1. Najděte všechny generátory grupy:

(a) $\mathbb{Z}_{12}$

(b) $\mathbb{Z}_7^*$

16.3.

a) $\mathbb{Z}_{12} = \langle 1 \rangle$

$\boxed{1, 5, 7, 11}$

7^k , $NSD(m, k) = 1$

$\underbrace{1 + \dots + 1}_{k}$

m = 12 = řád grupy

2. Hledali byste raději generátor grupy $\mathbb{Z}_{181}^*$, nebo grupy $\mathbb{Z}_{227}^*$?

$226 = 2 \cdot 113$

• 181, 227 jsou prvočísla

13 … je řád 13 226?

$180 = \underline{2 \cdot 2 \cdot 3 \cdot 3 \cdot 5}$

$13^{113 \cdot 2} = 1$

$a^2 = 1$

1 -1

$a^{113} = 1$

$(-a)^{113} = -a^{113} = -1$

3. Napište všechny podgrupy grupy. Jak jsou podgrupy uspořádány inkluzí?

(a) $\mathbb{Z}$

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Z}_{23}^*$

(d) $\mathbb{Z}_{17}^*$

4 $\mathbb{Z}_{18} \simeq \mathbb{Z}_2 \times \mathbb{Z}_9$

m, n nesoudělná

4. Rozložte dané grupy na direktní součin co nejvíce netriviálních cyklických grup:

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{29}^*$

(c) $\mathbb{Z}_{21}^*$

(d) $\mathbb{Z}_{30}^*$

p prvočíslo

$\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$

mod $m \cdot n$ $\leftrightarrow$ mod m, mod n

$\mathbb{Z}_{m \cdot n} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

$\cancel{\mathbb{Z}_9 \simeq \mathbb{Z}_3 \times \mathbb{Z}_3}$

$\underline{\mathbb{Z}_{29}^*} \simeq \underline{\mathbb{Z}_{28}}$

kon.

Věta 16.7. T těleso $\rightarrow T^*$ je cykl. grupa

$\mathbb{Z}_{29}^*$	$\mathbb{Z}_{28}$
a	b
a^2	b^2
a^3	b^3
⋮	⋮
$a^{28} = 1$	$b^{28} = 1$

$\mathbb{Z}_{29}^* \simeq \mathbb{Z}_{28} \simeq \mathbb{Z}_7 \times \mathbb{Z}_4$

5. Rozhodněte, zda jsou následující grupy cyklické:

(a) $\mathbf{S}_3$

(b) $\mathbf{A}_3$

(c) $\mathbb{Z}_{12}^*$

(d) $\mathbb{Z}_{14}^*$

$A_3 \leq S_3$ sudé permutace

a) NENÍ: $\boxed{(1\,2\,3)}$ ... řád 3

$\boxed{(1\,3\,2)}$ ... řád 3

(12), (13), (23) } řády 2

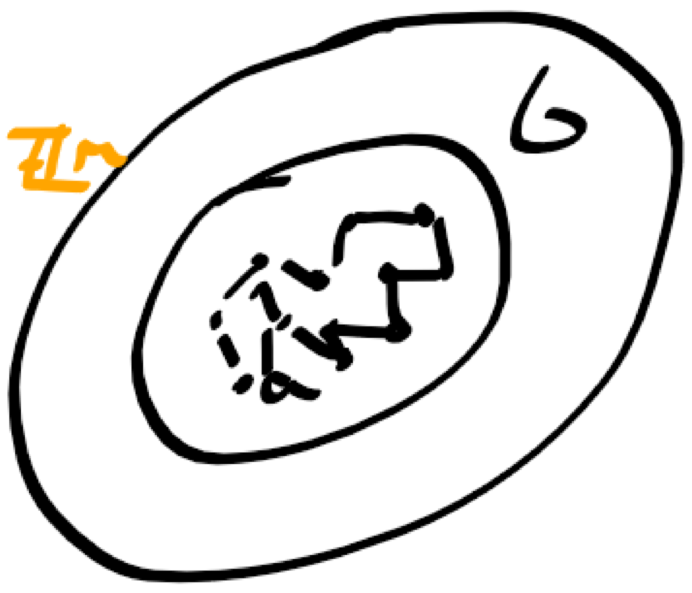
$\boxed{id}$ ... řád 1

$|S_3| = 6$

m, n nesoudělná

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

$\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$



$G \leq H \qquad a \in G$

řád a je n v H

$\Rightarrow$ řád a je n v G

d) $\mathbb{Z}_{14}^* \simeq \underbrace{\mathbb{Z}_2^*}_{1} \times \underbrace{\mathbb{Z}_7^*}_{6} \simeq \mathbb{Z}_7^* \simeq \mathbb{Z}_6$

prvky

je cyklická

(a, b)

(a', b')

$(1, a) \mapsto a$

$\varphi(14) = \varphi(2) \cdot \varphi(7) =$

$= 1 \cdot 6 = 6$

6. Najděte všechny homomorfismy

(a) ze $\mathbb{Z}_3$ do $\mathbb{Z}_5$

(b) ze $\mathbb{Z}_6$ do $\mathbb{Z}_8$

(c) ze $\mathbb{Z}_{11}$ do $\mathbb{Z}_{2021}$

φ homomorf. z $G \to H$

$\operatorname{ord}(\varphi(a))$ v H $\mid$ $\operatorname{ord}(a)$ v G

homomorf. je určen obrazy generátorů

a) $\mathbb{Z}_3 = \langle 1 \rangle$

$0, 1, 2$

$\operatorname{ord}(1) = 3$

$0 \mapsto 0$

$1 \mapsto 0$

$2 \mapsto 0$

v $\mathbb{Z}_5$ řády 1 nebo 5

5 prvků

jediný triviální homomorfismus