Razni zadaci

Obavezno pogledati sve iskucane zadatke, koji pokrivaju mnogo detaljnije sve oblasti koje smo prešli do sad.

Definicija ($Hom(G,H)$)

Neka su G i H dvije date grupe. Definišimo skup $Hom(G,H)$ kao skup svih homomorfizama iz grupe G u grupu H.

Može se
Nije teško dokazati da ako su G i H abelove grupe tada skup $Hom(G,H)$ je također Abelova grupa u odnosu na operaciju sabiranja koja je definisana sa

$$(h+k)(a) = h(a) + k(a) \quad \forall a \in G \quad \forall h,k \in Hom(G,H).$$

(#) Odrediti sve homomorfizme iz grupe $(\mathbb{Z}, +)$ u grupu $(\mathbb{Q}, +)$.

R:) Prisjetimo se: Preslikavanje $\phi: G \to H$ iz grupe G u grupu H nazivamo homomorfizam akko

$$\phi(xy) = \phi(x)\,\phi(y) \quad \text{za } \forall x, y \in G.$$

Iz definicije vidimo da homomorfizam preslikava jedinicu u jedinicu i inverz u inverz.

$\mathbb{Z}$ je ciklična grupa, i mi imamo operaciju sabiranja

$$\mathbb{Z} = \langle 1 \rangle \Rightarrow \forall n \in \mathbb{Z} \Rightarrow n = \underbrace{1+1+\ldots+1}_{n \text{ puta}}$$

Promatrajmo proizvoljan homomorfizam $\phi: \mathbb{Z} \to \mathbb{Q}$ za koji je $\phi(1) = q$ $(q \in \mathbb{Q})$.

Primjetimo da

$$\phi(n) = \phi(\underbrace{1+1+\ldots+1}_{n \text{ puta}}) = \underbrace{\phi(1)}_{=q} + \underbrace{\phi(1)}_{=q} + \ldots + \underbrace{\phi(1)}_{=q} = nq$$

(ovo znači da je $\phi(n) = nq$ funkcija)

$$\phi(m) = \phi(\underbrace{1+\ldots+1}_{m \text{ puta}}) = \underbrace{\phi(1)+\ldots+\phi(1)}_{m \text{ puta}} = mq$$

$q(m+n)$

$$\Rightarrow \phi(m+n) = \phi(m) + \phi(n) \quad \forall m, n \in \mathbb{Q}$$

$\phi(m)$ → qm, $\phi(n)$ → qn

Odavde vidimo da nije bitno koji racionalni broj $q \in \mathbb{Q}$ izberemo, Homomorfizama iz grupe $\mathbb{Z}$ u grupu $\mathbb{Q}$ ima onoliko koliko ima racionalnih brojeva ili $\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}$.

Ako grupu $\mathbb{Q}$ zamijenimo nekom drugom grupom H, imamo da

$$\mathrm{Hom}(\mathbb{Z}, H) \cong H$$

(#) Odrediti sve homomorfizme iz grupe $(\mathbb{Q},+)$ u grupu $(\mathbb{Z},+)$.

Rj: U jednom od prethodnih zadataka smo pokazali da grupa $\mathbb{Q}$ nije ciklička grupa. Pokazaćemo da postoji samo jedan homomorfizam iz $\mathbb{Q}$ u $\mathbb{Z}$.

Posmatrajmo proizvoljan homomorfizam $\phi:\mathbb{Q}\to\mathbb{Z}$ i neka je $\phi(1)=m$. Posmatrajmo sad $\phi(\frac{1}{n})$ za neki $n\in\mathbb{N}$.

$$m=\phi(1)=\phi(\underbrace{\tfrac{1}{n}+\tfrac{1}{n}+\dots+\tfrac{1}{n}}_{n\text{ puta}})=n\,\phi(\tfrac{1}{n})$$

$$\Rightarrow \quad m=n\,\phi(\tfrac{1}{n})$$

Odavde slijedi da je cijeli broj m $(m=\phi(1))$ djeljiv sa n za svaki prirodan broj n. To je moguće samo ako je $m=0$, tačnije ako je $\phi(q)=0\ \ \forall q\in\mathbb{Q}$.

Možemo zaključiti

$$\mathrm{Hom}(\mathbb{Q},\mathbb{Z})\cong\{0\}.$$

(#) Odrediti sve homomorfizme iz grupe $(\mathbb{Z}_n, +)$ u grupu $(\mathbb{Z}, +)$.

Rj:

$(\mathbb{Z}_n, +)$ je ciklička grupa, $\mathbb{Z}_n = \langle 1 \rangle$. Ovo znači da je svaki homomorfizam precizno određen sa slikom elementa 1.

Pa neka je $\phi: \mathbb{Z}_n \to \mathbb{Z}$ proizvoljan homomorfizam za koji vrijedi $\phi(1) = m$.

0 je neutralni element pa je $\phi(0) = 0$. S druge strane

$$\phi(\underbrace{1+1+\ldots+1}_{\substack{n \text{ sabiraka} \\ \text{u } \mathbb{Z}_n}}) = \phi(0) = 0$$

$$\phi(\underbrace{1+1+\ldots+1}_{n \text{ sabiraka}}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n \text{ sabiraka}} = nm$$

Time smo dobili da je $nm = 0$ za neki prirodan broj $n \in \mathbb{N}$. Ovo znači da m mora biti $= 0$.

Pa ako je $\phi(1) = 0$ postoji samo jedan homomorfizam tj. $\phi(k) = 0 \ \forall k \in \mathbb{Z}_n$. Prema tome

$$\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}) \cong \{0\}.$$

(#) Odrediti sve homomorfizme iz grupe $(\mathbb{Z}_n, +)$ u grupu $(U, \cdot)$, gdje je $U = \{z \in \mathbb{C} : |z| = 1\}$.

Rj.

Jedinica grupe U je 1. Neutralni element grupe $\mathbb{Z}_n$ je 0. Iskoristićemo osobinu da je $\mathbb{Z}_n$ ciklička grupa i da je $\mathbb{Z}_n = \langle 1 \rangle$.

Neka je $\phi: \mathbb{Z}_n \to U$ proizvoljan homomorfizam za koji vrijedi da je $\phi(1) = w$. Prema pretpostavci $|w| = 1$.

Imamo

$$\phi(0) = 1$$

$$\phi(0) = \phi(\underbrace{1+1+\ldots+1}_{\text{n sabiraka u } \mathbb{Z}_n}) = \underbrace{\phi(1)\,\phi(1)\cdot\ldots\cdot\phi(1)}_{\text{n puta}} = \left(\phi(1)\right)^n = w^n$$

Ovo povlači da je $w^n = 1$.

