Řešení Zkoušky 1. termín – MIN401 – jaro 2022 – 21.6.2022

Příklad 1: [4 body] Uvažme permutace

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 2 & 1 & 9 & 8 & 6 & 5 \end{pmatrix},$$
$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 1 & 4 & 3 & 8 & 7 & 6 & 9 \end{pmatrix},$$
$$u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 4 & 6 & 3 & 7 & 5 & 9 & 2 \end{pmatrix}.$$

(i) Rozložte permutaci s na součin nezávislých cyklů.

(ii) Rozložte permutaci s na součin transpozic a určete její paritu.

(iii) Spočtěte t^{-1} a u^{211}.

(iv) Spočtěte $(s^{120} \circ t^{-3})^{17} \circ u^{23}$.

Řešení:

(i) $s = (1378695)(24)$.

(ii) $s = (13)(37)(78)(86)(69)(95)$. Permutace je sudá, protože počet transpozic v rozkladu je sudý.

(iii) Pro výpočet inverze stačí prohodit řádky a nový horní řádek seřadit:

$$t^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 5 & 4 & 1 & 8 & 7 & 6 & 9 \end{pmatrix}.$$

Máme rozklad $u = (1892)(34675)$. Číslo 211 dává zbytek 3, resp. 1 po dělení 4, resp. 5. Takže $u^{211} = (1298)(34675)$.

(iv) Platí $t^{-1} = (153)(68)$. Tedy $t^{-3} = (68)$. Stejně jako v předchozí části získáme $u^{23} = (1298)(37456)$ a $s^{120} = (1378695)$. Tedy $s^{120} \circ t^{-3} = (895137)$. Takže $(s^{120} \circ t^{-3})^{17} = (873159)$. Celkem tedy

$$(s^{120} \circ t^{-3})^{17} \circ u^{23} = (873159)(1298)(37456) = (12856)(497).$$

Příklad 2: [2 body] Ukažte, že množina $\{a+b\sqrt{3} \mid a,b \in \mathbb{Q}, a^2+b^2>0\}$ je podgrupa grupy $(\mathbb{R}\setminus\{0\},\cdot)$.
Řešení: Označme množinu ze zadání M. Zřejmě $1 = 1+0\sqrt{3} \in M$. Nechť $a+b\sqrt{3} \in M$. Potom

$$\frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{(a+b\sqrt{3})(a-b\sqrt{3})} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} + \frac{-b}{a^2-3b^2}\sqrt{3} \in M.$$

Všimněme si, že $a^2-3b^2 \neq 0$, protože $\sqrt{3}$ je iracionální. Navíc nemůže nastat, že by oba zlomky byli nulové, protože nemohou být a,b zároveň obě nulové. Nyní, nechť $a+b\sqrt{3} \in M$ a $c+d\sqrt{3} \in M$. Potom

$$(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd)+(bc+ad)\sqrt{3} \in M.$$

Vskutku, pro spor nechť $ac+3bd = bc+ad = 0$. Víme, že $c \neq 0$ nebo $d \neq 0$. Nechť $d \neq 0$, tedy $-\frac{bc}{d}c+3bd = 0$, takže $\frac{b(c^2-3d^2)}{d} = 0$. Z iracionality $\sqrt{3}$ plyne tedy $b=0$. Takže $ac = ad = 0$. Víme, že $a \neq 0$ (protože $b=0$), tedy $c=d=0$, což je spor s $d \neq 0$. Analogicky vede $c \neq 0$ ke sporu.

Příklad 3: [2 body] Pro následující dva předpisy rozhodněte zda se jedná o zobrazení, homomorfismus, zda je injektivní, surjektivní, a určete jádro a obraz.

(i) $f\colon (\mathbb{Z}_3\setminus\{[0]_3\},\cdot)\times(\mathbb{Z}_5,+) \to (\mathbb{Z}_5,+)$, $f([a]_3,[b]_5) = [b^{|a|}]_5$ pro $a,b \in \mathbb{Z}$.

(ii) $g\colon (\mathbb{Z}_{15},+) \to (\mathbb{Z}_5,+)\times(\mathbb{Z}_3,+)$, $g([a]_{15}) = ([a]_5,[a]_3)$ pro $a \in \mathbb{Z}$.

