Janez Šter

Zbirka rešenih nalog iz Algebre 2

Julij 2021

Predgovor

V tej zbirki so zbrane naloge z rešitvami s preverjanj znanja pri predmetu Algebra 2 za 2. letnik univerzitetnega študija 1. stopnje Matematika na Fakulteti za matematiko in fiziko Univerze v Ljubljani. Izpitne naloge so iz let, ko sem bil asistent pri tem predmetu, in sicer 2011/12, 2012/13, 2014/15 in 2020/21. Iz leta 2020/21 so zbrane le naloge dveh izpitnih rokov, iz preostalih let pa so zbrane naloge vseh petih izpitov/kolokvijev za vsako leto. Skupaj torej zbirka vsebuje 17 izpitov in kolokvijev.

Vsem nalogam so priložene rešitve. Rutinski premisleki v nekaterih rešitvah so izpuščeni, zato je zbirka primerna predvsem kot dodatna priprava na izpite ali kolokvije, medtem ko je osnova za pripravo seveda snov predavanj in vaj pri predmetu. Bralcu bodo rešitve nalog morda koristne tudi pri učenju matematičnega izražanja.

Notacija, uporabljena v rešitvah nalog, je večinoma enotna. Kljub temu je nekaj minimalnih razlik, ki pa bralca ne bi smele zmesti. Nekaj je tudi drobnih vsebinskih razlik, ki so posledica drugačnega podajanja snovi na predavanjih ali vajah v različnih letih. Tako na primer beseda 'kolobar' v nekaterih nalogah pomeni kolobar z enoto (enico), medtem ko spet v drugih le kolobar, ki nima nujno enote. Pomen teh izrazov bo bralec brez težav razbral iz konteksta naloge in njene rešitve.

Poleg tega se je z leti lahko minimalno spremenila tudi snov predmeta, zato se med nalogami za kakšno leto lahko izjemoma najde tudi takšna, ki je snov predmeta v kakšnem drugem letu ni zaobjela.

Ljubljana, julij 2021 Janez Šter

Kazalo

1. kolokvij 2011/12

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, saj je že v predpostavkah naloge navedeno, da je $\circ$ operacija na množici A. Dokaz, da A 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 $G = (\mathbb{C} \setminus \{0\}, \cdot)$ 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 $H \triangleleft G$.

Dokažimo, da je $G/H \cong (\mathbb{R}^+, \cdot)$, tako da poiščem surjektivni homomorfizem $f : G \to \mathbb{R}^+$ z jedrom H. Definirajmo $f(z) = |z|$. Potem je f homomorfizem, saj $f(zw) = |zw| = |z||w| = f(z)f(w)$. Homomorfizem f je surjektiven, saj za vsak $a \in \mathbb{R}^+$ velja $f(a) = |a| = a$, torej $a \in \mathrm{im}(f)$. Jedro f je $\{z \in G, f(z) = 1\} = \{z \in G, |z| = 1\} = H$. (Preverjanje, da je H podgrupa edinka, je bilo v resnici nepotrebno, saj je jedro homomorfizma vselej podgrupa edinka.)

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

$$gzg^{-1}h = gz(g^{-1}hg)g^{-1} = g(g^{-1}hg)zg^{-1} = hgzg^{-1},$$

kot je bilo potrebno dokazati.

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

$$f(a, b) = f(a, 0) + f(0, b) = f(1, 0) + \cdots + f(1, 0) + f(0, 1) + \cdots + f(0, 1) = af(1, 0) + bf(0, 1).$$

(Na drugi komponenti operacijo $+$ gledamo po modulu 2, enakost pa seveda velja tudi za negativne a in b.) 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 $\langle x \rangle$ podgrupa moči 7, torej bi bila enaka eni od osmih podgrup Sylowa, kar je protislovje).

2. kolokvij 2011/12

1. Poišči vse neizomorfne Abelove grupe moči 200.

   Rešitev: Vsaka končna Abelova grupa je do izomorfizma natančno enaka

   $$\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}},$$

   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 $x \in D \setminus \{0\}$. 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. (Pozor: vnaprej ne smemo predpostaviti, da je I oblike $I = A_1 \times A_2$ za neki podmnožici $A_i \subseteq K_i$. Takšnim podmnožicam množice K pravimo *škatlaste* podmnožice.)

   Dokažimo, da je podmnožica I škatlasta. Definirajmo

   $$I_1 = \{x \in K_1, (x, 0) \in I\} \quad \text{in} \quad I_2 = \{y \in K_2, (0, y) \in I\}.$$

   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 $r(X)$. Odtod 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 $\{p;\ p \mid m \text{ in } p \mid n\}$ prazna množica. Torej sta m in n tuji si števili.

1. izpit 2011/12

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

   $$f(q) = f(n \cdot \frac{q}{n}) = f(\frac{q}{n} + \cdots + \frac{q}{n}) = f(\frac{q}{n}) + \cdots + f(\frac{q}{n}) = nf(\frac{q}{n}) \in n\mathbb{Z}.$$

   Torej je $f(q)$ deljiv 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

   $$\varphi : A \hookrightarrow S(G), \quad \varphi(f) = f.$$

   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 $p \mid |\overline{x}|$. 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

   $$f : \mathbb{R}[X] \to K, \quad p_0 + p_1 X + \ldots + p_n X^n \mapsto \begin{bmatrix} p_0 & p_1 \\ 0 & p_0 \end{bmatrix}.$$

   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.

2. izpit 2011/12

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

   $$\begin{aligned} f((g_1, g_2)(g_1', g_2')) &= f(g_1g_1', g_2g_2') = (g_1g_1'H_1, g_2g_2'H_2) \\ &= (g_1H_1, g_2H_2)(g_1'H_1, g_2'H_2) = f(g_1, g_2)f(g_1', g_2') \end{aligned}$$

   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 $a \in K \setminus I$ 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

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

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

   Rešitev: V dokaz, da je 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 $q = \frac{m}{n} \in J \setminus I$. 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 $J = K$.

3. izpit 2011/12

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 opisanih 20 grup.

3. Naj bo K kolobar z enico. Označimo z $Z(K)$ center kolobarja K, to je

   $$Z(K) = \{x \in K \mid xy = yx \text{ za vsak } y \in K\}.$$

   (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

   $$z(x-y) = zx - zy = xz - yz = (x-y)z \quad \text{in} \quad z(xy) = zxy = (xy)z,$$

   torej $x - y \in Z(K)$ in $xy \in Z(K)$. 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 $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in I \setminus I_1$. 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.

1. kolokvij 2012/13

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

   Rešitev: Grupo D_{2n}, kot običajno, predstavimo kot množico

   $$D_{2n} = \{\pi^i \rho^j \mid i = 0, 1, \ldots, n-1,\ j = 0, 1\}.$$

   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 je $\pi^{2i} = \mathrm{id}$ in zato $n \mid 2i$. Ker je n liho, sledi $n \mid i$, 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 $n \mid 2$, 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 $f(x) = \left\{ \begin{smallmatrix} 0, & x>0 \\ 1, & x<0 \end{smallmatrix} \right.$ (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 $HK = \{hk \mid h \in H, k \in K\}$.)

   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 $\langle a, b \mid ab = ba\rangle \cong \mathbb{Z} \times \mathbb{Z}$ (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 $f : \langle a, b \mid ab = ba\rangle \to \mathbb{Z} \times \mathbb{Z}$, ki slika a v α in b v β. Pokažimo, da je f izomorfizem. Definirajmo preslikavo

   $$g : \mathbb{Z} \times \mathbb{Z} \to \langle a, b \mid ab = ba\rangle, \quad (m, n) \mapsto a^m b^n.$$

   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.

2. kolokvij 2012/13

1. Poišči vse neizomorfne Abelove grupe moči 3000.

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

2. Naj bo K kolobar in $e \in K$ idempotent. Pokaži, da je $eKe = \{exe \mid x \in K\}$ 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
   $$f : K \to \mathbb{R} \times \mathbb{R}, \quad f(\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)) = (a, c).$$
   Hitro lahko preverimo, da je f homomorfizem kolobarjev. Očitno je f surjektiven. Njegovo jedro pa je točno
   $$\ker(f) = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in K \mid f(\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)) = 0\} = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in K \mid (a, c) = (0, 0)\} = \{\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \in K\} = I.$$
   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 $k \mid 4$, torej $k = 1$. Torej obstaja v G podgrupa edinka H moči 5^3. Vsaka grupa moči p^n, kjer je 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.

