

$$1) \quad a) \quad (\boxed{987}^{911}) \mod 911 = (987 \mod 911)^{911} \mod 911 =$$

$$\mathbb{Z}_{911}^* = \langle \mathbb{Z}_{911}^*, \cdot, 1 \rangle \quad (76^{911}) \mod 911$$

$$\varphi(911) = 910$$

$$a \in G: a^{\text{ord}(G)} = 1$$

$$76^{910} = 1$$

$$(76^{910} \cdot 76) \mod 911 =$$

$$((76^{910} \mod 911) \cdot (76 \mod 911)) \mod 911 =$$

$$(1 \cdot 76) \mod 911 = 76$$

$$a^k = a^{k \mod \text{ord}(G)}$$

$$987^{909} \mod 911 \equiv 76^{909} \mod 911$$

$$a^k \equiv a^{k - \varphi(n)}$$

$$\Rightarrow 76^{909} = 76^{909-910} = 76^{-1} \equiv 12$$

$$\boxed{76 \in \mathbb{Z}_{911}^*} \rightarrow 76 \text{ ist teilerfremd zu } 911$$

$$\text{ggT}(76, 911) = 1$$

$$(\alpha \cdot 76 + \beta \cdot 911) = 1 \rightarrow (\alpha \cdot \overbrace{76} + \beta \cdot \overbrace{911}) \mod 911 = 1$$

$$((\alpha \cdot 76 \mod 911) + (\beta \cdot 911 \mod 911)) \mod 911 = 1$$

$$((\alpha \cdot 76 \mod 911) + 0) \mod 911 = 1$$

$$\boxed{\alpha} \cdot 76 \bmod 911 = 1$$

$$\alpha \cdot 76 \bmod 911 = 1 \rightarrow 76^{-1} = \alpha$$

a	b		k		α	β
76	911		11		12	-1
75	76		1		-1	1
1	75		75		1	0

$$\rightarrow 76^{-1} = 12$$

b) $\pi = \boxed{(1, 2, 3)} (4, 5)$

$$\pi^k = \text{id}$$

$$\rightarrow \text{für } 1, 2, 3: k = 3, 6, 9, \dots$$

$$\rightarrow \text{für } 4, 5: k = 2, 4, 6, 8, \dots$$

$$\rightarrow \text{für } 6: k = 1, 2, 3, 4, \dots$$

k ist kgV aller Zykellängen

$$\rightarrow k = \text{kgV}(3, 2, 1) = 6$$

$$\pi^6 = \text{id}$$

$$\text{ord}(\pi) = 6$$

$$\forall a \in G: a^{\text{ord}(a)} = \text{id}$$

$$\rightarrow a^k = \text{id}, \text{ wenn } k \bmod \text{ord}(a) = 0$$

$$\pi^{787} = \pi^{787 \bmod 6} = \pi^1 = \pi = (1, 2, 3)(4, 5)$$

$$\pi^{785} = \pi^{785 \bmod 6} = \pi^5 = \pi^{-1} \leftarrow \text{Umkehrfunktion}$$

von π

x	1	2	3	4	5	6
$\pi(x)$	2	3	1	5	4	6

$$\rightarrow \pi^{-1} = (1, 3, 2)(4, 5)$$

2) $n=16$

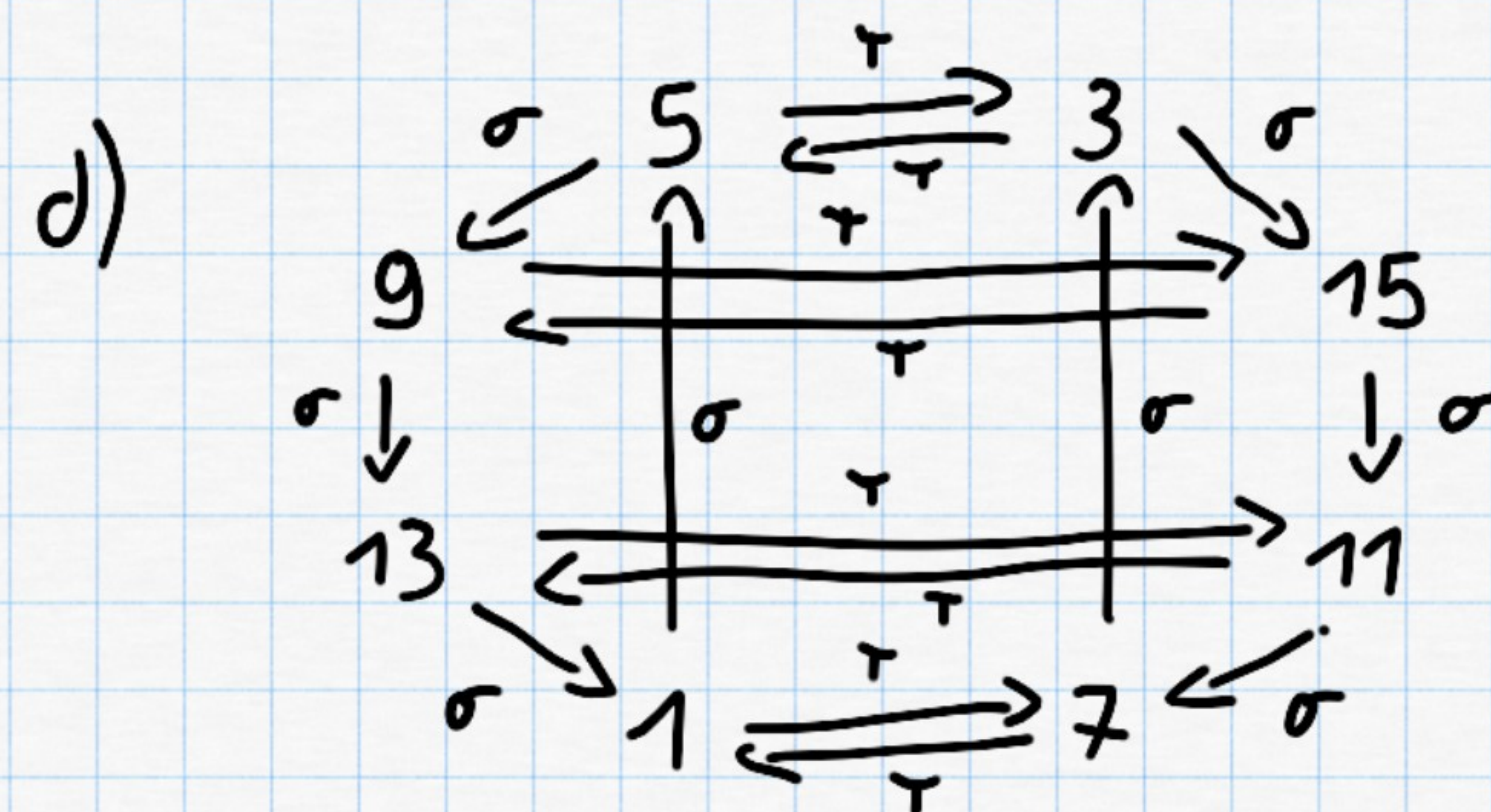
$$a) |\mathbb{Z}_n^*| = \varphi(16) = \varphi(2^4) = 2^{4-1} \cdot (2-1) = 2^3 = 8$$