Ovo povlači da homomorfizama iz $\mathbb{Z}_n$ u grupu U postoji onoliko, koliko je n-tih korijena jedinice. Korijena broja 1 postoji n, i oni su jednaki $w_k = e^{\frac{i2k\pi}{n}}$ za $k = 0, 1, \ldots, n-1$.

Homomorfizam koji pripada korijenu w_k je $\phi_k: \mathbb{Z}_n \to U$

$$\phi_k(m) = w_k^m = e^{\frac{i2k\pi m}{n}} \quad \text{za } m \in \mathbb{Z}_n.$$

Time vrijedi i

$$\mathrm{Hom}(\mathbb{Z}_n, U) \cong \mathbb{Z}_n.$$

(#) Odrediti sve homomorfizme iz grupe $\mathbb{Z}_8$ u grupu S_3.

Rj.

$\mathbb{Z}_8$ je ciklička grupa, $\langle 1 \rangle = \mathbb{Z}_8$.

Neutralni element za $\mathbb{Z}_8$ je 0, a neutralni element za S_3 je id ($id = (12)(12)$).

Neka je $\phi: \mathbb{Z}_8 \to S_3$ proizvoljan homomorfizam, za koji vrijedi da je $\phi(1) = a$. (Jasno je da $a \in S_3$).

Imamo

$$\phi(0) = id$$

$$\phi(0) = \phi(\underbrace{1+1+\ldots+1}_{8 \text{ sumanda}}) = \phi(1) \cdot \phi(1) \cdot \ldots \cdot \phi(1) = a^8$$

Ovo znači da je $a^8 = id \Rightarrow$ a mogu biti oni elementi a iz grupe S_3 za osobinom da je $a^8 = id$.

Drugim riječima red elementa a treba da dijeli broj 8.

Imamo četiri mogućnosti

$$\phi(1) = (1)(2)(3) = id$$
$$\phi(1) = (12)$$
$$\phi(1) = (13)$$
$$\phi(1) = (23)$$

Postoje četiri homomorfizma iz grupe $\mathbb{Z}_8$ u grupu S_3 i oni su oblika $\phi: \mathbb{Z}_8 \to S_3$

$$k \to a^k$$

gdje je $a \in \{id, (12), (13), (23)\}$.

(#) Odrediti sve homomorfizme iz grupe $\mathbb{Z}_4$ u grupu $\mathbb{Z}_3$.

Rj: $\mathbb{Z}_4 = \{0,1,2,3\}$, $\mathbb{Z}_4$ ciklička grupa, $\mathbb{Z}_4 = \langle 1 \rangle$.

Neka je $\phi: \mathbb{Z}_4 \to \mathbb{Z}_3$ proizvoljan homomorfizam iz $\mathbb{Z}_4$ u $\mathbb{Z}_3$ i neka je $\phi(1) = a$.

Iz definicije homomorfizma znamo da se neutralni element slika u neutralni element (i invert u invert), pa je

$$\phi(0) = 0 \qquad \ldots(1)$$

S druge strane

$$\phi(0) = \phi(1+1+1+1) = \phi(1)+\phi(1)+\phi(1)+\phi(1)$$
$$= 4\phi(1) = 4a \qquad \ldots(2)$$

Na osnovu (1) i (2) $4a = 0$ u grupi $\mathbb{Z}_3 = \{0,1,2\}$

Kako je

$1+1+1+1 = 1$ u $\mathbb{Z}_3$ i $2+2+2+2 = 2$ u $\mathbb{Z}_3$ to a mora biti 0. Drugim riječima $\phi(1) = 0$.

Postoji samo jedan homomorfizam iz grupe $\mathbb{Z}_4$ u grupu $\mathbb{Z}_3$ i to je

$$\phi: \mathbb{Z}_4 \to \mathbb{Z}_3$$
$$k \to 0$$

(#) Pokazati da za proizvoljni $l \in U(n)$, f-ja $\phi: \mathbb{Z}_n \to \mathbb{Z}_n$ definisana sa $\phi(x) = xl \pmod n$ je automorfizam grupe $\mathbb{Z}_n$.

Rj: $l \in U(n) \Rightarrow \gcd(n, l) = 1$, $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$, operacija je $+$.

ϕ JE INJEKCIJA

Neka su $x, y \in \mathbb{Z}_n$ t.d. $\phi(x) = \phi(y)$. Tada

$$xl \pmod n = yl \pmod n$$

$$\left(xl \pmod n - yl \pmod n\right) \bmod n = 0$$

Teorem o ostatku:
$m \in \mathbb{Z}$, $n \in \mathbb{Z}^+$ $\exists! q \in \mathbb{Z}$, $r \in \mathbb{Z}^+$
$m = nq + r$, $r \in \{0, 1, \dots, n-1\}$

Prisjetimo se da ako je $a \bmod n = a'$ i $b \bmod n = b'$ tada je $(a+b) \bmod n = (a' + b') \bmod n$

$$xl - yl \pmod n = 0$$

$$(x-y)l \pmod n = 0$$

$\Updownarrow \gcd(l, n) = 1$

$$x - y \pmod n = 0$$

$$\left((x \bmod n) + (-y \bmod n)\right) \bmod n = 0$$

$$x \pmod n = y \pmod n \overset{x,y \in \mathbb{Z}_n}{\Rightarrow} x = y$$

$xl = nq_1 + r_1$, $r_1 = r_2$
$yl = nq_2 + r_2$

$xl - nq_1 = yl - nq_2$

$xl - yl = n(q_1 - q_2)$

$(x-y)l = nq$

ϕ je injekcija

ϕ JE SURJEKCIJA

Izaberimo proizvoljan $y \in \mathbb{Z}_n$ i pokažimo da postoji $x \in \mathbb{Z}_n$ t.d. $\phi(x) = y$.

Kako je $\gcd(n, l) = 1$ to $\exists s, t \in \mathbb{Z}$ t.d. $sn + tl = 1$.

Neka je $x = ty$,

$\Rightarrow sny + tly = y \dots (1)$

$\phi(x) = \phi(ty) = lty \pmod n$

$(1) \Rightarrow lty = -sny + y = (-sy)n + y = qn + y$

$lty = qn + y,\ q \in \mathbb{Z},\ y \in \mathbb{Z}_n \Rightarrow lty \pmod n = y$

Prema tome $\phi(x) = y$.

