Martin Števko

MFF UK, Informatika, 1. ročník

Úloha 1.

Nutnými postačujúcimi podmienkami sú z dafinície tieto 3:

1. $\forall a, b \in H : a \circ b \in H$
2. $\forall a \in H : a^{-1} \in H$
3. $e \in H$

(Podmienku o asociativite dokazovať nemusíme, keďže tá vyplýva priamo z faktu, že ide o podmnožinu a rovnakú operáciu než v grupe, kde táto podmienka platí.)

Najprv dokážem implikáciu, kedy predpokladám, že ide o podgrupu. Viem teda, že platí

$$\forall a, b \in H : a, b^{-1} \in H \wedge a \circ b \in H \Rightarrow a \circ b^{-1} \in H$$

čo som chcel dokázať.

Pozrime sa teraz na opačnú implikáciu. Viem, že

$$\forall a, b \in H : a \circ b^{-1} \in H$$

Na dokázanie 3. podmienky si zoberme $a = b$. Potom platí

$$a \circ b^{-1} \in H \Leftrightarrow a \circ a^{-1} \in H \Leftrightarrow e \in H$$

Na dokzanie 2. podmienky si zoberme $a = e$ ($e \in H$ už viem), potom

$$\forall b \in H : e \circ b^{-1} \in H \Leftrightarrow b^{-1} \in H$$

čo som chcel dokázať. Nakoniec si zvoľme ľubovoľné x také, že $x \in H$. Potom nech $b = x^{-1}$, pričom $b \in H$ podľa už dokázanej podmienky 2. Z predpokladu teda viem

$$\forall a \in H : a \circ b^{-1} \in H$$

čo po dosadení bude

$$\forall a \in H : a \circ x \in H$$

Naviac ale viem, že x som si zvolil ľubovoľne z množiny H, takže podmienka musí platiť pre všetky x, čiže viem povedať

$$\forall a, x \in H : a \circ x \in H$$

čo už je ekvivalentné prvej podmienke. Tým sú všetky 3 dokázané, takže skutočne ide o podgrupu grupy G.

Martin Števko

MFF UK, Informatika, 1. ročník

Úloha 2.

Na to aby som dokázal, že ide o podgrupu potrebujem dokázať 3 veci:

- $\forall a, b \in H : a \circ b \in H$
- $\forall a \in H : a^{-1} \in H$
- $e \in H$

Podmienku o asociativite dokazovať nemusíme, keďže tá vyplýva priamo z faktu, že ide o podmnožinu a rovnakú operáciu než v grupe, kde táto podmienka platí.

Keďže H_1 a H_2 sú podgrupy, platí

$$e \in H_1 \wedge e \in H_2 \Rightarrow e \in H_1 \cap H_2$$

takisto platí

$$\forall a \in H_1 : a^{-1} \in H_1 \wedge \forall a \in H_2 : a^{-1} \in H_2 \Rightarrow \forall a \in H_1 \cap H_2 : a^{-1} \in H_1 \cap H_2$$

a tiež

$$\forall a, b \in H_1 : a \circ b \in H_1 \wedge \forall a, b \in H_2 : a \circ b \in H_2 \Rightarrow \forall a, b \in H_1 \cap H_2 : a \circ b \in H_1 \cap H_2$$

pretože

$$x \in H_1 \wedge x \in H_2 \Leftrightarrow x \in H_1 \cap H_2$$

Tým som ale dokázal všetky 3 podmienky.

Martin Števko

MFF UK, Informatika, 1. ročník

Úloha 3.

Začnem s výpočtom inverznej matice v $\mathbb{Z}_3$.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Pričítam 1. riadok k 2. a 3. raz a ku 4. dvakrát.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 \end{array}\right)$$

3. riadok dám na 2. miesto, 2. na 4. miesto a ku pôvodnému 4. pripočítam pôvodný 3. a dám ho na 3. miesto.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 \end{array}\right)$$

4. riadok najprv pričítam k 1. a 2. a potom k nemu pričítam 3. riadok.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 \end{array}\right)$$

4. riadok vynásobim dvomi.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 2 & 2 & 2 \end{array}\right)$$

Na ľavej strane sme dostali jednotkovú maticu, takže tá na strane pravej bude inverzná k matici v zadaní. Pre skúšku môžeme matice v $\mathbb{Z}_3$ vynásobiť a skutočne dostaneme jednotkovú, takže sú inverzné.

Teraz vypočítam inverznú maticu v $\mathbb{Z}_5$.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

1. riadok odpočítam od 2. a 3. dvakrát a od 4. raz.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 4 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 3 & 3 & 0 & 1 & 0 \\ 0 & 2 & 0 & 4 & 4 & 0 & 0 & 1 \end{array}\right)$$

Najprv k 1. riadku pripočítam 2. a potom dám 3. riadok na 2. miesto, 2. na 4. miesto a 4. na 3. miesto.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 3 & 3 & 3 & 0 & 1 & 0 \\ 0 & 2 & 0 & 4 & 4 & 0 & 0 & 1 \\ 0 & 0 & 4 & 4 & 3 & 1 & 0 & 0 \end{array}\right)$$

Od 3. riadku dvakrát odpočítam 2. a 4. vynásobím štyroma.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 3 & 3 & 3 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 3 & 0 & 3 & 1 \\ 0 & 0 & 1 & 1 & 2 & 4 & 0 & 0 \end{array}\right)$$

K 2. a 3. riadku pripočítam dvojnásobok 4. riadku a následne od 4. riadku odpočítam nový 3. riadok.

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 3 & 3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 4 \end{array}\right)$$

Na ľavej strane sme znova dostali jednotkovú maticu, takže tá na strane pravej bude inverzná k matici v zadaní. Pre skúšku môžeme matice v $\mathbb{Z}_5$ vynásobiť a skutočne dostaneme jednotkovú, takže sú inverzné.