

ALGEBRA 2:
Kolokvijske in izpitne naloge
iz študijskih let 2022/23 – 2024/25

Ganna Kudryavtseva

Ljubljana, 2026

Kazalo

1	Študijsko leto 2022/23	2
1.1	1. kolokvij - 21.12.2022.	2
1.2	2. kolokvij - 20.3.2023	6
1.3	3. kolokvij - 29.5.2023	10
1.4	1. izpit - 14.6.2023	13
1.5	2. izpit - 16.8.2023	16
1.6	3. izpit - 29.8.2023	18
2	Študijsko leto 2023/24	20
2.1	1. kolokvij - 19.12.2023	20
2.2	2. kolokvij - 19.3.2024	23
2.3	3. kolokvij - 14.5.2024	26
2.4	1. izpit - 14.6.2024	30
2.5	2. izpit - 21.8.2024	33
2.6	3. izpit - 3.9.2024	37
3	Študijsko leto 2024/25	40
3.1	1. kolokvij - 18.12.2024	40
3.2	2. kolokvij - 24.3.2025	43
3.3	3. kolokvij - 19.5.2025	45
3.4	1. izpit - 18.6.2025	48
3.5	2. izpit - 20.8.2025	51
3.6	3. izpit - 5.9.2025	54

Predgovor

Ta zbirka je sestavljena iz kolokvijskih in izpitnih nalog, ki so bile ponujene pri predmetu Algebra 2 v študijskih letih 2022/23, 2023/24 in 2024/25, med mojim sodelovanjem kot asistentka pri Algebri 2.

Za vsako študijsko leto zbirka vključuje tri kolokvije in tri izpite. Vsak kolokvij vsebuje naloge iz ustrezne tretjine snovi, izpiti pa vsebujejo naloge, ki pokrivajo celotno snov predmeta.

Bralce opozarjam, da je v študijskem letu 2024/25 snov zadnjega meseca prvič zajemala uvod v Galoisovo teorijo; ta snov je nadomestila snov iz Evklidovih kolobarjev, ki je bila v programu v študijskih letih 2022/23 in 2023/24. Posledično se je ustrezno prilagodila tudi vsebina 3. kolokvija in izpitov.

Vsak preizkus znanja v zbirki vsebuje tri naloge (z izjemo prvega kolokvija v letu 2022/23, ki je vseboval 4 naloge in se je izkazal kot preobsežen). Naloge so razbite na podnaloge (običajno 4 do 5), ki so pogosto vsebinsko povezane (čeprav so v glavnem neodvisne).

Vse naloge so navedene z (večinoma podrobnimi) rešitvami. Pri nalogah, kjer je navedenih več načinov reševanja, vam svetujem, da preučite vse pristope. Vse nedefinirane pojme lahko najdete v standardnih učbenikih, npr. [1, 2].

Nekatere naloge so povzete ali prilagojene po literaturi [1, 2, 3], nekatere spadajo v matematično folkloro, nekatere pa (zlasti naloge o konkretnih grupah/kolobarjih/poljih malega reda, o konkretnih polinomih, konkretnih razširitvah polj, ipd.) pa sem sestavila sama.

Ljubljana, 6. marec 2026

Ganna Kudryavtseva

Poglavje 1: Študijsko leto 2022/23

1.1 1. kolokvij - 21.12.2022.

1. (a) Koliko podgrup reda 2 ima grupa D_8 ?
- (b) Koliko cikličnih podgrup reda 4 ima grupa D_8 ?
- (c) Določi vse podgrupe grupe D_8 , ki imajo red 4 in niso ciklične.
- (d) Ali D_8 poleg cikličnih podgrup in podgrup iz točke (c) vsebuje še kako pravo podgrupo?
- (e) Ali je vsaka prava podgrupa grupe D_8 izomorfna kakšni podgrupi grupe D_{12} ?

Rešitev. (a) Podgrupe reda 2 so oblike $\{1, a\}$, kjer je a reda 2. Elementi reda 2 pa so vsa zrcaljenja $r^k z$, $k = 0, 1, 2, 3$, in r^2 , ki je geometrijsko zasuk za kot π . Zato D_8 vsebuje 5 podgrup reda 2.

(b) Ciklična podgrupa reda 4 je generirana z elementom reda 4. V grupi D_8 sta dva elementa reda 4, r in r^3 , oba generirata podgrupo $\{1, r, r^2, r^3\}$, ki je edina ciklična podgrupa reda 4.

(c) Naj bo G podgrupa reda 4, ki ni ciklična. Ker so vsi njeni elementi reda kvečjemu 2, je

$$G \subseteq \{1, r^2, z, rz, r^2z, r^3z\}.$$

Sledi, da G vsebuje vsaj dve različni zrcaljenji $r^k z, r^m z$, $k \neq m$. Potem tudi $r^k z \cdot r^m z = r^k z \cdot z r^{-m} = r^{k-m} \in G$. Zato $r^{k-m} = r^2$, kar velja, ko je

$$\{k, m\} = \{0, 2\} \quad \text{ali} \quad \{k, m\} = \{1, 3\}.$$

Zato je G enaka

$$\{1, r^2, z, r^2z\} \quad \text{ali} \quad \{1, r^2, rz, r^3z\}.$$

Enostavno je videti, da sta obe ti množici podgrupi. Dodamo, da je vsaka od teh dveh podgrup izomorfna grupi K_4 . Geometrijsko gledano, vsaka od njiju vsebuje dve pravokotni zrcaljenji in zasuk za kot π .

(d) Prave podgrupe grupe D_8 so reda 1, 2 in 4. Iz prejšnjih točk sledi, da smo že določili vse podgrupe reda 2 in 4. To so ciklične podgrupe in podgrupe iz točke (c). Ker je trivialna podgrupa $\{1\}$ tudi ciklična, drugih pravih podgrup, razen cikličnih in podgrup iz točke (c), grupa D_8 nima.

(e) Vsako zrcaljenje v D_{12} ima red 2, redi elementov r^k pa delijo 6. Zato D_{12} nima nobenega elementa reda 4 in posledično ne vsebuje ciklične podgrupe

reda 4. Zato podgrupa grupe D_8 iz rešitve (b) ni izomorfna nobeni podgrupi grupe D_{12} .

2. (a) Pokaži, da grupa ne more biti unija dveh svojih pravih podgrup.
- (b) Pokaži, da ima grupa D_4 tri podgrupe H_1, H_2 in H_3 , za katere velja $H_i \cap H_j = \{1\}$ za vse $i \neq j$ in katerih unija je D_4 .
- (c) Naj bo končna grupa G unija svojih podgrup H_1, H_2 in H_3 , kjer $|H_1| = |H_2| = 2$ in $|H_3| \geq 2$. Pokaži, da je potem $|H_3|$ sodo število.
- (d) Ali velja zaključek točke (a), če grupo nadomestimo z monoidom, podgrupi pa s podmonoidoma?

Rešitev. (a) Naj bo G unija svojih pravih podgrup H in K . Potem $H \not\subseteq K$, ker bi sicer imeli $G = K$ in podobno $K \not\subseteq H$. Naj bo $h \in H \setminus K$ in $k \in K \setminus H$. Potem $hk \notin K$ (če bi $hk = k' \in K$, bi potem imeli $h = k^{-1}k' \in K$, v protislovju z izbiro h), in podobno $kh \notin H$. Potem $hk \notin H \cup K = G$, kar ni mogoče. Zato G ne more biti unija dveh svojih pravih podgrup.

(b) Označimo $D_4 = \{1, a, b, ab\}$ kjer $a^2 = b^2 = (ab)^2 = 1$. Vzamemo $H_1 = \{1, a\}$, $H_2 = \{1, b\}$ in $H_3 = \{1, ab\}$. Potem so H_1, H_2 in H_3 podgrupe grupe D_4 , ki zadoščajo pogojem naloge.

(c) 1. *način.* Ker red podgrupe deli red grupe, je $|G|$ sodo število. Če $H_3 = G$, je $|H_3| = |G|$ sodo število. Predpostavimo, da $H_3 \neq G$. Ker $|H_1 \cup H_2| \in \{2, 3\}$, G vsebuje en ali dva elementa, ki niso v H_3 . Če označimo $|H_3| = k$, potem je $|G| \leq k + 2$. Ker red podgrupe deli red grupe in je H_3 prava podgrupa, je $|G| \geq 2k$. Zato velja $2k \leq |G| \leq k + 2$ in je tako $k \leq 2$. Z upoštevanjem predpostavke je potem $|H_3| = 2$.

2. *način.* Podobno kot prej, je $|G|$ sodo število. Najprej si oglejmo primer, ko $H_1 = H_2$. Potem je $G = H_1 \cup H_3$. Po točki (a) je potem $G = H_3 \supseteq H_1$ ali $G = H_1 \supseteq H_3$. V obeh primerih je potem $H_3 = G$ in je tako $|H_3|$ sodo število. Sedaj si oglejmo primer, ko $H_1 \neq H_2$. Naj bo $H_1 = \{1, a\}$, $H_2 = \{1, b\}$, kjer $a \neq b$. Predpostavimo, da je $|H_3| = 2k + 1$ liho število. Potem H_3 nima elementov sodega reda, in sicer $a, b \notin H_3$. Ker je $G = H_3 \cup \{a, b\}$, je $|G| = 2k + 3$, kar je v protislovju z dejstvom, da ima G sod red. Zato je predpostavka napačna, in je $|H_3|$ sodo število.

3. *način.* Podobno kot prej, dovolj je ogledati primer, ko so vse podgrupe prave in paroma različne. Naj bo $H_1 = \{1, a\}$, $H_2 = \{1, b\}$, kjer $a \neq b$. Po točki (a) $G \neq H_1 \cup H_2$. Naj bo $c \in H_3$, kjer $c \neq 1, a, b$. Potem $c^{-1} \neq 1, a, b$ (ker

sta a in b reda 2). Zato $c^{-1} \in H_3$. Če $ca \in H_3$, potem tudi $a = c^{-1} \cdot ca \in H_3$, kar ni mogoče. Zato je element ca enak 1, a ali b . Če $ca = 1$, potem $c = a$, kar ni mogoče, če $ca = a$, potem $c = 1$, kar ni mogoče. Zato je $ca = b$ in $c = ba$. Podobno $ac = b$ in zato $c = ab$. Torej je $ab = ba$, $G = \{1, a, b, ab\}$ in $H_3 = \{1, ab\}$.

Opomba. Iz rešitve sledi, da nujno velja $H_3 = G$ ali pa $G = \{1, a, b, ab\} \simeq D_4$ in $H_1 = \{1, a\}$, $H_2 = \{1, b\}$, $H_3 = \{1, ab\}$.

(d) Ne. Navedemo enega od veliko možnih protiprimerov. Naj bo \mathbb{N}^* monoid naravnih števil z operacijo množenja. Označimo z $N_1 = 2\mathbb{N} \cup \{1\}$ množico vseh sodih naravnih števil skupaj z 1, in z $N_2 = \mathbb{N} \setminus 2\mathbb{N}$ množico vseh lih naravnih števil. Potem sta N_1 in N_2 prava podmonoida monoida \mathbb{N}^* in je njuna unija \mathbb{N}^* .

3. Dana sta realna polinoma $f(X) = X^3$ in $g(X) = X^4$.

- Določi podgrupo aditivne grupe $\mathbb{R}[X]$, generirano s $f(X)$ in $g(X)$.
- Določi podkolobar kolobarja $\mathbb{R}[X]$, generiran s $f(X)$ in $g(X)$.
- Določi podalgebro realne algebre $\mathbb{R}[X]$, generirano s $f(X)$ in $g(X)$.
- Določi podpolje polja $\mathbb{R}(X)$, generirano s $f(X)$ in $g(X)$.

Rešitev. (a) Naj bo G iskana podgrupa. Potem G vsebuje množico

$$G' = \{mX^3 + nX^4 : m, n \in \mathbb{Z}\}.$$

Ker je množica G' grupa, je $G' = G$ zaradi minimalnosti G .

(b) Naj bo K podkolobar, generiran z X^3 in X^4 . Potem seveda $X^n \in K$ za $n = 0, 3, 4$. Preizkus sugestira, da $X^n \in K$ tudi za vse $n \geq 6$. Strogo se v tem prepričamo takole. Ker $X^3 \in K$, tudi $X^{3k} = (X^3)^k \in K$ za vse $k \in \mathbb{N}$. Ker $1, X^3, X^4 \in K$, tudi

$$X^{3k+1} = X^{3(k-1)+4} = (X^3)^{k-1} X^4 \in K$$

za vse $k \in \mathbb{N}$. Podobno

$$X^{3k+2} = X^{3(k-2)+8} = (X^3)^{k-2} (X^4)^2 \in K$$

za vse $k \geq 2$. Vsako naravno število $n \geq 6$ pa ima obliko $3k$, $3k+1$ ali $3k+2$ za nek naravni $k \geq 2$. Zato je

$$K' = \{a_0 + a_1x + \dots + a_nx^n : n \in \mathbb{N}, a_i \in \mathbb{Z}, a_1 = a_2 = a_5 = 0\}$$

kolobar, ki vsebuje X^3 in X^4 in $K' \subseteq K$. Zaradi minimalnosti K , je potem $K' = K$.

(c) Naj bo A iskana podalgebra. Podobno, kot v točki (b), upoštevajoč še zaprtost A za množenje z realnimi skalarji, imamo

$$A = \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{N}, a_i \in \mathbb{R}, a_1 = a_2 = a_3 = 0\}.$$

(d) Naj bo F iskano podpolje. Ker $1 \in F$, tudi $\mathbb{Q} \subseteq F$. Ker $X^3, X^4 \in F$, tudi $\frac{X^4}{X^3} = X \in F$. Zato $\mathbb{Q}(X) \subseteq F$. Ker je $\mathbb{Q}(X)$ podpolje polja $\mathbb{R}(X)$, ki vsebuje X^3 in X^4 , in zaradi minimalnosti F velja $\mathbb{Q}(X) = F$.

Opomba. Nalogo se da rešiti tudi hitreje z uporabo znanja iz teorije o strukturi grupe (kolobarja, algebre, polja), generirane s podano množico.

4. Naj bo \mathbb{H} algebra kvaternionov.

- (a) Pokaži, da inverz vsakega neničelnega kvaterniona $a \in \mathbb{H}$ leži v množici $D(a) = \{\lambda + \mu a : \lambda, \mu \in \mathbb{R}\}$ in od tod izpelji, da je vsaka podalgebra \mathbb{H} obseg (torej podobseg \mathbb{H}).
- (b) Pokaži, da je centralizator $C(a) = \{b \in \mathbb{H} : ab = ba\}$ vsakega elementa $a \in \mathbb{H}$ podalgebra.
- (c) Za katere $a \in \mathbb{H}$ je $C(a) = D(a)$?
Namig. Koliko je lahko v luči točke (a) dimenzija $C(a)$?
- (d) Pokaži, da je s predpisom $a \sim b \iff ab = ba$ definirana ekvivalenčna relacija na množici $\mathbb{H} \setminus \mathbb{R}$.

Rešitev. (a) Označimo $a = \alpha + \beta i + \gamma j + \delta k$ in $\mu = \frac{1}{\alpha^2 + \beta^2 + \gamma^2 + \delta^2} \in \mathbb{R}$. Potem je

$$a^{-1} = \frac{1}{a\bar{a}} \bar{a} = \mu(\alpha - \beta i - \gamma j - \delta k).$$

Potem je $a^{-1} + \mu a = 2\mu\alpha$, in zato $a^{-1} \in D(a)$. Naj bo A podalgebra \mathbb{H} in $a \in A$, $a \neq 0$. Ker $1, a \in A$, imamo $D(a) \subseteq A$. Iz $a^{-1} \in D(a)$ potem sledi $a^{-1} \in A$. Zato je A obseg.

(b) Enostavno je videti, da je $C(a)$ podgrupa aditivne grupe \mathbb{H} , vsebuje 1, je zaprta za množenje in za množenje s skalarji. Zato je podalgebra.

(c) Očitno $1, a \in C(a)$, zato po prejšnji točki $D(a) \subseteq C(a)$ za vsak $a \in \mathbb{H}$. Če $a \in \mathbb{R}$, potem $C(a) = \mathbb{H}$, $D(a) = \mathbb{R}$ in $C(a) \neq D(a)$. Naj bo $a \in \mathbb{H} \setminus \mathbb{R}$. Potem je dimenzija $D(a)$ enaka 2. Nadaljujemo lahko na več načinov.

1. način. Dovolj je pokazati, da je dimenzija $C(a)$ kvečjemu 2. Iz predavanj

vemo, da realna algebra dimenzije 3, ki je obseg, ne obstaja. Ker je $C(a)$ podalgebra, je po točki (a) tudi obseg, zato ne more biti dimenzije 3. Ker $a \notin \mathbb{R}$, a ne komutira z vsemi kvaternioni, zato $C(a) \neq \mathbb{H}$. Torej je dimenzija $C(a)$ kvečjemu 2.

2. *način.* Predpostavimo, da $C(a) \neq D(a)$. Potem obstaja neničelni $b \in C(a) \setminus D(a)$. Naj bo $\alpha + \beta a + \gamma b + \delta ab = 0$. To prepisimo kot $(\alpha + \beta a) + (\gamma + \delta a)b = 0$. Če je $\gamma + \delta a = 0$, se pravi $\gamma = \delta = 0$, potem tudi $\alpha = \beta = 0$. Sicer $\gamma + \delta a \neq 0$ in zato je $b = -(\gamma + \delta a)^{-1}(\alpha + \beta a) \in D(a)$, v protislovju z izbiro b . Potem so elementi $1, a, b, ab$ linearno neodvisni in je zato dimenzija $C(a)$ vsaj 4. Potem $C(a) = \mathbb{H}$, in zato $a \in Z(\mathbb{H}) = \mathbb{R}$, v protislovju z izbiro a .

3. *način.* Dovolj je pokazati, da je dimenzija $C(a)$ kvečjemu 2. Naj bo $a = s + pi + qj + rk$ in $b = \alpha + \beta i + \gamma j + \delta k$. Potem razvoja produktov ab in ba po bazi $1, i, j, k$ imata enak koeficient pri 1, in sicer, $s\alpha - p\beta - q\gamma - k\delta$. Naj velja $ab = ba$. Ker je $i = jk = -kj$, je koeficient pri i v produktu ab enak $s\beta + p\alpha + q\delta - r\gamma$, v produktu ba pa $s\beta + p\alpha - q\delta + r\gamma$. Ko vsoti izenačimo, dobimo $q\delta = r\gamma$. Podobno, ko obravnavamo koeficienta pri j in k v ab in ba , dobimo enakosti $r\beta = p\delta$ in $p\gamma = q\beta$. Iz dobljenih enakosti sledi linearna odvisnost (neničelnih) vektorjev (p, q, r) in (β, γ, δ) . Zato $b \in C(a)$ implicira, da ima b obliko $\alpha + \mu(pi + qj + rk) \in \mathcal{L}\{1, pi + qj + rk\}$. Zato je dimenzija $C(a)$ kvečjemu 2, kot je potrebno.

(d) Dana relacija je očitno refleksivna in simetrična. Pokažemo, da je tranzitivna. Naj $a \sim b$ in $b \sim c$, kjer $a, b, c \in \mathbb{H} \setminus \mathbb{R}$. Ker $a \sim b$, $b \in C(a)$. Iz prejšnje točke sledi, da $C(a) = D(a)$, zato $b \in D(a)$, torej $b = \lambda + \mu a$ za ustrezna $\lambda, \mu \in \mathbb{R}$. Podobno $c = \alpha + \beta b = \alpha + \beta(\lambda + \mu a)$ za ustrezna $\alpha, \beta \in \mathbb{R}$. Sledi, da $c \in D(a) = C(a)$, torej $a \sim c$.

1.2 2. kolokvij - 20.3.2023

1. Naj bo

$$T_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}$$

kolobar vseh zgoraj trikotnih matrik nad kolobarjem \mathbb{Z} .

(a) Ali je množica

$$I_1 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{Z} \right\}$$

ideal kolobarja $T_2(\mathbb{Z})$? Ali je levi ali desni ideal?

(b) Pokaži, da je množica

$$I_2 = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z} \right\}$$

ideal kolobarja $T_2(\mathbb{Z})$ in je kvocientni kolobar $T_2(\mathbb{Z})/I_2$ izomorfen kolobarju $\mathbb{Z} \times \mathbb{Z}$.

(c) Poišči tak ideal I_3 kolobarja $T_2(\mathbb{Z})$, da je kvocientni kolobar $T_2(\mathbb{Z})/I_3$ izomorfen kolobarju $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(d) Ali obstaja vložitev kolobarja $T_2(\mathbb{Z})$ v kolobar $\mathbb{Z} \times \mathbb{Z}$?