Primjetimo da smo za x izabrali ty. Međutim ne znamo da li je $ty \in \mathbb{Z}_n$.

U slučaju da $ty \notin \mathbb{Z}_n$ bude $\exists!\, \tilde{q}, r$ t.d. $ty = \tilde{q}n + r$, $r \in \mathbb{Z}_n$.

Ali sad $\phi(r) = lr \pmod n$

$$ty = \tilde{q}n + r \Rightarrow lr = lty - l\tilde{q}n = \left| lty = qn + y \right| =$$

$$= qn + y - l\tilde{q}n = (q - l\tilde{q})n + y$$

Drugim riječima $lr \pmod n = y$

ϕ JE HOMOMORFIZAM

$$\phi(x+y) = (x+y) \pmod n = \left| \begin{matrix} x \bmod n = x' \\ y \bmod n = y' \end{matrix} \right\} \Rightarrow (x'+y') \bmod n = (x+y) \bmod n \Big|$$

$$= \Big((x \bmod n) + (y \bmod n) \Big) \bmod n = \phi(x) + \phi(y).$$

Data fja ϕ jest automorfizam grupe $\mathbb{Z}_n$.

Polgrupe in grupe

(1) Razišči strukturo naslednjih grupoidov:

(a) $S = \mathbb{R}$ za operacijo $x \circ y = x + y + xy$,

(b) $S = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \;\middle|\; x \in \mathbb{R} \right\}$ za operacijo množenje matrik,

(c) $S = \mathbb{R}^3$ za operacijo vektorski produkt,

(d) $S = \mathbb{R}$ za operaciji $a *_L b = a$ in $a *_R b = b$,

(e) $S = \{1, 2, 3, 4, 5\}$ za operacijo, ki je podana s tabelo

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	5	3
3	3	5	4	2	1
4	4	1	5	3	2
5	5	3	2	1	4

.

Rešitev: Pri tej nalogi bomo študirali različne lastnosti binarnih operacij. Najprej začnimo z nekaj terminologije:

- *Grupoid* S je množica z binarno operacijo $\circ : S \times S \to S$.
- *Polgrupa* je grupoid z asociativno operacijo. To pomeni, da velja

$$(a \circ b) \circ c = a \circ (b \circ c)$$

za vsako trojico $a, b, c \in S$.

- *Enota* grupoida S je tak element $e \in S$, da velja

$$e \circ a = a \circ e = a$$

za vsak $a \in S$. Če velja samo $e \circ a = a$ ali pa samo $a \circ e = a$ za vsak $a \in S$, rečemo, da je e leva oziroma desna enota. Če ima grupoid vsaj eno levo in vsaj eno desno enoto, sta enaki in sta avtomatično enota grupoida.

- *Monoid* je polgrupa z enoto.
- Če ima grupoid S enoto e, je *inverz* elementa $a \in S$ tak element $x \in S$, da velja

$$x \circ a = a \circ x = e.$$

Inverz elementa a označimo z a^{-1}. Če velja samo $x \circ a = e$ ali pa $a \circ x = e$, rečemo elementu x levi oziroma desni inverz elementa a. Če ima element a iz neke polgrupe levi in desni inverz, sta ta inverza enaka. V grupoidu to ni nujno res.

· *Grupa* je monoid, v katerem ima vsak element inverz.

· Grupoid S je *komutativen*, če velja

$$a \circ b = b \circ a$$

za vsak par $a, b \in S$.

(a) $S = \mathbb{R}$ za operacijo $x \circ y = x + y + xy$:

- Najprej pokažimo, da je operacija asociativna. To sledi iz enakosti

$$(x \circ y) \circ z = (x + y + xy) \circ z = x + y + xy + z + xz + yz + xyz,$$
$$x \circ (y \circ z) = y \circ (y + z + yz) = x + y + z + yz + xy + xz + xyz.$$

- Število 0 je enota za operacijo $\circ$.
- Operacija je komutativna.
- Inverz x^{-1} elementa $x \in \mathbb{R}$ mora zadoščati pogoju

$$x^{-1} \circ x = x^{-1} + x + x^{-1}x = 0.$$

Od tod lahko izpeljemo, da je

$$x^{-1} = -\frac{x}{1+x},$$

kar pomeni, da so obrnljivi vsi elementi razen $x = -1$.

- Iz vsega navedenega sledi, da je $(S, \circ)$ komutativen monoid. Imamo izomorfizem

$$f : (S, \circ) \to (\mathbb{R}, \cdot),$$
$$x \mapsto x + 1.$$

(b) $S = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \;\middle|\; x \in \mathbb{R} \right\}$ za operacijo množenje matrik:

- Najprej bomo preverili, da je množica S zaprta za množenje. To sledi iz enakosti

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}.$$

- Asociativnost operacije sledi iz asociativnosti matričnega množenja.
- Enota za dano operacijo je matrika $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- Inverz poljubnega elementa je enak

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}.$$

- Dokazali smo, da je $(S, \cdot)$ grupa. Izomorfna je grupi realnih števil za seštevanje. Ekspliciten izomorfizem je podan s predpisom

$$f : (S, \cdot) \to (\mathbb{R}, +),$$
$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mapsto x.$$

(c) $S = \mathbb{R}^3$ za operacijo vektorski produkt:

- Vektorski produkt dveh vektorjev iz $\mathbb{R}^3$ je spet vektor iz $\mathbb{R}^3$, zato je operacija dobro definirana.
- Pri preverjanju asociativnosti vektorskega produkta bomo uporabili formuli za dvojni vektorski produkt:

$$\vec{a} \times (\vec{b} \times \vec{c}) = \vec{b}(\vec{a} \cdot \vec{c}) - \vec{c}(\vec{a} \cdot \vec{b}),$$
$$(\vec{a} \times \vec{b}) \times \vec{c} = \vec{b}(\vec{a} \cdot \vec{c}) - \vec{a}(\vec{b} \cdot \vec{c}).$$

  Ti dve enakosti nam dasta slutiti, da vektorski produkt ni asociativna operacija. Konkretno lahko to vidimo na primeru:

$$\vec{i} \times (\vec{i} \times \vec{j}) = \vec{i} \times \vec{k} = -\vec{j},$$
$$(\vec{i} \times \vec{i}) \times \vec{j} = 0 \times \vec{j} = 0.$$

- Ker je vektorski produkt dveh vektorjev pravokoten na oba vektorja, ta operacija nima enote.
- Glede na našo definicijo je torej $(\mathbb{R}^3, \times)$ le grupoid. Je pa kljub temu vektorski produkt primer zelo razširjene algebraične strukture, ki se ji reče Liejeva algebra.