1. izpit 2012/13

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: Števila $3, 4, 5, 7$ so paroma tuja, torej je največji skupni delitelj števil $4 \cdot 5 \cdot 7 = 140$, $3 \cdot 5 \cdot 7 = 105$, $3 \cdot 4 \cdot 7 = 84$ in $3 \cdot 4 \cdot 5 = 60$ enak 1. Zato rešitev lahko iščemo z nastavkom

$$x = 140a + 105b + 84c + 60d, \quad a, b, c, d \in \mathbb{Z}.$$

Dobimo sistem

$$\begin{aligned} 140a &\equiv 2 \pmod 3, \\ 105b &\equiv 3 \pmod 4, \\ 84c &\equiv 4 \pmod 5, \\ 60d &\equiv 5 \pmod 7, \end{aligned}$$

kar se poenostavi v $-a \equiv 2 \pmod 3$, $b \equiv 3 \pmod 4$, $-c \equiv 4 \pmod 5$ in $4d \equiv 5 \pmod 7$. Hitro lahko najdemo eno od rešitev: $a = 1$, $b = -1$, $c = 1$, $d = 3$. Dobimo $x = 299$, torej je splošna rešitev

$$x = 299 + 420n, \quad n \in \mathbb{Z}.$$

(Število 420 je tu seveda najmanjši skupni večkratnik števil 140, 105, 84 in 60.)

2. Naj bo dana grupa $G = \{z \in \mathbb{C} \mid |z| = 1\}$ 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

$$f : G \to G, \quad f(z) = z^2.$$

Preslikava f je dobro definirana, saj je $|z^2| = |z| \cdot |z| = 1$ za vsak $z \in G$. Velja tudi

$$f(zw) = (zw)^2 = z^2 w^2 = f(z)f(w)$$

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

$$\ker(f) = \{z \in G \mid z^2 = 1\} = \{1, -1\} = H,$$

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 $I = \{f \in K \mid \mathrm{im}(f) \leq H\}$. 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

$$\varphi : G \to S(G/H), \quad g \mapsto (aH \mapsto gaH).$$

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. izpit 2012/13

1. Naj bo $G = \{\left(\begin{smallmatrix} x & x-y \\ 0 & y \end{smallmatrix}\right) \mid x, y \in \mathbb{R} \setminus \{0\}\}$. 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

   $$f : (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\}) \to \mathrm{GL}_2(\mathbb{R}), \quad f(x,y) = \begin{pmatrix} x & x-y \\ 0 & y \end{pmatrix}.$$

   Preslikava je dobro definirana, saj je matrika $\left(\begin{smallmatrix} x & x-y \\ 0 & y \end{smallmatrix}\right)$ 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 $7^{40} = 1 \pmod{100}$ in zato $7^{7^{70}} = 7^{7^{70} \pmod{40}} \pmod{100}$. Nadalje, velja $\varphi(40) = 16$, torej $7^{16} = 1 \pmod{40}$ in zato

   $$7^{70} = 7^{70 \pmod{16}} = 7^6 = 49^3 = 9^3 = 81 \cdot 9 = 9 \pmod{40}.$$

   Odtod dobimo

   $$7^{7^{70}} = 7^9 = 343^3 = 43^3 = 79507 = 7 \pmod{100}.$$

   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 $H = PQ$.

3. izpit 2012/13

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 $K = \{\frac{a}{b} \in \mathbb{Q} \mid 2 \nmid b,\ 5 \nmid b\}$. 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 (tj. 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

$$f : \mathbb{Q}^+ \to \bigoplus_{n \in \mathbb{Z}} \mathbb{Z}, \quad f(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}) = (\alpha_1, \alpha_2, \ldots, \alpha_k, 0, 0, \ldots).$$

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

$$A = 0 \oplus \ldots \oplus 0 \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus 0 \oplus \ldots \oplus 0 \quad \text{in} \quad B = 0 \oplus \ldots \oplus 0 \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus 0 \oplus \ldots \oplus 0,$$

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 $\alpha \geq 0$.

1. kolokvij 2014/15

1. Naj bo $G = \{\left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right] \mid a, b \in \{1, -1\},\ x \in \mathbb{Z}\}$.

   (a) Preveri, da je G grupa za matrično množenje.

   (b) Dokaži, da grupa G ni Abelova.

   (c) Dokaži, da je G končno generirana.

   (d) Naj bo $H = \{\left[\begin{smallmatrix} a & x \\ 0 & 1 \end{smallmatrix}\right] \mid a \in \{1, -1\},\ x \in 2\mathbb{Z}\} \subseteq G$. Dokaži, da je H podgrupa edinka v G (pokaži tudi, da je podgrupa).

   (e) Dokaži, da je G/H grupa moči 4.

   (f) Dokaži, da je $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

   Rešitev: (a) Očitno je $G \subseteq GL_2(\mathbb{R})$. Za poljubna $\left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right], \left[\begin{smallmatrix} c & y \\ 0 & d \end{smallmatrix}\right] \in G$ velja tudi

   $$\left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right]\left[\begin{smallmatrix} c & y \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} ac & ay+dx \\ 0 & bd \end{smallmatrix}\right] \in G \quad \text{in} \quad \left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} a & -abx \\ 0 & b \end{smallmatrix}\right] \in G,$$

   torej je $G \leq GL_2(\mathbb{R})$.

   (b) Velja $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \neq \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.

   (c) Preverimo, da množica

   $$X = \{\left[\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right] \mid a, b \in \{1, -1\}\} \cup \{\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\}$$

   generira grupo G. Vzemimo $A = \left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right] \in G$. Potem je $A = \left[\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & ax \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]^{ax}$ in zato res $A \in \langle X \rangle$.

   (d) Za poljubna $\left[\begin{smallmatrix} a & x \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} b & y \\ 0 & 1 \end{smallmatrix}\right] \in H$ je $\left[\begin{smallmatrix} a & x \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} b & y \\ 0 & 1 \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} ab & x-aby \\ 0 & 1 \end{smallmatrix}\right] \in H$, saj $x - aby \in 2\mathbb{Z}$. Za poljuben $\left[\begin{smallmatrix} c & z \\ 0 & d \end{smallmatrix}\right] \in G$ je tudi $\left[\begin{smallmatrix} c & z \\ 0 & d \end{smallmatrix}\right]\left[\begin{smallmatrix} a & x \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} c & z \\ 0 & d \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} a & cdx+(d-ad)z \\ 0 & 1 \end{smallmatrix}\right] \in H$, saj $cdx \in 2\mathbb{Z}$ in $d - ad \in 2\mathbb{Z}$. Torej je res $H \triangleleft G$.

   (e) Preverimo, da so $\left[\begin{smallmatrix} 1 & x \\ 0 & a \end{smallmatrix}\right]H$, $a \in \{1, -1\}$, $x \in \{0, 1\}$, natanko vsi paroma različni levi odseki grupe G/H. Najprej vidimo, da so paroma različni. Res, denimo, da je $\left[\begin{smallmatrix} 1 & x \\ 0 & a \end{smallmatrix}\right]H = \left[\begin{smallmatrix} 1 & y \\ 0 & b \end{smallmatrix}\right]H$, kjer je $a, b \in \{1, -1\}$ in $x, y \in \{0, 1\}$. Potem je $\left[\begin{smallmatrix} 1 & y \\ 0 & b \end{smallmatrix}\right]^{-1}\left[\begin{smallmatrix} 1 & x \\ 0 & a \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & x-aby \\ 0 & ab \end{smallmatrix}\right] \in H$, od koder sledi $a = b$ in $x - aby \in 2\mathbb{Z}$. Dobimo $x - y \in 2\mathbb{Z}$, torej $x = y$.

   Preverimo še, da so to vsi elementi. Naj bo $\chi = \left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right]H \in G/H$ poljuben levi odsek. Pišimo $x = x_0 + 2t$, kjer je $x_0 \in \{0, 1\}$. Potem je $\chi = \left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right]H = \left[\begin{smallmatrix} 1 & x_0 \\ 0 & b \end{smallmatrix}\right]\left[\begin{smallmatrix} a & 2t \\ 0 & 1 \end{smallmatrix}\right]H = \left[\begin{smallmatrix} 1 & x_0 \\ 0 & b \end{smallmatrix}\right]H$, torej je χ res enak enemu od zgoraj naštetih 4 elementov. S tem smo pokazali $|G/H| = 4$.