Rešitev. (a) Ker za $q, a \neq 0$ je

$$\begin{bmatrix} p & q \\ 0 & s \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 0 & qa \\ 0 & sa \end{bmatrix} \notin I_1,$$

množica I_1 ni levi ideal, zato seveda tudi ni ideal. Produkt v nasprotnem vrstnem redu pa je enak $\begin{bmatrix} 0 & 0 \\ 0 & as \end{bmatrix}$, zato je I_1 desni ideal.

(b) Označimo $K = T_2(\mathbb{Z})$. Definirajmo preslikavo $\varphi: K \rightarrow \mathbb{Z} \times \mathbb{Z}$,

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mapsto (a, c).$$

S preprostim računom vidimo, da je φ homomorfizem kolobarjev, npr., če je

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} p & q \\ 0 & r \end{bmatrix},$$

je

$$AB = \begin{bmatrix} ap & aq + br \\ 0 & cr \end{bmatrix},$$

zato je

$$\varphi(AB) = (ap, cr) = (a, c)(p, r) = \varphi(A)\varphi(B).$$

Jedro tega homomorfizma je množica I_2 , zato je I_2 ideal kolobarja K . Ker je poleg tega φ očitno surjektivna, iz izreka o izomorfizmu sledi, da je $K/I_2 \simeq \mathbb{Z} \times \mathbb{Z}$.

(c) Naj bo preslikava $\psi: K \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ podana s predpisom

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mapsto (a \pmod{2}, c \pmod{2}).$$

Ta preslikava je surjektivni homomorfizem kolobarjev (z upoštevanjem prejšnje točke je dovolj preveriti, da je preslikava

$$(a, c) \mapsto (a \pmod{2}, c \pmod{2})$$

iz $\mathbb{Z} \times \mathbb{Z}$ v $\mathbb{Z}_2 \times \mathbb{Z}_2$ surjektivni homomorfizem kolobarjev, kar je enostavno videti). Jedro tega homomorfizma je ideal

$$I_3 = \left\{ \begin{bmatrix} 2a & b \\ 0 & 2c \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}.$$

(d) Ne. Kolobar $T_2(\mathbb{Z})$ je nekomutativni, zato se ga ne da vložiti v komutativni kolobar $\mathbb{Z} \times \mathbb{Z}$.

2. (a) Do izomorfizma natančno določi vse Abelove grupe reda 360.
- (b) Določi največji red elementa v grupi $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$.
- (c) Ali ima grupa $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$ podgrupo, izomorfnu grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$?
- (d) Koliko elementov reda 10 je v grupi $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$?
- (e) Koliko podgrup reda 10 je v grupi $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$?

Rešitev. (a) Če je G grupa reda $360 = 2^3 3^2 5$, je $G = H_1 \oplus H_2 \oplus H_3$, kjer je $|H_1| = 2^3$, $|H_2| = 3^2$, $|H_3| = 5$. Z upoštevanjem klasifikacije končnih Abelovih grup, dobimo grupe:

- $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

(b) Red elementa $(a, b) \in \mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$ je najmanjši skupni večkratnik redov svojih komponent. Ker red a deli 30, red b deli 12 in ima $(1, 1)$ red 60, sledi, da je največji red elementa 60.

(c) Da. Podgrupa grupe $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$, generirana z elementoma $(5, 0)$ in $(0, 2)$, je izomorfnu grupi $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

(d) Uporabimo izomorfizem $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. Če ima element $(a, b, c, d, e) \in \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ red 10, potem je nujno $c = d = 0$

(sicer bi bil red deljiv s 3), red elementa e mora biti 5, red elementa (a, b) v grupi $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ pa mora biti 2. Če to velja, ima $(a, b, 0, 0, e)$ red 10. Za izbiro para (a, b) imamo 3 možnosti: $(0, 1), (2, 0), (2, 1)$, za izbiro e pa 4 možnosti: 1, 2, 3, 4. Zato imamo 12 elementov reda 10.

(e) Vsaka Abelova grupa reda 10 je ciklična, torej je generirana z elementom reda 10, ki smo jih opisali v prejšnji točki. Od tod hitro sledi, da so različne podgrupe reda 10 podgrupe, generirane z $(0, 1, 0, 0, 1), (2, 0, 0, 0, 1)$ in $(2, 1, 0, 0, 1)$. Imamo torej 3 podgrupe reda 10.

3. (a) Naj bosta p in q praštevili in G grupa reda pq , kjer $q < p$ in q ne deli $p - 1$. Pokaži, da G vsebuje eno samo podgrupo Sylowa reda p in prav tako eno samo podgrupo Sylowa reda q . Izpelji, da je potem $G \simeq \mathbb{Z}_{pq}$.
- (b) Pokaži, da je množica

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \{1, 2, 4\}, b \in \mathbb{Z}_7 \right\}$$

nekomutativna podgrupa grupe $\text{GL}_2(\mathbb{Z}_7)$ reda 21.

- (c) Naj bosta p in q praštevili, kjer $q < p$ in q deli $p - 1$. Poišči primer nekomutativne grupe G reda pq . *Namig.* Posploši primer iz prejšnje točke.

Rešitev. (a) Izrek Sylowa nam pove, da za število n_p podgrup Sylowa reda p velja $n_p = pk + 1$ za neko pozitivno celo število k , in n_p deli pq . Iz zadnjega pogoja in $(p, q) = 1$ takoj sledi $n_p | q$. Ker $q < p$, velja $n_p = 1$. Podobno je $n_q = pm + 1$ za neko pozitivno celo število m in n_q deli p , zato je 1 ali p . Ker q ne deli $p - 1$, je $n_q = 1$. Ker je za vsak $g \in G$ grupa $gH_p g^{-1}$ podgrupa Sylowa reda p , je $gH_p g^{-1} = H_p$, in je zato H_p edinka. Podobno je tudi H_q edinka. Ker je red vsakega elementa iz H_p enak 1 ali p in red vsakega elementa iz H_q enak 1 ali q , je $H_p \cap H_q = \{1\}$. Naj bo H podgrupa, generirana s H_p in H_q . Ker vsebuje elemente reda p in q , je red H vsaj pq , zato je $H = G$. Sedaj je G enaka notranjemu direktnemu produktu svojih podgrup edink H_p in H_q . Ker je $H_p \simeq \mathbb{Z}_p$ in $H_q \simeq \mathbb{Z}_q$, je $G \simeq \mathbb{Z}_{pq}$.

(b) Enostavno je videti, da je množica $\{1, 2, 4\}$ podgrupa grupe \mathbb{Z}_7^* . Zato za

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} \in H$$

velja:

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ac & ad+b \\ 0 & 1 \end{bmatrix} \in H$$

in

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{bmatrix} \in H.$$

Grupa H je nekomutativna, ker na primer matriki

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{in} \quad \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$$

ne komutirata.

(c) Ker je vsak neničelni element v \mathbb{Z}_p obrnljiv, je $|\mathbb{Z}_p^*| = p - 1$. Ker v končnih Abelovih grupah velja obrat Lagrangeovega izreka in q deli $p - 1$, ima grupa \mathbb{Z}_p^* podgrupo reda q . (Ta zaključek tudi takoj sledi iz dejstva, da je \mathbb{Z}_p^* ciklična grupa reda $p - 1$.) Naj bo A taka podgrupa. Potem je

$$K = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in A, b \in \mathbb{Z}_p \right\}$$

nekomutativna podgrupa grupe $\text{GL}_2(\mathbb{Z}_p)$ reda pq .

1.3 3. kolokvij - 29.5.2023

1. Podani so polinomi $f(X) = X^5 - 12X^3 + 36X - 12$, $g(X) = X^3 + 3X^2 + 2$ in $h(X) = X^5 + X^2 + 1$.

- Pokaži, da je $f(X)$ nerazcepen v $\mathbb{Q}[X]$. Ali je nerazcepen tudi v $\mathbb{R}[X]$?
- Pokaži, da je $g(X)$ nerazcepen v $\mathbb{Z}_5[X]$. Ali je nerazcepen tudi v $\mathbb{Q}[X]$?
- Pokaži, da je $h(X)$ nerazcepen v $\mathbb{Z}_2[X]$.

Rešitev. (a) $f(X)$ je nerazcepen v $\mathbb{Q}[X]$ po Eisensteinovem kriteriju za $p = 3$. Ker ima vsak nerazcepen polinom v $\mathbb{R}[X]$ stopnjo največ 2, $f(X)$ ni nerazcepen v $\mathbb{R}[X]$.

(b) Če bi bil $g(X)$ razcepen v $\mathbb{Z}_5[X]$, bi imel ničlo v \mathbb{Z}_5 . Ker je $g(0) = 2$, $g(1) = 1$, $g(2) = 2$, $g(3) = 1$ in $g(4) = g(-1) = 4$, ničel nima in je tako nerazcepen. Če bi bil $g(X)$ razcepen v $\mathbb{Q}[X]$, bi ga lahko netrivialno faktorizirali kot $g(X) = g_1(X)g_2(X)$ v $\mathbb{Z}[X]$. Oglejmo si homomorfizem $\varphi: \mathbb{Z}[X] \rightarrow \mathbb{Z}_5[X]$, ki preslika vsak polinom $\sum_{i=0}^n a_i X^i$ v polinom

$\sum_{i=0}^n a_i(\bmod 5)X^i$. Ker je vodilni koeficient polinoma $g(X)$ enak 1, se $g(X)$ preslika v polinom stopnje 5, prav tako se ohrani tudi stopnja polinomov $g_1(X)$ in $g_2(X)$. Sledi, da če bi bil $g(X)$ razcepen v $\mathbb{Q}[X]$, bi bil razcepen tudi v $\mathbb{Z}_5[X]$, kar vemo, da ne drži. Zato je nerazcepen v $\mathbb{Q}[X]$.

(c) Ker je $h(0) = h(1) = 1$, $h(X)$ nima ničel. Zato bi bila edina možnost, da bi bil $h(X)$ razcepen, če bi veljalo $h(X) = h_1(X)h_2(X)$, kjer sta oba faktorja nerazcepna in ima en od njiju stopnjo 2, drugi pa stopnjo 3. Edini nerazcepni polinom stopnje 2 v $\mathbb{Z}_2[X]$ je $X^2 + X + 1$. Zato bi se moral polinom $h(X)$ deliti z $X^2 + X + 1$. To pa ne drži, saj je

$$\begin{aligned} h(X) &= X^5 + X^2 + 1 = X^3(X^2 + X + 1) + X^4 + X^3 + X^2 + 1 = \\ &X^3(X^2 + X + 1) + X^2(X^2 + X + 1) + 1 = (X^3 + X^2)(X^2 + X + 1) + 1. \end{aligned}$$

Torej, $h(X)$ je nerazcepen v $\mathbb{Z}_2[X]$.

2. (a) Pokaži, da je element $2 + i \in \mathbb{Z}[i]$ nerazcepen.
 (b) Poišči največji skupni delitelj elementov $5 + 5i$ in $4 - 3i$ kolobarja $\mathbb{Z}[i]$.
 (c) Naj bo $(2 + i)$ glavni ideal kolobarja $\mathbb{Z}[i]$, generiran z elementom $2 + i$. Pokaži, da je

$$(2 + i) = \{a + bi \in \mathbb{Z}[i] : 2a + b \equiv 0(\bmod 5)\}.$$

- (d) Pokaži, da je kvocientni kolobar $\mathbb{Z}[i]/(2 + i)$ izomorfen polju \mathbb{Z}_5 .

Rešitev. (a) Naj bo $N(a + bi) = a^2 + b^2$ norma elementa $a + bi \in \mathbb{Z}[i]$. Ker je $N(2 + i) = 5$ praštevilo, je element $2 + i$ nerazcepen.

(b) Razstavimo elementa $5 + 5i$ in $4 - 3i$ na nerazcepne faktorje. Takoj vidimo, da je $5 + 5i = 5(1 + i) = (2 + i)(2 - i)(1 + i)$. Ker so norme faktorjev praštevila, so faktorji nerazcepni. Iz $N(4 - 3i) = 25$ sledi, da če obstaja netrivialni razcep $4 - 3i = z_1 z_2$, je $N(z_1) = N(z_2) = 5$. Do asociiranosti natančno imamo le dva elementa z normo 5, in sicer $2 + i$ in $2 - i$. Vidimo, da je $4 - 3i = (2 + i)(1 - 2i)$. Ker imata oba faktorja praštevilsko normo, sta nerazcepna. Zato je $2 + i$ skupni delitelj elementov $5 + 5i$ in $4 - 3i$. Ker je

$$\frac{5 + 5i}{4 - 3i} = \frac{(5 + 5i)(4 + 3i)}{25} = \frac{5 + 35i}{25} \notin \mathbb{Z}[i],$$

$4 - 3i$ ni delitelj $5 + 5i$. Sledi, da je iskani največji skupni delitelj enak $2 + i$. Nalogo bi lahko rešili tudi z Evklidovim algoritmom.

(c) Število $a + bi \in \mathbb{Z}[i]$ leži v idealu $(2 + i)$ natanko tedaj, ko $\frac{a+bi}{2+i} \in \mathbb{Z}[i]$. Potem je

$$\frac{a + bi}{2 + i} = \frac{(a + bi)(2 - i)}{5} = \frac{(2a + b) + (2b - a)i}{5} \in \mathbb{Z}[i]$$

natanko tedaj ko sta števili $x = 2a + b$ in $y = 2b - a$ deljivi s 5. Ker je $y = 2x - 5a$, sta števili x in y deljivi s 5 natanko takrat, ko je x deljiv s 5. Zato je število $a + bi$ deljivo z $2 + i$ v $\mathbb{Z}[i]$ natanko takrat, ko je $2a + b \equiv 0 \pmod{5}$.

(d) Označimo $I = (2 + i)$. Enakost $a + bi + I = c + di + I$ je ekvivalentna temu, da je $(a - c) + (b - d)i \in I$, kar po točki (c) velja natanko takrat, ko je celo število $2(a - c) + (b - d)$ deljivo s 5 oz. ko velja:

$$(2a + b) \pmod{5} = (2c + d) \pmod{5}.$$

Zato je odsek $a + bi + I$ določen z ostankom $(2a + b) \pmod{5}$. Imamo torej 5 odsekov. Vsak kolobar, ki vsebuje 5 elementov, pa je polje, izomorfnu polju \mathbb{Z}_5 .

Opombe. 1. To, da je kvocientni kolobar polje, sledi tudi iz dejstva, da je element $2 + i \in \mathbb{Z}[i]$ nerazcepen in je zato ideal $(2 + i)$ maksimalen. 2. To, da je kvocientni kolobar izomorfnu \mathbb{Z}_5 , bi lahko pokazali tudi s pomočjo opazke, da je preslikava $z \mapsto z + I$ surjektivni homomorfizem iz kolobarja \mathbb{Z} v kolobar $\mathbb{Z}[i]/I$ z jedrom $5\mathbb{Z}$.

3. (a) Poišči minimalni polinom elementa $\sqrt[4]{3} + i\sqrt[4]{3}$ v $\mathbb{Q}[X]$ in stopnjo razširitve $[\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) : \mathbb{Q}]$.
- (b) Pokaži, da velja stroga vključitev $\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) \subsetneq \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$.
- (c) Ali je $\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})$ razpadno polje minimalnega polinoma elementa $\sqrt[4]{3} + i\sqrt[4]{3}$ nad \mathbb{Q} ?

Rešitev. (a) Označimo $a = \sqrt[4]{3} + i\sqrt[4]{3} = \sqrt[4]{3}(1 + i)$. Potem je $a^2 = 2\sqrt{3}i$ in $a^4 = -12$. Zato je a ničla polinoma $f(X) = X^4 + 12 \in \mathbb{Q}[X]$. Ta polinom je nerazcepen nad \mathbb{Q} po Eisensteinovem kriteriju za $p = 3$, zato je minimalni polinom elementa a nad \mathbb{Q} . Sledi, da je $[\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) : \mathbb{Q}] = 4$.

(b) Zapišemo verigo razširitev:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}).$$

Prva razširitev je stopnje 4, saj je $X^4 - 3$ minimalni polinom elementa $\sqrt[4]{3}$ nad \mathbb{Q} . Druga razširitev je stopnje 2: ker $i\sqrt[4]{3} \notin \mathbb{Q}(\sqrt[4]{3})$, je stopnje vsaj 2,

ker je $i\sqrt[4]{3}$ ničla polinoma $X^2 + \sqrt{3}$ nad $\mathbb{Q}(\sqrt[4]{3})$, je stopnje največ 2. Sledi:

$$[\mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}) : \mathbb{Q}] = 8.$$

Ker $\sqrt[4]{3} + i\sqrt[4]{3} \in \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$, velja:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) \subseteq \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}).$$

Sledi, da je

$$[\mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}) : \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})] = 2$$

in zato $\mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}) \neq \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})$.

(c) Ničle polinoma $f(X) = X^4 + 12$ so $a = \sqrt[4]{3} + i\sqrt[4]{3}$, $b = \sqrt[4]{3} - i\sqrt[4]{3}$, $-a$ in $-b$. Zato je razpadno polje tega polinoma enako $\mathbb{Q}(a, b)$. Pokažemo, da velja:

$$\mathbb{Q}(a, b) = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}).$$

Ker $a, b \in \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$, imamo vključitev:

$$\mathbb{Q}(a, b) \subseteq \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}).$$

Ker je $\sqrt[4]{3} = (a+b)/2$, in $i\sqrt[4]{3} = (a-b)/2$, sledi, da velja tudi nasprotna vključitev. Zato razpadno polje polinoma $f(X)$ sovпада s poljem $\mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$. Iz točke (b) vemo, da to polje ni enako polju $\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})$.

1.4 1. izpit - 14.6.2023

1. Podani sta matriki $A = \begin{bmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & 1 \end{bmatrix}$ in $B = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$.

- Poišči presek $\langle A \rangle \cap \langle B \rangle$ podgrup grupe $\text{GL}_2(\mathbb{C})$, ki ju generirata A in B .
- Pokaži, da je podgrupa $G = \langle A, B \rangle$ grupe $\text{GL}_2(\mathbb{C})$ ciklična, generirana z elementom AB . Poišči njen red.
- Koliko elementov reda 4 vsebuje grupa $G = \langle A, B \rangle$?
- Naj bo $D \in \text{GL}_2(\mathbb{C})$ poljubna matrika. Pokaži, da če je D končnega reda, je $|\det(D)| = 1$. Ali velja nasprotna implikacija?

Rešitev. (a) S preprostim računom preverimo, da ima A red 3 in B red 4. Očitno, identična matrika I leži v preseku $\langle A \rangle \cap \langle B \rangle$. Ker ima vsak neidentični element grupe $\langle A \rangle$ red 3, in vsak neidentični element grupe $\langle B \rangle$ sodi red, drugih elementov v preseku ni. Zato je $\langle A \rangle \cap \langle B \rangle = \{I\}$.

(b) Ker sta obe matriki diagonalni, $AB = BA$. Zato lahko vsak element grupe $G = \langle A, B \rangle$ zapišemo v obliki $A^k B^m$, kjer $k = 0, 1, 2$ in $m = 0, 1, 2, 3$. Poljubna dva taka elementa očitno komutirata, zato je G Abelova grupa. Upoštevajoč še, da je $\langle A \rangle \cap \langle B \rangle = \{I\}$, sklepamo, da je G izomorfna notranjemu direktnemu produktu A in B , ki je izomorfen $\mathbb{Z}_3 \oplus \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$. Sledi, da je $|G| = 12$. Ker je red A enak 3 in red B enak 4, je red AB enak 12. Zato je matrika AB generator grupe G .

(c) Ker je red elementa $(AB)^k$, $k \neq 0$, enak $\frac{12}{(12,k)}$, iščemo $k \in \{1, \dots, 11\}$, da je $(12, k) = 3$. To velja za $k = 3$ in $k = 9$. Zato ima G dva elementa reda 4.

(d) Če je D končnega reda, je $D^n = I$ za nek $n \in \mathbb{N}$. Zato je $1 = \det(D^n) = \det(D)^n$. Sledi, da je $|\det(D)| = 1$. Obratna implikacija ne drži, ker ima npr. matrika $D = \begin{bmatrix} e^{i\pi\sqrt{2}} & 0 \\ 0 & 1 \end{bmatrix}$ determinanto z absolutno vrednostjo 1 in je neskončnega reda. Če bi imela končni red, bi bilo za nek $n \in \mathbb{N}$ število $n\pi\sqrt{2}$ cel večkratnik 2π , kar ne drži, saj $\sqrt{2} \notin \mathbb{Q}$.

2. Naj bo \mathcal{F} kolobar vseh funkcij $f: \mathbb{R} \rightarrow \mathbb{R}$ z operacijama seštevanja in množenja funkcij po točkah, tj. $(f + g)(x) = f(x) + g(x)$ in $(fg)(x) = f(x)g(x)$ za vse $f, g \in \mathcal{F}$ in za vsak $x \in \mathbb{R}$.