(d) $S = \mathbb{R}$ za operaciji $a *_L b = a$ in $a *_R b = b$:

- Vzemimo najprej operacijo $*_L$. Asociativnost te operacije sledi iz enakosti

$$a *_L (b *_L c) = a *_L b = a,$$
$$(a *_L b) *_L c = a *_L c = a.$$

  Analogno lahko pokažemo, da je tudi operacija $*_R$ asociativna.
- Operacija $*_L$ nima niti enote niti nobene leve enote. Je pa vsak element $x \in \mathbb{R}$ desna enota. Podobno operacija $*_R$ nima nobene desne enote, je pa vsak element leva enota.
- Množica $\mathbb{R}$ je za obe operaciji polgrupa.

(e) $S = \{1, 2, 3, 4, 5\}$ za operacijo, ki je podana s tabelo:

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	5	3
3	3	5	4	2	1
4	4	1	5	3	2
5	5	3	2	1	4

.

- Preverjanje asociativnosti operacije, ki je podana s tabelo je včasih časovno zelo zahtevno. Lažje pa je dokazati, da operacija ni asociativna, če najdemo protiprimer. V našem primeru je

$$2 \circ (2 \circ 3) = 2 \circ 1 = 2,$$
$$(2 \circ 2) \circ 3 = 4 \circ 3 = 5,$$

  kar pomeni, da dana operacija ni asociativna.

- Operacija $\circ$ ima enoto 1.
- Vsak element S ima tako levi kot desni inverz, ki pa nista vedno enaka, kot kaže primer $4 \circ 2 = 2 \circ 3 = 1$.
- Grupoidu z enoto, v katerem ima vsak element levi in desni inverz, rečemo zanka. Če je operacija asociativna, sta oba inverza avtomatično enaka, ta primer pa kaže, da pri neasociativni operaciji to ni več nujno res.

□

(2) Dokaži, da sta naslednji množici z danima operacijama grupi:

(a) $S = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \,\middle|\, x, y \in \mathbb{R},\, x \neq 0 \right\}$ za operacijo množenje matrik,

(b) $S = \left\{ a + b\sqrt{2} \,|\, a, b \in \mathbb{Q},\, (a,b) \neq (0,0) \right\}$ za množenje števil.

Rešitev: (a) $S = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \,\middle|\, x, y \in \mathbb{R},\, x \neq 0 \right\}$ za operacijo množenje matrik:

- Najprej preverimo, da je množica S zaprta za množenje. Velja

$$\begin{bmatrix} x_1 & y_1 \\ 0 & 1 \end{bmatrix} . \begin{bmatrix} x_2 & y_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x_1x_2 & x_1y_2 + y_1 \\ 0 & 1 \end{bmatrix}.$$

  Ker sta x_1 in x_2 neničelna, je tudi x_1x_2 neničelno število, zato je produkt danih matrik tudi matrika iz S.
- Asociativnost operacije sledi iz asociativnosti matričnega množenja.
- Enota za dano operacijo je matrika $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- Inverz poljubnega elementa lahko izračunamo po formuli

$$\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{bmatrix}.$$

(b) $S = \left\{ a + b\sqrt{2} \,|\, a, b \in \mathbb{Q},\, (a,b) \neq (0,0) \right\}$ za množenje števil:

- Produkt dveh števil iz S je enak

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_2b_1 + a_1b_2)\sqrt{2},$$

  kar pomeni, da je množica S zaprta za množenje.
- Asociativnost operacije sledi iz asociativnosti množenja realnih števil.
- Enota za dano operacijo je število 1.
- Inverz števila $a + b\sqrt{2}$ je enak

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

□

(3) Izračunaj rede vseh elementov v grupah $\mathbb{Z}_{20}$, S_3 in S_5.

Rešitev: Red elementa a iz grupe G je najmanjše naravno število n, za katero velja ena izmed enakosti

$$na = 0,$$
$$a^n = e,$$

odvisno od tega, ali pišemo grupno operacijo aditivno ali pa multiplikativno. Če takšen n ne obstaja, rečemo, da ima a neskončen red. Red elementa a označimo z $\mathrm{red}(a)$.

$\underline{\mathbb{Z}_{20}}$:

Elementi ciklične grupe $\mathbb{Z}_{20}$, ki so tuji proti 20 imajo maksimalen možni red 20. Če nek tak element množimo z 2, dobimo element reda 10. Če ga množimo s 4, dobimo element reda 5. Podobno velja tudi za ostale delitelje števila 20. Tako dobimo:

- elementi $1, 3, 7, 9, 11, 13, 17, 19$ imajo red 20,
- elementi $2, 6, 14, 18$ imajo red 10,
- elementi $4, 8, 12, 16$ imajo red 5,
- elementa 5 in 10 imata red 4,
- element 10 ima red 2,
- enota 0 ima red 1.

Bolj splošno imajo redi elementov ciklične grupe $\mathbb{Z}_n$ naslednje lastnosti:

- elementi, ki so tuji proti n, imajo red n. Takih elementov je $\phi(n)$, njihovi večkratniki pa tvorijo celo grupo $\mathbb{Z}_n$. Rečemo jim generatorji grupe $\mathbb{Z}_n$.
- enota 0 ima red 1,
- ostali elementi imajo red, ki zadošča pogoju $1 < \mathrm{red}(a) < n$ in ki deli število n.

$\underline{S_3}$:

Permutacijska grupa S_3 ima šest elementov. Njihovi redi so:

- elementi $(1\,2), (1\,3), (2\,3)$ imajo red 2,
- elementa $(1\,2\,3)$ in $(1\,3\,2)$ imata red 3,
- enota $(1)(2)(3)$ ima red 1.

$\underline{S_5}$:

Permutacijska grupa S_5 ima 120 elementov. Njihovi redi so odvisni samo od ciklične strukture, zato si bomo pogledali vse možne ciklične oblike elementov iz S_5.

- $(1\,2\,3\,4\,5)\ldots$ 5-cikli imajo red 5. Takih elementov je 24.
- $(1\,2\,3\,4)(5)\ldots$ $4+1$-cikli imajo red 4. Takih elementov je 30.
- $(1\,2\,3)(4\,5)\ldots$ $3+2$-cikli imajo red 6. Takih elementov je 20.
- $(1\,2\,3)(4)(5)\ldots$ $3+1+1$-cikli imajo red 3. Takih elementov je 20.
- $(1\,2)(3\,4)(5)\ldots$ $2+2+1$-cikli imajo red 2. Takih elementov je 15.
- $(1\,2)(3)(4)(5)\ldots$ $2+1+1+1$-cikli imajo red 2. Takih elementov je 10.

