JAKUB LEVÝ

Úloha č. 1

Označme $K := \bigcap_{M \subseteq H \leq G} H$, $J := \{ m_1^{i_1} \cdot \ldots \cdot m_n^{i_n} \mid m_k \in M, i_k = \pm 1, k = 1, \ldots, n, n \in \mathbb{N} \}$

Budeme chtít ukázat, že $K = J$.

Inkluze $\supseteq$:

$H \leq G$ a $M \subseteq H \Rightarrow \forall x \in J : x \in H$ (H je uzavřená na bin. op., inverz a obsahuje všechny $x_i \in M$)

$\Rightarrow K \supseteq J$

Inkluze $\subseteq$:

Abychom dokázali tuto inkluzi postačí ukázat:

1) $J \supseteq M$
2) $J \leq G$

(Potom J bude mezi množinami H v průniku v def K a jistě $K \subseteq J$)

1) $J \supseteq M$

Nechť $m \in M$, zvolme $n = 1$, $k = 1$, $i_1 = 1$ a $m_1 = m$. Potom $m \in J$.

2) $J \leq G$

M neprázdná $\Rightarrow$ J neprázdná.
Z def J obsahuje s každým prvkem a i jeho inverz a^{-1} a tedy znovu aplikováním def J i $a \cdot a^{-1} = e \in J$.

J je uzavřená na bin. op.:
Nechť $s_1^{\alpha_1} \cdot \ldots \cdot s_m^{\alpha_m}$ a $t_1^{\beta_1} \cdot \ldots \cdot t_n^{\beta_n}$, $m, n \geq 1$, $\alpha_i, \beta_i \in \{-1, 1\}$, $s_i, t_j \in M$.
Potom: $(s_1^{\alpha_1} \cdot \ldots \cdot s_m^{\alpha_m})(t_1^{\beta_1} \cdot \ldots \cdot t_n^{\beta_n})^{-1} = r_1^{\gamma_1} \cdot \ldots \cdot r_{n+m}^{\gamma_{n+m}}$

$$r_i = \begin{cases} s_i & 1 \leq i \leq m \\ t_{n+m-i+1} & m < i \leq n+m \end{cases}$$

$$\gamma_i = \begin{cases} \alpha_i & 1 \leq i \leq m \\ -\beta_{n+m-i+1} & m < i \leq n+m \end{cases}$$

$\forall i \in \{1, \dots, n+m\}: r_i \in S$ a $j_i \in \{-1,1\} \Rightarrow r_1^{j_1} \dots r_{n+m}^{j_{n+m}} \in J \Rightarrow J \leq G$

Máme $K \supseteq J$ a $K \subseteq J \Rightarrow K = J$.

Úloha č. 2

a) $\langle\{12,18,22\}\rangle = \{x \in \mathbb{Z}_{24} : x = 12a + 18b + 22c \mid a, b \in \mathbb{Z}\}$

$= \{x \in \mathbb{Z}_{24} : x = 2 \cdot (6a + 9b + 11c) \mid a, b \in \mathbb{Z}\}$

Protože $GCD(11,9,6) = 1$ existují a, b, c takové, že $6a + 9b + 11c = 1$

$GCD(11,9,6) = GCD(GCD(11,9),6) = GCD(1,6) = 1$

$11 = 9 \cdot 1 + 2$

$9 = 2 \cdot 4 + 1$

$2 = 1 \cdot 2 + 0$

$\langle\{12,18,22\}\rangle = \{x \in \mathbb{Z}_{24} : x = 2n \mid n \in \mathbb{Z}\} = \langle 2 \rangle = \{0,2,4,\dots,22\}$

b) Nechť $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

Všimneme si, že $A^2 = I_3$ a $B^3 = I_3$. Potom platí, že

$\langle\{A,B\}\rangle = \{Q \in \mathbb{R}^{3\times3} : Q = A^i \times B^j \mid i \in \{1,2\}, j \in \{1,2,3\}\} \cup$

$\cup \{Q \in \mathbb{R}^{3\times3} : Q = B^j \times A^i \mid i \in \{1,2\}, j \in \{1,2,3\}\}$

Vypíšeme si všechny možnosti násobení matic:

$A \times B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ $\qquad B \times A = A \times B^2$

$A \times B^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\qquad \cancel{B \times A = B}$

$A \times B^3 = A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ $\qquad B^2 \times A = A \times B$

$A^2 \times B = B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ $\qquad B^2 \times A^2 = B^2$

$A^2 \times B^2 = B^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ $\qquad B^3 \times A = A$

$A^2 \times B^3 = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\qquad \cancel{B^3 \times A^2} = I_3$

$\langle\{A,B\}\rangle = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$

JAKUB LEVÝ

Úloha č. 3

$\Phi(\mathbb{Z}) \leq \mathbb{Z}_{1400}$. Podgrupy $\mathbb{Z}_{1400}$ velikosti 200 jsou isomorfní s $\mathbb{Z}_{200}$.
Hledáme tedy vlastně počet epimorfismů $\Psi : \mathbb{Z} \to \mathbb{Z}_{200}$.

$\mathbb{Z}$ je cyklická $\Rightarrow \mathbb{Z} = \langle g \rangle \Rightarrow \forall h \in \mathbb{Z} : g^n = h ,\ n \in \mathbb{N}_0 \Rightarrow \Phi(h) = \Phi(g^n) = \Phi(g)^n \Rightarrow$
$\Rightarrow$ homomorfismus je určen generátorem.

Aby se jednalo o epimorfismus musíme zajistit, že se generátor $\mathbb{Z}$ zobrazí na generátor $\mathbb{Z}_{200}$. Zbývá tedy zjistit kolik existuje generátorů $\mathbb{Z}_{200}$. Těch z přednášky víme, že odpovídá Eulerovy funkci.

$\varphi(200) = 1 \cdot 2^2 \cdot 4 \cdot 5 = \underline{80}$

$200 = 2 \cdot 100 = 4 \cdot 50 = 2 \cdot 2 \cdot 2 \cdot 25 = 2^3 \cdot 5^2$

Existuje 80 grupových homomorfismů $\Phi : \mathbb{Z} \to \mathbb{Z}_{1400}$ takových, že $|\Phi(\mathbb{Z})| = 200$