   (f) Edini grupi moči 4 sta $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$. Ker v $\mathbb{Z}_4$ obstaja element reda 4, zadošča preveriti, da so vsi elementi v G/H reda kvečjemu 2. Vzemimo poljuben $\chi = \left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right]H \in G/H$. Potem je res $\chi^2 = \left[\begin{smallmatrix} a & x \\ 0 & b \end{smallmatrix}\right]^2 H = \left[\begin{smallmatrix} 1 & (a+b)x \\ 0 & 1 \end{smallmatrix}\right]H = H$, saj je $(a + b)x \in 2\mathbb{Z}$.

2. (a) Naj bo $n \geq 3$, G grupa in $H_1, H_2, \ldots, H_n \triangleleft G$ njene podgrupe edinke, tako da velja $G = H_iH_j$ in $H_i \cap H_j = 1$ za poljubna $i \neq j$. Dokaži, da je $H_i \cong H_j$ za poljubna $i \neq j$. (Namig: pomagaj si z enim od izrekov o izomorfizmih.)

   (b) S primerom pokaži, da zgornja trditev ne velja za $n = 2$.

   Rešitev: (a) Naj bo $i \neq j$. Izberimo še $k \in \{1, 2, \ldots, n\}$, tako da je $k \neq i$ in $k \neq j$. Potem je po izreku o izomorfizmih

   $$H_i \cong H_i/(H_i \cap H_k) \cong (H_iH_k)/H_k = G/H_k = (H_jH_k)/H_k \cong H_j/(H_j \cap H_k) \cong H_j.$$

   (b) Naj bo G poljubna netrivialna grupa, $H_1 = 1 \leq G$ in $H_2 = G$. Potem je $H_1, H_2 \triangleleft G$, $H_1H_2 = G$, $H_1 \cap H_2 = 1$ in $H_1 \ncong H_2$.

3. Naj bo $n \geq 2$. Označimo grupo $G = S_n$ in množico $X = \mathbb{R}^n$. Za vsak $\pi \in G$ definirajmo bijekcijo $f_\pi : X \to X$ s predpisom

   $$f_\pi(x_1, x_2, \ldots, x_n) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}).$$

   (Preslikava f_π je res bijekcija na množici X, česar ni potrebno preverjati.)

   (a) Dokaži, da predpis

   $$\varphi : G \to S(X), \qquad \varphi(\pi) = f_{\pi^{-1}}$$

   podaja delovanje grupe G na množici X.

   (b) Določi stabilizator G_u in orbito $\overline{u}$ za $n = 3$ in $u = (2, 3, 3)$.

Rešitev: (a) Preslikava $\varphi : G \to S(X)$, $\pi \mapsto f_{\pi^{-1}}$, je dobro definirana, saj je $f_{\pi^{-1}} \in S(X)$ za vsak $\pi \in G$. Preverimo še, da je homomorfizem. Za poljubna $\pi, \rho \in G$ in $u = (x_1, \ldots, x_n) \in X$ je

$$\varphi(\pi\rho)(u) = (x_{(\pi\rho)^{-1}(1)}, \ldots, x_{(\pi\rho)^{-1}(n)}) = (x_{\rho^{-1}(\pi^{-1}(1))}, \ldots, x_{\rho^{-1}(\pi^{-1}(n))}).$$

Po drugi strani pa je

$$(\varphi(\pi)\varphi(\rho))(u) = \varphi(\pi)(x_{\rho^{-1}(1)}, \ldots, x_{\rho^{-1}(n)}).$$

Če označimo $y_i = x_{\rho^{-1}(i)}$, potem je

$$(\varphi(\pi)\varphi(\rho))(u) = \varphi(\pi)(y_1, \ldots, y_n) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}) = (x_{\rho^{-1}(\pi^{-1}(1))}, \ldots, x_{\rho^{-1}(\pi^{-1}(n))}).$$

Torej je res $\varphi(\pi\rho)(u) = (\varphi(\pi)\varphi(\rho))(u)$. Ker to velja za vsak u, je $\varphi(\pi\rho) = \varphi(\pi)\varphi(\rho)$.

(b) Pišimo $x_1 = 2$ in $x_2 = x_3 = 3$, tako da je $u = (x_1, x_2, x_3)$. Iščemo vse $\pi \in G$, za katere je $\varphi(\pi)(u) = u$. Pogoj $\varphi(\pi)(u) = u$ velja natanko tedaj, ko je $(x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, x_{\pi^{-1}(3)}) = (2, 3, 3)$. To pa je ekvivalentno pogoju $\pi^{-1}(1) = 1$ in zato $G_u = \{\pi \in G |\ \pi^{-1}(1) = 1\} = \langle (2, 3) \rangle$.

Orbita $\overline{u}$ pa je

$$\overline{u} = \{\varphi(\pi)(u) |\ \pi \in G\} = \{(x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, x_{\pi^{-1}(3)}) \mid \pi \in G\} = \{(2, 3, 3), (3, 2, 3), (3, 3, 2)\}$$

(komponente $2, 3, 3$ lahko poljubno permutiramo).

4. Naj bo G grupa moči 350.

   (a) Dokaži, da grupa G vsebuje podgrupo edinko moči 25.

   (b) Dokaži, da grupa G vsebuje bodisi natanko 6 bodisi natanko 300 elementov reda 7.

   (c) Dokaži, da grupa G vsebuje podgrupo edinko moči 175. (Nasvet: pokaži, da G vsebuje podgrupo moči 175.)

   Rešitev: (a) Razcepimo $|G| = 2 \cdot 5^2 \cdot 7$. Označimo z s_5 število 5-podgrup Sylowa, torej podgrup moči 25. Po izrekih Sylowa je $s_5 \mid 2 \cdot 7$ in $s_5 \equiv 1 \pmod 5$. Edina možnost je $s_5 = 1$.

   (b) Označimo z s_7 število 7-podgrup Sylowa. Podobno kot prej dobimo, da sta edini dve možnosti $s_7 = 1$ ali $s_7 = 50$. Če je $s_7 = 1$, potem imamo natanko 1 podgrupo moči 7, označimo jo s H_1, ki vsebuje 6 elementov reda 7. To so tudi vsi elementi reda 7, saj bi vsak drug tak element $a \notin H_1$ generiral neko novo podgrupo moči 7, kar je protislovje. Če pa je $s_7 = 50$, potem so $H_1, \ldots, H_{50}$ vse podgrupe moči 7. Te grupe so paroma disjunktne, saj so praštevilske moči, torej je v njih natanko $6 \cdot 50 = 300$ elementov reda 7. To so tudi vsi elementi reda 7, saj bi vsak drug element $a \notin H_1 \cup \ldots \cup H_{50}$ reda 7 generiral neko novo podgrupo moči 7, kar je protislovje.

   (c) Po točki (a) obstaja podgrupa edinka H moči 25, vemo pa tudi, da obstaja vsaj ena podgrupa K moči 7. Produkt podgrupe edinke in podgrupe je spet podgrupa. Torej je $HK \leq G$. Ta grupa ima moč kvečjemu $|H| \cdot |K|$, saj vsak element $g \in HK$ lahko zapišemo kot $g = g_1 g_2$, kjer imamo za $g_1 \in H$ le $|H|$ možnosti in za $g_2 \in K$ le $|K|$ možnosti. Moč grupe pa je tudi vsaj $|H| \cdot |K|$, saj je deljiva tako z $|H|$ kot s $|K|$ in sta si $|H|$ in $|K|$ tuji števili. Sklepamo, da je $|HK| = |H| \cdot |K| = 175$. Ker je HK podgrupa indeksa dva v G, je tudi $HK \triangleleft G$.

2. kolokvij 2014/15

1. Dana je grupa $G = \mathbb{Z} \oplus \mathbb{Z}/\langle(4,2)\rangle$.

   (a) V grupi G poišči element reda 2 in element neskončnega reda.