- Pokaži, da če za neničelni funkciji $f, g \in \mathcal{F}$ velja $fg = 0$, potem ima vsaka od funkcij f, g vsaj eno ničlo.
- Naj bo A množica tistih $f \in \mathcal{F}$, ki imajo vsaj eno ničlo. Ali je A ideal kolobarja \mathcal{F} ?
- Naj bo $I = \{f \in \mathcal{F}: f(0) = 0\}$. Pokaži, da je I ideal kolobarja \mathcal{F} in da je kvocientni kolobar \mathcal{F}/I izomorfen polju \mathbb{R} .
- Pokaži, da je I glavni ideal kolobarja \mathcal{F} , generiran s funkcijo $f \in \mathcal{F}$, podano s predpisom

$$f(x) = \begin{cases} 1, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

Rešitev. (a) Če sta $f, g \in \mathcal{F}$ neničelni funkciji, katerih produkt je ničelna funkcija, za vsak $x \in \mathbb{R}$ velja $f(x)g(x) = 0$. Ker $f \neq 0$, obstaja $a \in \mathbb{R}$, da je $f(a) \neq 0$. Potem je $g(a) = 0$, ker bi sicer imeli $(fg)(a) = f(a)g(a) \neq 0$, v protislovju s predpostavko $fg = 0$. Zato ima g vsaj eno ničlo. Ker je $fg = gf$, iz dokazanega sledi, da ima tudi f vsaj eno ničlo.

(b) Množica A ni zaprta za seštevanje, saj lahko vsota dveh funkcij iz A

nima nobene ničle, tj. za $f(x) = x^2$ in $g(x) = (x - 1)^2$ velja $f, g \in A$ in $f + g \notin A$. Zato A ni ideal.

(c) Očitno je I podgrupa aditivne grupe kolobarja \mathcal{F} . Če $f \in I$ in $g \in \mathcal{F}$, je $(fg)(0) = f(0)g(0) = 0$. Sledi, da je I ideal. Preslikava $\varphi: \mathcal{F} \rightarrow \mathbb{R}$, $\varphi(f) = f(0)$, je surjektivni homomorfizem kolobarjev z jedrom I (preveri). Zato je $\mathcal{F}/I \simeq \mathbb{R}$.

(d) Za vsako funkcijo $g \in I$ velja $g = gf$, saj za vsak $x \in \mathbb{R}$ velja $g(x) = g(x)f(x)$. Zato je I glavni ideal z generatorjem f .

3. Naj bosta $f(X) = X^3 + X + 1, g(X) = X^3 + 1 \in \mathbb{Z}_2[X]$. Označimo z $I = (f(X))$ in $J = (g(X))$ glavna ideala kolobarja $\mathbb{Z}_2[X]$, generirana z $f(X)$ in $g(X)$.

- Utemelji, da je kvocientni kolobar $F = \mathbb{Z}_2[X]/I$ polje. Zapiši vse elemente tega polja.
- Poišči največji skupni delitelj $d(X)$ polinomov $f(X)$ in X^2 v $\mathbb{Z}_2[X]$ in ga zapiši v obliki $d(X) = s(X)f(X) + t(X)X^2$ za ustrezna $s(X), t(X) \in \mathbb{Z}_2[X]$.
- Poišči polinom $h(X) \in \mathbb{Z}_2[X]$ stopnje največ 2, da je $(X^2 + I)^{-1} = h(X) + I$ v F .
- Utemelji, da kvocientni kolobar $H = \mathbb{Z}_2[X]/J$ ni polje. Navedi primer kakega neobrnljivega neničelnega elementa tega kolobarja.

Rešitev. (a) Ker je polinom $f(X)$ nerazcepen, je ideal I maksimalen in je zato F polje. Ker je $f(X)$ stopnje 3, je polje F moči $2^3 = 8$, njegovi elementi so odseki $aX^2 + bX + c + I$, kjer $a, b, c \in \mathbb{Z}_2$.

(b) Z Evklidovim algoritmom dobimo $d(X) = 1$ in

$$1 = (X + 1)f(X) + (X^2 + X + 1)X^2.$$

To, da je $d(X) = 1$, sledi tudi iz dejstva, da je $f(X)$ nerazcepen.

(c) Iz razcepa iz prejšnje točke sledi, da je

$$1 + I = (X^2 + X + 1 + I)(X^2 + I) = (X^2 + X + 1)X^2 + I.$$

Zato je $(X^2 + I)^{-1} = X^2 + X + 1 + I$.

(d) Ker ima polinom $g(X)$ ničlo, je razcepen. Zato ideal J ni maksimalen in posledično H ni polje. Ker je 1 ničla polinoma $g(X)$, je $g(X)$ deljiv z $X + 1$, zato je $X + 1 + I$ delitelj ničla v kvocientnem kolobarju H . Delitelj ničla pa ne

more biti obrnljiv. Zato je $X + 1 + I$ primer neobrnjljivega elementa kolobarja H .

1.5 2. izpit - 16.8.2023

1. Naj bo A množica vseh matrik oblike $\begin{bmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{bmatrix}$, kjer so $a, b, c, d \in \mathbb{R}$.

- Pokaži, da je A 4-razsežna podalgebra realne algebre $M_3(\mathbb{R})$.
- Pokaži, da je algebra A generirana z matrikama E_{12} in E_{23} .
- Poišči podgrupo aditivne grupe algebre A , generirano z matrikama E_{12} in E_{23} .
- Poišči primer podprostora realnega vektorskega prostora A , ki ni podalgebra algebre A .
- Pokaži, da algebra A ni izomorfna algebri $M_2(\mathbb{R})$.

Rešitev. (a) Enostavno je videti, da A vsebuje identično matriko, je zaprta za seštevanje, množenje in za množenje z realnimi skalarji, zato je podalgebra v $M_3(\mathbb{R})$. Ker matrike $I, E_{12}, E_{23}, E_{13}$ tvorijo bazo te podalgebre, je A 4-razsežna.

(b) Ker je $E_{12} \cdot E_{23} = E_{13}$, je vsak element algebre A linearna kombinacija matrik I, E_{12}, E_{23} in $E_{12} \cdot E_{23}$. Trditev sledi.

(c) To je grupa vseh matrik $\begin{bmatrix} 0 & b & 0 \\ 0 & 0 & d \\ 0 & 0 & 0 \end{bmatrix}$, kjer sta $b, d \in \mathbb{Z}$.

(d) Tak primer je na primer množica B vseh matrik iz A , za katere je $c = 0$. Očitno je B je 3-razsežen podprostor A z bazo I, E_{12}, E_{23} . Ker $E_{12}, E_{23} \in B$, $E_{12} \cdot E_{23} = E_{13} \notin B$, množica B ni zaprta za množenje, zato ni podalgebra algebre A .

(e) En od možnih razmislekov je naslednji. Element $E_{12} + E_{23} \in A$ je nilpotent stopnje 3, v $M_2(\mathbb{R})$ pa ima vsak nilpotent stopnjo največ 2. Slednje se da pokazati npr. z uporabo Jordanove kanonične oblike.

- Koliko 3-podgrup Sylowa ima grupa S_4 ?
 - Pokaži, da je vsaka 2-podgrupa Sylowa grupe S_4 izomorfna grupi D_8 .

- (c) Ali so vse podgrupe grupe S_4 reda 4 med seboj konjugirane?
 (d) Koliko 2-podgrup Sylowa ima grupa A_5 ?

Rešitev. (a) Ker je $24 = 2^3 \cdot 3$, ima 3-podgrupa Sylowa red 3. Grupa reda 3 je ciklična in je oblike $\{e, a, a^2\}$, kjer sta a in a^2 elementa reda 3. Ker ima S_4 8 elementov reda 3, so to vsi 3-cikli, ima S_4 štiri podgrupe reda 3.

(b) Če oglišča kvadrata oštevilčimo s števili 1, 2, 3 in 4, pridemo do vložitve grupe D_8 v grupo S_4 . Podgrupa, izomorfná grupi D_8 , je na primer

$$A = \{e, (1234), (13)(24), (1432), (14)(23), (12)(34), (13), (24)\}.$$

Ker je $|S_4| = 2^3 \cdot 3$, je red 2-podgrupe Sylowa enak 8, zato je A 2-podgrupa Sylowa. Ker so vse 2-podgrupe Sylowa med seboj konjugirane, so si tudi izomorfne, zato je vsaka od njih izomorfná grupi D_8 .

- (c) Primeri podgrup reda 4 so

$$A = \{e, (12)(34), (13)(24), (14)(23)\} \quad \text{in} \quad B = \{e, a, a^2, a^3\},$$

kjer je $a = (1234)$. Ker se pri konjugiranju ohrani ciklična struktura elementov, podgrupi A in B nista si konjugirani.

(d) Ker je $|A_5| = 2^2 \cdot 15$, je red 2-podgrupe Sylowa enak 4. Število n_2 2-podgrup Sylowa deli 15 in ima ostanek 1 pri deljenju z 2. Možnosti so 1, 3, 5, 15. Primer 2-podgrupe Sylowa je grupa $\{e, (12)(34), (14)(23), (13)(24)\}$ (tu je 5 negibna točka). Podobne podgrupe so še 4, za negibne točke 1, 2, 3 in 4. Ker so vse 2-podgrupe Sylowa med seboj konjugirane in se ciklična struktura permutacij pri konjugiranju ohrani, ima vsaka taka podgrupa eno negibno točko in 3 elemente oblike $(ij)(kl)$. Zato imamo 5 takih podgrup.

- 3.** (a) Pokaži, da $\mathbb{Q}(i\sqrt{3}) \neq \mathbb{Q}(i, \sqrt{3})$.
 (b) Pokaži, da je razpadno polje polinoma $g(X) = X^2 + X + 1$ nad \mathbb{Q} enako polju $\mathbb{Q}(i\sqrt{3})$.
 (c) Poišči polinom $h(X) \in \mathbb{Q}[X]$, katerega razpadno polje je polje $\mathbb{Q}(i, \sqrt{3})$.
 (d) Pokaži, da je razpadno polje polinoma $f(X) = X^4 + X^2 + 1$ nad \mathbb{Q} enako polju $\mathbb{Q}(i\sqrt{3})$.

Rešitev. (a) Minimalni polinom elementa $i\sqrt{3}$ nad \mathbb{Q} je $X^2 + 3$, zato je $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$. Po drugi strani, imamo:

$$\mathbb{Q}(i, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{3}) \supseteq \mathbb{Q},$$

kjer sta obe vključitvi očitno strogi. Zato je $[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] \geq 4$ (seveda, velja enakost, a tega tu ne potrebujemo).

(b) Ničli polinoma $g(X)$ sta

$$z_1 = e^{\frac{2\pi i}{3}} = \frac{1}{2}(-1 + i\sqrt{3}) \quad \text{in}$$

$$z_2 = \bar{z}_1 = e^{\frac{4\pi i}{3}} = \frac{1}{2}(-1 - i\sqrt{3}).$$

Razpadno polje F je po definiciji enako $\mathbb{Q}(z_1, z_2)$. Ker je $z_1 - z_2 = i\sqrt{3} \in F$, velja vključitev $\mathbb{Q}(i\sqrt{3}) \subseteq F$. Nasprotna vključitev tudi velja, saj $z_1, z_2 \in \mathbb{Q}(i\sqrt{3})$.

(c) Naj bo $h(X) = (X^2+1)(X^2-3)$. Ničle polinoma $h(X)$ so $i, -i, \sqrt{3}, -\sqrt{3}$, zato je njegovo razpadno polje enako $\mathbb{Q}(i, -i, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$.

(d) Ničle polinoma $f(X)$ so kompleksna števila z , za katera velja $z^2 = z_1$ ali $z^2 = z_2$. To so števila $e^{\frac{\pi i}{3}}, -e^{\frac{\pi i}{3}}, z_1, -z_1$. Zato je razpadno polje G polinoma $f(X)$ enako:

$$\mathbb{Q}(e^{\frac{\pi i}{3}}, e^{\frac{2\pi i}{3}}) = \mathbb{Q}(e^{\frac{\pi i}{3}}) = \mathbb{Q}\left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right).$$

Ker $\frac{1}{2} + \frac{i\sqrt{3}}{2} \in \mathbb{Q}(i\sqrt{3})$, je $G \subseteq \mathbb{Q}(i\sqrt{3})$. Ker $i\sqrt{3} = e^{\frac{\pi i}{3}} - e^{\frac{5\pi i}{3}} \in G$, velja tudi nasprotna vključitev.

1.6 3. izpit - 29.8.2023

1. Podana je podgrupa

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$$

multiplikativne grupe neničelnih kompleksnih števil \mathbb{C}^* .

- Opiši odseke grupe \mathbb{C}^* po podgrupi \mathbb{T} .
- Pokaži, da je kvocientna grupa \mathbb{C}^*/\mathbb{T} izomorfna grupi pozitivnih realnih števil (z operacijo množenja) \mathbb{R}^+ .
- Pokaži, da za vsak $n \in \mathbb{N}$ grupa \mathbb{T} vsebuje ciklično podgrupo reda n .
- Pokaži da grupa \mathbb{T} ne vsebuje podgrupe, izomorfne grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- Pokaži, da grupa \mathbb{T} vsebuje podgrupo, izomorfno grupi \mathbb{Z} .

Rešitev. (a) Odseki so $A_k = \{z \in \mathbb{C} : |z| = k\}$, $k \in \mathbb{R}^+$.

(b) Preslikava $f: \mathbb{C}^* \rightarrow \mathbb{R}^+$, podana s predpisom $f(z) = |z|$, je epimorfizem z jedrom \mathbb{T} .

(c) Element $z_n = e^{2\pi i/n}$ generira ciklično podgrupo grupe \mathbb{T} reda n .

(d) Grupa \mathbb{T} vsebuje le en element reda 2, in sicer -1 , grupa $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ pa 3 elemente reda 2.

(e) Element $e^{i\pi\alpha}$, kjer je $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ima neskončen red, zato generira podgrupo, izomorfnu \mathbb{Z} .

2. Podana je množica matrik

$$I = \left\{ \begin{bmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{bmatrix} : g, h, k \in \mathbb{Z} \right\}.$$

(a) Pokaži, da je I ideal kolobarja $T_3(\mathbb{Z})$ vseh zgoraj trikotnih 3×3 matrik nad \mathbb{Z} .

(b) Pokaži, da kvocientni kolobar $T_3(\mathbb{Z})/I$ vsebuje neničelni nilpotent.

(c) Pokaži, da kvocientni kolobar $T_3(\mathbb{Z})/I$ ni komutativen.

(d) Ali je preslikava $f: T_3(\mathbb{Z}) \rightarrow T_3(\mathbb{Z})$, podana s predpisom

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} \mapsto \begin{bmatrix} a & e & c \\ 0 & d & b \\ 0 & 0 & f \end{bmatrix},$$

endomorfizem kolobarja $T_3(\mathbb{Z})$?

Rešitev. (a) I je očitno podgrupa aditivne grupe kolobarja $T_3(\mathbb{Z})$. Ker je

$$\begin{bmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & gd & ge + hf \\ 0 & 0 & 2kf \\ 0 & 0 & 0 \end{bmatrix}$$

in

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} \begin{bmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & ag & ah + 2kb \\ 0 & 0 & 2kd \\ 0 & 0 & 0 \end{bmatrix},$$

je tudi ideal.

(b) Ker $E_{23} \notin I$, je $E_{23} + I$ neničelni element kvocientnega kolobarja. Ker je njegov kvadrat enak I , je nilpotenten.

(c) Naj bo $A = E_{22} + 2E_{33}$ in $B = E_{23}$. Potem je $AB = E_{23}$ in $BA = 2E_{23}$. Ker $AB - BA \notin I$, velja $(A + I)(B + I) \neq (B + I)(A + I)$.

(d) Ker je $f(E_{12})f(E_{23}) = E_{23}E_{12} = 0$ in $f(E_{12}E_{23}) = f(E_{13}) = E_{13}$, dana preslikava ni endomorfizem.

3. Za element $z = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ naj bo $N(z) = a^2 + 5b^2$ norma elementa z . Pri reševanju te naloge si lahko pomagaš z enakostjo $N(z_1z_2) = N(z_1)N(z_2)$ za vsaka $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$.

(a) Poišči vse obrnljive elemente kolobarja $\mathbb{Z}[\sqrt{-5}]$.

(b) Pokaži, da je največji skupni delitelj elementov 3 in $2 + \sqrt{-5}$ enak 1.

(c) Pokaži, da ideal $I = (3, 2 + \sqrt{-5})$ kolobarja $\mathbb{Z}[\sqrt{-5}]$ ni glavni.

Rešitev. (a) Če je element $p = a + b\sqrt{-5}$ obrnljiv, je $N(p) = a^2 + 5b^2 = 1$. Zato je $b = 0$ in $a = 1$ ali $a = -1$. Obrnljiva elementa sta zato dva: 1 in -1 .

(b) Če je $3 = z_1z_2$, je $9 = N(z_1)N(z_2)$. Zato je razcep $3 = z_1z_2$ netrivialen, če velja $N(z_1) = N(z_2) = 3$. Ker enačba $a^2 + 5b^2 = 3$ nima celoštevilskih rešitev, v kolobarju $\mathbb{Z}[\sqrt{-5}]$ ni elementov z normo 3. Zato je 3 nerazcepen element. Nejegovi delitelji so 1 in 3 (do asociiranosti natančno). Podobno je tudi $2 + \sqrt{-5}$ nerazcepen. Nejegovi delitelji so 1 in $2 + \sqrt{-5}$ (do asociiranosti natančno). Poleg tega, 3 in $2 + \sqrt{-5}$ si nista asociirana. Zato je njun največji skupni delitelj enak 1.

(c) Predpostavimo, da je ideal I glavni, generiran z elementom a . Potem a deli 3 in $2 + \sqrt{-5}$ in zato mora biti $a = 1$ (do asociiranosti natančno). Zato je $1 = 3s + (2 + \sqrt{-5})t$ za neka $s, t \in \mathbb{Z}[\sqrt{-5}]$. Če to enakost pomnožimo z $2 - \sqrt{-5}$, na levi strani dobimo $2 - \sqrt{-5}$, na desni strani pa element, deljiv s 3, kar ni mogoče. Zato ideal I ni glavni.

Poglavje 2: Študijsko leto 2023/24

2.1 1. kolokvij - 19.12.2023

1. (a) Pokaži, da ima ciklična grupa kvečjemu en element reda 2.

- (b) Koliko elementov reda 3 lahko ima ciklična grupa?
- (c) Ali ima grupa A_4 element reda 4?
- (d) Pokaži, da ima vsaka grupa reda 6 vsaj en element reda 2.
- (e) Denimo, da ima grupa G natanko en element reda 2. Pokaži, da ima center grupe G vsaj dva elementa.

Rešitev. (a) Neskončna ciklična grupa \mathbb{Z} nima nobenega elementa reda 2, saj ima vsak njen neničelni element neskončni red. Končna ciklična grupa lihega reda po Lagrangeovem izreku nima elementov reda 2. Grupa \mathbb{Z}_{2n} pa ima le en element reda 2, to je element n , saj iz $\frac{2n}{D(2n,k)} = 2$ sledi $D(2n,k) = n$.

(b) Iz Lagrangeovega izreka sledi, da če ima \mathbb{Z}_n element reda 3, velja $3 \mid n$. Red elementa k grupe \mathbb{Z}_{3n} je enak $\frac{3n}{D(3n,k)}$. Če je slednje število enako 3, je $n = D(3n,k)$, kar velja natanko za $k = n$ in $k = 2n$. Zato ima \mathbb{Z}_{3n} dva elementa reda 3. Možno število elementov reda 3 je tako 0 (kar velja npr. za grupo \mathbb{Z}_2) ali 2.

(c) Ne. Elementi A_4 so 1, elementi $(ij)(kl)$ reda 2 (3 elementi) in elementi (ijk) reda 3 (8 elementov).

(d) *1. način.* Predpostavimo, da ima vsak $a \in G \setminus \{1\}$ red vsaj 3. Definiamo ekvivalenčno relacijo ρ na G s predpisom $a \rho b \Leftrightarrow a = b$ ali $a = b^{-1}$. Potem ima vsak razred, razen razreda $\{1\}$, moč 2 in je tako red G (ki je disjunktna unija vseh razredov) liho število. Zato ima vsaka grupa reda 6 (ali, bolj splošno, sodega reda) vsaj en element reda 2.

2. način. Predpostavimo, da grupa G reda 6 nima nobenega elementa reda 2. Po Lagrangeovem izreku so potem možni redi elemenov iz $G \setminus \{1\}$ le 3 in 6. Če ima G element a reda 6, je a^3 reda 2. Zato ima vsak element iz $G \setminus \{1\}$ red 3. Naj bo a tak element. Potem ima tudi a^2 red 3 in $a^2 \neq a$. Naj bo b še en tak element, torej $b \neq a, a^2$. Potem tudi $b^2 \neq a, a^2$. Elementi $1, a, a^2, b, b^2$ so tako paroma različni. Potem je $G = \{1, a, a^2, b, b^2, c\}$ (kjer je $c \neq 1, a, a^2, b, b^2$ še en element reda 3), potem je $c^2 \in \{1, a, a^2, b, b^2\}$, zato tudi $c = (c^2)^2 \in \{1, a, a^2, b, b^2\}$, kar je protislovje.

