11.1 Komutativní grupy ⇝ klasifikace ⇝ součiny cyklických grup.

Řád $G$ je $8$ $\Rightarrow$

$$\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$\cong \mathbb{Z}_2 \times \mathbb{Z}_4$$
$$\cong \mathbb{Z}_8$$

se sčítáním

(i) $\mathbb{Z}_{15}^{\times} = \{a \in \mathbb{Z}_{15} \mid a$ invertibilní s násobením $\}$

$$|\mathbb{Z}_{15}^{\times}| = \varphi(15) = \varphi(3 \cdot 5) =$$
$$= 2 \cdot 4 = 8 \quad \text{Ok.}$$

Řády prvků v $\mathbb{Z}_{15}^{\times}$:

- 1 řád 1
- 2 řád 4 $2^4 = 16 \equiv 1 \mod 15$

↳ generuje $\{2, 4, 8, 1\}$

- 7 řád 4

↳ generuje $\{7, 4, -2, 1\}$

$7^2 = 49 \equiv -11 \mod 15$

$(-11)^2 = 121 \equiv 1 \mod 15$

- $11 \equiv -4 \mod 15$

$\Rightarrow$ řád $\leq 8$ atd.

$\Rightarrow$ všechny prvky jsou řádu nejvýše 4

Závěr: $\mathbb{Z}_{15}^{\times} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$

[Izo explicitně:

prvky řádu 4: 2, 8, 7, 13

$\hookrightarrow$ v $(\mathbb{Z}_{15}^{\times}, \cdot)$ $\quad 2 \cdot 8 \equiv 1 \mod 15$

$\quad 7 \cdot 13 \equiv 1$

Prvky řádu 4 v $(\mathbb{Z}_2 \times \mathbb{Z}_4, +)$

$(0,1), (0,3)$

$(1,1), (1,3)$

$\varphi: (\mathbb{Z}_{15}^{\times}, \cdot) \longrightarrow (\mathbb{Z}_2 \times \mathbb{Z}_4, +)$

- $\boxed{\varphi(2) = (0,1)}$

$\varphi(8) = (0,3)$

- $\boxed{\varphi(7) = (1,1)}$

jednoznačně určuje izomorfismus

$$1 \longmapsto (0,0)$$
$$2 \longmapsto (0,1)$$
$$4 \longmapsto (0,2)$$
$$7 \longmapsto (1,1)$$
$$-7 \longmapsto (0,-1)$$
$$-4 \longmapsto (-1,0)$$
$$-2 \longmapsto (-1,-1)$$
$$-1 \longmapsto (1,2)$$

(ii) $(\mathbb{Z}_{16}^{\times}, \cdot)$

$$|\mathbb{Z}_{16}^{\times}| = \varphi(16) = \varphi(2^4) = 1 \cdot 2^3 = 8$$

$$\mathbb{Z}_{16}^{\times} = \{1, 3, 5, 7, \cdot, 15\}$$

ord    ord 4    ord 4    ord 2

$3^4 = 9^2 = 81 \equiv 1 \mod 16$

$5^4 = 25^2 \equiv 9^2 = 81 \equiv 1$

$7^2 = 49 \equiv 1$

$\Rightarrow$ všechny prvky řádu $\leq 8$

$(\mathbb{Z}_{16}^\times, \cdot) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \cong (\mathbb{Z}_{15}^\times, \cdot)$

$(\bar{m}) \; (\mathbb{Z}_{17}^\times, \cdot)$

modulo podgrupa $\{+1, -1\} \leq \mathbb{Z}_{17}^\times$

$\mathbb{Z}_{17}^\times / \{\pm 1\}$ faktor

$|\mathbb{Z}_{17}^\times| = \varphi(17) = 16$

$|\mathbb{Z}_{17}^\times / \{\pm 1\}| = \frac{16}{2} = 8$

$$\mathbb{Z}_{17}^{\times} = \{1, 2, 3, 4, \dots, 8, -1, -2, -3, -4, \dots, -8\}$$

$$\mathbb{Z}_{17}^{\times} / \{\pm 1\} = \{a \cdot \{\pm 1\} \mid a \in \mathbb{Z}_{17}^{\times}\}$$

$$= \{a \cdot \{\pm 1\} \mid a \in \{1, 2, \dots, 8\}\}.$$

neboť $2 \cdot \{\pm 1\} = (-2) \cdot \{\pm 1\}$

Grupová operace:

$$(a \cdot \{\pm 1\}) \cdot (b \{\pm 1\}) = (a \cdot b) \cdot \{\pm 1\}$$

Řády prvků:

$1 \cdot \{\pm 1\}$ má řád 1

$2 \cdot \{\pm 1\}$ má řád 4

$$(2 \cdot \{\pm 1\})^2 = 4 \{\pm 1\} \neq 1 \cdot \{\pm 1\}$$

$$(2\cdot\{\pm 1\})^4 = 16\cdot\{\pm 1\} = \{\pm 1\}$$

$$16 \equiv -1$$

$\Rightarrow 3\cdot\{\pm 1\}$ má řád

$$(3\{\pm 1\})^2 = (-8)\{\pm 1\}$$

$$(3\{\pm 1\})^4 = 64\{\pm 1\} \neq \{\pm 1\}$$

$$64 \equiv -4 \mod 17$$

$$(3\{\pm 1\})^8 = \{\pm 1\}$$

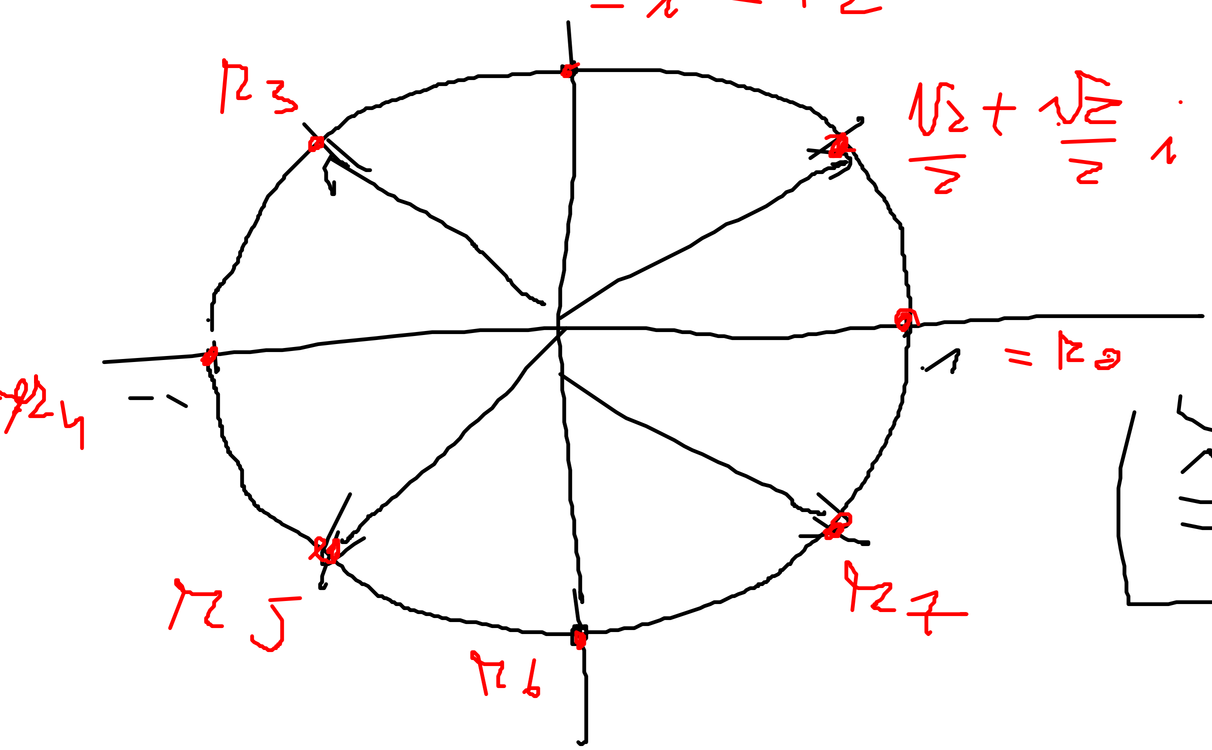
$\Rightarrow$ prvek řádu 8

$\Rightarrow$ je to cyklická grupa

Závěr: $(\mathbb{Z}_{17}^{\times}, \cdot)/\{\pm 1\} \cong (\mathbb{Z}_8, +)$

| řády prvků | |
|---|---|
| 0 | řád 1 |
| 1 | 8 |
| 2 | 4 |
| 3 | 8 |
| 4 | 2 |

(iv) kořeny pol. $z^8 - 1 = 0$ s násobením.