· $(1)(2)(3)(4)(5)\ldots$ enota ima red 1.

V splošnem je red permutacije enak najmanjšemu skupnemu večkratniku dolžin ciklov, ki nastopajo v dekompoziciji dane permutacije. □

(4) Dana je permutacija $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 5 & 6 & 4 & 8 & 1 \end{pmatrix} \in S_8$. Izračunaj a^{-1}, a^2 in a^{1000}.

Rešitev: Najprej zapišimo permutacijo a kot produkt disjunktnih ciklov

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 5 & 6 & 4 & 8 & 1 \end{pmatrix} = (1\,3\,7\,8)(4\,5\,6).$$

Pri računanju potenc permutacije nam pride prav dejstvo, da disjunktni cikli med sabo komutirajo, zato je dovolj potencirati vsak cikel posebej. Tako dobimo:

$$\begin{aligned} a^{-1} &= (1\,8\,7\,3)(4\,6\,5), \\ a^2 &= (1\,7)(3\,8)(4\,6\,5), \\ a^{1000} &= (4\,5\,6). \end{aligned}$$

□

(5) Poišči vse homomorfizme grup:

(a) $\mathbb{Z} \to \mathbb{Q}$,
(b) $\mathbb{Q} \to \mathbb{Z}$,
(c) $\mathbb{Z}_n \to \mathbb{Z}$,
(d) $\mathbb{Z}_n \to U(1)$.

Rešitev: Naj bosta G in H grupi. Homomorfizem grup $\phi : G \to H$ je preslikava, ki zadošča pogoju

$$\phi(xy) = \phi(x)\phi(y)$$

za vsaka $x, y \in G$. Pri tem moramo na levi vzeti operacijo v G na desni pa operacijo v H. Iz definicije sledi, da homomorfizem grup slika enoto v enoto in inverze v inverze. Če sta grupi G in H komutativni, ponavadi operacijo pišemo aditivno. V tem primeru je homomorfizem grup kar aditivna preslikava, ki po definiciji zadošča pogoju

$$\phi(x + y) = \phi(x) + \phi(y).$$

(a) Homomorfizmi $\mathbb{Z} \to \mathbb{Q}$:

Grupa $\mathbb{Z}$ je ciklična grupa z generatorjem 1, kar pomeni, da je vsak element $\mathbb{Z}$ večkratnik elementa 1. To preprosto dejstvo ima zanimivo posledico. Vsak homomorfizem iz grupe $\mathbb{Z}$ v neko grupo je namreč natanko določen s sliko elementa 1.

Vzemimo torej poljuben homomorfizem $\phi : \mathbb{Z} \to \mathbb{Q}$ in označimo $\phi(1) = q$. Po predpostavki je q racionalno število, pogoj aditivnosti pa nam potem pove, da za poljuben $n \in \mathbb{N}$ velja

$$\phi(n) = \phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n} = nq.$$

Ker homomorfizem slika inverze v inverze, od tod sledi, da velja

$$\phi(m) = mq$$

za poljuben $m \in \mathbb{Z}$. Vidimo, da je homomorfizmov iz $\mathbb{Z}$ v $\mathbb{Q}$ ravno toliko kot je racionalnih števil oziroma

$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}.$$

Podobno velja, če grupo $\mathbb{Q}$ zamenjamo s poljubno grupo H, saj je zmeraj

$$\mathrm{Hom}(\mathbb{Z}, H) \cong H.$$

(b) Homomorfizmi $\mathbb{Q} \to \mathbb{Z}$:

Sedaj iščemo aditivne preslikave iz grupe racionalnih števil v grupo celih števil. Grupa $\mathbb{Q}$ ni generirana z elementom 1, zato ne moremo uporabiti podobnega argumenta kot pri prejšnji nalogi. Videli bomo, da obstaja samo en homomorfizem iz $\mathbb{Q}$ v $\mathbb{Z}$.

Vzemimo poljuben homomorfizem $\phi : \mathbb{Q} \to \mathbb{Z}$ in naj bo $\phi(1) = m$. Poglejmo, kaj nam pogoj aditivnosti pove o vrednosti $\phi\left(\frac{1}{n}\right)$ za nek $n \in \mathbb{N}$. Velja

$$m = \phi(1) = \phi\Big(\underbrace{\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}}_{n}\Big) = n\phi\left(\frac{1}{n}\right).$$

Od tod sledi, da je število m večkratnik vsakega naravnega števila n. To je mogoče le, če je $m = 0$. Od tod pa potem sledi

$$\mathrm{Hom}(\mathbb{Q}, \mathbb{Z}) \cong \{0\}.$$

(c) Homomorfizmi $\mathbb{Z}_n \to \mathbb{Z}$:

Grupa $\mathbb{Z}_n$ je ciklična z generatorjem 1, zato je vsak homomorfizem iz $\mathbb{Z}_n$ v $\mathbb{Z}$ natanko določen s sliko elementa 1.

Naj bo $\phi : \mathbb{Z}_n \to \mathbb{Z}$ poljuben homomorfizem in naj velja $\phi(1) = m$. Ker je v grupi $\mathbb{Z}_n$

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0,$$

mora torej veljati

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \phi(0) = 0.$$

Po drugi strani pa iz aditivnosti sledi

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n} = nm.$$

Ker je po predpostavki n naravno število, mora biti $m = 0$. Torej je spet

$$\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}) \cong \{0\}.$$

(d) Homomorfizmi $\mathbb{Z}_n \to U(1)$:

Grupa $U(1)$ je grupa enotskih kompleksnih števil za množenje

$$U(1) = \{z \in \mathbb{C} \,|\, |z| = 1\}.$$

Enota grupe $U(1)$ je število 1. Pri študiju homomorfizmov iz $\mathbb{Z}_n$ v $U(1)$ bomo zopet uporabili dejstvo, da je 1 generator grupe $\mathbb{Z}_n$.

