1} b_k \;=\; (a_1 b_1^{-1}) \cdot \ldots \cdot (a_{k-1} b_{k-1}^{-1}) \cdot (a_{k+1} b_{k+1}^{-1}) \cdot \ldots \cdot (a_r b_r^{-1}) \;\in\; H_k \cap \widehat{H}_k$$

ergibt. Dabei ist $\widehat{H}_k := \langle \bigcup_{i \neq k} H_i \rangle$. Es genügt nun zu zeigen

$$(\star\star) \qquad H_k \cap \widehat{H}_k \;=\; \{1\} \quad \forall\, k = 1, 2, \ldots, r\,,$$

da dann $a_k^{-1} b_k = 1$ für alle k folgt, also $a_k = b_k$ für alle k, woraus sich die Eindeutigkeit der Darstellung $(\star)$ ergibt. Nun der Nachweis von $(\star\star)$:

Sei $c \in H_k \cap \widehat{H}_k$ beliebig. Wir wollen $\mathrm{ord}\,(c) = 1$ zeigen, woraus dann $c = 1$ folgt.

$c \in H_k \;\Longrightarrow\; l := \mathrm{ord}\,(c)$ ist eine Potenz von p_k

$c \in \widehat{H}_k \;\Longrightarrow\; c$ läßt sich als ein Produkt von Elementen aus H_i $(i \neq k)$ darstellen, d.h.

$$c \;=\; \prod_{i \neq k} d_i \quad \text{mit} \quad d_i \in H_i\,,\; \mathrm{ord}\,(d_i) = p_i^{s_i} \quad (s_i \in \mathbb{N}_0)\,.$$

Annahme: $l := \mathrm{ord}\,(c) > 1$. Mit $q := \prod_{i \neq k} p_i^{s_i}$ folgt dann

$$c^q \;=\; \prod_{i \neq k} d_i^q \;=\; \prod_{i \neq k} \left(d_i^{p_i{}^{s_i}}\right)^{t_i} \;=\; 1 \quad (\text{mit } t_i = q/p_i^{s_i})$$

und daraus $l \,|\, q$. Ist also p ein Primteiler von $l = \mathrm{ord}\,(c)$, so folgt $p \in \{p_1, \ldots, p_{k-1}, p_{k+1}, \ldots, p_r\}$. Folglich ist l teilerfremd zu jeder Potenz von p_k. l ist aber selbst eine Potenz von p_k, so daß $l = 1$ sein muß. **Widerspruch!**

(3) Die Abbildung $f : H_1 \times H_2 \times \ldots \times H_r \longrightarrow G$ sei definiert durch

$$f((a_1, a_2, \ldots, a_r)) := a_1 \cdot a_2 \cdot \ldots \cdot a_r$$

f ist ein Gruppenhomomorphismus:

Seien $x = (a_1, a_2, \ldots, a_r), y = (b_1, b_2, \ldots, b_r) \in H_1 \times H_2 \times \ldots \times H_r$. Dann gilt:

$f(x \cdot y) \;=\; f((a_1 b_1, \ldots, a_r b_r)) \;=\; (a_1 b_1) \cdot \ldots \cdot (a_r b_r) \;=\; (a_1 \cdot \ldots \cdot a_r) \cdot (b_1 \cdot \ldots \cdot b_r) \;=\; f(x) \cdot f(y)$

f ist injektiv: Sei $(a_1, a_2, \ldots, a_r)$ ein Element aus $\mathrm{Kern}(f)$. Dann folgt:

$a_1 \cdot \ldots \cdot a_r \;=\; f((a_1, \ldots, a_r)) \;=\; 1 \;=\; 1 \cdot \ldots \cdot 1$ wobei die 1 an der Stelle i das neutrale Element in H_i ist. Da die Darstellung nach $(\star)$ eindeutig bestimmt ist, folgt $(a_1, \ldots, a_r) = (1, \ldots, 1)$, d.h. $(a_1, \ldots, a_r)$ ist das neutrale Element in $H_1 \times \ldots \times H_r$. Folglich ist $\mathrm{Kern}(f)$ trivial und f injektiv.

f ist surjektiv: Sei $a \in G$ beliebig. Nach $(\star)$ gilt $a \;=\; a_1 \cdot a_2 \cdot \ldots \cdot a_r$ mit $a_i \in H_i$ $(\forall\, i = 1, 2, \ldots, r)$. Dann ist $(a_1, \ldots, a_r)$ ein Urbild von a unter f.

BEM: An vielen Stellen des Beweises ist stillschweigend von der Kommutativität der Gruppe Gebrauch gemacht worden!