$\cong (\mathbb{Z}_8, +)$

$\Rightarrow r_1^2 = r_2, \dots, r_1^k = r_k$

$k \in \{0, 7\}$

11.2 (i) $G \leq GL(3,\mathbb{R})$

$$G = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}$$

s množenjem

- $\det \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} = 1 \neq 0$

- $G \leq GL(3,\mathbb{R})$ je podgrupa

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ a_1 & 1 & 0 \\ b_1 & c_1 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 0 \\ a_2 & 1 & 0 \\ b_2 & c_2 & 1 \end{pmatrix}$$

$A_1, A_2 \in G$

$$A_1 \cdot A_2 = \begin{pmatrix} 1 & 0 & 0 \\ a_1 + a_2 & 1 & 0 \\ & c_1 + c_2 & 1 \end{pmatrix} \in G$$

$b_1 + c_1 a_2 + b_2$

$$A_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -a_1 & 1 & 0 \\ c_1a_1 - b_1 & -c_1 & 1 \end{pmatrix}$$

$$\cap$$

$$G$$

$$b_1 + c_1(-a_1) + b_2 = 0$$

$$b_1 = c_1a_1 - b_1$$

$G \subseteq GL(3, \mathbb{R})$ normální

$$\iff \forall A \in GL(3, \mathbb{R}):$$

$$A \cdot G \cdot A^{-1} = G$$

Jinak, $A \in GL(3, \mathbb{R}$

$$B \in G$$

$$\boxed{A \cdot B \cdot A^{-1} \in G}$$

A zvolíme $\left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right) = 1$

$$\cancel{\left(\begin{array}{cc|c} 1 & 0 & 0 \\ -1 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b+1 & 1 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

$$= \begin{pmatrix} * & -b \\ * & * \end{pmatrix} \notin G$$

$G = GL(3, \mathbb{R})$

není normální podgrup.

(ii) $Z(G) = \{ B \in G \mid \forall A \in G :$

$$AB = BA \}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}, \quad A' = \begin{pmatrix} 1 & 0 & 0 \\ a' & 1 & 0 \\ b' & c' & 1 \end{pmatrix}$$

$$A \cdot A' = \begin{pmatrix} 1 & 0 & 0 \\ a+a' & 1 & 0 \\ b+b'+c\cdot a' & c+c' & 1 \end{pmatrix}$$

$$A' \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ a'+a & 1 & 0 \\ b'+b+c'\cdot a & c'+c & 1 \end{pmatrix}$$

Chceme $a, b, c$ takové, že pro $\forall a', b', c'$ platí

$$b + b' + c \cdot a' = b' + b + c' \cdot a$$

$$c \cdot a' = a \cdot c' \quad \text{pro lib. } a', c'$$

$$c = a = 0$$

Závěr: $Z(G) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{R} \right\}$

11.3: • $S_2 = \{id, (1,2)\} \cong (\mathbb{Z}_2, +)$

$\hookrightarrow$ pouze triviální podgrupy

• $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$\rightsquigarrow$ triviální podgrupy

$\rightsquigarrow$ 3 podgrupy tvaru $\{id, \text{transpozice}\} \cong (\mathbb{Z}_2, +)$

$\rightsquigarrow \{id, (1,2,3)(1,3,2)\} = A_3 \cong (\mathbb{Z}_3, +)$

podgr. sudých permutací

Možné řády podgrup: 1, 2, 3, 6

$A_3 \leq S_3$ je normální

$\sigma_1 \in S_3$ | $\underline{\sigma_1} \sigma_2 \underline{\sigma_1^{-1}} \in A_3$

$\sigma_2 \in A_3$ | $\downarrow$   $\forall \sigma_2 \in S_3$

sudá

$$S_3 / A_3 \cong (\{\pm 1\}, \cdot)$$

$$\sigma_1 \in S_3$$

$$\sigma_1 \cdot A_3 \in S_3 / A_3$$

$$\shortparallel$$

{sudé perm, liché perm}

• podgrupy v $S_4$

možné řády 1, 2, 3, 4, 6, 8, 12

→ + triviální podg.

→ 6 možností pro $(\mathbb{Z}_2, +)$

⟶ třiprvkové podgrupy ($\cong (\mathbb{Z}_3, +)$)

cykly délky 3 $\cong (\mathbb{Z}_3, +)$

⟶ podgrupy se čtyřmi prvky jsou komutativní

$\Rightarrow \mathbb{Z}_4$ nebo $\mathbb{Z}_2 \times \mathbb{Z}_2$

cykly délky 4

Kleinova grupa

- $\{id, (1,2), (3,4), (1,2)(3,4)\}$

není normální ⟶ $\{id, (1,3), (2,4), (1,3)(2,4)\}$

$\{id, (1,4), (2,3), (1,4)(2,3)\}$

- $\{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$

$(1,2)(3,4)(1,3)(2,4) = (4,1)(2,3)$

je normální

⇝ 6-ti prvková podgrupa $S_3 \leq S_4$

⇝ $A_4 \leq S_4$

⇝ ještě $D_8 \leq S_4$

<u>Normální podgrupy v $S_4$</u>

- $A_4 \leq S_4$
- Kleinova $\leq S_4$
  - ↳ ale ne každá Kl. podg.
- mnoho ...