Izberimo poljuben homomorfizem $\phi : \mathbb{Z}_n \to U(1)$ in označimo $\phi(1) = w$. Po predpostavki je $|w| = 1$. Iz pogoja

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0,$$

tokrat sledi

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = 1.$$

Pogoj aditivnosti pa nam tokrat pove, da je

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \phi(1)^n = w^n.$$

Oboje skupaj nam da pogoj

$$w^n = 1.$$

Homomorfizmov iz $\mathbb{Z}_n$ v $U(1)$ je torej toliko, kot je n-tih korenov enote. Teh pa je ravno n in so enaki

$$w_k = e^{\frac{i2\pi k}{n}}$$

za $k = 0, 1, \ldots, n-1$. Predpis za homomorfizem, ki pripada korenu w_k, je

$$\phi_k(m) = e^{\frac{i2\pi km}{n}}$$

za $m \in \mathbb{Z}_n$. Velja torej

$$\mathrm{Hom}(\mathbb{Z}_n, U(1)) \cong \mathbb{Z}_n.$$

Opomba: Homomorfizmom iz grupe G v grupo $U(1)$ rečemo karakterji. Karakterji igrajo osrednjo vlogo v teorijah Fourierovih vrst, Fourierove transformacije in diskretne Fourierove transformacije. Pri posplošitvi Fourierove teorije na nekomutativne grupe karakterje nadomestimo s homomorfizmi dane grupe v matrične grupe, ki jih imenujemo tudi reprezentacije oziroma upodobitve. □

(6) Poišči vse avtomorfizme grup $\mathbb{Z}, \mathbb{Z}_5$ in $\mathbb{Z}_{10}$.

Rešitev: Avtomorfizem grupe G je bijektivni homomorfizem $\phi : G \to G$.

Avtomorfizmi grupe $\mathbb{Z}$:

Vsak homomorfizem $\phi : \mathbb{Z} \to \mathbb{Z}$ je določen s sliko generatorja 1 grupe $\mathbb{Z}$. Če označimo $\phi(1) = n$, je potem

$$\phi(m) = nm$$

za poljuben $m \in \mathbb{Z}$. V sliki preslikave ϕ so vsa števila, ki so deljiva z n. Če torej hočemo, da bo ϕ bijektivna, mora biti $n = \pm 1$. To pa pomeni, da je

$$\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}, -\mathrm{Id}\}.$$

Avtomorfizmi grupe $\mathbb{Z}_5$:

Grupa $\mathbb{Z}_5$ je ciklična, zato je vsak homomorfizem $\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$ določen s sliko generatorja. Če označimo $\phi(1) = n$, bo ϕ bijektivna preslikava natanko takrat, ko bo

$$n \in \{1, 2, 3, 4\}.$$

Torej je

$$\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_5^*.$$

Avtomorfizmi grupe $\mathbb{Z}_{10}$:

Tudi grupa $\mathbb{Z}_{10}$ je ciklična, zato velja podoben sklep kot zgoraj. Če označimo $\phi(1) = n$, bo tokrat ϕ bijektivna preslikava za

$$n \in \{1, 3, 7, 9\},$$

kar pomeni, da je

$$\mathrm{Aut}(\mathbb{Z}_{10}) \cong \mathbb{Z}_{10}^*.$$

Opomba: V splošnem so avtomorfizmi grupe $\mathbb{Z}_n$ v bijektivni korespondenci z elementi $\mathbb{Z}_n^*$. Elementu $m \in \mathbb{Z}_n^*$ pripada preslikava množenja z m po modulu n. □

~~(7) Ugotovi, ali sta dani grupi izomorfni in poišči eksplicitni izomorfizem, če sta:~~

~~(a) $\mathbb{Z}_6$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$,~~

~~(b) $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$,~~

~~(c) $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.~~

~~*Rešitev:* (a) Imamo Abelovi grupi reda 6:~~

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

~~Grupa $\mathbb{Z}_6$ je ciklična z generatorjem 1, medtem ko pri grupi $\mathbb{Z}_2 \times \mathbb{Z}_3$ ni na prvi pogled jasno, ali je generirana z enim elementom. Hitro pa lahko preverimo, da jo generira element $(1, 1)$, kar pomeni, da lahko definiramo izomorfizem $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ s predpisi:~~

$$\phi(1) = (1, 1),$$
$$\phi(2) = (0, 2),$$
$$\phi(3) = (1, 0),$$
$$\phi(4) = (0, 1),$$
$$\phi(5) = (1, 2),$$
$$\phi(0) = (0, 0).$$

~~(b) Sedaj imamo dve Abelovi grupi reda 4:~~

$$\mathbb{Z}_4 = \{0, 1, 2, 3\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Grupa $\mathbb{Z}_4$ je spet ciklična z generatorjem 1, medtem ko grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ tokrat ni ciklična. Če bi namreč bila, bi obstajal element reda 4. Preverimo pa lahko, da so vsi elementi, razen enote, reda 2, kar pomeni, da grupi $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$ nista izomorfni.

(c) Grupi $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ sta reda 30. Ker so 2, 3 in 5 paroma tuja števila, ima element $(1,1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ red 30, zato lahko definiramo izomorfizem $\phi : \mathbb{Z}_{30} \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ s predpisom:

$$\phi(k) = (k \mod (2), k \mod (3), k \mod (5)).$$

Opomba: Grupi $\mathbb{Z}_{mn}$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ sta izomorfni natanko takrat, ko sta števili m in n tuji. V tem primeru je izomorfizem $\phi : \mathbb{Z}_{mn} \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ dan s predpisom

$$\phi(k) = (k \mod (m), k \mod (n)).$$

Od tod med drugim sledi, da za vsako končno Abelovo grupo G obstaja izomorfizem

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}},$$

kjer so p_i praštevila, ki delijo red grupe G. Isto praštevilo se lahko ponovi večkrat, kot smo videli v primeru $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. □

(8) Poišči vse Abelove grupe reda 80.

Rešitev: Razcep števila 80 se glasi

$$80 = 5 \cdot 2^4.$$

Če je G Abelova grupa reda 80, je torej produkt faktorjev oblike $\mathbb{Z}_5, \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_8$ in $\mathbb{Z}_{16}$. Različne možnosti so:

$$\begin{aligned}
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_{16}, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_2, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_4, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

□

(9) Zapiši grupno tabelo za operacijo v grupi $\mathbb{Z}_{10}^*$. Kateri grupi je izomorfna grupa $\mathbb{Z}_{10}^*$?

Rešitev: Z oznako $\mathbb{Z}_n^*$ označimo grupo (za množenje) obrnljivih elementov v kolobarju $\mathbb{Z}_n$. Ta grupa ima $\phi(n)$ elementov, njena enota pa je element 1.

V našem primeru je

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\},$$

grupna tabela pa se glasi

$\circ$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Iz tabele lahko preberemo, da ima element 3 red 4, kar pomeni, da je

$$\mathbb{Z}_{10}^* \cong \mathbb{Z}_4.$$

□

(10) Dana je grupa G z grupno tabelo

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Kateri znani grupi je izomorfna grupa G?

