Vaje 1

1. Naj bo X neprazna množica. Potenčno množico $P(X)$ opremimo z operacijo $\setminus$ (brez). Pokaži, da $(P(X), \setminus)$ ni polgrupa.

2. Na množici $\mathbb{C}$ je dana operacija $\circ$ s predpisom $a \circ b = a + b + ab$. Pokaži, da je $\mathbb{C}$ za to operacijo komutativen monoid. Ali je tudi grupa?

3. Dana je polgrupa $(\{f : \mathbb{R} \to [0,1]\}, \circ)$. Poišči leve in desne enote v tej polgrupi.

4. Pokaži, da je vsaka grupa moči 4 Abelova.

5. Pokaži, da je $\{\left[\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right] \mid x, y \in \mathbb{R},\ x \neq 0\}$ grupa za operacijo matrično množenje. Ali je Abelova?

6. Pokaži, da je $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q},\ a^2 + b^2 \neq 0\}$ grupa za množenje.

7. Naj bo G grupa, v kateri velja $a^2 = e$ za vsak $a \in G$. Pokaži, da je G Abelova.

8. Naj bosta $(G, \cdot)$ in $(H, \cdot)$ grupi. Množico $G \times H$ opremimo z operacijo $\circ$ s predpisom $(g_1, h_1) \circ (g_2, h_2) = (g_1 g_2, h_1 h_2)$. Pokaži, da je $G \times H$ s to operacijo grupa.

9. Izračunaj
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 7 & 5 & 1 & 3 & 8 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix}.$$
Zapiši rezultat kot produkt disjunktnih ciklov.

10. Naj bo
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 6 & 2 & 8 & 4 & 9 & 5 & 1 \end{pmatrix}.$$
Izračunaj π^{-1} in π^{2012}.

11. Pokaži, da je $\{\left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right] \mid x \in \mathbb{R}\}$ grupa za operacijo matrično množenje. Kateri znani grupi je izomorfna?

Vaje 2

1. Naj bo dana grupa $G = M_2(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{R}\}$ z operacijo seštevanje po komponentah. Pokaži, da je množica $H = \{A \in G \mid \mathrm{sled}(A) = 0\}$ podgrupa v G.

2. Naj bo $f : G \to G'$ homomorfizem grup in $H \leq G$. Pokaži, da je $f(H) \leq G'$.

3. Določi vse podgrupe grupe $\mathbb{Z}$.

4. Poišči vse homomorfizme grup $\mathbb{Z} \to \mathbb{Q}$.

5. Naj bo $n \geq 2$. Pokaži, da ne obstaja neničeln homomorfizem grup $\mathbb{Z}_n \to \mathbb{Q}$.

6. Pokaži, da ne obstaja neničeln homomorfizem grup $\mathbb{Q} \to \mathbb{Z}$.

7. Pokaži, da je $Z(GL_2(\mathbb{R})) = \mathbb{R} \cdot \mathrm{id}$.

8. Naj bo H prava podgrupa grupe G (to je, $H \leq G$ in $H \neq G$). Pokaži, da je $\langle G \backslash H \rangle = G$.

Vaje 3

1. Določi vse končno generirane podgrupe grupe $\mathbb{Q}$.
2. Pokaži, da grupi $\mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$ nista izomorfni.
3. Poišči vse neizomorfne grupe moči 4.
4. Naj bo p praštevilo. Koliko podgrup ima grupa $\mathbb{Z}_p \times \mathbb{Z}_p$?
5. Naj bo G Abelova grupa in $H = \{x \in G | \operatorname{red}(x) < \infty\}$. Pokaži, da je $H \leq G$.
6. Pokaži, da grupi $(\mathbb{R}, +)$ in $(\mathbb{R}\backslash\{0\}, \cdot)$ nista izomorfni.
7. Naj bo G končna grupa in n naravno število, tuje proti $|G|$. Pokaži, da za vsak $x \in G$ obstaja $y \in G$, da je $y^n = x$.
8. Določi maksimalni red elementov v grupi S_6.
9. Določi grupo $\operatorname{Aut}(\mathbb{Z}_8)$.
10. Naj bo G grupa in $H, K \leq G$. Definiraj preslikavo $H/(H \cap K) \to G/K$, $x(H \cap K) \mapsto xK$.
    (a) Pokaži, da je ta preslikava dobro definirana in injektivna. Odtod sklepaj, da je $[H : H \cap K] \leq [G : K]$.
    (b) Pokaži, da je preslikava bijektivna natanko tedaj, ko je $G = KH$.
    (c) S pomočjo točke (a) pokaži, da je $[G : H \cap K] \leq [G : H][G : K]$. Posebej, če je $[G : H], [G : K] < \infty$, je $[G : H \cap K] < \infty$.

Vaje 4

1. Poišči vse podgrupe edinke grupe S_3.

2. Naj bo $f : G \to G'$ homomorfizem grup. Pokaži:

   (a) Če je $H \triangleleft G'$, je $f^{-1}(H) \triangleleft G$.

   (b) Če je $H \triangleleft G$ in je f surjektivna, je $f(H) \triangleleft G'$.

   Ali točka (b) še velja, če f ni surjektivna?

3. Naj bo $f : G \to H$ homomorfizem grup z jedrom $N = \ker(f)$ in naj bo $K \leq G$. Pokaži, da je $f^{-1}(f(K)) = KN$.

4. Naj bo G grupa, $\mathrm{Aut}(G)$ grupa avtomorfizmov in $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ množica vseh notranjih avtomorfizmov, to je $\mathrm{Inn}(G) = \{\varphi_a : G \to G \mid \varphi_a(g) = aga^{-1},\ a \in G\}$. Pokaži, da je $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

5. Naj bo $G = (M_2(\mathbb{Z}), +)$ in $H = \{A \in G \mid \mathrm{sled}(A) = 0\}$. Pokaži, da je H podgrupa edinka v G in $G/H \cong \mathbb{Z}$.

6. Naj bo $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ enotska krožnica v kompleksni ravnini, ki je grupa za množenje. Pokaži, da je $S^1 \cong \mathbb{R}/\mathbb{Z}$, pri čemer sta $\mathbb{R}$ in $\mathbb{Z}$ grupi za seštevanje.

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

8. Naj bosta G, G' grupi, $H \triangleleft G$ in $H' \triangleleft G'$. Pokaži, da je $H \times H'$ podgrupa edinka v $G \times G'$ (z operacijo množenje po komponentah) in $(G \times G')/(H \times H') \cong (G/H) \times (G'/H')$.

9. (a) Pokaži, da je množica vseh sodih permutacij A_n podgrupa edinka v S_n.

   (b) Naj bo G podgrupa v S_n, ki vsebuje vsaj eno liho permutacijo. Pokaži, da v G obstaja podgrupa edinka indeksa 2.

Vaje 5

1. Diedrska grupa D_{2n} je definirana kot podgrupa grupe S_n (za $n > 2$), generirana s permutacijama

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} \quad \text{in} \quad \rho = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & n & \dots & 3 & 2 \end{pmatrix}.$$

   (a) Pokaži da lahko vsak element iz D_{2n} enolično zapišemo kot $\pi^i \rho^j$, kjer je $i \in \{0, \dots, n-1\}$ in $j \in \{0, 1\}$. Od tod sklepaj, da je $|D_{2n}| = 2n$.

   (b) Naj bo p liho praštevilo. Pokaži, da ima grupa $\mathrm{Aut}(D_{2p})$ kvečjemu $p(p-1)$ elementov. (Nasvet: avtomorfizmi ohranjajo red.)

