

ALG Ü6

2.15) $p \in \mathbb{P}$

(1) Wie viele Untergruppen hat $C_p \times C_p$?

Zyklische Untergruppen: Werden erzeugt von $\langle \bar{x}, \bar{y} \rangle$ mit $\bar{x}, \bar{y} \in C_p$. Für $(\bar{a}, \bar{b}) \in \langle \bar{x}, \bar{y} \rangle \setminus \{(\bar{0}, \bar{0})\}$

gilt $\langle \bar{a}, \bar{b} \rangle = \langle \bar{x}, \bar{y} \rangle$. $\text{ord} \langle \bar{x}, \bar{y} \rangle = \begin{cases} 0 & \text{falls } \bar{x} = \bar{0} = \bar{y} \\ p & \text{sonst} \end{cases}$

\Rightarrow Es gibt $\frac{p \cdot p - 1}{p - 1} + 1 = p + 1 + 1 = p + 2$ zyklische Untergruppen von $C_p \times C_p$

Nicht zyklische Untergruppen: Werden von zumindest 2 Elementen $(\bar{x}, \bar{y}), (\bar{a}, \bar{b})$ erzeugt, für die gilt

$(\bar{x}, \bar{y}) \notin \langle \bar{a}, \bar{b} \rangle \wedge (\bar{a}, \bar{b}) \notin \langle \bar{x}, \bar{y} \rangle$. $\text{ord} \langle \bar{x}, \bar{y} \rangle = p$, da sie p^2 teilen muss, aber nicht ganz $C_p \times C_p$ erzeugen darf und aber auch nicht $(\bar{x}, \bar{y}) = (\bar{0}, \bar{0}) \in \langle \bar{a}, \bar{b} \rangle$ gelten kann.

$\langle (\bar{x}, \bar{y}), (\bar{a}, \bar{b}) \rangle \subseteq U \quad \text{ord} \langle \bar{x}, \bar{y} \rangle \cdot \text{ord} \langle \bar{a}, \bar{b} \rangle = p \cdot p = p^2 = \text{ord}(C_p \times C_p)$

$\Rightarrow U$ muss von genau 2 Elementen mit $\text{ord } p$ erzeugt werden. $\Rightarrow \text{ord } U = p^2$

$\Rightarrow U = C_p \times C_p \quad \Rightarrow$ Es gibt nur 1 nicht zyklische Untergruppe von $C_p \times C_p$

Insgesamt gibt es also $p + 3$ Untergruppen von $C_p \times C_p$.

(2) Wie viele Untergruppen hat C_{p^2} ?

Die Ordnung der Untergruppe muss p^2 teilen also sind nur 1, p , p^2 möglich.

$C_1 = \langle \bar{0} \rangle$ und $C_{p^2} = \langle \bar{x} \rangle$ mit $\bar{x} \in \{1, \dots, p^2 - 1\} \setminus \{p, 2p, \dots, (p-1)p\}$ sind triviale

Untergruppen, (da $\langle \bar{x} \rangle$ zyklisch ist und offenbar Untergruppe so muss $\text{ord}(\bar{x}) \mid p^2$

$\text{ord} \langle \bar{x} \rangle \neq 1$, da $\bar{x}, \bar{0} \in \langle \bar{x} \rangle$; $\text{ord} \langle \bar{x} \rangle \neq p$, da $p \cdot \bar{x} \neq p \cdot p = \bar{0} \Rightarrow \text{ord} \langle \bar{x} \rangle = p^2$)

Für $\bar{x} \in \{p, 2p, \dots, (p-1)p\}$ gilt $p \cdot \bar{x} = p \cdot kp = p \cdot p \cdot k = \bar{0} \Rightarrow \text{ord} \langle \bar{x} \rangle \leq p$

$\text{ord} \langle \bar{x} \rangle \neq 1$ weil wieder $\bar{0}, \bar{x} \in \langle \bar{x} \rangle \Rightarrow \text{ord} \langle \bar{x} \rangle = p \quad \langle \bar{x} \rangle \cong C_p$

\Rightarrow Es gibt 3 Untergruppen.

Bsp $C_3 \times C_3$:

$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 2 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \end{pmatrix}$

$\begin{matrix} 2 & 0 \\ 2 & 1 \\ 2 & 2 \end{matrix}$

$\begin{matrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 2 & 2 & 0 & 2 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \text{"} & \text{"} & \text{"} & \text{"} & \text{"} & \text{"} & \text{"} & \text{"} \\ 0 & 2 & 2 & 0 & 2 & 2 & 2 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$

Bsp $C_2 \times C_2$:

$\begin{matrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$

$\begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$