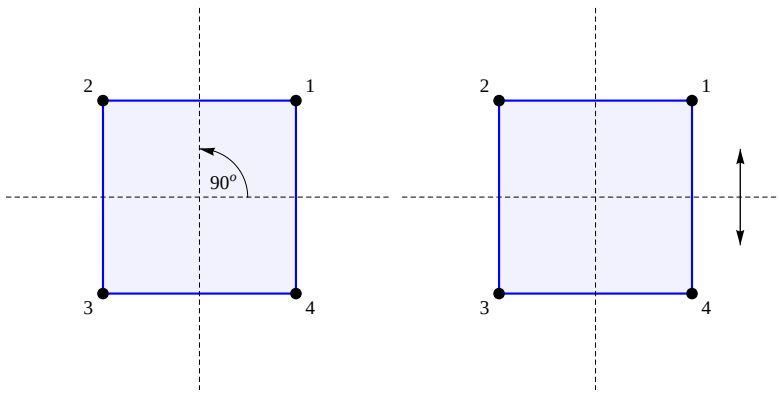
Rešitev: Iz tabele je razvidno, da je e enota grupe G in da je G komutativna. Torej je G izomorfna bodisi grupi $\mathbb{Z}_4$ bodisi grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$. Če bi bila G ciklična grupa, bi moral obstajati element reda 4, kar pa vidimo, da ni res. Od tod sledi

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

(11) Opiši grupo izometrij kvadrata.

Rešitev: Obstaja osem izometrij kvadrata. Identiteta, tri rotacije in štiri zracaljenja.



Izkaže se, da lahko vsako izmed teh izometrij izrazimo z eno rotacijo in z enim zrcaljenjem. Izberemo lahko na primer:

- $a = (1\,2\,3\,4)\ldots$ rotacija za 90° v pozitivni smeri,
- $b = (1\,4)(2\,3)\ldots$ zrcaljenje preko vodoravnice.

Preostale netrivialne izometrije so potem:

- $a^2 = (1\,3)(2\,4)\ldots$ rotacija za 180°,
- $a^3 = (1\,4\,3\,2)\ldots$ rotacija za 270°,
- $ab = (1\,3)(2)(4)\ldots$ zrcaljenje preko simetrale sodih kvadrantov,

- $a^2b = (1\,2)(3\,4)\ldots$ zrcaljenje preko navpičnice,
- $a^3b = (2\,4)(1)(3)\ldots$ zrcaljenje preko simetrale lihih kvadrantov.

Grupi izometrij kvadrata rečemo diedrska grupa reda 8 in jo označimo z D_8. Dejstvo, da lahko vsako izometrijo izrazimo z a in b, pomeni, da je grupa D_8 generirana z elementoma a in b, ki pa še zadoščata nekim pogojem. Reda elementov a in b nam dasta pogoja $a^4 = 1$ in $b^2 = 1$. Poleg teh dveh pa velja še zveza $bab = a^3$. Kompaktno lahko te pogoje strnemo v naslednjem zapisu

$$D_8 = \{a, b \,|\, a^4 = 1,\, b^2 = 1,\, bab = a^3\}.$$

Opomba: V splošnem ima grupa izometrij pravilnega n-kotnika $2n$ elementov. Poleg identične preslikave ima še $n-1$ rotacij in pa n zrcaljenj. Označimo jo z D_{2n} in ji rečemo diedrska grupa reda $2n$. V primeru $n = 3$ je grupa D_6 izomorfna grupi S_3. □

(12) Poišči vse podgrupe grup $\mathbb{Z}, \mathbb{Z}_{10}$ in Q.

Rešitev: Podmnožica H grupe G je *podgrupa* grupe G, če je zaprta za množenje in za invertiranje. Pri tem uporabljamo oznako $H \leq G$.

Podgrupe grupe $\mathbb{Z}$:

Množica, ki vsebuje samo enoto $\{0\}$ je zmeraj podgrupa v vsaki grupi. Tej podgrupi rečemo trivialna podgrupa.

Naj bo sedaj H netrivialna podgrupa grupe $\mathbb{Z}$. Potem je za vsak $x \in H$ tudi $-x \in H$, zato obstaja neko naravno število, ki leži v H. Označimo z n najmanjše naravno število, ki leži v H. Ker je H zaprta za seštevanje, so potem vsi večkratniki števila n tudi v H, pokazali pa bomo, da so to natanko vsi elementi H.

Če bi namreč obstajal $m \in H$, ki ni večkratnik n, bi bil največji skupni delitelj d števil m in n manjši od n. Iz teorije diofantskih enačb potem sledi, da bi morala obstajati $a, b \in \mathbb{Z}$, da bi veljalo

$$an + bm = d,$$

od koder pa bi sledilo $d \in H$. To pa je v nasprotju z minimalnostjo števila n.

Vsaka podgrupa grupe $\mathbb{Z}$ je torej oblike

$$H_n = n\mathbb{Z},$$

za nek $n \geq 0$. Pri $n = 0$ dobimo trivialno podgrupo, pri $n = 1$ pa kar celo grupo.

Podgrupe grupe $\mathbb{Z}_{10}$:

Grupa $\mathbb{Z}_{10}$ ima štiri podgrupe. Te so:

$$\begin{aligned} H_1 &= \{0\}, \\ H_2 &= \mathbb{Z}_{10}, \\ H_3 &= \{0, 5\} \cong \mathbb{Z}_2, \\ H_4 &= \{0, 2, 4, 6, 8\} \cong \mathbb{Z}_5. \end{aligned}$$

Podgrupe kvaternionske grupe Q:

Kvaternionska grupa Q ima 8 elementov

$$Q = \{1, -1, i, -i, j, -j, k, -k\}.$$

Elementi $\pm i, \pm j, \pm k$ se množijo analogno, kot se vektorsko množijo vektorji $\pm\vec{i}, \pm\vec{j}, \pm\vec{k}$, poleg tega pa veljajo še enakosti

$$(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1.$$

Podgrupe kvaternionske grupe so:

$$\begin{aligned} H_1 &= \{0\}, \\ H_2 &= Q, \\ H_3 &= \{1, -1\} \cong \mathbb{Z}_2, \\ H_4 &= \{1, i, -1, -i\} \cong \mathbb{Z}_4, \\ H_5 &= \{1, j, -1, -j\} \cong \mathbb{Z}_4, \\ H_6 &= \{1, k, -1, -k\} \cong \mathbb{Z}_4. \end{aligned}$$

□

(13) Dokaži, da je vsaka grupa praštevilskega reda ciklična.