2. Pokaži, da je $Z(S_n)$ trivialna grupa za $n \geq 3$.

3. Poišči vse podgrupe grupe $\mathbb{Z}_{2000}$. Poišči še vse homomorfne slike.

4. Naj bo $f : G_1 \to G_2$ epimorfizem, $H_2 \triangleleft G_2$ in $H_1 = f^{-1}(H_2)$. Pokaži, da je $G_1/H_1 \cong G_2/H_2$. Ali to še velja, če f ni surjektiven?

5. Naj bo G grupa in $H \triangleleft G$. Pokaži, da je $Z(H) \triangleleft G$.

6. Pokaži, da je grupa neskončna natanko tedaj, ko vsebuje neskončno različnih podgrup.

Vaje 6

1. Naj bosta $m, n \geq 2$ naravni števili. Pokaži, da je $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ natanko tedaj, ko sta m in n tuji.

2. Naj bosta G_1, G_2 grupi, $G = G_1 \times G_2$ in $H \triangleleft G$. Pokaži, da $H \leq Z(G)$ ali pa H netrivialno seka vsaj eno od podgrup $G_1' = G_1 \times \{e\}$ in $G_2' = \{e\} \times G_2$.

3. Pokaži:

   (a) V vsaki grupi je $\mathrm{red}(ab) = \mathrm{red}(ba)$.

   (b) Če je F prosta grupa, tedaj v F ne obstaja element končnega reda.

4. Pokaži, da je $\langle a, b | a^2 = b^3 = e, ab = ba \rangle \cong \mathbb{Z}_6$.

5. Pokaži, da $\langle a, b | a^2 = b^3 = e \rangle$ ni abelova grupa.

6. Pokaži, da je $\langle a, b | a^2 = b^2 = e \rangle$ neskončna neabelova grupa.

7. Pokaži, da je $D_{2n} \cong \langle a, b | a^n = b^2 = e, abab = 1 \rangle$.

8. Naj bo F prosta grupa nad množico X in $Y \subseteq X$. Naj bo $H \triangleleft F$ podgrupa edinka, generirana z vsemi $y \in Y$. Pokaži, da je F/H prosta grupa nad $X \setminus Y$.

9. Pokaži, grupi $\prod_{n \in \mathbb{N}} \mathbb{Z}$ in $\bigoplus_{n \in \mathbb{N}} \mathbb{Z}$ nista izomorfni.

Vaje 7

1. Naj bo G grupa. Pokaži: če je $G/Z(G)$ ciklična, je G Abelova.
2. Pokaži, da je vsaka grupa moči p^2, kjer je p praštevilo, Abelova.
3. Naj bo G grupa. Pokaži: $G/Z(G) \cong \mathrm{Inn}(G)$.
4. Naj bo G grupa in $H \leq G$. Naj bo $\psi : G \to S(G/H)$ naravno delovanje grupe G na levih odsekih $G/H = \{xH | \ x \in G\}$. Pokaži: $\ker(\psi) = \bigcap_{g \in G} gHg^{-1} \leq H$.
5. Naj bo G končna grupa in H podgrupa indeksa p, kjer je p najmanjše praštevilo, ki deli moč grupe G. Pokaži, da je $H \triangleleft G$.
6. Naj bo G grupa moči 135 in H podgrupa moči 45. Pokaži, da je $H \triangleleft G$.
7. Naj bo G končna grupa, katere moč je deljiva s praštevilom p, in A neka podgrupa grupe $\mathrm{Aut}(G)$ moči p^k za nek $k \geq 1$. Pokaži, da obstaja tak $x \in G$, $x \neq 1$, da je $f(x) = x$ za vsak $f \in A$. (Nasvet: oglej si naravno delovanje A na množici G.)

Vaje 8

1. Naj bo G grupa moči 200. Koliko ima podgrup moči 25?

2. Naj bo G grupa moči 56. Pokaži, da G ni enostavna.

3. Pokaži:

   (a) Naj bo G grupa. Če je $H \triangleleft G$ in $K \triangleleft G$, potem je $HK \triangleleft G$.

   (b) Pokaži: če je $G = HK$, kjer sta H in K podgrupi edinki v G, takšni, da $H \cap K = \{e\}$ in $hk = kh$ za vsak $h \in H$ in $k \in K$, tedaj je $G \cong H \times K$.

   (c) Naj bo G grupa moči $5 \cdot 7 \cdot 19$. Pokaži, da v G obstaja podgrupa edinka moči 35.

4. Naj bo G enostavna grupa moči 168. Koliko elementov reda 7 je v G?

5. Naj bo G grupa moči 48. Pokaži, da v G obstaja podgrupa edinka moči 8 ali 16. (Nasvet: delovanje G na 2-podgrupah Sylowa s konjugiranjem.)

6. Naj bo G grupa moči 77. Pokaži: $G \cong \mathbb{Z}_{77}$.

Vaje 9

1. Poišči vse neizomorfne Abelove grupe moči 405.
2. Koliko je neizomorfnih Abelovih grup moči 10000?
3. Katere od grup $\mathbb{Z}_{12} \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_7$, $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{70}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{14}$, $\mathbb{Z}_{40} \oplus \mathbb{Z}_{21}$, $\mathbb{Z}_{840}$ so med seboj izomorfne?
4. Poišči minimalno število generatorjev grupe $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.
5. Kateri znani grupi je izomorfna grupa $\mathbb{Z}_{18} \oplus \mathbb{Z}_2 / \langle (9,1) \rangle$?
6. Pokaži, da je vsaka grupa moči 200 rešljiva.
7. Pokaži, da je vsaka grupa moči p^n, kjer je n praštevilo, rešljiva.
8. Pokaži, da je vsaka grupa moči pqr, kjer so p, q, r različna praštevila, rešljiva.
9. Poišči normalizator podgrupe $\langle (1\ 2) \rangle$ v grupi S_3.
10. Naj bo G grupa vseh zgornje trikotnih $n \times n$ matrik s koeficienti iz obsega $\mathbb{Z}_p$ z 1 po diagonali, z operacijo matrično množenje. Pokaži, da je G rešljiva.

Vaje 10

1. Na množici $\mathbb{R}$ sta dani operaciji $\oplus, *$ s predpisoma $a \oplus b = a + b + 1$ in $a * b = a + b + ab$. Pokaži, da je $(\mathbb{R}, \oplus, *)$ kolobar. Ali je tudi obseg?

2. Pokaži, da je množica $\mathbb{Z} \times \mathbb{Z}$ kolobar za operaciji $+$ in $\cdot$ po komponentah. Kaj so delitelji niča v tem kolobarju?

3. Poišči vse obrnljive elemente in vse delitelje niča v kolobarju $\mathbb{Z}_n$.

4. Naj bo K kolobar, v katerem velja $a^2 = a$ za vsak $a \in K$. Pokaži, da je K komutativen.

5. Element e kolobarja K imenujemo *idempotent*, če je $e^2 = e$. Pokaži: če je K kolobar z enico in je e idempotent v K, potem je tudi $1 - e$ idempotent v K.

6. Naj bosta $m, n \geq 2$ tuji števili. Pokaži, da v kolobarju $\mathbb{Z}_{mn}$ obstaja netrivialen idempotent (to je idempotent, različen od 0 in 1).

7. Pokaži, da je kolobar K brez nilpotentov natanko tedaj, ko velja $x^2 = 0 \Rightarrow x = 0$ za vsak $x \in K$.

Vaje 11

1. Naj bo K končen kolobar, v katerem obstaja element a, ki ni niti levi niti desni delitelj niča. Pokaži, da je K kolobar z enico.