(e) Predpostavimo, da je $g \in G$ edini element reda 2. Ker imata elementa g in $x^{-1}gx$ enak red, je $x^{-1}gx = g$ za vsak $x \in G$. Torej, je $gx = xg$ za vsak $x \in G$. Zato $Z(G) \supseteq \{1, g\}$.

2. (a) Pokaži, da je množica obrnljivih elementov R^* poljubnega kolobarja R grupa za operacijo množenja.
- (b) Poišči vse obrnljive in nilpotentne elemente kolobarjev \mathbb{Z}_8 in \mathbb{Z}_5 .

- (c) Pokaži, da je grupa \mathbb{Z}_5^* ciklična. Ali je grupa \mathbb{Z}_8^* ciklična?
- (d) Pokaži, da je vsak element kolobarja \mathbb{Z}_n bodisi obrnljiv bodisi nilpotenten natanko takrat, ko je $n = p^s$, kjer je p praštevilo in $s \in \mathbb{N}$.
- (e) Naj bo R neskončen kolobar, ki ni obseg. Pokaži, da ima R vsaj dva neničelna neobrnljiva elementa.

Rešitev. (a) Če sta a in b obrnljiva z inverzoma a' in b' , je $abb'a' = b'a'ab = 1$, zato je element ab obrnljiv. Poleg tega je za vsak obrnljiv element a njegov inverz a' obrnljiv (z inverzom a).

(b) Element $k \in \mathbb{Z}_n$ je obrnljiv natanko tedaj, ko je $D(k, n) = 1$. Obrnljivi elementi v \mathbb{Z}_8 so tako 1, 3, 5, 7, v \mathbb{Z}_5 pa 1, 2, 3, 4. Obrnljiv element ne more biti delitelj ničla in zato tudi ne more biti nilpotenten. Edini nilpotent v \mathbb{Z}_5 je tako 0. Nilpotenti v \mathbb{Z}_8 so 0, 2, 4 in 6, saj je $2^3 = 0$, $4^2 = 2^3 \cdot 2 = 0$ in $6^3 = 2^3 \cdot 3^3 = 0$.

(c) Ker je $|\mathbb{Z}_5^*| = 4$ in je red elementa 2 enak 4 (saj $2^2 = 4 \neq 1$), je grupa \mathbb{Z}_5^* ciklična. Ker je $|\mathbb{Z}_8^*| = 4$ in $3^2 = 5^2 = 7^2 = 1$, elementov reda 4 v grupi \mathbb{Z}_8^* ni, zato ta grupa ni ciklična.

(d) Naj bo $n = p^s$, kjer je p - praštevilo in $s \in \mathbb{N}$. Potem so elementi \mathbb{Z}_n oblike kp nilpotenti, saj je $(kp)^s = k^s p^s = 0$ v \mathbb{Z}_n . Za vsak drug element m velja $D(m, p) = 1$ in je zato m obrnljiv. Sedaj predpostavimo, da ima n vsaj dva različna praštevilska delitelja, p in q . Potem element $p \in \mathbb{Z}_n$ ni obrnljiv, saj $D(p, n) = p \neq 1$, in tudi ni nilpotenten, saj za poljuben $m \in \mathbb{N}$ število p^m ni deljivo s q in zato tudi z n , torej $p^m \neq 0$ v \mathbb{Z}_n .

(e) Predpostavimo, da ima R le en neničelni neobrnljiv element, a . Za vsak $b \in R^*$ velja $ba \notin R^*$, saj bi sicer bilo $a = b^{-1} \cdot ba \in R^*$. Zato je $ba \in \{0, a\}$. Ker je b obrnljiv, ne more biti delitelj ničla, zato $ba \neq 0$, ostane le možnost $ba = a$, kar se prepíše v $(b - 1)a = 0$. Sledi, da $b - 1 \in \{0, a\}$ in tako $b \in \{1, a + 1\}$. To pa je v nasprotju s tem, da je b poljuben element iz neskončne grupe R^* .

Opomba. Da se pokazati, da ima R neskončno mnogo neobrnljivih elementov.

3. Naj bo \mathbb{H} obseg kvaternionov.

- (a) Poišči podkolobar A kolobarja \mathbb{H} , generiran z elementom $i + j$.
- (b) Ali je podkolobar A iz prejšnje točke podobseg v \mathbb{H} ?
- (c) Ali elementa $i + j$ in $i + k$ generirata \mathbb{H} kot vektorski prostor nad

\mathbb{R} ?

(d) Ali elementa $i + j$ in $i + k$ generirata \mathbb{H} kot \mathbb{R} -algebro?

Rešitev. (a) Ker $1, i + j \in A$, velja vključitev:

$$K := \{a + b(i + j) : a, b \in \mathbb{Z}\} \subseteq A.$$

Ker je množica K aditivna podgrupa \mathbb{H} , vsebuje 1 in je zaprta za množenje (saj je $(i + j)^2 = -2 \in K$), sledi, da je K podkolobar v \mathbb{H} , ki vsebuje $i + j$. Potem je $K = A$, zaradi minimalnosti A .

(b) A ni podobseg, saj je npr. $(i + j)^{-1} = -\frac{1}{2}(i + j) \notin A$.

(c) Ne, saj ima $\text{Lin}_{\mathbb{R}}\{i + j, i + k\}$ dimenzijo 2, dimenzija \mathbb{H} nad \mathbb{R} je pa 4.

(d) Vemo, da i in j generirata \mathbb{H} kot \mathbb{R} -algebro. Označimo $a = i + j$, $b = i + k$ in $z \in B$ podalgebro \mathbb{H} , generirano z a in b . Potem je $ab = -1 - j - k + i \in B$, zato je $c = -j - k + i \in B$. Sledi, da je $c + a + b = 3i \in B$, zato tudi $i \in B$ in potem $j = a - i \in B$. Sledi vključitev $\mathbb{H} \subseteq B$, torej a in b generirata \mathbb{H} .

2.2 2. kolokvij - 19.3.2024

1. Naj bo $M_2(\mathbb{Z})$ kolobar vseh 2×2 matrik nad \mathbb{Z} in $T_2(\mathbb{Z})$ kolobar vseh zgoraj trikotnih 2×2 matrik nad \mathbb{Z} .

(a) Podana je preslikava $\varphi: T_2(\mathbb{Z}) \rightarrow \mathbb{Z} \times \mathbb{Z}$,

$$\varphi \left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \right) = (a, d).$$

Pokaži, da je φ epimorfizem kolobarjev in poišči njegovo jedro.

(b) Ali je preslikava

$$\psi: M_2(\mathbb{Z}) \rightarrow \mathbb{Z} \times \mathbb{Z}, \quad \psi \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = (a, d),$$

homomorfizem kolobarjev?

(c) Naj bo $n \in \mathbb{N}$. Pokaži, da je

$$M_2(n\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) : a, b, c, d \in n\mathbb{Z} \right\}$$

ideal kolobarja $M_2(\mathbb{Z})$ in da je $M_2(\mathbb{Z})/M_2(n\mathbb{Z}) \simeq M_2(\mathbb{Z}_n)$.

- (d) Označimo $I = M_2(2\mathbb{Z})$ in $J = M_2(3\mathbb{Z})$. Poišči vsoto $I+J$, produkt IJ in presek $I \cap J$ idealov I in J kolobarja $M_2(\mathbb{Z})$.

Rešitev. (a) Ker je

$$\begin{bmatrix} \mathbf{a} & b \\ 0 & \mathbf{d} \end{bmatrix} + \begin{bmatrix} \mathbf{s} & t \\ 0 & \mathbf{v} \end{bmatrix} = \begin{bmatrix} \mathbf{a} + \mathbf{s} & b + t \\ 0 & \mathbf{d} + \mathbf{v} \end{bmatrix}$$

in

$$\begin{bmatrix} \mathbf{a} & b \\ 0 & \mathbf{d} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{s} & t \\ 0 & \mathbf{v} \end{bmatrix} = \begin{bmatrix} \mathbf{as} & at + bv \\ 0 & \mathbf{dv} \end{bmatrix},$$

sledi, da je φ epimorfizem. Njegovo jedro je $\left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{Z} \right\}$.

(b) Ker je

$$\begin{bmatrix} \mathbf{a} & b \\ c & \mathbf{d} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{s} & t \\ u & \mathbf{v} \end{bmatrix} = \begin{bmatrix} \mathbf{as} + \mathbf{bu} & at + bv \\ cs + du & ct + \mathbf{dv} \end{bmatrix},$$

množenje matrik ni usklajeno s pokomponentnim množenjem diagonalcev, zato preslikava ψ ne ohranja množenja.

(c) S predpisom

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a(\bmod n) & b(\bmod n) \\ c(\bmod n) & d(\bmod n) \end{bmatrix}$$

podana preslikava $M_2(\mathbb{Z}) \rightarrow M_2(\mathbb{Z}_n)$ je epimorfizem z jedrom $M_2(n\mathbb{Z})$.

(d) Ker je

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} - \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in I + J,$$

je $I + J = M_2(\mathbb{Z})$. Če je

$$C = \begin{bmatrix} 6a & 6b \\ 6c & 6d \end{bmatrix} \in M_2(6\mathbb{Z}),$$

je

$$C = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 3a & 3b \\ 3c & 3d \end{bmatrix} \in IJ.$$

Poljuben produkt AB , kjer $A \in I$, $B \in J$, pa je v $M_2(6\mathbb{Z})$. Zato je $IJ = M_2(6\mathbb{Z})$. Po definiciji tudi takoj sledi, da je $I \cap J = M_2(6\mathbb{Z})$.

- 2.** (a) Ali sta si grupi $\mathbb{Z}_{12} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_3$ in $\mathbb{Z}_{12} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_4$ izomorfni?

- (b) Poišči največji red elementa v grupi $\mathbb{Z}_{12} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_4$.
- (c) Naj bo H podgrupa grupe $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$, generirana z elementom $(1, 1, 1)$. Pokaži, da je $(\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4)/H \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4$.
- (d) Naj bo G podgrupa grupe $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$, generirana z elementoma $(1, 1, 0)$ in $(0, 0, 2)$. Pokaži, da ima G red 8.
- (e) Ali je vsaka podgrupa grupe $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$ reda 8 izomorfna grupi G iz prejšnje točke?

Rešitev. (a) Ker je

$$\mathbb{Z}_{12} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

in

$$\mathbb{Z}_{12} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_4 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3,$$

si grupi nista izomorfni.

(b) Red elementa $(a, b, c) \in \mathbb{Z}_{12} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_4$ je enak najmanjšemu skupnemu večkratniku redov elementov a, b, c . Največji red, 36, dobimo, ko je a element reda 12 in b element reda 9.

(c) S predpisom $(a, b, c) \mapsto (a - b, a - c)$ podana preslikava $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \oplus \mathbb{Z}_4$ je epimorfizem z jedrom $\langle (1, 1, 1) \rangle$.

(d) Označimo $a = (1, 1, 0)$ in $b = (0, 0, 2)$. Ker je $\langle a \rangle \simeq \mathbb{Z}_4$, $\langle b \rangle \simeq \mathbb{Z}_2$ in $\langle a \rangle \cap \langle b \rangle = \{(0, 0, 0)\}$, je $G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2$ podgrupa reda 8.

(e) Ni vsaka podgrupa grupe $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$ reda 8 izomorfna grupi G , ker je podgrupa $\langle (2, 0, 0), (0, 2, 0), (0, 0, 2) \rangle$ reda 8 in je izomorfna $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

- 3.** (a) Poišči vse podgrupe Sylowa grupe D_{10} .
- (b) Koliko je različnih 5-podgrup Sylowa in 2-podgrup Sylowa v nekomutativni grupi reda 20?
- (c) Denimo, da je p praštevilo in P p -podgrupa končne grupe G . Pokaži, da je P p -podgrupa Sylowa natanko takrat, ko sta si števili $[G : P]$ in p tuji.
- (d) Naj bo G končna grupa, $H \triangleleft G$ in P p -podgrupa Sylowa grupe G , kjer je p praštevilo. Pokaži, da je PH/H p -podgrupa Sylowa grupe G/H .
Nasvet. Pomagaj si s prejšnjo točko in 2. izrekom o izomorfizmu: $P/(P \cap H) \simeq PH/H$.

Rešitev. (a) 5-podgrupa Sylowa je reda 5 in je podgrupa $\langle r \rangle = \{1, r, r^2, r^3, r^4\}$. Ker drugih elementov reda 5 ni, drugih podgrup reda 5 ni. (*Plan B:* $n_5 \equiv 1 \pmod{5}$ in $n_5 \mid 2$, zato je $n_5 = 1$. *Plan C:* podgrupa reda 5 ima indeks 2 in je zato edinka, od kod sledi da je $n_5 = 1$.) 2-podgrupe Sylowa so vse 2-elementne podgrupe: $\{1, r^k z\}$, $k = 0, 1, 2, 3, 4$.

(b) Naj bo G nekomutativna grupa reda 20. Ker $n_5 \mid 4$ in $n_5 \equiv 1 \pmod{5}$, je $n_5 = 1$. Ker $n_2 \mid 5$ in $n_2 \equiv 1 \pmod{2}$, je $n_2 = 1$ ali $n_2 = 5$. Predpostavimo, da je $n_2 = 1$. Označimo z A edino 5-podgrupo Sylowa in B edino 2-podgrupo Sylowa. Ker sta obe edinki in $A \cap B = \{1\}$, je $\langle A, B \rangle = A \times B$ podgrupa reda 20, zato sovпада s G . Ker sta A in B Abelovi, je G Abelova, kar je protislovje. Zato je $n_2 = 5$.

(c) Naj bo $|G| = p^k t$, kjer je $D(p, t) = 1$. Potem je $|P| = p^k$. Sledi, da je $[G : P] = \frac{|G|}{|P|} = t$, zato je $D([G : P], p) = 1$.

(d) Ker je $P/(P \cap H) \simeq PH/H$, je PH/H p -grupa. Ker $P \subseteq PH \subseteq G$, $[G : PH]$ deli $[G : P]$. Po prejšnji točki, je $D([G : P], p) = 1$, zato tudi $D([G : PH], p) = 1$. Ker je

$$[G/H : PH/H] = [G : PH],$$

sledi, da je

$$D([G/H : PH/H], p) = 1$$

in je po prejšnji točki PH/H p -podgrupa Sylowa grupe G/H .

2.3 3. kolokvij - 14.5.2024

1. Podan je polinom $f(X) = X^5 - 1$. Razstavi $f(X)$ na nerazcepne faktorje:

- (a) nad \mathbb{Z}_2 ;
- (b) nad \mathbb{Q} ;
- (c) nad \mathbb{R} .
- (d) Z uporabo točk (b) in (c) pokaži, da je število $\cos \frac{2\pi}{5}$ algebraično stopnje 2.

Rešitev. (a) Zapišimo $f(X) = (X - 1)g(X)$, kjer je

$$g(X) = X^4 + X^3 + X^2 + X + 1.$$

Ker je $g(0) = g(1) = 1$, edina možnost, da bi bil polinom $g(X)$ razcepen, bi bila, če bi bil produkt dveh nerazcepnih polinomov stopnje 2. Nad \mathbb{Z}_2 je

le en sam nerazcepen polinom stopnje 2, to je $h(X) = X^2 + X + 1$. Ker $h(X)^2 \neq g(X)$, je $g(X)$ nerazcepen, in je tako $f(X) = (X - 1)g(X)$ razcep na nerazcepne faktorje.

(b) Ker je slika polinoma $g(X) = X^4 + X^3 + X^2 + X + 1$ pri naravni preslikavi $\mathbb{Z}[X] \rightarrow \mathbb{Z}_2[X]$ nerazcepna po prejšnji točki, je $g(X)$ nerazcepen nad \mathbb{Z} , in je zato nerazcepen tudi nad \mathbb{Q} . Zato je $f(X) = (X - 1)g(X)$ razcep na nerazcepne faktorje nad \mathbb{Q} .

(c) Ker je $a = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$ primitivni koren stopnje 5 iz 1, so a^k , $k = 0, 1, 2, 3, 4$, vse kompleksne ničle polinoma $f(X)$. Ker velja $a^4 = \bar{a}$, $a^3 = \bar{a}^2$ in $a^0 = 1$, z uporabo enakosti

$$(X - z)(X - \bar{z}) = X^2 - 2\operatorname{Re}(z)X + |z|^2$$

dobimo razcep

$$f(X) = (X - 1)\left(X^2 - 2\cos \frac{2\pi}{5}X + 1\right)\left(X^2 - 2\cos \frac{4\pi}{5}X + 1\right)$$

nad \mathbb{R} . Kvadratna faktorja sta nerazcepna nad \mathbb{R} , saj nimata realnih ničel.

(d) Ker je a ničla nerazcepnega polinoma $X^2 - 2\cos \frac{2\pi}{5}X + 1$ nad $\mathbb{Q}(\cos \frac{2\pi}{5})$, je

$$[\mathbb{Q}(a) : \mathbb{Q}(\cos \frac{2\pi}{5})] = 2.$$

Iz točke (b) sledi, da je $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. V verigi razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(\cos \frac{2\pi}{5}) \subseteq \mathbb{Q}(a)$$

je tako

$$[\mathbb{Q}(\cos \frac{2\pi}{5}) : \mathbb{Q}] = \frac{4}{2} = 2.$$

2. Naj bo $d \in \mathbb{Z}$. Za element $z = m + n\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ naj bo $N(z) = m^2 - dn^2$ norma elementa z . Pri reševanju te naloge si lahko pomagaš z enakostjo $N(z_1z_2) = N(z_1)N(z_2)$ za vsaka $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$.

- Pokaži, da sta 1 in -1 edina obrnljiva elementa kolobarja $\mathbb{Z}[\sqrt{-3}]$, nista pa edina obrnljiva elementa kolobarja $\mathbb{Z}[\sqrt{3}]$.
- Ali sta elementa $\sqrt{3}$ in $3 + 2\sqrt{3}$ kolobarja $\mathbb{Z}[\sqrt{3}]$ asociirana?
- Pokaži, da je množica vseh elementov kolobarja $\mathbb{Z}[\sqrt{3}]$ s sodo normo glavni ideal kolobarja $\mathbb{Z}[\sqrt{3}]$ in poišči njegov generator.

- (d) Pokaži, da kolobar $\mathbb{Z}[\sqrt{-3}]$ ni kolobar z enolično faktorizacijo.
- (e) Pokaži, da za vsako celo število $n \geq 3$ kolobar $\mathbb{Z}[\sqrt{-n}]$ ni kolobar z enolično faktorizacijo.

Rešitev. (a) Če je $a \in \mathbb{Z}[\sqrt{-3}]$ obrnljiv, je $ab = 1$ za nek $b \in \mathbb{Z}[\sqrt{-3}]$ in zato $N(a)N(b) = 1$. Ker je $N(m+n\sqrt{-3}) = m^2 + 3n^2$, je $N(m+n\sqrt{-3}) = 1$ natanko tedaj, ko je $m = 1$ in $n = 0$ ali $m = -1$ in $n = 0$. Element $2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ je obrnljiv, saj je $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$.

(b) Da, ker je $3 + 2\sqrt{3} = \sqrt{3}(2 + \sqrt{3})$ in je $2 + \sqrt{3}$ obrnljiv.

(c) Naj bo A množica elementov kolobarja $\mathbb{Z}[\sqrt{3}]$ s sodo normo. Opazimo, da je $1 + \sqrt{3}$ element z najmanjšo (po absolutni vrednosti) neničelno sodo normo in pokažemo, da je $A = (1 + \sqrt{3})$. Če $m + n\sqrt{3} \in A$, enostavno je videti, da sta števili m in n bodisi obe sodi bodisi obe lihi. Potem je

$$\frac{m + n\sqrt{3}}{1 + \sqrt{3}} = \frac{(m + n\sqrt{3})(1 - \sqrt{3})}{-2} = \frac{3n - m}{2} + \frac{m - n}{2}\sqrt{3} \in \mathbb{Z}[\sqrt{3}],$$

zato velja: $A \subseteq (1 + \sqrt{3})$. Ker

$$(1 + \sqrt{3})(m + n\sqrt{3}) = (m + 3n) + (m + n)\sqrt{3}$$

in je $(m + 3n)^2 - 3(m + n)^2$ sodo število, nasprotna vključitev tudi drži.

(d) Opazimo, da velja $4 = 2 \cdot 2$ in $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Če je $2 = ab$, je $4 = N(a)N(b)$, zato je za netrivialen razcep $N(a) = N(b) = 2$. Nobenega elementa z normo 2 v $\mathbb{Z}[\sqrt{-3}]$ ni, saj enačba $m^2 + 3n^2 = 2$ nima celoštevilskih rešitev. Zato je 2 nerazcepen element. Ker 2 ne deli $1 + \sqrt{-3}$ in $1 - \sqrt{-3}$ (zato, ker $2(m + n\sqrt{-3}) = 2m + 2n\sqrt{-3}$, kar ne more biti enako $1 + \sqrt{-3}$ ali $1 - \sqrt{-3}$), element 4 nima enoličnega razcepa na nerazcepne faktorje.