Řešení:

(i) Není to ani zobrazení, protože například $[2^1]_5 \neq [2^4]_5$.

(ii) Jedná se o zobrazení, protože $g([a+15k]_{15}) = ([a+15k]_5,[a+15k]_3) = ([a]_5,[a]_3) = g([a]_{15})$ pro všechna $a,k \in \mathbb{Z}$. Dokonce se jedná i o homomorfismus, protože

$$g([a]_{15}+[b]_{15}) = g([a+b]_{15}) = ([a+b]_5,[a+b]_3) = ([a]_5,[a]_3)+([b]_5,[b]_3) = g([a]_{15})+g([b]_{15}).$$

Jádro je zřejmě $\{[0]_{15}\}$ a obraz je $(\mathbb{Z}_5,+)\times(\mathbb{Z}_3,+)$. Je to tedy injektivní i surjektivní homomorfismus.

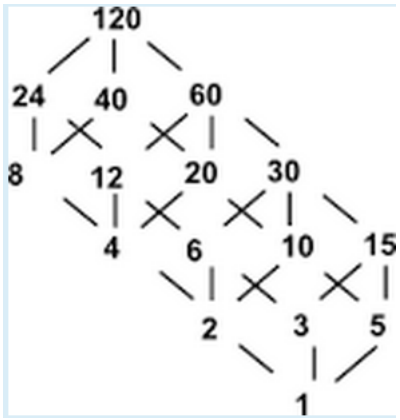
Příklad 4: [2 body] Určete všechny $a \in \mathbb{Q}$ takové, že polynom $f = x^5-ax^2-ax+1 \in \mathbb{Q}[x]$ má dvojnásobný kořen -1.
Řešení: Derivace zadaného polynomu je $5x^4-2ax-a$. Dosazením $x=-1$ a položením derivace rovno nule zjistíme, že $5+2a-a=0$, tedy $a=-5$. Jediné možné $a \in \mathbb{Q}$ splňující zadání je tedy $a=-5$, a opravdu dosazením -1 do x^5+5x^2+5x+1 a $5x^4+10x+5$ zjistíme, že $x=-1$ je vskutku kořen těchto dvou polynomů. Tedy hledané $a \in \mathbb{Q}$ je právě $a=-5$.

Příklad 5: [4 body] Určete všechny ireducibilní polynomy nad $\mathbb{Z}_2$ stupně menšího než 5.
Řešení: Jsou to právě polynomy

$$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4, +x+1, x^4+x^3+1, x^4+x^3+x^2+x+1.$$

Vskutku, u polynomů stupně menšího než 4 můžeme o ireducibilitě rozhodnout podle toho jestli mají kořen (V $\mathbb{Z}_2$ stačí vyzkoušet dva potenciální kořeny $[0]_2$, $[1]_2$). U polynomů stupně 4 můžeme rozhodnout pomocí existence kořenů a vyloučením všech součinů dvojic kvadratických ireducibilních polynomů, takový polynom je ovšem pouze jeden, tedy jediný takový polynom, který vyloučíme, je $(x^2+x+1)^2 = x^4+x^2+1$.

Příklad 6: [2 body] Nakreslete Hasseho diagram svazu kladných dělitelů čísla 120.
Řešení: (Obrázek převzat ze stackexchange vlákna.)



Příklad 7: [4 body] Uvažme lineární (11,7)-kód generovaný polynomem $1+x^3+x^4$.

(i) Určete generující matici a matici kontroly parity.

(ii) Dekódujte slovo 00000100100 za předpokladu, že došlo k nejmenšímu množství chyb.

Řešení:

(i) Pomocí algoritmu ze cvičení najdeme generující matici

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Z tohoto ihned vidíme i matici kontroly parity

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

(ii) Vypočteme $G \cdot (0100100)^T = (10100100100)^T$. Chyba je 10100000000. Přičtením kombinací alespoň dvou sloupců bychom určitě stále měli chybu alespoň s dvěma jedničkama. Zmenšit chybu lze tedy pouze potenciálně pomocí přičtení nějakého sloupce. Je ihned vidět, že jediný sloupec, který zmenší chybu je šestý sloupec, a přičtením tohoto sloupce dostaneme chybu 00000000010. Poslaná zpráva byla tedy 00000100110, a informační část této zprávy je 0100110.