2. Naj bo $f : K_1 \to K_2$ homomorfizem kolobarjev. Denimo, da sta K_1, K_2 kolobarja z enico. Pokaži:

   (a) $f(1)$ je vselej idempotent kolobarja K_2.

   (b) Če je f surjektiven, je $f(1) = 1$ (to je, f je unitalni homomorfizem).

   (c) Če f ni surjektiven, potem to ni nujno res.

3. Poišči vse homomorfizme kolobarjev $\mathbb{Z}_{200} \to \mathbb{Z}_{300}$.

4. Poišči vse homomorfizme kolobarjev $\mathbb{Q} \to \mathbb{Q}$.

5. Reši enačbi $x^2 = 1 + i + j + k$ in $x^2 = -1$ v kolobarju z deljenjem $\mathbb{H}$.

6. Pokaži, da je kolobar endomorfizmov $\mathrm{End}(\mathbb{Z})$ Abelove grupe $\mathbb{Z}$ izomorfen kolobarju $\mathbb{Z}$.

Vaje 12

1. Naj bosta m in n tuji si števili. Pokaži, da je $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, kjer je kolobar $\mathbb{Z}_m \times \mathbb{Z}_n$ opremljen z operacijama po komponentah.

2. Koliko idempotentov ima kolobar $\mathbb{Z}_{300}$?

3. Naj bo $K = \{\frac{p}{q} \in \mathbb{Q} | q \text{ liho}\}$. Pokaži, da je K podkolobar v $\mathbb{Q}$. Pokaži še, da je (2) maksimalni ideal tega kolobarja.

4. Naj bo K komutativen kolobar in P njegov praideal. Pokaži, da potem P vsebuje vse nilpotente kolobarja K.

5. Naj bo K kolobar matrik $K = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b, c \in \mathbb{R}\}$, opremljen s standarnim matričnim seštevanjem in množenjem. Pokaži, da je $I = \{\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$ maksimalni ideal tega kolobarja.

6. Naj bosta K in I kot v prejšnji nalogi. Pokaži, da je $K/I \cong \mathbb{R}$.

7. Naj bosta K_1, K_2 kolobarja z idealoma $I_1 \triangleleft K_1$ in $I_2 \triangleleft K_2$. Označimo kolobar $K = K_1 \times K_2$ (z operacijama po komponentah). Pokaži, da je $I = I_1 \times I_2$ ideal kolobarja K in da velja $K/I \cong (K_1/I_1) \times (K_2/I_2)$.

Vaje 13

1. Reši sistem kongruenc:
$$\begin{aligned} x &\equiv 7 \ (10) \\ x &\equiv 1 \ (9) \\ x &\equiv 2 \ (7) \end{aligned}$$

2. Reši sistem kongruenc:
$$\begin{aligned} x &\equiv 1 \ (2) \\ x &\equiv 2 \ (3) \\ x &\equiv 3 \ (5) \\ x &\equiv 4 \ (7) \end{aligned}$$

3. Naj bosta I in J ideala kolobarja K. Poišči vložitev kolobarjev $K/(I \cap J) \to (K/I) \times (K/J)$. Poišči primer, ko ta vložitev ne bo surjektivna. Pokaži še: če je K kolobar z enico in je $I + J = K$, potem je vložitev surjektivna.

4. Poišči vse homomorfizme kolobarjev $\mathbb{Z}_{200} \to \mathbb{Z}_{300}$.

5. Poišči vse pare $(x, y) \in \mathbb{N}^2$, za katere je $1 + 2^x = y^2$.

6. Pokaži, da velja $\varphi(n^k) = n^{k-1}\varphi(n)$ za poljubni naravni števili n, k.

7. Poišči vsa naravna števila n, ki zadoščajo $\varphi(n) = \frac{n}{2}$.

8. Izračunaj $5^{6^{7^8}}$ (11).

9. Izračunaj zadnji dve števki števila $14^{15^{16}}$.

Vaje 14

1. Naj bo K kolobar $K = \{\frac{p}{q} \in \mathbb{Q} | \; q \text{ liho}\}$ za običajno seštevanje in množenje. Pokaži, da je K glavni kolobar.

2. Naj bo K kolobar števil $K = \{\alpha + \beta i\sqrt{5} | \; \alpha, \beta \in \mathbb{Z}\}$ za običajno seštevanje in množenje. Za vsak $a = \alpha + \beta i\sqrt{5} \in K$ definirajmo 'normo' števila a, $N(a) = \alpha^2 + 5\beta^2$.

   (a) Pokaži, da je $N(ab) = N(a)N(b)$ za poljubna $a, b \in K$.

   (b) Poišči obrnljive elemente v K.

   (c) Pokaži, da so 2, 3, $1 + i\sqrt{5}$ in $1 - i\sqrt{5}$ nerazcepni neasociirani elementi v K in da velja $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Odtod sklepaj, da K ni Gaussov kolobar.

3. Naj bo K kolobar *Gaussovih števil*, $K = \{\alpha + \beta i | \; \alpha, \beta \in \mathbb{Z}\}$ za običajno seštevanje in množenje. Za vsak $a = \alpha + \beta i \in K$ definiramo 'normo' števila a, $N(a) = \alpha^2 + \beta^2$.

   (a) Pokaži, da velja $N(ab) = N(a)N(b)$ za poljubna $a, b \in K$, in poišči obrnljive elemente v K.

   (b) Pokaži, da je 2 razcepen element v K. Pokaži, da je vsako praštevilo p, za katerega je $p \equiv 3(4)$, nerazcepen element v K. Poišči primer praštevila p, ki je razcepno v K in $p \equiv 1(4)$.

4. Naj bosta K in L celostni polji in $f : K \to L$ surjektivni homomorfizem. Pokaži: če je K glavni, je tudi L glavni.

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).

1. kolokvij iz Algebre 2
4. 12. 2012

1. Naj bo $n \geq 3$ liho število. Določi center diedrske grupe D_{2n}.

   Rešitev: Grupo D_{2n}, kot običajno, predstavimo kot množico elementov $\pi^i\rho^j$, kjer $i = 0, 1, \ldots, n-1$ in $j = 0, 1$. Vzemimo $\tau = \pi^i\rho^j \in Z(D_{2n})$. Potem je $\rho\pi^i\rho^j = \pi^i\rho^j\rho$. Z desne pomnožimo z ρ^{-j} in dobimo $\rho\pi^i = \pi^i\rho$. Velja pa $\rho\pi^i = \pi^{-i}\rho$, torej $\pi^{-i}\rho = \pi^i\rho$ in zato $\pi^{-i} = \pi^i$. Torej $\pi^{2i} = \mathrm{id}$ in zato $n|2i$. Ker je n liho, sledi $n|i$, torej $i = 0$. Pokažimo še, da je $j = 0$. Če bi bil $j = 1$, bi iz enakosti $\pi\pi^i\rho^j = \pi^i\rho^j\pi$ dobili $\pi\rho = \rho\pi$, torej $\pi\rho = \pi^{-1}\rho$, torej $\pi^{-1} = \pi$, torej $\pi^2 = \mathrm{id}$, torej $n|2$, kar je protislovje. Torej $i = j = 0$ in zato $Z(D_{2n}) = \{\mathrm{id}\}$.

2. Pokaži, da obstajata natanko 2 homomorfizma grup $(\mathbb{R} \setminus \{0\}, \cdot) \to \mathbb{Z}_2$ (kjer je grupa $\mathbb{Z}_2$ opremljena s standardnim seštevanjem po modulu 2).

