**Izpit iz Algebre 2, 11. 5. 2012 – Rešitve**

1. Naj bosta $G_1$ in $G_2$ grupi in $H_i \triangleleft G_i$ podgrupi edinki za $i = 1, 2$. Pokaži: $H_1 \times H_2 = \{(h_1, h_2);\ h_i \in H_i\}$ je podgrupa edinka grupe $G_1 \times G_2$ in velja $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$.

   *Rešitev:* Definirajmo preslikavo

   $$f : G_1 \times G_2 \to (G_1/H_1) \times (G_2/H_2), \quad f(g_1, g_2) = (g_1H_1, g_2H_2).$$

   Ta preslikava je homomorfizem grup, saj je

   $$f((g_1, g_2)(g_1', g_2')) = f(g_1g_1', g_2g_2') = (g_1g_1'H_1, g_2g_2'H_2) =$$
   $$= (g_1H_1, g_2H_2)(g_1'H_1, g_2'H_2) = f(g_1, g_2)f(g_1', g_2')$$

   za poljubne $g_i, g_i' \in G_i$. Očitno je $f$ surjektivna, njeno jedro pa je točno $\ker(f) = \{(g_1, g_2);\ g_1 \in H_1, g_2 \in H_2\} = H_1 \times H_2$. Torej je $H_1 \times H_2$ podgrupa edinka v $G_1 \times G_2$, po izreku o izomorfizmu pa je $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$.

2. Naj bo $G$ grupa moči 585. Pokaži, da v njej obstaja podgrupa edinka moči 65. (Nasvet: najprej pokaži, da v $G$ obstajata podgrupi edinki moči 5 in 13.)

   *Rešitev:* S pomočjo izrekov Sylowa pokažemo, da v $G$ obstaja podgrupa edinka $H$ moči 5 in podgrupa edinka $K$ moči 13. Potem je po znanem izreku $HK$ spet podgrupa edinka. Pokažimo še, da je $|HK| = 65$. Ker je $H \cap K = 1$ (saj sta grupi $H$ in $K$ tujih moči), je $|HK|/|K| = |HK/K| = |H/(H \cap K)| = |H|$, torej $|HK| = |H| \cdot |K| = 65$.

3. Naj bo $K$ komutativen kolobar z enoto, ki ima natanko 3 ideale: 0, $I$ in $K$. Pokaži:

   (a) Vsak $a \in K \backslash I$ je obrnljiv v $K$.

   (b) Za vsaka dva $a, b \in I$ velja $ab = 0$.

   *Rešitev:*

   (a) Naj bo $a \in K$, $a \notin I$. Ideal $(a) = Ka$ je po predpostavki enak 0, $I$ ali $K$. Prvi dve možnosti odpadeta, saj je $a \notin I$. Torej je $Ka = K$ in zato obstaja tak $r \in K$, da je $ra = 1$. Ker smo v komutativnem kolobarju, je potem $a$ obrnljiv.

   (b) Naj bo $a, b \in I$ in denimo, da je $ab \neq 0$. Potem je $(ab) = Kab = I$ (ideal $Kab$ ne more biti enak 0, saj $ab \neq 0$, niti $K$, saj $Kab \subseteq I$). Torej obstaja tak $r \in K$, da je $rab = a$. Odtod dobimo $a(1 - rb) = 0$. Element $1 - rb$ je zunaj $I$, saj bi sicer bilo $1 \in I$. Torej je po točki (a) $1 - rb$ obrnljiv v $K$ in zato iz $a(1 - rb) = 0$ sledi $a = 0$, kar je protislovje.

4. Naj bo $K$ cel kolobar z enoto in $f(X)$ polinom v $K[X]$. Pokaži: če je $f(X)$ obrnljiv v $K[X]$, potem je oblike $f(X) = a$ za nek obrnljiv $a \in K$. Poišči še protiprimer za primer, ko $K$ ni cel (to je, poišči necel kolobar z enoto $K$ in obrnljiv polinom $f(X) \in K[X]$, ki ni oblike $f(X) = a$).

   *Rešitev:* Če je $K$ cel kolobar, potem se stopnje polinomov v $K[X]$ z množenjem seštevajo. Če sta torej $f$ in $g$ polinoma s produktom $f(X)g(X) = 1$, potem imata $f$ in $g$ stopnjo

0, to je $f(X) = a$ in $g(X) = b$ za neka $a, b \in K$. Iz enakosti $f(X)g(X) = 1$ dobimo $ab = 1$, iz enakosti $g(X)f(X) = 1$ pa $ba = 1$. Torej je $a$ obrnljiv v $K$.

Če $K$ ni cel, sklep ne drži. Res, polinom $f(X) = 1 + 2X \in \mathbb{Z}_4[X]$ je obrnljiv (njegov inverz je kar $f$), ni pa oblike $f(X) = a$.

5. Naj bo $K$ podkolobar racionalnih števil z lihim imenovalcem, to je

$$K = \{\frac{m}{n} \in \mathbb{Q};\ \frac{m}{n} \text{ okrajšani ulomek, } n \text{ lih}\}.$$

Pokaži, da je $K$ res podkolobar s standardnim seštevanjem in množenjem. Pokaži, da je (2) maksimalni ideal tega kolobarja.

*Rešitev*: Da bo $K$ podkolobar, moramo preveriti zaprtost za odštevanje in množenje. Za poljubna $\frac{m}{n}, \frac{m'}{n'} \in K$ velja $\frac{m}{n} - \frac{m'}{n'} = \frac{mn'-m'n}{nn'} \in K$ (ta ulomek ima lih imenovalec, saj sta $n$ in $n'$ liha) in $\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'} \in K$ (tudi ta ulomek ima lih imenovalec). (Tudi če se ulomka okrajšata, ostaneta imenovalca liha.) Torej je $K$ res podkolobar. (Seveda je $K$ tudi komutativen in ima enoto 1.)

Preverimo, da je $I = (2)$ maksimalni ideal v $K$. Najprej vidimo, da je $I \neq K$. Res, sicer bi bilo $1 \in (2) = 2K$, torej bi obstajal $\frac{m}{n} \in K$, da bi bilo $1 = 2 \cdot \frac{m}{n}$, in bi bil zato $n$ sod, kar je protislovje.

Pokažimo še maksimalnost. Pa denimo, da je $I \subsetneq J$ za nek ideal $J \lhd K$. Potem obstaja $q = \frac{m}{n} \in J \backslash I$. Ulomek $\frac{m}{n}$ ima lih imenovalec (ker je v $K$) in tudi lih števec (saj bi sicer bilo $m = 2k$, od koder bi dobili $q = 2 \cdot \frac{k}{n} \in (2) = I$, kar je protislovje). Torej je $\frac{n}{m} \in K$ in je $q$ obrnljiv v $K$ (z inverzom $\frac{n}{m}$). Torej ideal $J$ vsebuje obrnljiv element in zato $J = K$.