   (b) Utemelji, zakaj v grupi G obstaja natanko 1 element končnega reda (poleg enote).

   (c) Kateri znani grupi je izomorfna grupa G?

   Rešitev: (a) Element $(2,1) + \langle(4,2)\rangle$ je reda 2, element $(1,0) + \langle(4,2)\rangle$ pa neskončnega reda.

   (b) Naj bo $\alpha = (a,b) + \langle(4,2)\rangle \in G$ poljuben element končnega reda. Potem je $k\alpha = 0$ za nek $k \geq 1$, torej $(ka, kb) \in \langle(4,2)\rangle$, kar pa pomeni $(ka, kb) = (4n, 2n)$ za nek $n \in \mathbb{Z}$. Odtod sledi $a = 2b$, torej je α večkratnik elementa $(2,1) + \langle(4,2)\rangle$. Edini neničelni večkratnik tega elementa pa je ravno $(2,1) + \langle(4,2)\rangle$.

   (c) G je Abelova grupa, generirana z dvema elementoma (saj je homomorfna slika grupe $\mathbb{Z} \oplus \mathbb{Z}$). Torej je $G \cong \mathbb{Z} \oplus \mathbb{Z}$, $G \cong \mathbb{Z} \oplus \mathbb{Z}_n$, $G \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ za neka m, n, ali pa je G ciklična. Ker G vsebuje element neskončnega reda in natanko en element končnega reda, pride v poštev le možnost $\mathbb{Z} \oplus \mathbb{Z}_n$, kjer je $n = 2$. Torej $G \cong \mathbb{Z} \oplus \mathbb{Z}_2$.

2. Naj bo $R = (R, +, \cdot)$ kolobar z enico in $a \in R$ nek element. Na množici R definirajmo operacijo $*$ s predpisom $x * y = xay$.

   (a) Preveri, da je $R_a = (R, +, *)$ kolobar.

   (b) Dokaži, da je R_a kolobar z enico natanko tedaj, ko je a obrnljiv v R.

   (c) Dokaži, da je R_a kolobar z enico natanko tedaj, ko sta kolobarja R_a in R izomorfna.

   Rešitev: (a) Ker je R kolobar, je $(R, +)$ Abelova grupa. Hitro vidimo, da velja

   $$(x + y) * z = xaz + yaz = x * z + y * z, \quad x * (y + z) = xay + xaz = x * y + x * z$$

   in

   $$(x * y) * z = xayaz = x * (y * z)$$

   za poljubne $x, y, z \in R_a$.

   (b) Denimo, da je R_a kolobar z enico e. Potem je $1 * e = 1$ (kjer je 1 enica kolobarja R), torej $1ae = 1$. Odtod vidimo, da ima a desni inverz. Podobno dobimo, da iz $e*1 = 1$ sledi, da ima a levi inverz. Obratno, denimo, da je a obrnljiv v R. Hitro se lahko prepričamo, da je potem a^{-1} enica kolobarja R_a.

   (c) Denimo najprej, da je R_a kolobar z enico. Torej je a obrnljiv. Definirajmo preslikavo $f : R_a \to R$, $f(x) = xa$. Ta preslikava je homomorfizem kolobarjev, saj je

   $$f(x + y) = (x + y)a = xa + ya = f(x) + f(y) \quad \text{in} \quad f(x * y) = f(xay) = xaya = f(x)f(y)$$

   za poljubna $x, y \in R_a$. Očitno je f tudi bijektivna preslikava z inverzom $x \mapsto xa^{-1}$ in zato izomorfizem. Obratno, če sta kolobarja R_a in R izomorfna, potem ima R_a enico, saj ima R enico.

3. Naj bo R podkolobar realnih števil $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\,;\ a, b \in \mathbb{Z}\}$ in I podmnožica $I = \{a + b\sqrt{2}\,;\ 4 \mid a \text{ in } 2 \mid b\}$.

   (a) Dokaži, da je I ideal v R. Dokaži še, da je glavni ideal.

   (b) Ali je I maksimalni ideal?

   Rešitev: (a) Velja

   $$(2\sqrt{2}) = \{(a + b\sqrt{2})2\sqrt{2} \mid a, b \in \mathbb{Z}\} = \{4b + 2a\sqrt{2} \mid a, b \in \mathbb{Z}\} = I,$$

   torej je I glavni ideal.

   (b) I ni niti praideal, saj je $2, \sqrt{2} \notin I$ in $2\sqrt{2} \in I$.

4. Naj bo R komutativen kolobar in P njegov ideal.

   (a) Dokaži: če je P praideal, potem iz $I \cap J \subseteq P$ sledi $I \subseteq P$ ali $J \subseteq P$ za poljubna ideala I, J v R.

   (b) S primerom pokaži, da obratno ne drži. (To je, poišči primer kolobarja R in ideala P, tako da P ni praideal v R in iz $I \cap J \subseteq P$ sledi $I \subseteq P$ ali $J \subseteq P$ za poljubna ideala I, J v R.)

Rešitev: (a) Naj bo P praideal in I, J ideala, tako da je $I \cap J \subseteq P$. Denimo, da je $I \nsubseteq P$ in $J \nsubseteq P$. Vzemimo $x \in I \setminus P$ in $y \in J \setminus P$. Potem je $xy \in I$ in $xy \in J$, torej $xy \in P$. To pa je protislovje, saj $x \notin P$ in $y \notin P$.

(b) Vzemimo $R = \mathbb{Z}_4$ in $P = 0$. Potem P ni praideal, saj R/P ni cel kolobar. Edini ideali v R pa so 0, $\mathbb{Z}_4$ in $2\mathbb{Z}_4$. Za poljubna dva I, J med temi pa je implikacija $I \cap J = 0 \Rightarrow (I = 0$ ali $J = 0)$ očitno izpolnjena.

5. Poišči vse $n \in \mathbb{N}$, za katere je $15^{18^n} \equiv 9\ (11)$.

   Če naloge ne znaš rešiti v splošnosti, potem preveri, da je $n = 9$ rešitev zgornje kongruence.

   Rešitev: Izberimo nek $n \in \mathbb{N}$. Želimo izračunati $15^{18^n}\ (11)$. Po Fermatovem izreku je $15^{10} \equiv 1\ (11)$. Torej želimo izračunati $18^n\ (10)$. Seveda je $18^n \equiv 0\ (2)$, po Fermatovem izreku pa tudi $18^4 \equiv 1\ (5)$, torej $18^n \equiv 18^{n\ (4)}\ (5)$. Odtod vidimo, da moramo obravnavati 4 možnosti. Najprej, če je $n \equiv 0\ (4)$, potem je $18^n \equiv 18^0 \equiv 1\ (5)$, kar nam da $18^n \equiv 6\ (10)$ in zato $15^{18^n} \equiv 15^6 \equiv 4^6 \equiv 16^3 \equiv 5^3 \equiv 125 \equiv 4\ (11)$. Naslednja možnost, če je $n \equiv 1\ (4)$, je $18^n \equiv 18 \equiv 3\ (5)$, torej $18^n \equiv 8\ (10)$ in zato $15^{18^n} \equiv 15^8 \equiv 4^8 \equiv 16^4 \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9\ (11)$. Podobno za $n \equiv 2\ (4)$ dobimo $15^{18^n} \equiv 3\ (11)$, za $n \equiv 3\ (4)$ pa $15^{18^n} \equiv 5\ (11)$. Rešitve so torej natanko $n = 4k + 1$, $k \geq 0$.

1. izpit 2014/15

1. Poišči vsa cela števila, ki rešijo sistem kongruenc:

$$\begin{aligned} x &\equiv 1 \quad (3) \\ x &\equiv 2 \quad (5) \\ x &\equiv 3 \quad (7) \\ x &\equiv 4 \quad (8) \end{aligned}$$

Rešitev: Iz prve enačbe dobimo $x = 3a + 1$. Druga enačba nam da $5 \mid 3a - 1$, torej $5 \mid 2(3a - 1) = 6a - 2$ in zato $5 \mid a - 2$. Torej $a = 5b + 2$ in $x = 15b + 7$.

Tretja enačba nam da $7 \mid 15b+4$, torej $7 \mid b+4$, od koder sledi $b = 7c+3$ in $x = 15 \cdot 7c+52$. Zadnja enačba pa nam da $8 \mid 15 \cdot 7c + 48$, torej $8 \mid (-1)(-1)c$ in zato $c = 8d$. Končna rešitev je tako $x = 15 \cdot 7 \cdot 8d + 52$, $d \in \mathbb{Z}$.