   Rešitev: Naj bo $f : (\mathbb{R} \setminus \{0\}, \cdot) \to \mathbb{Z}_2$ homomorfizem. Potem za vsak $x > 0$ velja $f(x) = f(\sqrt{x}^2) = 2f(\sqrt{x})$. V grupi $\mathbb{Z}_2$ je $2y = 0$ za vsak $y \in \mathbb{Z}_2$, torej odtod sledi $f(x) = 0$ za vsak $x > 0$. Če pa je $x < 0$, pa je $-x > 0$ in zato $f(x) = f((-1)(-x)) = f(-1) + f(-x) = f(-1)$. Torej je f že določen z vrednostjo $f(-1)$. Če postavimo $f(-1) = 0$, dobimo $f = 0$ (trivialni homomorfizem), če pa je $f(-1) = 1$, pa je $f(x) = \begin{cases} 0, & x>0 \\ 1, & x<0 \end{cases}$ (ki je prav tako homomorfizem, saj je očitno $f(xy) = f(x) + f(y)$ za poljubna $x, y \in \mathbb{R} \setminus \{0\}$).

3. Naj bo G končna grupa in H, K takšni podgrupi, da sta indeksa $|G : H|$ in $|G : K|$ tuji si števili. Pokaži, da je $HK = G$. (HK označuje množico vseh produktov $HK = \{hk |\ h \in H, k \in K\}$.)

   Rešitev: Zadošča pokazati $|HK| = |G|$. Velja $|HK| = \frac{|H|\cdot|K|}{|H\cap K|} = \frac{|G|}{|G:H|} \cdot \frac{|G|}{|G:K|} \cdot \frac{1}{|H\cap K|} = \frac{|G:H\cap K|}{|G:H|\cdot|G:K|} \cdot |G|$. Ker je $|G : H \cap K| = |G : H| \cdot |H : H \cap K|$, je $|G : H \cap K|$ deljiv z $|G : H|$. Podobno je $|G : H \cap K|$ deljiv tudi z $|G : K|$. Ker sta $|G : H|$ in $|G : K|$ tuji si števili, je potem $|G : H \cap K|$ deljiv z $|G : H| \cdot |G : K|$. Sledi, da je $|HK| = k|G|$ za neko naravno število k. Torej $|HK| \geq |G|$ in zato $|HK| = |G|$.

4. Pokaži, da je $\langle a, b | ab = ba\rangle \cong \mathbb{Z} \times \mathbb{Z}$ (pri čemer je grupa $\mathbb{Z} \times \mathbb{Z}$ opremljena s standardnim seštevanjem po komponentah).

   Rešitev: Elementa $\alpha = (1, 0) \in \mathbb{Z} \times \mathbb{Z}$ in $\beta = (0, 1) \in \mathbb{Z} \times \mathbb{Z}$ generirata grupo $\mathbb{Z} \times \mathbb{Z}$ in zadoščata $\alpha + \beta = \beta + \alpha$ v grupi $\mathbb{Z} \times \mathbb{Z}$, torej po van Dyckovem izreku obstaja natanko en epimorfizem $f : \langle a, b|ab = ba\rangle \to \mathbb{Z} \times \mathbb{Z}$, ki slika a v α in b v β. Pokažimo, da je f izomorfizem. Definirajmo preslikavo $g : \mathbb{Z} \times \mathbb{Z} \to \langle a, b|ab = ba\rangle$, $(m, n) \mapsto a^m b^n$. Najprej vidimo, da je g homomorfizem, saj je $g((m, n) + (m', n')) = g(m + m', n + n') = a^{m+m'} b^{n+n'} = a^m b^n a^{m'} b^{n'} = g(m, n)g(m', n')$ za poljubne $m, n, m', n' \in \mathbb{Z}$. Velja $g \circ f = \mathrm{id}$, saj se $g \circ f$ in id ujemata na obeh generatorjih. Res, $(g \circ f)(a) = g(f(a)) = g(\alpha) = a$ in $(g \circ f)(b) = g(f(b)) = g(\beta) = b$. Torej je res $g \circ f = \mathrm{id}$ in je zato f injektiven in zato izomorfizem.

5. Naj bo G grupa moči $p^n r$, kjer je p praštevilo, $n \geq 1$, $r \geq 2$, p ne deli r in p^n ne deli $(r-1)!$. Pokaži, da v grupi G obstaja prava netrivialna podgrupa edinka. (Nasvet: izberi si podgrupo moči p^n in si oglej delovanje grupe G na levih odsekih.)

Rešitev: Po izreku Sylowa obstaja podgrupa $H \leq G$ moči p^n. Naj bo G/H množica vseh levih odsekov (ki je moči $|G : H| = r$). Označimo z $f : G \to \mathrm{Sym}(G/H) \cong S_r$ naravno delovanje na tej množici, torej $f : g \mapsto (xH \mapsto gxH)$. Če je $\ker(f) = G$, je $xH = gxH$ za vsak $g, x \in G$ in zato $H = gH$ za vsak $g \in G$, od koder sledi $H = G$, kar je protislovje. Torej je $\ker(f) \neq G$. Če je $\ker(f) = \{e\}$, je f injektiven in zato $|G| = p^n r$ deli $|\mathrm{Sym}(G/H)| = r! = r(r-1)!$, torej p^n deli $(r-1)!$, kar je protislovje. Torej je $\ker(f)$ prava netrivialna podgrupa edinka v G.

Algebra 2

Izpit 14. 6. 2013

Vsaka naloga je vredna 20 točk.

1. Naj bo $G = \{\begin{pmatrix} x & x-y \\ 0 & y \end{pmatrix} \mid x, y \in \mathbb{R} \setminus \{0\}\}$. Pokaži, da je G grupa za matrično množenje in da velja $G \cong (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\})$. (Grupa $\mathbb{R} \setminus \{0\}$ je opremljena z običajnim množenjem.)

   Rešitev: Definirajmo preslikavo $f : (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\}) \to \mathrm{GL}_2(\mathbb{R})$, $f(x, y) = \begin{pmatrix} x & x-y \\ 0 & y \end{pmatrix}$. Preslikava je dobro definirana, saj je matrika $\begin{pmatrix} x & x-y \\ 0 & y \end{pmatrix}$ obrnljiva za poljubna $x, y \in \mathbb{R} \setminus \{0\}$. Preslikava f je tudi homomorfizem grup, saj je $f((x, y)(z, w)) = f(xz, yw) = \begin{pmatrix} xz & xz-yw \\ 0 & yw \end{pmatrix} = \begin{pmatrix} x & x-y \\ 0 & y \end{pmatrix} \begin{pmatrix} z & z-w \\ 0 & w \end{pmatrix} = f(x, y)f(z, w)$ za poljubna $(x, y), (z, w) \in (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\})$. Očitno je f injektivna preslikava in $\mathrm{im}(f) = G$, torej je res $(\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\}) \cong \mathrm{im}(f) = G$.

2. Izračunaj zadnji dve števki števila $7^{7^{70}}$.

   Rešitev: Velja $\varphi(100) = 40$, torej je po Fermatovem izreku $7^{40} = 1 \mod 100$ in zato $7^{7^{70}} = 7^{7^{70} \mod 40} \mod 100$. Nadalje, velja $\varphi(40) = 16$, torej $7^{16} = 1 \mod 40$ in zato $7^{70} = 7^{70 \mod 16} = 7^6 = 49^3 = 9^3 = 81 \cdot 9 = 9 \mod 40$. Odtod dobimo $7^{7^{70}} = 7^9 = 343^3 = 43^3 = 79507 = 7 \mod 100$. Zadnji dve števki sta torej 07.

