ALG Ü6

167)

(1) $C_n \times C_m$ ...zyklisch $\Leftrightarrow$ n, m besitzen keinen Teiler $d > 1$

$\Rightarrow$ Wir zeigen zuerst n, m besitzen einen gemeinsamen Teiler $\ell > 1 \Rightarrow C_n \times C_m$ ...nicht zyklisch.

Sei $(x,y) \in C_n \times C_m$ bel. $\operatorname{ord}(x,y) \leq \frac{n \cdot m}{\ell} < n \cdot m$, da $\frac{n \cdot m}{\ell} x = n \cdot \frac{m}{\ell} x$ und $\frac{n \cdot m}{\ell} y = \frac{n}{\ell} m y$ jeweils wird x bzw. y durch n bzw. m annulliert, da $\operatorname{ord}(x) \leq n$ und $\operatorname{ord}(y) \leq m$.

Wäre $C_n \times C_m$ zyklisch gäbe es ein $(x,y) \in C_n \times C_m$ mit $\operatorname{ord}(x,y) = n \cdot m = |C_n \times C_m|$.

Da $C_n \times C_m = \langle (x,y) \rangle$. $\Rightarrow C_n \times C_m$ ist nicht zyklisch.

$\Leftarrow$ Für die andere Richtung betrachten wir $f: C_{n \cdot m} \to C_n \times C_m$, $\overline{x}^{nm} \mapsto (\overline{x}^{n}, \overline{x}^{m})$. *

Wir wollen nun unter der Annahme, dass n, m keinen gemeinsamen Teiler > 1 besitzt, zeigen, dass f ein Isomorphismus ist und somit $C_n \times C_m$ als Bild einer zyklischen Gruppe ebenfalls zyklisch ist.

$\overline{x}^{n \cdot m}, \overline{y}^{n \cdot m} \in C_{n \cdot m}$ bel. $f(\overline{x}^{n \cdot m} \overline{+} \overline{y}^{n \cdot m}) = f(\overline{x \overline{+} y}^{n \cdot m}) = (\overline{x \overline{+} y}^{n}, \overline{x \overline{+} y}^{m}) = (\overline{x}^{n} \overline{+} \overline{y}^{n}, \overline{x}^{m} \overline{+} \overline{y}^{m}) = f(\overline{x}) + f(\overline{y})$

Offenbar gilt $|C_n \times C_m| = n \cdot m = |C_{n \cdot m}|$ also reicht es Injektivität zu zeigen, damit Bij.

Sei $\overline{x}^{n \cdot m} \in C_{n \cdot m}$ mit $f(\overline{x}^{n \cdot m}) = (\overline{0}^{n}, \overline{0}^{m})$ bel. $\Rightarrow (\overline{x}^{n}, \overline{x}^{m}) = (\overline{0}^{n}, \overline{0}^{m})$

$\Rightarrow x + n\mathbb{Z} = 0 \wedge x + m\mathbb{Z} = 0 \Rightarrow x = -n\mathbb{Z} = n\mathbb{Z} \wedge x = -m\mathbb{Z} = m\mathbb{Z}$

$\Rightarrow \exists k, l \in \mathbb{Z} : k \cdot n = x = l \cdot m$, da n, m teilerfremd sind muss $k \in m\mathbb{Z}$ und $l \in n\mathbb{Z}$ sein.