(e) Če je n liho število, podobno, kot v (c), imamo:

$$(1 + \sqrt{-n})(1 - \sqrt{-n}) = 1 + n = 2 \cdot \frac{1 + n}{2}.$$

Ker je 2 nerazcepen element in ne deli $1 + \sqrt{-n}$ in $1 - \sqrt{-n}$ (podobno kot prej), element $1 + n$ nima enoličnega razcepa na nerazcepne faktorje. Če je n sodo število, je 2 nerazcepen in deli $-n = \sqrt{-n}\sqrt{-n}$, ne deli pa $\sqrt{-n}$. Sklepamo, da element $-n$ nima enoličnega razcepa na nerazcepne faktorje.

3. Označimo $a = \sqrt{3} + i \in \mathbb{C}$.

- (a) Pokaži, da je $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

- (b) Poišči minimalni polinom elementa a nad \mathbb{Q} .
- (c) Poišči polinom $p(X) \in \mathbb{Q}[X]$, katerega razpadno polje je $\mathbb{Q}(a)$.
- (d) Pokaži, da je $[\mathbb{Q}(a) : \mathbb{Q}(a^3)] = 2$ in poišči minimalni polinom elementa a nad $\mathbb{Q}(a^3)$.
- (e) Pokaži, da za vsak $b \in \mathbb{C}$, za katerega je $[\mathbb{Q}(b) : \mathbb{Q}] = 4$, velja $[\mathbb{Q}(b) : \mathbb{Q}(b^3)] \leq 2$. Ali vedno velja enakost $[\mathbb{Q}(b) : \mathbb{Q}(b^3)] = 2$?

Rešitev. (a) Očitno je $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{3}, i)$. Ko enakost $a - i = \sqrt{3}$ kvadriramo, dobimo $a^2 - 1 - 2ai = 3$, zato $i \in \mathbb{Q}(a)$. Potem tudi $\sqrt{3} = a - i \in \mathbb{Q}(a)$. Torej velja:

$$\mathbb{Q}(a) = \mathbb{Q}(\sqrt{3}, i).$$

V verigi razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, i)$$

ima prva razširitev stopnjo 2, saj je $X^3 - 3$ minimalni polinom elementa $\sqrt{3}$ nad \mathbb{Q} . Druga vključitev je stroga, saj

$$i \notin \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}.$$

Po drugi strani je $X^2 + 1$ polinom stopnje 2 nad $\mathbb{Q}(\sqrt{3})$, ki uniči i . Zato je stopnja druge razširitve enaka 2. Iskana stopnja je tako $2 \cdot 2 = 4$.

(b) Iz $a^2 - 1 - 2ai = 3$ izrazimo $i = \frac{a^2 - 4}{2a}$. Ko to kvadriramo, dobimo $-1 = \frac{a^4 - 8a^2 + 16}{4a^2}$. Sledi, da je a ničla polinoma $X^4 - 4X^2 + 16 \in \mathbb{Q}[X]$. Ker je stopnje 4, je minimalni polinom za a .

(c) To je na primer polinom $p(X) = (X^2 + 1)(X^2 - 3)$.

(d) Ker je $a^3 = 8i$, je $\mathbb{Q}(a^3) = \mathbb{Q}(i)$. V verigi razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\sqrt{3}, i)$$

je prva razširitev stopnje 2, zato velja:

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(i)] = 2.$$

Iskani minimalni polinom je tako stopnje 2. Iz $a^2 - 1 - 2ai = 3$ sledi, da je a ničla polinoma $X^2 - 2iX - 4$ nad $\mathbb{Q}(i)$. Ker ima stopnjo 2, je minimalni polinom za a .

(e) 1. način. V verigi razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(b^3) \subseteq \mathbb{Q}(b)$$

je $[\mathbb{Q}(b^3) : \mathbb{Q}] \geq 2$, sicer bi imeli $b^3 \in \mathbb{Q}$, in bi bil b ničla polinoma nad \mathbb{Q} stopnje 3, kar ni mogoče, saj je $[\mathbb{Q}(b) : \mathbb{Q}] = 4$. Sledi:

$$[\mathbb{Q}(b) : \mathbb{Q}(b^3)] \leq 2.$$

2. način. Naj bo $X^4 + c_3X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Q}[X]$ minimalni polinom elementa b . Potem je b ničla polinoma $b^3X + c_3b^3 + c_2X^2 + c_1X + c_0$ stopnje 2 nad $\mathbb{Q}(b^3)$, zato je $[\mathbb{Q}(b) : \mathbb{Q}(b^3)] \leq 2$.

Enakost $[\mathbb{Q}(b) : \mathbb{Q}(b^3)] = 2$ ne velja vedno, saj ima $b = \sqrt[4]{2}$ stopnjo 4 nad \mathbb{Q} , ampak $b = \frac{b^4}{b^3} = \frac{2}{b^3} \in \mathbb{Q}(b^3)$ in tako $[\mathbb{Q}(b) : \mathbb{Q}(b^3)] = 1$.

2.4 1. izpit - 14.6.2024

1. Podana je podgrupa

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$$

multiplikativne grupe neničelnih kompleksnih števil \mathbb{C}^* .

- Opiši odseke grupe \mathbb{C}^* po podgrupi \mathbb{T} in pokaži, da je kvocientna grupa \mathbb{C}^*/\mathbb{T} izomorfna grupi pozitivnih realnih števil (z operacijo množenja) \mathbb{R}^+ .
- Pokaži, da za vsak $n \in \mathbb{N}$ grupa \mathbb{T} vsebuje natanko eno podgrupo reda n .
- Naj bo G Abelova grupa, generirana z dvema elementoma. Pokaži, da je vsaka podgrupa grupe G generirana z največ dvema elementoma.
Nasvet. Lahko uporabiš znano dejstvo, da je vsaka podgrupa ciklične grupe ciklična.
- Ali trditev iz prejšnje točke še vedno velja brez predpostavke, da je G Abelova?
Nasvet. Lahko si pomagaš s Cayleyjevim izrekom.

Rešitev. (a) Odseki so $A_k = \{z \in \mathbb{C} : |z| = k\}$, $k \in \mathbb{R}^+$. Preslikava $f : \mathbb{C}^* \rightarrow \mathbb{R}^+$, podana s predpisom $f(z) = |z|$, je epimorfizem z jedrom \mathbb{T} .

(b) Grupa \mathbb{T} vsebuje podgrupo $H_n = \langle e^{\frac{2\pi i}{n}} \rangle$ reda n . Elemente te grupe so natanko vsa kompleksna števila z , za katera je $z^n = 1$. Če je G kaka druga podgrupa reda n in $a \in G$, je po Lagrangeovem izreku $a^n = 1$, zato je $a \in H_n$. Torej je $G \subseteq H_n$ in zaradi enakosti redov velja $G = H_n$.

(c) Predpostavimo, da je $G = \langle a, b \rangle$ in $H \triangleleft G$. Če za vsak element $ma + nb \in H$ velja $n = 0$, je H podgrupa grupe $\langle a \rangle$, ki je ciklična. Zato je tudi H

ciklična. Predpostavimo, da obstaja $ma + nb \in H$, kjer $n \neq 0$. Vzamemo tak $z = ma + nb \in H$, kjer ima n najmanjšo možno neničelno absolutno vrednost in pokažimo, da je H generirana z a in z . Naj bo $x = \alpha a + \beta b \in H$. Če je $\beta b = 0$, je $x \in \langle a, z \rangle$. Sedaj predpostavimo, da $\beta b \neq 0$. Potem n deli β , sicer bi hitro prišli v protislovje z izbiro n . Če je $\beta = kn$, je $x - kz \in \langle a \rangle$, torej je $x \in \langle a, z \rangle$.

(d) Cayleyjev izrek pove, da lahko vsako grupo G vložimo v simetrično grupo $\text{Sim}(G)$. Vsako končno grupo potem lahko vložimo v Sim_n za nek $n \in \mathbb{N}$. Grupa Sim_n je generirana z dvema elementoma $(1\ 2 \dots n)$ in $(1\ 2)$ (znano iz vaj). Ampak ni vsaka končna grupa generirana z največ dvema elementoma. Na primer, grupa $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ni generirana z nobenima dvema svojima elementoma (vsak njen neničelni element ima red dva, dva taka elementa generirata grupo reda 4 izomorfno $\mathbb{Z}_2 \oplus \mathbb{Z}_2$).

2. Podana je množica matrik

$$I = \left\{ \begin{bmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{bmatrix} : g, h, k \in \mathbb{Z} \right\}.$$

- Pokaži, da je I ideal kolobarja $T_3(\mathbb{Z})$ vseh zgoraj trikotnih 3×3 matrik nad \mathbb{Z} .
- Pokaži, da kvocientni kolobar $T_3(\mathbb{Z})/I$ vsebuje neničelni nilpotent.
- Pokaži, da kvocientni kolobar $T_3(\mathbb{Z})/I$ ni komutativen.
- Ali je preslikava $f: T_3(\mathbb{Z}) \rightarrow T_3(\mathbb{Z})$, podana s predpisom

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} \mapsto \begin{bmatrix} a & e & c \\ 0 & d & b \\ 0 & 0 & f \end{bmatrix},$$

endomorfizem kolobarja $T_3(\mathbb{Z})$?

Rešitev. (a) I je očitno podgrupa aditivne grupe kolobarja $T_3(\mathbb{Z})$. Ker je

$$\begin{bmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & gd & ge + hf \\ 0 & 0 & 2kf \\ 0 & 0 & 0 \end{bmatrix}$$

in

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} \begin{bmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & ag & ah + 2kb \\ 0 & 0 & 2kd \\ 0 & 0 & 0 \end{bmatrix},$$

je tudi ideal.

(b) Ker $E_{23} \notin I$, je $E_{23} + I$ neničelni element kvocientnega kolobarja. Ker je njegov kvadrat enak I , je nilpotenten.

(c) Naj bo $A = E_{22} + 2E_{33}$ in $B = E_{23}$. Potem je $AB = E_{23}$ in $BA = 2E_{23}$. Ker $AB - BA \notin I$, velja $(A + I)(B + I) \neq (B + I)(A + I)$.

(d) Ker je $f(E_{12})f(E_{23}) = E_{23}E_{12} = 0$ in $f(E_{12}E_{23}) = f(E_{13}) = E_{13}$, dana preslikava ni endomorfizem.

3. (a) Razstavi polinom $f(X) = X^4 + X + 1$ na nerazcepne faktorje nad \mathbb{Z}_3 in nad \mathbb{Z}_2 .
- (b) Razstavi element $2 + 16i$ kolobarja $\mathbb{Z}[i]$ na nerazcepne faktorje.
- (c) Poišči največji skupni delitelj d elementov $2 + 16i$ in $3 + i$ kolobarja $\mathbb{Z}[i]$ in ga zapiši v obliki $d = (2 + 16i)\alpha + (3 + i)\beta$, kjer $\alpha, \beta \in \mathbb{Z}[i]$.
- (d) Pokaži, da sta si elementa 2 in $1 + \sqrt{-5}$ kolobarja $\mathbb{Z}[\sqrt{-5}]$ tuja. Ali obstajata $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$, za katera je $1 = 2\alpha + (1 + \sqrt{-5})\beta$?

Rešitev. (a) Ker je $f(1) = 0$, je $f(X)$ deljiv z $X - 1$. Ko opravimo deljenje, dobimo razcep $f(X) = (X - 1)(X^3 + X^2 + X + 2)$. Polinom $X^3 + X^2 + X + 2$ nima ničel v \mathbb{Z}_3 , zato je nerazcepen. Nad \mathbb{Z}_2 polinom nima ničel. Ker tudi ni deljiv z edinim nerazcepnim polinomom $X^2 + X + 1$ stopnje 2, je nerazcepen.

(b) Očitno je $2 + 16i = 2(1 + 8i) = (1 + i)(1 - i)(1 + 8i)$. Element $1 + 8i$ ima normo $65 = 5 \cdot 13$. Iščemo njegove delitelje z normo 5: preverimo element $2 + i$. Imamo:

$$\frac{1 + 8i}{2 + i} = \frac{(1 + 8i)(2 - i)}{5} = 2 + 3i.$$

Zato je

$$2 + 16i = (1 + i)(1 - i)(2 + i)(2 + 3i).$$

Ker je norma vsakega od faktorjev praštevilo, smo dobili razcep na nerazcepne faktorje.

(c) Z uporabo Evklidovega algoritma računamo:

$$\frac{2 + 16i}{3 + i} = \frac{(2 + 16i)(3 - i)}{10} = \frac{22 + 46i}{10} \approx 2 + 5i.$$

Ostanek je tako enak:

$$r_1 = 2 + 16i - (3 + i)(2 + 5i) = 2 + 16i - (1 + 17i) = 1 - i.$$

V naslednjem koraku delimo $3 - i$ z r_1 in dobimo:

$$\frac{3 - i}{1 - i} = \frac{(3 - i)(1 + i)}{2} = 2 + 2i.$$

Največji skupni delitelj je zato zadnji neničelni ostanek, to je $r_1 = 1 - i$. Iskani zapis je $1 - i = 2 + 16i - (3 + i)(2 + 5i)$.

(d) Ker je norma elementa 2 enaka 4 in je norma elementa $1 + \sqrt{-5}$ enaka 6, edina možnost za netrivialni skupni delitelj d bi bila, da bi imel d normo 2. Ker je $N(a + b\sqrt{-5}) = a^2 + 5b^2$, elementa z normo 2 ne obstaja. Zato sta si dana elementa tuja. Če enakost $1 = 2\alpha + (1 + \sqrt{-5})\beta$ pomnožimo z $1 - \sqrt{-5}$, dobimo $1 - \sqrt{-5} = 2\alpha(1 - \sqrt{-5}) + 6\beta$. Ker je desna stran deljiva z 2, enako mora veljati za levo stran. Element $1 - \sqrt{-5}$ pa ni deljiv z 2, kar je protislovje. Zato enakost $1 = 2\alpha + (1 + \sqrt{-5})\beta$ ne velja za nobena $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

2.5 2. izpit - 21.8.2024

1. (a) Naj bo \mathbb{H} obseg kvaternionov. Definirajmo množenji $*$ in \bullet na \mathbb{H} s praviloma

$$x * y = 2xy, \quad x \bullet y = ixy.$$

Pokaži, da je $(\mathbb{H}, +, *)$ kolobar. Ali je $(\mathbb{H}, +, \bullet)$ kolobar?

- (b) Pokaži, da grupa obrnljivih elementov kolobarja

$$L = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\} \subseteq \mathbb{H}$$

sovpada s kvaternionsko grupo $Q = \{1, -1, i, -i, j, -j, k, -k\}$.

- (c) Poišči center $Z(Q)$ grupe Q in pokaži, da je kvocientna grupa $Q/Z(Q)$ izomorfna grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- (d) Poišči konjugiranostne razrede grupe Q .
- (e) Ali so vsi avtomorfizmi grupe Q notranji?

Rešitev. (a) Ker $2 \in Z(\mathbb{H})$, se hitro vidi, da je množenje asociativno. Distributivnost očitno tudi velja. Enota pa je element $1/2$. Ker $i \notin Z(\mathbb{H})$, množenje \bullet ni asociativno: na primer $(j \bullet j) \bullet 1 = (ijj) \bullet 1 = (-i) \bullet 1 = 1$, ampak $j \bullet (j \bullet 1) = j \bullet (ij) = ijk = -1$.

(b) Elementi grupe Q so očitno obrnljivi. Če je neničelni element $z = a + bi + cj + dk \in L$ obrnljiv, njegov inverz sovpada z inverzom v \mathbb{H} in je enak

$$z^{-1} = \frac{a - bi - cj - dk}{\sqrt{a^2 + b^2 + c^2 + d^2}}.$$

Če sta vsaj dva elementa izmed a, b, c, d različna od 0, na primer $a, b \neq 0$, je

$$0 < \frac{|a|}{\sqrt{a^2 + b^2 + c^2 + d^2}} < 1$$

in zato $z^{-1} \notin L$. Če $a \neq 0$ in $b, c, d = 0$, potem je $a = 1$ ali $a = -1$. Sledi, da leži vsak obrnljiv element v Q .

(c) Očitno $\{1, -1\} \subseteq Z(Q)$. Ker $ij \neq ji$, sledi, da $i, -i \notin Z(Q)$. Podobno imamo: $j, -j, k, -k \notin Z(Q)$. Zato je $Z(Q) = \{1, -1\}$. Preslikava $\varphi: Q \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ s predpisom

$$\begin{aligned}\varphi(1) &= \varphi(-1) = (0, 0), \\ \varphi(i) &= \varphi(-i) = (1, 0), \\ \varphi(j) &= \varphi(-j) = (0, 1), \\ \varphi(k) &= \varphi(-k) = (1, 1),\end{aligned}$$

je epimorfizem z jedrom $\{1, -1\}$, zato je

$$Q/Z(Q) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Lahko bi tudi sklicali na izomorfizem $Q/Z(Q) \simeq Inn(Q)$ in preverili, da je

$$Inn(Q) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

(d) Konjugiranje z 1 in -1 preslika vsak element vase. Konjugiranje z i in $-i$ preslika $i \mapsto i, j \mapsto -j, k \mapsto -k$. Podobne ugotovitve držijo za konjugiranje z $j, -j, k$ in $-k$. Sledi, da so konjugiranostne razrede $\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}$. Lahko bi tudi uporabili dejstvo, da je moč konjugiranostnega razreda elementa enaka indeksu njegovega centralizatorja. Ker i komutira natanko z $1, -1, i, -i$, je indeks njegovega centralizatorja enak 2 in hitro sledi, da je njegov konjugiranostni razred enak $\{i, -i\}$.

(e) Preslikava $\psi: Q \rightarrow Q$, ki slika $1 \mapsto 1, i \mapsto j \mapsto k \mapsto i$, definira avtomorfizem grupe Q . Ta avtomorfizem ni notranji, saj iz prejšnje točke sledi, da notranji avtomorfizem lahko slika i le v i ali v $-i$.

2. (a) Do izomorfizma natančno zapiši vse Abelove grupe reda 100.
- (b) Pokaži, da (do izomorfizma natančno) obstaja ena sama Abelova grupa reda 100, ki ni ciklična, ima element reda 50 in nima elementa reda 4.
- (c) Koliko elementov reda 10 ima grupa $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$?

- (d) Koliko do izomorfizma natančno različnih Abelovih grup reda največ 20, v katerih je red vsakega elementa 1, 2 ali 4?
- (e) Naj bo G grupa reda 10, ki ni ciklična. Pokaži, da je G izomorfna grupi D_{10} .

Rešitev. (a) Ker je $100 = 2^2 5^2$, z uporabo izreka o končnih Abelovih grupah dobimo naslednji seznam grup: $A = \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$, $B = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$, $C = \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ in $D = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.

(b) Danemu pogoju zadošča le grupa $B = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$ iz prejšnje točke (grupa A je ciklična, grupa C ima element reda 4, grupa D pa nima elementa reda 50).

(c) Uporabimo izomorfizem $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$. Element (a, b, c, d) slednje grupe je reda 10, če ima (a, b) red 2 in (c, d) red 5. Za (a, b) imamo tako 3 možnosti (lahko vzamemo vsak element grupe $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ razen elementa $(0, 0)$) in za (c, d) 24 možnosti (lahko vzamemo vsak element grupe $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ razen elementa $(0, 0)$). Skupaj je torej $3 \cdot 24 = 72$ elementov reda 10.

(d) Če ima netrivialna Abelova grupa le elemente redov 1, 2 ali 4, sta v njenem razvoju v direktno vsoto grup oblike \mathbb{Z}_{p^n} (kjer je p praštevilo in $n \geq 1$) le grupi \mathbb{Z}_2 in \mathbb{Z}_4 . Iskane netrivialne grupe so zato \mathbb{Z}_2 , \mathbb{Z}_4 , $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. Skupaj z trivialno grupo imamo torej 9 takih grup.

(e) Po Cauchijevev izreku ima grupa G element a reda 5 in b reda 2. Označimo $A = \langle a \rangle$ in $B = \langle b \rangle$. Ker ima A indeks 2, je edinka. Zato je AB podgrupa grupe G . Ker $A \cap B = \{1\}$ je $|AB| = 10$ in je zato $G = AB$. Če je $ba = a^k b$, kjer $k \in \{0, 1, 2, 3, 4\}$, sledi, da je

$$ba^2 = (ba)a = a^k(ba) = a^{2k}b$$

in potem tudi $ba^t = a^{kt}b$ za vsak t . Zato je

$$a = bba = ba^k b = a^{k^2} bb = a^{k^2}$$

in je potem $1 = a^{k^2-1}$. Sledi, da mora biti $k = 1$ ali $k = 4$. Če je $k = 1$, je $G \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_2 \simeq \mathbb{Z}_{10}$ in je ciklična, če je $k = 4$ je $ba = a^{-1}b$ in je $G \simeq D_{10}$.