2. Naj bo R kolobar matrik $R = \{\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right] \mid a, b \in \mathbb{Z}\}$ za običajno matrično seštevanje in množenje.

   (a) Preveri, da je R komutativen.

   (b) Naj bo I ideal, generiran z matriko $A = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. Opiši vse elemente ideala I.

   (c) Ali je I praideal?

   Rešitev: (a) Za poljubni matriki $\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right], \left[\begin{smallmatrix} c & d \\ 0 & c \end{smallmatrix}\right] \in R$ hitro preverimo

$$\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right]\left[\begin{smallmatrix} c & d \\ 0 & c \end{smallmatrix}\right] = \left[\begin{smallmatrix} ac & ad+bc \\ 0 & ac \end{smallmatrix}\right] = \left[\begin{smallmatrix} c & d \\ 0 & c \end{smallmatrix}\right]\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right].$$

   (b) Ker smo v komutativnem kolobarju z enico, je $I = RA = \{\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] \mid a, b \in \mathbb{Z}\} = \{\left[\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right] \mid a \in \mathbb{Z}\}$.

   (c) I je praideal. Res, če za $X = \left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right] \in R$ in $Y = \left[\begin{smallmatrix} c & d \\ 0 & c \end{smallmatrix}\right] \in R$ velja $XY \in I$, potem je $ac = 0$, od koder sledi $a = 0$ ali $c = 0$, torej $X \in I$ ali $Y \in I$.

3. (a) Poišči vse neizomorfne Abelove grupe moči $7 \cdot 8 \cdot 9$.

   (b) Med grupami iz točke (a) poišči vse tiste, ki vsebujejo element reda 72.

   (c) Med grupami iz točke (a) si izberi najljubšo in povej, koliko ima avtomorfizmov.

   Rešitev: (a) $\mathbb{Z}_7 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9$, $\mathbb{Z}_7 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_7 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_7 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

   (b) Edina takšna grupa je $\mathbb{Z}_7 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9$.

   (c) Preštejmo avtomorfizme grupe $\mathbb{Z}_7 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{7 \cdot 8 \cdot 9}$. Vsak avtomorfizem $f : \mathbb{Z}_{7 \cdot 8 \cdot 9} \to \mathbb{Z}_{7 \cdot 8 \cdot 9}$ je že določen s sliko $f(1)$, torej je vsak f oblike $f(x) = ax$ za nek $a \in \mathbb{Z}_{7 \cdot 8 \cdot 9}$. Zaradi bijektivnosti mora biti a tuje številu $7 \cdot 8 \cdot 9$. Torej je število možnosti za a enako ravno $\varphi(7 \cdot 8 \cdot 9) = 7 \cdot 8 \cdot 9 \cdot \frac{6}{7} \cdot \frac{1}{2} \cdot \frac{2}{3} = 144$.

4. Naj bo n naravno število in m liho naravno število. Pokaži, da ne obstaja netrivialni homomorfizem grup $S_n \to \mathbb{Z}_m$. (Namig: kam se slikajo generatorji?)

   Rešitev: Naj bo $f : S_n \to \mathbb{Z}_m$ homomorfizem grup. Potem za poljubno transpozicijo $(a\ b) \in S_n$ velja $2f((a\ b)) = f((a\ b)^2) = f(\mathrm{id}) = 0$. Ker je 2 tuje številu m, sledi $f((a\ b)) = 0$. Ker je S_n generirana s transpozicijami, sledi $f = 0$.

5. Naj bo G končna grupa, katere moč je deljiva s praštevilom p. Denimo, da v G obstaja p-podgrupa edinka Sylowa H. Naj bo še K podgrupa G, katere moč je deljiva s p. Pokaži, da je potem $K \cap H$ p-podgrupa edinka Sylowa v K. (Namig: uporabi kakega od izrekov o izomorfizmih.)

   Rešitev: Pišimo $|G| = p^k r$, kjer $p \nmid r$, torej $|H| = p^k$. Pišimo še $|K| = p^l s$, kjer $1 \leq l \leq k$ in $p \nmid s$. Ker je $H \triangleleft G$, je po izreku Emmy Noether $K \cap H \triangleleft K$ in $K/(K \cap H) \cong KH/H$. Pokazati moramo še, da je $K \cap H$ p-podgrupa Sylowa v K. Ker je $K \cap H \leq H$, je $|K \cap H| = p^m$ za nek $m \leq k$. Ker je KH/H podgrupa G/H, njena moč ni deljiva s p. Torej število $\frac{|K|}{|K \cap H|} = \frac{|KH|}{|H|} = |KH/H|$ ni deljivo s p. Torej je $K \cap H$ res p-podgrupa Sylowa v K.

2. izpit 2014/15

1. Naj bo G netrivialna grupa. Pokaži, da je $\{H \mid H \triangleleft G\}$ monoid za operacijo $H_1 \circ H_2 = H_1H_2$. Ali je tudi grupa?

   Rešitev: Označimo $A = \{H \mid H \triangleleft G\}$. Očitno je A polgrupa, saj je $(H_1H_2)H_3 = H_1(H_2H_3)$ za poljubne $H_1, H_2, H_3 \triangleleft G$. Enota je trivialna grupa $E = 1$, saj je $HE = EH = H$ za vsak $H \in A$. Množica A ni grupa, saj $G \in A$ nima inverza (za vsak $H \in A$ je $GH = G \neq E$).

2. Naštej vse Abelove grupe moči 4500. Med njimi poišči tiste, v katerih so vse podgrupe Sylowa ciklične.

   Rešitev: Razcepimo $4500 = 2^2 \cdot 3^2 \cdot 5^3$. Torej dobimo 12 grup: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{125}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{125}$. Med njimi ima ciklične podgrupe Sylowa le $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{125}$.

3. Naj bo R kolobar $R = \{a + 2bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$ za običajno seštevanje in množenje. Ali sta $I = (2)$ in $J = (2i\sqrt{2})$ praideala v R?

   Rešitev: Ideal I je natanko

   $$I = \{2(a + 2bi\sqrt{2}) \mid a, b \in \mathbb{Z}\} = \{2a + 4bi\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

   Odtod vidimo, da I ni praideal, saj $2i\sqrt{2} \cdot 2i\sqrt{2} = -8 \in I$ in $2i\sqrt{2} \notin I$.

   Podobno je

   $$J = \{2i\sqrt{2}(a + 2bi\sqrt{2}) \mid a, b \in \mathbb{Z}\} = \{8a + 2bi\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

   Torej J prav tako ni praideal, saj $4 \cdot 2 = 8 \in J$ in $4, 2 \notin J$.

4. Poišči vsa naravna števila n, za katera je $n^n \equiv 2 \pmod 3$.

   Rešitev: Očitno $3 \nmid n$, torej $n \equiv 1 \pmod 3$ ali $n \equiv -1 \pmod 3$. Prva možnost odpade, saj je potem $n^n \equiv 1^n \equiv 1 \pmod 3$. V drugem primeru pa je $n^n \equiv (-1)^n$, kar je 1, če je n sodo, in -1, če je n liho. Ker mora biti $n^n \equiv -1 \pmod 3$, sledi, da je n liho. Skupaj s pogojem $n \equiv -1 \pmod 3$ dobimo $n \equiv 5 \pmod 6$, torej so rešitve natanko $n = 6k + 5$.

5. Naj bosta A in B Abelovi grupi in $\mathrm{End}(A)$, $\mathrm{End}(B)$ pripadajoča kolobarja endomorfizmov.

   (a) Za endomorfizma $\alpha \in \mathrm{End}(A)$ in $\beta \in \mathrm{End}(B)$ definirajmo preslikavo

   $$\Phi(\alpha, \beta) : A \oplus B \to A \oplus B, \quad \Phi(\alpha, \beta)(x, y) = (\alpha(x), \beta(y)).$$

   Dokaži, da je $\Phi(\alpha, \beta) \in \mathrm{End}(A \oplus B)$.

