2. kolokvij iz Algebre 2 - Rešitve
20. 1. 2012

1. Poišči vse neizomorfne Abelove grupe moči 200.

   Rešitev: Vsaka končna Abelova grupa je do izomorfizma natančno enaka $\mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}$, kjer so p_i praštevila, ki delijo moč grupe. Ta zapis je enoličen do vrstnega reda faktorjev natančno. Če torej razcepimo $200 = 2^3 \cdot 5^2$, potem imamo 6 možnosti: $\mathbb{Z}_8 \times \mathbb{Z}_{25}$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

2. Naj bo D (ne nujno komutativen) obseg in $K \leq D$ takšen podkolobar, da je $x \in K$ ali $x^{-1} \in K$ za vsak $x \in D \backslash \{0\}$. Pokaži, da velja $I \subseteq J$ ali $J \subseteq I$ za poljubna ideala I, J kolobarja K.

   Rešitev: Naj bosta I, J ideala kolobarja K in naj bo $J \nsubseteq I$. Pokazati moramo $I \subseteq J$. Vzemimo poljuben $x \in I$. Lahko predpostavimo $x \neq 0$. Ker je $J \nsubseteq I$, obstaja tak $a \in J$, da $a \notin I$. Ker je $a \notin I$, je $a \neq 0$. Ker je $x(x^{-1}a) = a \notin I$, je $x^{-1}a \notin K$. Torej je $x^{-1}a \neq 0$ in $(x^{-1}a)^{-1} = a^{-1}x \in K$ in zato $x = a(a^{-1}x) \in J$. Torej je res $I \subseteq J$.

3. Naj bosta K_1 in K_2 kolobarja z enico in $K = K_1 \times K_2$ kolobar z operacijama po komponenetah. Pokaži, da je vsak ideal v kolobarju K oblike $I_1 \times I_2$, kjer je I_i ideal v K_i za $i = 1, 2$.

   Rešitev: Naj bo $I \triangleleft K$ poljuben ideal. Definirajmo množici $I_1 = \{x \in K_1, (x, 0) \in I\}$ in $I_2 = \{y \in K_2, (0, y) \in I\}$. Množici I_1, I_2 sta ideala v K_1 oziroma K_2. Res, če je $x, x' \in I_1$, je $(x - x', 0) = (x, 0) - (x', 0) \in I$, torej $x - x' \in I_1$. Če vzamemo še $r \in K_1$, je $(rx, 0) = (r, 0)(x, 0) \in I$ in $(xr, 0) = (x, 0)(r, 0) \in I$, torej $rx, xr \in I_1$. Torej je I_1 res ideal v K_1. Podobno preverimo, da je tudi I_2 ideal v K_2.

   Pokažimo še $I = I_1 \times I_2$. Če je $(x, y) \in I$, je $(x, 0) = (x, y)(1, 0) \in I$, torej $x \in I_1$. Podobno vidimo, da je $y \in I_2$. Torej je $(x, y) \in I_1 \times I_2$. Obratno, če je $x \in I_1$ in $y \in I_2$, je $(x, 0) \in I$ in $(0, y) \in I$, torej $(x, y) = (x, 0) + (0, y) \in I$. S tem je enakost pokazana.

4. Naj bo K cel komutativen kolobar z enico, ki ni obseg. Pokaži, da $K[X]$ ni glavni kolobar. (Nasvet: izberi neobrnljiv element $a \in K$, $a \neq 0$, in pokaži, da ideal (a, X) ni glavni ideal v $K[X]$.)

   Rešitev: Naj bo $a \in K$, $a \neq 0$ neobrnljiv element in $I = (a, X)$. Pokažimo, da I ni glavni ideal v $K[X]$. Pa denimo nasprotno, da je $I = (p(X))$ za nek polinom $p(X)$. Ker je $a \in I$, je $a = p(X)q(X)$ za nek polinom $q(X)$. Od tod sledi, da sta $p(X)$ in $q(X)$ polinoma stopnje 0. Pišimo $p(X) = c$ za nek $c \in K$. Ker je $X \in I$, je $X = p(X)r(X) = cr(X)$ za nek polinom $r(X)$. Od tod sledi, da je polinom $r(X)$ oblike $r(X) = dX$ in $cd = 1$, torej je $c = p(X)$ obrnljiv element. Torej je $I = K[X]$ in zato $1 \in I$ oziroma $1 = a\alpha(X) + X\beta(X)$ za neka polinoma $\alpha(X), \beta(X)$. To pa pomeni, da je a obrnljiv element v K, kar je protislovje. Torej I ni glavni ideal.

5. Naj bosta m in n naravni števili z lastnostjo $\varphi(mn) = \varphi(m)\varphi(n)$. Pokaži, da sta m in n tuji si števili.

   Rešitev: Uporabimo formulo $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ (p preteče vsa praštevila, ki delijo n).

Iz enakosti $\varphi(mn) = \varphi(m)\varphi(n)$ dobimo $mn \prod_{p|mn}(1-\frac{1}{p}) = mn \prod_{p|m}(1-\frac{1}{p}) \prod_{p|n}(1-\frac{1}{p})$, torej

$$\prod_{p|mn}(1-\frac{1}{p}) = \prod_{p|m}(1-\frac{1}{p}) \prod_{p|n}(1-\frac{1}{p}).$$

Leva stran te enakosti je produkt vseh izrazov $1-\frac{1}{p}$, ko p preteče praštevila, ki delijo mn. Desna stran je enaka levi, le da se za praštevila, ki delijo tako m kot n, faktorji $1-\frac{1}{p}$ pojavijo dvakrat. Ko torej krajšamo obe strani enačbe, dobimo $1 = \prod_{p|m \text{ in } p|n}(1-\frac{1}{p})$. Ker so vsa števila $1-\frac{1}{p}$ manjša od 1, je torej $\{p,\ p|m \text{ in } p|n\}$ prazna množica. Torej sta m in n tuji si števili.