3. Naj bo K glavni kolobar in naj bodo $p_1, \ldots, p_k \in K$ paroma neasociirani nerazcepni elementi v K. Pokaži, da ima kvocientni kolobar $K/(p_1 p_2 \ldots p_k)$ natanko 2^k idealov.

   Rešitev: Ideali v $K/(p_1 p_2 \ldots p_k)$ so v bijektivni korespondenci s tistimi ideali I v K, za katere je $(p_1 p_2 \ldots p_k) \subseteq I$. Ker je K glavni kolobar, je $I = (a) \supseteq (p_1 p_2 \ldots p_k)$ za nek $a \in K$, od koder sledi $a \mid p_1 \ldots p_k$. Do asociiranosti natančno je potem $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, kjer je $\alpha_i \in \{0, 1\}$, od koder dobimo 2^k različnih (paroma neasociiranih) elementov a in s tem 2^k idealov $I = (a)$. Ti ideali so tudi paroma različni, saj je $(a) \neq (b)$ za poljubna neasociirana elementa $a, b \in K$.

4. Naj bo K kolobar z enico, takšen, da je vsak njegova podgrupa za seštevanje ideal v K. Pokaži, da je K izomorfen bodisi $\mathbb{Z}$ bodisi $\mathbb{Z}_n$ za nek $n \in \mathbb{N}$.

   Rešitev: Kolobar K vsebuje podkolobar $\mathbb{Z}_n$, kjer je $n = \mathrm{char}(K)$, oziroma $\mathbb{Z}$, če je $\mathrm{char}(K) = 0$. Ta podkolobar je podgrupa za seštevanje, torej je po predpostavki naloge ideal v K. Ker vsebuje tudi enico kolobarja K, je potem ta podkolobar enak celemu kolobarju K. Torej je res $K \cong \mathbb{Z}_n$ ali $K \cong \mathbb{Z}$.

5. Naj bo G končna grupa in naj bosta p in q dve različni praštevili, ki delita moč grupe G. Denimo, da v G obstajata p-podgrupa Sylowa P in q-podgrupa Sylowa Q, tako da je $P \triangleleft G$ in $Q \triangleleft G$. Pokaži, da obstaja natanko ena podgrupa v G moči $|P| \cdot |Q|$.

   Rešitev: Pišimo $|G| = p^\alpha q^\beta n$, kjer $p, q \nmid n$. Ker je $P \triangleleft G$, je PQ podgrupa v G. Ta grupa ima moč $|P| \cdot |Q|$, saj je $P \cap Q = 1$ in zato $|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = |P| \cdot |Q|$. Pokažimo še, da je PQ edina podgrupa moči $|P| \cdot |Q|$. Naj bo $H \leq G$ podgrupa moči $|H| = |P| \cdot |Q| = p^\alpha q^\beta$. Po izreku Sylowa v grupi H obstajata podgrupi P' moči p^α in Q' moči q^β. Ker je tudi $P', Q' \leq G$ in sta P in Q edini podgrupi v G moči p^α in q^β, je $P' = P$ in $Q' = Q$. Zato je $PQ \leq H$ in s tem $H = PQ$.

Algebra 2

Izpit 26. 8. 2013

Vsaka naloga je vredna 20 točk.

1. Poišči vse $x \in \mathbb{Z}$, ki rešijo sistem kongruenc:

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 6 \end{aligned}$$

Rešitev: Prva enačba nam da $x = 4k - 1$, $k \in \mathbb{Z}$. Druga enačba nam da $4k - 1 \equiv 2 \pmod 5$, torej $-k + 2 \equiv 0 \pmod 5$. Odtod sledi $k = 5l + 2$, torej $x = 20l + 7$. Tretja enačba nam da $20l + 7 \equiv 3 \pmod 6$, torej $2l - 2 \equiv 0 \pmod 6$ oziroma $l - 1 \equiv 0 \pmod 3$. Torej $l = 3m + 1$ in zato $x = 20(3m+1) + 7 = 60m + 27$. Torej so rešitve vsa števila oblike $60m + 27$, $m \in \mathbb{Z}$.

2. Naj bo G grupa moči 80. Pokaži, da v G obstaja prava netrivialna podgrupa edinka. (Nasvet: izreki Sylowa.)

Rešitev: Pišimo $|G| = 80 = 2^4 \cdot 5$. Označimo z s_2 število 2-podgrup Sylowa in z s_5 število 5-podgrup Sylowa. Po izrekih Sylowa dobimo $s_2 \in \{1, 5\}$ in $s_5 \in \{1, 16\}$. Denimo, da je $s_5 = 16$. Potem v G obstaja 16 podgrup moči 5, ki so praštevilske moči in zato paroma disjunktne (oziroma imajo skupni element le e). V njih je torej skupno $16 \cdot 4 = 64$ elementov reda 5. Zato v G obstaja kvečjemu $80 - 64 = 16$ elementov, ki niso reda 5. Ker noben izmed elementov grupe moči 16 nima reda 5, je torej v G kvečjemu 1 podgrupa moči 16. Ta podgrupa je potem tudi podgrupa edinka.

3. Naj bo $K = \{\frac{a}{b} \in \mathbb{Q} | \ 2 \nmid b, \ 5 \nmid b\}$. Ta množica je kolobar za običajno seštevanje in množenje.

   (a) Dokaži, da sta (2) in (5) maksimalna ideala v K.

   (b) Dokaži, da (10) ni praideal v K.

Rešitev:

(a) Pokažimo samo, da je (5) maksimalni ideal (dokaz za (2) je analogen). Naj bo I ideal kolobarja K, tako da je $(5) \subsetneq I$. Izberimo $\frac{a}{b} \in I \setminus (5)$. Potem je $a \in I$. Ker je $\frac{a}{b} \notin (5)$, število a ni deljivo s 5, torej je $\alpha a + \beta \cdot 5 = 1$ za neka $\alpha, \beta \in \mathbb{Z}$. Ker je $\alpha a, \beta \cdot 5 \in I$, odtod sledi $1 \in I$ in zato $I = K$. Torej je (5) res maksimalni ideal.

(b) Velja $2 \notin (10)$ in $5 \notin (10)$. Res, če bi bilo $2 \in (10)$, potem bi lahko pisali $2 = \frac{10a}{b}$ in bi sledilo $5 \mid b$, kar pa je protislovje. Analogno, če bi veljalo $5 \in (10)$, bi odtod sledilo $5 = \frac{10a}{b}$, od koder bi sledilo $2 \mid b$, kar je spet protislovje. Torej je res $2 \notin (10)$ in $5 \notin (10)$. Po drugi strani pa je $2 \cdot 5 = 10 \in (10)$, torej (10) ni praideal.

4. Množica $\mathbb{Q}^+$ vseh pozitivnih racionalnih števil je grupa za običajno množenje. Dokaži, da je ta grupa izomorfna šibkemu direktnemu produktu (t.j. direktni vsoti) $\bigoplus_{n\in\mathbb{N}} \mathbb{Z}$.

   Rešitev: Označimo s $p_1, p_2, \ldots$ vsa praštevila. Potem lahko vsak element q grupe $\mathbb{Q}^+$ zapišemo na enoličen način kot $q = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ za neke $k \geq 0$ in $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}$. Definirajmo preslikavo $f : \mathbb{Q}^+ \to \bigoplus \mathbb{Z}$, $f(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}) = (\alpha_1, \alpha_2, \ldots, \alpha_k, 0, 0, \ldots)$. Ta preslikava je očitno homomorfizem grup, saj je množenje števil v $\mathbb{Q}^+$ ekvivalentno seštevanju eksponentov. Prav tako je očitna surjektivnost in injektivnost. Torej je f izomorfizem grup.