- 3.** (a) Poišči stopnjo razširitve $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.
- (b) Poišči minimalni polinom elementa $\sqrt{2} + \sqrt{3}$ nad \mathbb{Q} .
- (c) Poišči stopnjo razširitve $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}]$.

(d) Poišči stopnjo razširitve $[\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) : \mathbb{Q}]$.

Rešitev. (a) V verigi razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

ima prva razširitev stopnjo 2 (ker $\sqrt{2} \notin \mathbb{Q}$ in je ničla polinoma $X^2 - 2$). Če bi veljalo $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, bi bilo $\sqrt{3} = a + b\sqrt{2}$ za racionalna a in b , od kod sledi $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Ker $\sqrt{2} \notin \mathbb{Q}$, je $ab = 0$. Če je $a = 0$, bi sledilo, da je $\sqrt{6} \in \mathbb{Q}$, če je $b = 0$, pa da je $\sqrt{3} \in \mathbb{Q}$. Dobljeno protislovje pove, da ima tudi druga razširitev stopnjo 2 in je tako

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

(b) Iz enakosti

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

hitro sledi, da je

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

torej je

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4.$$

Če označimo $a = \sqrt{2} + \sqrt{3}$, je $(a - \sqrt{2})^2 = 3$, kar se prepíše v $2a\sqrt{2} = a^2 - 1$. Če to kvadriramo, dobimo $8a^2 = a^4 - 2a^2 + 1$. Zato je a ničla polinoma $f(X) = X^4 - 10X^2 + 1$. Ker je stopnja polinoma enaka stopnji razširitve, je $f(X)$ minimalni polinom.

(c) Ker je

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

in je stopnja prve razširitve 4, je iskana stopnja najmanj 4. Ker je $\sqrt{5}$ ničla polinoma $X^2 - 5$, je stopnja druge razširitve največ 2, zato je iskana stopnja 4 ali 8. Če bi bila 4, bi imeli

$$\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}),$$

torej $\sqrt{5} = a + b\sqrt{3}$, kjer $a, b \in \mathbb{Q}(\sqrt{2})$. Ko to kvadriramo, dobimo

$$5 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Ker $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, je $ab = 0$. Če je $a = 0$, je $\sqrt{5} = b\sqrt{3}$, od kot dobimo

$$\sqrt{15} = 3b \in \mathbb{Q}(\sqrt{2}).$$

Če je $b = 0$, je $\sqrt{5} = a \in \mathbb{Q}(\sqrt{2})$. Podobno kot v točki (a), oba primera vodita v protislovje. Zato je

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2,$$

in je iskana stopnja enaka 8.

(d) Na prvi površni pogled se morda zdi, da je odgovor, podobno kot prej, enak 8. Opazimo pa, da je

$$\sqrt{15} = \frac{\sqrt{6}\sqrt{10}}{2} \in \mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

Torej je

$$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

Sedaj podobno kot prej sklepamo, da ima v verigi razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{6}, \sqrt{10})$$

vsaka razširitev stopnjo 2 in je zato iskana stopnja enaka 4.

2.6 3. izpit - 3.9.2024

1. Označimo $K = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b \in \mathbb{Q}, c \in \mathbb{Z} \right\}$.

- Pokaži, da je K podkolobar kolobarja $M_2(\mathbb{Q})$.
- Opiši vse obrnljive elemente kolobarja K .
- Pokaži, da je s predpisom $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mapsto c + 2\mathbb{Z}$ podana preslikava $\varphi: K \rightarrow \mathbb{Z}_2$ epimorfizem kolobarjev ter poišči njeno jedro.
- Pokaži, da ima K neskončno mnogo idealov.
- Pokaži, da ima K neskončno mnogo desnih idealov I_n , $n \in \mathbb{N}$, za katere velja $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$.

Rešitev. (a) Ker je K zaprta za operacije množenja in odštevanja in vsebuje identično matriko, je podkolobar kolobarja $M_2(\mathbb{Q})$.

(b) Če je $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} p & q \\ 0 & r \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, kjer sta oba faktorja iz K , je $c = 1$ ali $c = -1$. Ker je determinanta obrnljive matrike neničelna, mora biti $a \neq 0$. Po

drugi strani, se hitro vidi, da inverz matrice $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, kjer $a \neq 0$ in $c \in \{1, -1\}$, leži v K in je zato vsaka taka matrika obrnljiva v K .

(c) To preverimo z direktnim računom, jedro je ideal $\begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & 2\mathbb{Z} \end{bmatrix}$.

(d) Različni ideali so na primer $I_n = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & n\mathbb{Z} \end{bmatrix}$, $n \in \mathbb{N}$.

(e) Na primer, $J_n = \left\{ \begin{bmatrix} 0 & \frac{c}{2^n} \\ 0 & 0 \end{bmatrix} : c \in \mathbb{Z} \right\}$, $n \in \mathbb{N}$.

Opomba. Da se pokazati, da neskončne naraščajoče verige levih idealov (ali idealov) kolobar K nima.

- 2.** (a) Ali sta si grupi $\mathbb{Z}_{20} \oplus \mathbb{Z}_{50}$ in $\mathbb{Z}_{10} \oplus \mathbb{Z}_{100}$ izomorfni?
 (b) Koliko do izomorfizma natančno je Abelovih grup reda 2000?
 (c) Koliko podgrup reda 6 ima Abelova grupa reda 18, ki ni ciklična?
 (d) Pokaži, da je vsaka grupa reda 45 Abelova.

Rešitev. (a) Vsaka od danih grup je izomorfna grupi $\mathbb{Z}_5 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$, zato sta si grupi izomorfni.

(b) Ker je $2000 = 5^3 \cdot 2^4$, pogledamo, koliko je Abelovih grup redov 5^3 in 2^4 . Za Abelovo grupo reda 5^3 je 3 možnosti (\mathbb{Z}_{5^3} , $\mathbb{Z}_{5^2} \oplus \mathbb{Z}_5$, $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$), za Abelovo grupo reda 2^4 pa je podobno 5 možnosti. Skupaj je torej 15 grup.

(c) Ker je $18 = 2 \cdot 3^2$, je Abelova grupa reda 18 izomorfna bodisi grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_9$, ki je ciklična, bodisi grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Element (a, b, c) slednje grupe ima red 6, če ima a red 2 (torej je nujno $a = 1$) in (b, c) red 3 (ustreza vsak element iz $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, razen elementa $(0, 0)$, torej je 8 možnosti). Potem je 8 elementov reda 6. Če imata dve podgrupi reda 6 skupen element reda 6, potem sovpadata (saj sta ciklični z istim generatorjem). Grupa reda 6 pa ima 2 elementa reda 6 (v \mathbb{Z}_6 sta to 1 in 5). Zato je $\frac{8}{2} = 4$ podgrupe reda 6.

(d) Naj bo G grupa reda 45. Z uporabo izreka Sylowa je $n_5 \equiv 1 \pmod{5}$ in $n_5 | 9$. Zato je $n_5 = 1$. Podobno je $n_3 = 1$. Torej ima G podgrupo edinko A reda 5 in podgrupo edinko B reda 9. Ker ima vsak element grupe A red 1 ali 5, in vsak element grupe B red 1, 3 ali 9, je $A \cap B = \{1\}$. Zato je G notranji direktni produkt podgrup A in B in je tako izomorfna njenemu zunanjemu direktnemu produktu $A \times B$. Grupa A ima praštevilski red in je zato Abelova. Če ima grupa B element reda 9, je Abelova, sicer ima

vsak njen neidentični element red 3. Element a reda 3 generira podgrupo $\langle a \rangle = \{1, a, a^2\}$, če vzamemo $b \neq a, a^2$, je $\langle b \rangle = \{1, b, b^2\}$ še ena podgrupa reda 3 in je zato $B \simeq \langle a \rangle \times \langle b \rangle$ Abelova. Potem je tudi G Abelova.

3. (a) Poišči vse nerazcepne polinome stopnje 2 nad \mathbb{Z}_3 .
 (b) Razstavi polinom $X^4 + 1$ na nerazcepne faktorje nad \mathbb{Z}_3 .
 (c) Poišči stopnjo razpadnega polja polinoma $X^4 + 1$ nad \mathbb{Q} .
 (d) Naj bo $c \in \mathbb{C}$ tak, da je $[\mathbb{Q}(c) : \mathbb{Q}] = 6$. Koliko je potem lahko $[\mathbb{Q}(c^2) : \mathbb{Q}]$?

Rešitev. (a) Polinom stopnje 2 ima obliko $f(X) = aX^2 + bX + c$, kjer $a \neq 0$. Ker imata $f(X)$ in $2f(X)$ iste ničle, je $f(X)$ nerazcepen natanko takrat, ko je $2f(X)$ nerazcepen, zato lahko pri iskanju nerazcepnih polinomov predpostavimo, da je $f(X) = X^2 + bX + c$. Ta polinom ima ničlo 0 natanko tedaj, ko je $c = 0$, ničlo 1, ko je $1 + b + c = 0$ (torej $b = 1$ in $c = 1$ ali $b = 0$ in $c = 2$) in ničlo 2, ko je $1 + 2b + c = 0$ (torej $b = 2$ in $c = 1$ ali $b = 0$ in $c = 2$). Nerazcepni so torej vsi ostali polinomi:

$$h_1(X) = X^2 + 1, \quad h_2(X) = X^2 + X + 2, \quad h_3(X) = X^2 + 2X + 2$$

in njihovi dvakratniki.

(b) Nad \mathbb{Z}_3 polinom $X^4 + 1$ nima ničel. Če je kljub temu razcepen, je produkt dveh nerazcepnih polinomov stopnje 2. Hitro se vidi da $X^4 + 1$ ni deljiv s $h_1(X)$, vendar je deljiv s $h_2(X)$ in je zato $X^4 + 1 = h_2(X)h_3(X) = ((X^2 + 2) + X)((X^2 + 2) - X)$ iskani razcep.

(c) Naj bo $f(X) = X^4 + 1$. Ker je

$$g(X) = f(X + 1) = (X + 1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$$

nerazcepen nad \mathbb{Q} po Eisensteinovem kriteriju za $p = 2$, je tudi $f(X)$ nerazcepen nad \mathbb{Q} . Ničle polinoma $X^4 + 1$ v \mathbb{C} so $\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7$, kjer je $\varepsilon = e^{\frac{i\pi}{4}}$, zato razpadno polje $f(X)$ je polje $\mathbb{Q}(\varepsilon)$. Stopnja slednjega polja nad \mathbb{Q} je 4, saj je $f(X)$ nerazcepen in je tako minimalni polinom za ε nad \mathbb{Q} .

(d) Ker elementi $1, c, c^2, c^3, c^4, c^5$ tvorijo bazo $\mathbb{Q}(c)$ nad \mathbb{Q} , so $1, c^2, c^4$ linearno neodvisni in je tako

$$[\mathbb{Q}(c^2) : \mathbb{Q}] \geq 3.$$

Ker $[\mathbb{Q}(c^2) : \mathbb{Q}]$ deli 6, je lahko le 3 ali 6. Preverimo, ali sta te možnosti realizirani. Če vzamemo $c = \sqrt[6]{2}$, je $c^2 = \sqrt[3]{2}$ in je potem

$$[\mathbb{Q}(c) : \mathbb{Q}] = 6 \quad \text{in} \quad [\mathbb{Q}(c^2) : \mathbb{Q}] = 3.$$

Sedaj si oglejmo polinom $h(X) = X^6 + 2X + 2$, ki je nerazcepen nad \mathbb{Q} po Eisensteinovem kriteriju za $p = 2$. Če je c ničla tega polinoma, je $[\mathbb{Q}(c) : \mathbb{Q}] = 6$. Ker $(c^2)^3 + 2c + 2 = 0$, je $c \in \mathbb{Q}(c^2)$. Ker tudi $c^2 \in \mathbb{Q}(c)$, imamo enakost $\mathbb{Q}(c) = \mathbb{Q}(c^2)$. Zato je

$$[\mathbb{Q}(c) : \mathbb{Q}] = [\mathbb{Q}(c^2) : \mathbb{Q}] = 6.$$

Poglavje 3: Študijsko leto 2024/25

3.1 1. kolokvij - 18.12.2024

1. (a) Zapiši leve in desne odseke grupe D_{12} po podgrupi $H = \{e, r^2, r^4\}$ in sklepaj, da je $H \triangleleft D_{12}$.
- (b) Ali je $D_{12}/H \simeq \mathbb{Z}_4$?
- (c) Poišči center $Z(D_{12})$ grupe D_{12} .
- (d) Pokaži, da je $D_{12}/Z(D_{12}) \simeq D_6$.
- (e) Ali je $D_{12} \simeq A_4$?

Rešitev. (a) Imamo $D_{12} = \{e, r, r^2, r^3, r^4, r^5, z, rz, r^2z, r^3z, r^4z, r^5z\}$. Levi odseki so:

$$H, rH = \{r, r^3, r^5\}, zH = \{z, r^2z, r^4z\}, rzH = \{rz, r^3z, r^5z\}.$$

Desni odseki so:

$$H, Hr = \{r, r^3, r^5\}, Hz = \{z, r^2z, r^4z\}, Hrz = \{rz, r^3z, r^5z\}.$$

Podgrupa je H torej edinka.

(b) Elementi Z_{12}/H so H, rH, zH, rzH . Ker $e \in (rH)^2, (zH)^2, (rzH)^2$, je $(rH)^2 = (zH)^2 = (rzH)^2 = H$, kvocientna grupa Z_{12}/H nima elementa reda 4, zato $Z_{12}/H \not\cong \mathbb{Z}_4$.

(c) Enostavno je videti, da $\{e, r^3\} \subseteq Z(D_{12})$. Ker nobena simetrija ne komutira z r in r, r^2, r^4, r^5 ne komutirajo z z , je $Z(D_{12}) = \{e, r^3\}$.

(d) Naj bo $D_6 = \{e, a, a^2, b, ab, a^2b\}$. Definirajmo preslikavo $f: D_{12} \rightarrow D_6$ s predpisom

$$f(r^i z^j) = a^{i \pmod{3}} z^j.$$

Ker je

$$f(r^i z^j r^s z^t) = f(r^{(i-s) \pmod{6}} z^{(j+t) \pmod{2}}) = a^{(i-s) \pmod{3}} b^{(j+t) \pmod{2}},$$

$$f(r^i z^j) f(r^s z^t) = a^{i(\bmod 3)} z^j a^{s(\bmod 3)} z^t = a^{(i-s)(\bmod 3)} b^{(j+t)(\bmod 2)},$$

je f homomorfizem. Iz definicije f sledi, da je f surjektiven. Ker je jedro f podgrupa $Z(D_{12})$, iz prvega izreka o izomorfizmu sledi, da je $D_{12}/Z(D_{12}) \simeq D_6$.

(e) Grupa A_4 ima elemente $e, (12)(34), (14)(32), (13)(24)$ in osem 3-ciklov. Ker A_4 nima nobenega elementa reda 6, D_{12} pa ima element r reda 6, $D_{12} \not\cong A_4$.

2. Naj bo G grupa.

- (a) Naj bo $H \triangleleft G$ in $a, b \in G$ taka, da $ab \in H$. Pokaži, da $ba \in H$.
- (b) S primerom pokaži, da brez pogoja $H \triangleleft G$ trditev iz prejšnje točke ne drži.
- (c) Naj bo G končna grupa in H, K podgrupi grupe G , za kateri sta $[G : H]$ in $[G : K]$ tuji števili. Označimo

$$HK = \{hk : h \in H, k \in K\} \subseteq G.$$

Pokaži, da je $HK = G$.

Namig. Uporabi enakost $|HK| = \frac{|H||K|}{|H \cap K|}$.

- (d) Pokaži, da je $\text{Aut}(S_3) \simeq S_3$.
- (e) Pokaži, da je $\text{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2) \simeq S_3$.

Rešitev. (a) $ab \in H$ velja natanko tedaj, ko je $a^{-1}H = bH$. Ker je H edinka, se slednja enakost prepíše v $Ha^{-1} = Hb$, ki je ekvivalentna enakosti $H = Hba$. Slednja pa velja natanko tedaj, ko $ba \in H$.

(b) Naj bo $G = S_3$ in z e njena enota. Za elementa $a = (12)$ in $b = (123)$ velja $ab = (12)(123) = (23)$ in $ba = (123)(12) = (13)$. Torej, če vzamemo $H = \{e, (23)\}$, imamo $ab \in H$ in $ba \notin H$.

(c) Ker je $|H| = \frac{|G|}{[G:H]}$ in $|K| = \frac{|G|}{[G:K]}$, velja

$$|HK| = \frac{|G|}{[G:H]} \frac{|G|}{[G:K]} \frac{1}{|H \cap K|} = \frac{[G : (H \cap K)]}{[G:H][G:K]} |G|.$$

Ker je $H \cap K < H < G$, je

$$[G : (H \cap K)] = [G:H][H : (H \cap K)],$$

torej $[G : H]$ deli $[G : (H \cap K)]$ in podobno $[G : K]$ deli $[G : (H \cap K)]$. Ker sta si števili $[G : K]$ in $[G : H]$ tuji, njiun produkt deli $[G : (H \cap K)]$, torej je število

$$\frac{[G : (H \cap K)]}{[G : H][G : K]}$$

celo, in je zato $|HK| \geq |G|$. Ker $HK \subseteq G$, velja enakost $HK = G$.

(d) Ker je $Z(S_3) = \{1\}$, je $\text{Inn}(S_3) \simeq S_3/Z(S_3) \simeq S_3$. Ostane le pokazati, da je vsak avtomorfizem grupe S_3 notranji. Naj bo φ netrivialni avtomorfizem. Ker φ ohranja red elementov, preslika transpozicije v transpozicije. Ker (12) in (23) generirata S_3 , je φ določen z vrednostmi $\varphi(12)$ in $\varphi(13)$. Za $\varphi(12)$ so 3 možnosti: (12), (13) in (23), za $\varphi(13)$ potem preostaneta dve možnosti. Zato skupaj imamo največ 6 avtomorfizmov. Ker S_3 ima 6 notranjih avtomorfizmov, ima natanko 6 avtomorfizmov in so vsi notranji.

(e) Grupa $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ima strukturo dvorazsežnega vektorskega prostora nad \mathbb{Z}_2 . Avtomorfizmi grupe so tako podani z 2×2 obrnljivimi matrikami nad \mathbb{Z}_2 . Ker je takih matrik 6, imamo 6 avtomorfizmov. Ker grupa $\text{GL}_2(\mathbb{Z}_2)$ ima moč 6 in ni Abelova, je izomorfna S_3 .

3. (a) Pokaži, da je podalgebra algebre $M_2(\mathbb{R})$, generirana z matrikama $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in $B = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}$, izomorfna algebri $T_2(\mathbb{R})$ vseh realnih zgoraj trikotnih matrik.
- (b) Pokaži, da matrika $C = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ generira podalgebro algebre $M_2(\mathbb{R})$, ki je izomorfna realni algebri kompleksnih števil \mathbb{C} .
- (c) Naj bo $L \neq \{0\}$ levi ideal in $R \neq \{0\}$ desni ideal kolobarja $M_2(\mathbb{R})$. Pokaži, da enakost $rl = 0$ ne more veljati za vse $r \in R$ in $l \in L$.
- (d) Poišči primer levega ideala $L \neq \{0\}$ in desnega ideala $R \neq \{0\}$ kolobarja $M_2(\mathbb{R})$, za katera velja $LR = \{0\}$.

Rešitev. (a) Označimo dano podalgebro z \mathcal{A} . Ker je

$$A = E_{11} \in \mathcal{A}, \quad \frac{1}{2}AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = E_{12} \in \mathcal{A} \quad \text{in} \quad B - \frac{1}{2}AB = E_{22} \in \mathcal{A},$$

sledi, da $T_2(\mathbb{R}) \subseteq \mathcal{A}$. Po drugi strani, ker sta A, B zgoraj trikotni, $\mathcal{A} \subseteq T_2(\mathbb{R})$. Potem velja $\mathcal{A} = T_2(\mathbb{R})$.

(b) Ker je $C^2 = -I$, C generira dvorazsežno podalgebro

$$\{\alpha I + \beta C : \alpha, \beta \in \mathbb{R}\}$$

in je preslikava $\alpha I + \beta C \mapsto \alpha + \beta i$ izomorfizem med to podalbebno in \mathbb{C} .

(c) Naj bo $A \in R$ in $B \in L$ poljubni neničelni matriki. Potem obstajata neničelna vektorja $v, w \in \mathbb{R}^2$, da $Av \neq 0$ in $w^T B \neq 0$. Potem tudi $(Av)(w^T B) \neq 0$. Torej $(Avw^T)B \neq 0$. Ker je R desni ideal, $Avw^T \in R$.