   (b) Dokaži, da preslikava

   $$\Phi : (\alpha, \beta) \mapsto \Phi(\alpha, \beta)$$

   določa injektivni homomorfizem kolobarjev $\mathrm{End}(A) \times \mathrm{End}(B) \to \mathrm{End}(A \oplus B)$.

   (c) Denimo, da so vsi homomorfizmi grup $f : A \to B$ in $g : B \to A$ enaki nič. Dokaži, da je potem Φ izomorfizem kolobarjev. (Namig: dokaži, da vsak endomorfizem $f \in \mathrm{End}(A \oplus B)$ zadošča $f(A) \subseteq A$ in $f(B) \subseteq B$.)

   Rešitev: (a) Za poljubna $(x_1, y_1), (x_2, y_2) \in A \oplus B$ je

   $$\begin{aligned}\Phi(\alpha, \beta)((x_1, y_1) + (x_2, y_2)) &= \Phi(\alpha, \beta)(x_1 + x_2, y_1 + y_2) = (\alpha(x_1 + x_2), \beta(y_1 + y_2)) \\ &= (\alpha(x_1) + \alpha(x_2), \beta(y_1) + \beta(y_2)) = (\alpha(x_1), \beta(y_1)) + (\alpha(x_2), \beta(y_2)) \\ &= \Phi(\alpha, \beta)(x_1, y_1) + \Phi(\alpha, \beta)(x_2, y_2).\end{aligned}$$

   (b) Izberimo poljubna $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \mathrm{End}(A) \times \mathrm{End}(B)$ in $(x, y) \in A \oplus B$. Potem je

   $$\begin{aligned}\Phi((\alpha_1, \beta_1) + (\alpha_2, \beta_2))(x, y) &= \Phi(\alpha_1 + \alpha_2, \beta_1 + \beta_2)(x, y) \\ &= ((\alpha_1 + \alpha_2)(x), (\beta_1 + \beta_2)(y)) = (\alpha_1(x) + \alpha_2(x), \beta_1(y) + \beta_2(y)) \\ &= (\alpha_1(x), \beta_1(y)) + (\alpha_2(x), \beta_2(y)) = \Phi(\alpha_1, \beta_1)(x, y) + \Phi(\alpha_2, \beta_2)(x, y) \\ &= (\Phi(\alpha_1, \beta_1) + \Phi(\alpha_2, \beta_2))(x, y).\end{aligned}$$

Ker to velja za poljuben $(x,y) \in A \oplus B$, sledi $\Phi((\alpha_1,\beta_1)+(\alpha_2,\beta_2)) = \Phi(\alpha_1,\beta_1)+\Phi(\alpha_2,\beta_2)$. Podobno preverimo

$$\begin{aligned}\Phi((\alpha_1,\beta_1)(\alpha_2,\beta_2))(x,y) &= \Phi(\alpha_1\alpha_2,\beta_1\beta_2)(x,y)\\ &= (\alpha_1\alpha_2(x),\beta_1\beta_2(y)) = (\alpha_1(\alpha_2(x)),\beta_1(\beta_2(y)))\\ &= \Phi(\alpha_1,\beta_1)(\alpha_2(x),\beta_2(y)) = \Phi(\alpha_1,\beta_1)\Phi(\alpha_2,\beta_2)(x,y),\end{aligned}$$

od koder sledi $\Phi((\alpha_1,\beta_1)(\alpha_2,\beta_2)) = \Phi(\alpha_1,\beta_1)\Phi(\alpha_2,\beta_2)$. Torej je Φ homorfizem kolobarjev. Injektivnost pa je očitna, saj iz $\Phi(\alpha,\beta) = 0$ za nek $(\alpha,\beta) \in \mathrm{End}(A) \times \mathrm{End}(B)$ takoj sledi $(\alpha(x),\beta(y)) = 0$ za poljuben $(x,y) \in A \oplus B$, torej $\alpha = 0$ in $\beta = 0$.

(c) Najprej preverimo trditev v namigu. Naj bo $f \in \mathrm{End}(A \oplus B)$. Označimo s $p : A \oplus B \to B$ kanonično projekcijo. Potem je $pf|_A : A \to B$ homomorfizem grup in zato $pf|_A = 0$, to je $pf(A) = 0$. To pa ravno pomeni, da je $f(A) \subseteq A$. Simetrično tudi dobimo $f(B) \subseteq B$.

Dokažimo sedaj, da je Φ surjektiven. Vzemimo poljuben $f \in \mathrm{End}(A \oplus B)$. Potem je po zgoraj dokazanem $f|_A \in \mathrm{End}(A)$ in $f|_B \in \mathrm{End}(B)$ in velja $\Phi(f|_A, f|_B)(x,y) = (f(x),f(y)) = f(x,y)$ za poljuben $(x,y) \in A \oplus B$. (Na zadnjem koraku upoštevamo, da je

$$f(x,y) = f(x+y) = f(x)+f(y) = (f(x),f(y)),$$

saj je $f(x) \in A$ in $f(y) \in B$.) Torej je res $\Phi(f|_A, f|_B) = f$ in je Φ surjektiven.

3. izpit 2014/15

1. Naj bo $n \geq 2$ naravno število. Na Abelovi grupi $R = \mathbb{Z} \oplus \mathbb{Z}_n$ definirajmo operacijo $*$ s predpisom

$$(m, x) * (n, y) = (mn, nx + my).$$

(a) Pokaži, da je $(R, +, *)$ kolobar.

(b) Ali je R komutativen kolobar? Ali ima enico?

(c) Pokaži, da je $I = 0 \times \mathbb{Z}$ ideal tega kolobarja.

(d) Ali je I praideal v R?

Rešitev: (a) Preverjanje, da je R Abelova grupa, glede na navodilo naloge ni potrebno. V dokaz asociativnosti preverimo, da je za poljubne $(m, x), (n, y), (p, z) \in R$

$$((m, x) * (n, y)) * (p, z) = (mn, nx + my) * (p, z) = (mnp, p(nx + my) + mnz) = (mnp, npx + mpy + mnz),$$

kar je enako kot

$$(m, x) * ((n, y) * (p, z)) = (m, x) * (np, py + nz) = (mnp, npx + m(py + nz)) = (mnp, npx + mpy + mnz).$$

V dokaz distributivnosti pa preverimo

$$\begin{aligned}((m, x) + (n, y)) * (p, z) &= (m + n, x + y) * (p, z) = ((m + n)p, p(x + y) + (m + n)z) \\ &= (mp + np, px + py + mz + nz) = (mp, px + mz) + (np, py + nz) \\ &= (m, x) * (p, z) + (n, y) * (p, z)\end{aligned}$$

in

$$\begin{aligned}(m, x) * ((n, y) + (p, z)) &= (m, x) * (n + p, y + z) = (m(n + p), (n + p)x + m(y + z)) \\ &= (mn + mp, nx + px + my + mz) = (mn, nx + my) + (mp, px + mz) \\ &= (m, x) * (n, y) + (m, x) * (p, z).\end{aligned}$$

(b) Kolobar je komutativen, saj za poljubna $(m, x), (n, y) \in R$ velja

$$(n, y) * (m, x) = (nm, my + nx) = (mn, nx + my) = (m, x) * (n, y).$$

Kolobar ima enico $(1, 0)$, saj je

$$(1, 0) * (x, m) = (x, m) = (x, m) * (1, 0)$$

za poljuben $(x, m) \in R$.

(c) Za poljubne $(0, x), (0, y) \in I$ in $(m, z) \in R$ je $(0, x) - (0, y) = (0, x - y) \in I$ in $(m, z)(0, x) = (0, mx) \in I$.

(d) I je praideal. Res, če za elementa $(m, x), (n, y) \in R$ velja $(m, x) * (n, y) \in I$, potem je $(mn, nx + my) \in I$, torej $mn = 0$, torej $m = 0$ ali $n = 0$, torej $(m, x) \in I$ ali $(n, y) \in I$.