5. Naj bo G končno generirana grupa, v kateri velja $A \leq B$ ali $B \leq A$ za poljubni dve podgrupi $A, B \leq G$. Pokaži, da je G ciklična grupa moči p^n, kjer je p praštevilo in $n \geq 0$. (Nasvet: najprej dokaži, da je G Abelova.)

   Rešitev: Pokažimo najprej, da je G Abelova. Naj bo $a, b \in G$. Po predpostavki je $\langle a \rangle \subseteq \langle b \rangle$ ali $\langle b \rangle \subseteq \langle a \rangle$. V prvem primeru je $a = b^n$, v drugem pa $b = a^n$ za nek $n \in \mathbb{Z}$. V obeh primerih pa sledi, da je $ab = ba$. Torej je G res Abelova grupa.

   Ker je G končno generirana Abelova grupa, lahko pišemo $G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$ za neka praštevila p_i in $n, \alpha_i, k \geq 0$. V grupi $\mathbb{Z}$ lahko najdemo podgrupi $A = 2\mathbb{Z}$ in $B = 3\mathbb{Z}$, ki ne zadoščata niti $A \subseteq B$ niti $B \subseteq A$, torej mora biti $n = 0$. Če je $k \geq 2$, potem lahko v grupi G najdemo podgrupi $A = 0 \oplus \ldots \oplus 0 \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus 0 \oplus \ldots \oplus 0$ in $B = 0 \oplus \ldots \oplus 0 \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus 0 \oplus \ldots \oplus 0$, za kateri ne velja niti $A \subseteq B$ niti $B \subseteq A$. Torej je $k = 1$ in je grupa G res oblike $G \cong \mathbb{Z}_{p^\alpha}$, kjer je p praštevilo in $\alpha \geq 0$.

Izpit 5. 2. 2013

1. Poišči vsa cela števila $x \in \mathbb{Z}$, ki zadoščajo sistemu kongruenc:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

Rešitev: Pišemo $x = 140a + 105b + 84c + 60d$. Dobimo sistem $140a \equiv 2 \pmod 3$, $105b \equiv 3 \pmod 4$, $84c \equiv 4 \pmod 5$ in $60d \equiv 5 \pmod 7$. Ena od rešitev tega sistema je $a = 1$, $b = -1$, $c = 1$, $d = 3$. Dobimo $x = 299$, torej je splošna rešitev $x = 299 + 420n$, $n \in \mathbb{Z}$.

2. Naj bo dana grupa $G = \{z \in \mathbb{C} |\ |z| = 1\}$ za operacijo množenje števil in podmnožica $H = \{1, -1\} \subseteq G$. Pokaži, da je H podgrupa edinka v G in da velja $G/H \cong G$.

Rešitev: Definirajmo $f : G \to G$, $f(z) = z^2$. Preslikava f je dobro definirana, saj je $|z^2| = |z| \cdot |z| = 1$ za vsak $z \in G$. Velja tudi $f(zw) = (zw)^2 = z^2w^2 = f(z)f(w)$ za vsaka dva $z, w \in G$, torej je f homomorfizem. Očitno je f surjektiven, saj za vsak $z = e^{it} \in G$ obstaja $w = e^{\frac{it}{2}}$, da je $f(w) = z$. Jedro homomorfizma f je točno $\ker(f) = \{z \in G |\ z^2 = 1\} = \{1, -1\} = H$, torej je po izreku o izomorfizmu $G/H \cong G$. Posebej je $H = \ker(f)$ podgrupa edinka v G.

3. Naj bo A Abelova grupa in $H \leq A$ podgrupa. Označimo kolobar endomorfizmov $K = \mathrm{End}(A)$ in podmnožico $I = \{f \in K |\ \mathrm{im}(f) \leq H\}$. Pokaži, da je I desni ideal kolobarja K. Pokaži še: če velja $f(H) \subseteq H$ za vsak $f \in K$, potem je I tudi levi ideal kolobarja K.

Rešitev: Za poljubna $f, g \in I$ in $x \in G$ je $(f - g)(x) = f(x) - g(x) \in H$, saj $f(x), g(x) \in H$. Torej je $\mathrm{im}(f - g) \subseteq H$ in zato $f - g \in I$. Nadalje, za poljuben $h \in K$ je $\mathrm{im}(fh) \subseteq \mathrm{im}(f) \subseteq H$, torej je $fh \in I$. Torej je I desni ideal.

Če predpostavimo še $q(H) \subseteq H$ za vsak $q \in K$, potem pa je tudi $\mathrm{im}(hf) = h(f(A)) \subseteq h(H) \subseteq H$ in je zato I tudi levi ideal.

4. Naj bo K komutativen kolobar z enico. Denimo, da za vsak $a \in K$ obstaja $n \geq 2$ (odvisen od a), da velja $a = a^n$. Pokaži, da je potem vsak praideal v K maksimalni ideal.

Rešitev: Naj bo I praideal v K in $I \subsetneq J \subsetneq K$ za nek ideal J. Vzemimo $a \in J \setminus I$. Po predpostavki je $a = a^n$ za nek $n \geq 2$, torej $a(1 - a^{n-1}) = 0 \in I$. Ker je I praideal, je potem $a \in I$ ali $1 - a^{n-1} \in I$. Prva možnost odpade, torej $1 - a^{n-1} \in I$ in zato $1 = (1 - a^{n-1}) + a^{n-1} \in I + (a) \subseteq J$. Od tod sledi $J = K$, kar je protislovje. Torej je I res maksimalni ideal.

5. Grupa G se imenuje *deljiva*, če za vsak $y \in G$ in $n \geq 2$ obstaja tak $x \in G$, da je $x^n = y$. Naj bo G deljiva grupa. Pokaži, da G ne vsebuje prave podgrupe končnega indeksa. (Nasvet: pomagaj si s primernim delovanjem.)

   Rešitev: Naj bo $H \leq G$ podgrupa končnega indeksa n. Pokazati želimo, da je $n = 1$ oziroma $H = G$. Oglejmo si delovanje na levih odsekih $\varphi : G \to S(G/H)$, $g \mapsto (aH \mapsto gaH)$. Pokazati želimo, da je to delovanje trivialno. Vzemimo $g \in G$. Po predpostavki obstaja $x \in G$, da je $g = x^{n!}$. Ker je $\pi^{n!} = \mathrm{id}$ za vsak $\pi \in S(G/H) \cong S_n$, je $\varphi(g) = \varphi(x^{n!}) = \varphi(x)^{n!} = \mathrm{id}$. Torej je delovanje res trivialno. Posebej to pomeni, da je $gH = H$ za vsak $g \in G$, in zato $H = G$.

2. kolokvij iz Algebre 2

8. 1. 2013

1. Poišči vse neizomorfne Abelove grupe moči 3000.

   Rešitev: Ker je $3000 = 3 \cdot 2^3 \cdot 5^3$, imamo 9 neizomorfnih grup: $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{125}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{125}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{125}$.

2. Naj bo K kolobar in $e \in K$ idempotent. Pokaži, da je $eKe = \{exe | x \in K\}$ podkolobar kolobarja K. Pokaži še, da je $e \in eKe$ in da je e enica kolobarja eKe.