(d) Naj bo $L = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \right\}$ in $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\}$. Enostavno je videti, da je L levi ideal, R desni ideal in $LR = \{0\}$.

3.2 2. kolokvij - 24.3.2025

1. (a) Do izomorfizma natančno določi vse Abelove grupe reda 2025.
- (b) Koliko elementov reda 4 ima grupa $\mathbb{Z}_{12} \oplus \mathbb{Z}_4$?
- (c) Pokaži, da ima grupa $\mathbb{Z}_{12} \oplus \mathbb{Z}_4$ natanko eno podgrupo, izomorfnu $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- (d) Koliko podgrup reda 4 ima grupa $\mathbb{Z}_{12} \oplus \mathbb{Z}_4$?
- (e) Pokaži, da je grupa $\mathbb{Z} \oplus \mathbb{Z}$ notranji direktni produkt podgrup $A = \langle (1, 2) \rangle$ in $B = \langle (3, 5) \rangle$.

Rešitev. (a) To so vse grupe $H_1 \oplus H_2$, kjer je H_1 ena izmed grup \mathbb{Z}_{25} ali $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ in H_2 ena izmed grup \mathbb{Z}_{81} , $\mathbb{Z}_{27} \oplus \mathbb{Z}_3$, $\mathbb{Z}_9 \oplus \mathbb{Z}_9$, $\mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

(b) Zapišemo $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$. Element $(a, b, c) \in \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$ ima red 4 natanko tedaj, ko je (a, b) reda 4 in $c = 0$. Ker ima $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ 3 elemente reda 2 in en element reda 1, ima 12 elementov reda 4.

(c) Ker ima $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ 3 elemente reda 2, ima tudi $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$ natanko 3 elemente reda 2. Zato ima eno podgrupo, izomorfnu $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. To je podgrupa $\{(0, 0, 0), (2, 0, 0), (0, 2, 0), (2, 2, 0)\}$.

(d) Če je $(a, b, 0)$ element reda 4, generira podgrupo, izomorfnu \mathbb{Z}_4 , ki poleg tega elementa vsebuje še en element reda 4 (ki generira isto podgrupo). Zato imamo $\frac{12}{2} = 6$ podgrup, izomorfnih \mathbb{Z}_4 . Skupaj s podgrupo iz prejšnje točke imamo torej 7 podgrup reda 4.

(e) Naj bo (a, b) poljubni element grupe $\mathbb{Z} \oplus \mathbb{Z}$. Če velja $(a, b) = s(1, 2) + t(3, 5)$, je $a = s + 3t$ in $b = 2s + 5t$. Potem je $t = 2a - b$ in $s = a - 3t = -5a + 3b$. Zato lahko vsak element grupe $\mathbb{Z} \oplus \mathbb{Z}$ enolično zapišemo kot vsoto elementa iz A in elementa iz B , in je tako $\mathbb{Z} \oplus \mathbb{Z}$ notranji direktni produkt podgrup A in B .

2. (a) Določi orbito 3-cikla $(123) \in S_3$ za delovanje grupe S_3 na sebi s konjugiranjem.
- (b) Določi centralizator 3-cikla $(123) \in S_3$ v grupi S_3 .
- (c) Določi normalizator $N_{S_4}(H)$ podgrupe $H = \langle (1234) \rangle$ grupe S_4 .
- (d) Določi število ogrlic iz 5 korald rdeče, modre in zelene barve.
Opomba. Predpostavi, da sta dve ogrlici enaki, če sta v isti orbiti pri delovanju grupe D_{10} . Pomagaj si z Burnsidovo lemo.

Rešitev. (a) Ker so orbite pri delovanju grupe na sebi s konjugiranjem natanko konjugiranostni razredi, je iskana orbita sestavljena iz vseh 3-ciklov grupe S_3 . Ima 2 elementa, (123) in (132) .

(b) Enakost $g(123) = (123)g$ očitno velja za $g_1 = 1$, $g_2 = (123)$ in $g_3 = (132)$. Torej centralizator elementa (123) vsebuje g_1, g_2, g_3 . Ker je indeks centralizatorja enak dolžini orbite elementa (123) , torej 2, je iskan centralizator enak $\{g_1, g_2, g_3\} = \langle (123) \rangle$.

(c) *1. način.* Naj velja $gHg^{-1} = H$. Potem element $g(1234)g^{-1}$ leži v H in ima red 4, zato je enak (1234) ali (1432) . Enakost $g(1234)g^{-1} = (1234)$ velja za $g \in H = \{1, (1234), (13)(24), (1432)\}$. Ker je $g(1234)g^{-1} = (g(1)g(2)g(3)g(4))$, enakost $g(1234)g^{-1} = (1432)$ velja za

$$g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24), \quad g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23),$$

$$g_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13), \quad g_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34).$$

Torej je

$$N_{S_4}(H) = H \cup \{g_1, g_2, g_3, g_4\}.$$

2. način. Naj bo $G = \{(1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$ podgrupa S_4 , izomorfná grupi D_8 . Ker ima H v G indeks 2, je $H \triangleleft G$, in zato $G \subseteq N_{S_4}(H)$. Zato $|N_{S_4}(H)| \geq 8$. Ker H ni edinka S_4 in $|N_{S_4}(H)|$ deli 24, je $|N_{S_4}(H)| = 8$, torej je $N_{S_4}(H) = G$.

(d) Označimo $D_{10} = \{1, r, r^2, r^3, r^4, z_1, z_2, z_3, z_4, z_5\}$. Za vsak $a \in D_{10}$ izračunajmo število negibnih točk. Za $a = 1$ lahko vsako koraldo pobarvamo s katerokoli barvo in imamo tako 3^5 negibnih točk. Za $a = r, r^2, r^3, r^4$ mora biti koralda enobarvna, in imamo tako 3 negibne točke. Os vsakega od petih zrcaljenj poteka čez eno oglišče in središče nasprotne stranice pravilnega petkotnika, zato imamo 3^3 negibnih točk. Z uporabo Burnsidove leme dobimo,

da je iskano število ogrlic enako

$$\frac{1}{10}(3^5 + 4 \cdot 3 + 5 \cdot 3^3) = \frac{3}{10}(81 + 4 + 45) = \frac{3 \cdot 130}{10} = 39.$$

3. (a) Pokaži, da je $\langle(123)\rangle \times \langle(456)\rangle$ 3-podgrupa Sylowa grupe S_6 .
 (b) Koliko 3-podgrup Sylowa ima grupa S_6 ?
 (c) Pokaži, da je vsaka grupa reda 35 Abelova.
 (d) Pokaži, da grupa reda 105 ne more biti enostavna.
 (e) Pokaži, da je vsaka grupa reda 105 rešljiva.

Rešitev. (a) Ker je $|S_6| = 720 = 2^4 \cdot 3^2 \cdot 5$, ima 3-podgrupa Sylowa red 9. Ker je $\langle(123)\rangle \times \langle(456)\rangle$ izomorfna grupi $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, ima red 9 in je zato 3-podgrupa Sylowa.

(b) Število 3-podgrup Sylowa je enalo številu neurejenih razbitij 6-elementne množice na dva 3-elementna bloka, to je $\binom{6}{3} \cdot \frac{1}{2} = 10$.

(c) Grupa G reda 35 ima edinko H reda 7 in edinko K reda 5 (kar enostavno sledi iz izreka Sylowa). Njun notranji direktni produkt $H \times K$ je vsebovan v G in ima red 35, zato sovпада z G . Ker je $H \times K \simeq \mathbb{Z}_7 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{35}$, je G Abelova (in celo ciklična).

(d) Naj bo G grupa reda 105. Ker je $105 = 3 \cdot 5 \cdot 7$, je $n_7 \in \{1, 15\}$ in $n_5 \in \{1, 21\}$, kjer je n_7 število 7-podgrup Sylowa in n_5 število 5-podgrup Sylowa. Če je $n_7 = 15$ in $n_5 = 21$, imamo $6 \cdot 15$ elementov reda 7 in $4 \cdot 21$ elementov reda 5, kar je skupaj več, kot 105. Zato je $n_7 = 1$ ali $n_5 = 1$. Torej je 7-podgrupa Sylowa ali 5-podgrupa Sylowa edinka.

(e) Po prejšnji točki ima G bodisi 5-podgrupo Sylowa, ki je edinka, bodisi 7-podgrupo Sylowa, ki je edinka. Predpostavimo, da je $H \triangleleft G$ in $|H| = 5$. Potem je $G/H = 35$. Grupa reda 35 pa je po prejšnji točki nujno Abelova. Ker je razširitev rešljive grupe s pomočjo rešljive grupe rešljiva, je G rešljiva. Drugi primer, ko je $H \triangleleft G$ in $|H| = 7$, je podoben.

3.3 3. kolokvij - 19.5.2025

1. (a) Razstavi polinom $X^4 - 3$ na nerazcepne faktorje nad \mathbb{R} .
 (b) Razstavi polinom $X^4 - 3$ na nerazcepne faktorje nad $\mathbb{Q}(\sqrt{3})$.
 (c) Razstavi polinom $X^8 - 81$ na nerazcepne faktorje nad \mathbb{Q} .

- (d) Ali je polinom $X^3 + 2X + 16$ nerazcepen nad \mathbb{Q} ?
- (e) Naj bo \overline{X} ničla polinoma $g(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ v polju $F = \mathbb{Z}_2[X]/(X^3 + X + 1)$. Ali je polinom $h(t) = t^2 + \overline{X} \in F[t]$ nerazcepen?

Rešitev. (a) $X^4 - 3 = (X^2 - \sqrt{3})(X^2 + \sqrt{3}) = (X - \sqrt[4]{3})(X + \sqrt[4]{3})(X^2 + \sqrt{3})$. Zadnji faktor je nerazcepen, ker nima realnih ničel.

(b) Nad $\mathbb{Q}(\sqrt{3})$ velja $X^4 - 3 = (X^2 - \sqrt{3})(X^2 + \sqrt{3})$. Če bi bil prvi faktor razcepen, bi imeli $\sqrt[4]{3} \in \mathbb{Q}(\sqrt{3})$. Sledilo bi

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{Q}(\sqrt{3}),$$

torej $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] \leq 2$, kar ne drži, saj je stopnja $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}]$ enaka stopnji minimalnega polinoma $X^4 - 3$ elementa $\sqrt[4]{3}$ nad \mathbb{Q} , torej je

$$[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4.$$

(c) $f(X) = (X^4 - 9)(X^4 + 9) = (X^2 - 3)(X^2 + 3)(X^4 + 9)$. Prva dva faktorja sta nerazcepna nad \mathbb{Q} , ker nimata racionalnih ničel. Če je $h(X) = X^4 + 9$, je $h(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 10$ nerazcepen po Eisensteinovem kriteriju za $p = 2$, zato je tudi $h(X)$ nerazcepen.

(d) Nad \mathbb{Z}_3 je ta polinom enak $X^3 + 2X + 1$. Ker nima ničel v \mathbb{Z}_3 , je nerazcepen nad \mathbb{Z}_3 . Zato je tudi nerazcepen nad \mathbb{Q} .

(e) Označimo $a = \overline{X}$. Elementi polja F so

$$0, 1, a, a + 1, a^2, a^2 + 1, a^2 + a, a^2 + a + 1.$$

Množenje upošteva enakost $a^3 + a + 1 = 0$ oz. $a^3 = a + 1$. Če bi bil polinom $h(t)$ razcepen, bi imel ničlo v F , hitro pa se vidi, da je

$$h(0) = a, \quad h(1) = a + 1, \quad h(a) = a^2 + a,$$

$$h(a + 1) = a^2 + a + 1, \quad h(a^2) = a^4 + a = a(a + 1) + a = a^2,$$

$$h(a^2 + 1) = a^4 + 1 + a = a(a + 1) + a + 1 = a^2 + 1,$$

$$h(a^2 + a + 1) = a^4 + a^2 + 1 + a = a(a + 1) + a^2 + a + 1 = 1,$$

$$h(a^2 + a) = a^4 + a^2 + a = a(a + 1) + a^2 + a = 0,$$

torej je $h(t) = (t + a^2 + a)^2$.

- 2.** (a) Poišči $[\mathbb{Q}(\sqrt{1 + \sqrt{3}}) : \mathbb{Q}]$.

- (b) Poišči $[\mathbb{Q}(\sqrt{1+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})]$.
- (c) Naj bo L razpadno polje polinoma $X^6 - 1 \in \mathbb{Q}[X]$. Pokaži, da je $[L : \mathbb{Q}] = 2$.
- (d) Naj bo $f(X) \in \mathbb{Q}[X]$ nerazcepen polinom stopnje n in E razširitev polja \mathbb{Q} . Pokaži, da če sta n in $[E : \mathbb{Q}]$ tuji števili, $f(X)$ ostane nerazcepen tudi nad E .
Namig. Naj bo a poljubna ničla $f(X)$ v \mathbb{C} . Kaj lahko poveš o stopnji $E(a)$ nad \mathbb{Q} ?

Rešitev. (a) Označimo $a = \sqrt{1+\sqrt{3}}$. Ker je $a^2 = 1 + \sqrt{3}$, je $\sqrt{3} = a^2 - 1$ in je zato $3 = a^4 - 2a^2 + 1$. Zato je a ničla polinoma $f(X) = X^4 - 2X^2 - 2$. Ker je slednji polinom po Eisensteinovem kriteriju nerazcepen, je $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

(b) Zapišemo verigo razširitev

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(a).$$

Ker je

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \quad \text{in} \quad [\mathbb{Q}(a) : \mathbb{Q}] = 4,$$

je $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{3})] = 2$.

(c) Ničle polinoma $X^6 - 1$ so

$$\pm 1, \quad \frac{1}{2} \pm \frac{\sqrt{3}}{2}i \quad \text{in} \quad -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i.$$

Sledi, da vse ničle ležijo v polju $\mathbb{Q}(\sqrt{3}i)$ in je zato $L = \mathbb{Q}(\sqrt{3}i)$. Ker je $\sqrt{3}i$ ničla polinoma $X^2 + 3$ nad \mathbb{Q} , je $[L : \mathbb{Q}] \leq 2$. Ker očitno $L \neq \mathbb{Q}$, je $[L : \mathbb{Q}] = 2$.

(d) Označimo $[E : \mathbb{Q}] = k$. Ker je

$$E(a) \supseteq \mathbb{Q}(a) \supseteq \mathbb{Q} \quad \text{in} \quad [\mathbb{Q}(a) : \mathbb{Q}] = n,$$

n deli $[E(a) : \mathbb{Q}]$. Po drugi strani je $E(a) \supseteq E \supseteq \mathbb{Q}$. Če označimo $m = [E(a) : E]$, je $[E(a) : \mathbb{Q}] = mk$. Upoštevajoč $(k, n) = 1$, sledi, da n deli m . Po drugi strani pa je a ničla polinoma $f(X) \in E[X]$ in je zato $m \leq n$. Torej je $m = n$ in je zato $f(X)$ nerazcepen nad E .

3. (a) Ali je razširitev $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ normalna?

(b) Poišči vse avtomorfizme polja $\mathbb{Q}(\sqrt[3]{2})$.

- (c) Naj bo K razpadno polje polinoma $g(X) = X^3 - 2$. Pokaži, da je $\text{Gal}(K|\mathbb{Q}) \simeq S_3$.
- (d) Naj bo $L = \mathbb{Q}(\sqrt[3]{2})$. Določi grupo $\text{Gal}(K|L)$, kjer je K polje iz prejšnje točke.

Rešitev. (a) Naj bo $f(X) = X^3 - 2$. Ta polinom ima v $\mathbb{Q}(\sqrt[3]{2})$ ničlo $\sqrt[3]{2}$. Ker $f(X)$ ne razpade nad $\mathbb{Q}(\sqrt[3]{2})$ (saj ima ničle, ki niso realne), razširitev ni normalna.

(b) Ničle $f(X)$ so $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ in $\sqrt[3]{2}\omega^2$, kjer je ω primitivni koren stopnje 3 iz 2. Če je σ avtomorfizem $\mathbb{Q}(\sqrt[3]{2})$, se mora $\sqrt[3]{2}$ preslikati v ničlo polinoma $X^3 - 2$ in hkrati seveda v element polja $\mathbb{Q}(\sqrt[3]{2})$. Zato je $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Sledi, da σ deluje identično na \mathbb{Q} , $\sqrt[3]{2}$ in $\sqrt[3]{4}$. Ker je $1, \sqrt[3]{2}, \sqrt[3]{4}$ baza $\mathbb{Q}(\sqrt[3]{2})$ nad \mathbb{Q} , je σ identični avtomorfizem. Zato ima $\mathbb{Q}(\sqrt[3]{2})$ le identični avtomorfizem.

(c) Razpadno polje $f(X)$ je $\mathbb{Q}(\sqrt[3]{2}, \omega)$, kjer je ω primitivni koren stopnje 3 iz 1. Ker je

$$\mathbb{Q}(\sqrt[3]{2}, \omega) \supseteq \mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$$

in ima prva razširitev stopnjo 2 (ω je ničla $X^2 + X + 1$), druga pa stopnjo 3, je

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6.$$

Ker je dana razširitev Galoisova, je $|\text{Gal}(K|\mathbb{Q})| = 6$. Sledi, da je $\text{Gal}(K|\mathbb{Q})$ podgrupa reda 6 v S_3 , torej sovпада s S_3 .

(d) Ker je $K \supseteq \mathbb{Q}$ Galoisova razširitev in je $K \supseteq L \supseteq \mathbb{Q}$, je tudi $K \supseteq L$ Galoisova. Ker je $[K : L] = 2$, je $|\text{Gal}(K|L)| = 2$. Poleg trivialnega avtomorfizma, $\text{Gal}(K|L)$ vsebuje še avtomorfizem σ , ki je konstanten na $\mathbb{Q}(\sqrt[3]{2})$ in $\sigma(\omega) = \omega^2$.

3.4 1. izpit - 18.6.2025

1. Podani sta matriki $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{R})$.

- (a) Opiši podgrupo grupe obrnljivih 2×2 realnih matrik, ki jo generira matrika A , in pokaži, da je ta grupa izomorfna grupi \mathbb{Z} .
- (b) Pokaži, da podalgebra realne algebre $M_2(\mathbb{R})$, generirana z matrikama A in B , sovпада z algebro $M_2(\mathbb{R})$.
- (c) Opiši podalgebro \mathcal{A} realne algebre $M_2(\mathbb{R})$, ki jo generira matrika A .

- (d) Ali je algebra \mathcal{A} iz prejšnje točke izomorfna realni algebri kompleksnih števil?
- (e) Navedi primer kake podalgebre algebre $M_2(\mathbb{R})$, ki je izomorfna realni algebri kompleksnih števil.

Rešitev. (a) To so vse matrike oblike $A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$, kjer $k \in \mathbb{Z}$. Preslikava $\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \mapsto k$ je izomorfizem z grupo \mathbb{Z} .

(b) Ker je $e_{12} = A - I$ (tudi $e_{12} = A^2 - A$) in $e_{21} = B$, imamo $e_{12}, e_{21} \in \mathcal{B}$, kjer je \mathcal{B} dana algebra. Zato tudi $e_{11} = e_{12}e_{21} \in \mathcal{B}$ in $e_{22} = e_{21}e_{12} \in \mathcal{B}$. Ker \mathcal{B} vsebuje vse 4 matrične enote, sovпада z $M_2(\mathbb{R})$.

(c) Ker je $A = I + e_{12}$, je dana podalgebra generirana z e_{12} . Ker je $e_{12}^2 = 0$, je algebra sestavljena iz matrik $\alpha I + \beta e_{12} = \begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix}$, kjer $\alpha, \beta \in \mathbb{R}$.

(d) Naj bo $X = \begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix} \in \mathcal{A}$. Potem je $X^2 = \begin{bmatrix} \alpha^2 & 2\alpha\beta \\ 0 & \alpha^2 \end{bmatrix}$. Zato algebra \mathcal{A} ne vsebuje elementa X , ki bi zadoščal $X^2 = -I$ in zato ni izomorfna algebri \mathbb{C} .

(e) Oglejmo si podalgebro \mathcal{C} , generirano z $Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Ker je $Y^2 = -I$, je $\mathcal{C} = \{\alpha I + \beta Y : \alpha, \beta \in \mathbb{R}\}$ in je $\alpha I + \beta Y \mapsto \alpha + \beta i$ izomorfizem z algebro kompleksnih števil.

- 2.** (a) Do izomorfizma natančno opiši vse Abelove grupe reda 108.
- (b) Naj bo G grupa reda n in p praštevilski delitelj števila n . Označimo z \mathcal{H} množico p -podgrup Sylowa grupe G . Pokaži, da predpis

$$g \cdot H = gHg^{-1},$$

kjer $g \in G$ in $H \in \mathcal{H}$, definira delovanje grupe G na množici \mathcal{H} .

- (c) Pokaži, da grupa reda 56 ne more biti enostavna.
- (d) Pokaži, da grupa reda 108 ne more biti enostavna.