2. Koliko je Abelovih grup moči 100000?

Rešitev: Razcepimo $100000 = 2^5 \cdot 5^5$. Abelovo grupo A moči 100000 lahko pišemo kot direktno vsoto $A_1 \oplus A_2$, kjer je $|A_1| = 2^5$ in $|A_2| = 5^5$. Število možnosti za grupo A_1 je je enako številu razcepov števila 5 na vsoto naravnih števil. Ti razcepi so $1+1+1+1+1$, $1+1+1+2$, $1+1+3$, $1+2+2$, $1+4$, $2+3$ in 5 (in ustrezajo grupam $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2}$, $\ldots$, $\mathbb{Z}_{2^5}$). Za grupo A_1 imamo torej 7 možnosti. Enak sklep velja tudi za grupo A_2. Za grupo A imamo torej skupaj $7 \cdot 7 = 49$ možnosti.

3. Naj bo $G = \mathbb{C} \setminus \{0\}$ grupa za množenje. Pokaži, da je $H = \{1, -1, i, -i\}$ podgrupa edinka v G in velja $G/H \cong G$.

Rešitev: Definirajmo preslikavo

$$f : G \to G, \quad f(z) = z^4.$$

Ker je $f(zw) = (zw)^4 = z^4 w^4 = f(z)f(w)$ za poljubna $z, w \in G$, je f homomorfizem grup. Očitno je f surjektiven, saj za vsak $z = re^{i\varphi} \in \mathbb{C} \setminus \{0\}$ velja $z = f(\sqrt[4]{r}e^{\frac{i\varphi}{4}})$. Ker je $\ker(f) = \{z \in G \mid z^4 = 1\} = H$, je torej H podgrupa edinka in je po izreku o izomorfizmih $G/H \cong G$.

4. Naj bo G enostavna grupa in H, K njeni podgrupi, tako da je $[G : H] = p$ in $[G : K] = q$ za neki praštevili p, q. Pokaži, da je $p = q$. (Namig: predpostavi, da je $p < q$, nato si oglej delovanje grupe G na levih odsekih podgrupe H.)

   Rešitev: Predpostavimo $p < q$ in naj G/H označuje množico levih odsekov po podgrupi H. Oglejmo si delovanje

   $$\varphi : G \to S(G/H), \quad \varphi(g)(xH) = gxH.$$

   Ker je G enostavna grupa, je bodisi $\ker(\varphi) = G$ bodisi $\ker(\varphi) = 1$. Prva možnost odpade, saj za poljuben $g \in G \setminus H$ velja $\varphi(g)(H) = gH \neq H$ in zato $\varphi(g) \neq \mathrm{id}$. Torej velja druga možnost in je zato $\varphi : G \to S(G/H)$ injektivni homomorfizem. Ker je $|S(G/H)| = |S_p| = p!$, je torej G končna grupa, njena moč pa je delitelj števila $p!$. Ker je $|G|/|K| = q$ (tu upoštevamo, da je G končna grupa), je q delitelj števila $|G|$. Torej je q delitelj števila $p!$, kar pa je v protislovju s predpostavko $p < q$.

5. Naj bo R tak kolobar z enico, da za vsak $a \in R$ obstaja natanko en $b \in R$, da velja $aba = a$. Dokaži, da je R obseg. (Nasvet: najprej dokaži, da je R cel kolobar.)

   Rešitev: Dokažimo, da je R cel kolobar. Naj bo $ax = 0$, kjer je $a, x \in R \setminus \{0\}$. Po predpostavki naloge obstaja $b \in R$, tako da je $aba = a$. Ker je tudi $a(b+x)a = aba + axa = aba = a$, je po predpostavki naloge $b = b + x$, torej $x = 0$, kar je protislovje. Torej je R cel kolobar.

   Dokažimo še, da je R obseg. Naj bo $a \in R \setminus \{0\}$. Po predpostavki naloge obstaja $b \in R$, tako da je $aba = a$. Torej je $a(ba - 1) = 0$. Ker je R cel kolobar, sledi $ba - 1 = 0$, torej $ba = 1$. Simetrično je tudi $(ab - 1)a = 0$, od koder sledi $ab - 1 = 0$ in zato $ab = 1$. Torej je a obrnljiv v R, kar je bilo potrebno dokazati.

1. izpit 2020/21

1. V množici vseh 2×2 matrik nad poljem $\mathbb{Z}_5$ je dana podmnožica

$$G = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \{1, -1\}, b \in \mathbb{Z}_5 \}$$

(kjer je $-1 = 4$ v polju $\mathbb{Z}_5$).

(a) Dokaži, da je G grupa za matrično množenje.

(b) Dokaži, da je grupa G izomorfna grupi $\mathbb{Z}_{10}$.

Rešitev: (a) Za poljubni dve matriki $A = \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ in $B = \left(\begin{smallmatrix} c & d \\ 0 & c \end{smallmatrix}\right)$ je $AB = \left(\begin{smallmatrix} ac & ad+bc \\ 0 & ac \end{smallmatrix}\right) \in G$ (saj je $ac \in \{1, -1\}$) in $A^{-1} = \left(\begin{smallmatrix} a & -b \\ 0 & a \end{smallmatrix}\right) \in G$. Torej je G podgrupa grupe $GL_2(\mathbb{Z}_5)$ in zato grupa.

(b) Lahko preverimo, da je G Abelova. Ker je $|G| = 10$ in je $\mathbb{Z}_{10}$ edina Abelova grupa moči 10, sledi $G \cong \mathbb{Z}_{10}$.

Drugi način: Ker je $|G| = 10$, zadošča preveriti, da je G ciklična. Zadošča poiskati kak element reda 10. V ta namen npr. preverimo, da red elementa $A = \left(\begin{smallmatrix} -1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ ni niti 2 niti 5, torej je lahko le 10, saj red deli moč grupe.

Tretji način: Upoštevamo, da je $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$, in poiščemo eksplicitni izomorfizem $\varphi : \mathbb{Z}_2 \oplus \mathbb{Z}_5 \to G$. Takšen izomorfizem je npr. $\varphi(a, b) = \begin{pmatrix} (-1)^a & (-1)^a b \\ 0 & (-1)^a \end{pmatrix}$.

2. Ugotovi, koliko ima diedrska grupa D_{50} podgrup moči 2, 5 in 25.

Rešitev: Pišimo $D_{50} = \{r^i z^j \mid i \in \{0, \ldots, 24\}, j \in \{0, 1\}\}$. Elementi oblike $r^i z$ so reda 2, saj je $r^i z r^i z = r^i r^{-i} z z = 1$. Elementi r^i pa so bodisi reda 1, 5 ali 25. Vsaka podgrupa moči 2 je generirana z elementom reda 2. Ker je teh elementov 25, imamo torej 25 podgrup moči 2 (ki so seveda paroma različne). Podobno je podgrupa moči 5 generirana z elementom reda 5, takšni elementi pa so v grupi štirje: $r^5, r^{10}, r^{15}, r^{20}$. Očitno vsi štirje generirajo isto pogrupo $\{1, r^5, r^{10}, r^{15}, r^{20}\}$. Podgrupa moči 5 je torej ena sama. Podgrupa moči 25 pa je $\{r^i \mid i \in \{0, \ldots, 24\}\}$ in je prav tako ena sama, saj sme vsebovati le elemente reda 1, 5 ali 25 (ki so vsi oblike r^i).

3. (a) Naj bo I neničeln ideal kolobarja $\mathbb{Z}[i]$. Dokaži, da je $\mathbb{Z}[i]/I$ končen kolobar.

(b) Kateremu kolobarju je izomorfen kolobar $\mathbb{Z}[i]/(2+i)$?

Rešitev: (a) Ker je $\mathbb{Z}[i]$ glavni kolobar, lahko pišemo $I = (a + bi)$ za nek $a + bi \in \mathbb{Z}[i]$. Ker je $a^2 + b^2 = (a + bi)(a - bi) \in I$, v kvocientnem kolobarju $\mathbb{Z}[i]/I$ velja $a^2 + b^2 + I = 0$. Torej je

$$\mathbb{Z}[i]/I = \{x + yi + I \mid 0 \leq x \leq a^2 + b^2 - 1,\ 0 \leq y \leq a^2 + b^2 - 1\},$$

ta množica pa je končna.