   Rešitev: Vzemimo $\alpha\beta \in eKe$ in preverimo, da je $\alpha - \beta, \alpha\beta \in eKe$. Pišimo $\alpha = exe$ in $\beta = eye$, $x, y \in K$. Potem je $\alpha - \beta = exe - eye = e(xe - ye) = e(x - y)e \in eKe$, saj $x - y \in K$. Podobno je $\alpha\beta = exeeye = exeye \in eKe$, saj je $xey \in K$.

   Ker je $e = ee = eee$, je $e \in eKe$. Preverimo še, da je e enica kolobarja eKe. Vzemimo $\alpha = exe \in eKe$. Potem je $e\alpha = eexe = exe = \alpha$ in $\alpha e = exee = exe = \alpha$, torej je e res enica v eKe.

3. Naj bo K kolobar zgornje trikotnih matrik $K = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b, c \in \mathbb{R}\}$ za operaciji standardno matrično seštevanje in množenje. Označimo $I = \{\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mid b \in \mathbb{R}\} \subseteq K$. Pokaži, da je I ideal v K in da velja $K/I \cong \mathbb{R} \times \mathbb{R}$ (kjer je $\mathbb{R} \times \mathbb{R}$ kolobar z operacijama po komponentah).

   Rešitev: Definirajmo preslikavo $f : K \to \mathbb{R}\times\mathbb{R}$, $f(\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)) = (a, c)$. Hitro lahko preverimo, da je f homomorfizem kolobarjev. Očitno je f surjektiven. Njegovo jedro pa je točno $\ker(f) = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in K |\ f(\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)) = 0\} = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in K |\ (a, c) = (0, 0)\} = \{\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \in K\} = I$. Torej je I ideal v K in po izreku o izomorfizmu velja $K/I \cong \mathbb{R} \times \mathbb{R}$.

4. Naj bo K kolobar zgornje trikotnih matrix $K = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b, c \in \mathbb{Z}\}$ za operaciji standardno matrično seštevanje in množenje. Pokaži, da je $I = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b \in \mathbb{Z},\ c \in 2\mathbb{Z}\}$ maksimalni ideal tega kolobarja (pokaži tudi, da je ideal).

   Rešitev: Hitro lahko preverimo, da je $A - B \in I$ in $CA, AC \in I$ za poljubne $A, B \in I$ in $C \in K$. Torej je I res ideal v K. Preverimo še, da je I maksimalni. Pa denimo, da obstaja $J \triangleleft K$ z lastnostjo $I \subsetneq J \subsetneq K$. Ker je $I \subsetneq J$, obstaja $A = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in J \setminus I$. Ker $A \notin I$, je c liho število. Torej je $1 - c$ sodo in zato $B = \left(\begin{smallmatrix} 1-a & -b \\ 0 & 1-c \end{smallmatrix}\right) \in I \subseteq J$. Torej $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = A + B \in J$ in zato $J = K$, kar je protislovje. Torej je I res maksimalni ideal.

5. Pokaži, da je vsaka grupa moči 500 rešljiva. (Nasvet: izreki Sylowa.)

   Rešitev: Naj bo G grupa moči $500 = 2^2 \cdot 5^3$. S k označimo število 5-podgrup Sylowa. Potem je $k \equiv 1\ (5)$ in $k|4$, torej $k = 1$. Torej obstaja v G podgrupa edinka H moči 5^3. Vsaka grupa moči p^n, p praštevilo, je rešljiva. Torej je H rešljiva. Vidimo tudi, da je $|G/H| = \frac{|G|}{|H|} = 4$, torej je tudi G/H moči p^n in zato rešljiva. Ker sta H in G/H rešljivi, je potem G rešljiva.

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.

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 $J \triangleleft K$. 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 $J = K$.

Izpit iz Algebre 2, 14. 2. 2012 – Rešitve

1. Pokaži, da ne obstaja neničelni homomorfizem grup $(\mathbb{Q},+) \to (\mathbb{Z},+)$.

   Rešitev: Naj bo $f:(\mathbb{Q},+)\to(\mathbb{Z},+)$ poljuben homomorfizem in $q\in\mathbb{Q}$. Potem za vsak $n\in\mathbb{N}$ velja $f(q)=f(n\cdot\frac{q}{n})=f(\frac{q}{n}+\ldots+\frac{q}{n})=f(\frac{q}{n})+\ldots+f(\frac{q}{n})=nf(\frac{q}{n})\in n\mathbb{Z}$. Torej je $f(q)$ deljivo z n za vsak n in zato $f(q)=0$. Ker je bil q poljuben, je potem $f=0$.

2. Koliko podgrup moči 5 ima grupa S_5?

   Rešitev: Grupa S_5 ima $120=2^3\cdot 3\cdot 5$ elementov, torej so podgrupe moči 5 ravno 5-podgrupe Sylowa. Z izreki Sylowa pokažemo, da je teh podgrup natanko 6 ali 1. Če bi bila 1, bi bila to podgrupa edinka. Ogledamo si kakšno podgrupo moči 5, na primer $H=\langle(1\ 2\ 3\ 4\ 5)\rangle=\{(1\ 2\ 3\ 4\ 5),(1\ 3\ 5\ 2\ 4),(1\ 4\ 2\ 5\ 3),(1\ 5\ 4\ 3\ 2),\mathrm{id}\}$; ta ni podgrupa edinka, saj $(1\ 2)(1\ 2\ 3\ 4\ 5)(1\ 2)^{-1}=(1\ 3\ 4\ 5\ 2)\notin H$. Torej je podgrup moči 5 natanko 6.

3. Naj bo G končna grupa, katere moč je deljiva s praštevilom p, in A neka podgrupa grupe $\mathrm{Aut}(G)$ moči $|A|=p^k$ za neko naravno število k. Pokaži, da obstaja tak $x\in G$, $x\neq 1$, da je $f(x)=x$ za vsak $f\in A$. (Nasvet: oglej si naravno delovanje grupe A na množici G.)

   Rešitev: Grupa A deluje na množici G kot naravna vložitev $\varphi: A\hookrightarrow S(G)$, $\varphi(f)=f$. Če je $x\in G$ točka iz G, potem označimo z $\overline{x}$ njeno orbito in z A_x stabilizator. Ker je $|\overline{x}|=[A:A_x]$, je moč vsake orbite delitelj moči grupe A in zato bodisi $|\overline{x}|=1$ (točka x je fiksna točka delovanja) bodisi $p||\overline{x}|$. Množica G pa je disjunktna unija orbit nefiksnih točk (te orbite imajo po pravkar dokazanem moč, deljivo s p) in množice fiksnih točk. Ker je moč G deljiva s p, je potem tudi število fiksnih točk deljivo s p in zato večje ali enako p (točka 1 je seveda fiksna točka delovanja). Posebej to pomeni, da obstaja vsaj ena netrivialna fiksna točka delovanja, to je točka $x\in G$, za katero je $f(x)=x$ za vsak $f\in A$.

4. Pokaži, da je kolobar $\mathbb{R}[X]/(X^2)$ izomorfen kolobarju matrik $K=\{\left[\begin{smallmatrix} a & b\\ 0 & a\end{smallmatrix}\right],\ a,b\in\mathbb{R}\}$.

   Rešitev: Definiramo preslikavo $f:\mathbb{R}[X]\to K$, $p_0+p_1X+\ldots+p_nX^n\mapsto\left[\begin{smallmatrix} p_0 & p_1\\ 0 & p_0\end{smallmatrix}\right]$. Preverimo lahko, da je f homomorfizem kolobarjev. Očitno je f surjektiven in $\ker(f)=(X^2)$, torej je po izreku o izomorfizmih $\mathbb{R}[X]/(X^2)\cong K$.