Rešitev: Denimo, da ima grupa G red p, kjer je p praštevilo in naj bo $a \in G$ nek element, ki ni enota grupe. Ker red poljubnega elementa deli red grupe, mora imeti element a red p. To pa pomeni, da velja

$$G = \{e, a, a^2, a^3, \ldots, a^{p-1}\}$$

oziroma, da je G ciklična grupa z generatorjem a.

~~Z dosedaj zbranim znanjem lahko zapišemo seznam vseh grup do reda 10.~~

~~red~~	~~grupe~~
~~1~~	~~$\{0\}$~~
~~2~~	~~$\mathbb{Z}_2$~~
~~3~~	~~$\mathbb{Z}_3$~~
~~4~~	~~$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$~~
~~5~~	~~$\mathbb{Z}_5$~~
~~6~~	~~$\mathbb{Z}_6$, S_3~~
~~7~~	~~$\mathbb{Z}_7$~~
~~8~~	~~$\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_8, Q~~
~~9~~	~~$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$~~
~~10~~	~~$\mathbb{Z}_{10}$, D_{10}~~

□

~~(14) V grupi $\mathbb{Z}_{11}^*$ izračunaj diskretna logaritma $\log_2 5$ in $\log_6 2$.~~

~~*Rešitev:* Grupa $\mathbb{Z}_{11}^*$ je ciklična grupa reda 10. Če je a poljuben generator grupe $\mathbb{Z}_{11}^*$, mora veljati~~

$$\mathbb{Z}_{11}^* = \{1, a, a^2, \ldots, a^9\}.$$

~~Za vsak generator a grupe $\mathbb{Z}_{11}^*$ in poljuben $k \in \mathbb{Z}_{11}^*$ lahko definiramo diskretni logaritem $\log_a k$ kot število, ki je implicitno določeno s pogojem~~

$$a^{\log_a k} = k.$$

(8) Poišči vse podgrupe grupe $\mathbb{Z}_2 \times \mathbb{Z}_4$ in S_3.

Rešitev:

Podgrupe grupe $\mathbb{Z}_2 \times \mathbb{Z}_4$ so:

$$
\begin{aligned}
H_1 &= \{(0,0)\}, \\
H_2 &= \mathbb{Z}_2 \times \mathbb{Z}_4, \\
H_3 &= \{(0,0),(1,0)\} \cong \mathbb{Z}_2, \\
H_4 &= \{(0,0),(0,1),(0,2),(0,3)\} \cong \mathbb{Z}_4, \\
H_5 &= \{(0,0),(0,2)\} \cong \mathbb{Z}_2, \\
H_6 &= \{(0,0),(1,2)\} \cong \mathbb{Z}_2, \\
H_7 &= \{(0,0),(1,1),(0,2),(1,3)\} \cong \mathbb{Z}_4, \\
H_8 &= \{(0,0),(1,2),(1,0),(0,2)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}
$$

Podgrupe grupe S_3 so:

$$
\begin{aligned}
H_1 &= \{(1)(2)(3)\}, \\
H_2 &= S_3, \\
H_3 &= \{(1)(2)(3),(1\,2)(3)\} \cong \mathbb{Z}_2, \\
H_4 &= \{(1)(2)(3),(1\,3)(2)\} \cong \mathbb{Z}_2, \\
H_5 &= \{(1)(2)(3),(1)(2\,3)\} \cong \mathbb{Z}_2, \\
H_6 &= \{(1)(2)(3),(1\,2\,3),(1\,3\,2)\} \cong \mathbb{Z}_3.
\end{aligned}
$$

(9) Grupa G je podana s tabelo

$\circ$	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	e	c	g	b	f	1	d
b	b	c	f	1	e	g	d	a
c	c	g	1	a	f	d	b	e
d	d	b	e	f	a	c	g	1
e	e	f	g	d	c	1	a	b
f	f	1	d	b	g	a	e	c
g	g	d	a	e	1	b	c	f

.

(a) Poišči rede vseh elementov grupe G.

(b) Ugotovi, kateri znani grupi je izomorfna grupa G in poišči eksplicitni izomorfizem.

Rešitev:

(a) Redi elementov grupe G so: $\mathrm{red}(1) = 1$, $\mathrm{red}(a) = 4$, $\mathrm{red}(b) = 8$, $\mathrm{red}(c) = 8$, $\mathrm{red}(d) = 8$, $\mathrm{red}(e) = 2$, $\mathrm{red}(f) = 4$ in $\mathrm{red}(g) = 8$.

(b) Grupa G je izomorfna grupi $\mathbb{Z}_8$. Eksplicitni izomorfizem $\phi : G \to \mathbb{Z}_8$ je podan s predpisom:

$$\begin{aligned}\phi(1) &= 0,\\ \phi(a) &= 2,\\ \phi(b) &= 7,\\ \phi(c) &= 1,\\ \phi(d) &= 5,\\ \phi(e) &= 4,\\ \phi(f) &= 6,\\ \phi(g) &= 3.\end{aligned}$$

(10) Poišči največja skupna delitelja naslednjih Gaussovih celih števil:

(a) $a = 11 + 3i$ in $b = 1 + 8i$,

(b) $a = 32 + 9i$ in $b = 4 + 11i$.

Rešitev:

(a) $D(a, b) = 1 + 2i$,

(b) $D(a, b) = 1$.

(11) Na kolobarju $K = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ definirajmo normo s predpisom

$$N(a + b\sqrt{5}i) = a^2 + 5b^2.$$

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

(b) Ali v kolobarju K velja izrek o enolični faktorizaciji?

Rešitev:

(a) Obrnljiva sta elementa 1 in -1.

(b) Ne. Protiprimer je $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.

(12) (a) Pokaži, da je polinom $p(x) = x^4 + x^3 + 1$ nerazcepen v kolobarju $\mathbb{Z}_2[x]$.

(b) Poišči vse nerazcepne kvadratne polinome v kolobarju $\mathbb{Z}_3[x]$.

Rešitev: Če se omejimo na polinome z vodilnim koeficientom 1, so v kolobarju $\mathbb{Z}_3[x]$ nerazcepni naslednji kvadratni polinomi:

$$\begin{aligned}p_1(x) &= x^2 + 1,\\ p_2(x) &= x^2 + x + 2,\\ p_3(x) &= x^2 + 2x + 2.\end{aligned}$$