Rešitev. (a) Ker je $108 = 3^3 \cdot 2^2$, imamo možnosti $\mathbb{Z}_{27} \oplus \mathbb{Z}_4$, $\mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$, $\mathbb{Z}_{27} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(b) Ker so p -podgrupe Sylowa konjugirane, je $gHg^{-1} \in \mathcal{H}$. Hitro sledi, da predpis definira delovanje.

(c) Velja $56 = 7 \cdot 2^3$. Število 7-podgrup Sylowa je potem 1 ali 8. Če bi takih podgrup bilo 8, bi imeli 49 elementov reda 7. Potem je 2-pogrupa Sylowa (ki ima red 8) edinka.

(d) Predpostavimo, da je G grupa reda 108 in da je enostavna. Število 3-podgrup Sylowa je 1 ali 4. Ker je G enostavna, je takih podgrup 4. Grupa G deluje na množici 3-podgrup Sylowa s predpisom iz točke (b). Jedro tega delovanja je edinka v G , zato mora biti trivialno (saj ne more biti G !) Sledi, da obstaja vložitev grupe G reda 108 v grupo S_4 reda 24, kar je nemogoče. Zato G ne more biti enostavna.

3. (a) Ali je polinom $f(X) = X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$ nerazcepen?
 (b) Pokaži, da nerazcepen polinom $g(X) \in \mathbb{Z}_2[X]$ ne more imeti ničelnega odvoda.
 (c) Poišči stopnjo razširitve $[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}]$.
 (d) Pokaži, da je razširitev $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \supseteq \mathbb{Q}$ Galoisova.
 (e) Pokaži, da je Galoisova grupa razširitve $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \supseteq \mathbb{Q}$ izomorfna grupi K_4 .

Rešitev. (a) Dani polinom nima ničel. Če bi bil razcepen, bi bil deljiv z edinim nerazcepnim polinomom stopnje 2 nad \mathbb{Z}_2 , torej z $X^2 + X + 1$. Z direktnim računom preverimo, da to ne drži. Torej je podan polinom nerazcepen.

(b) Predpostavimo, da je $g'(X)$ ničelni polinom. Potem je $g(X) = h(X^2)$ za nek polinom $h(X)$. Po 'brucovih sanjah' je potem $g(X) = h(X)^2$ in je zato razcepen.

(b) Iz izreka o primitivnem elementu sledi, da je

$$\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5}).$$

Enostavno je videti, da $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$. Ker je

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) \supseteq \mathbb{Q}(\sqrt{3}) \supseteq \mathbb{Q},$$

hitro sledi, da je

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4.$$

(c) Ker ima \mathbb{Q} karakteristiko 0 in je dana razširitev razpadno polje polinoma $(X^2 - 3)(X^2 - 5)$, trditev sledi.

(d) Ker je razširitev Galoisova, je moč Galoisove grupe enaka stopnji razširitve, torej 4. Po drugi strani, ker sta $\pm\sqrt{3}$ ničli polinoma $X^2 - 3$ z racionalnimi koeficienti, je $\varphi(\sqrt{3}) = \pm\sqrt{3}$ za poljuben avtomorfizem φ iz Galoisove grupe. Podobno tudi $\varphi(\sqrt{5}) = \pm\sqrt{5}$. Torej imamo kvečjemu 4 avtomorfizme. Zato imamo natanko 4 avtomorfizme. Ker ima vsak netrivialen avtomorfizem red 2, je grupa izomorfna K_4 .

3.5 2. izpit - 20.8.2025

1. (a) Ali je grupa \mathbb{Z} izomorfna direktni vsoti dveh svojih netrivialnih podgrup?
- (b) Pokaži, da grupa \mathbb{Q} ni končno generirana.
- (c) Preveri, da je s predpisom $\varphi(s, t) = (s, (s + t)(\text{mod } 2))$ podana preslikava $\varphi: \mathbb{Z} \oplus \mathbb{Z}_2 \rightarrow \mathbb{Z} \oplus \mathbb{Z}_2$ avtomorfizem grupe $\mathbb{Z} \oplus \mathbb{Z}_2$.
- (d) Pokaži, da je $\text{Aut}(\mathbb{Z} \oplus \mathbb{Z}_2) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Rešitev. (a) Vsaka netrivialna podgrupa grupe \mathbb{Z} ima obliko $n\mathbb{Z}$ za nek $n \in \mathbb{N}$. Zato \mathbb{Z} nima dveh podgrup s trivialnim presekom, saj $nm \in n\mathbb{Z} \cap m\mathbb{Z}$ in tako ne more biti direktna vsota dveh svojih netrivialnih podgrup.

(b) Vsaka končna podmnožica $\{s_1/t_1, \dots, s_n/t_n\} \subseteq \mathbb{Q}$, kjer so ulomki okrajšani, generira grupo, katere elemente imajo imenovalce, ki ne presegajo $t_1 \cdot \dots \cdot t_n$.

(c) Preverimo injektivnost, surjektivnost in homomorfnost preslikave. Na primer,

$$\begin{aligned} \varphi((s, t) + (p, q)) &= \varphi(s + p, t + q) = (s + p, s + p + t + q(\text{mod } 2)) \\ &= \varphi((s, t)) + \varphi((p, q)). \end{aligned}$$

(d) Označimo $a = (1, 0)$ in $b = (0, 1)$. Naj bo $\varphi: \mathbb{Z} \oplus \mathbb{Z}_2 \rightarrow \mathbb{Z} \oplus \mathbb{Z}_2$ avtomorfizem. Ker je b edini element reda 2, velja $\varphi(b) = b$. Naj bo $\varphi(a) = (s, t)$. Potem je prva koordinata vsakega elementa v sliki φ deljiva s s , zato mora biti $s = \pm 1$, od kod sledi, da je $\varphi(a) = (1, 0)$ ali $\varphi(a) = (-1, 0)$ ali $\varphi(a) = (1, 1)$ ali $\varphi(a) = (-1, 1)$. V prvem primeru dobimo identični avtomorfizem. V drugem primeru je $\varphi(s, t) = (-s, t)$. V tretjem primeru imamo

$$\varphi(s, t) = (s, (s + t)(\text{mod } 2)),$$

v zadnjem primeru pa

$$\varphi(s, t) = (-s, (-s + t)(\text{mod } 2)).$$

Enostavno je videti, da vsak predpis definira avtomorfizem. Poleg tega, ima vsak netrivialni avtomorfizem red 2.

2. Naj bo $K = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}$ kolobar zgoraj trikotnih matrik nad \mathbb{Z} .

(a) Pokaži, da sta

$$I = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in K : a = c = 0 \right\}$$

in

$$J = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in K : c \text{ je sodo število} \right\}$$

ideala kolobarja K .

(b) Pokaži, da $K/I \simeq \mathbb{Z} \times \mathbb{Z}$.

(c) Kateremu znanemu kolobarju je izomorfen kolobar K/J ?

(d) Poišči taka ideala L in M kolobarja K , da je $|K/L| = |K/M| = 4$ ampak $K/L \not\cong K/M$.

(e) Naj bo N poljuben ideal kolobarja K z lastnostjo, da je kvocientni kolobar K/N komutativen. Pokaži, da je $I \subseteq N$ (kjer je I ideal iz točke (a)).

Rešitev. (a) Preverimo z direktnim računom.

(b) S predpisom

$$f \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = (a, c)$$

definirana preslikava $f: K \rightarrow \mathbb{Z} \times \mathbb{Z}$ je epimorfizem kolobarjev z jedrom I .

(c) S predpisom

$$g \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = c \pmod{2}$$

definirana preslikava $f: K \rightarrow \mathbb{Z}_2$ je epimorfizem kolobarjev z jedrom J .

(d) Definirajmo

$$L = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in K : a, c \in 2\mathbb{Z} \right\}$$

in

$$J = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in K : c \in 4\mathbb{Z} \right\}.$$

Potem je $K/L \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ in $K/M \simeq \mathbb{Z}_4$.

(e) Naj bosta $A, B \in K$ poljubni matriki. Ker $A + N$ in $B + N$ komutirata v K/N , je $AB + N = BA + N$, torej je $AB - BA \in N$. Za matriki

$$A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in K$$

pa velja, da je $AB - BA = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$. Zato je

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \in N$$

za vsak $a \in \mathbb{Z}$. Sledi, da je $I \subseteq N$.

3. Naj bo $a = \sqrt{2 + \sqrt{2}}$.

- (a) Poišči stopnjo razširitve $[\mathbb{Q}(a) : \mathbb{Q}]$ in minimalni polinom elementa a nad \mathbb{Q} .
- (b) Poišči stopnjo razširitve $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})]$ in minimalni polinom elementa a nad $\mathbb{Q}(\sqrt{2})$.
- (c) Označimo $b = \sqrt{2 - \sqrt{2}}$. Pokaži, da $b \in \mathbb{Q}(a)$.
- (d) Pokaži, da je razširitev $\mathbb{Q}(a) \supseteq \mathbb{Q}$ Galoisova.
Namig. Poišči vse ničle minimalnega polinoma elementa a in uporabi rezultat prejšnje točke.
- (e) Naj $\sigma \in \text{Gal}(\mathbb{Q}(a))$ zadošča $\sigma(a) = b$. Pokaži, da ima σ red 4 in sklepaj, da je $\text{Gal}(\mathbb{Q}(a)) \simeq \mathbb{Z}_4$.

Rešitev. (a) Ker je $a^2 - 2 = \sqrt{2}$, je $(a^2 - 2)^2 - 2 = 0$, torej je a ničla polinoma $p(X) = X^4 - 4X^2 + 2$. Ker je ta polinom po Eisensteinovem kriteriju za $p = 2$ nerazcepen, je minimalni polinom za a . Sledi, da je $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

(b) Najprej opazimo, da je $\sqrt{2} = a^2 - 2 \in \mathbb{Q}(a)$, torej

$$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(a).$$

Zapišemo verigo razširitev:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(a).$$

Ker ima prva razširitev stopnjo 2, z upoštevanjem prejšnje točke sledi, da je

$$[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})] = 2.$$

Polinom

$$X^2 - (2 + \sqrt{2}) \in \mathbb{Q}(\sqrt{2})[X]$$

je torej iskani minimalni polinom.

(c) Opazimo, da je

$$\frac{1}{a} = \frac{1}{\sqrt{2 + \sqrt{2}}} \cdot \frac{\sqrt{2 - \sqrt{2}}}{\sqrt{2 - \sqrt{2}}} = \frac{b}{\sqrt{2}}.$$

Zato je

$$b = \frac{\sqrt{2}}{a} \in \mathbb{Q}(a).$$

(d) Označimo $t = X^2$ in dobimo $t^2 - 4t + 2 = 0$, torej je $t = 2 \pm \sqrt{2}$. Zato so $\pm a$, $\pm b$ vse ničle $p(X)$. Sledi, da je $\mathbb{Q}(a)$ razpadno polje polinoma $p(X)$ in je zato razširitev Galoisova.

(e) Ker Galoisova grupa deluje na ničlah $p(X)$ tranzitivno, obstaja $\sigma \in \text{Gal}(\mathbb{Q}(a))$, da velja $\sigma(a) = b$. Potem je $\sigma(a^2) = b^2$, torej je

$$\sigma(2 + \sqrt{2}) = 2 - \sqrt{2}.$$

Ker je $\sigma(2) = 2$, sledi, da je

$$\sigma(\sqrt{2}) = -\sqrt{2}.$$

Z upoštevanjem enakosti $b = \frac{\sqrt{2}}{a}$, imamo $\sigma(b) = \frac{-\sqrt{2}}{b} = -a$. Torej

$$\sigma(\sigma(a)) = \sigma(b) = -a.$$

Sledi, da σ^2 ne deluje identično. Ker ima $\text{Gal}(\mathbb{Q}(a))$ red 4, iz Lagrangeovega izreka sledi, da ima σ red 4.

3.6 3. izpit - 5.9.2025

1. (a) Za vsako od naslednjih množic določi, ali je kolobar in ali je polje glede na običajne operacije s števili:

(i) $A_1 = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$,

(ii) $A_2 = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$,

- (iii) $A_3 = \{a \in \mathbb{Z} : a \geq 0\}$.
- (b) Pokaži, da polje nima deliteljev ničā.
- (c) Pokaži, da je karakteristika končnega polja različna od 0.
- (d) Pokaži, da kolobar \mathbb{Z} nima strukture algebre nad nobenim poljem.

Rešitev. (a) A_1 - kolobar, ker je zaprta za operaciji in vsebuje 1, ni polje, ker element 2 nima inverza, A_2 - polje, A_3 - ni kolobar, saj ni grupa glede na seštevanje, npr. 1 nima nasprotnega elementa.

(b) Obrnljiv element ne more biti delitelj ničā: če $ab = 0$ kjer sta a in b neničelna, je $b = a^{-1}(ab) = 0$, kar je nemogoče (element a^{-1} pa obstaja, ker je v polju vsak neničelni element obrnljiv).

(c) Če je karakteristika enaka 0, so elementi $1, 1 + 1, 1 + 1 + 1, \dots$ paroma različni. Zato je polje neskončno.

(d) Predpostavimo, da ima \mathbb{Z} strukturo algebre nad poljem F . Označimo 0_F in 1_F ničelni element in enoto polja F . Če ima F karakteristiko 2, je $0 = (1_F + 1_F) \cdot 1 = 1_F \cdot 1 + 1_F \cdot 1 = 1 + 1 = 2 \in \mathbb{Z}$, kar ne drži. Če ima F karakteristiko različno od 2, spet zapišemo $2 = 1 + 1 = 1_F \cdot 1 + 1_F \cdot 1 = (1_F + 1_F) \cdot 1$. Ker je element $\alpha = 1_F + 1_F \in F$ neničelni, je obrnljiv v F . Zato je $\alpha^{-1} \cdot 2 = 1$, torej $(\alpha^{-1} \cdot 1) \cdot 2 = 1$. Sledi, da je 2 obrnljiv element v naši algebri, kar je protislovje s tem, da sta le ± 1 obrnljiva elementa v \mathbb{Z} .

- 2.** (a) Koliko je (do izomorfizma natančno) abelovih grup reda 400?
- (b) Koliko je abelovih grup reda 400, v katerih je red vsakega elementa največ 50?
- (c) Pokaži, da grupa reda 175 ne more biti enostavna.
- (d) Pokaži, da je vsaka grupa reda 175 abelova.
- (e) Koliko 2-podgrup Sylowa ima grupa S_4 ?

Rešitev. (a) Ker je $400 = 2^4 \cdot 5^2$, je vsaka taka podgrupa direktna vsota $H \oplus K$, kjer je H 2-grupa in K 5-grupa. Ker je $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$ in $2 = 1 + 1$, imamo $5 \cdot 2 = 10$ takih grup.

(b) Red elementa $(a, b) \in H \oplus K$, kjer je H 2-grupa in K 5-grupa, je enak $\text{red}(a) \cdot \text{red}(b)$. Če je $H = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, lahko vzamemo $K = \mathbb{Z}_{25}$ ali $K = \mathbb{Z}_5 \oplus \mathbb{Z}_5$. Če je pa $H = \mathbb{Z}_4 \oplus \mathbb{Z}_4$, $H = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, ali $H = \mathbb{Z}_8 \oplus \mathbb{Z}_2$, je nujno $K = \mathbb{Z}_5 \oplus \mathbb{Z}_5$. Imamo torej 5 takšnih grup.

(c) Imamo razcep $175 = 5^2 \cdot 7$. Enostavno je videti, da je 5-podgrupa Sylowa ena sama in je tako edinka, zato grupa ne more biti enostavna.

(d) Obstaja podgrupa reda 7, ki je abelova in ima trivialni presek z grupo reda 25, ki je tudi abelova kot grupa reda p^2 . Direktni produkt teh dveh grup ima red 175, zato sovпада z celotno grupo. Dana grupa je potem abelova kot direktni produkt dveh abelovih grup.

(e) Ker je $24 = 2^3 \cdot 3$, je 2-podgrupa Sylowa reda 8. Število teh podgrup deli 3 in je liho, torej je 1 ali 3. Grupa S_4 vsebuje kopijo grupe D_8 , ki ima 2 cikla dolžine 4. Ker ima S_4 6 ciklov dolžine 4 in so 2-podgrupe Sylowa konjugirane, imamo 3 2-podgrupe Sylowa.

3. (a) Naj bo $f(X) = X^2 + 1 \in \mathbb{Z}_3[X]$.

(i) Naj bo a ničla polinoma $f(X)$ v neki razširitvi polja \mathbb{Z}_3 . Izračunaj $[\mathbb{Z}_3(a) : \mathbb{Z}_3]$.

(ii) Zapiši bazo $\mathbb{Z}_3(a)$ nad \mathbb{Z}_3 in izrazi element $\frac{a^3+a+1}{a^2}$ preko izbrane baze.

(b) Pokaži, da $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

(c) Poišči stopnjo razširitve $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$.

(d) Naj bo $c \in \mathbb{C}$ tak, da je $[\mathbb{Q}(c) : \mathbb{Q}] = 4$. Pokaži, da je stopnja $[\mathbb{Q}(c^2) : \mathbb{Q}]$ lahko enaka le 2 ali 4. Ali sta obe te možnosti realizirani?

Rešitev. (a) (i) Ker je $f(X)$ nerazcepen nad \mathbb{Z}_3 (ker nima ničel), je minimalni polinom elementa a , zato je $[\mathbb{Z}_3(a) : \mathbb{Z}_3] = 2$. (ii) Baza je $1, a$. Ker je $a^2 = -1 = 2$, je

$$a^2 \cdot 2 = 2 \cdot 2 = 1 \quad \implies \quad \frac{1}{a^2} = 2.$$

Zato je iskani element enak $2(a^3 + a + 1) = 2(2a + a + 1) = 2$.

(b) Če bi imeli $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, bi lahko zapisali $\sqrt{3} = \alpha + \beta\sqrt{2}$ za $\alpha, \beta \in \mathbb{Q}$. Če $\beta = 0$, bi bilo $\sqrt{3} \in \mathbb{Q}$, kar ne drži. Če $\alpha = 0$, enakost pomnožimo s $\sqrt{2}$ in dobimo $\sqrt{6} = 2\beta \in \mathbb{Q}$, kar spet ne drži. Če $\alpha, \beta \neq 0$, enakost kvadriramo in pridemo do zaključka, da $\sqrt{2} \in \mathbb{Q}$, kar spet seveda ne drži.

(c) Naj bo $a = \sqrt{2} + \sqrt{3}$. Najprej opazimo, da je $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (bodisi direktno, bodisi s pomočjo izreka o primitivnem elementu). Ker je $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ in polinom $X^2 - 3$ uniči $\sqrt{3}$, z upoštevanjem prejšnje točke sledi, da je iskana stopnja enaka 2.

(d) Ker $c^2 \in \mathbb{Q}(c)$, je

$$\mathbb{Q} \subseteq \mathbb{Q}(c^2) \subseteq \mathbb{Q}(c).$$

Zato $[\mathbb{Q}(c^2) : \mathbb{Q}]$ deli $[\mathbb{Q}(c) : \mathbb{Q}] = 4$. Če bi bila ta stopnja enaka 1, bi imeli $c^2 \in \mathbb{Q}$, in bi potem polinom $f(X) = X^2 - c^2 \in \mathbb{Q}[X]$ druge stopnje uničil c , v nasprotju s $[\mathbb{Q}(c) : \mathbb{Q}] = 4$. Sledi, da je stopnja

$$[\mathbb{Q}(c^2) : \mathbb{Q}]$$

enaka 2 ali 4. Če vzamemo $c = \sqrt[4]{2}$, je $X^4 - 2$ minimalni polinom za c in je $c^2 = \sqrt{2}$. Zato je

$$[\mathbb{Q}(c) : \mathbb{Q}] = 4 \quad \text{in} \quad [\mathbb{Q}(c^2) : \mathbb{Q}] = 2.$$

Sedaj si oglejmo polinom $h(X) = X^4 + 2X + 2$, ki je nerazcepen nad \mathbb{Q} po Eisensteinovem kriteriju za $p = 2$. Za ničlo c tega polinoma velja $[\mathbb{Q}(c) : \mathbb{Q}] = 4$. Ker $(c^2)^2 + 2c + 2 = 0$, je $c \in \mathbb{Q}(c^2)$. Sledi enakost $\mathbb{Q}(c) = \mathbb{Q}(c^2)$. Zato je

$$[\mathbb{Q}(c) : \mathbb{Q}] = [\mathbb{Q}(c^2) : \mathbb{Q}] = 4.$$

Literatura

- [1] M. Brešar, *Uvod v Algebro*, Ljubljana, DMFA - založništvo, 2018.
- [2] M. Brešar, *Undergraduate algebra, A Unified approach*, Springer Undergraduate Mathematics Series, Springer, Cham, 2019.
- [3] A. I. Kostrikin (Ed.), *Exercises in Algebra: A Collection of Exercises in Algebra, Linear Algebra and Geometry*, Gordon and Breach Publishers, 1996.