5. Naj bo K komutativen kolobar z enico in P njegov praideal. Pokaži: če P ne vsebuje netrivialnih deliteljev niča kolobarja K, potem je K cel kolobar.

   Rešitev: Denimo nasprotno, da je $xy=0$ za neka $x,y\in K$, $x,y\neq 0$. Ker je P praideal in $xy=0\in P$, je $x\in P$ ali $y\in P$. To pa je protislovje s predpostavko, da P ne vsebuje netrivialnih deliteljev niča kolobarja K.

Izpit iz Algebre 2
30. 8. 2012

1. Naj bo G grupa in H neka ciklična podgrupa edinka grupe G. Pokaži, da je vsaka podgrupa $K \leq H$ podgrupa edinka v G. Ali to še velja, če H ni ciklična?

   Rešitev: Naj bo $a \in H$ generator grupe H. Podgrupa ciklične grupe je ciklična, torej je $K = \langle a^n \rangle$ za nek $n \in \mathbb{Z}$. Izberimo poljuben $x \in K$ in $g \in G$. Preveriti moramo, da je $gxg^{-1} \in K$. Pišimo $x = a^{nk}$ za nek k. Ker je $gag^{-1} \in H$, je $gag^{-1} = a^l$ za nek l, torej $gxg^{-1} = ga^{kn}g^{-1} = (gag^{-1})^{kn} = a^{kln} \in K$.

   Če H ni ciklična, to ne velja. Npr., $G = S_3$, $H = G$ in $K = \langle (1\ 2) \rangle$.

2. Koliko podgrup ima grupa $\mathbb{Z}_{2000}$? Odgovor utemelji.

   Rešitev: Število $2000 = 2^4 \cdot 5^3$ ima 20 deliteljev (števila $2^i \cdot 5^j$ za $i \leq 4$ in $j \leq 3$). Za vsak delitelj d števila 2000 je $\langle d \rangle = d\mathbb{Z}_{2000}$ podgrupa moči $2000/d$ (saj je $2000/d$ red elementa d tej grupi). Torej imamo 20 podgrup različnih moči.

   Te grupe so tudi vse podgrupe. Res, naj bo H poljubna podgrupa grupe $\mathbb{Z}_{2000}$. Označimo z n generator grupe H. Potem je H točno množica vseh $n\alpha + 2000\beta$ po modulu 2000, kjer α in β pretečeta cela števila. Števila $n\alpha + 2000\beta$ pa so točno večkratniki največjega skupnega delitelja $d = d(n, 2000)$. Torej je $H = \langle d \rangle$, kjer je d nek delitelj števila 2000, in je zato H ena od zgoraj naštetih 20 grup.

3. Naj bo K kolobar z enico. Označimo z $Z(K)$ center kolobarja K, to je
$$Z(K) = \{x \in K |\ xy = yx \text{ za vsak } y \in K\}.$$
   (a) Pokaži, da je $Z(K)$ podkolobar kolobarja K.

   (b) Kolobar se imenuje *enostaven*, če ne vsebuje pravega netrivialnega dvostranskega ideala. Pokaži: če je K enostaven, je $Z(K)$ podobseg v K.

   Rešitev:

   (a) Izberimo $x, y \in Z(K)$ in $z \in K$. Potem je $z(x - y) = zx - zy = xz - yz = (x - y)z$ in $z(xy) = zxy = (xy)z$, torej $x - y, xy \in Z(K)$. Torej je $Z(K)$ podkolobar.

   (b) Najprej vidimo, da $Z(K)$ očitno vsebuje enico kolobarja K. Izberimo $x \in Z(K)$, $x \neq 0$. Potem je $(x) = Kx$ neničeln dvostranski ideal kolobarja K. Ker je K enostaven, je potem $Kx = K$. Torej obstaja $y \in K$, da je $yx = 1$. Ker je x v centru, je tudi $xy = 1$, torej je x obrnljiv v K. Preverimo še, da je $x^{-1} \in Z(K)$: Naj bo $z \in K$ poljuben. Potem je $xz = zx$. Če množimo to enačbo z leve in desne z x^{-1}, dobimo $zx^{-1} = x^{-1}z$. Torej je res $x^{-1} \in Z(K)$ in je x obrnljiv v $Z(K)$. Ker je bil $x \neq 0$ poljuben, je torej $Z(K)$ obseg.

4. Poišči vse vrednosti a v kolobarju $\mathbb{Z}_3$, za katere je $\mathbb{Z}_3[X]/(X^3 + X^2 + aX + 1)$ obseg.

   Rešitev: Ta kolobar bo obseg natanko tedaj, ko bo $(X^3 + X^2 + aX + 1)$ maksimalni ideal, ali ekvivalentno, praideal, to pa bo natanko tedaj, ko bo polinom $p(X) = X^3 + X^2 + aX + 1$ nerazcepen. To pa bo natanko tedaj, ko ne bo imel ničle v $\mathbb{Z}_3$. (Če bi imel ničlo, bi bil očitno razcepen, in obratno, če bi bil razcepen, tedaj bi bil deljiv s polinomom stopnje 1 in bi zato imel ničlo.) Izračunamo $p(0) = 1$, $p(1) = a$ in $p(2) = 1 - a$. Torej mora biti $a \neq 0$ in $a \neq 1$. Edina možnost je $a = 2$.

5. Naj bo K kolobar zgornje trikotnih matrik $K = \{\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \mid x, y, z \in \mathbb{R}\}$.

(a) Pokaži, da so obrnljivi elementi v K točno vse matrike $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)$, kjer $x, z \neq 0$.

(b) Ideal I kolobarja K se imenuje *maksimalen*, če je $I \neq K$ in če ne obstaja dvostranski ideal $I \subsetneq I' \subsetneq K$. Pokaži, da sta $I_1 = \{\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \mid x, y \in \mathbb{R}\}$ in $I_2 = \{\left(\begin{smallmatrix} 0 & y \\ 0 & z \end{smallmatrix}\right) \mid y, z \in \mathbb{R}\}$ maksimalna ideala kolobarja K.

Rešitev:

(a) Vsaka matrika $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)$, kjer $x, z \neq 0$, je obrnljiva v K, saj ima inverz $\frac{1}{xz}\left(\begin{smallmatrix} z & -y \\ 0 & x \end{smallmatrix}\right) \in K$. Obratno, če je $A = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)$ obrnljiva v K, je obrnljiva v $M_2(\mathbb{R})$ in zato $\det(A) = xz \neq 0$, torej $x, z \neq 0$.

(b) Najprej vidimo, da je I_1 očitno zaprt za seštevanje. Velja tudi $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)\left(\begin{smallmatrix} u & v \\ 0 & 0 \end{smallmatrix}\right) \in I_1$ in $\left(\begin{smallmatrix} u & v \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in I_1$ za poljubne $u, v, x, y, z \in \mathbb{R}$, torej je I_1 ideal v K. Podobno vidimo, da je tudi I_2 ideal.

Preverimo še maksimalnost. Naj bo $I_1 \subsetneq I$ za nek ideal I. Izberimo $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in I \backslash I_1$. Torej je $z \neq 0$. Ker je $\left(\begin{smallmatrix} 1-x & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I_1 \subseteq I$, je potem $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1-x & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & y \\ 0 & z \end{smallmatrix}\right) \in I$. Ta matrika pa je obrnljiva. Torej I vsebuje obrnljiv element in zato $I = K$. Torej je I_1 maksimalni ideal. Podobno preverimo, da je tudi I_2 maksimalni ideal.