**1. kolokvij iz Algebre 2 - Rešitve**

2. 12. 2011

1. Na množici $A = \mathbb{Z} \times \mathbb{Z}$ je dana operacija $\circ$ s predpisom
$$(m, n) \circ (m', n') = (m + m', n + (-1)^m n'), \quad m, m', n, n' \in \mathbb{Z}.$$
Pokaži, da je $(A, \circ)$ grupa, ki ni Abelova.

   Rešitev: Preverimo asociativnost, obstoj enote $(0, 0)$ in obstoj inverza. Zaprtosti operacije ni potrebno preverjati (v nalogi je bila dana binarna operacija; če je množica opremljena z binarno operacijo, potem je tudi avtomatično zaprta za to operacijo). Dokaz, da ni Abelova: poiščemo 2 elementa, ki ne komutirata, npr. $(1, 0)\circ(0, 1) = (1, -1)$ in $(0, 1) \circ (1, 0) = (1, 1) \neq (1, 0) \circ (0, 1)$.

2. Naj bo $G = (\mathbb{C}\backslash\{0\}, \cdot)$ in $H = \{z \in G, |z| = 1\}$. Pokaži, da je $H$ podgrupa edinka v $G$. Kateri znani grupi je izomorfna grupa $G/H$?

   Rešitev: Preverimo, da je $H$ podgrupa: $x, y \in H \Rightarrow |xy^{-1}| = |x \cdot \frac{1}{y}| = \frac{|x|}{|y|} = \frac{1}{1} = 1 \Rightarrow xy^{-1} \in H$. Ker je $G$ Abelova, je potem tudi $H \triangleleft G$.

   Dokaz, da je $G/H \cong (\mathbb{R}^+, \cdot)$: Poiščemo surjektivni homomorfizem $f : G \to \mathbb{R}^+$ z jedrom $H$. Definiramo $f(z) = |z|$. $f$ je homomorfizem, saj $f(zw) = |zw| = |z||w| = f(z)f(w)$. $f$ je surjektiven, saj $a \in \mathbb{R}^+ \Rightarrow f(a) = |a| = a \Rightarrow a \in \mathrm{im}(f)$. Jedro $f$ je $\{z \in G, f(z) = 1\} = \{z \in G, |z| = 1\} = H$. (Niti ne bi bilo treba preverjati, da je $H$ podgrupa edinka, saj to sledi iz tega, da je $H = \ker(f)$.)

3. Naj bo $G$ grupa in $H$ njena podgrupa edinka. Pokaži, da je $Z(H) \triangleleft G$.

   Rešitev: Očitno je $Z(H) \leq G$, saj $Z(H) \leq H$. Pokažimo, da je $Z(H) \triangleleft G$. Naj bo $g \in G$ in $z \in Z(H)$. Preverjamo $gzg^{-1} \in Z(H)$. Najprej vidimo, da je $gzg^{-1} \in H$, saj je $H \triangleleft G$ in $z \in H$. Pokazati moramo še, da velja $gzg^{-1}h = hgzg^{-1}$ za poljuben $h \in H$. Ker je $H \triangleleft G$, je $g^{-1}hg \in H$. Ker je $z \in Z(H)$, je potem $gzg^{-1}h = gz(g^{-1}hg)g^{-1} = g(g^{-1}hg)zg^{-1} = hgzg^{-1}$. QED.

4. Določi grupo avtomorfizmov grupe $\mathbb{Z} \times \mathbb{Z}_2$.

   Rešitev: Naj bo $f \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}_2)$. Ker sta $(1, 0)$ in $(0, 1)$ generatorja grupe $\mathbb{Z} \times \mathbb{Z}_2$, je $f$ natanko določen s slikama generatorjev $f(1, 0)$ in $f(0, 1)$, saj je potem $f(a, b) = f(a, 0) + f(0, b) = f(1, 0) + \ldots + f(1, 0) + f(0, 1) + \ldots + f(0, 1) = af(1, 0) + bf(0, 1)$ (na drugi komponenti operacijo + seveda gledamo po modulu 2). Ker $f$ ohranja red elementov in je $(0, 1)$ reda 2, je tudi $f(0, 1)$ reda 2; edini element reda 2 v grupi $\mathbb{Z} \times \mathbb{Z}_2$ je $(0, 1)$, torej je $f(0, 1) = (0, 1)$. Pogledamo še, katere so možnosti za $f(1, 0)$.

   Označimo $f(1, 0) = (m, n)$. Če je $m = 0$, $f$ ne bo surjektiven, saj bo $\mathrm{im}(f) \leq \{0\} \times \mathbb{Z}_2$. Če bo $|m| \geq 2$, $f$ spet ne bo surjektiven, saj bo $\mathrm{im}(f) \leq m\mathbb{Z} \times \mathbb{Z}_2$. Torej je $m = 1$ ali $m = -1$. Ker imamo tudi za $n$ 2 možnosti (0 ali 1), imamo skupaj kvečjemu 4 možnosti, $f(1, 0) \in \{(1, 0), (1, 1), (-1, 0), (-1, 1)\}$. Dobimo štiri homomorfizme $f_1(a, b) = (a, b)$, $f_2(a, b) = (a, a + b)$, $f_3(a, b) = (-a, b)$ in $f_4(-a, a + b)$. Prvi je identiteta, ostali pa imajo red 2 (preverimo $f_i(f_i(a, b)) = (a, b)$ za $i = 2, 3, 4$), od koder tudi sledi, da so vsi bijektivni (torej avtomorfizmi). Grupa $\mathrm{Aut}(\mathbb{Z}\times\mathbb{Z}_2)$ ima tako 4 elemente, vsi razen enote pa so reda 2, torej $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}_2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

5. Naj bo $G$ enostavna grupa moči 168 (grupa je enostavna, če ne vsebuje nobene prave netrivialne podgrupe edinke). Koliko elementov reda 7 je v grupi $G$?

   Rešitev: Razcepimo $168 = 2^3 \cdot 3 \cdot 7$. Z izreki Sylowa preverimo, da v $G$ obstaja natanko 1 ali 8 podgrup Sylowa z močjo 7. Ker je $G$ enostavna, je takih grup potem 8. Ker so praštevilske moči, so te grupe paroma disjunktne, torej skupaj premorejo $7 + 7 \cdot 6 = 49$ elementov. Vsi razen enote so reda 7, torej imamo 48 elementov reda 7. To so tudi vsi elementi reda 7 v $G$ (če bi bil $x$ še kak drug element reda 7 v $G$, ki bi bil zunaj teh osmih podgrup Sylowa, bi bila $< x >$ podgrupa moči 7, torej bi bila enaka eni od osmih podgrup Sylowa, kar je protislovje).