ALG Ü*

167) (1) zz: $C_n \times C_m$ ... zyklisch $\Leftrightarrow$ $ggT(n,m)=1$

($\Leftarrow$) $f: C_{nm} \to C_n \times C_m$ • $f(\overline{0}^{nm}) = (\overline{0}^n, \overline{0}^m)$ ... neutrales Element von $C_n \times C_m$

$\overline{a}^{nm} \mapsto (\overline{a}^n, \overline{a}^m)$ • $f(\overline{a+b}^{nm}) = (\overline{a+b}^n, \overline{a+b}^m) = (\overline{a}^n, \overline{a}^m) + (\overline{b}^n, \overline{b}^m)$

• Sei $\overline{a}^{nm}$ mit $f(\overline{a}^{nm}) = (\overline{0}^n, \overline{0}^m)$ bel. $= f(\overline{a}^{nm}) + f(\overline{b}^{nm})$ $\Rightarrow$ Homomorphismus

$\Rightarrow f(\overline{a}^{nm}) = (\overline{a}^n, \overline{a}^m) = (\overline{0}^n, \overline{0}^m)$ $\quad \overline{a}^n = \overline{0}^n \Leftrightarrow a \in n\mathbb{Z}$, $\overline{a}^m = \overline{0}^m \Leftrightarrow a \in m\mathbb{Z}$

Da $ggT(n,m)=1 \Rightarrow a \in nm\mathbb{Z} \Rightarrow \overline{a}^{nm} = \overline{0}^{nm}$ $\Rightarrow$ injektiv

• $|C_{nm}| = nm = |C_n \times C_m| \Rightarrow$ bijektiv $\Rightarrow$ Isomorphismus

$\Rightarrow C_{nm} \simeq C_n \times C_m$ und da C_{nm} zyklisch ist folgt das auch $C_n \times C_m$ zyklisch sein muss.

($\Rightarrow$) $C_n \times C_m$ ... zyklisch $\Rightarrow \exists (x,y) \in C_n \times C_m : \langle (x,y) \rangle = C_n \times C_m$

$nm = ord(x,y) = kgV(ord(x), ord(y)) = \dfrac{ord(x) \cdot ord(y)}{ggT(ord(x), ord(y))} = \dfrac{nm}{ggT(n,m)}$

(da $kgV(a,b) \cdot ggT(a,b) = ab$) $\Rightarrow ggT(n,m) = 1$

(2) zz: C_n ... zyklische Gruppe $n = \prod_{p \in \mathbb{P}} p^{e_p} \Rightarrow C_n \simeq \bigoplus_{p \in \mathbb{P}} C_{p^{e_p}}$

wobei e^p nur endlich oft $\neq 0$ ist. Sei $z \in \mathbb{N}$ maximal mit z-te Primzahl $p: e^p \neq 0$.

$D_k := C_{2^{e_2}} \times C_{3^{e_3}} \times \ldots \times C_{p^{e_p}}$ $\quad o_k := 2^{e_2} \cdot 3^{e_3} \cdot \ldots \cdot p^{e_p}$ jeweils bis zur k-te Primzahl.

Vollständige Induktion um zu zeigen $D_k \simeq C_{o_k}$ $\forall k$

$k=1$: $D_1 = C_{2^{e_2}}$ $\quad o_k = 2^{e_2}$ $\Rightarrow C_{2^{e_2}} \cong C_{2^{e_2}}$

$k+1$: Angenommen $D_k \simeq C_{o_k}$ Sei p' die $k+1$-te Primzahl

Oben haben wir gezeigt, dass $ggT(o_k, p'^{e_{p'}}) = 1 \Rightarrow C_{o_k} \times C_{p'^{e_{p'}}} \cong C_{o_{k+1}}$

Da $D_k \cong C_{o_k} \Rightarrow D_k \times C_{p'^{e_{p'}}} = D_{k+1} \cong C_{o_{k+1}}$

Nach endlich vielen Schritten erreichen wir $z \Rightarrow D_z \simeq C_{o_z}$

$\bigoplus_{p \in \mathbb{P}} C_{p^{e_p}} \simeq D_z \simeq C_{o_z} = C_n$ $\square$

$f: C_n \to C_{2^{e_2}} \times C_{3^{e_3}} \times \ldots$

$\overline{a}^n \mapsto (\overline{a}^{2^{e_2}}, \overline{a}^{3^{e_3}}, \ldots)$