b)

·16	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

c)

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{3, 9, 11, 1\} \\ \langle 5 \rangle &= \{5, 9, 13, 1\} \\ \langle 7 \rangle &= \{7, 1\} \\ \langle 9 \rangle &= \{9, 1\} \\ \langle 11 \rangle &= \{11, 9, 3, 1\} \\ \langle 13 \rangle &= \{13, 9, 5, 1\} \\ \langle 15 \rangle &= \{15, 1\} \\ \Rightarrow \lambda &= \text{kgV}(1, 4, 2) = 4 \end{aligned}$$



→ Wähle σ , sodass es
den Graphen in 2
Kreise teilt

→ Wähle τ , sodass es
zwischen den Kreisen
wechselt

→ z.B. $\sigma = 5, \tau = 7$

Aufgabe 12.4

- (a) Bestimmen Sie die Ordnung von 3 in $\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$.
(b) Bestimmen Sie die Ordnung von 3 in $\langle \mathbb{Z}_{34}^*, \cdot_{34}, 1 \rangle$.
(c) Bestimmen Sie die Ordnung von $\pi: [5] \rightarrow [5]$ in $\langle S_5, \circ, \text{id}_{[5]} \rangle$ mit

$$\pi(1) = 2 \quad \pi(2) = 4 \quad \pi(3) = 5 \quad \pi(4) = 1 \quad \pi(5) = 3$$

- (d) Bestimmen Sie den Gruppenexponent $\lambda_{\mathbb{Z}_{20}^*} = \min\{\lambda \in \mathbb{N} : \forall x \in \mathbb{Z}_{20}^* : x^\lambda = 1\}$ von $\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$.
(e) Bestimmen Sie den Gruppenexponent $\lambda_{\mathbb{Z}_{34}^*} = \min\{\lambda \in \mathbb{N} : \forall x \in \mathbb{Z}_{34}^* : x^\lambda = 1\}$ von $\langle \mathbb{Z}_{34}^*, \cdot_{34}, 1 \rangle$.
(f) Bestimmen Sie den Gruppenexponent $\lambda_{S_5} = \min\{k \in \mathbb{N} : \forall x \in S_5^* : x^k = \text{id}_{[5]}\}$ von $\langle S_5, \circ, \text{id}_{[5]} \rangle$

a) $\text{ord}(3) \mid |G| \quad |G| = 8$

$$\text{ord}(3) \in \{1, 2, 4, 8\}$$

$$3^1 \equiv_{20} 3 \neq 1$$

$$3^2 \equiv_{20} 9 \neq 1$$

$$3^4 \equiv_{20} 1$$

$$\text{ord}(3) = 4$$

b) $|G| = 16 \quad |\mathbb{Z}_{34}^*| = \varphi(34) = \varphi(2) \cdot \varphi(17) = 1 \cdot 16 = 16$

$$\text{ord}(3) \in \{1, 2, 4, 8, 16\}$$

$$3^4 \equiv_{34} 13 \neq 1$$

$$3^8 \equiv_{34} 13^2 \neq_{34} 1$$

$$3^{16} \equiv_{34} 1$$

$$\text{ord}(3) = 16 \quad \hookrightarrow \text{Erzeuger}$$

c) $(1, 2, 4) (3, 5)$
 $\text{kgV}(2, 3) = 6$

$\text{ord}(\pi) = 6$

d) $\lambda_{Z_{20}^*} = 4$

e) $\lambda_{Z_{34}^*} = 16$

f) $\lambda_{S_5} = \text{kgV}(1, 2, 3, 4, 5) = 60$