(b) Ker je $N(2 + i) = 5$ praštevilo, je $2 + i$ nerazcepen element. Torej je $I = (2 + i)$ maksimalni ideal (saj je $\mathbb{Z}[i]$ glavni kolobar) in zato $\mathbb{Z}[i]/(2 + i)$ polje. Ker je $5 = (2 + i)(2 - i) \in I$, ima to polje karakteristiko 5. Pokažimo, da je $\mathbb{Z}[i]/I \cong \mathbb{Z}_5$. Definirajmo

$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5, \quad \varphi(x + yi) = x - 2y$$

(element i želimo slikati v -2, saj v kvocientnem kolobarju velja $i + I = -2 + I$). Lahko se prepričamo, da je φ homomorfizem kolobarjev. Očitno je surjektiven, jedro pa vsebuje $2 + i$ in zato celoten ideal I. Ker je I maksimalni ideal in je $\ker \varphi \neq \mathbb{Z}[i]$, sledi $\ker \varphi = I$. Po izreku o izomorfizmih sledi $\mathbb{Z}[i]/I \cong \mathbb{Z}_5$.

4. Določi razpadno polje polinoma $p(X) = X^5 - 3X^3 - X^2 + 3$ nad poljem $\mathbb{Q}$. Določi še stopnjo razširitve tega razpadnega polja nad $\mathbb{Q}$.

Rešitev: Razstavimo $p(X) = (X^3 - 1)(X^2 - 3) = (X - 1)(X^2 + X + 1)(X^2 - 3)$. Ničle tega polinoma so 1, $\pm\sqrt{3}$ in $\frac{-1 \pm i\sqrt{3}}{2}$, torej je iskano razpadno polje

$$\mathbb{Q}(\sqrt{3}, \frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2}) = \mathbb{Q}(\sqrt{3}, i\sqrt{3}) = \mathbb{Q}(\sqrt{3}, i).$$

Stopnja razširitve je enaka

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

Ker sta obe stopnji na desni strani enaki 2 (prva od teh ima minimalni polinom $X^2 + 1$, druga pa $X^2 - 3$), je rezultat $2 \cdot 2 = 4$.

2. izpit 2020/21

1. Naj bo G grupa moči p^n, kjer je p praštevilo in n naravno število. Naj bo X množica vseh elementov v G maksimalnega reda. Dokaži: če je G Abelova, potem X generira G. Ali to še velja, če G ni Abelova?

   Rešitev: Naj bo m največje število, tako da obstaja v G element reda p^m. X je torej množica vseh elementov reda p^m. Naj bo $g \in G$ poljuben. Dokazati želimo, da je $g \in \langle X \rangle$.

   Če je $\mathrm{red}(g) = p^m$, je $g \in X$ in ni kaj dokazovati. Predpostavimo torej, da je $\mathrm{red}(g) = p^{m'}$, kjer je $m' < m$. Vzemimo poljuben $h \in X$. Potem je

   $$(gh)^{p^m} = g^{p^m} h^{p^m} = (g^{p^{m'}})^{p^{m-m'}} h^{p^m} = 1$$

   in

   $$(gh)^{p^{m-1}} = g^{p^{m-1}} h^{p^{m-1}} = (g^{p^{m'}})^{p^{m-m'-1}} h^{p^{m-1}} = h^{p^{m-1}} \neq 1.$$

   Torej je $\mathrm{red}(gh) = p^m$ in zato $gh \in X$. Torej je tudi v tem primeru $g = gh \cdot h^{-1} \in \langle X \rangle$.

   Pokažimo, da trditev ne velja, če G ni Abelova. Vzemimo $G = D_8$ (diedrska grupa moči 8). Označimo z $r, z \in G$ rotacijo in zrcaljenje v G kot običajno, tako da je $G = \{r^i z^j \mid i \in \{0,1,2,3\},\ j \in \{0,1\}\}$. Potem je $X = \{r, r^3\}$ (to so elementi reda 4, vsi ostali razen enote pa imajo red 2). Torej je $\langle X \rangle = \{1, r, r^2, r^3\} \neq G$.

2. Naj bo G grupa moči $5 \cdot 9 \cdot 13$. Dokaži, da v grupi G obstaja podgrupa edinka moči 65. (Nasvet: izreki Sylowa.)

   Rešitev: Označimo z n_5 in n_{13} število podgrup Sylowa moči 5 in 13. Po izrekih Sylowa je $n_5 \in \{1, 13, 3, 39, 9, 117\}$ in $n_5 = 1 \pmod 5$ ter $n_{13} \in \{1, 5, 3, 15, 9, 45\}$ in $n_{13} = 1 \pmod{13}$, od koder sledi $n_5 = 1$ in $n_{13} = 1$. Torej imamo v grupi G podgrupo edinko H moči 5 ter podgrupo edinko K moči 13. Torej je tudi HK podgrupa edinka, njena moč pa je $|HK| = |H| \cdot |K| / |H \cap K| = 5 \cdot 13 = 65$.

3. (a) Dokaži, da je 2 razcepen element v kolobarju $\mathbb{Z}[i]$ in nerazcepen v kolobarju $\mathbb{Z}[2i]$.

   (b) Dokaži, da $\mathbb{Z}[2i]$ ni glavni kolobar.

   Rešitev: (a) Razcep v kolobarju $\mathbb{Z}[i]$ je znan: $2 = (1+i)(1-i)$, kjer sta elementa $1 \pm i$ neobrnljiva, saj imata normo 2. Denimo, da je $2 = \alpha \cdot \beta$ razcep v kolobarju $\mathbb{Z}[2i]$ (torej $\alpha = a + bi$ in $\beta = c + di$, kjer sta števili b in d sodi). Zaradi enoličnosti razcepa v $\mathbb{Z}[i]$ lahko predpostavimo, da je α asociiran elementu $1+i$, β pa elementu $1-i$. To pa je protislovje, saj so vsi elementi v $\mathbb{Z}[i]$, ki so asociirani elementu $1+i$, oblike $\pm 1 \pm i$, noben od teh pa ne pripada kolobarju $\mathbb{Z}[2i]$.

   (b) Dokažimo, da ideal $I = (2, 2i)$ v $\mathbb{Z}[2i]$ ni glavni. Ideal I vsebuje natanko vse elemente $a + bi$, kjer sta a in b soda. Denimo, da je I glavni ideal. Pišimo $I = (\alpha)$, $\alpha \in \mathbb{Z}[2i]$. Potem je $2 = \alpha\beta$ za nek $\beta \in \mathbb{Z}[2i]$. Zaradi nerazcepnosti elementa 2 v kolobarju $\mathbb{Z}[2i]$ sledi, da je bodisi α bodisi β obrnljiv v $\mathbb{Z}[2i]$, od koder sledi $I = \mathbb{Z}[2i]$ ali $I = (2)$. Prva možnost odpade, torej je $I = (2)$ in zato $2i = 2 \cdot \beta$ za nek $\beta \in \mathbb{Z}[2i]$. Sledi $\beta = i$, kar je pa je zopet protislovje, saj $i \notin \mathbb{Z}[2i]$.

4. Določi stopnji razširitev $[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}]$ in $[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}(i)]$.

   Rešitev: Velja

   $$[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}(\sqrt[4]{6})][\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}].$$

   Polinom $p(X) = X^2 + 1$ uniči i in je nerazcepen nad $\mathbb{Q}(\sqrt[4]{6})$, saj nima ničle v $\mathbb{Q}(\sqrt[4]{6})$. Torej je p minimalni polinom za i nad poljem $\mathbb{Q}(\sqrt[4]{6})$, od koder sledi $[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}(\sqrt[4]{6})] = 2$. Polinom $q(X) = X^4 - 6$ pa uniči $\sqrt[4]{6}$ in je nerazcepen nad $\mathbb{Q}$ po Eisensteinovem kriteriju (npr. za praštevilo 2), torej je to minimalni polinom za $\sqrt[4]{6}$ nad $\mathbb{Q}$. Sledi $[\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}] = 4$, rezultat pa je $2 \cdot 4 = 8$.

   Nadalje, velja

   $$[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}],$$

   kar je enako 8 po zgoraj dokazanem. Ker je $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ (očitno, minimalni polinom za i nad $\mathbb{Q}$ je $X^2 + 1$), sledi $[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}(i)] = 4$.

Janez Šter

ZBIRKA REŠENIH NALOG IZ ALGEBRE 2

Izdano v elektronski obliki v formatu PDF

URL: `https://www.fmf.uni-lj.si/~ster/zbirka_alg2.pdf` (prost dostop)

Cena: brezplačno

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID 69906947

ISBN 978-961-07-0651-9 (PDF)