$\Rightarrow x \in n \cdot m\,\mathbb{Z}$ also $\overline{x}^{n \cdot m} = \overline{0}^{n \cdot m}$ $\Rightarrow f$ ...injektiv $\Rightarrow f$... Isomorphismus

$\Rightarrow C_n \times C_m$ ... zyklisch

* wohldefiniert: $\overline{x}^{n \cdot m} = \overline{y}^{n \cdot m} \Rightarrow x + nm\mathbb{Z} = y + nm\mathbb{Z} \Rightarrow x = y + nm\mathbb{Z}$

$x = y + n(\underbrace{m\mathbb{Z}}_{\in \mathbb{Z}}) \in y + n\mathbb{Z}$ $\quad x = y + m(\underbrace{n\mathbb{Z}}_{\subseteq \mathbb{Z}}) \in y + m\mathbb{Z}$ $\Rightarrow \overline{x}^{n} = \overline{y}^{n} \wedge \overline{x}^{m} = \overline{y}^{m}$

$f(\overline{x}^{n \cdot m}) = (\overline{x}^{n}, \overline{x}^{m}) = (\overline{y}^{n}, \overline{y}^{m}) = f(\overline{y}^{n \cdot m})$ ✓

ALG Ü6

167) (2) $C_n \cong \bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$ $\quad C_n$ ... zyklische Gruppe der Ordnung $n = \prod_{p\in\mathbb{P}} p^{e_p}$

$\operatorname{ord}(C_n) = \prod_{p\in\mathbb{P}} p^{e_p}$, $\quad \operatorname{ord}(\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}) = \prod_{p\in\mathbb{P}} \operatorname{ord}(C_{p^{e_p}}) = \prod_{p\in\mathbb{P}} p^{e_p}$ $\quad$ also gleich

$f: C_n \to \bigoplus_{p\in\mathbb{P}} C_{p^{e_p}} \quad \bar{x} \mapsto (x \bmod p^{e_p})_{p\in\mathbb{P}}$

wohldefiniert: $\bar{x} = \bar{y} \Leftrightarrow \exists k\in\mathbb{Z} : x = y + kn$

$f(\bar{x}) = (x \bmod p^{e_p})_{p\in\mathbb{P}} = ((y+kn) \bmod p^{e_p})_{p\in\mathbb{P}} = ((y \bmod p^{e_p}) + (kn \bmod p^{e_p}))_{p\in\mathbb{P}}$

$= (y \bmod p^{e_p})_{p\in\mathbb{P}} + (k \cdot \prod_{p\in\mathbb{P}} p^{e_p} \bmod p^{e_p})_{p\in\mathbb{P}} = f(y) + (0)_{p\in\mathbb{P}} = f(\bar{y})$

Homomorphismus: $\bar{x}, \bar{y} \in C_n$ bel.

$f(\bar{x}+\bar{y}) = f(\overline{x+y}) = (x+y \bmod p^{e_p})_{p\in\mathbb{P}} = (x \bmod p^{e_p})_{p\in\mathbb{P}} + (y \bmod p^{e_p})_{p\in\mathbb{P}}$

$= f(\bar{x}) + f(\bar{y})$

Injektivität: $\bar{x} \in C_n$ mit $f(\bar{x}) = (0)_{p\in\mathbb{P}}$ bel.

$f(\bar{x}) = (x \bmod p^{e_p}) = (0)_{p\in\mathbb{P}} \Leftrightarrow \forall p\in\mathbb{P}: x \in p^{e_p}\mathbb{Z} \Rightarrow x \in \prod_{p\in\mathbb{P}} p^{e_p}\mathbb{Z} = n\mathbb{Z}$

$\Rightarrow \bar{x} = \overline{0} \in C_n$

Bijektivität: Da $\operatorname{ord}(C_n) = n = \prod_{p\in\mathbb{P}} p^{e_p}$ und aus $p,q\in\mathbb{P}, p\neq q$ und $k,l\in\mathbb{N}$:

p^k, q^l haben keine gemeinsamen Teiler >1 folgt

$\operatorname{ord}(\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}) = \prod_{p\in\mathbb{P}} p^{e_p}$ (alle $p\in\mathbb{P}$ mit $e_p = 0$ tragen nichts zur Ordnung bei, davon sind nach Definition fast alle) also gleich

$\Rightarrow$ injektiv $\Rightarrow$ bijektiv

$\Rightarrow f$ ... Isomorphismus